BLUE TEAM CON 2023

August 25-27, 2023
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

Welcome, everyone, to the third iteration of Blue Team Con.

It's our 3rd year and growing so that means many of you will be with us for the first time. We've come a long way, but the mission remains the same. We aim to bring the cybersecurity defender community together. This means young and old. Leaders and practitioners. Engineers and policy nerds. Students and mentors. Employees and employers. And the whole swath of methods, solutions, services, principles, and practices for the Blue Team. No one is an island. We need each other.

But let's have fun. Because, face it, you identify as a cybersecurity nerd and a defender. All the conversations we've been having all year on social media and the great hacking cons gain focus here at Blue Team Con. We've become friends from helping each other, learning from each other, and guiding the industry with our facts, opinions, research, and collaboration. The democratically elected speakers are already part of the greater conversation that accelerates in person.

This year we've added the Lounge. Now you can continue post-talk discussion or grab a group or just see who's there to have a chat. And coming back is the Unconference where anyone can grab a slot to present. That goes all night! Our quiet party room gives you an alternative vibe to the big party so make some new friends in the atmosphere best for you.

Best of all we've added a full day of training right before the conference. People asked for formal training in addition to talks so we delivered. Tickets have sold out, so we know we hit it. And for the first time at any cybersecurity conference, we have cybersecurity training for boards, thanks to our collaboration with the Private Director's Association.

This conference is for you. Whether you're capturing that face-to-face time with old friends, making new ones, influencing the industry, checking out great products, or just racking up some CPE, it's all about our community of defenders.

Thanks for joining us and welcome to Blue Team Con!

Stel Valavanis
Blue Team Con Advisory Board Member

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.

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, your choice. You may return to the event once you have deposited your device in a secure location, 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

@LittleR3d

BECKY
Selzer

becky@blueteamcon.com

@BeckySecurity

CARL
Hertz

carl@blueteamcon.com

@cillic

PHIL
Skentelbery

phil@blueteamcon.com

@PhilSkents

FRANK
McGovern

frank@blueteamcon.com

@FrankMcG

STEL
Valavanis

stel@blueteamcon.com

@StelValavanis

ALYSSA
Miller

alyssa@blueteamcon.com

@AlyssaM_Infosec

CFP
Board Members

JOHN
Behen

CHRIS
Lemmon

KAYLEE
Burns

ERICH
Nieskes

TISH
Harper

CHRISTINA
Stokes

KEVIN
Jackson

AMBER
Welch

Schedule *All times are in CDT.*

Thursday, August 24

Registration: (Lobby) 6:00pm to 9:00pm

Friday, August 25

Registration: (Lobby) 7:00am to 10:00am and 6:00pm to 9:00pm

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

Training: 8:45am to 5:00pm

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/

Saturday, August 26

Registration: 7:00am to 5:00pm

Swag Hours: 11:00am to 4:00pm

SPONSORED BY VULCAN.

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

8:30 AM

8:30am to 8:55am
Opening Ceremonies with Blue Team Con Advisory Board

9:00 AM

9:00am to 9:45am
Keynote: We're All Scared, Too: 10 Years of Lessons from Cybersecurity Mentorship
with Lesley Carhart

10:00 AM

10:00am to 10:50am
Who's to blame for the lack of DEI Opportunities in Cybersecurity? I am
with Daniel Magallanes

10:00am to 10:50am
Scraping new territory: Defending privacy in the new world
with Dana Baril and Steven Hsieh

11:00 AM

11:00am to 11:50am
An Enterprise on Fire: Successful Strategies in Triage
with K "Turb0Yoda" Singh, Bluescreenofwin

11:00am to 11:25am
Vulnerability Cognition: Adding Psychology to VulnMgmt Programs
with Nikki Robinson

11:30am to 11:55am
Vulnerability Prioritization: Addressing The Great Debate
with John Behen

Saturday, August 26

SPONSORED BY

VULCAN.

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

12:00 PM

12:00pm to 12:50pm
PCI DSS v4.0 Is Here – Now What?
with Kyle Hinterberg

12:00pm to 12:25pm
Building Yourself Into a Strong Identity Practitioner
with Eric Woodruff

12:30pm to 1:00pm
From 1-on-1s to 1s and 0s
with Sochima Okoye

1:00 PM

2:00 PM

2:00pm to 2:50pm
Non-Traditional Paths Into Cyber-Security: How recognizing and targeting complimentary skillsets can ease the skills shortage
with Kayla Williams

2:00pm to 2:25pm
Can't Trust These Logs
with Jose A. Martinez

2:30pm to 2:55pm
The Anatomy of a Threat Hunting Hypothesis
with Lauren Proehl

3:00 PM

3:00pm to 3:50pm
"Defending Beyond Defense"
with Dr. Catherine J. Ullman aka investigatorchic

3:00pm to 3:25pm
Network scanning in the era of IoT / OT: Challenges and solutions for blue teams
with Huxley Barbee

3:30pm to 3:55pm
You have a SIEM, Now What?
with Chris Maulding

4:00 PM

4:30pm to 4:55pm
The Modern CISO
with Sahan Fernando

5:00 PM

5:00pm to 5:50pm
Transforming Vulnerability Management – How CSAF, VEX, SBOMs and SSVC Work Together
with Justin Murphy

5:00pm to 5:25pm
Why not all metrics are created equal
with Pedro Jimenez-Hernandez aka spapjh

5:30pm to 5:55pm
There is no 'I' in team, but if you look closely, there is a me – being the first dedicated security hire and growing a team.
with Mike Sheward

6:00 PM

Saturday, August 26

SPONSORED BY

VULCAN.

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

7:00 PM

8:00 PM

9:00 PM

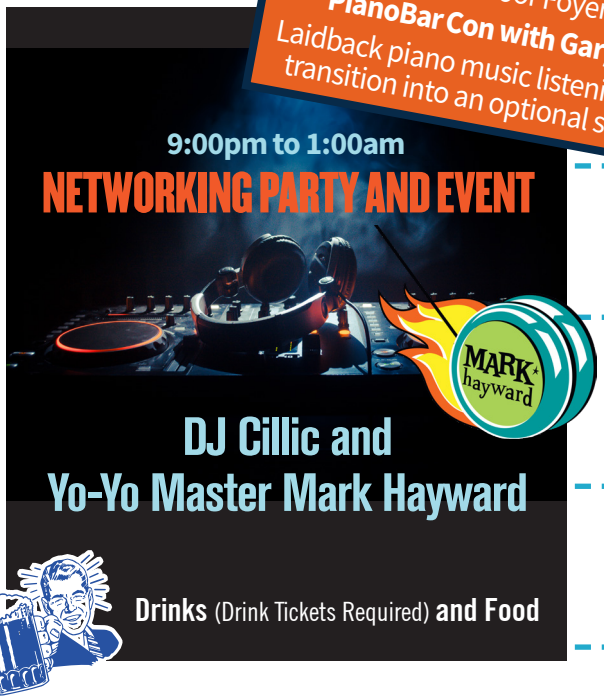
10:00 PM

11:00 PM

12:00 PM

1:00 AM

8:30pm to 9:30pm
3rd Floor Foyer
PianoBar Con with Gary Rimar
Laidback piano music listening that will transition into an optional sing-along.



