

CELEBRATING OUR 5TH YEAR



20

25

September 4-7, 2025
Fairmont Chicago

BlueTeamCon.com

CELEBRATING OUR 5TH YEAR



20

25

CONTENTS

CODE OF CONDUCT

ADVISORY BOARD

CFP BOARD MEMBERS

VENUE

KEYNOTE SPEAKER

SCHEDULE - SATURDAY

SCHEDULE - SUNDAY

TRAININGS

LABS

VILLAGES

PARTNERS

SPONSORS

FOOD STUFFS

CPE INFORMATION

BLUE TEAM CON SCHOLARSHIP

SPEAKERS - 50 MINUTES

SPEAKERS - 25 MINUTES



Mission

Cultivate a community-driven experience that focuses on educating and connecting anyone interested in defensive cybersecurity through a safe, inclusive, friendly, and fun ecosystem.

Welcome to Blue Team Con

Blue Team Con Attendees,

Welcome to the fifth year of Blue Team Con! It's an incredible milestone – one only possible because of the community that gathers here year after year. What started as a simple idea, that defenders deserve a space to meet, discuss, and share, has now become a thriving tradition. Each year we've adapted, grown, and celebrated the role of the Blue Team together, and this year we take another step forward.

Blue Team Con has always been about making connections and sharing knowledge, but as we reach this milestone, it also gives time for reflection. We've seen our industry change rapidly, from the threats we face to the tools we use, but that one thing has remained constant: the value of defenders coming together. Whether you are a first-time attendee or a long-time supporter; whether you come from policy, engineering, or even apply your offensive knowledge to create a better defense, your presence here strengthens the community we are all building.

This year, you'll notice new additions to the program: from a third talk track to expanded labs, CTFs, and even a sponsored attendee appreciation dinner, we've worked hard to bring more chances for hands-on learning, peer collaboration, and community building. Whether in training, villages, unconference sessions or lobbycon chats, we hope to create opportunities for every kind of learner and contributor.

Blue Team Con is an effort of love from all of us - the board, volunteers, speakers, sponsors, trainers, and villages - but most importantly, Blue Team Con is about you: the professionals, students, leaders, and builders who dedicate yourselves to protecting systems, technology, and the people that use them every day. Help us celebrate your work, your passion, and your willingness to share.

Thank you for being part of this fifth year. Together, we continue to grow stronger as defenders.

Welcome to Blue Team Con 2025!

Tillery

Advisory Board Member
Blue Team Con

Code of Conduct

In case of a life-threatening emergency, please call 9-1-1 immediately.

Who is Our Code of Conduct For?

Blue Team Con aims to be a conference for EVERYONE. We expect all event attendees, speakers, sponsors, partners, vendors, facilities staff, committee, and board members to agree to and follow the code of conduct guidelines. Should you have questions, concerns or doubts about whether an action would be in violation of the Code of Conduct, please contact us at board@blueteamcon.com.

Publication

The Code of Conduct is available online at <https://www.blueteamcon.com/about/code-of-conduct/>. Printed versions of the Code of Conduct will be made available at all official Blue Team Con events and activities, and links to the Code of Conduct will be supplied on all official Blue Team Con community forums and chat rooms.

Purpose

Security events present opportunities to learn, share knowledge and network. As a security event organizer, we believe these events should represent a safe, enjoyable and inclusive environment for all people, irrespective of gender, race, ethnicity, age, sexuality, religion, disability, socioeconomic background, experience, size, shape and so on. No one should undergo harassment, bullying, or abuse. Such behavior is deemed unacceptable and will be addressed. We will, when possible, address the behavior directly. We will apply consistent, specific sanctions as required, regardless of the circumstances to ensure they do not recur. This code of conduct explains what we mean by unacceptable behavior and it outlines the steps someone subjected to such behavior at an event can take to report it.

Why Do We Need a Code of Conduct?

Unfortunately, unwanted behavior still occurs, and while harassment metrics are yet to be introduced and measured, anecdotal reports are widespread and have been reported in the media and social media platforms for years. This has reportedly resulted in increased dissatisfaction and non-attendance by women, nonbinary, people of color, and other minorities who feel disenfranchised and threatened. The purpose of this code of conduct is to get participants fully aligned on what constitutes unacceptable behavior, how the aggrieved can report it, and what will be done about it by Blue Team Con organizers and staff.

How We Define Acceptable and Unacceptable Behavior?

People's interpretation of acceptable or unacceptable behavior is subjective and influenced by personal experience, religion, and cultural background. That's why we believe it's important to define what we mean by both.

Code of Conduct

Acceptable Behavior

As an event organizer, we expect everyone to be professional and respectful to others at all times. Everyone should be aware of the impact their behavior can have on others.

We ask that you:

- » Respect the venue, the staff, and any equipment you may be allowed to use.
- » Be courteous and well-mannered when speaking to someone or engaging with them.
- » Treat people the same way you would like to be treated.
- » Respect someone's personal space and body – when someone says no, it is no, not maybe.

Unacceptable Behavior

Unacceptable behavior is offensive in nature – it disturbs, upsets or threatens. It lowers self-esteem or causes overwhelming torment.

It can take, but is not limited to, the following forms:

- » Derogatory, inflammatory or discriminatory language, comments, or conduct
- » Engineered episodes of intimidation, aggressive actions, or repeated gestures
- » Repetitive heckling and disruption of talks
- » Wearing of inappropriate attire (e.g., sexualized clothing)
- » Using sexual images or sex toys in public spaces
- » Inappropriate photography or recordings (where inappropriate is defined as used later in a sexual, derogatory, defamatory manner, or for exploitation)
- » Stalking or following
- » Persistent and unwanted sexual advances
- » Unwanted physical contact
- » Intentional use of improper/incorrect pronouns
- » Contact with assistive devices or services animals without affirmative consent.
- » Encouraging any of the above behaviors

Alcohol and Other Substances

The following substance-related conduct is also prohibited:

- » Excessive or irresponsible consumption of alcohol;
- » Possession, sale, or use of marijuana, any marijuana derivative, or any other illicit or controlled substance other than under the prescription and supervision of a licensed physician (Blue Team Con prohibits the use of marijuana and derivative products at its events, even when validly prescribed by a licensed state authority. Blue Team Con may require documentary proof of other prescriptions.);

Code of Conduct

- » Providing or participating in the service of alcohol to anyone under the legal drinking age, in accordance with applicable laws and regulations; and
- » Smoking, except in designated areas.

Blue Team Con's contracted venue providers reserve the right to further prohibit the use or possession of drugs (legal, prescription, or other), tobacco, or other substances on their property, per the terms of the rental contract.

Photo, Video, and Recording Policy

Ensure you have permission from anyone you photograph or record. This includes those in the background of your shot. "Crowd shots" from the front (facing the crowd) are not allowed. If you've accidentally taken a picture without permission, delete it. If you are asked by a participant to delete/blur a picture they did not give you permission to take, please do so immediately.

Blue Team Con media staff will be taking photos of the event and is the only one allowed to take "crowd shots" and general room photos. Blue Team Con media staff will work towards taking "crowd shots" with least amount of identifying faces as possible, and any close-ups with approval. Blue Team Con reserves the right to utilize photography taken by media staff in advertising, marketing, and promotional materials. If you do not want to be in a photo, please notify the Blue Team Con media staff or inform us at any point at info@blueteamcon.com.

Upon a first infraction, you will receive one warning from Blue Team Con Staff. Upon a second infraction you will be asked to give up your device to Blue Team Con Safety for the duration of the event or to leave the event with your device. You may return once your device is secured offsite.

How to Report Unacceptable Behavior

Option 1: If you feel safe to do so, speak up. See it, say it, sort it.

If you are disrespected, or witness this happening to someone else, engage politely with the person involved, if you feel able to, and let them know that you find their behavior unacceptable and offensive. Sometimes the best way to change unacceptable behavior is by bringing it to the perpetrator's attention and giving them an opportunity to acknowledge this and apologize.

Option 2: Report it to Blue Team Con staff via any of the following ways:

Inform a member of our event staff who can be identified by their badge.

Email us at safety@blueteamcon.com.

Complete our event feedback form (this can be done anonymously), which will be sent out to all attendees after the event concludes.

Code of Conduct

When reporting, please provide as much detail as possible, preferably:

- » Your name and contact details (email, cell/mobile phone, and address).
- » The time it occurred.
- » The place it occurred.
- » The names and contact details of any witnesses.
- » The outcome you are expecting (e.g. letter of apology, steps taken to prevent a similar instance from occurring, etc.).

Note: you can remain anonymous if you so wish and providing any of the above information is optional. Anyone can report harassment. If you are being harassed, notice that someone else is being harassed, or have any other concerns, please report the situation to us as indicated above.

We don't have a time limit for reporting unacceptable behavior, although we encourage you to do it as quickly as possible, as it can be difficult to obtain accurate witness statements the longer time passes. If you report unacceptable behavior more than three months after an incident, you should explain why as it may impact the ability to respond accordingly. We will consider your explanation and then endeavor to deal with your report.

How We Handle Unacceptable Behavior

We are committed to ensuring that you experience a positive, enjoyable and inclusive event. We strive for customer service excellence when reporting unacceptable behavior. That's why, for the duration of our event, we will have a number of reporting mechanisms available (e.g., suitable informed event staff, event feedback forms, etc.). When you report unacceptable behavior to us, we will respond promptly and with care, consideration, and respect. Our process does not replace nor remove the formal mechanisms available to you as an individual to report inappropriate or offensive behavior such as making a police report. Our process is as follows:

- » We will acknowledge your report and reply via email (if an email was sent) as soon as is practical.
- » We will perform a thorough investigation starting immediately.
- » We will not comment on your experience or perception of it.
- » We will keep it wholly professional and confidential.
- » We will treat all of the people involved fairly and objectively, irrespective of what our relationship with them is.
- » We will apply the appropriate sanctions/remediation (e.g., warnings, direction to learning resources on the topic of harassment, bullying or anti-social behavior, temporary or permanent suspensions, and if necessary, report them to the police). We will take into consideration your wishes in any enforcement.
- » We will suggest measures we can take to ensure incidents of this nature do not recur at future events.
- » We reserve the right to remove people from the event or prevent people from joining the event.
- » We will not name and shame individuals, but we will analyze our progress with regards to unacceptable behavior and publish our findings annually on our website.

