September 5-8, 2024
Fairmont Chicago

BlueTeamCon.com

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 fourth Blue Team Con! On behalf of the advisory board, I am thrilled to welcome you all to this year's event in Chicago. Whether you're a returning attendee or joining us for the first time, we are excited to have you with us as we embark on another conference filled with learning, collaboration, and fun in the world of defensive cybersecurity.

Over the past four years, Blue Team Con has grown into a unique gathering place for security professionals dedicated to safeguarding our digital world. This year is no exception, and we've curated an incredible lineup of speakers, villages, training and other activities that reflect the latest developments, challenges, and solutions in our field. Our goal is to provide you with practical insights and invaluable connections that will empower you to strengthen your defenses and elevate your cybersecurity practice.

As you explore the conference, I encourage you to take full advantage of the opportunities to engage with our community. Whether it's during a talk, at a village, or competing in our Capture The Flag events (my favorite! If you haven't participated before, try it!), the conversations you have here can lead to lasting professional relationships, fresh perspectives, and new ideas that will help drive your success in the coming year.

None of this would be possible without the dedication and hard work of our advisory board, volunteers, speakers, trainers, sponsors, and partners. Their contributions have been instrumental in making Blue Team Con a great event for the defensive cybersecurity community. I would also like to thank you, our attendees, for your commitment to being here and for your passion for the work we do together.

As we kick off this year's conference, I'm confident that you'll leave with a wealth of knowledge, inspiration, and perhaps a few new connections. Here's to a fantastic and enriching experience at Blue Team Con 2024!

Thank you for being part of our community, and welcome once again!

Becky Selzer
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.

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 is characteristically and can take 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.
- ✓ Presenting staff or volunteers in 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.)
- ✓ Providing or participating in the service of alcohol to anyone under the legal drinking age, in accordance with applicable laws and regulations
- ✓ 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 unsafe, 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.

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

@L1ttleR3d

BECKY
Selzer

becky@blueteamcon.com

@BeckySecurity

FRANK
McGovern

frank@blueteamcon.com

@FrankMcG

PHIL
Skentelbery

phil@blueteamcon.com

@PhilSkents

ALYSSA
Miller

alyssa@blueteamcon.com

@AlyssaM_Infosec

STEL
Valavanis

stel@blueteamcon.com

@StelValavanis

CFP
Board Members

KAYLEE
Burns

XENA
Olsen

KEVIN
Jackson

CASEY
Shuniak

CHRIS
Lemmon

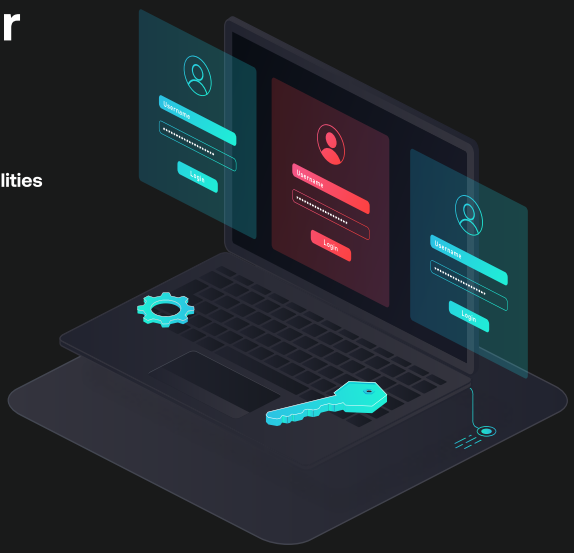
CHRISTINA
Stokes

Push
pushsecurity.com

Push turns every browser into a telemetry source and control point

Proactively harden your identity attack surface

- Discover all your identities, apps, accounts and vulnerabilities
- Get unmanaged accounts behind SSO
- Block unapproved SaaS apps
- Enforce MFA and SSO logins
- Detect stolen credentials for sale on the dark web
- Eliminate leaked, weak and reused passwords



Detect and respond to identity attacks

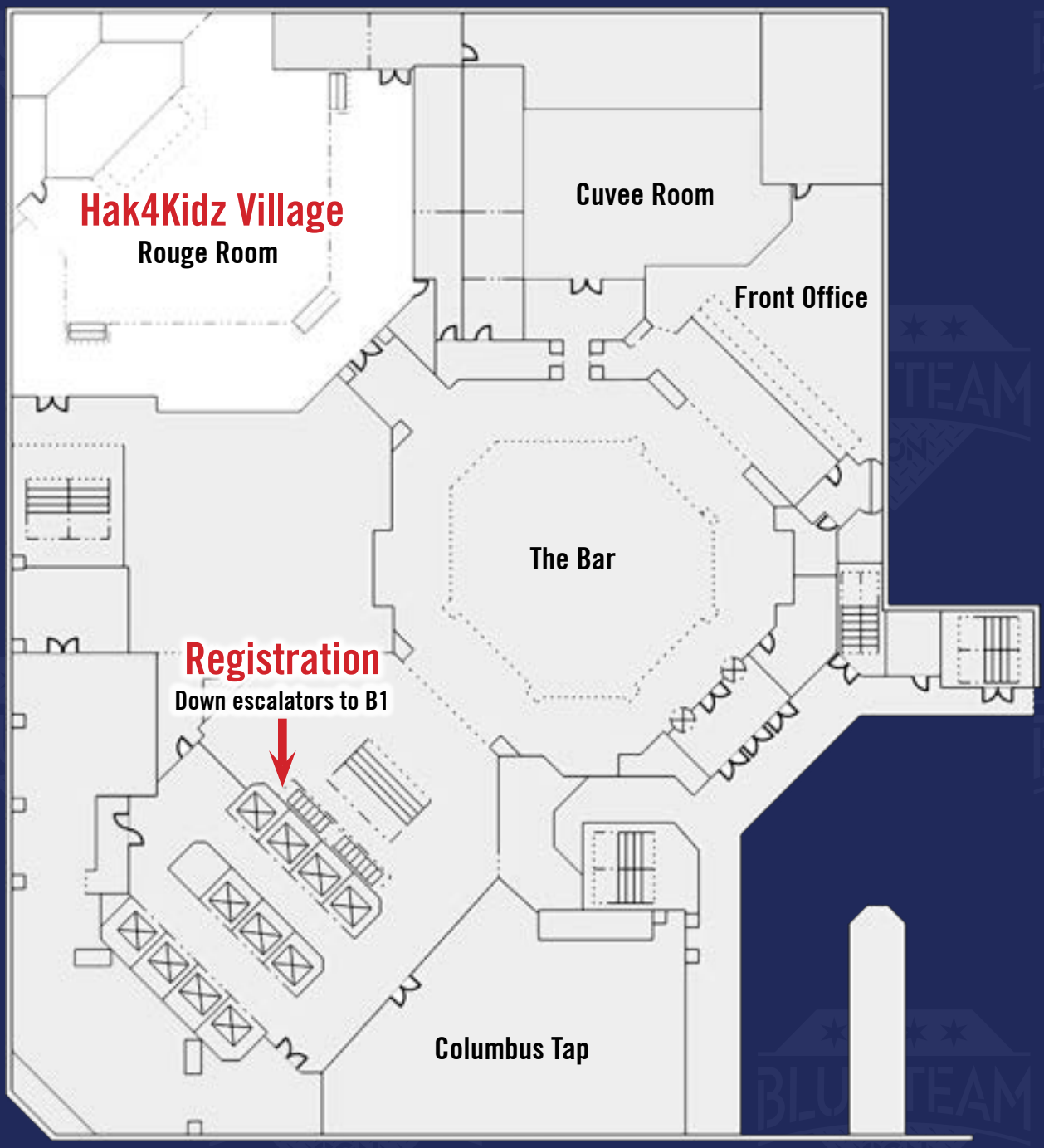
- Stop employees entering creds into phishing sites
- Block AitM and BitM toolkits
- Detect and block cloned app login pages
- Block malicious URLs
- Detect session hijacking using stolen tokens
- Get rich telemetry across your identity attack surface

SOPHOS GitLab tray.io British Heart Foundation upvest Sanlam THINKST CANARY PortSwigger