Sunday, August 27

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

SPONSORED BY

VULCAN.

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 25 Minutes
Crystal Room

10:00 AM

10:00am to 10:50am
Keep the F in DFIR: The Importance of Digital Forensics in Incident Response
with Partha Alwar and Carly Battaile

10:30am to 10:55am
Volunteering FTW: A Path to Learning, Career, and Community Growth with Tabatha DiDomenico

11:00 AM

11:00am to 11:50am
Dude, Where's My Domain Admins?
with Joel M. Leo

11:00am to 11:25am
Killing the Skills-Gap (from the inside and out)!
with Jacob Bond

11:30am to 11:55am
How to Deal With Human Malware in the Workplace
with Gary Rimar

12:00 PM

1:00 PM

1:00pm to 1:50pm
HOW TO MAKE AI COMPLY
with Raul Rojas (AKA El Jefe De Security)

1:00pm to 1:25pm
Smoke and Mirrors: Wasting a hacker's time with misdirection & obscurity
with Mishaal Khan

1:30pm to 1:55pm
Breaking the Mold: The Same Approach to Breaking into Information Security but {d!f3r3nt}
with Veran Patel

2:00 PM

2:00pm to 2:50pm
New AI who dis? Building an APT hunting detection pipeline with GPT3
with Matt Coons

2:00pm to 2:25pm
Authentication Proxy Attacks: Detection, Response and Hunting
with Chris Merkel and Chester Le Bron

3:00 PM

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

4:00 PM

KEYNOTE SPEAKER

Lesley Carhart

DIRECTOR OF INCIDENT RESPONSE, DRAGOS

We're All Scared, Too: *10 Years of Lessons from Cybersecurity Mentorship*

For the past decade, Lesley has been running career clinics for job seekers and changers in cybersecurity. For the past year, they have added on 1:1 mentorship office hours. Helping people choose career trajectories and overcome hurdles in employment has been a fascinating window into the fears, insecurities, concerns, problems, and victories of a wide range of people who work (or want to work) in cybersecurity. Many of their challenges are more universal than people are brave enough to admit, and everyone can learn from them to have a happier career.

About Lesley

Lesley Carhart is a Chicago-based Digital Forensics and Incident response professional specializing in investigations of industrial control system networks. They currently work for the industrial control cybersecurity company, Dragos, Inc - investigating intrusions into utilities, manufacturing, and transportation systems. Lesley speaks, teaches, and blogs about the topic around the world. In their free time, Lesley runs a virtual conference, as well as resume and career clinics for cybersecurity job-seekers, as well as teaching small kids to kick things. They are honored to have received awards like DEF CON Hacker of the Year and SANS Difference Maker Lifetime Achievement.

hacks4pancakes@infosec.exchange @hacks4pancakes lcarhart

TRAINING FRIDAY, AUGUST 25TH

PRIVATE DIRECTORS ASSOCIATION®

Creating Value Through Board Excellence

Presents

CYBERSECURITY BOARD TRAINING

Robert Barr, Rochelle Campbell, Matt DeChant, Julie Liu, Troy Mattern, Alyssa Miller, Jeff Olejnik, David Olivencia, Anthony Petitte, Michael Phillips, Ralston Simmons, and Stel Valavanis.

The Private Director's Association is proud to present the PDA Cybersecurity Board Training, designed in collaboration with Blue Team Con. This all-day training targets directors of company boards and 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 in 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 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.

New SEC regulations require that board cybersecurity expert be listed in their 10-K reports along with protective and detective measures. While this does not legally affect private boards, PDA considers the requirement to be good practice and, furthermore, recommends that all board members receive basic cybersecurity training. Leading organizations do not wait for regulation to lead them and neither should their boards!

The PDA Cybersecurity Board Training provides a full day of panels, workshops, and tabletop exercises. Coffee, lunch, and an evening networking dinner with instructors and PDA committee members are included.

ADVANCED MEMORY FORENSICS

with Jamie Levy

Director of R&D, Huntress and Sr Dev, Volatility

Memory Forensics is a required skill for digital analysts these days; it is also a needed in order to keep up with advanced attackers. In addition to attackers avoiding disk, thousands of nodes and BYOD are increasing the complexity of investigations. Gone are the days when an analyst could examine one machine at a time- results must be quick and precise. Oftentimes if you are not proactive, you've already lost the war before you even knew it was raging.

This workshop demonstrates the importance of including Volatile memory in your investigations by covering several attack methodologies that we've seen in the field. It also includes an overview of the most widely used memory forensics tool, Volatility, by one of its developers.

DEFENDING YOUR ENTERPRISE USING SECURITY ONION

with Bryant Treacle

Senior Engineer and Training Manager, Security Onion Solutions

This one-day class will equip students with the necessary skills to properly place network sensors and investigate malicious activity using network and host data in enterprise environments. Students will learn core analyst techniques needed to investigate alerts, determine the scope of an incident, and manage a case using the Security Onion 2 platform.

TRAINING

FRIDAY, AUGUST 25TH

RANSOMWARE ATTACK SIMULATION AND INVESTIGATION FOR BLUE TEAMERS

Markus Schober

Founder, Blue Cape Security

As a cyber security defender and investigator, we mostly only get to see a backwards perspective on how attacks unfolded, typically from impact and ransomware execution we are trying to make our way back in time to understand the scope and initial infection vectors of a breach. This is why it can help tremendously to be familiar with the typical TTPs that often employed by ransomware threat actors. This workshop will provide hands-on training on performing a typical ransomware attack in a Windows lab environment, using PowerShell Empire. Participants will gain an understanding of the techniques and tactics used by ransomware attackers, from initial access and reconnaissance to privilege escalation, credential dumping, lateral movement, defense evasion, data exfiltration, and encryption. Individual online lab access will be provided via RDP to follow along with the instructor throughout the workshop. By the end of the workshop, attendees will have a better understanding of the ransomware attack lifecycle, the tactics used by ransomware attackers and how to detect, respond and ultimately prevent them.

USE YOUR BOOTH PASSPORT FOR YOUR CHANCE TO WIN COOL PRIZES

BLUE TEAM CON 2023

ENTER TO WIN
THE OFFICIAL BLUE TEAM CON QUILT

Official Blue Team Con Quilt Raffle. See Swag to fill out a free entry ticket (No Purchase Necessary). Must be present at Closing Ceremonies to win!

Talk Track One
50 MINUTES

SPONSORED BY VULCAN.