Advisory Members of the Board



Phoenix Fier

phoenix@blueteamcon.com



Frank McGovern

frank@blueteamcon.com



Alyssa Miller

alyssa@blueteamcon.com



Becky Selzer

becky@blueteamcon.com



Stel Valavanis

stel@blueteamcon.com



Tillery

tillery@blueteamcon.com

CFP Review Board Members



Kaylee Burns



Kevin Jackson



Chris Lemmon



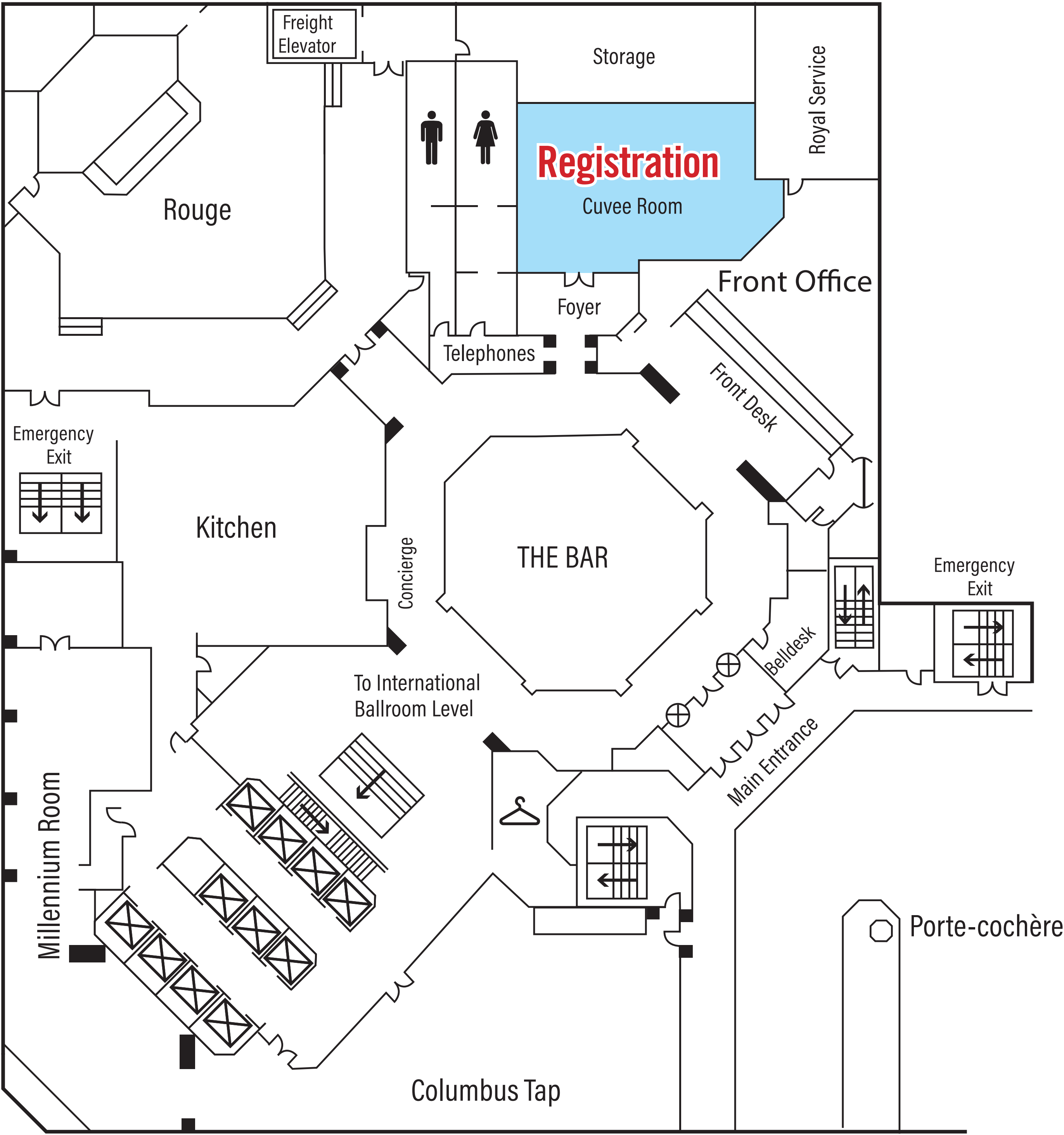
Xena Olsen



Lauren Rodgers

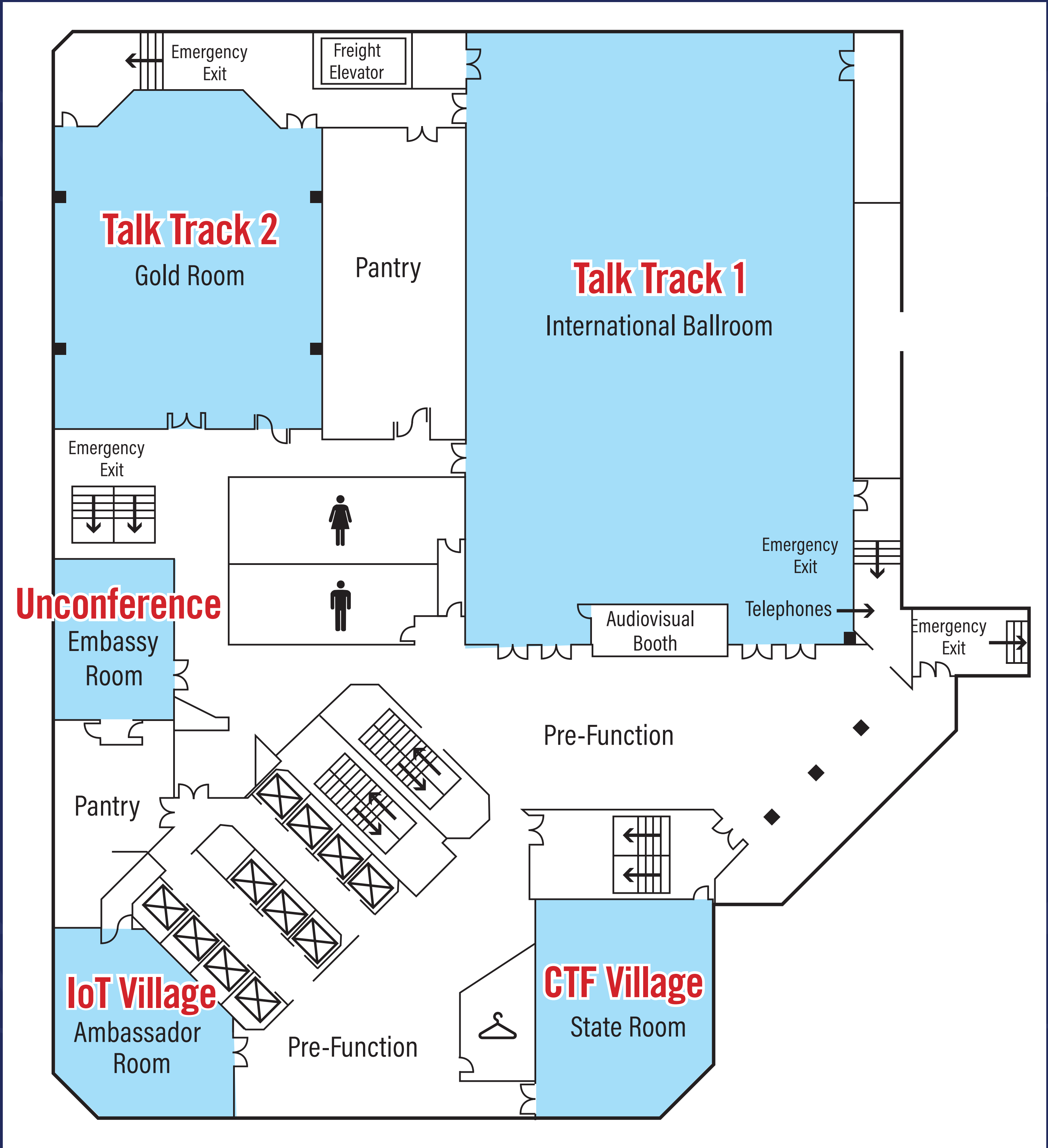
Venue

Level ONE



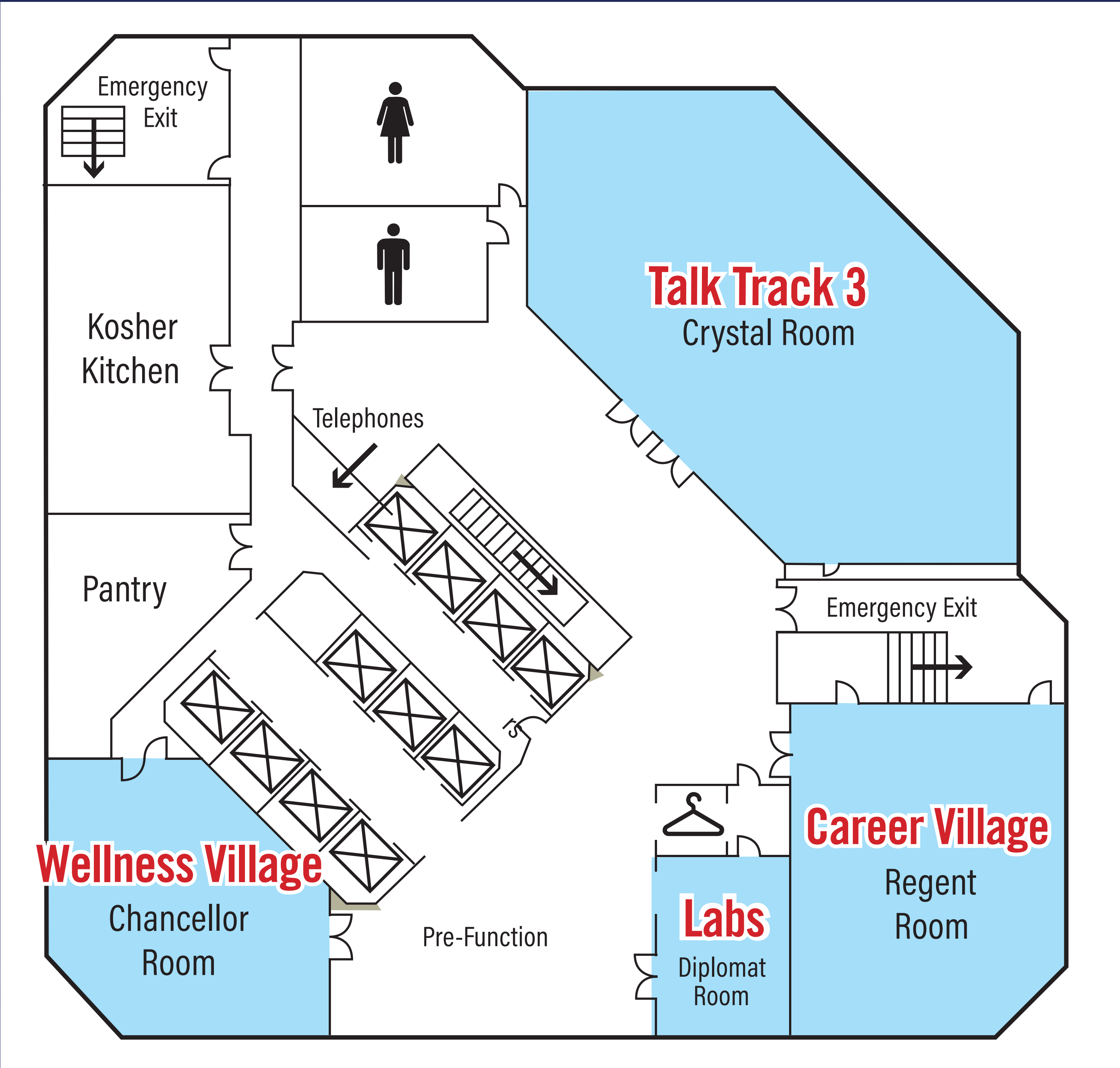
Venue

Level TWO



Venue

Level THREE





**KEYNOTE
SPEAKER**

Jake Williams

**VP OF R&D AT
HUNTER STRATEGY**

Talk Title

***Less Resources, More Impact:
Doing More With Less In Cybersecurity***

If you're not being asked to do more with less in your cyber program right now, count yourself among the lucky few. But don't worry: AI will save the day! Just kidding, I'm not that stupid (even if your CTO is). In this talk, we'll discuss zero/low cost strategies for force multiplying your efforts in cybersecurity. This session will focus on both building efficient processes and low-cost tools to gain needed visibility for the blue team when budgets for new licenses are tight to non-existent. Even organizations rolling in cash will still find takeaways for advancing their programs, even though we know that's the vast majority of us.

hunterstrategy.net

LEARN MORE

H

Thursday, September 4

Training Registration Only: 7:00 am to 10:00 am
(Aon Center, Next Door to The Fairmont)

Attendees with a training badge should check in at the front desk of Aon.
You will be directed to the Registration Desk in the Microsoft Technology Center.

Training Breakfast: 8:15 am to 8:45 am

Training: 9:00 am to 5:00 pm

Training Lunch: 12:00 pm to 1:00 pm

Friday, September 5

Training Breakfast: 8:15 am to 8:45 am

Training: 9:00 am to 5:00 pm

Training Lunch: 12:00 pm to 1:00 pm

General Conference Registration: 3:00pm to 9:00pm
(Fairmont Cuvee Room, 1st Floor)

Saturday, September 6

Registration: 7:00am to 7:00pm (Fairmont Cuvee Room, 1st Floor)

Swag: 11:00am to 4:00pm

Join us for these after hours events

A close-up image of a custom-built electronic circuit board with various colored buttons (yellow, green, red, blue) and wires, resembling a game controller or a specialized keyboard.

HACKER
CHARLATAN
GAMESHOW

7:30 PM TO 9:00 PM

Held in Talk Track 2

A DJ in a blue hoodie is performing at a DJ booth with two turntables. The scene is lit with vibrant purple and blue stage lights, and silhouettes of people are visible in the background.

NETWORKING
EVENT AND PARTY
with DJ Cillic

Drinks (Drink Tickets Required) and Food

9:00 pm to 1:00 am

Held in Talk Track 1

An illustration showing hands playing board games on a table. The scene is lit with colorful, neon-like lights in shades of purple, blue, and green, creating a vibrant, cyber-themed atmosphere.

SATURDAY NIGHT
SOBER GAMES

9:00 pm to 1:00 am

Hosted by Sober in Cyber

Tunes by DJ Selina Style

Mocktails (Drink Tickets Required) and Food

No Alcohol Allowed

9:15pm: Ghost Hunt in The Congress Hotel – RPG

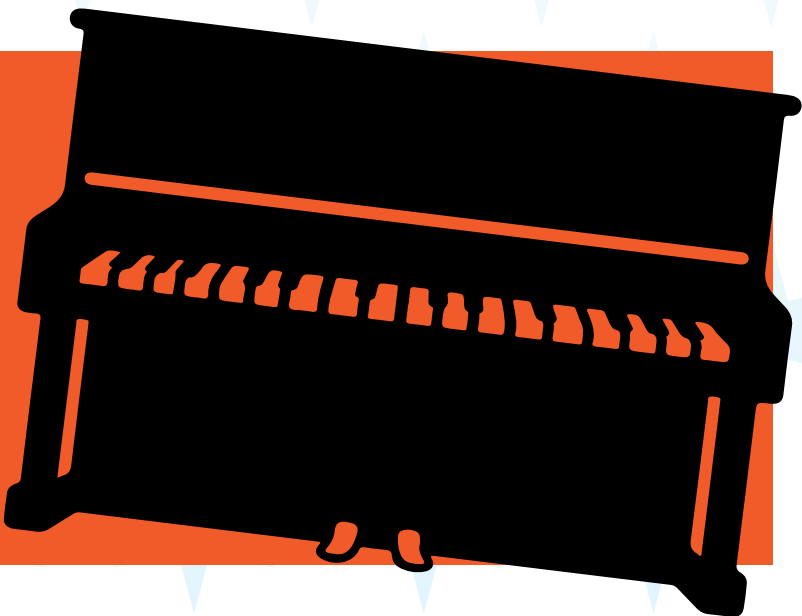
9:30pm: Backdoors & breaches – Tabletop

Held in Talk Track 3

PIANOBAR CON WITH GARY RIMAR

LAIDBACK PIANO MUSIC LISTENING THAT WILL TRANSITION
INTO AN OPTIONAL SING-ALONG.

8:30 to ???



Saturday, September 6

Registration: 7:00 am to 7:00 pm (Fairmont Cuvee Room, 1st Floor)
Swag: 11:00am to 4:00pm

Talk Track 1

Sponsored by  Microsoft
50-Minute Talks – International Room

9:00 AM	Opening Ceremonies with Blue Team Con Advisory Board
9:30 AM	Keynote: “Less Resources, More Impact: Doing More With Less In Cybersecurity” with Jake Williams
11:00 AM	“SkyScalpel: Making & Breaking {“Policy”: “Obfu0075scA**Tion”} in the Cloud” with Abian Morina
12:00 AM	“Ransomware Rampage: Gamifying Your Incident Response Playbook” with Anushree Vaidya
1:00 PM	“.e”X”es and “O”auths (They Haunt Me): An In-Depth Analysis of OAuth & OIDC Misconfigurations and Token Replay Attack” with Darryl G. Baker
2:00 PM	“Ensuring Data Integrity in Incident Response: Tools and Techniques for Forensically Sound Log Extraction” with Colin Meek
3:00 PM	“Transforming Cyber Risk Assessments Through Continuous Validation” with Irina Loktionova and Chris Oshaben



Saturday, September 6

ctd.

50-Minute Talks – International Room

- 4:00 PM
- “Leading Multi-Generational Cybersecurity Teams with Transparency, Candor, and Empathy”
with Mike Glatz

“Unseen but Not Unheard: Exposing the Cases of CSS Abuse in Email Threats and Fortifying Defenses” with Omid Mirzaei

- 9:00 PM
- Networking Event and Party
with DJ Cillic

Drinks and Food - Drink tickets required
(Held in Talk Track 1)

Saturday, September 6

Registration: 7:00 am to 7:00 pm (Fairmont Cuvee Room, 1st Floor)
Swag: 11:00am to 4:00pm

Talk Track 2

25-Minute Talks – Gold Room

10:30 AM	–	“Detection Opportunities for Countering Remote Employment Fraud: A Phase-based Strategy” with Alex Orleans and Jonathan Heckinger
11:00 AM	–	“What Now? Navigating the Transition from Engineer to Manager” with Cory Roop
11:30 AM	–	“Building a Threat Hunting Program from the Ground Up” with Ryan Fried and Estefania Michael
12:00 PM	–	“Technical Writers: Your Cybersecurity Secret Weapon” with Jennifer Miller
12:30 PM	–	“Foundations of Resilience: Mastering the Business Impact Analysis” with Jeremy Croghan
1:00 PM	–	“DFIR-as-Code: Scaling Incident Response Beyond Human Limits” with Justin Borland
1:30 PM	–	“LLM-Powered Vulnerability Management Operations: Use Cases and Success Stories” with Cong Zheng and Darcy Meyer
2:00 PM	–	“Securing Sideways: Thwarting Lateral Movement, with no extra software!” with R. Tyler Schroder
2:30 PM	–	“How Attackers are using AI and how to defend against them, by an incident responder turned AI researcher.” with Eyal Fisher

Saturday, September 6

ctd.

25-Minute Talks – Gold Room

- 3:00 PM
- “Decoding Dyslexia: Thriving in Cybersecurity with a Different Brain” with Caleb Grossnickle
- 3:30 PM
- “AI-Powered Cloud Security: Defending Cloud Workloads from Next-Gen Cyber Threats” with Advait Patel
- 4:00 PM
- “From Alerts to Action - LLMs for Explainability, Entity Analysis, and Escalation” with Scott Rodgers and Kevin Gonzalez
- 4:30 PM
- “Did I Do Thaaat? How not to “whoopsie” production away, a humanist risk-management-based approach.” with Daniel (Bogo) Bogomolny
- 5:00 PM
- “AI as the SOC Sidekick: Streamlining Security Without Stepping Over Humans” with Cliff Crosland
- 5:30 PM
- “Hidden Dangers Of AI In Developer Workflows: Navigating Security Risks with Human Insight” with Dwayne McDaniel
- 7:30 PM
- Hacker Charlatan Gameshow - Sponsored by OffSec, Hosted by Lintile (Held in Talk Track 2)
- 8:30 PM
- 3rd Floor Foyer
- PianoBar Con with Gary Rimar
- Laidback piano music listening that will transition into an optional sing-along.

Saturday, September 6

Registration: 7:00 am to 7:00 pm (Fairmont Cuvee Room, 1st Floor)
Swag: 11:00am to 4:00pm

Talk Track 3

25-Minute Talks – Crystal Room

10:30 AM	–	“A New Era of Brute Forcing in Active Directory” with David Horak
11:00 AM	–	“Why Your Email Matters” with BitsDanceForMe
11:30 AM	–	“Crypto Agility Lifecycle: A Backbone of a Resilient System” with Sandip Dholakia
12:00 PM	–	“Lies, Lures, and LLMs; Augmenting Cyber Deception with AI” with Dylan Shroll
12:30 PM	–	“The Cost of an Incident” with Amanda Draeger
1:00 PM	–	“Which Witch is Which - Navigating the Complicated World of Threat Actor Taxonomy” with Jeffrey Bell
1:30 PM	–	“Going Beyond Box Checking with Annual Pentests” with Sean “4dw@r3” Juroviesky
2:00 PM	–	Solving Secrets Sprawl Takes More Than Security: Why Machine Identity Is Everyone’s Problem with Dwayne McDaniel
2:30 PM	–	“Prescription for Security: Hardening Healthcare Email Against Advanced Threats” with Akash Parasumanna Sridhar
3:00 PM	–	“Introducing a password manager and policy” with L

Saturday, September 6

ctd.