4.9/5 on G2 | 5/5 on Capterra

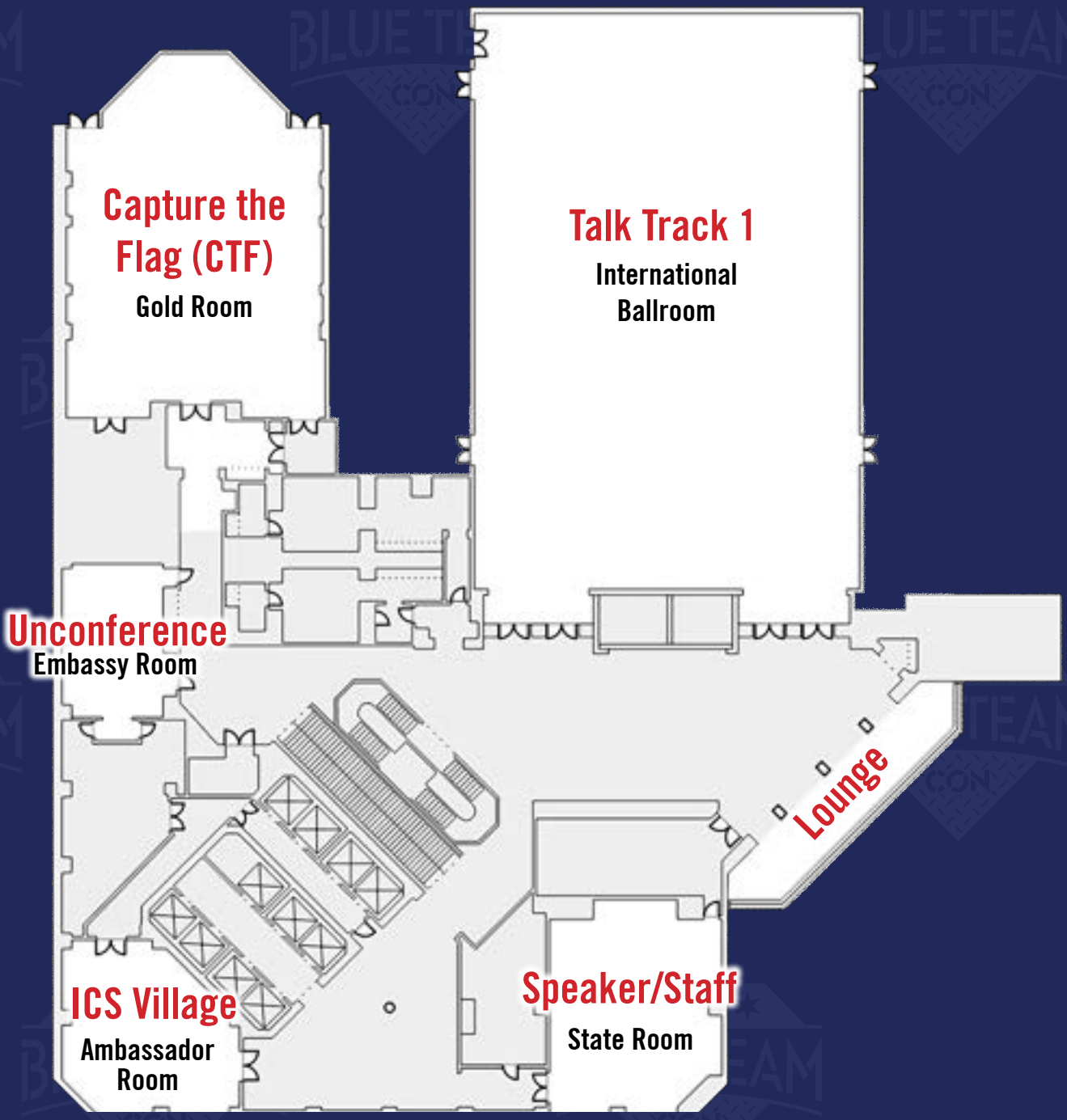
Venue

Level ONE



Venue

Level TWO



Venue

Level THREE

Schedule *All times are in CDT.*

Wednesday, September 4

Training Registration Only: 6:00 pm to 8:00 pm (Fairmont Level B1)

Thursday, September 5

Training Registration Only: 7:00 am to 11:00 am (Fairmont Level B1)

You will be guided to Training via the Registration Desk.

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 6

Training Registration Only: 7:00 am to 10:00 am (Fairmont Level B1)

You will be guided to Training via the Registration Desk.

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: 3:00 pm to 9:00 pm (Fairmont Level B1)

Join us for these after hours events

Saturday, September 7

Registration: 7:00 am to 7:00 pm (Fairmont Level B1)

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

9:00 AM

9:00 am to 9:30 am
Opening Ceremonies with
Blue Team Con Advisory Board

9:30 AM

9:35 am to 10:20 am
Keynote: "How to be a Responsible Consumer of Open Source Software"
with Aeva Black

10:00 AM

10:30 am to 10:55 am
"Building on CVSS, EPSS, and KEV: A practical approach to vulnerability prioritization"
with Omer Tal

11:00 AM

11:00 am to 11:50 am
"Defense-in-Depth Engineering"
with John Poulin

11:00 am to 11:25 am
"Social Engineering: Hacking the Brain and Systems"
with Rianat Abbas

11:30 am to 11:55 am
"Look around and find out – How to use OSINT to Protect your OT/ICS environment"
with Wesley Lee

12:00 PM

12:00 pm to 12:50 pm
"Dennis, this is the big one."
with Patrick Scherrer

12:00 pm to 12:25 pm
"Operationalizing AI for Network/SOC Analysts"
with Chris Roffe

12:30 pm to 12:55 pm
"SQL Injection: A History' OR 1=1; –"
with Will McCardell

1:00 PM

2:00 PM

2:00 pm to 2:50 pm
"Securing Your Azure Cloud – Adventures in Cloud Hacking"
with Edwin David

2:00 pm to 2:25 pm
"Cloud Kleptos: Lessons Learned Responding to Scattered Spider"
with Abian Morina

Saturday, September 7

Registration: 7:00 am to 7:00 pm (Fairmont Level B1)

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

3:00 PM

3:00 pm to 3:50 pm
"Team-Up Tactics: GRC Powers Up Offensive Cybersecurity"
with Darryl MacLeod

2:30 pm to 2:55 pm
"Cracking the Security Coding Round: A Paradigm Shift for AppSec Engineer Hiring"
with Sairam Kunapareddy

3:00 pm to 3:25 pm
"How did we get Here: The Key to Managing Employees with Non-Traditional Backgrounds"
with Katherine Jackson

3:30 pm to 3:55 pm
"Like a Hurricane: The Life and Times of Privileged Access Management"
with Aria Langer

4:00 PM

4:00 pm to 4:50 pm
"EMS and IR Professionals Have a Lot More in Common Than Just a Bunch of Acronyms"
with Emily Skaggs

4:00 pm to 4:25 pm
"Building Stronger Cyber Defenses for Major Data Stewards: SMBs and MSPs"
with Amanda Berlin

4:30 pm to 4:55 pm
"Wait. . .Are you really hunting threats?"
with Nathalie Cornejo

5:00 PM

5:00 pm to 5:50 pm
"The Fault in Our Metrics: Rethinking How We Measure Detection & Response"
with Allyn Stott

5:00 pm to 5:25 pm
"Undocumented Hacking"
with José A. Martinez Castro

6:00 PM

6:45 pm to 8:15 pm
Hacker Charlatan Gameshow

7:00 PM

8:00 PM

9:00 PM

9:00 pm to 1:00 AM
Networking Event and Party with DJ cillic

Drinks (Drink Tickets Required) and Food

Technology Art by School Art Institute of Chicago

9:00 pm to 1:00 AM
Board and Card Games

Mocktails (Drink Tickets Required) and Food

No Alcohol Allowed

1:00 AM

Sunday, September 8

Registration & Swag Hours: 9:00 am to 1:00 pm

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

10:00 AM

10:00am to 10:50am
"Death by a thousand control planes: The reality of modern privileged access"
with Eric Woodruff

10:00am to 10:25am
"Illuminating Azure: Navigating Log Complexities with a Novel Key"
with Nathan Eades

10:30am to 10:55am
"Website Fingerprinting: Predicting User Behavior Based on Encrypted Metadata Using Machine Learning"
with Josh Honig and Nathan Ferrell

11:00 AM

11:00am to 11:50am
"The Secret Life of Forgotten Malware C2 (I think I found a new hobby)"
with Eli Woodward

11:00am to 11:25am
"Data to Defense: Shaping Tomorrow's Cybersecurity Analysts with AI"
with Maya Omere and Tawon Saetang (Jibby)

11:30am to 11:55am
"Bridging The Generation Gap: Cyber Workforce Development through STEM Outreach and Mentorship"
with Moeiini Reilly

12:00 PM

1:00 PM

1:00pm to 1:50pm
"Maturing Sec-Ops with Detection as Code"
with David French and Wade Wells

1:00pm to 1:25pm
"EHLO World: Living Off The Land in the Email Domain"
with Josh Kamdjou

1:30pm to 1:55pm
"Combining OSINT and SIGINT to Enumerate IRL Threat Actors"
with Benjamin Speckien

2:00 PM

2:00pm to 2:50pm
"Taking the Human Element to the MAX"
with Alyssa Miller

2:00pm to 2:25pm
"Security In An IaC Defined World"
with Dwayne McDaniel

2:30pm to 2:55pm
"Excel-lence in Cybersecurity: Unveiling the Hidden Powers of Spreadsheets"
with Emma Doyley

3:30 PM

3:30pm to 4:30pm
Closing Ceremonies with
Blue Team Con Advisory Board

4:30 PM

KEYNOTE SPEAKER

BLUE TEAM CON 2024

Aeva Black

SECTION CHIEF, OPEN SOURCE SECURITY, CISA

How to be a Responsible Consumer of Open Source Software

As global digital threats evolve, the interdependence between open source software communities and commercial software vendors, and the interplay between open source stakeholders and global governments, have become increasingly vital. Recent policy actions in both the US and EU have focused on this intersection, and the formation of government Open Source Program Offices (OSPOs) shows the indispensable role of open source software in national infrastructure and national security.

Recognizing that many community-driven open source software projects are critical to the digital supply chain, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has recently taken several actions towards supporting the secure development, distribution, and utilization of open source software.

Attendees of this talk will learn from CISA's Section Chief for Open Source Security about recent policy changes in both the US and the EU, gain an understanding of common characteristics of open source communities that are resilient to threats, and learn how to apply a guideline – developed in partnership between several US agencies and private sector entities – for the responsible and sustainable usage of open source software in the enterprise.

About Aeva

Aeva Black is an open source hacker, advocate, and international public speaker with over 20 years of experience building digital infrastructure and leading open source projects at technology companies. She is the Section Chief for Open Source Security at the U.S. Cybersecurity and Infrastructure Security Agency, and serves as the Secretary of the Board of the Open Source Initiative. Aeva spends her spare time riding motorcycles and supporting her local LGBTQ+ community.

aeva@infosec.exchange @aevaonline

PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

PRESENTS

PDA CYBERSECURITY BOARD GOVERNANCE TRAINING

Our trainers are Matt DeChant, Alyssa Miller, and John Barker, with opening remarks by Robert Barr and Stel Valavanis

The Private Director's Association is proud to present the PDA Cybersecurity Board Governance Training, designed in collaboration with experts in the PDA Cybersecurity Committee. The all-day training targets directors of company boards but also those who aspire to become one and prepares them for participation in the board of the future with greater understanding, support, and governance of cybersecurity practices, privacy, and technology in private companies. While not a certification, the training will provide a certificate of completion and an opportunity to empower the participant with a firm grounding in cybersecurity, privacy, and technology at the board level, and a cohort of experts and peers with which to network. The instructors have been curated from leading organizations and range from enterprise CISOs to top consultants in the industry to seasoned board members who have helped define the board cybersecurity role.

SEC regulations now require that an attestation of cybersecurity skills on public boards be made on annual 10Ks. While this does not legally affect private boards, PDA considers cybersecurity skills to be a requirement, and that all board members receive basic cybersecurity training. Leading organizations do not wait for regulation to lead them and neither should their boards!