An Enterprise on Fire: Successful Strategies in Triage

K "Turb0Yoda" Singh - Incident Response Consultant, CrowdStrike
Bluescreenofwin - Senior Security Engineer, Accretive

0900 PST. You grab your cup of coffee and get into your chair. You begin the day with some small cheese factory in Wisconsin claiming that they've been hacked. As you log in, you behold default creds, no MFA, and a small Cisco firewall set to ALLOW ANY:ANY because hey, having a rule means passing compliance checks. In the corner of your eye, you suddenly start to see alerts appear. Mimikatz, Metasploit, some Cobalt Strike Beacons, LSASS dumps, the lot quickly piles on and on in your environment. No amount of caffeinated adrenaline will help as you watch your environment go up in flames.

Even the most seasoned veterans can be stricken by keyboard fright when facing the unknown state of a compromised system. Maybe your playbooks are woefully inadequate, out of date, or simply don't exist. Perhaps you've assumed that your tooling will feed you information, but the right information may not always be available or easily consumable. It can be daunting when faced with the prospect of manual box-by-box triage.

If you've ever been in any of the aforementioned situations and have stared in incredulity at your terminal then this talk is for you.

We will examine the compromised environment from the 2023 WRCCDC security competition and discuss the foundation of the competition and the infrastructure from where all the data was pulled. Next, we will explore the strategies of the teams based on data from images taken at specific and timed intervals. Lastly, we will attempt to rank the strategies undertaken by the top eight collegiate cybersecurity teams in the competition and focus on what steps led to the most success in remediating the threat, which were not successful, and what kept threat actors out of systems the longest.

Defending Beyond Defense

Dr. Catherine J. Ullman - Principal Technology Architect, Security, University at Buffalo

Assumptions burn defenders every day. Perhaps the most pernicious one is that systems and their controls will always work as designed. Best practices in security may be good guidelines, but unfortunately also suffer from these same blind spots. For example, best practice recommends the use of LAPS for local administrator account passwords of domain-joined computers, yet misconfiguration of active directory can turn it from a protective control into a vulnerability. But what if there was a way to challenge these assumptions up front? The best way to dismantle these types of assumptions is to experience how deeply flawed they are. There is no better way to gain first hand experience into this perspective than immersion in the offensive security space. In this talk we'll explore how to immerse yourself in the offensive security world to obtain this knowledge without needing to change careers or obtain additional certifications. By being more informed about offensive security, defenders are better able to recognize relevant intel, understand existing threats, and more readily discover attacker behavior. Join me as I discuss how there's more to defending than just defense, and how you can find and engage with the amazing resources that are out there waiting to be explored.

Dude, Where's My Domain Admins?

Joel M. Leo - Experienced Infosec Architect

Attacker pops a workstation on your domain
Attacker establishes her foothold and local persistence
Attacker begins recon of AD, starting with Domain Admins

ERROR: The group name could not be found.

Attacker, with a disconcerted look on her face: "Dude, where's my Domain Admins?"

Killchains that involve AD usually involve enumeration of highly-privileged accounts: members of Domain/Enterprise/Builtin Admins, Server Operators, etc. Those groups and their members can be enumerated in AD by default, exposing members as targets of exploitation to obtain those privileges. However, there's a way to use in-the-box AD capabilities to thwart these attempts. Using List Object mode, implicit deny, and AdminSDHolder/SDProp, AD defenders can hide these principals from unprivileged users. In this talk, I'll walk you through the principles, process, and pitfalls, so you can raise the bar on your AD defenses without blowing things up.

HOW TO MAKE AI COMPLY

Raul Rojas (AKA El Jefe De Security) - CSO/Principal Hacker in Residence, Microsoft

How are you adopting AI/ML into your enterprise? How hard can building an AI really be? What should you consider when introducing an AI model? Are you prepared for the consequences? How to do set guard rails so that your developers don't break you into jail?

This talk is a Treatise on AI/ML challenges for governance and strategic guidance for securing AI/ML scenarios within an enterprise for product research and development. Developed from years of experience learning how to approach AI/ML projects in Microsoft Research, I will attempt to shed light on some of the current thinking and best practices for AI models for internal and public use.

You can expect to learn about the explosion of technologies becoming available to industry and the challenges facing platform builders and enterprises now that these features are present.
We'll take a journey through the current regulatory landscape and share some considerations that Security governance programs should think about for their own AI/ML compliance.

Learn about how security fundamentals have not really changed but must be enhanced to deal with these new realities, including new perspectives on protecting the supply chain, approaching AI scenarios in threat modeling, building controls for resilience and the new demands of logging and auditing in real time for intentional behavior vs malicious behavior.

Then we wrap up with how to approach educating compliance organizations, your leaders, and your developers to be prepared to understand AI/ML risks and adopt AI with due diligence.

Keep the F in DFIR: The Importance of Digital Forensics in Incident Response

Partha Alwar - Director, Stroz Friedberg
Carly Battaile - Manager, Stroz Friedberg

In recent years, blue teamers have greatly benefited from advanced security tools such as EDRs and XDRs. While these tools provide valuable visibility and containment mechanisms during DFIR investigations, over-reliance of these tools in DFIR investigations may lead to an incomplete picture of the incident. In this presentation, we will discuss how traditional forensic analysis methods can provide a more holistic look at an incident and reduce gaps in visibility.

Our presentation will provide an overview of challenges encountered when using EDR tools such as telemetry retention, OS compatibility, deployment scope and the lack of forensic artifacts that track interactive activity by an attacker. Next, we will introduce several forensic artifacts such as Amcache, Shellbags, Windows UAL etc. that provide deeper, historical visibility into attacker activity. Using forensic artifacts introduced in this presentation, blue teamers will be able to piece together and timeline crucial pieces of evidence on systems that provide insight into historical process executions, file/folder access, lateral movement, etc. Finally, we will introduce real-life case studies where forensic methods have proved vital in incident response investigations.

Attendees of this presentation will gain a better understanding of forensic artifacts and how they can be utilized in incident response investigations. They will also learn about free and open-source tools available to parse these artifacts at scale.

Talk Track One
50 MINUTES

SPONSORED BY VULCAN.

New AI who dis? Building an APT hunting detection pipeline with GPT3

Matt Coons - Security Manager, Incident Response, GitLab

You can't browse Twitter or TikTok without seeing a video or post about ChatGPT, but how good is the engine behind ChatGPT when it comes to generating AI written threat detections that are high fidelity, actionable, and automatically mapped to MITRE ATT&CK techniques? In this talk we will explore the capabilities of GPT3, combined with the powerful CI/CD capabilities of GitLab to build a fully automated YARA based detection development pipeline to identify, test, and create high fidelity threat detection rules automatically mapped to their relevant MITRE ATT&CK techniques.

Participants will leave this the talk with a greater understanding of the capabilities of AI engines like ChatGPT and GPT3 and understand the power of using a CI/CD pipeline to automate detection testing and deployment.