25-Minute Talks – Crystal Room

3:30 PM

Things didn’t go as planned...
because you didn’t have a plan with ODDJOBB

4:00 PM

“Forged in Fire: Building Elite Cybersecurity Teams
with a Warrior’s Mindset” with Chris Reider

4:30 PM

“Maturing your cyber deception program: what’s
the plan?” with Suril Desai

5:00 PM

“Beyond the SLA: Measuring What Truly Matters”
with Swati Babbar and Kashif Memon

5:30 PM

Adventures in the Underland: Uncommon Hacker’s
Persistence Methods and Countermeasures
with Paula Januszkiewicz

9:00 PM

SOBER GAMES

Sponsored by Stellar Cyber

Hosted by Sober in Cyber

Mocktails and Food (Drink Tickets Required)

No Alcohol Allowed

Held in Talk Track 3

Sunday, September 7

Registration: 9:00 am to 1:00 pm (Fairmont Cuvee Room, 1st Floor)
Swag: 9:00 am to 1:00 pm

Talk Track 1

Sponsored by  Microsoft
50-Minute Talks – International Room

- 10:00 AM

“Breaking the CI/CD Chain: Security Risks in GitHub Actions” with Alexey Shchukarev
- 11:00 AM

“Can opposites attract? Domain Admins - meet Red Tenant” with Jake Hildreth and Eric Woodruff
- 12:00 PM

“Analysis without Paralysis: Mastering the Art of Investigation” with Terryn Valikodath
- 1:00 PM

“My Cyber Sense Is Tingling! Detection Engineering With Free Tools” with Matthew Gracie
- 2:00 PM

“You Need a Jay-z and a Beyoncé: How Sponsors and Mentors Can Supercharge Your Career in Cybersecurity” with Anthony Hendricks
- 3:30 PM

Closing Ceremonies

Sunday, September 7, 2025

Registration: 9:00am to 1:00pm (Fairmont Cuvee Room, 1st Floor)

Swag: 9:00am to 1:00pm

Talk Track 2

25-Minute Talks – Gold Room

10:00 AM	–	“Inside Ransomware Negotiations: Strategies and Insights from the Front Lines” with Matthew Leidlein
10:30 AM	–	“Business Logic Flaws: How to Prevent Them in Your Web Apps” with Antoine Carossio
11:00 AM	–	“The Death and Rebirth of Vulnerability Management” with HD Moore
11:30 AM	–	“Advancing from Individual Contributor to Cybersecurity Leader” with Kevin Bong
12:00 PM	–	“Introducing QELP: Parsing ESXi Logs for Incident Response” with Phalgun Kulkarni, Partha Alwar, and Mitchell Green
12:30 PM	–	“Agents of Change: Practical Adoption Framework for Agentic AI in Security Operations” with Ryan Rowcliffe
1:00 PM	–	“Adaptive Risk-Tiered Framework for Responsible AI Governance” with Sky Bell
1:30 PM	–	“Hunting Path Traversal in Open Source” with Nishant Jain
2:00 PM	–	“Flipping the Script: Threat Intelligence Mining of Ransomware Chat Leaks” with Mark Reibel
2:30 PM	–	“The False Sense of Security: Defense Becoming a Vulnerability” with Nathan Eades

Sunday, September 7

Registration: 7:00 am to 7:00 pm (Fairmont Cuvee Room, 1st Floor)
Swag: 11:00am to 4:00pm

Talk Track 3

50-Minute Talks – Crystal Room

10:00 AM	–	“Firewalls and Fire Alarms: What to Do When Your Best Defenses Go Up in Smoke” with Catherine Ullman
11:00 AM	–	“Inboxfuscation: Out-of-the-Box Mailbox Obfuscation - Turning BEC into Business Email Chaos” with Andi Ahmeti
12:00 PM	–	“Cultural Due Diligence: Hard Won Lessons from My Job Hunt” with Munish Walther-Puri
1:00 PM	–	“UNFAIR after all; Critical considerations for risk management frameworks” with Jack Burgess
2:00 PM	–	“Threat hunting in the browser” with Luke Jennings

Advanced Threat Hunting with AI Support



with

Paula Januszkiewicz
Founder & CEO at CQURE

This course provides a detailed, hands-on approach to modern threat hunting, focusing on identifying, tracing, and mitigating advanced cyber threats. Through case studies, real-world examples, and practical labs, participants will deepen their understanding of how to proactively defend against today's sophisticated attacks.

This course is designed for Security Analysts, IT Administrators, Incident Responders, and Threat Hunters who want to leverage AI in threat detection and response. By combining practical knowledge with AI-enhanced methodologies, participants will be better equipped to address the dynamic challenges of modern cybersecurity.

NOTE: This training is a 2-day (8 hours/day) course from September 4 to 5.

LEARN MORE

Detection as Code: Modernizing Threat Detection with Sigma



with

Patrick Bareiss

**Principal Threat Researcher
at Splunk**

This comprehensive training course explores the implementation of Detection as Code principles using Sigma, an open standard for SIEM rule definitions. Designed for security analysts, engineers, and architects, this course bridges the gap between traditional detection methods and modern DevOps practices. Participants will gain hands-on experience with industry-standard tools and methodologies that enable collaborative, consistent, and repeatable detection engineering. By leveraging Sigma's platform-agnostic approach, you can apply this training regardless of which SIEM or security tool your organization uses.

NOTE: This training is a 2-day (8 hours/day) course from September 4 to 5.

LEARN MORE

Hacking the Human OS: Using Gamified Social Engineering to Build Real Security Awareness



with
Jayson E. Street
Chief Adversarial Officer
at Secure Yeti

Traditional security awareness programs often fall short by relying on outdated methods that fail to engage employees or address real-world threats. This class takes a radically different approach—leveraging the same social engineering techniques used by adversaries, but in a safe, controlled, and gamified environment. Participants will explore how to circumvent human nature, not fight it, using immersive scenarios that challenge and reshape instinctual responses to manipulation.

NOTE: This training is a 1-day (8 hour) course on September 4.

LEARN MORE

Whiteboard Hacking – aka Hands-on Threat Modeling for Defenders



with

Robert Hurlbut

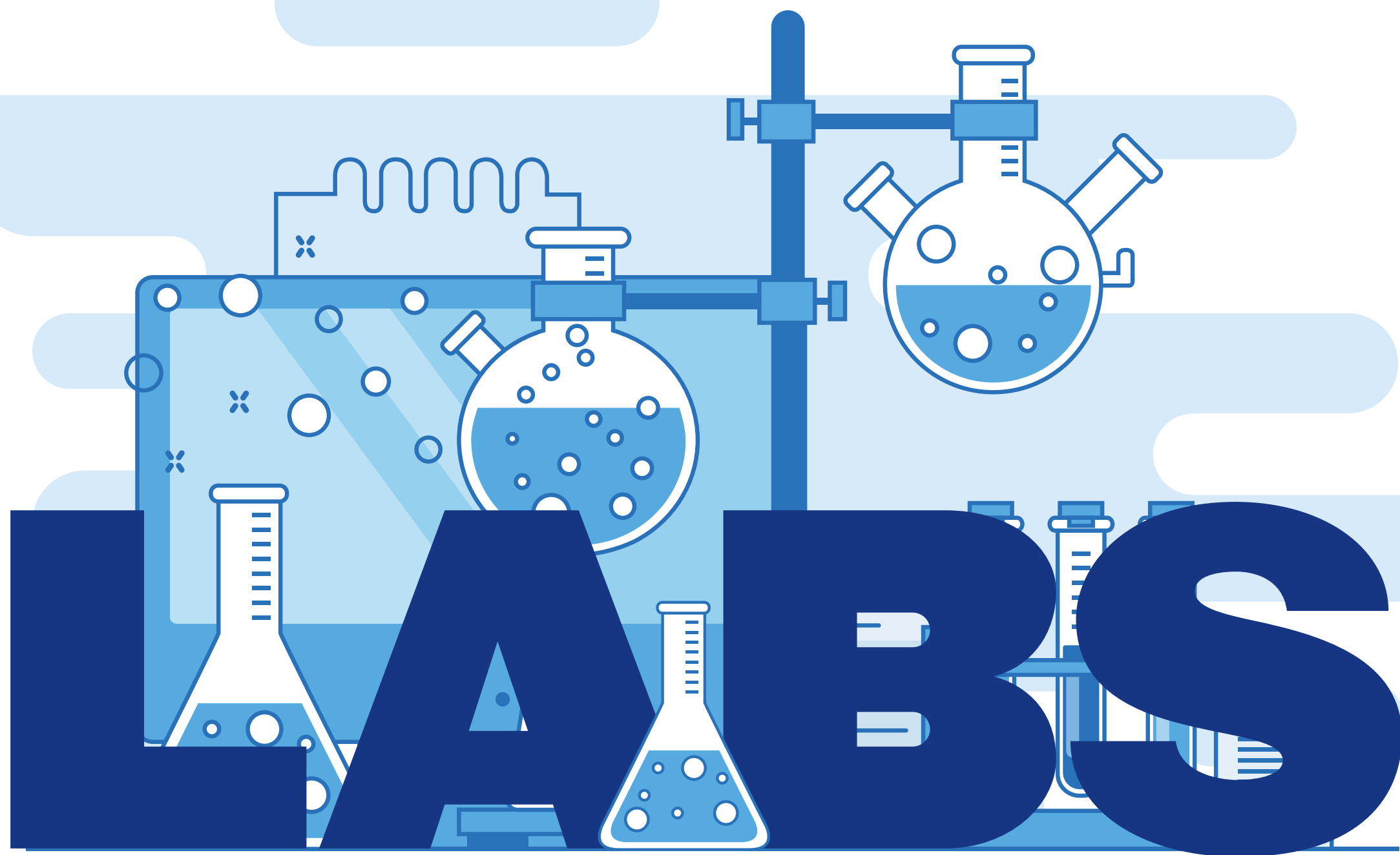
Principal Product

Security Architect at Toreon

This training takes you into the practical world of threat modeling, combining hands-on exercises and real-world scenarios. This hands-on threat modeling training offers an immersive experience, grounded in 25 years of practical expertise and refined through a decade of delivery at various conferences and organizations, avoiding a lecture-heavy approach. By the end of this training, you'll walk away not just with knowledge, but the ability to practice threat modeling effectively in your organization.

NOTE: This training is a 2-day (8 hours/day) course on September 4 & 5.

LEARN MORE



The Lab room is a place where attendees can get an in-depth walk-through or workshop through use cases with hands-on experience using cybersecurity products developed by our sponsors. Each Lab is open for two hours, so if there is a particular company or product that you'd like to see, make note of their Lab timeslot



HORIZON3.ai
~~TRUST~~ BUT VERIFY

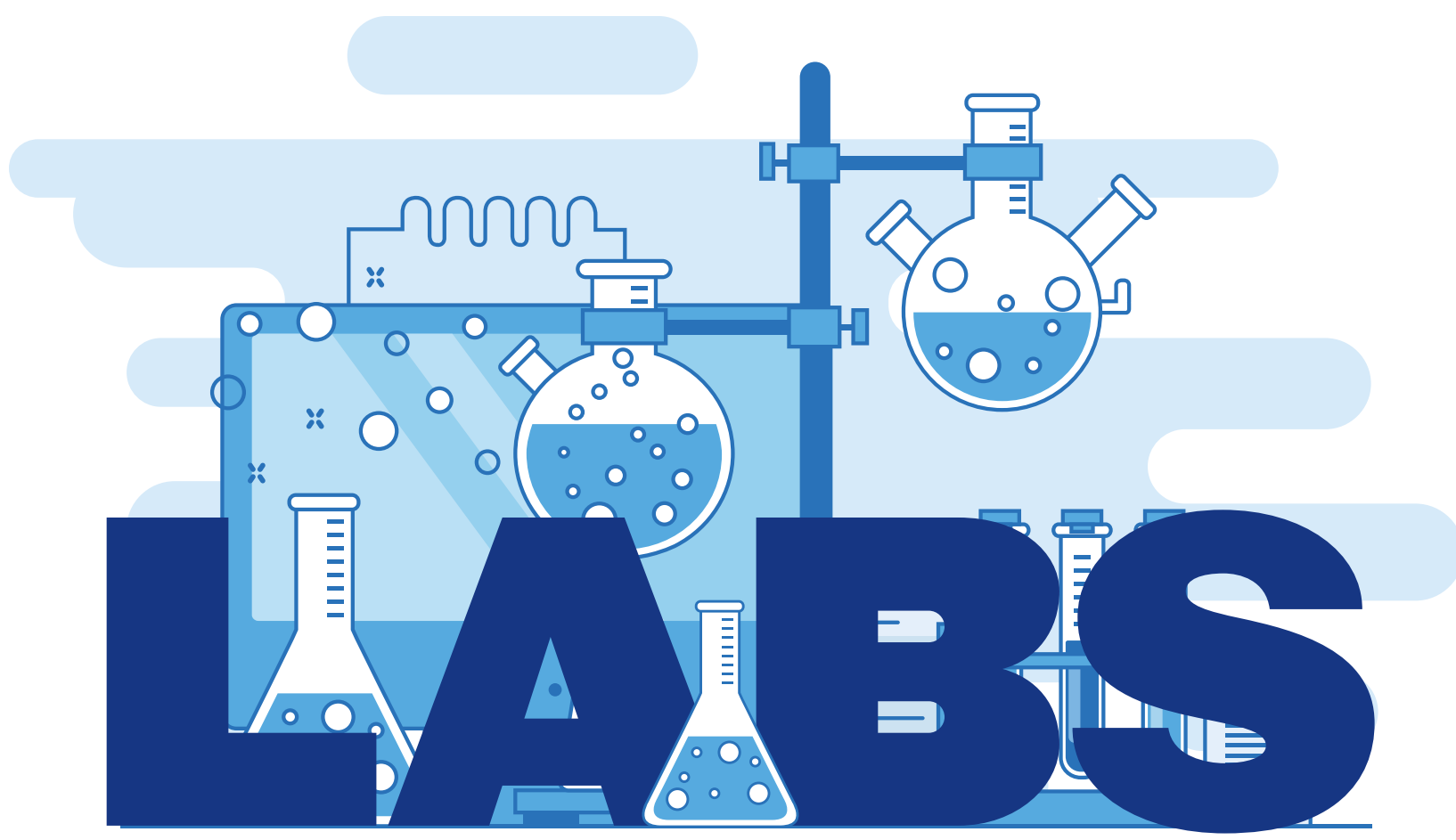
Saturday, September 6, 2025 from 10am to 12pm CT

Experience NodeZero in action during our interactive lab session. Dive into hands-on demonstrations to see how autonomous pentesting enables continuous assessment of your security posture, revealing your exploitable attack surface in real time.

Learn to identify and prioritize your most critical vulnerabilities with proof of exploitability, receive actionable remediation guidance, and use 1-Click Verify to ensure fixes are effective.

Explore how NodeZero uncovers risks beyond traditional CVEs, including easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies. Focus remediation on what matters most, helping you reduce risk efficiently.





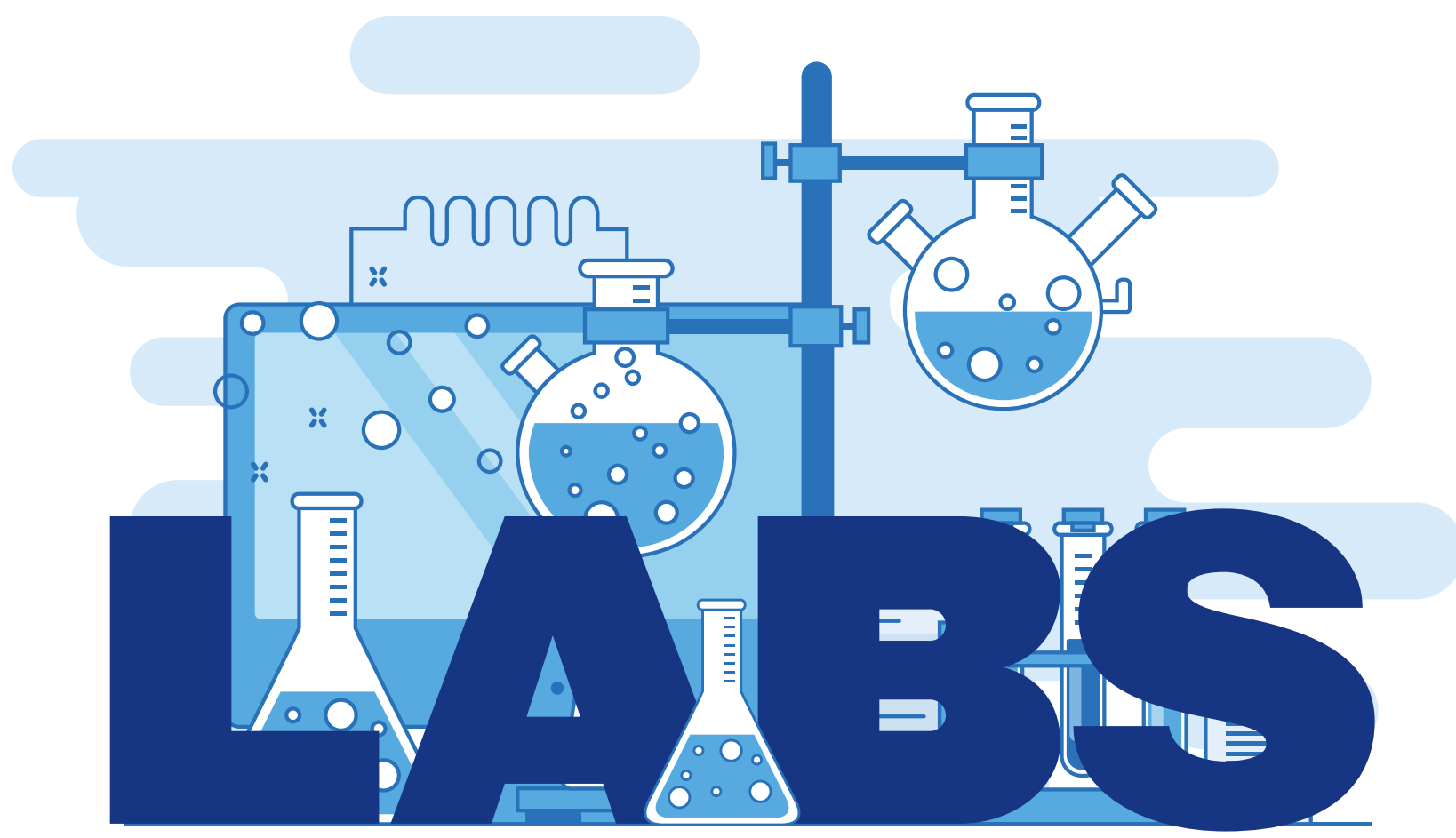
Saturday, September 6, 2025 from 12pm to 2pm CT

Struggling to keep up with vulnerabilities, exposures, and remediation chaos? In this hands-on lab, you'll step into a live environment to experience how Semplicity helps security teams automate and scale their vulnerability and exposure management programs across the entire stack.