This year's training includes pre-study materials, Cybersecurity Fundamentals, Board Responsibilities, Compliance and Reporting, CISO Board Exercise, Incident Response Exercise, and Risk Management Interactive. Our trainers are Matt DeChant, Alyssa Miller, and John Barker, with opening remarks by Robert Barr and Stel Valavanis.

THURSDAY, SEPTEMBER 5TH & FRIDAY, SEPTEMBER 6TH

GOING BEYOND THE RISK REGISTER: CRAFTING COMPELLING RISK NARRATIVES AND GAINING EXECUTIVE BUY-IN

with Celina Stewart

Head of Integrated Risk Management, Neuvik

Many cybersecurity organizations struggle to translate technical outcomes into compelling, business-risk focused narratives for executive and Board-level stakeholders. On Day 1, this training enables cybersecurity and GRC leadership and practitioners to build, measure, and track compelling cybersecurity metrics, to convert metrics to insightful, executive-ready reporting, and to build engagement across their organization. Several common issues will be addressed in this training: incomplete understanding or tracking of cyber risks, siloes between cybersecurity and business stakeholders, and lack of integration with broader Enterprise risk processes.

With those challenges tackled, Day 2 focuses on the struggle many enterprises have when trying to appropriately gauge the impact of cybersecurity risks to the business, in turn leading many organizations to devalue cybersecurity as a cost center. In this portion of the training, we'll discuss tools to align cyber risk to business risk and communicate cybersecurity and GRC program value, thus shifting organizational mindset and facilitating a culture around security.

THURSDAY, SEPTEMBER 5TH & FRIDAY, SEPTEMBER 6TH

SECURITY INTELLIGENCE: PRACTICAL SOCIAL ENGINEERING & OPEN-SOURCE INTELLIGENCE FOR SECURITY TEAMS

with Christina Lekati

Social Engineering Security – Trainer & Consultant

Social engineering attacks remain at the top of the threat landscape and data breach reports. But although most reports tend to simplify many breaches as the result of a successful phishing attack, the reality we get from current threat research is evidently more complex. Today, the pathway that leads to that successful phishing email is often the result of a larger attack kill chain based on research and good open-source intelligence that helped attackers identify organizational vulnerabilities. But it doesn't stop there. Weaponized psychology is still a strong component of those attacks.

The training provides participants with the necessary knowledge on open-source intelligence and social engineering, and helps security teams build better protective measures (proactive & reactive). It also helps penetration testers improve their attack scenarios, their recommendations and provide better and more realistic insights to their clients. The training includes a special section on artificial intelligence and the future of social engineering attacks.

Attendees will leave this class having acquired the psychological knowledge along with the technical capability to simulate social engineering attacks and improve their prevention.

TRAINING THURSDAY, SEPTEMBER 5TH & FRIDAY, SEPTEMBER 6TH

REVERSE-ENGINEERING AND FUZZING CUSTOM NETWORK PROTOCOL

with Munawwar Hussain Shelia

Head of Integrated Risk Management, Neuvik

The communication protocol defines the format and semantics of message exchange between applications. In modern times there are a myriad of proprietary application protocols like Skype Protocol, Dropbox Protocol, etc. which applications use to achieve various goals like bandwidth efficiency, custom encryption/compression, etc. These protocols could have security vulnerabilities. Protocol Reverse Engineering (PRE) is not only useful for offensive purposes but also used by modern Intrusion Detection Systems(IDS), they use the knowledge of protocol specification to do Deep Packet Inspection(DPI) which can enhance its capabilities, where it earlier relied just based on pattern matching which may produce lots of false positives.

Protocol Reverse Engineering(PRE) is an art and science of recovering the protocol specification of the obscure/proprietary protocol whose documentation is unavailable or poorly documented. There are efforts to develop automated PRE tools but they are largely academic and are not mature enough to be usable, and can't give the accuracy a human analyst can offer. Automated tools face the challenges of heterogeneous protocol data which is often a mixture of text and binary, and it has different data types and variable-length fields and this is the reason I have created this training, it is to help you understand these challenges and learn to recover protocol specification.

This training is divided into two parts, in the first part we will learn about Protocol Reverse Engineering principles. We will look at some of the common data formats and other protocol structures and with that understanding we will write a protocol dissector using Scapy framework for a target Desktop game Minetest (open source implementation of Minecraft). Minetest is online multiplayer game in which different players can connect to the server and play with other players, there are also many public servers which you can connect and play. Once we have written the decoder we will sniff the connection and look at the communication flow between the client and the server which we will capture and re-analyze the traffic to improve the dissector further, using this newly improved dissector we will implement a custom game client/bot which will connect to the server and play as a Bot player.

In the second part, with a decent understanding of the Minetest Protocol we will move on to the offensive side of the training and try to fuzz the game server to find some security vulnerabilities, we will start with basic Fuzzer and try to do incremental improvement such that we have good code coverage. Leveraging their reverse-engineered understanding of the protocol, participants will employ Generational Fuzzing by defining the protocol specification in the Boofuzz fuzzing framework and subsequently fuzzing the application.

This hands-on game hacking training is a takes project-based learning approach, ensuring a comprehensive and practical understanding of Protocol Reverse Engineering. In summary, this training aims to equip you with the knowledge and skills to reverse engineer and understand obscure protocols, enhance IDS capabilities, and explore offensive techniques such as protocol fuzzing to uncover potential security weaknesses.

THURSDAY, SEPTEMBER 5TH & FRIDAY, SEPTEMBER 6TH

PRACTICAL MALWARE ANALYSIS BOOTCAMP

In this program, participants will get to know the internals of malwares, understanding its behavior, origins, and modes of infiltration. The session explores topics from fundamental structure of PE files to advanced techniques seen in a day to day analysis of malwares. You'll gain hands-on experience in dissecting malicious code and get familiar with various tools used by Malware analysts and reverse engineers.

The session will cover the fundamental principles of malware analysis, guiding you through the identification and classification of various types of malware. The training is designed to bridge the gap between entry-level and intermediate malware analysts. Participants will be working hands-on with recent malware samples to get a good grasp over sophisticated evasion techniques.

Neel Pathak
Staff Security Researcher, Trellix

Pratik Kadam
Security Researcher, Zscaler

FRIDAY, SEPTEMBER 6TH

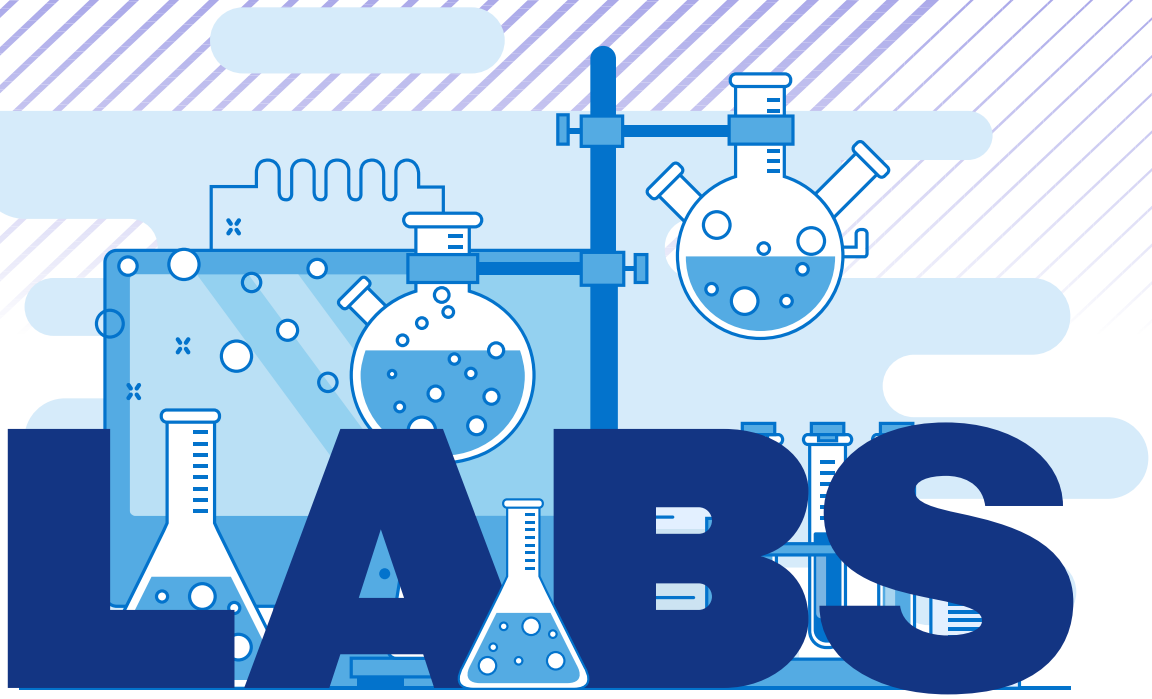
MASTERCLASS/TABLETOP FOR DETERMINING CYBERSECURITY INCIDENT MATERIALITY

The premier executive learning experience focused on helping CISO's lead their boardrooms and executive teams through an informed and deliberative process for identifying the material impacts and aspects of a cybersecurity incident. Whether complying with SEC cybersecurity incident materiality disclosure rules or adopting leading practices, this masterclass and case-based tabletop program teaches the BLAST RADIUS-FALLOUT (BRFO) process.

Delivered as a four hour in-person masterclass and tabletop, this workshop is instructed by CISOs, Directors, and the thought leaders and experts on digital and cybersecurity oversight.

Bob Zukis
CEO and Founder,
Digital Directors Network

Tony Cole
Advisory Board Member and
Senior Faculty, Digital Directors Network



NEW FOR 2024

NEW for Blue Team Con 2024 – Labs! 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.

ASSUMED

Sunday, September 8, 2024 from 10am to 12pm CT

Assumed is excited to introduce our new cyber-deception platform at Blue Team Con. As you may have inferred from your lanyards or honey jar included in the swag bag, Assumed Seeds are honey tokens and honey accounts. Honey tokens and honey accounts are fake data or user accounts set up to lure cyber attackers, helping organizations detect and respond to unauthorized access attempts without risking real information under their care. During this lab session, get hands on with the Assumed platform to create honey tokens to detect data leaks faster, identify insider threats, vet data partners, and most importantly – slow attackers down, reveal their tactics and identify abuse of personal data.