Non-Traditional Paths Into Cyber-Security: How recognizing and targeting complimentary skillsets can ease the skills shortage

Kayla Williams - Chief Information Security Officer, Devo

Since inception, the Information Security industry has had a perpetual human capital and skills gap. With the advent of a variety of Massive Open Online Course (MOOC) programs such as EdX, Khan Academy and The Great Courses, the barrier to upskill across numerous domains is easier than ever. In addition, as companies explore removing college degree requirements, job requisitions open up to more candidates. As a result, the opportunity for a growing successful career in Information Security has not been greater. Despite this, the perception of the skills gap still exists.

As a result of these false perceptions, employers may miss out on skilled candidates with unique backgrounds and perspectives. Thus, organizations may suffer from the same issues as intelligence agencies by being stuck in old ways of thinking, much in the way Richard Heuer describes in The Psychology of Intelligence in 1999. By integrating these new and unique perspectives, employers can build in diversity of thought with different base skill-sets and come up with new perspectives and innovations.

This talk will dissect how to approach this systemic issue. Included will be the presenter's personal experiences, professional experiences with individuals transitioning into the industry, and provide concrete solutions for companies looking to overcome this hurdle. Solutions will focus on how to apply these new hiring paradigms from the top down, in addition to a potential avenue to resolution by building a pipeline avenue by creating relationships with education institutions.

PCI DSS v4.0 Is Here - Now What?

Kyle Hinterberg - Manager, LBMC

The Payment Card Industry Security Standards Council (PCI SSC) released v4.0 of the PCI Data Security Standard (DSS) in 2022 and the countdown is on. Organizations that need to comply with PCI DSS only have until April 2025 to implement all the new requirements. Are you ready and, more importantly, do you even know what it will take to be ready?

Many organizations need to comply with the PCI DSS and a major version change can be daunting. To make things worse, most of the information provided by the PCI SSC and other organizations can be vague and/or marketing focused. This leaves individuals confused as to what they really need to be doing to prepare themselves and their organizations. My goal is to break it down Barney-style so that no one gets stuck behind the eight ball when they run their first v4.0 assessment.

This presentation will:

- ✓ *Provide brief definitions of the PCI SSC and PCI DSS*
- ✓ *Explain the history of the PCI DSS (how we got to where we are)*
- ✓ *Provide an overview of the changes in v4.0, specifically avoiding any vague marketing talk and focusing on actionable items to help prepare organizations for v4.0*
- ✓ *Provide a summary of the big-ticket items that organizations should be working on to ease into v4.0*

Transforming Vulnerability Management - How CSAF, VEX, SBOMs and SSVC Work Together

Justin Murphy - Vulnerability Disclosure Analyst, DHS/CISA

There is no such thing as a “vulnerability-free” product. As we get more insights into our supply chains, we can easily be overwhelmed by the number of potential vulnerabilities. All of our manual processes are failing. Instead of burning people out with boring tasks, we need to change the way we handle vulnerability management. The presentation will show the interconnection and relationship of different standards, like the Common Security Advisory Framework (CSAF), the Vulnerability Exploitability eXchange (VEX), the Known Exploited Vulnerability (KEV) catalog, Stakeholder Specific Vulnerability Categorization (SSVC) and Software Bill of Materials (SBOM). It will cover what needs to change to keep up with the vulnerabilities and threats discovered today. Taking the November 2022 blog post Transforming the Vulnerability Management Landscape by Eric Goldstein, CISA’s Executive Assistant Director for Cybersecurity, as a starting point, the presentation will shed light on how the US government believes the situation can be improved. It will also cover the actions necessary to support the ecosystem to transform its vulnerability management. That includes the support of tools, use of procurement regulation, education and much more.

Who’s to blame for the lack of DEI Opportunities in Cybersecurity? I am.

Daniel Magallanes - Director of the Fusion Cell (Threat Intel/Hunt/Adversary Simulation), Cigna

As the world becomes increasingly digitalized, cybersecurity has emerged as one of the most critical fields in the world today. Cyber threat actors are becoming more sophisticated and adaptive. This has made cybersecurity professionals some of the most in-demand professionals in the global job market. However, as the demand for cybersecurity professionals grows, which the latest numbers hover around 3.5 million unfilled global jobs, the field is facing significant challenges when it comes to the lack of DEI representation. I’m to blame for this lack of representation because I’ve fell for the myth that all people coming into cybersecurity require a four-year technical degree, a myriad of certifications, and be able to code in C++ or Python. I’ve remained silent when we don’t recruit from Historically Black Colleges and Universities and Hispanic Serving Institutions.

My presentation will revolve around several key positions â€“ Hiring Managers, Recruiters, HR, C-Suite â€“ 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.

Talk Track Two
25 MINUTES

Authentication Proxy Attacks: Detection, Response and Hunting

Chris Merkel - Senior Director, Cyberdefense, Northwestern Mutual
Chester Le Bron - Lead Engineer, Threat Detection and Response

Over five years ago, Evilnginx was released, demonstrating the ease of stealing authentication session tokens from MFA-enabled logon processes with a simple reverse proxy. Despite being a well-known technique, few of these attacks were seen in widespread use among cybercrime threat actors, until recently.

The advent of the EvilProxy and similar platforms has now given attackers the ability to compromise targets with strong authentication without resorting to burdensome SIM swapping or noisy push fatigue attacks. With rapid adoption of phish-resistant MFA outside government-aligned sectors, organizations need to know how to detect and respond to these attacks.

In this talk, we will provide an in-depth look at the tactics, tools and procedures (TTPs) used by threat actors to effect account-takeover of MFA-enabled accounts. We'll demonstrate how the ingenuity of this attack has a fatal flaw at its core, allowing us to hunt, detect, mitigate and block this type of attack.

Breaking the Mold: The Same Approach to Breaking into Information Security but {d!f3r3nt}

Veran Patel - Associate InfoSec Analyst, Green Thumb Industries

Are you looking to break into information security, but are the requirements too high or don't match you? The demand for security professionals is growing, but many job seekers struggle to meet the high requirements set by employers. I will be sharing with you my experience trying to get into my current role, my mistakes, and the challenges I faced. We will discuss the problem faced by job seekers in the information security field, including the high requirements for education and certifications while presenting a unique/personal approach to job hunting that focuses on soft skills such as communication, problem-solving, critical thinking, and teamwork. Along with soft skills, I will show you exercises and study materials, such as websites, blogs, and videos that I used to develop my technical skills. Last but not least important, we will talk about networking "how to start" and getting YOU equipped with strategies for building professional connections in the current job market.

Building Yourself Into a Strong Identity Practitioner

Eric Woodruff - Semperis

Whether you're a seasoned Active Directory admin who cut your chops as a sysadmin, or coming into the identity space fresh, it can be daunting to understand how to get started within the identity space or transform yourself at the rapid pace the industry moves. And while "identity is the new security perimeter", it is often overlooked as a skillset in most cybersecurity degree programs.