You'll learn how to:

- » Aggregate signals from scanners, cloud platforms, and other security tools into a single platform
- » Automate ticketing, escalation, and validation processes across teams
- » Prioritize remediation based on context, risk, and ownership
- » Gain visibility into remediation progress with real-time dashboards and reporting

This lab is ideal for security engineers, vulnerability managers, and anyone looking to cut MTTR and streamline collaboration between AppSec, DevOps, and Infrastructure teams.



graylog

Saturday, September 6, 2025 from 2pm to 4pm CT

The Graylog sandbox is an interactive demo system which will allow the end user to experience a powerful threat detection, investigation, and response (TDIR) platform. In this demo the user will be able to identify, prioritize and respond to security events leveraging curated anomaly detection and sigma rules utilizing the guided analyst workflow. The user will be able to harness the full range of functionality within Graylog security, leveraging a wide range of data sources at their fingertips.

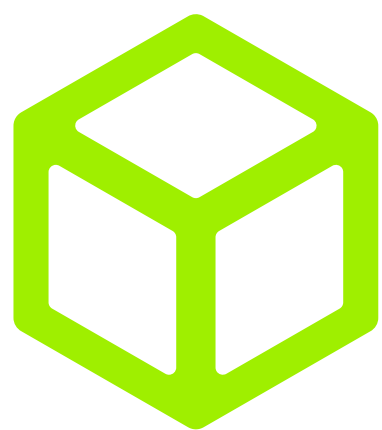
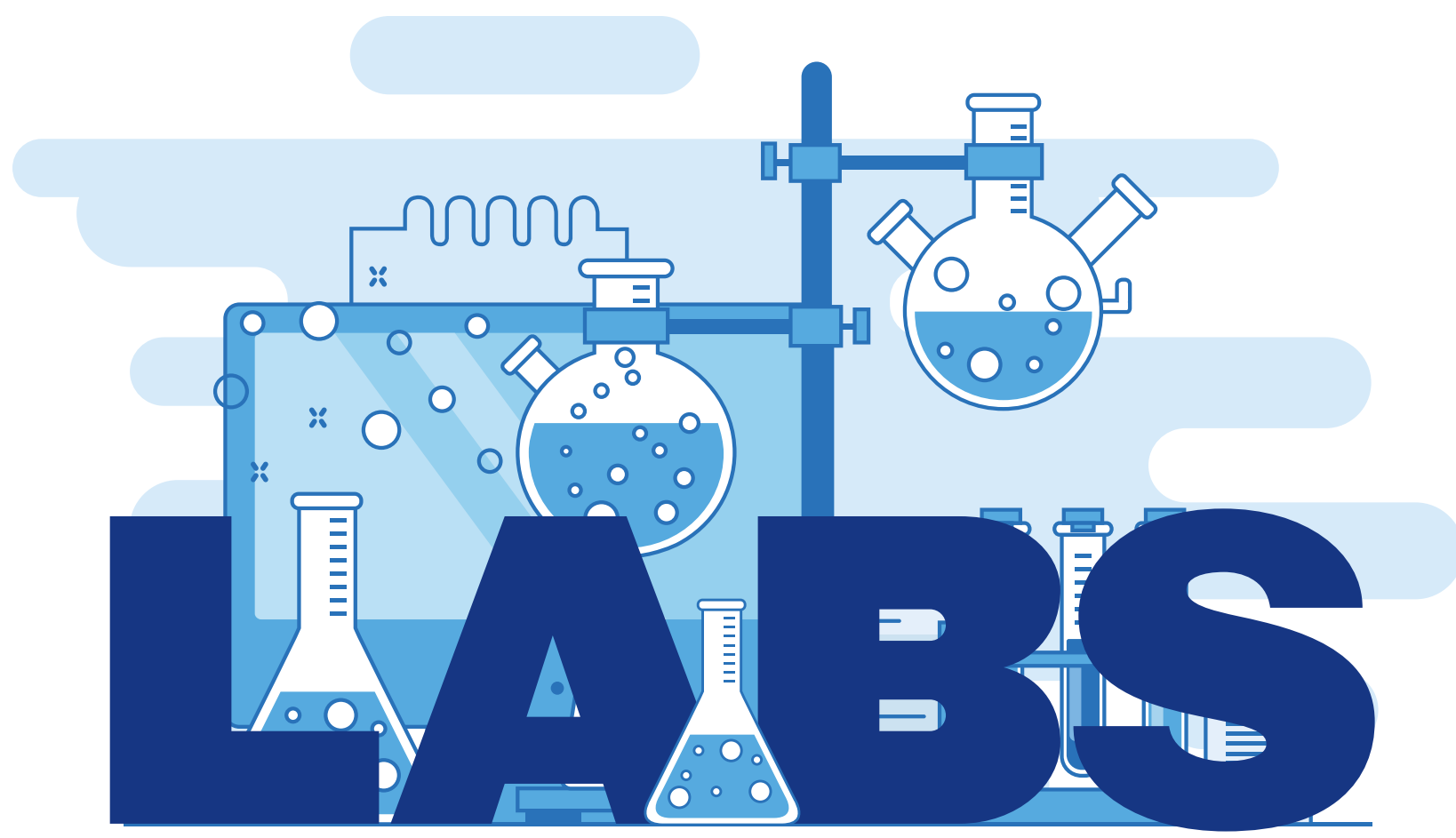


Saturday, September 6, 2025 from 4pm to 6pm CT

Take control with LimaCharlie's Security Operations platform in this hands-on lab where you'll gain visibility across multiple data sources as we simulate real infrastructure attacks using EDR and Cloud telemetry.

You'll learn to leverage pre-existing detections AND build custom detection and response rules from scratch, giving you control most vendors don't offer. Additionally, you'll have access to powerful incident response tools to manage and neutralize threats via both manual and automated workflows. Perfect for security engineers who want to build solutions, not just consume vendor black boxes. Walk away with working detections you can immediately deploy in your environment.





HACKTHEBOX

Sunday, September 7, 2025 from 12pm to 2pm CT

In today's unpredictable threat landscape, where attackers use advanced techniques, automation, and multi-vector strategies to exploit vulnerabilities, the cybersecurity gap is no longer just about skills — it's about speed.

SOC teams must detect, investigate, and respond faster than ever.

In this session, Hack The Box, will demonstrate HTB Threat Range, a gamified, live-fire simulation that takes security operations center (SOC) analysts and digital forensics (DFIR) investigators through the full incident response cycle in one high-intensity exercise. Attendees and participants will see how realistic scenarios, real-time metrics, and collaborative challenges sharpen detection, triage, and investigation skills, closing the gap in both capability and response time.



WELLNESS VILLAGE

Saturday, September 6, 2025 from 10:00 am to 6:00 pm CT
Sunday, September 7, 2025 from 10:00 am to 3:00 pm CT

The Wellness Village will be ran by Mental Health Hackers, a 501(c)(3) organization.

The Mental Health Hacker's (MHH) mission is to educate tech professionals about the unique mental health risks faced by those in our field – and often by the people who we share our lives with – and provide guidance on reducing their effects and better manage the triggering causes. This will be done through numerous talks and speakers conducted within the village during the conference. There will also be fun activities, crafts, coloring, and more to help you reduce stress and take a mental break from the conference activities and attendees.

MHH also aims at providing support services to those who may be susceptible to related mental health issues such as anxiety, depression, social isolation, eating disorders, etc.

Please understand that MHH does not provide counseling or therapy services.

Their website can be found at <https://www.mentalhealthhackers.org/>.

Wellness Talks

When Red Flags Are Hidden in Code: Spotting Abuse in Tech Spaces - Dr. Gregory Carpenter

Saturday, September 6 2025, 11:00 am - 12:00 pm CT

Cybersecurity professionals work in high-pressure environments where isolation, long hours, and blurred work-life boundaries are common. These conditions can make it harder to recognize and respond to abusive relationships—whether personal, professional, or digital. This talk offers practical tools to help identify red flags of abuse, including coercive control, digital surveillance, and workplace manipulation. I will cover how abuse presents differently in technical fields, how to document and respond safely, and what resources exist for support. The goal is to equip cyber professionals with the awareness and language to protect themselves and others in their networks, both online and offline.

Balancing the Scales: Managing Mental Health in Cybersecurity - Patrick Kelley

Saturday, September 6, 2025, 2:00 pm - 3:00 pm CT

Cybersecurity professionals are facing unprecedented levels of stress, leading to significant mental health challenges. This paper explores the multifaceted pressures within the cybersecurity industry, including imposter syndrome, sleep deprivation, and concentration difficulties. It examines the systemic nature of these stressors, highlighting the prevalence of burnout and the lack of psychological safety in the field. Through a comprehensive analysis, this presentation provides insight into the mental health vulnerabilities unique to cybersecurity professionals, and offers practical strategies for prevention and coping. By addressing these issues, we aim to foster a healthier, more sustainable work environment for those on the front lines of digital defense.

Demystifying Counseling - Investigatorchic

Saturday, September 6, 2025, 4:00pm - 5:00pm CT

Everyone faces mental struggles at some point in their lives, some more than others. Counseling can be a fantastic way to work through these challenges. Though the introduction of some personal stories, Investigatorchic will discuss what therapy actually entails and what it does not, in order to dispel commonly held myths. In addition, information will be provided about different kinds of counseling and how to select a counselor that can be most helpful for a particular situation/concern.

Massage Therapy @ The Wellness Village

We've brought in two massage therapists offering 10-minute massages from 10am to 3pm CT on Saturday, September 6th. Massages are first come, first serve.



9 Bridge Challenge with Chief Wellness Officer, Matthew Abahazi

Join Mental Health Hackers' Chief Wellness officer, Matthew Abahazi, on the inaugural 9 Bridge Challenge the morning of Sunday, September 7th and enjoy a scenic run of approximately 4.5 miles.

To participate, meet just outside the parking roundabout at 7:45am CT – Strava and paper maps will be provided.





IoT VILLAGE

Saturday, September 6, 2025 from 10:00 am to 6:00 pm CT
Sunday, September 7, 2025 from 10:00 am to 3:00 pm CT

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).

Follow both ISE (@ISEsecurity) and IoT Village (@loTvillage) on Twitter for updates on talks, contests, and giveaways.



<hunter_strategy>

Open during the entire time (even through the night) of the conference.

The Lounge, your post-Talk oasis, is a dedicated space to develop connections with fellow attendees and continue Q&As with speakers in a relaxed setting. Unwind on comfortable furniture while you recharge your batteries and indulge in your favorite retro video games from Nintendo, Super Nintendo, and PlayStation!

Join us for exclusive mini-labs hosted daily by Jake Williams: Email Header Analysis: "Return-Path to the Future" at 11 AM and Linux Log Analysis: "Lastlog and Found" at 2 PM. These interactive workshops offer practical skills development in an informal, engaging environment.

CAREER VILLAGE

Saturday, September 6, 2025 from 10:30 am to 6:00 pm CT

Sunday, September 7, 2025 from 10:00 am to 12:00 pm CT

Are you starting a new career in cybersecurity? Or maybe you're looking for a change in scenery or direction?

This village is an opportunity for people at all stages in their career to get 1:1 insider advice and tips from real recruiters and hiring managers. Seek guidance about what could be your (next) career in cybersecurity, learn how to effectively highlight your knowledge, experiences, and abilities on your resume, and learn how to prepare for interview settings that employers are utilizing today. You'll even have the chance to practice your interview skills and get direct feedback so you can feel more confident in your job search.

Masks are required to participate in this village. Please bring your own if you can. We'll have limited masks on hand for those who do not have them.

Walk-ins will be accepted based on availability.

Career Talks

**Hacking the Job Application Process
- Kimber Amos**

Saturday, September 6, 2025, 12:30 pm - 1:00 pm CT

In the current market, employers are receiving submissions from 300-3000 (yes, THREE THOUSAND) applicants per single posted tech or tech-adjacent role.

If you're currently looking for a job, you've probably already figured out that your traditional job search methods are falling short. Stop by the Career Village at 12:30 for a brief talk about how to face challenges head on in the current market. I'll cover job seeker frustrations like extended cycles, skills mismatches, and increased competition, while providing actionable strategies for success. Then I'll dive into key topics like optimizing resumes for ATS systems with quantified achievements and preparing for technical interviews using some basic research methodologies. I'll also briefly cover the STAR method to improve your answers to behavioral questions.

Although 70% of roles are filled through referrals before public posting, there are some actions you can take during the application process to improve your chances of landing your next great role.

CLICK FOR MAP



UNCONFERENCE

**Open during the entire time (even through the night)
of the conference.**

The Unconference Village is an open-mic setup with a podium and a projector. No talks are selected or scheduled before the start of the conference. Once the conference opens, you can sign up for a slot to present. If your amazing talk didn't get selected by the Blue Team Con CFP committee, this is your chance to present on your topic in a creative way. If you didn't submit but wished you would have – here you go! If you want to do a fishbowl about knitting – have at it! The topics do not have to be cybersecurity related. It's an Unconference!



The [Last Minute] Capture the Flag [CTF] event is back for another year during Blue Team Con. This is a beginner-friendly CTF competition.

Friday, September 5 at 6:00pm to Sunday, September 7 at 1:00 pm

Originally, this was a very last minute thing. This time, not quite so late, and with much better planning, but “Not [Last Minute] CTF” isn’t as fun. However, we continue to provide a fun game via a unique learning experience. As this is being run at Blue Team Con, all of the puzzles and challenges will be related as best we can to defensive cybersecurity topics. Remember, we want you to learn, we just might not make everything too easy...

However, a big difference that we can impart on this competition compared to other competitions, is that the [Last Minute] CTF wants to see you document your work and provide write-ups for each of the challenges. Half of the available points will come directly from these write-ups. While documentation is not something for everyone, it is a highly desirable skill to have and use in any day-to-day operation and who knows, we may even feature your write-up and tell everyone how awesome you did the thing!

CTF Prizes

Coveted Blue Badge (Offers free admission to Blue Team Con indefinitely), Books, and more to be announced!

CTF Hours

The competition homepage will go live for player signups (and to allow people early access to complete the introduction) when registration opens on Friday, September 5th, at 6:00pm CDT.

The rest of the challenges and the competition will begin Saturday, September 6th, at 10:30am CDT until Sunday, September 7th, at 1:00pm CDT.

Help and Assistance

Join the Blue Team Con Discord and then the #last-minute-ctf channel
Stop by the CTF Room during Admin Availability Hours* for Assistance.

**Friday, September 5th: 6:00 pm to
Sunday, September 7th: 1:00 pm**

*Hours are subject to change. This is not a flag.

CTF Win Categories

We will have numerous categories that one can win in our Last Minute CTF.

Some examples are:

1st Place

2nd Place

3rd Place

Kickstarter (First Score)

Down to the Wire (Last Score)

Best Write-Up



<https://btcon.link/CTF>

HTB CTF

@ BLUE TEAM CON



SPONSORED BY

HACKTHEBOX

Saturday, September 6 from 10:00 am to 6:00 pm

In this CTF, attendees will have a chance to test their skills in Forensic challenges of varying difficulty.

Number of Challenges: **6**

Category: **Forensics**

Difficulty: **Easy to Hard**

Max Team Size: **3**

**Highest Score Wins a Silver Annual Subscription for the first team
(Valued at \$490 USD)!**



Black Girls Hack provides training, community, and needs-based services to help educate, empower, and prepare our members for careers in technology and cybersecurity. Since 2019, we have served as a community-based not for profit organization that helps bridge the gap between what is taught in schools and what is required for industry employment. We partner with leading-edge solutions and training providers to help career changers and the industry outliers find a home within cybersecurity. Our organization represents the industry as we desire it to be while being inclusive and reflective of our community. Our vision is a diverse and inclusive cyber industry where Black women are represented in technical, leadership, and executive roles.

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



The goal of Sober in Cyber is to grow a community of sober people within the cybersecurity industry who can share resources, network together, and find "sober buddies" at infosec conferences. We started by launching a Discord community in May 2023 (sober folks in cyber: join the server [here](https://www.soberincyber.org/)). We're also in the development stage of launching a podcast that will highlight the multitude of personalities and pathways within the Sober in Cyber community.

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



Docent Institute (Docent) is a 501(c)(3) registered charitable non-profit educational institution based in Iowa. Its mission is "Cybersecurity and STEM education, inclusion, and outreach for the benefit of society."

Docent organizes cybersecurity/STEM camps for K-12 students, cybersecurity career days for high school students and competitions for college students. Docent hosts the premier Midwest annual cybersecurity conference, CornCon, held in the fall in Davenport, IA. Docent provides college scholarships, mentoring, apprenticeships/internships, career services and performs other public outreach related to cybersecurity education and career development, advancing technology, and the ethical use of technology. Docent also works with IEEE to develop industry standards around the ethical application of technology. Current projects include developing a process for evaluating the trustworthiness of news sources, and a standard on the ethical use of AI.