---

graylog

Saturday, September 7, 2024 from 4pm to 6pm CT
Sunday, September 8, 2024 from 12pm to 2pm 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.

Ontinue
AI-Powered MXDR

Saturday, September 7, 2024 from 2pm to 4pm CT

Join us for a hands-on lab demo focused on maximizing your organization's security using Microsoft Defender. In this live demo, we will explore practical strategies to streamline security operations, reduce redundancies, and retire costly legacy controls. Attendees will learn to:

- **Simplify Security Management: Integrate and consolidate security tools within the Microsoft ecosystem.**
- **Minimize Operational Complexity: Reduce the number of management interfaces and streamline workflows.**
- **Optimize Resource Allocation: Free up your team to focus on strategic initiatives and more pressing matters.**
- **Utilize Existing Microsoft Licensing: Maximize the value of your current Microsoft investments by utilizing built-in security features.**

This interactive lab will provide practical insights and techniques to help you achieve a more efficient, robust, and cost-effective security strategy using Microsoft Defender.

Push

Saturday, September 7, 2024 from 10am to 12pm CT

During the Push Security Lab Slot, see how you can get hands on with Push to detect and prevent identity breaches, stop corporate password reuse and phishing, in addition to exploring in-browser security guardrails for employee endpoints, and visualized metrics to track improvements in your overall identity security posture.

SLEUTH KIT LABS

Saturday, September 7, 2024 from 10am to 12pm CT

In this hands-on lab we will review a Play ransomware attack and you can review the collected data to find evidence. We'll look at the methods of initial access, tools used to pivot and exfiltrate data and culminating in the deployment of the Play encryptor. In addition to an overview of the attack we will conduct a deep dive into the incident investigation. Examining the artifacts created during the attack and how they can be leveraged to build a picture of what happened. The primary tool for the lab will be Cyber Triage, which is an automated investigation platform that focuses on identifying the relevant artifacts.

Talk Track One
50 MINUTES

The Fault in Our Metrics: Rethinking How We Measure Detection & Response

Allyn Stott
Senior Staff Engineer, Airbnb

Your metrics are boring and dangerous. Recycled slides with meaningless counts of alerts, incidents, true and false positives… SNOOZE. Even worse, it's motivating your team to distort the truth and subvert progress. This talk is your wake-up call to rethink your detection and response metrics.

Metrics tell a story. But before we can describe the effectiveness of our capabilities, our audience first needs to grasp what modern detection and response is and its value. So, how do we tell that story, especially to leadership with a limited amount of time?

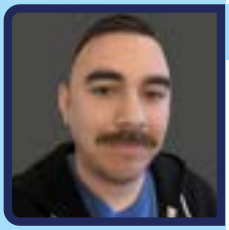
Measurements help us get results. But if you're advocating for faster response times, you might be encouraging your team to make hasty decisions that lead to increased risk. So, how do we find a set of measurements, both qualitative and quantitative, that incentivizes progress and serves as a north star to modern detection and response?

Metrics help shape decisions. But legacy methods of evaluating and reporting are preventing you from getting the support and funding you need to succeed. At the end of this talk, you'll walk away with a practical framework for developing your own metrics, a new maturity model for measuring detection and response capabilities, data gathering techniques that tell a convincing story using micro-purple testing, and lots of visual examples of metrics that won't put your audience to sleep.

Taking the Human Element to The MAX

Alyssa Miller
CISO, Epiq Global

In the aviation world, when bad things happen there is a culture of avoiding the blame game and instead focusing instead on how we can learn from our mistakes to make everyone safer. With the issues surrounding the 737 MAX series of aircraft over the past couple years, the FAA and NTSB have again held the line on focusing on safety and learning from mistakes despite media sensationalization. But we in the cybersecurity community can also take advantage of this learning opportunity. With news and whistleblower accounts of the design and quality issues leading to the MAX series aircraft, there are many parallels to what happens in the cybersecurity space when we fail to properly account for and incorporate the human element into our programs. In this presentation, we will take that same approach of not bashing or blaming but focusing on learning. We'll step through the issues that have come to light regarding the 737 MAX series and show how those correlate to cybersecurity. We'll identify what lessons we can learn and how we can apply those when selecting technology and building processes for our organizations' security programs. Finally, we'll discuss the Swiss Cheese model as it applies to cybersecurity and examine best practices for closing those holes before they align and result in disaster.



Maturing Sec-Ops With Detection as Code

David French
Lead Detection Engineer

Wade Wells
Detection & Response Engineer / Threat Hunter, Google

"This presentation is for security practitioners who are interested in learning about the fundamentals and benefits of Detection-as-Code and how to build a CI/CD pipeline to manage threat detection rules.

A traditional approach to detection rule management is for security practitioners to manually configure and maintain them within their security tools. Detection-as-Code is often a good fit for enterprises that need more collaboration and change management around their detection engineering processes.

Detection-as-Code is a set of principles that use code and automation to implement and manage threat detection capabilities. By leveraging software development practices, security teams can streamline their process for creating, testing, deploying, and maintaining detections by treating them as code artifacts.

This presentation will introduce the core concepts and benefits of Detection-as-Code before walking through a process of building and implementing a CI/CD pipeline. A practical threat detection use case will be utilized throughout the presentation before testing it end-to-end."

Team-Up Tactics: GRC Powers Up Offensive Cybersecurity

Darryl MacLeod
Advisory Services (vCISO), Lares

Collaboration between Governance, Risk, and Compliance (GRC) teams and offensive security teams is vital for a strong security stance. This presentation highlights the role of GRC teams in augmenting offensive security efforts. Traditionally, GRC teams are seen as policymakers, compliance assessors, and risk managers. Their role, however, can significantly contribute to offensive security strategies.

The presentation emphasizes how GRC teams can enhance offensive security through risk-informed strategies, ensuring that offensive measures align with policies and compliance, optimizing resources, and bridging communication between technical and executive teams. The session aims to provide cybersecurity professionals and organizational leaders with a thorough understanding of the importance of GRC teams in offensive security and practical approaches for integrating these functions within their organizations.

Securing Your Azure Cloud – Adventures in Cloud Hacking

Edwin David
Security Consultant, TrustedSec

This talk will dive into different phases of cloud penetration testing and will focus on real world attack paths into the Azure Cloud. Cloud attack paths in this talk will include reconnaissance, password spraying, device code phishing, data theft in Entra ID from a low privileged user perspective, dumping public storage blobs, lateral movement with unsecured azure applications, pivoting from cloud to internal network, and finally achieving full cloud compromise using Kerberos in the cloud.

Fear not blue team! The only way to counter good offensive tradecraft is with good defensive cloud strategies. I will be giving out plenty of cloud defensive tactics during this talk. Can I do this in 50 mins? Come find out as I hack some clouds.

The Blue Teamers who attend this presentation will learn traditional incident management practices, triage strategies, “soft skills” and communication tips that can complement their security program’s incident response procedures.

The Secret Life of Forgotten Malware C2 (I think I found a new hobby)

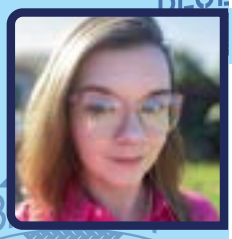
Eli Woodward
Cyber Threat Intelligence

Almost daily, we encounter new headlines and blog posts from various researchers and intelligence vendors, highlighting exploits from APT and crimeware groups that utilize custom domains with clever and unique names, such as Pandorasong. But what happens to these domains after they’re publicly named? Do threat actors immediately abandon them? Are they repurposed for future campaigns? And should we continue to monitor these domains in our Threat Intelligence Platforms (TIPs) for intelligence purposes, especially in light of their activities being exposed by open-source intelligence?

This presentation delves into these questions, offering a deep dive from the perspective of a Cyber Threat Intelligence (CTI) analyst and researcher curious about the fate of these domains once they are ‘burned.’ After spending way too much money and time buying up old domains, observing compromised machines still ‘calling home,’ and identifying who else is vying to purchase these domains, the overlooked world of forgotten malware C2 domains has revealed itself to be incredibly fascinating.

Building upon the seminal work of David Bianco’s ‘Pyramid of Pain,’ this talk aims to cast a new light on the threat posed by custom malware domains and the lasting value they offer to both scammers and researchers. It is hoped that industry professionals will come to place a special emphasis on custom malware domains, recognizing their persistent and long-term value to both attackers and defenders.

Talk Track One
50 MINUTES



EMS and IR Professionals Have a Lot More in Common Than Just a Bunch of Acronyms

Emily Skaggs
Cybersecurity Engineer – Incident Response

EMS and IR professionals are the "first responders" to incidents that people never want to happen. Whether the incident is a ransomware infection at your local hospital; or a respiratory infection caused by a virus that spreads through the air; the people on the front lines of responding to both of those incidents share many similarities in their work. Moreover, even NIST uses an ambulance to symbolize the Containment and Recovery step in the "Computer Security Incident Handling Guide" (NIST SP 800-61 Section 3), which inspired this talk.

We as cyber incident responders can learn a lot from the IR professionals who must interact with the most unpredictable systems in the world: human beings.

In this presentation, we will examine how these EMS professionals execute this type of high-stress, high-stakes work on a daily basis, including hearing real-world examples from professionals on the ambulance. We will gain insight into triage techniques including the START (simple triage and rapid treatment) triage system, the most common triage system in the United States, as well as learning tips on gathering evidence while under pressure to aid in incident response.

The Blue Teamers who attend this presentation will learn traditional incident management practices, triage strategies, "soft skills" and communication tips that can complement their security program's incident response procedures.

Death by a Thousand Control Planes: The Reality of Modern Privileged Access

Eric Woodruff
Senior Security Researcher, Semperis

We are hurdling through a period of profound change to our business applications, mostly unnoticed from the perspective of privilege. These applications that run our enterprises, which hold our business-critical data, have historically been sheltered by our corporate networks. As we modernize and move to a world of software-as-a-service (SaaS), we introduce new attack surfaces, and new control planes. The simplification and agility that Salesforce, Workday, ServiceNow, and the infinity of other SaaS applications out there bring to our businesses, they present a new challenge for defining who, and what, is privileged access.