In this conversation we'll dive into building yourself as a strong identity practitioner. For those newer to identity, we'll take a look at the many areas available for specialization. If you're looking to advance or change your career, we'll explore the different types of roles available as well â€“ from security researchers to identity program managers, the types of jobs available in identity are as deep as identity platforms themselves. Along with a look at the field, we'll explore ways to gain the technical and non-technical skills to bring yourself and your career to the next level.

Can't Trust These Logs

Jose A. Martinez

Logs are usually the foundation of a blue teamer's handbook, helping form the basis for audits and reconstructing events if an incident occurs.

But what if the information within your logs cannot be trusted, or their very existence is subverted, becoming an asset for an attacker instead of for your team? In this talk we will go over the approaches an attacker might take to bypass authentication, impersonate users, and use poorly secured logs to try and take over your application instead.

"Secure" GUIs with a poor API implementation, insecure cookie configurations, non authenticated endpoints with juicy data. These case studies will be briefly touched on, and inform how logs that just cannot be trusted (without further analysis) can come to be.

From 1-on-1s to 1s and 0s

Sochima Okoye - Associate Security Consultant, WithSecure

One thing we all know is how hard it can be to break into the technical side of security, even more so for those from unconventional backgrounds. If you don't speak Python as a first language or have a computer science degree, it feels like you don't have a shot.

This talk will show a unique perspective of how a Project Delivery Manager with no technical experience became a Pentester for a Cyber Security Firm, and what companies could stand to benefit by investing in people that don't always fit the mold. Managers and leaders who prioritize diversity of thought and strive to cultivate an individualist and forward-thinking culture should encourage hiring from a range of sectors when building their teams. So, to anyone contemplating making the switch to the technical side, this talk is for you.

Attendees will learn about the pitfalls faced on this journey and some tips and tricks for any aspirants looking to making a similar transition. In addition, how to support, mentor and hire those aspirants keen to get a foothold or side-step to a technical role.

How to Deal With Human Malware in the Workplace

Gary Rimar

Toxic maladaptive personalities ("human malware") both in our field and among the professionals we serve contribute to employee turnover in our field because jobs are plentiful and good people feel they don't need to put up with bad behavior. That, and many of us were never trained how to remediate human malware; it isn't like we can just reimage their operating systems to clean up the mess, and as much as we might like, "deleting" them is out of the question (unless we can fire them as the boss).

This talk will discuss some of the most toxic workplace behaviors and provide practical steps to combat these maladaptive workplace behaviors. It will discuss the power dynamics aspect of handling the maladaptive behavior among subordinates, peers, and supervisors. And, if the human malware is too pervasive to be managed, when you go apply for that better job with normal people, you will be able to succinctly describe the behaviors that led you to leave.

Talk Track Two
25 MINUTES

Killing the Skills-Gap (from the inside and out)!

Jacob Bond - Security Analyst, CyberArk

News headlines, Reddit posts, LinkedIn articles, and even internal corporate conversations everywhere often touch on a very common, and unfortunately, ongoing problem â€“ the skills-gap. Itâ€™s the reality that organically comes with the ever-evolving tech space: new technology breeds new threats, requiring new tools (or updated ones), thus introducing a new need for your InfoSec team: practical skills.

The impact of this “everywhere-at-once” issue ranges from increased risk due to uncoordinated response to plain old burnout among even some of the most determined individuals in the field. Several proposed solutions exist to combat skills-gaps, yet I believe event most Skill Ranges, Certifications, and Higher Education courses can become futile without proper planning stemmed from a simple question: “how exactly will this help us?”

My tested theory is that skills development, as a continuous endeavor for any team, requires its own lifecycle. One that acts as the bridge to an organization’s security needs and requirements, broken down and then defined by its applicability for said business. Its steps include identify, breakdown, hypothesize, align, research, assess, and practice (and will be presented as a framework with a template as a takeaway).

By incorporating this developed lifecycle, Leaders and Managers alike can create a tangible program to significantly reduce most any learning curve. Tested disciplines include Detection Engineering and Automation, Incident Response (all phases), Documentation, and Public Speaking.

The benefit for audience members is to walk away with a more scientific approach to handling their own skills gaps with a newly obtained conceptual approach that I am confident has universal results for almost any InfoSec skill gap.

Network scanning in the era of IoT / OT: Challenges and solutions for blue teams

Huxley Barbee - Security Evangelist, RunZero

The Internet of Things (IoT) and the rise of Operational Technology (OT) networks have brought about a significant increase in the number of connected devices in modern networks, creating new challenges for blue teams in terms of inventorying assets, identifying and mitigating vulnerabilities, and verifying security controls coverage. This presentation will explore the unique challenges that IoT and OT pose for network scanning and provide solutions for effectively addressing these challenges while ensuring the safety and availability of these systems. The presentation will cover topics such as identifying IoT and OT devices on a network, understanding the context of vulnerabilities associated with these devices, and implementing appropriate security controls to mitigate these risks while ensuring the safety and availability of these systems. Attendees will also learn about best practices and tools for IoT and OT network scanning, such as using automated asset inventory, performing regular vulnerability assessments and testing the changes in a controlled environment before implementing them. The goal of this presentation is to equip blue teams with the knowledge and skills they need to effectively protect their organizations' networks in the era of IoT and OT while ensuring the safety and availability of these systems.

Scraping new territory: Defending privacy in the new world

Dana Baril - Security Engineering Manager, Meta
Steven Hsieh - Security Engineer, Meta

Data scraping is a unique threat, as adversaries apply offensive security techniques to obtain private user data at scale. Detecting and preventing scraping threats also entails a unique set of technical challenges, as it involves a variety of adversary profiles with limited incident signals for defenders. In recent years - in addition to the technical battle online - the battle against scrapers has transformed into a legal battle in the courts, with notable precedents impacting the overall scraping landscape.

In this talk, you will learn about the scraping threat landscape, and the lessons learned through defending and preventing scraping threats in the world's largest social networks, Facebook and Instagram. We will cover attack scenarios, unique threat requirements, adversary profiles, and share our best practices for reducing scraping risks by adjusting common practices, such as Static Analysis and Red Teaming. In addition, we will provide context on the latest legal precedent in the scraping field, and how it can shape defense practices and user behavior. We will end with a call for action for security professionals, and how you can and should be more involved when setting industry standards for users' privacy.

Smoke and Mirrors: Wasting a hacker's time with misdirection & obscurity

Mishaal Khan - vCISO

In the world of DevSecOps, it's not enough to simply secure your applications and systems against known vulnerabilities. As cybercriminals become more sophisticated, taking additional steps is important to make it more difficult and expensive for them to breach your defenses. Obfuscation techniques can be a powerful tool in this fight, costing hackers valuable time, resources, and money.