<https://docent.org/>



Women in CyberSecurity (WiCyS) is a non-profit and membership-based organization dedicated to the recruitment, retention and advancement of women in the cybersecurity field. The organization is working to improve diversity and pipeline in the cybersecurity workforce, and it does so through numerous initiatives, together with Strategic Partners and an army of energetic volunteers.

WiCyS helps build a strong cybersecurity workforce with gender equality by facilitating recruitment, retention and advancement for women in the field. WiCyS offers mentoring, training programs, scholarships, virtual and in-person conferences, leadership series, career fairs, webinars, and more to women at all stages of their cybersecurity career journey!

Visit their booth at Blue Team Con to learn more.

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

Next-Gen Email Security

Prevent, detect, and
respond to threats faster
and with confidence.

ULTIMATE

SPONSOR²⁰₂₅



HORIZON3.ai

~~TRUST~~ BUT VERIFY

TRAINING

SPONSOR



Microsoft

PLATINUM
SPONSOR **2025**

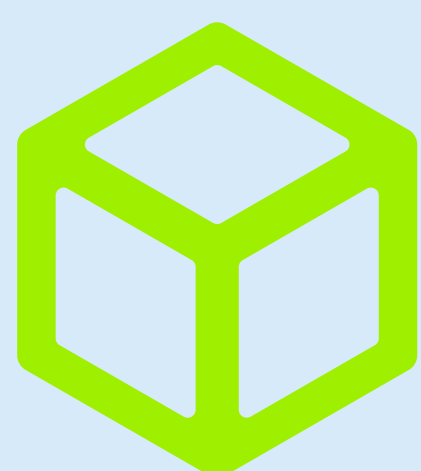
LEGION



**Sublime
Security**

THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

GOLD SPONSOR²⁰²⁵



HACKTHEBOX



LATACORA



PERMISO



seemplicity



SPACEWALK

SILVER
SPONSOR²⁰₂₅

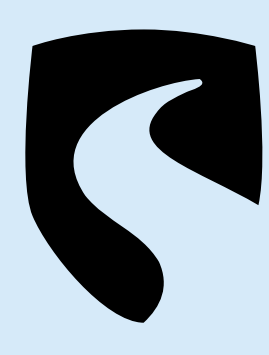


SILVER
SPONSOR²⁰₂₅

//O Push Security

RAPID

 **rubrik**[®]

 **Stream.Security**

WIZ

BRONZE SPONSOR ²⁰₂₅



Orchid



snyk

LAB SPONSORS²⁰₂₅

graylog

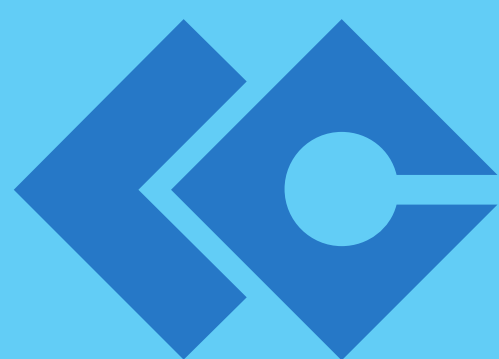


HACKTHEBOX

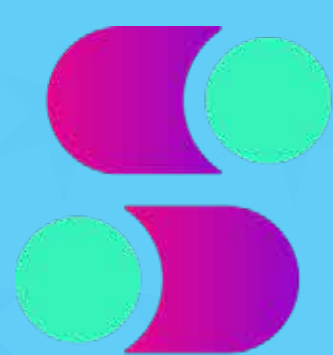


HORIZON3.ai

~~TRUST~~ BUT VERIFY

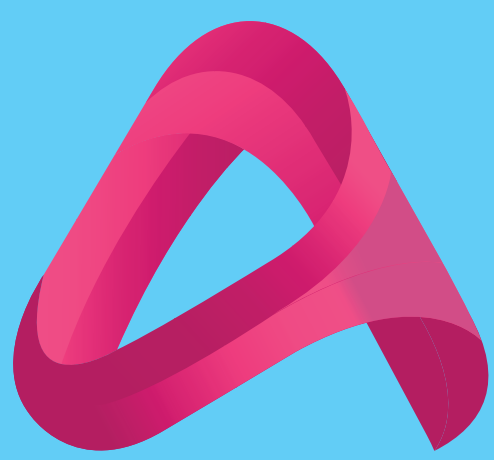


LIMA
CHARLIE

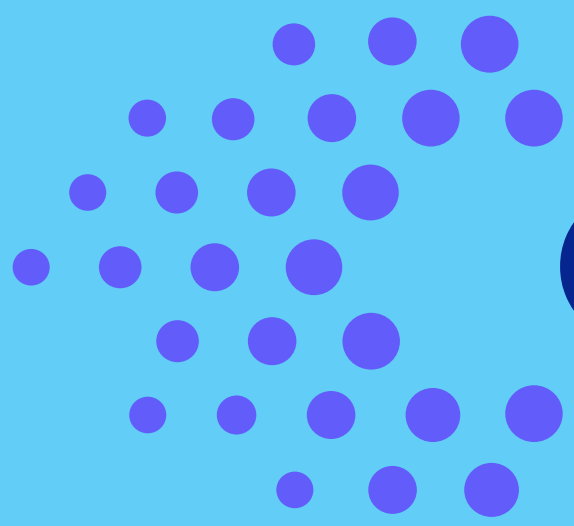


seemplicity

ATTENDEE DINNER SPONSORS²⁰²⁵



abstract.security



CONCENTRIC



FLASHPOINT



OPTIV

OTHER SPONSORS²⁰²⁵



Swag Bag Sponsor



Last Minute CTF Sponsor



Lounge Sponsor



Talk Track 1 Sponsor

OTHER SPONSORS²⁰²⁵



OffSecTM

The Path to a Secure FutureTM

Saturday Night Hacker Charlatan Sponsor



STELLAR
CYBER[®]

Saturday Night Sober Games Sponsor

StoneX[®]

Afternoon Coffee & Tea Break Sponsor



Stream.Security

Speaker & Trainer Dinner Sponsor



Foodstuffs

Coffee Fix

Dunkin

75 E Washington St

Starbucks

200 N Michigan Ave

Stan's Donuts & Coffee

181 Michigan Ave

Quick Bites

Chipotle

316 N Michigan Ave

McDonalds

119 N Wabash Ave

Intelligentsia

53 E Randolph St

5 Guys Burgers & Fries

180 N Michigan Ave

Potbelly Sandwich Shop

190 N State Street

Brown Bag Seafood Co.

340 E Randolph St

Roti (Mediterranean)

80 E Lake St

Sweetgreen

150 N Michigan Ave

Nandos Peri-Peri

117 E Lake St

Panda Express

180 N Wabash Ave

Wildberry Pancakes & Cafe

130 E Randolph St

Get your food truck favorites with a halal twist at Yummy Halal Food. This Chicago truck serves up an assortment of burgers, hot dogs, tacos, rice bowls, and more, all prepared to halal standards



Saturday from
12:30pm to 2:30pm

Click to View Menu

Fairmont Amenities

20%
discount off
mySpa services

Complimentary
access to mySpa
Fitness Center
(valued at \$15.00 per day)

Complimentary
standard guestroom
internet access
(valued at \$14.95 per day)

H

Submitting CPE Information

Don't forget to submit your attendance for Continuing Professional Education (CPE) credits to your certification organizations! Sessions at this conference will cover topics related to many or all the (ISC), ISACA, AICPA, IAPP, GIAC, CompTIA, and others' domains, suitable for CPE credit for your certifications.

Attending one hour of the conference is typically equated to one hour of CPE credit, but please verify with your certification organization handbook. Submission of your Blue Team Con ticket as evidence and a listing of talks attended should suffice. A CPE template will be emailed out to you following the conclusion of Blue Team Con as validation that you attended the conference.

If you ever need something more for CPE submissions, please email us at info@blueteamcon.com for assistance.

In an effort to make Blue Team Con more accessible, we have published our Accessibility Policy. You can find it here:
**[https://blueteamcon.com/about/
accessibility-policy/](https://blueteamcon.com/about/accessibility-policy/)**



blueteamcon.com/scholarship



.e"X"es and "O"auths (They Haunt Me): An In-Depth Analysis of OAuth & OIDC Misconfigurations and Token Replay Attack

Darryl G. Baker

Senior Solutions Architect, Netwrix

OAuth 2.0 and OpenID Connect (OIDC) are the backbone of modern identity and access management, but poor implementations leave organizations dangerously exposed. In this talk, I'll move beyond theory and demonstrate how subtle misconfigurations in OAuth and OIDC flows can be exploited by attackers to bypass authentication, impersonate users, and replay tokens for unauthorized access. We'll walk through real-world vulnerabilities such as missing state parameters, improperly validated discovery documents, and token validation failures. Then I'll demonstrate a live token replay attack using OWASP ZAP to intercept and reuse a captured JWT — illustrating how easily these weaknesses can be exploited in the wild. Attendees will leave with actionable knowledge on how to identify, exploit, and mitigate these flaws in enterprise environments, along with open-source scripts and tools to reproduce the attack scenarios in their own labs.

Experience Level: Intermediate



“SkyScalpel: Making & Breaking “Policy”: “Obfuscation” in the Cloud”

Abian Morina

Threat Researcher, Permiso Security

This talk explores how attackers can obfuscate cloud policies, remote administration scripts, and permissions parameters to evade detections at multiple stages of the detection pipeline. When “Allow” becomes “Alu006Cow” and “iam:PassRole” becomes “iam:P*ole”, do your detections still work? Some obfuscation techniques are caught during creation but sanitized upon storage; others persist and silently bypass detection, break console rendering, or manipulate what defenders see depending on the viewing method.

I will present offensive and defensive findings from these obfuscation scenarios, highlighting inconsistencies across official cloud tooling (CLI, SDKs, consoles), and introduce SkyScalpel—a custom-built JSON tokenizer and syntax tree parser equipped with cloud-aware obfuscation, deobfuscation, and detection capabilities. SkyScalpel demonstrates just how easily attackers can bend cloud policies and how defenders can fight back.

Experience Level: Intermediate



Analysis without Paralysis: Mastering the Art of Investigation

Terryn Valikodath

DFIR Consultant, Cisco Talos

Effective analysis is essential for identifying and mitigating cybersecurity threats, yet most analysts are never formally taught how to conduct investigations. This talk serves as a primer, equipping you with the insights and techniques needed to structure your investigations—regardless of the operating system or hardware.

We will introduce a structured analysis workflow designed to help analysts systematically transform raw data into actionable findings, uncovering an adversary's movements with precision. The session will break down key investigative pillars:

- » Investigation Strategy – Defining objectives, scope, and a clear plan of action.
- » Findings – Organizing and documenting evidence to drive your investigation forward.
- » Correlation – Connecting discrete events to build a coherent case.
- » Timeline – Establishing a clear sequence of events for deeper insight.
- » Enrichment – Leveraging external intelligence to fill gaps and identify patterns.

Finally, we'll tie it all together into a comprehensive yet efficient report, one so well-structured and insightful that it demands attention and drives meaningful change. Whether you're new to investigations or looking to refine your approach, this talk will provide the tools to elevate your analysis from chaotic guesswork to forensic mastery.

Experience Level: Foundational



Breaking the CI/CD Chain: Security Risks in GitHub Actions

Alexey Shchukarev

*Team Leader and Security Architect,
Axonius*

GitHub Actions have become a critical part of CI/CD pipelines, but do you really know what's happening under the hood?

This talk will break down GitHub Actions concepts, explore their security risks, and highlight how third-party actions in the supply chain can introduce vulnerabilities. We'll examine real-world examples of misconfigurations, critical security risks, and unexpected workflow behaviors that attackers can exploit.

We'll also discuss the recent security issue with tj-actions/changed-files, and we'll analyze how attackers can exploit these risks and what security best practices can help to mitigate them.

Additionally, we'll compare existing security tools, from static analysis scanners to runtime monitoring solutions, and discuss how teams can integrate them into their CI/CD pipelines. Finally, I'll introduce a new tool designed to help identify and analyze transitive actions, making it easier to assess their impact and reduce security risks.

Attendees will gain a deeper understanding of GitHub Actions' security landscape, real-world case studies, and practical techniques for proactively securing their workflows, alongside a new tool to simplify the process.

Experience Level: Intermediate



Can opposites attract? Domain Admins – meet Red Tenant

Jake Hildreth

*Principal Security Consultant,
Semperis*



Eric Woodruff

*Chief Identity Architect,
Semperis*

A few years ago, Microsoft deprecated the Enhanced Security Admin Environment (aka ESAE aka red forest) model and replaced it with their Rapid Modernization Plan (RAMP). Where ESAE was focused solely on legacy Active Directory (AD), RAMP is built for protecting privileged users in both AD and Entra ID. However, all is far from perfect in this new model, and the focus is heavily slanted towards protecting the cloud.

Over the past few years, there has been talk about “red tenants”, and a few products have been released that use a red tenant approach to protect a Microsoft cloud estate with a privileged Entra tenant.

But why should the cloud have all the fun stuff? What if we took the red tenant model and used it to protect AD?

In this session we explore the design of an Entra tenant that has one sole purpose – protecting Tier 0 resources in Active Directory. Sound wild? We think so. But if we break ALL the rules along the way, we might end up in a place where our attack surface is reduced, our AD authentication methods are strong, and Entra might become the go to replacement for ESAE.

Join us as we explore the architecture and what it takes to roll out the red tenant for all your AD Admins!

Experience Level: Intermediate



Cultural Due Diligence: Hard Won Lessons from My Job Hunt

Munish Walther-Puri

Perennial Job Hunter

After 18 months and countless job applications, I learned that the real key to professional satisfaction isn't just the role you land—it's the environment you land in. In this talk, I'll share hard-won lessons from my own job search journey, drawing on techniques from OSINT (Open Source Intelligence), risk analysis, and maturity assessment. Attendees will learn how to conduct "cultural due diligence" on prospective employers, maximize their chances of landing interviews, and ask the right questions to uncover an organization's true values. The goal: to help job seekers avoid toxic environments, align with workplaces that match their values, and save time, money, and frustration in the job hunt.

Organizational culture—shared values, beliefs, and behaviors—has a profound impact on job satisfaction and performance. Studies show that cultural misalignment is a leading cause of employee turnover and even failed mergers and acquisitions. Yet, most job seekers focus on titles and responsibilities rather than the environment they'll be working in. My own experience, as well as best practices from risk analysis and OSINT, demonstrates that understanding and vetting company culture is as critical as evaluating the job description.

Cultural due diligence borrows from the worlds of M&A and security: it means digging beneath surface-level statements to uncover how an organization really operates, what it values, and whether those values are lived out at every level. By applying OSINT techniques, job seekers can gather actionable intelligence from public sources, informal networks, and direct conversations, empowering them to make informed decisions about where they'll thrive.

Experience Level: Foundational



Firewalls and Fire Alarms: What to Do When Your Best Defenses Go Up in Smoke

Dr. Catherine J. Ullman

*Principal Technology Architect, Security,
University at Buffalo*

Imagine your shock in seeing your newly installed “fireproof” wall completely engulfed in flames. In both fire safety and information security, we often think that we design layers of controls to prevent disaster. In reality, these layers are actually meant to delay disaster. But what happens when those trusted defenses fail? This talk draws on real-world scenarios where controls everyone assumed were in place—from fire doors to firewalls—unexpectedly gave way, leading to chaos and damage.

Using compelling examples from both fields, we’ll examine situations where preventative, detective, and containment controls fell short and explore the lessons they offer for information security. Attendees will learn how layered defenses, regular testing, and resilient response plans can make a difference when systems don’t perform as expected. By blending fire safety insights with actionable security strategies, this talk will prepare you to handle the flames when your own controls go up in smoke.

Foundational



Ensuring Data Integrity in Incident Response: Tools and Techniques for Forensically Sound Log Extraction

Colin Meek

*DFIR Consultant, Stroz Friedberg,
an Aon Company*

Logs are foundational to nearly all DFIR engagements, yet reliably extracting logs from sources such as network appliances, SaaS applications, and cloud environments can be challenging. When standard UI-based exports fail, due to volume restrictions, technical limitations, or undocumented interfaces, investigators must turn to APIs for programmatic log collection. This session will share practical tips for API-driven log extraction, including a detailed real-life case study involving extraction from an undocumented API of a proprietary client application. Additionally, we will discuss real-life cases where log data was discovered to be incomplete during collection and highlight the impact this could have had on investigative outcomes.

This presentation will also introduce an open-source log-analysis tool designed to assist DFIR professionals in quickly identifying potential issues in collected logs. The tool helps quickly highlight suspicious patterns, such as unexpected time gaps, duplicate events, suspiciously rounded event counts, JSON formatting errors, or indicators of potential redactions. Incorporating this tool into investigative workflows helps examiners proactively recognize potential data-quality concerns, supporting more informed decisions in high-stakes investigations.