In this session, we will explore the reality of modern privileged access and its intersection with modern authentication and identity management. We will define the new attack surfaces SaaS applications present and the challenges they bring to securing the enterprise estate. We won't just discuss theory; we will walk through common integration patterns and the challenges with privileged access that arise. Moreover, we will outline the road ahead and provide actionable steps organizations should take to protect their enterprises, applications, and data, in our SaaS-driven world.

Defense-in-Depth Engineering

John Poulin
CTO, Cloud Security Partners

The 2021 OWASP Top Ten introduced a category "Insecure Design" to focus on risks related to design flaws. In this talk, we will focus on techniques we can use to build defense-in-depth software. What can we do to proactively architect software to be more resilient to attacks? What type of findings may not be discovered via automated static analysis? How can we design our software to be more friendly during incident response scenarios? Throughout this talk, we will focus on identifying often-overlooked architectural anti-patterns and vulnerabilities to be on the lookout for. We will source code to analyze patterns for improvement in both real-world applications as well as intentionally vulnerable applications. Engineers will leave this talk with a solid understanding of defense-in-depth software architecture and design. Security engineers or consultants can expect to leave with an increased understanding of insecure design patterns and vulnerabilities.

“Dennis, This is The Big One.”

Patrick Scherrer
Information Security Manager, Rea Magnet Wire

On September 9th, 2023 at about 0500, our organization was hit with a ransomware attack that impacted every level of our operation. The title refers to my first phone call to my boss that morning. We are a manufacturing company that operates around the clock, with on-prem, computer-based workloads running on nearly 1000 computers. Our small team of 5 sprung into action and restored or rebuilt nearly 800 objects in 7 facilities and two countries in less than 48 hours while also discovering and removing the threat actor’s point of entry. This talk will focus on what happened, what we learned, but also how the dynamics of the team came together to achieve a speedy recovery. From the blind luck of having recently finished an upgrade to immutable on-site backups to embracing the brilliance of the auto-didact on our team and trusting their instincts about when to escape the established plan. I believe other organizations, especially those with the resource constraints many manufacturing companies face, can benefit from hearing our story.

Talk Track Two
25 MINUTES

Cloud Kleptos: Lessons Learned Responding to Scattered Spider

Abian Morina
Associate Threat Researcher, Permiso Security

Cloud-focused attacks are on the rise, moving far beyond the commonplace cryptomining campaigns or initial access gained by poor password policies and lack of MFA. Persistent threat actors have adapted to rising defensive best practices, even evading MFA by push fatigue attacks and SIM swapping.

LUCR-3 (Permiso's name for the threat actor group also known as Scattered Spider), who notably compromised MGM and Caesars in late 2023, epitomizes this level of persistence in their methodical approach to targeting specific industry verticals and effectively compromising, escalating and exfiltrating the desired intellectual property from their victims. Permiso's P0 Labs team has tracked and responded to LUCR-3 for the last 1.5 years, noting their effective traversal of technology boundaries from IaaS to SaaS and even PaaS. Additionally noteworthy is their practice of infiltrating internal communications and SaaS-based knowledge sharing platforms immediately upon initial access to retrieve internal processes, playbooks and stakeholders required to carry out their mission.

This presentation will inform defenders about many of LUCR-3's notable TTPs, with a specific technical focus on those TTPs targeting the SaaS and IaaS layers from both an offensive and defensive perspective. While Scattered Spiders' TTPs range widely, their persistence and focus is anything but scattered.

My presentation will revolve around several key positions – Hiring Managers, Recruiters, HR, C-Suite – and how they need to be better aligned with employment gaps, job requirements, training, and provide a healthy environment where people are heard and valued. Additionally, I'll expand on how certification vendors are hindering and not helping by introducing financial barriers. Lastly, I will acknowledge industry leaders, that are paving the way and increasing diversity of thought and tackling our current and future problems. In closing, if we continue to fail, as a profession, to bring in more diversity of thought, then our most sensitive global networks and personal data will continue to be at risk.

Building Stronger Cyber Defenses forMajor Data Stewards: SMBs and MSPs

Amanda Berlin
Lead Incident Detection Engineer at Blumira

Small and medium-sized businesses (SMBs) and managed service providers (MSPs) are pivotal in shaping cybersecurity, collectively constituting over 90% of global businesses. Despite their prevalence, they receive disproportionately less cybersecurity attention than enterprises, yet collectively harbor a significant amount of sensitive data, making them prime targets for cyberattacks, notably ransomware campaigns.

This presentation advocates for empowering SMBs and MSPs through:

- Using SMB and MSP incident retrospectives to cast a light on common attacks.
- Implementing cost-effective solutions that can scale across multiple clients.
- Streamlining implementation and management of security measures.
- Maximizing limited security budgets and resources.
- Employing layered defense strategies that strike a balance between protection and usability.
- Developing threat models that specifically target the most probable attack vectors for SMBs.
- Tailoring security fundamentals to suit the unique environments of SMBs.
- Promoting industry-wide outreach and educational initiatives.

The goal is to democratize security, recognizing SMBs and MSPs as major data custodians. Customized solutions are essential to support their security needs and acknowledge them as the future of cybersecurity. By supporting this majority, we can achieve a more inclusive ecosystem with robust security measures for all businesses.

Like a Hurricane: The Life and Times of Privileged Access Management

Aria Langer
Security Engineer, Morningstar Inc.

So you want to implement a modern PAM (Privileged Access Management) solution? Awesome. More robust access controls are what the Infosec Gods say your Wild-Wild-West organization needs to inch closer to the mythic land of Pretty-Pretty Zero Trust. How are you going to accomplish this? How do you sell this to those who make the $$$ decisions (who claim to align with the principles of PAM but shudder at the threat of productivity loss)?

Or maybe the full vision of modern PAM isn't being bought. The risk is "so-low" that it is not worth the trouble and your organization accepts this risk. Is the risk REALLY understood?

But first—what is PAM? This talk will explore iterations of access control across history. Then, let's kick it up a notch; we'll discuss how each control (adding up to the idealized "Modern PAM Solution") plays a vital role (AKA, the difference between solutions provided by traditional PAM vs Modern PAM), and how gaps persist when any one of the controls is missing. We will also talk about the logistical nightmares that come with not just implementing these solutions but even proposing such a program to an organization.

And now for something completely different—I will accomplish all the above using DuckTales metaphors. Life is like a hurricane here in Duckburg! (ooo-WOO-oo!)

Combining OSINT and SIGINT to Enumerate IRL Threat Actors

Benjamin Speckien
cLabs

Can your organization's security posture be strengthened by monitoring WiFi Probe Requests? What about Bluetooth Low Energy Beacons? Can identifying names and device information sent in cleartext help you authenticate who you're talking to? Location data of wireless networks people have previously connected to combined with current location can be used to validate identity.

Insecure wireless settings can leak information such as names, travel patterns, places of work, language preferences and even types of cars driven. Imagine a potential candidate at a job fair beaconing in the language of a nation-state threat actor, or a potential business partner with probe requests correlating to a competitor's office, or even being notified of a Flipper Zero close enough to clone your RFID badge.

This talk is about real-time application of intelligence gained from passively monitoring wireless transmissions from common mobile devices. I will demonstrate an unobtrusive method of collecting and displaying this information. Findings from analyzing large data sets will be presented, demonstrating that this method can be applied to enumerate potential threat actors within a given proximity.

Finally, mitigation techniques and the importance of securing your network preferences will be discussed.

Operationalizing AI For Network/SOC Analysts

Chris Roffe
Director, SentryWire Engineering and Product Development

The presentation focuses on using Human Design Engineering (HDE) principles for the development of AI tools that are more adaptable to the varying levels of expertise within a SOC or analyst team.

Using logic-rails, behaviors, and trigger-actions to craft the AI assistant into a functional interface that integrates disparate systems, and enable analysts to access and cross-reference data. This integration is crucial for rapid threat identification and response, as it allows analysts to draw connections between indicators of compromise and potential threats without manually navigating through multiple platforms

We will also highlight how AI assistants can be configured to align with the workflows and preferences of human analysts, ensuring that the technology adapts to the user rather than the other way around. This user-centric design is essential for maintaining the human analyst's role as the decision-maker, leveraging the AI's processing power to enhance their situational awareness and investigative capabilities. The concept of "human in the loop" is a critical component of this approach. It emphasizes the importance of human oversight in automated processes to ensure that decisions are made with a level of discernment that AI currently cannot replicate.

By reducing the time spent on manual data aggregation and preliminary analysis, AI assistants empower analysts to dedicate more effort to tasks that require their expertise. AI Assistants help not only improve the efficiency of a task workflow but also ensures that human judgment remains at the forefront of the decision-making process for small, medium, or global sized security teams.

Talk Track Two
25 MINUTES

Security In An IaC Defined World

Dwayne McDaniel
Senior Security Developer Advocate, GitGuardian

While it would be amazing to focus 100% on our code in our work, the reality of modern DevOps is we also need to worry about where it runs. In a simpler time, the operations team would grant us precious disk and machine resources after a requisition request. Security was tight, as those servers were locked down behind private networks and gateways. Living in the modern world of platforms as a service and infrastructure as code, IaC, means just taking security for granted is no longer an option.

Even if the security team could manage every possible bit of your infrastructure, understanding how to manage security better is going to help everyone stay safe, especially at scale.

Takeaways:

- What does good security look like
- Everything you need to know about Infrastructure as Code in 3 minutes
- The security issues (and benefits) IaC brings
- Securing the world around your IaC
- When the security team should be involved
- Local/individual testing for scale

There is a huge misunderstanding of vulnerability management. It is commonly incorrectly defined as being synonymous with software updates and patches. It is so much more than that! We will take the audience through a hands-on journey of scanning, enriching data, and creating high-value prioritization to protect against the number one method of threat actor initial access: software vulnerabilities.

Excel-lence in Cybersecurity: Unveiling The Hidden Powers of Spreadsheets

Emma Doyley
Head of Information Security, TT Electronics

In an era where cybersecurity threats loom large, organisations are constantly seeking effective and cost-efficient strategies to fortify their defences. Amidst the abundance of sophisticated tools and technologies available, spreadsheets emerge as a surprisingly versatile and accessible resource for supporting information security efforts.