In this talk, we'll explore some simple obfuscation techniques that can be used to make life harder for hackers. We'll cover simple to advanced techniques like hiding the login page, redirecting hackers to honeypots, using fake data that triggers canaries, preventing email scraping, feeding fake emails to scanning tools, using dummy DNS entries, and using fake comments in code to mislead attackers about vulnerabilities that do not exist. We'll also discuss strategies for obscuring code and purposely leaking API keys to create distractions and dead ends for attackers.

Whether you're a developer, security professional, or DevOps practitioner, this introduction will provide valuable insights into how you can use obfuscation to make your applications more secure and resilient against cyber attacks. Join me and learn how to make life harder for hackers in DevSecOps!

The Anatomy of a Threat Hunting Hypothesis

Lauren Proehl - Sr. Manager, Global Cyber Defense, Marsh McLennan

This presentation is based off a blog post that explains how to create more effective threat hunting hypotheses using sentence diagramming and impact multipliers. A version of this presentation has been given in 20 minute and 45 minute formats.

The first half of the presentation will illustrate a technique called hypothesis diagramming. This process involves defining a technique, target, and action on objective (or payload) for each hunt. This method teaches analysts or threat hunters a repeatable process for creating hypotheses that ensures an adequate scope is always defined. This is almost like Mad Libs for threat hunt hypotheses. In addition, I will include several examples of real hunt hypotheses with the respective elements mapped.

The second half of the presentation will focus on the various impact multipliers that can be applied to a hypothesis to increase relevancy and potential output. This will discuss five common impact multipliers of relevancy: industry, geolocation, technology stack, VIP status, and trends. Each impact multiplier can tweak a hypothesis to take it from generic to organization specific. For example, if you work for university in Kansas that doesn't operate out of the state, hunting for point of sale malware that impacts North Korean grocery stores may not be the best use of the time.

Wrapping up, this presentation will give examples of hypothesis diagramming + impact multipliers and real hypothesis examples. Several more advanced hunting resources will be provided at the end of the presentation, in addition to ten more hypotheses for people to explore further.

The Modern CISO

Sahan Fernando - Chief Information Security Officer, Rady Children's

This talk is geared towards those that has aspirations to lead a security program. I plan to cover:

Do you really want to do it? What is the role these days
What are some routes to build the right experience?
What do you really end up doing?
How can you try to be successful in the role?

All of this will entail different aspects including team management, vendor management, program assessment and building strategic goals, communication strategies, and other relevant details. This could be expanded to a fifty minute talk as well!

Talk Track Two
25 MINUTES

There is no 'I' in team, but if you look closely, there is a me - being the first dedicated security hire and growing a team.

Mike Sheward - Head of Security, Xeal

Being the first dedicated security hire at any organization is an incredible learning experience. One moment you could be hands-on deploying EDR and MDM tools, the next, you're on a sales call with a prospect, or talking to the board. But amongst the opportunity, there is of course plenty of stress, anxiety, and burnout. When you're doing the things that might otherwise be done by a team of folks, how do you know where to get started? How do you prioritize? In this talk we'll answer those questions.

I've gone from being the first dedicated security hire, to building teams on three separate occasions now, and each time, I've done some things in the same way, and some things differently. The talk is a lesson's learned going from absolutely nothing on day one to a reasonably large security team with dedicated sub teams.

We'll discuss how the decisions you make early on, as the wearer of many hats, can have long lasting impacts when you start to distribute those hats. This includes technology and process decisions, along with hiring and delegation.

A final key message in the talk will be that even though there may only be one dedicated security person at a company, that person should never be expected to carry the weight of the whole company's security and privacy decisions, so we'll talk about how to set that boundary as well.

After all, there is no 'I' in team, but if you look closely, there is a me.

Volunteering FTW: A Path to Learning, Career, and Community Growth

Tabatha DiDomenico -

Are you looking to level up your skills, advance your career, and contribute to the infosec community? Volunteering is a fantastic way to achieve all three. It exposes you to new people, opportunities, and ideas that can help you grow personally and professionally while giving back to the community.

In this talk, attendees will learn practical advice and actionable tips to volunteer effectively, regardless of experience level. You'll discover where to find volunteering opportunities, what to expect, common pitfalls to avoid, and tips for successful participation. Additionally, you'll learn how to make the most of your time while gaining valuable skills and connections.

Explore how to find the right volunteering match for you and provide guidance on evaluating organizations, roles, and time commitments to avoid becoming overwhelmed. By volunteering, you'll gain new skills, make valuable connections, and positively impact the community.

After attending this talk, you'll have the knowledge and confidence to answer the next call for volunteers. Join us to learn how to volunteer effectively and positively impact your community.

Vulnerability Cognition: Adding Psychology to VulnMgmt Programs

Nikki Robinson - Security Architect, IBM

Vulnerability Management continues to be more and more complex, especially with large sprawling API's, containers and serverless deployments, and introducing a CI/CD pipeline. With all of these factors, it is increasingly important to understand psychological concepts behind VulnMgmt programs. Without understanding mental workloads, cognition, and perception, it will continue to be a struggle to keep up on vulnerabilities. With the numerous vulnerability scoring metrics, increasing severity and exploitability, blue teams must consistently learn about new exploits and what that means to their environments. This session will cover what "Vulnerability Cognition" is, how it affects VulnMgmt programs, and how Blue Teams can use these skills to increase awareness and effectiveness in their VulnMgmt programs.

Vulnerability Prioritization: Addressing The Great Debate

John Behen - Vulnerability Management Specialist, Fortellar

In recent years, there has been a push in the Vulnerability Management space to focus on risk reduction, rather than pure remediation. Part of this push has been recognizing the need to prioritize which vulnerabilities should be remediated, and in what order. This has given rise to a great debate on how to best handle prioritization. At the core of the debate is how we calculate and address the risk that vulnerabilities present.

Here, we will dive into the debate, understand the underlying motivations, discuss different prioritization methods, identify the pitfalls that should be avoided, and identify effective reporting strategies throughout the organization.

Why not all metrics are created equal

Pedro Jimenez-Hernandez aka Spapjh

As blue team professionals, we often hear about the importance of metrics and how they can help measure the effectiveness of our efforts and help create more mature security operations. However, it is important to remember that not all metrics are created equal, and some, if not most of the widely shared ones, can even be harmful to security teams if used incorrectly and help spread burnout at high rates. This is why I feel we all need to take a step back and carefully consider the metrics that we use to evaluate the performance of our security teams.

In this talk, I will go over metrics that provide great insight into a team's performance or maturity levels, while also not promoting bad habits or spreading burnout on blue teams. I will use the great insight Gitlab's cybersecurity team (no affiliation) shares via their public performance indicators as a base, and provide more ideas on sustainable and helpful metrics to use in this our industry.