Experience Level: Intermediate



Inboxfuscation: Out-of-the-Box Mailbox Obfuscation - Turning BEC into Business Email Chaos

Andi Ahmeti

Threat Researcher, Permiso Security

Email remains vital in most organizations, from user logins to daily business communications. Business Email Compromise (BEC) continues to threaten companies' operations as attackers disrupt communications, perform reconnaissance, or leverage this foothold as a springboard for targeting additional organizations.

This research shares examples of common TTPs from first-hand attacks before exploring multiple categories of never-before-seen obfuscation techniques targeting Exchange mailboxes and their administration tools. These obfuscation categories begin with numerous undocumented functional tricks like null-character inbox rule names and single-space conditions that perform unexpected filtering while simultaneously breaking rule name-ID correlations in runtime logs relied upon for detections. We then explore a larger genre of syntactical obfuscation, highlighting problematic characters (null character, backspace, carriage return, RTL, zero-width space) while introducing many new classes of characters with differing evasive qualities.

While many homoglyph attacks rely on look-alike characters to evade visual analysis, we uncovered undocumented normalizations that transform visually bizarre, Unicode-laden keywords to ASCII counterparts while still logging as Unicode. Beyond visual and logging-mismatch evasions, we discovered functionality-breaking techniques that render Exchange UI and CLI tools ineffective for administrative and investigative purposes. We end with a vulnerability allowing email deletion while entirely bypassing all logging.

From subscripts to symbols, come and ****exchange**** (ha!) everything you thought you'd seen about BEC attacks and experience the depths of evasion that our Inboxfuscation research and open-source tool can provide to offensive- and defensive-minded security professionals alike.

Experience Level: Advanced



Leading Multi-Generational Cybersecurity Teams with Transparency, Candor, and Empathy

Mike Glatz

Director of Security Engineering, StoneX

The cybersecurity workforce is rapidly evolving, now spanning multiple generations. Baby Boomers, Gen X, Millennials, and Gen Z, with Gen Alpha on the horizon. Each brings distinct values, expectations, and communication styles. As people work longer and teams become more age-diverse, the ability to lead across generations is critical to long-term success. This talk explores practical strategies for managing multi-generational cybersecurity teams by embracing transparency, radical candor, and empathy.

Drawing from personal experiences as an elder millennial who navigated traditional workplace cultures, I will discuss the challenges and solutions in adapting leadership styles to meet the needs of today's dynamic workforce. Attendees will gain actionable insights into fostering inclusive environments that harness the strengths of all generations, enhancing team cohesion and innovation in cybersecurity.

This session aims to equip leaders with the tools to bridge generational gaps, build trust, and cultivate collaborative teams, ultimately advancing security and retention in the field.

Experience Level: Intermediate



My Cyber Sense Is Tingling! Detection Engineering With Free Tools

Matthew Gracie

Senior Engineer, Security Onion Solutions

Every threat hunt, every incident response, and every bulletin from your ISAC comes with a wealth of intelligence and indicators that you can leverage to spot suspicious or malicious activity in the future. The process of taking that information and turning it into reliable, repeatable alerting is known as Detection Engineering.

In this presentation I will introduce the free and open Security Onion enterprise monitoring platform, the methods by which it can generate or ingest logs about what's happening in your environment, and how we can use that log data to trigger alerts for potential incidents. Whether you're looking for artifacts in network traffic, file structures, or endpoint logs, it's easy to create new detection rules so your analysts are aware when something suspicious rears its head.

Experience Level: Intermediate



Ransomware Rampage: Gamifying Your Incident Response Playbook

Anushree Vaidya

Cybersecurity Analyst

With the alarming rate of ransomware proliferation, there is a stark disparity in the percentage of cyber professionals with hands-on experience in managing such incidents. This session addresses this gap through a Gamified Ransomware Playbook creation experience and offers a unique, immersive experience designed to elevate participants' skills in crafting robust, standardized procedures enhanced by research to combat the ransomware plague. A playbook adds standardization to incident response and is equally helpful for a cyber professional with varied levels of expertise over the spectrum. This session goes beyond theoretical knowledge, providing participants with practical, hands-on experience in navigating the entire ransomware incident lifecycle. Participants will engage in realistic scenarios, including the crucial aspects of communicating with senior leadership and legal teams during a crisis. The session will also cover complex situations where organizational data is either fully or partially encrypted and a ransom demand is made, offering insights into the delicate balance of technical, legal, and ethical considerations.

Through this gamified approach, participants will draft comprehensive playbooks tailored to various ransomware scenarios, incorporating both proactive measures and reactive strategies. With the focus on creating adaptable, tool-agnostic response strategies, it aims to instill confidence in cybersecurity professionals facing the daunting challenge of ransomware incidents with improved crisis management abilities. The session's impact extends beyond individual skill enhancement, contributing to the broader cybersecurity community's resilience. As more professionals become adept at crafting effective ransomware playbooks, organizations collectively strengthen their defense against this pervasive threat, fostering a more secure digital ecosystem.

Experience Level: Foundational



Threat hunting in the browser

Luke Jennings

VP, R&D, Push Security

In the previous decade we saw a huge pivot to endpoint based attacks, which the security industry was initially ill prepared for. In particular, common intrusion detection approaches of the past had been largely network sensor focused and were not well suited to dealing with endpoint focused attacks. This led to the explosion of endpoint-orientated approaches which eventually led to the creation of the entire EDR market.

Fast-forward to the current decade and we are in the midst of a rapid shift towards identity-based attacks and SaaS attack techniques due partly to the increasing difficulty of endpoint attacks and partly to the ever increasing attack surface posed by SaaS usage and spiraling numbers of cloud identities. These attacks rarely touch the endpoint and so security teams are facing a loss of visibility once again.

This talk will cover why the browser is becoming the new frontline battleground in the increasingly identity attack-based world. We'll then consider how browser extensions provide defenders with a unique opportunity to gain unparalleled visibility into attacks targeting both users themselves and the cloud identities that they have access to via their own browsers. We'll also consider why hunting in the browser can be a more advantageous approach with modern web technologies and working practices than network based tools like the web proxies of yesterday.

Experience Level: Intermediate



Transforming Cyber Risk Assessments Through Continuous Validation

Irina Loktionova

*Senior Cyber Risk Management Architect,
Delta Dental of California*



Chris Oshaben

*Senior Security Auditor,
Delta Dental of California*

Traditional cyber risk assessments often provide limited value. They rely on subjective ratings, compliance checklists, and infrequent evaluations that fail to drive actionable security improvements. This session introduces a modern approach to make risk assessments more timely, relevant, and actionable by increasing assessment frequency, focusing on real-world threats, and building a continuous feedback loop to validate control effectiveness.

Attendees will learn a structured methodology integrating threat intelligence, asset inventory, vulnerability analysis, prioritized controls, and ongoing validation. The talk will also provide real-world examples of continuous control validation methods, such as leveraging Micro-Purple Testing to continuously validate SIEM detections and using automated configuration monitoring tools to ensure endpoint detection and response protections remain effective. This session will help security practitioners shift from compliance-driven assessments to dynamic risk management that continuously improves cyber resilience.

Experience Level: Intermediate



UNFAIR after all; Critical considerations for risk management frameworks

Jack Burgess

Principal, Triangle Wave Security

Current cybersecurity risk models often contain blind-spots from established risk management principles. Highlighting failures of systems like CVSS and EPSS to address the real-world impact of vulnerabilities on individual organizations. We argue that businesses don't suffer from inaccurate predictions, but from the cost of being wrong, especially when a significant breach leaves no opportunity for recovery. Using key examples from the literature and original research we challenge the reliance on likelihood-based risk assessments, proposing a shift towards understanding the true impact of threats through empirical, context-specific analysis. In this way organizations can better allocate resources, maximize return on investment, and improve cybersecurity preparedness. For practitioners we introduce a set of practical extensions to existing frameworks to better manage their security posture. For the information security community we call for a reevaluation of existing standards emphasizing the need for more robust, real-world value based approaches to information security risk management.

Experience Level: Intermediate



Unseen but Not Unheard: Exposing the Cases of CSS Abuse in Email Threats and Fortifying Defenses

Omid Mirzaei

Security Research Leader, Cisco Talos

Threat actors are constantly exploring innovative methods to exploit benign technologies and applications in their attacks. One such example is using Living-Off-the-Land Binaries (LOLBins) to deliver malware. Another example is exploiting the features of JavaScript to deliver malware to victims' devices. Cisco Talos has observed an increase in the number of email threats that exploit the properties of HTML and CSS to include text in different parts that are not visible to the recipients of emails. This technique is often referred to as hidden text salting (or poisoning). We have also seen cases of CSS abuse to track users and fingerprint their systems.

This talk will cover a wide range of examples of CSS abuse in email threats. In particular, we will discuss and demonstrate various techniques we've identified in the wild that threat actors have used to conceal content in emails. We will address a number of challenges that this technique may pose to conventional and advanced ML-based defensive solutions. Additionally, we will introduce a novel approach to detecting hidden text salting by leveraging the capabilities of Large Language Models (LLMs). These models show promise in improving the accuracy and reliability of email threat detection, paving the way for stronger cybersecurity defense solutions.

Experience Level: Advanced



You Need a Jay-z and a Beyoncé: How Sponsors and Mentors Can Supercharge Your Career in Cybersecurity Defenses

Anthony Hendricks

*Director and Chair of Cybersecurity Practice
Group, Crowe & Dunlevy*

At the 2024 Grammys, rapper Jay-Z took the stage to accept the Global Impact Award. Instead of the typical awards speech, Jay-Z spent part of that moment not just talking about himself but his wife – Beyoncé, amplifying her accomplishments, defending her work, and advocating for her artistry. While met with criticism by some, the speech embodies the elements that experts characterize as sponsorship. Mentors and sponsors are vital for advancing your career in cybersecurity, especially for women and people of color. One of the often cited reasons in studies for why women leave careers in tech is a lack of mentors. Likewise, sponsors play an even more critical role in helping employees reach the top levels of their organizations by ensuring that their protégés get the high-stakes assignments that are often a prerequisite for C-level jobs. Without it, employees can be left feeling burnt out, frustrated with their career advancements, and ready to leave not just their current company but sometimes the industry as a whole. The roles of mentors and sponsors are often confused and misunderstood – even by mentors and sponsors. This presentation will define the roles of mentors and sponsors and highlight ways they can help people accelerate their careers. Next, we discuss why you need both a mentor and a sponsor by using the examples of Jay-Z and Beyoncé and recent business literature on the topic. We will also explore leaders' roles and outline how they can be better mentors and sponsors. Then, finally, focus on what you can do to get a mentor and sponsor and how to be a good protégés.

Experience Level: Foundational



A New Era of Brute Forcing in Active Directory

David Horak

*System Security Engineer,
Horizon Secured*

Active Directory Domain Services recently celebrated 25 years, making it far from a young technology, yet it is not going anywhere anytime soon. Most companies still rely on Active Directory as their primary identity provider and management solution. One might assume that after all these years, we have ve already mastered securing Active Directory with best practices. However, the reality is quite the opposite and Active Directory environments are often poorly secured, making them one of the main targets for attackers.

In this talk, I will explain some fundamental yet not always known concepts of Account Policies, Replication, and related best practices. More importantly, I will demonstrate a technique to bypass the Account Lockout Policy, allowing almost limitless brute-force attacks on Active Directory accounts. This brute-forcing technique is rarely documented—in fact, I had never heard of it myself until I stumbled upon it by “accident”.

By the end of this session, you will leave with a few key Active Directory configurations to enhance security and most importantly, the knowledge to defend against this brute-force technique.

Experience Level: Intermediate



Adaptive Risk-Tiered Framework for Responsible AI Governance

Sky Bell

Founder, Capital Region AI Catalyst

The rapid advancement of artificial intelligence (AI) technologies presents both unprecedented opportunities and significant governance challenges for organizations worldwide. This policy brief proposes an Adaptive Risk-Tiered Framework for AI deployment and application, ensuring safe, ethical, and innovative AI operations across various sectors. The framework emphasizes proportional oversight mechanisms that scale with risk levels, balancing innovation with appropriate safety precautions. By adopting this framework, organizations can lead in responsible AI governance, fostering trust and driving innovation while mitigating potential risks.

The framework is informed by global best practices, including the EU AI Act and the NIST AI Risk Management Framework, and is designed to be adaptable to the unique needs and contexts of any organization. It addresses the critical need for safeguards to ensure responsible and ethical AI use, particularly in high-stakes domains such as healthcare, transportation, public safety, employment, criminal justice, human rights, and finance.

Key objectives include ensuring the safe and ethical deployment of AI, fostering trust through transparency and accountability, promoting innovation while mitigating risks, and aligning with global best practices. The framework also strengthens organizational leadership in AI governance, providing a structured yet flexible approach to managing AI risks effectively.

Implementing this framework will allow organizations to enhance safety, build public trust, foster innovation, and position themselves as leaders in responsible AI governance. The proposed approach is particularly well-suited to the dynamic and evolving nature of AI technologies, making it a promising strategy for AI governance in any organizational context.

Experience Level: Foundational



Advancing from Individual Contributor to Cybersecurity Leader

Kevin Bong

*Director, Cybersecurity,
Ghostscale*

If you're feeling stuck... you've mastered analyzing alerts, configuring firewall rules and creating user accounts, and are wondering how to move your career forward from a task worker to someone who can lead people or programs... this talk is for you.

We'll dig into what leadership really looks like in security: how to influence without authority, get buy-in, and make things happen. You'll learn the skills and competencies used by successful leaders, and how to develop them yourself. You leave with practical tools, like risk registers, POA&Ms, and frameworks that actually work, and strategies to build trust, lead initiatives, and earn that next role. Whether you're aiming to own a technology stack, lead a team, become a CISO, or just want your ideas to land, this will help you take the next step.

Experience Level: Intermediate



Agents of Change: Practical Adoption Framework for Agentic AI in Security Operations

Ryan Rowcliffe
Field CTO, Legion Security

As AI evolves from theoretical potential to operational necessity, security teams face a critical inflection point in adopting agentic systems that can autonomously execute complex defensive workflows. This presentation unveils a field-tested framework for implementing agentic AI across incident response and OSINT functions – moving security operations beyond basic alert refinement to true defensive automation. Drawing from multiple deployments, I'll demonstrate how security leaders can establish meaningful adoption metrics, implement proper oversight controls, and address the emerging challenge of "AI identity sprawl" as these digital deputies increasingly act on our behalf.

Unlike conceptual discussions of AI's future, this session delivers actionable guidance for security teams to evaluate, implement, and govern AI agents based on organizational maturity and risk tolerance. Attendees will gain a systematic approach to defining autonomy boundaries, establishing acceptance criteria for both assisted and unassisted deployments, and measuring security outcomes – ultimately transforming how their teams detect, analyze, and respond to threats in an increasingly complex landscape.

Experience Level: Intermediate



AI as the SOC Sidekick: Streamlining Security Without Stepping Over Humans

Cliff Crosland

CEO, Co-founder at Scanner.dev

Security Operations Centers face an overwhelming volume of alerts, many of which are false positives that drain analyst resources and attention.

While artificial intelligence promises to revolutionize SOC operations through automated alert triage and summarization, there are significant risks in delegating critical security decisions entirely to AI systems.

The most dangerous outcome in security operations is missing genuine threats (false negatives), making complete automation of alert analysis particularly risky.

This presentation explores the optimal balance between human expertise and AI assistance in modern SOC environments.

Rather than replacing human analysts, AI tools should enhance their capabilities by explaining complex logs, providing context for alerts, analyzing false positive patterns, and suggesting improvements to detection rules.

We'll examine how properly implemented AI can accelerate information synthesis without hiding critical data from human review, allowing analysts to focus their expertise where it matters most.

The future of effective security operations lies not in AI replacement but in augmentation – creating a partnership where machines handle repetitive tasks while humans maintain oversight and make the final security judgments that require nuanced understanding and contextual awareness.

Experience Level: Intermediate



AI-Powered Cloud Security: Defending Cloud Workloads from Next-Gen Cyber Threats

Advait Patel

Senior Site Reliability Engineer, Broadcom

As AI-driven cloud workloads continue to scale, so do sophisticated cyber threats targeting cloud-based AI models, infrastructure, and data. Adversarial AI attacks, cloud misconfigurations, and automated malware are evolving, forcing security teams to rethink their defensive strategies.

In this session, I will explore the intersection of Cloud, AI, and Security, highlighting real-world attack scenarios and defense mechanisms. From securing generative AI models against adversarial attacks to leveraging AI for threat detection, I will cover practical, cutting-edge solutions that security engineers, cloud architects, and DevSecOps teams can implement today.

Attendees will gain insights into:

- » Emerging AI-driven threats in cloud environments – how attackers exploit cloud-hosted AI.
- » Zero Trust for AI workloads – best practices for securing AI-driven applications in the cloud.
- » AI-powered threat intelligence – how AI is revolutionizing cybersecurity automation.
- » Case studies – real-world breaches and lessons learned in defending AI workloads.

By the end of the session, attendees will leave with a deeper understanding of AI security challenges, actionable strategies to secure AI in cloud environments, and the future of AI-powered cybersecurity solutions.