Prepare to embark on an journey into the world of cybersecurity, where the unassuming Excel spreadsheet emerges as a silent hero, wielding unparalleled prowess in fortifying digital defences. In this talk, we'll unravel the mystique surrounding spreadsheets and unveil their potential to revolutionise information security management.

From the depths of data organisation to the heights of vulnerability tracking, we'll showcase how spreadsheets morph from humble grids into dynamic fortresses of security resilience. With the agility of a cyber ninja, we'll demonstrate how these seemingly simple tools can be customised to thwart threats and comply with the most rigorous standards, while keeping costs lean and processes nimble.

For those eager to take their cybersecurity game to the next level, we'll unveil the secret weapon: SharePoint. Picture spreadsheets on steroids, with next level collaborative power. By seamlessly integrating SharePoint into your cybersecurity arsenal, you'll unlock a treasure trove of capabilities for team collaboration, document management, and workflow automation. With SharePoint as your trusty sidekick, you'll transcend the limitations of standalone spreadsheets, fostering real-time collaboration and knowledge sharing among your cyber cohorts. Together, Excel and SharePoint form an unstoppable duo, propelling your cybersecurity initiatives to new heights of efficiency and effectiveness.

Undocumented Hacking

José A. Martinez Castro
Security Delivery Senior Analyst, Consulting

As security practitioners, it is our job to take advantage of both documented and undocumented functionality, and then go on to take appropriate measures for both. This may arise as new vulnerabilities from unexpected uses of software or processes, or taking advantage of little known but well documented behavior in novel ways. Coming up with mitigations or fixes can sometimes mean taking a non standard path.

Similarly, the way many of us get into the field might be non conventional, and the way we might need to approach hiring or introducing new talent to the field. In this talk, I'll go over my path into security as an undocumented immigrant without a college degree, while drawing parallels to security. Concluding with the way we might approach hiring talent with unconventional backgrounds, what might have made a similar journey easier, and sharing resources available.

Expect answers to questions like: How is preparing for a civil disobedience or escalation similar to planning for a security engagement? What is the risk assessment and legal preparation beforehand, when the individual involved is weighting their personal risk, and how does this mirror compliance? And, how is navigating the immigration system when renewing a work permit, navigating the bureaucracy, and escalating your case like a web application pen test.

EHLO World: Living Off The Land in The Email Domain

Josh Kamdjou
Founder and CEO, Sublime Security

Email-based attacks remain at the forefront of the cybersecurity threat landscape, ever-evolving to circumvent defenses and trick unsuspecting users. In this presentation, we delve into the strategies attackers use to manipulate high-reputation infrastructure and services to deliver attacks that reach end user inboxes.

We'll show real, in-the-wild examples of how attackers abuse trusted platforms like DocuSign, SalesForce, Google Drive, PayPal, and Box, how they abuse free subdomain hosts, mass mailers, open redirects, compromised WordPress sites, and more. We'll then explore how attackers persist in the inbox through the creation of malicious mail forwarding rules to siphon data without having to leave repeated access logs.

Finally, we'll discuss detection and hunting methodologies and other defense-in-depth techniques to mitigate these attack vectors. Attendees will leave the talk with practical knowledge on novel email attack techniques and how to defend against them.

How Did We Get Here: The Key to Managing Employees with Non-Traditional Backgrounds

Katherine Jackson
Director of OSINT Engineering

The first thing I want you to know is that I'm the manager of an OSINT Engineering Team. I have the honor of leading 6 other brilliant minds through the creation, documentation, and daily execution of a never before done OSINT Harvesting Process. Over the last year and a half alone we have successfully parameterized 23 domains and have collected over 2,000,000 data points. We have first-hand experience of what it means to work with OSINT and the number of challenges and benefits it brings. And we are constantly pushing to refine this process in hopes of unlocking its potential.
The second thing I want you to know is that every single person on my team, me included, come from a nontraditional, non cyber background.

So how did we get here?

The answer is training and culture. Daily meaningful engagement that focuses on four main elements:

- Real on the job learning
- People First Culture
- Open and intentional communication
- Constant refinement

The reality is, having a non cyber background does not have to be a deterrent to working in the Cybersecurity industry. If we as managers and leaders are willing to rethink how we approach training our teams, we will find ourselves with homegrown experts who are truly masters at what they do. These four elements have been my approach to training over the last two years and they have allowed our department to go above and beyond, and I am confident you can do the same.

Talk Track Two
25 MINUTES

Data to Defense: Shaping Tomorrow's Cybersecurity Analysts with AI

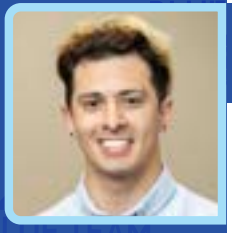
Maya Omere
Threat Intelligence Analyst

Tawon Saetang (Jibby)
Threat Intelligence Analyst, KC7 Foundation

We engineered a way to use AI to turn threat intelligence reports into real data, and we're using it to transform the way cybersecurity is taught, and make the industry more accessible to everyone. At the core of our approach is a python engine that generates realistic intrusion datasets by mimicking the tactics, techniques, and procedures (TTPs) of real-world cyber threat actors. We augmented the engine by using a custom LLM that can turn intrusion reports into configurations that the engine can consume. This innovative use of AI accelerates our ability to provide story-driven, gamified training modules that immerse participants in the role of cyber defenders, where they confront authentic cybersecurity challenges, investigate threat actor behaviors, and learn to recognize sophisticated attack techniques.

In the resulting game, called KC7, participants are guided through investigations of simulated cyberattacks against fictional companies, created to reflect the complexity and nuance of genuine cyber incidents. They learn to navigate and analyze intricate datasets, mapping their findings to MITRE ATT&CK, enhancing their threat hunting and incident response capabilities. They learn to contextualize evidence, unravel the story behind cyber incidents, and develop critical thinking skills crucial for effective threat detection and response.

The use of AI to generate game data enabled us to deliver hundreds of hours of free, fun, and effective training to thousands of people at no cost. As a result, we've helped so many people, from different backgrounds, fall in love with cybersecurity defense, ranging from transitioning professions, to K-12 students.



Bridging the Generation Gap: Cyber Workforce Development Through STEM Outreach and Mentorship

Moeiini Reilly
Research Technologist, Georgia Tech Research Institute

The future of cybersecurity is defined by today's workforce evolving and persisting through volatile threat landscapes. In order to facilitate this growth, the next generation of information technology (IT) and cybersecurity leaders must enter the field with diverse perspectives and fundamental understandings of computing. As industry professionals, we feel first-hand how gaps in the cybersecurity workforce affect the risk postures of the organizations we work for, and the intensity with which ourselves and our colleagues experience burnout. Instead of waiting for the next generation to find the cyber industry, this presentation showcases research that incorporates industry-led outreach and mentorship networks to bridge the gap between what is accessible through traditional career pathways, and what we need to develop and improve the cybersecurity community. Attendees will gain insights into concrete programming designed to address these challenges head-on. From paid high school internships to immersive job shadowing experiences, from extracurricular STEM club mentorship to interdisciplinary networking between students, educators, and industry professionals, we outline a comprehensive roadmap for nurturing talent and fostering community engagement. Together, we can bolster our collective resilience and ensure a vibrant future for cybersecurity.

Wait… Are You Really Hunting Threats?

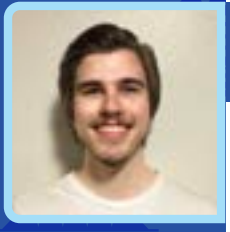
Nathalie Cornejo
Threat Hunter Team Lead

In a world where cyberattacks are increasing and stealthier, it is essential to take the lead in uncovering an attacker on the network that defense tools haven't detected; that's where threat hunting becomes more relevant. Doing a proactive search for malicious activity and understanding if we are focusing on the actors that can affect our business becomes crucial; also, taking into consideration SOC detections won't be enough to detect sophisticated adversaries who change their behaviors and way to go. This presentation wants to address this to help defenders start a threat-hunting process and have a guide on the most relevant points they should focus on, such as prioritizing the adversaries that they want to detect according to business purpose and, at the same time, demystify threat hunting; these points are fundamental to creating a robust process that ensures you are in the right way to find real threats, additionally, impacting the dwell time in our organizations. Finally, understand the impact of Threat Hunting on blue team processes by translating hunting queries into long-running threat detections, adding further visibility to the SOC, and fostering Google's "Hunt Once" rule; it is a key learning the author wants to bring to the audience.

Illuminating Azure: Navigating Log Complexities with a Novel Key

Nathan Eades
Senior Threat Researcher

In the intricate ecosystem of cloud computing, Azure Monitor Activity Logs serve as a critical tool for tracking and understanding operations within Azure environments. However, navigating these logs can be as challenging as it is essential, with complexities that can obscure crucial insights. This session aims to shed light on the nuances of Azure Monitor Activity Logs, highlighting both their strengths and the obstacles they present. I will introduce the concept of a composite key designed to re-orient and review events with a "correlation" that goes beyond Azure's existing correlation and operation ID constructs, offering a clearer perspective. This approach promises to provide enhanced clarity and actionable insights for your Azure infrastructure.



Website Fingerprinting: Predicting User Behavior Based on Encrypted Metadata Using Machine Learning

Nathan Ferrell
Undergraduate Student, Loyola University Chicago

Josh Honig
Undergraduate Student, Loyola University Chicago

In an ongoing project, student researchers at Loyola University Chicago seek to understand how machine learning can be used to identify user web browsing behavior based solely on the metadata of encrypted network traffic, eliminating the need to decrypt data for identification. In order to create a training dataset, researchers created a Python program to repeatedly visit a list of websites and collect network traffic data. The size and direction of the encrypted HTTPS packets were extracted to create a sample for each website and a Random Forest classifier was trained and evaluated on this data. Researchers were able to prove that the trained model provided a reasonably accurate prediction of the website a user was visiting, based only on the metadata of encrypted network traffic (that is, without breaking encryption). This threat model is easy for a lone attacker to establish; the computational requirements are average, and the network visibility required to perform the attack is trivial to obtain. Entities such as Internet Service Providers, corporate network managers, and government agencies already have sufficient visibility to perform the attack we describe.