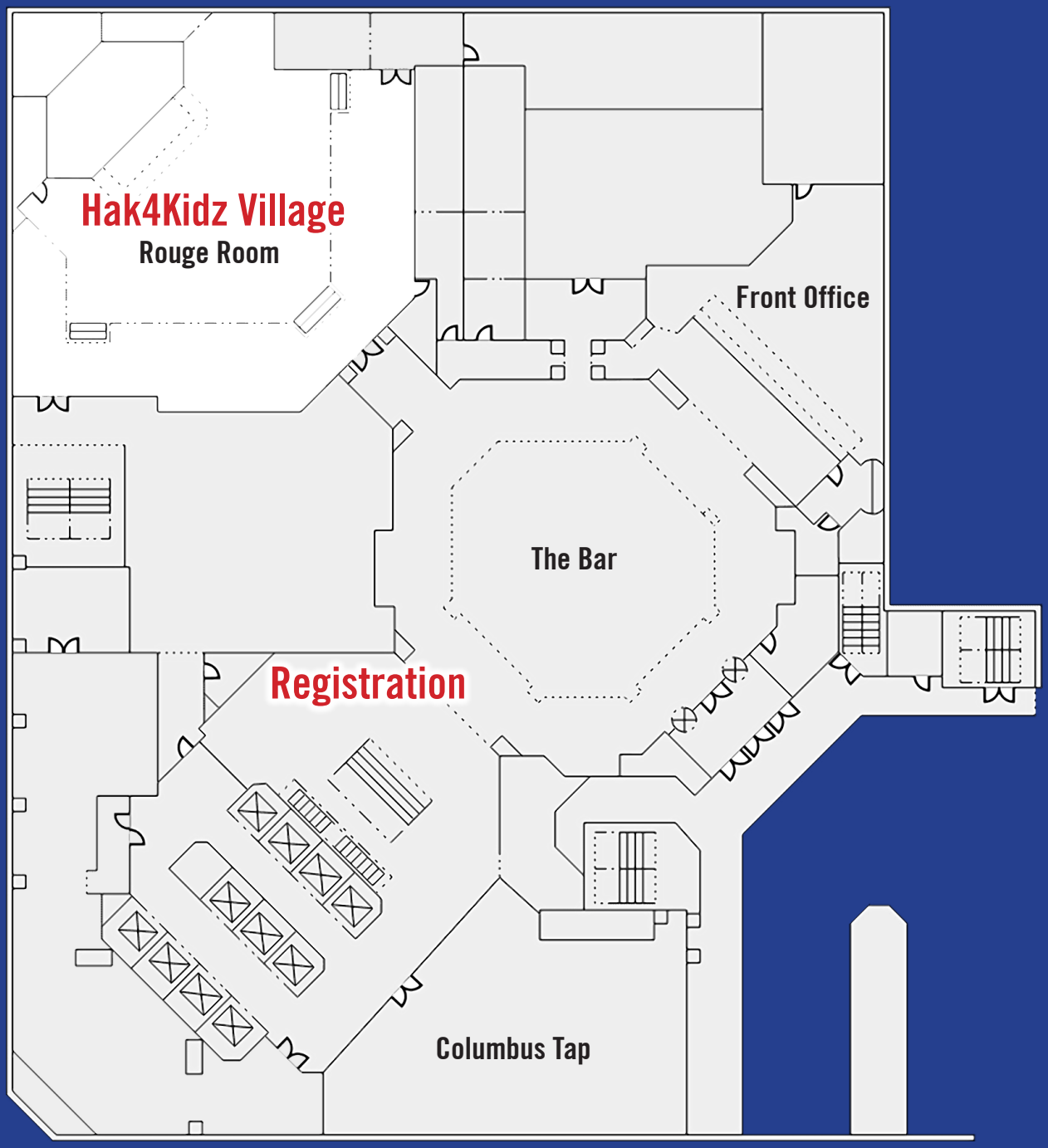
You have a SIEM, Now What?

Chris Maulding - Lead Security Engineer, Entegral

This talk will cover what to do once you have a SIEM approved by management. How do you configure it? How do you tune from it? During the talk we will touch on what is needed to deploy the SIEM, along with where the logs should come from. We will also touch on if there are compliance and regulatory requirements for retention. We will talk about how to ingest and tune the logs for your specific use case because there is no cookie cutter way to deploy a SIEM. We will touch on where the logs should come from what devices that you should obtain information from. We will also touch on what Open source tools that you can use and how they can integrate with cloud environments which organizations are moving. We will also touch on the topic of NIDS, HIDS and Threat Intel in the context of using them with a SIEM.