Experience Level: Intermediate



Beyond the SLA: Measuring What Truly Matters

Swati Babbar

*Security Engineer II,
Amazon*



Kashif Memon

*Security Engineer II,
Amazon*

We've been taught to believe that if vulnerabilities are closed within SLA, our environments are secure. But in reality, SLAs often provide a false sense of protection. In this session, we'll challenge the status quo of how vulnerability management success is measured and uncover the illusion of security that box-checking creates.

You'll walk away understanding why timely remediation doesn't always equal real risk reduction — and how legacy systems, resource constraints, third-party bottlenecks, and low-context prioritization often leave critical exposures wide open. This talk will help you reframe security metrics to reflect actual risk posture, not just resolution timelines. Whether you're a security engineer, a risk analyst, or a leader driving strategic programs, you'll learn how to shift your org's focus from SLA compliance to measurable, meaningful security health.

Experience Level: Intermediate



Building a Threat Hunting Program from the Ground Up

Ryan Fried

*Principal Security Consultant,
Mandiant*



Estefania Michael

*Senior Security Consultant,
Mandiant*

Go beyond traditional detection methods and proactively hunt for threats lurking within your environment. This session provides a practical guide to building a threat hunting program from scratch. Learn how to assemble a team leveraging existing people from the SOC, IR and penetration testers, establish documented processes, and leverage expertise to identify post-compromise behavior. Discover the essential components of a successful program, including access to data, team members threat intelligence, and the right tools and licenses. Explore different types of threat hunting: hypothesis-driven, TTP-based, anomaly-based, and IOC-driven, with real-world examples. Understand how proactive threat hunting minimizes the impact of breaches, reduces dwell time, prevents financial losses, and improves overall security posture. Walk away with actionable steps to implement a threat hunting program and enhance your organization's security.

Experience Level: Foundational



Business Logic Flaws: How to Prevent Them in Your Web Apps

Antoine Carossio

CTO & Co-founder, Escape

Business Logic vulnerabilities are not bugs in code—they're failures in design, especially difficult to detect in modern applications. They occur when an attacker leverages valid features in unintended ways to bypass rules, abuse workflows, or manipulate sensitive operations. These flaws don't show up in typical vulnerability scans, yet they can lead to major financial, reputational, and compliance damage.

This session explores how these issues arise in real-world systems, including REST and GraphQL APIs, and why they often go undetected until exploitation. Drawing from field experience building detection algorithms that analyze undocumented API behavior, we'll discuss practical techniques to identify logic flaws early.

Attendees will learn how to incorporate business logic awareness into their threat modeling, improve test coverage in CI/CD pipelines, and build more resilient applications by understanding how users—and attackers—can interact with functionality at scale.

Experience Level: Intermediate



Crypto Agility Lifecycle: A backbone of a Resilient System

Sandip Dholakia

*Principal Security Architect,
SAP America*

Are quantum computers a real threat to information security? If quantum computers were available today, how safe would your data be? How can we prepare to migrate and adapt to new cryptographic algorithms faster and seamlessly?

Any organization's goal should be to create and establish a crypto agility lifecycle that not only protects us from the imminent threats of quantum computing but also allows us to modify, replace, and adapt cryptographic algorithms, protocols, and implementations to make the cryptographic transition agile and protect against potential threats.

Join Cybersecurity professional and cryptographer Sandip Dholakia as he proposes the Crypto Agility Lifecycle, which streamlines cryptographic transitions and enhances security. Find out if quantum computers are a real threat to cryptography and how to implement the crypto agility lifecycle to prepare your data and applications for post-quantum cryptography and other potential cryptography transitions.

Experience Level: Intermediate



Decoding Dyslexia: Thriving in Cybersecurity with a Different Brain

Caleb Grossnickle

*Cybersecurity Analyst 2,
StoneX*

Cybersecurity is a field that thrives on diverse thinking, pattern recognition, and creative problem-solving — all strengths that often come naturally to those with dyslexia. But for many, dyslexia is still seen as a barrier instead of an asset. In this talk, we'll challenge that perception.

I'll share a personal journey of working in cybersecurity while navigating dyslexia, offering practical strategies for success. From how to advocate for yourself in the workplace and build a support system, to using free tools like dyslexia-friendly fonts, high-contrast settings, and even ChatGPT to simplify complex logs — this session is packed with real-world advice.

We'll also reframe the narrative around dyslexia, focusing on the unique strengths it brings to our field. Whether you're dyslexic, work with someone who is, or just want to make your team more inclusive, you'll leave this talk with a better understanding of how neurodiversity can elevate cybersecurity.

Experience Level: Foundational



Detection Opportunities for Countering Remote Employment Fraud: A Phase-based Strategy

Alex Orleans

Principal Threat Intelligence Analyst, Splunk



Jonathan Heckinger

Director, Threat Detection, Splunk

Various threat actors, particularly those associated with the North Korean government, are actively pursuing insider access to Western companies through acquiring remote work positions, particularly in the information technology (IT) sector. These remote employment fraud (REF) operations — also known as “fraudulent remote IT work”, “remote work scams”, and “IT worker fraud” — are typically meant to generate revenue for either individuals or their governments; they can also be used to facilitate initial access for network intrusions or intellectual property theft.

Detailed analysis of malicious activity has enabled our team to reconstruct a three-phase model of how REF operations are run and identify behavioral and technical detection opportunities to interdict threat actors throughout their operational lifecycle. The three operational phases of “Pre-Hire”, “Hiring and Onboarding”, and “Immediate Post-Hire” each present opportunities for multiple business units to contribute to disrupting threat actors’ efforts to acquire remote work roles. Given the fundamental nature of REF as a threat and a strategy, early behavioral detection is the first and best line of defense, although technical indicators are also vital when countering particularly skilled adversaries.

Since the challenges associated with REF are more akin to those associated with insider threats than network intrusion activity, how they present through REF raises significant social and legal challenges. This emphasizes the criticality of cross-functional collaboration between security teams, talent acquisition specialists, and line hiring managers in countering innovations in REF tradecraft.

Experience Level: Intermediate



DFIR-as-Code: Scaling Incident Response Beyond Human Limits

Justin Borland

*Director of Threat Engineering,
Abstract Security*

Incident response is still broken. We still treat DFIR like an unpredictable, ad-hoc fire drill. Manual evidence collection, inconsistent analysis, and re-invented wheels on investigations. It's time to evolve. DFIR-as-Code is the missing framework: a paved path for automating forensic data collection, enrichment, and triage. This talk breaks down how to apply IaC principles to DFIR, predefine secondary collection mechanisms, and map out an extended lifecycle that ensures repeatability, speed, and accuracy. Whether you're hunting for adversaries in memory, uncovering new persistence mechanisms, or automating forensic pipelines, this session will show you how to shift DFIR from chaos to code – at scale.

Some concepts of DFIR-as-Code have been used in many large environments where scale preempts performing things manually. This talk provides a framework for evolving how DFIR is currently performed from art into science. By leveraging successful IaC concepts in the continually evolving DFIR landscape, defenders can continually improve threat detection, and decrease response time across many different facets of the incident response lifecycle.

Experience Level: Intermediate



Did I Do Thaaat? How not to “whoopsie” production away, a humanist risk-management-based approach.

Daniel (Bogo) Bogomolny

*Head of Research,
Seemplicity Security*

We’ve all been there—a mistyped command, an unintended click, a moment of bad judgment, or just a house cat in the wrong place at the wrong time—and suddenly, something goes awfully wrong.

Whether it’s an accidental table drop on a critical db, an unintended network outage, or a whole filesystem going bye-bye, the consequences can be dire. Your heart rate skyrockets, you’re drenched in sweat, and it’s possibly even worse if it’s a red team engagement in someone else’s environment (yikes).

Human error is an inevitable part of working with live environments. But while mistakes are unavoidable, their impact doesn’t have to be catastrophic—and many can be prevented entirely.

This talk covers both how to avoid mistakes and how to minimize their impact when they do occur, through a risk management approach.

We’ll discuss practical tactics to reduce both the likelihood and impact of human error in our critical environments, addressing aspects from both the technical (keep the cat away) and the mental (be humble, it CAN happen to you).

We’ll also explore how to quickly learn from our mistakes (and others’), and ensure that knowledge is passed on to our colleagues and especially to juniors—so we all get better together, All while fostering a culture where learning from mistakes is encouraged rather than feared, and where taking pride in our hard-earned lessons is the norm.

This talk is for everyone—from students to managers, Blue Teamers to Red Teamers alike.

Experience Level: Foundational



Flipping the Script: Threat Intelligence Mining of Ransomware Chat Leaks

Mark Reibel

Principal Incident and Threat Analyst

Frequently, threat intelligence teams are relegated to consuming threat intelligence, whether it be via paid indicator feeds, cybersecurity company write-ups, or social media posts. While this data is critical for day-to-day cyber operations, threat intelligence analysts should ultimately strive to produce quality, original, and actionable threat intelligence themselves. With the recent Conti and BlackBasta ransomware chat leaks, threat intelligence teams have been gifted a treasure trove of data containing valuable insights into ransomware operations, the advanced TTPs deployed during network intrusions, and rare visibility into the “humans behind the keyboard.” Aimed at threat intelligence analysts as well as cybersecurity operations teams, this talk will use sample data from the recent BlackBasta chat leak to show how teams can triage indicators of compromise for quick tactical wins (without having to wait for security vendor feeds/write-ups), identify strategic and operational patterns, and incorporate these new intelligence insights into an organization’s threat model. Attendees will walk away with a strategy for processing mined data from ransomware chat logs, actioning these findings into future threat hunting scenarios/detection engineering opportunities, and options for sharing this newly produced intelligence with the broader threat intelligence community.

Experience Level: Intermediate



Forged in Fire: Building Elite Cybersecurity Teams with a Warrior's Mindset

Chris Reider
GreenThumb Industries

In 2020, I found myself at a robotics startup in Silicon Valley, building an Information Security program from scratch. No team, no tools, no roadmap — just a mandate to get us FedRAMP Moderate compliant while supporting the building of a highly complex robot. As I dove in, I realized I was drawing heavily from a different life — one built on leadership forged in pressure.

I spent my early career in the U.S. Marine Corps, supporting a Special Operations training detachment as a true “keyboard warrior.” That was followed by nine years in law enforcement, eight of which were with a Special Operations team as both an operator and a leader. I didn’t grow up obsessed with tech, but I always used it as a critical tool — from red teaming and security audits to building field tech and tracking child predators online.

Along the way, I saw firsthand how ineffective leadership could derail progress. Too often, IT leaders resisted change, innovation, or simply leading from the front. I promised myself I’d be different.

In this talk, I’ll share the leadership principles that have shaped my teams and my career:

- » Leading with Purpose, Not Process
- » Building Trust and Grit
- » Thinking Tactically, Acting Strategically
- » Leading from the Front
- » Becoming a Leadable Leader

Through real-world stories — some wild, some hilarious — I’ll deliver lessons attendees can apply immediately to become stronger, more adaptive leaders in InfoSec and beyond.

Experience Level: Intermediate



Foundations of Resilience: Mastering the Business Impact Analysis

Jeremy Croghan

*Director – Cyber Risk Advisory,
Coalfire*

What would happen if your organization faced a significant outage, cyberattack, or supply chain disruption tomorrow? If you can't quickly identify critical functions, acceptable downtime, or cascading impacts, your continuity strategy may fail precisely when needed most. Effective continuity planning begins with a Business Impact Analysis (BIA).

This session explores why a BIA is the foundational step for building robust business continuity, disaster recovery, and incident response capabilities. Attendees will learn how conducting a BIA clarifies operational priorities, maps critical dependencies, and establishes essential recovery metrics such as Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and Maximum Tolerable Downtime (MTD). Practical guidance will be provided on conducting stakeholder interviews, accurately documenting dependencies, validating results, and effectively communicating findings to executive leadership.

Additionally, the discussion will highlight how a well-executed BIA strengthens cross-domain integration across Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and Incident Response Planning (IRP), facilitating a cohesive resilience strategy. Common pitfalls, including inadequate stakeholder involvement and lack of executive sponsorship, will be addressed with pragmatic recommendations for overcoming these challenges. Whether creating a new continuity plan or refining an existing one, participants will gain actionable insights into conducting an impactful BIA, fostering stronger alignment between business and technology teams, smarter resource allocation, and enhanced organizational resilience.

Experience Level: Foundational



From Alerts to Action - LLMs for Explainability, Entity Analysis, and Escalation

Kevin Gonzalez

*Vice President of Security Operations and Data,
Anvilogic*



Scott Rodgers

*Principal Data Scientist,
Anvilogic*

Analysts are flooded with alerts, but understanding them fast and accurately is the real challenge. In this talk, we'll show how language models (LLMs) and entity recognition techniques can transform alert triage and escalation workflows.

Using named-entity recognition (NER), we'll show how alerts can be enriched at scale with actionable context automatically identifying IPs, hosts, and users. We'll also demonstrate how LLMs can extract indicators of compromise (IOCs) from unstructured data, summarize alert chains, and even generate human-readable explanations to assist triage.

This talk isn't about hypothetical AI. It's a grounded, practical walkthrough of how defenders can operationalize natural language models today to make alerts clearer, faster to act on, and more informative.

Experience Level: Advanced



Going Beyond Box Checking with Annual Pentests

Sean "4dw@r3" Juroviesky
Senior Security Engineer

Every year in order to maintain compliance or satisfy client requests, your organization purchases an independent penetration test. How often do you already know 95% what a Pentest will turn up? You've probably had a lot of these risks for years without the funding, time, or staff to fix them.

Oftentimes executives see the opinions of a 3rd party to be impartial and unfortunately more compelling than their own staff. You can use this strategically to help acquire the resources your department needs to finally close out these risks.

We'll walk through how to communicate your needs to your pentesting partner so they can tailor the executive summary to precisely communicate the potential business impact of these risks using language your executives are familiar with.

Experience Level: Intermediate



Hidden Dangers Of AI In Developer Workflows: Navigating Security Risks with Human Insight

Dwayne McDaniel

*Senior Developer Advocate,
GitGuardian*

AI tools like ChatGPT and Copilot have become indispensable in developers' daily workflows. Whether it is for code samples and scaffolding, prototyping, or documentation, AI can help eliminate a lot of toil from the developer's day-to-day.

The hidden dangers that AI have introduced that are worth exploring.

This presentation will look at the critical security challenges associated with AI-enhanced development workflows and the essential role of human oversight in mitigating these risks.

We'll look into three major areas of concern:

1. The AI told me to do it that way
2. Hallucinations everywhere
3. Where did my data go?

Join this talk to see some real examples of AI getting it wrong, but stay for a discussion on how you can leverage already existing tools to make the best use of the most valuable resource in the company, your team's time. Expect to leave with a fresh perspective on how bright a future we can build as people fostering more secure and efficient development practices.

Experience Level: Foundational



How Attackers are using AI and how to defend against them, by an incident responder turned AI researcher.

Eyal Fisher
CTO

This talk analyzes how attackers' use of AI is amplifying existing cyber threats, making them more sophisticated and numerous. Particularly, how attackers are using AI to enhance phishing campaigns, automate social engineering, conduct influence operations, and craft malware—significantly reducing the time to exploit vulnerabilities. We'll review recent publications by top AI labs exposing malicious uses of AI, including the potential for identifying new exploits and zero-day vulnerabilities.

We'll demonstrate that AI training methods can predict which offensive activities AIs will excel in, offering insights into attackers' capabilities and informing defenders on how to prioritize their efforts. By understanding these patterns, security teams can better anticipate future threats. As AI technology continues to improve, these threats are expected to escalate, leading to higher alert volumes, shorter exploitation windows, and increased discovery of vulnerabilities.

We'll highlight the implications for security teams and discuss strategic preparation steps: adopting advanced application security programs, protecting application perimeters against zero-days, managing legacy code challenges, and leveraging AI-powered solutions to enhance your Security Operations Center (SOC) and improve security automation. Attendees will gain actionable insights to fortify their defenses and stay ahead in the evolving cybersecurity landscape.

Experience Level: Intermediate



Hunting Path Traversal in Open Source

Nishant Jain

*Application Security Lead,
Loom*

Ever wonder if path traversal bugs are a thing of the past? In this talk, we'll see how one advisory led me to discover multiple vulnerabilities across various open-source projects. I'll walk through how I tested both unprotected and "defended" systems, collaborated with maintainers on fixes, sometimes even writing them, and uncovered issues with weak sanitizers. Expect practical tips, lessons learned, and ideas for better security reporting so you can spot and fix path traversal flaws before they become major issues.

Experience Level: Intermediate



Inside Ransomware Negotiations: Strategies and Insights from the Front Lines

Matthew Leidlein

*Founder & President,
Digital Asset Redemption*

Ransomware negotiations represent critical intelligence-gathering opportunities that most organizations overlook. This presentation reveals how security teams can extract and leverage threat intelligence during ransomware incidents while working with professional negotiators. Drawing from case studies of actual negotiations, we'll demonstrate how properly collected intelligence shapes response strategies and informs future defenses.