Building on CVSS, EPSS, and KEV: A Practical Approach to Vulnerability Prioritization

Omer Tal
Security Researcher, Seemplicity

These days, the overwhelming number of vulnerabilities in any system, combined with resource constraints, makes it impossible to remediate all vulnerabilities. Effective prioritization is essential, ensuring that the most critical threats are tackled first to safeguard an organization's key assets efficiently.

Frameworks like CVSS, EPSS, the KEV catalog, and SSVC have been widely adopted to aid this task. Each framework offers unique insights, yet they often fall short of providing a holistic solution. This leaves organizations juggling multiple tools without a clear path to optimal prioritization.

Join my talk where I explore the strengths and weaknesses of these popular frameworks. I will discuss why no single framework should be used alone and how to develop a comprehensive vulnerability prioritization strategy that leverages the best aspects of each framework. Learn how to transform these theoretical tools into a practical, actionable plan that fits your security needs.

Talk Track Two
25 MINUTES

Social Engineering: Hacking The Brain and Systems

Rianat Abbas
Cybersecurity Analyst

Recent trends and insights in social engineering attacks reveal a landscape marked by increased sophistication and targeted strategies. This presentation will delve into the novelty insight of the latest trends in Social engineering attacks and how it has evolved to incorporate advanced techniques such as deepfake recordings, leveraging artificial intelligence to create realistic simulations of individuals' appearances and voices. These deepfake recordings are exploited to trick victims into divulging sensitive information or performing actions beneficial to the attacker. While awareness efforts are essential, they must be complemented by actionable strategies to identify and mitigate risks effectively.

Part of the latest trends organizations and individuals should be aware of is how cybercriminals capitalize on current events like natural disasters or global crises to craft social engineering attacks, leveraging heightened emotions or uncertainties to deceive victims and elicit desired responses. These recent attacks heavily rely on psychological manipulation, exploiting human emotions, trust, and curiosity to coerce individuals into compromising security which will be covered during the session.

However, the focus is not solely on the latest trends. This presentation will also look into actionable frameworks and an extensive toolkit to empower organizations and individuals in defending against the latest trends of social engineering attacks. This toolkit includes frameworks for identifying vulnerable employees, strategies to improve security awareness programs, maintaining effective communication channels, and fortifying security infrastructure. Frameworks like the Phishing Detection and Response Framework, improvements to the Security Awareness Training Programs: Guidance on developing and improving the security awareness training programs to align with the latest social engineering attacks and educate employees about social engineering threats and best practices for mitigating risks.

We will also complement the session with an in-depth analysis of several case studies to illustrate the application of psychological tactics by cybercriminals in executing social engineering attacks. Attendees can expect to explore case studies such as the LinkedIn Impersonator, Tech Support Scams, and Spear Phishing Attacks, which highlight the multifaceted nature of social engineering threats and the importance of proactive defense measures.

Cracking The Security Coding Round: A Paradigm Shift for AppSec Engineer Hiring

Sairam Kunapareddy
Product Security Engineer, Ripple

Have you ever entered a security coding interview round, questioning the purpose and relevance of the challenges presented? Feeling disoriented, wondering how precisely the tasks assess your candidacy? This discussion aims to address these issues and present a more precise approach to evaluating the ideal candidate.

Look Around and Find Out – How to Use OSINT to Protect Your OT/ICS Environment

Wesley Lee
Senior Manager, Protiviti

One thing is clear, an incident in an OT/ICS environment affects everyone in almost every industry. If you have read or followed any cybersecurity framework, guidance, best practices, or document that directs you how to protect your organization from an incident or breach, typically you will always find something around understanding or knowing your assets. The same guidance is important in OT/ICS environments as well. This presentation will introduce the world of OT/ICS assets, device, and network discovery using OSINT (Open-Source Intelligence) tools and techniques in order better understand your OT/ICS attack surface. While this talk will focus mainly on the OT/ICS attack surface discovery, this presentation will also point out how some of these OSINT tools and techniques can be modified to understand the IT environment attack surface. Attendees of this presentation will be able to walk away with a methodology, roadmap, and guidance that can be used to perform their own OSINT on their OT/ICS environment.

Look Around SQL Injection: A History' OR 1=1;

Will McCardell
Application Security Architect, SysLogic Inc

SQL Injection is one of the most widely known software attacks out there. But how did it get to that point? How have defenses changed over the years to protect against it? And why aren't pentesters finding it anymore?

For 8 years, SQL Injection was the top vulnerability in the OWASP Top 10. The damages it can cause are severe. But in 2021, it dropped two places in the ranking, reflecting changes in the industry that reduced both the frequency and the impact of this vulnerability.

This talk will go over the history of SQL Injection, with an emphasis on what and how defenses have changed over the years, covering the effect that training, better SQL deployment capabilities, golden path tooling, microservices, and other things all had on SQL injections. It will also cover the lessons from these applicable to defensive security at large.

Finally, the talk will dig in to the fact that penetration testers are not seeing this vulnerability as often anymore and what implications that has for CVE-based security programs.

Capture The Flag (CTF) Events

The Last Minute Capture the Flag [CTF] event is back for another year during Blue Team Con. This is a beginner-friendly CTF competition. 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 Room Hours:
Friday, September 6th: 10:30 am to 5:00 pm
Saturday, September 7th: 10:00 am to 1:00 pm

CTF winners will be announced at the closing ceremonies!

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 6th, at 6:00 pm CDT.

The rest of the challenges and the competition will begin Saturday, September 7th, at 10:30 am CDT until Sunday, September 8th, at 11:30 am CDT.

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://btcctf.com

Put your gray matter to the test at Graylog's upcoming Capture The Flag (CTF) event! Immerse yourself in our virtual sandbox environment, where you'll take on unique and captivating puzzles sure to entertain and challenge your wit and skill in data analytics and cybersecurity.

This event isn't just about answering multiple-choice questions or writing essays. It's about diving into complex scenarios that will push you to think in new ways while hunting for hidden clues, threats, and terrible puns. Whether you're a beginner looking to learn new concepts or a seasoned pro wanting to showcase your expertise, our inclusive format ensures everyone can participate and thrive.

Join us for an unforgettable experience where education meets excitement. Unlock your potential, compete for fun prizes, and emerge victorious in Graylog's one-of-a-kind CTF event, "Logs in the Shell"!

Saturday, September 7:00 am from 9 am until Sunday, September 8 at 1:00 pm (yes, overnight)

https://ctfd.logfather.org

Trend Micro's "Thieves in the Temple" Capture the Flag (CTF) event is tailored to those who are new to hacking challenges, offering an engaging experience for participants with a basic skill set. If this is your first foray into hacking games, this event is the perfect starting point. Beginner CTF players can dive in and achieve success, while those with some experience—though not yet at an expert level—can tackle the "hard mode" for added complexity and a greater challenge.

"Thieves in the Temple" Participants will navigate the CTF challenges using common hacking tools to infiltrate an environment, escalate privileges, and exfiltrate data to achieve the objective. They will gain a unique "purple team" experience, getting hands-on with cybersecurity incident response by exploring response actions and detections. This will involve uncovering forensic artifacts from the threats they've executed, completing the CTF challenges from both an offensive and defensive perspective.

The challenge will take a total of about 3 hours to complete (if played without a break) but players will be able to play the entire duration of the conference.

Saturday, September 7:00 pm from 9:00 am until Sunday, September 8 at 1:00 pm (yes, overnight)

https://www.eventcreate.com/e/blueteamcon

Villages

Saturday, September 7, 2024 from 10am to 6pm CT
Sunday, September 8, 2024 from 10am to 3pm CT

High profile industrial control system (ICS) security issues have grabbed headlines and sparked change throughout the global supply chain. The ICS Village allows defenders of any experience level to understand the unique failure modes of these systems and how to better prepare and respond to the changing threat landscape.

Interactive simulated ICS environments, such as Hack the Plan(e)t and Howdy Neighbor, provide safe yet realistic environments to preserve safe, secure, and reliable operations. The ICS Village brings a compelling experience for all experience levels and types, with IT and industrial equipment. Our interactive learning approach invites you to get hands on with the equipment to build your skills.

We bring you real components such as programmable logic controllers (PLC), human-machine interfaces (HMI), remote telemetry units (RTU), and actuators to simulate a realistic environment by using commonly used components throughout different industrial sectors. You will be able to connect your machine to the different industrial components and networks and try to assess these ICS devices with common security scanners to sniff the industrial traffic, and more!

Why is it Running Windows XP?
Bryson Bort, CEO/Founder, SCYTHE and Co-Founder, ICS Village

[Saturday 10:00 am, 2:00 pm] [Sunday 10:00 am]

Introduction to the practical space of industrial control systems and critical infrastructure. Why are things the way they are? What is the government doing? How does ICS affect you today? How do you threat model and conduct risk assessments in OT?

Introduction to ICS with demonstration
Kenny Warren, Staff OT/Offensive Security Engineer, GRIMM

[Saturday 11:00 am, 3:00 pm] [Sunday 11:00 am]

Overview of Industrial Control Systems (ICS), explaining how they consist of field devices like sensors and valves, controllers such as PLCs and RTUs, and Human-Machine Interfaces (HMIs). We will then discuss ICS network protocols, focusing on Modbus/TCP. I will introduce "TinyTown," a miniature ICS network range, consisting of a PLC, HMI, physical outputs, and networking components. The talk will also cover ICS network attacks, specifically how Modbus/TCP can be exploited to modify system states. Finally, I will demonstrate using Metasploit to send Modbus commands to the TinyTown PLC, showing how this can manipulate the system to produce a real-world effect.

Cyber Informed Engineering - or - How I Learned to Stop Worrying and Love the Complexity
Chris Rose, Senior Director, AEGIS (Architecture, Engineering, Infrastructure and OT Solutions)
MorganFranklin Consulting, Cybersecurity

[Saturday 12:00 pm, 4:00 pm] [Sunday 12:00 pm]

In an era where cyber threats are becoming more sophisticated and targeting the very core of our critical infrastructure, it's time to elevate our Blue Team activities by rethinking security from the ground up. Cyber Informed Engineering (CIE) offers a transformative approach, positioning cybersecurity as a 'First Principle' in the engineering and operation of secure systems. In this talk, I will propose CIE as a model for deeply integrating 'Secure By Design' principles into the technical fabric of our defenses, uplifting Blue Team efforts from reactive measures to proactive, deeply embedded resilience. By embracing CIE, we can enhance the technical integration of security practices into daily operations, empowering our Blue Teams to anticipate, detect, and mitigate threats with unprecedented precision and effectiveness. This approach not only strengthens our defenses but also positions us at the forefront of a new wave of thought leadership in information security.

Villages

Hak4Kidz

Saturday, September 7, 2024 from 9am to 5pm CT

NOTE: The Hak4Kidz village is restricted to children (and their parents) with a Hak4Kidz's ticket only.

Hak4Kidz operates as a public charity registered with the IRS under 501(c)(3) regulations.

Ethical hackers, information security professionals, and educators will bring the benefits of white hat hacking to the children and young adults at the conference. Hak4Kidz plans to accomplish this mission by putting their collective expertise and passion on display for the attendees to interact with at their will. An open area of stations will enable the attendees to expand and enlighten their technical interests. For innovation to perpetuate, it's imperative that today's young users are exposed to the bigger picture of how we got here and to help realize their potential.

Activities for kids will include SpyMath, SnapCircuits, Heal's Ask Me Anything, and more. If participating, please have kids bring a laptop with Wireshark installed and tested.

Their website can be found at https://www.hak4kidz.com/.

Wellness Village

Saturday, September 7, 2024 from 10am to 6pm CT
Sunday, September 8, 2024 from 10am to 3pm 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.

Wellness Village Schedule

Saturday, September 7

10:30 AM: Healing Leadership – Apply Trauma-Informed Concepts in your Organization | presented by Molly Mackey

12:00 PM: Discussion group – Leading with Heart: Leveraging Emotional Intelligence for Effective Leadership | presented by Molly Mackey

2:00 PM: When Failure Cuts | presented by Dan Tuuri

3:00 PM: Discussion Group – Navigating Tragedy and Grief with Grace | presented by Amanda Scheldt (The Glam Techie)

4:00 PM: Resilient Relationship Security: Reduce Lost Connections | presented by Zoe Lindsey

5:00 PM: Discussion Group – Fostering Psychosocially Safe Teams and Work Practices | presented by George Sanford

Sunday, September 8

11:00 AM: Yourself Matters – Building a Self-aid Kit | presented by Gabriel

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

Massage Therapy @ The Wellness Village

New for 2024, we've brought in two massage therapists offering 10-minute massages from 10am to 3pm CT on Sunday September 8th. Massages are first come, first serve.

Villages

SPONSORED BY

<hunter_strategy>

Ready for a break?

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!

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

Career Village

Saturday, September 7, 2024 from 10:30am to 6:00pm CT
Sunday, September 8, 2024 from 10:00am to 12:00pm CT

A Career Village that involves hiring managers and business professionals.

Are you starting a new career in cybersecurity? Or maybe you're looking for a change in scenery or direction? This village is your opportunity to schedule one-on-one 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. Learn how to prepare for interview settings that employers are utilizing today. Practice your interview skills and get direct feedback so you can feel more confident in your job search.

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!

Partners

CISA – Cybersecurity & Infrastructure Security Agency

CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. We are designed for collaboration and partnership. Learn about our layered mission to reduce risk to the nation's cyber and physical infrastructure.

Visit their booth Blue Team Con to learn more.

https://www.cisa.gov/

Docent Institute

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/

NCL – National Cyber League

The mission of the NCL is to prepare the next generation of cybersecurity professionals by providing high school and college students, as well as their coaches, an online, safe platform of real-world cybersecurity challenges. We build pathways for students that lead to successful career placements in the cybersecurity field.

Visit their booth at Blue Team Con to learn more.

https://nationalcyberleague.org/

Partners

SAIC – School of the Art Institute of Chicago

SAIC is distinct in the way that we provide graduate, post-baccalaureate, and undergraduate students an interdisciplinary curriculum and the necessary freedom to develop as artists, designers, and scholars. We strive for a level of rigor, investigation, and cultural relevance that makes SAIC truly special.

Make sure to check out the SAIC Student art installations at the BTC networking party Saturday night!

https://www.saic.edu

Sober in Cyber

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). 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/

WiCyS – Women in Cybersecurity

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/

WSC – Women's Society of Cyberjutsu

Founded in 2012, the Women's Society of Cyberjutsu (WSC) is a 501(c)3 International nonprofit community, focused on empowering women to succeed in the cybersecurity industry. WSC's mission is to advance women in cybersecurity careers by providing programs and partnerships that promote networking, education, training, mentoring, resource-sharing and other professional opportunities.

https://womenscyberjutsu.org

Sponsors

BLUE TEAM CON 2024 FOUNDING SPONSOR

onShore SECURITY

TRAINING SPONSOR

Microsoft

ULTIMATE SPONSOR

Push

PLATINUM SPONSORS

gravwell

TRIMARC

corelight

Sponsors

GOLD SPONSORS

Turn gate

LIMA CHARLIE

Sublime Security

SLEUTH KIT LABS

SPECTEROPS

SILVER SPONSORS

illumio

seemplicity

Cribl

Ontinue AI-Powered MXDR

TRUSTEDSEC

SecureIdeas professionally evil

PATRIOT CONSULTING

cydarm

onShore SECURITY

<hunter_strategy>

+Villages Sponsor

BRONZE SPONSORS

TECHNOLOGY SEMINAR SERIES

Sponsored by NineStar Connect.

STATS ON STATS

Focivity

no starch press

OTHER SPONSORS

ASSUMED

Badge Sponsor

CLEARVECTOR

Speaker/Trainer Dinner Sponsor

STELLAR CYBER®

Saturday Night Party Sponsor

graylog

Logs in the Shell CTF

TREND MICRO™

Thieves in The Temple CTF

StoneX — 100 years —

Swag Bag Sponsor

SHMOOCON

Saturday Night Board Game 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

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)

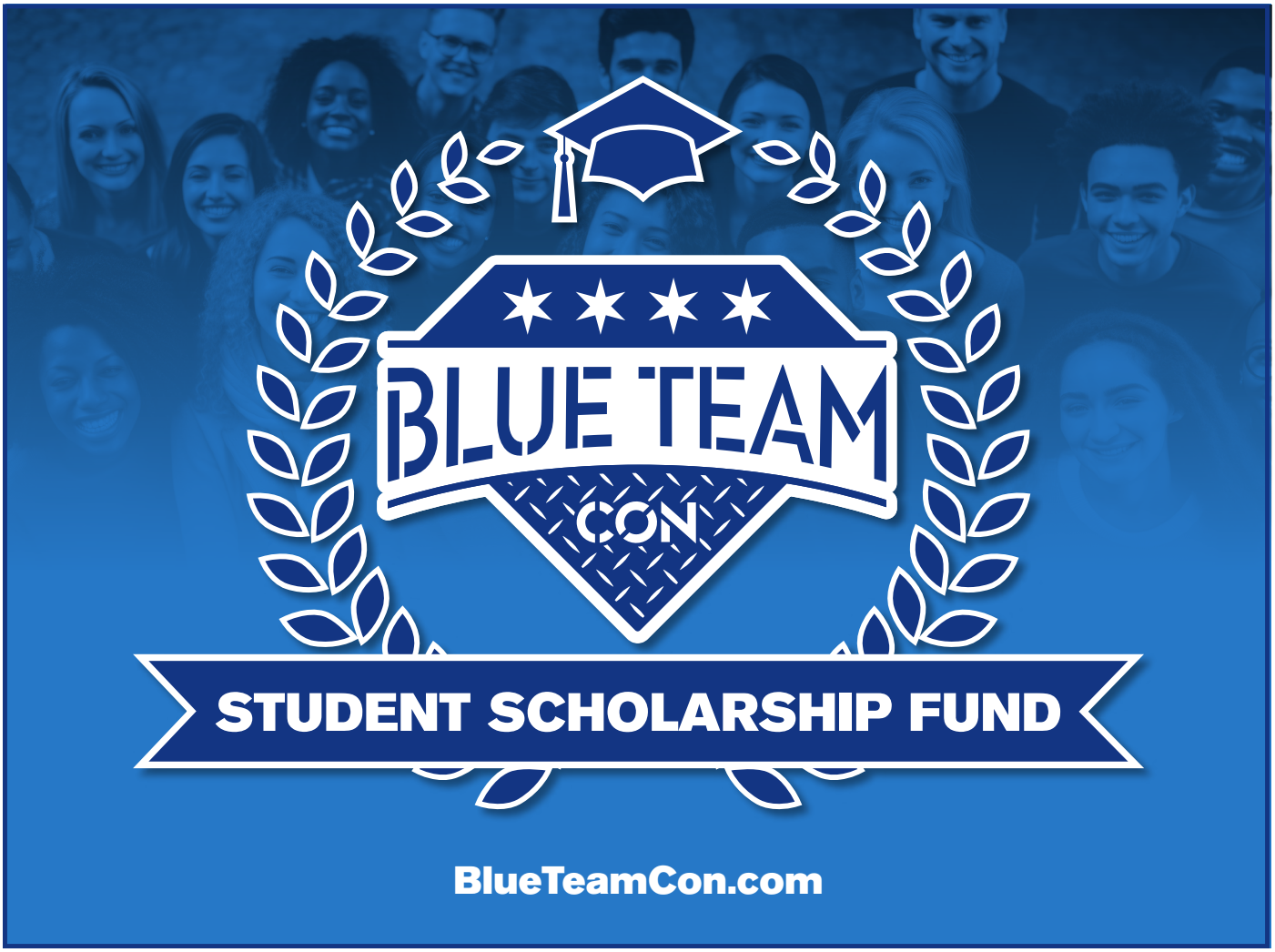
Submitting CPE Information

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)², 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/



BLUE TEAM CON 2024

THANK YOU

for attending Blue Team Con!

SEE YOU NEXT YEAR!


BLUE TEAM
CON