Attendees will learn which technical artifacts to preserve during negotiations, how to identify threat actor TTPs from negotiation patterns, and methods for correlating negotiation behaviors with specific threat groups. We'll examine how intelligence gathered during negotiations has helped organizations prevent follow-up attacks and strengthen their security postures.

The presentation includes examples of intelligence collection frameworks that security teams can implement before incidents occur, ensuring they capture valuable data when ransomware strikes. We'll also discuss how to effectively partner with professional negotiators, what information they need from technical teams, and how this collaboration produces better outcomes.

This session equips security leaders and practitioners with practical approaches to transform the crisis of ransomware negotiations into valuable intelligence that strengthens organizational security posture and contributes to the broader defense community.

Experience Level: Intermediate



Introducing a password manager and policy

L
Cloud Operations Manager

Implementing a password policy and password manager at an organization is a challenge that winds up touching every aspect of a business. There can be entrenched processes, kingdoms, and assumptions that will have to be addressed every step of the way.

In this presentation I will talk through some of the tribulations that I experienced through this step on the security modernization process and share the lessons I learned and things I wish I had known. It will also cover important considerations when looking at various vendors, determining requirements, and how to talk about modernization to company leadership.

Along the way there will be unexpected complexity and challenges requiring technical, procedural, and political skills. There is a lot to be gained but a lot of hurdles to be overcome.

It's kind of like a role playing video game but the reward at the end is slightly better sleep.

Foundational



Introducing QELP: Parsing ESXi Logs for Incident Response

Phalgun Kulkarni

*Sr. DFIR consultant,
Aon/Stroz Friedberg*

Partha Alwar

*DFIR Director,
Aon / Stroz Friedberg*

Mitchell Green

*Director,
Aon's Cyber Solutions*

Threat actors frequently target ESXi servers to disrupt business environments and deploy ransomware to encrypt datastores. We have identified common tactics and techniques that threat actors have used to disrupt services on ESXi servers. Some of these TTPs include enabling SSH to access ESXi servers remotely, changing root user passwords to disrupt access to ESXi servers, and deploying ransomware binaries to encrypt ESXi servers and datastores. Detecting this malicious activity can be time consuming and challenging, especially when dealing with a significant number of logs from multiple ESXi servers or partial encryption of the logs during ransomware incidents.

To better overcome these analysis challenges, we are introducing an open-source CLI tool named Quick ESXi Log Parser ("QELP") that will enhance investigations by swiftly parsing ESXi logs at scale and producing CSV reports in timeline format. Key features of QELP include:

1. Parsing ESXi logs from multiple ESXi servers in a timely and efficient manner.
2. Parsing partially encrypted ESXi logs.
3. Output to CSV reports for easy ingestion and analysis.
4. Timeline generation of the most relevant events to form an overall picture of the events that occurred on ESXi server.

Additionally, we also touch upon how the logs can be collected from ESXi servers, ensuring a comprehensive approach to log analysis.

Attendees will gain insights into threat actor activities observed on ESXi servers, information on logs containing relevant information, as well as a tool (QELP) to overcome the challenges faced during parsing and analyzing ESXi logs.

Experience Level: Foundational



Lies, Lures, and LLMs; Augmenting Cyber Deception with AI

Dylan Shroll

Security Engineer, revology

The presentation, “Lies, Lures, and LLMs,” explores how Large Language Models (LLMs) can revolutionize cyber deception operations by crafting realistic digital personas, automating interactions, and producing high-fidelity artifacts to mislead adversaries. These advancements enhance cybersecurity by revealing adversary behavior, minimizing risks to organizations, and enabling deception at scale.

Persona development is central to this approach, requiring alignment of primary attributes (e.g., age, occupation) and secondary characteristics (e.g., personality, communication style) to create convincing digital footprints. Through effective prompt engineering and fine-tuned LLMs, synthetic personas can autonomously engage adversaries, as demonstrated by a case study involving 10 personas that produced thousands of interactions, flagged suspicious activity, and connected with hundreds of users.

This scalable approach shifts the power dynamics in cyberspace, allowing defenders to proactively disrupt attackers’ tactics while reducing operational costs. The research underscores the transformative potential of AI-driven deception to safeguard organizations, elucidate adversarial behaviors, and maintain an edge in the evolving threat landscape. Future efforts will focus on broader adoption, fine-tuning models, and testing on major platforms to further scale these capabilities.

Experience Level: Intermediate



LLM-Powered Vulnerability Management Operations: Use Cases and Success Stories

Cong Zheng

*Software Engineer,
Meta Platforms Inc.*



Darcy Meyer

*Software Engineer,
Meta Platforms Inc.*

Vulnerability management is critical for any organization's security posture, but the volume of vulnerabilities, combined with the complexity of modern software systems, makes it challenging for vulnerability management teams to prioritize and remediate effectively by manual efforts.

In this talk, we will explore the practical applications of LLMs in vulnerability management operations. We will discuss how LLMs can be used for automations in the SecOps daily operations, including: identify the ownership of a vulnerability task, identify the impacted products by a vulnerability task, triage the third-party library vulnerability, detect the third-party library metadata for vulnerability detection and triage static and dynamic analysis issues.

Through real-world use cases and success stories, we will also provide guidance on how to use LLM and integrate LLM into existing vulnerability management workflows and highlight the benefits of using AI-powered tools to improve the efficiency of security operations.

Experience Level: Intermediate



Maturing your cyber deception program: What's the plan?

Suril Desai

VP Engineering, Acalvio

Defense teams are adopting cyber deception to detect and hunt threats. Honeypots and honeytokens provide early warning of attacker actions. One of the challenges that defenders grapple with is: where should I place these deceptions? How many should I deploy? What should they represent?

This session provides real-world insights from a security practitioner on strategies for an effective rollout of cyber deception. Learn about the importance of identifying the goals for your deception program, one that focuses on defending against threats, protecting high-value assets, slowing down the adversary.

See how deception can be used to defend against identity threats, insider risk, and ransomware. Learn about the considerations and best practices for deception design. This provides you with practical insights that can be applied on a daily basis for cyber defense.

Experience Level: Foundational



Prescription for Security: Hardening Healthcare Email Against Advanced Threats

Akash Parasumanna Sridhar

*IT Cybersecurity Analyst,
Campbell Clinic*

Email remains one of the most critical yet vulnerable components of healthcare cybersecurity, often serving as a primary vector for sophisticated cyberattacks such as phishing, business email compromise (BEC), and targeted malware infections. Drawing from hands-on experience defending healthcare organizations, this talk will examine real-world email threats uniquely targeting healthcare, including advanced techniques like Captcha-based phishing (Luma Stealer attacks), QR code phishing, and multi-factor authentication (MFA) bypass using adversary-in-the-middle (AiTM) tactics.

The presentation will highlight practical challenges healthcare security teams face, such as the risks posed by excessive email whitelisting, misconfigured authentication protocols (DMARC, DKIM, SPF), and the growing threat of sensitive data leakage driven by employee use of AI tools. Attendees will gain actionable insights and strategies for enhancing email security posture through smarter threat detection, optimized security policies, and tailored data loss prevention (DLP) controls to protect against AI-driven data leaks.

Designed specifically for blue team professionals, SOC analysts, and cybersecurity leaders, this session will equip participants with practical techniques to detect emerging email threats, reduce attack surface from third-party risks, and implement proactive, healthcare-focused security defenses.

Experience Level: Foundational



Securing Sideways: Thwarting Lateral Movement, with no extra software!

R. Tyler Schroder

*Cybersecurity Engineer,
MITRE*

“What keeps me up at night? Active Directory (AD) infrastructure without proper segmentation”

What if there was a way to prevent ransomware breakouts from owning an entire environment, without any new tooling or licenses? AD tiering offers defenders a chance to contain, if not completely prevent, threat actors from escalating privileges to deploy malware.

Identity is the crown jewel of any corporate network. In a traditional network, threat actors compromise high-risk, low-privilege end-users and work their way up to the identity plane to establish control over an environment. With control over the environment, ransomware or other theft can happen easily.

Tiering provides an additional layer to defense in depth strategies. Tiering splits a domain into three logical boundaries: Tier 0 (identity/management), Tier 1 (non-IT management infrastructure), and Tier 2 (end-users, high risk endpoints). Identities and devices from Tier 2 cannot access Tier 1 or Tier 0, and Tier 1 cannot log in to Tier 0 devices. Tiering pulls inspiration from watertight bulkheads on a ship: a compromise in one component cannot take out others. A threat actor breaking into a Tier 2 laptop has no lateral movement pathway to a domain controller or other identity management device. Damage is contained to just Tier 2.

Current available blog posts or documentation focus are exclusive to tech or business concerns, in one specific environment type. This session packages everything together in an easy-to-follow format. In this thirty-minute session, Securing Sideways will introduce the audience to tiering, how to implement tiering in an on-prem, hybrid, or cloud environment, and address operational and business concerns before tiering should be implemented.

Intermediate



Things didn't go as planned... because you didn't have a plan"

ODDJOB

Host of Glassof0J

Planning for incident response is too late when an incident has struck! With no clear path for decision making, roles and responsibility, or technical capabilities, an organization will flounder and blunder its way through often making an incident far worse than it has to be. You will walk away from this talk with a clear set of goals and starting points to drafting and publishing your own Incident Response Plan!

Experience Level: Foundational



Solving Secrets Sprawl Takes More Than Security: Why Machine Identity Is Everyone's Problem

Dwayne McDaniel

*Senior Developer Advocate,
GitGuardian*

When a security event occurs, most teams tend to jump into a circle of blame. Everyone takes their turn saying, "It can't be my fault. If only that user had not clicked on that link," or "If that developer had not hardcoded that credential, then none of this would have happened." Unfortunately, for many companies, the Security team is ultimately seen as at fault when a breach happens; after all, it is a security incident.

Long-lived credential leaks, aka secrets sprawl, are possibly the single largest security risk every organization is currently facing. The reality is that no security team can solve this growing issue on its own. This is going to take a full team effort and rethinking some of the relationships and silos we have become accustomed to in the tech world. There has never been a better time to rethink how we build complex applications and how they interact with the world.

In this talk, you will:

- » Get an update on the latest secrets security research
- » Ask who really owns security and identity
- » Map possible routes for a secrets-free future
- » Rethink git and pull requests workflows and see why that is more involved than you think

Experience Level: Foundational



Technical Writers: Your Cybersecurity Secret Weapon

Jennifer Miller

*Senior Technical Writer - Information Security,
PRA Group*

Technical writers are a fixture in software development, but you may not realize the business value technical writers add to Cybersecurity teams. In this presentation, a Cybersecurity technical writer shares the data and research that demonstrates the value across multiple dimensions: operational efficiency, cost optimization, team productivity and retention, improved security posture, and knowledge management.

With trust and reliability being cornerstones of Cybersecurity, it follows that communication and documentation are more than just basic requirements; professionally crafted and managed communication and documentation shared with external stakeholders provide an outward representation of your team's reliability and professionalism. Similarly, professionally crafted internal communication and documentation, as well as professional document management, optimizes your team's operations and provides cost savings. Development teams have long seen the value in technical writers as team members. Now learn how a technical writer can take your Information Security team to the next level – and provide value far behind what ChatGPT offers.

This presentation provides the data and research that demonstrates the real cost savings, enhanced productivity, and improved team and knowledge retention that a managed documentation program provides. As a Senior Technical Writer assigned to an Information Security team, the presenter will share not only the data and research that shows the benefits but also her experience building out the documentation plan for her team.

Experience Level: Foundational



The Cost of an Incident

Amanda Draeger

*Principal Cyber Risk Engineer,
Liberty Mutual Insurance*

For those incidents that are publicly reported, we see things like “this cost \$X million dollars”. Where do those costs come from? How can you use these costs to convince your leadership to invest in security? This talk will look at data from insurance claims to explain where the costs of an incident come from.

Experience Level: Intermediate



The Death and Rebirth of Vulnerability Management

HD Moore

Founder of runZero

The year is 2025. We have successfully built a process that takes creative, complex, and innovative security research and turns it into the duller workflow imaginable. Vulnerability management is now a checkbox feature in every major IT product suite. The few remaining first-wave vulnerability scanners have long-since shifted investments into adjacent markets to maintain their growth. Security teams struggle to piece data together from disparate tools. Aggregation products and a funnel-based prioritization process have become the norm, but attackers are still winning. There are a few bright spots on the horizon, but the path between here and there isn't clear.

This session will dig deep into the state of vulnerability management and explore the effectiveness of modern tools at preventing real-world incidents. This will include an analysis of vulnerability coverage, detection methods, and their tradeoffs between traditional vulnerability scanners, endpoint-based vulnerability management, and the bleeding edge of open source security tools.

Experience Level: Intermediate



The False Sense of Security: Defense Becoming a Vulnerability

Nathan Eades

Director of Adversary Detection

In the evolving landscape of identity security, Microsoft Entra ID's Privileged Identity Management (PIM) stands as a cornerstone solution promising just-in-time (JIT) access and least privilege enforcement. However, beneath this security veneer lies a troubling reality that many organizations fail to recognize, or won't admit. This session will peel back the layers of PIM and JIT implementation to reveal how this widely-adopted control has often created a false sense of security rather than meaningful protection.

Drawing from experience analyzing diverse customer environments, I'll demonstrate how common PIM implementations can reduce security to a mere procedural formality – transforming “just-in-time” into “just-a-button” that sophisticated adversaries easily circumvent.

I'll reveal a couple gaps in PIM and improvements that convert checkbox security into actual protection.

Experience Level: Intermediate



What Now? Navigating the Transition from Engineer to Manager

Cory Roop

Senior Manager, Security, Spring Health

In the early days of my career I never thought beyond the next job, the next pay increase, the next promotion. That is until I made the shift fully into security. Frustrated at the lack of impact I was able to have at an organizational level as an engineer, I made the decision to push for a shift into management without fully understanding what that shift would entail. When the time came I was woefully unprepared.

My situation is not unique and I don't claim to have a magic solution that will work for every engineer who tries to make the same career move that I did. My goal is to point out some of the things that made my transition harder than it needed to be so that others don't make the same mistakes.

1. You're not an island (or if you are, what can you do to make things easier?)
2. "I'll definitely still have plenty of time for engineering work."
3. Your team are not your peers anymore.
4. Learn to think strategically rather than tactically.
5. Don't neglect your mental health.

Experience Level: Foundational



Which Witch is Which – Navigating the Complicated World of Threat Actor Taxonomy

Jeffrey Bell

Principal Information Security Engineer and CTI Lead, Norstella

Navigating the vast landscape of threat intelligence can be overwhelming, particularly when an organization is trying to determine who may be targeting them. If an intelligence team suspects the ransomware group Akira is behind suspicious activity, it's crucial to understand their Tactics, Techniques, and Procedures (TTPs). However, Akira may be referenced under different aliases depending on the vendor, making it difficult to form a full picture of the threat actor. This inconsistency often stems in part from the commercialization of Threat Research Programs (TRPs), which led to fragmented naming and attribution across the industry. Establishing a "perfect" taxonomy for Threat Actors (TAs) is no easy task – technical aliases like "APT63" are precise but forgettable, while names like "WARLOCK DUST" are memorable but provide the TA with super-villain notoriety. Further complicating matters, threat actor groups frequently evolve, merge, rebrand, or reappear, making identification even more challenging. This presentation will unpack how these confusing naming conventions developed and share actionable ways to gather intelligence from multiple sources to better understand and respond to threat actors.

Experience Level: Intermediate



Why Your Email Matters

BitsDanceForMe

*Systems Architect,
BlueHalo*

With all the ways to create new accounts, people often forget the value of their email address. In this presentation, we will take a look at how creating accounts with the wrong email address greatly reduces the bar for any social engineering attack. Specifically, we will look at how multiple accounts can be combined to gain a complete picture of who you are. The innocent will be protected but their shame will not.

Hopefully we will also get a glimpse into responsible vulnerability disclosure (I'm working on these now, FWIW.)

We will also discuss how you can find accounts linked to your email address.

Experience Level: Foundational



Adventures in the Underland: Uncommon Hacker's Persistence Methods and Countermeasures

Paula Januszkiewicz

*Founder & CEO,
CQURE*

Persistence is one of the main aspects that hackers pay special attention to during the malware development and during the attack phase. The goal is very simple: to be as stealth as possible. Usually, attackers aim to maintain the presence in the target's network by installing malware on various workstations and servers. However, the main challenge for them is that the malicious code needs to be available also after reboot, so the best solution would be to put it in a place that most monitoring tools will not discover. Sneaky, right? And when this persistence finally pays off, ransomware begins to act and problems arise. Since there are so many places on Windows to hide even from the best monitoring tools, it would be great to become familiar with at least some of them, especially the uncommon ones!

During this session, Paula will demonstrate several less common persistence methods we should all be aware of. All the stories and scenarios presented during the demonstration are taken from real life, so don't miss it and leave with suggestions & ideas on how to reach the next level of security in your workspaces.

Experience Level: Intermediate