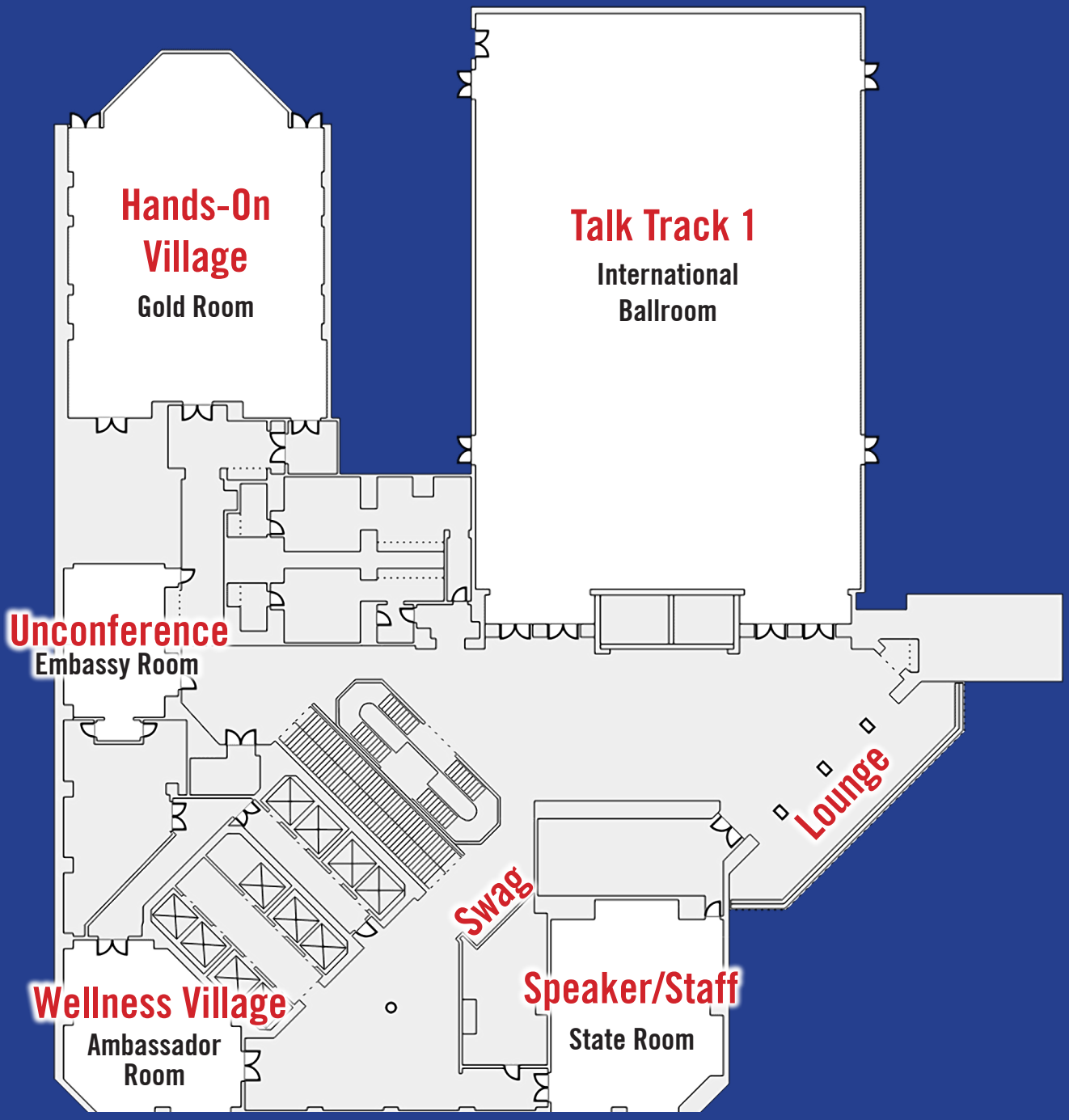
Venue

Level ONE



Venue

Level TWO



Venue

Level THREE

Partners

MY BLOCK MY HOOD MY CITY™

To inspire youth, empower communities, and build a better world one block at a time.

ENCOURAGE: We believe in providing opportunities for others to step outside their comfort zone and explore new communities, cultures, and cuisines in an effort to gain a greater understanding of the world.

EXPERIENCE: We believe in encouraging others to fully immerse themselves in new experiences, continuously soaking up new knowledge and expanding their network.

EVOLVE: We believe that each and every one of us needs to take responsibility for our communities; it is only through our efforts of service, empathy, and collaboration will we see our communities truly evolve.

www.formyblock.com

women in CYBERSECURITY WiCyS

Our Mission is to help build a strong gender-diverse cybersecurity workforce by facilitating recruitment, retention and advancement for women in the field.

At WiCyS, a global community of women, allies and advocates, we are dedicated to bringing talented women together to celebrate and foster their passion and drive for cybersecurity. We unite local communities of aspiring and thriving women cybersecurity professionals across the world to collaborate, share their knowledge, network and mentor. We create opportunities through professional development programs, conferences, career fairs, and more.

www.wicys.org

year up®

Year Up is committed to ensuring equitable access to economic opportunity, education, and justice for all young adults—no matter their background, income, or zip code.

Employers face a growing need for talent while millions are left disconnected from the economic mainstream. These inequities only further perpetuate the Opportunity Divide that exists in our country—a divide that Year Up is determined and positioned to close.

In addition to driving impact through direct service and strategic partnerships with employers, talent providers, and policymakers, Year Up is committed to addressing the root causes of the Opportunity Divide in this country and creating pathways to opportunity at broad scale. Helping to power the opportunity movement and make this work possible are two essential partnerships with Grads of Life and YUPRO.

www.yearup.org

Capture The Flag (CTF)

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!

Whether you have never played a CTF before, or have been completing challenges for years, we want you to play.

CTF Room Hours:
Saturday, August 26th: 10:30am to 5:00pm
Sunday, August 27th: 10:00am to 1:00pm

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, August 25th, at 6:00pm CDT.

The rest of the challenges and the competition will begin Saturday, August 26th, at 10:30am CDT until Sunday, August 27th, at 1:00pm 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

btcon.link/CTF

Villages

Career Village

Saturday from 10:30am to 6:00pm CDT.
Sunday from 10:00am to 12:00pm CDT.

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.

Wellness Village

Saturday from 10:30am to 6:00pm CDT.
Sunday from 10:00am to 3:00pm CDT.

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

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

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

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

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

Lightning Talks on Saturday from 12pm to 2pm, sign up on site!

Come share your thoughts in presentation or discussion group format. We're looking for topics related to your experience in anything related to mental health and wellness.

CTF Room

Saturday from 10:30am to 5:00pm CDT.
Sunday from 10:00am to 1:00pm CDT.

A space dedicated to all things Capture the Flag [CTF]. The Last Minute CTF admins will be available, during competition hours, to assist as appropriate. Some challenges may require a physical presence to obtain flags, this would be a good place to start. Devices will not be provided; you will need to source your own. And no, this is not a flag.

To see all information and enter the CTF, go to ***https://blueteamcon.com/2023/ctf/***

Quiet Room

The quiet room is available for all attendees if they need a location to nurse, take medication, or simply need some private space in the conference area. ***Please see a member of safety staff for more details when in need.***

Villages

HAK4KIDZ

Saturday 8:30am to 4:00pm CDT

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/.

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!

LOUNGE

SPONSORED BY <hunter_strategy>

The Lounge is setup to promote networking, allow for speakers to continue questions and answers after their talks, and to provide a relaxing atmosphere for attendees. Comfortable furniture is provided to ensure attendees can take a break from the remainder of the conference to plug in and recharge if needed.

Hunter Strategy will be providing the following quick talks presented by AJ King, CISO of Hunter Strategy, in this village on both Saturday and Sunday.

12:30pm to 12:45pm CDT: Fractal SOC & Why It Works
2:30pm to 2:45pm CDT: Third-Party Vendor Risk Management Simplified

Hands-On Village

Saturday from 10:30am to 6:00pm CDT.
Sunday from 10:00am to 3:00pm CDT.

The Hands-On Village is a location where labs and interactive activities will take place. The goal of this village is to allow attendees to get hands-on experience with numerous technologies, processes, or useful activities.

Vulcan Cyber: Gain hands-on experience prioritizing vulnerability risk by interacting with Vulcan Cyber researchers from the Voyager18 team. Learn best practices for contextualizing and mitigating vulnerability risk. Get hands-on to community tools developed by Vulcan Cyber, including VulnRX, the largest, curated library of vulnerability risk and threat intelligence, and MITRE Mapper, a service that maps prioritized CVEs to relevant remediation tactics and techniques from MITRE ATT&CK.

Trimarc: Trimarc is hosting Identity Security Village. This hands-on experience for all attendees consists of 2 domains with various common misconfigurations. Conference attendees have the opportunity to learn how to defend their networks by emulating an attacker: attempting to hack their way into a Domain Controller as either a Malicious Insider (using compromised window creds on a window 10 machine), or as a red teamer/penetration tester with a Kali machine on the same network. There are several layers of complexity in this environment extending its attack surface in ways that are very common and realistic including, certificate services, VMware environments, Azure Active Directory Sync, etc.

Escape Room: An Escape Room with a twist. Come see to find out!

Book-Swap: This year, we're introducing the First Annual Blue Team Con Book Swap-O-Rama!

Here's how it works:

- ✓ *We'll be accepting books published within the past 7 years as long as they're still relevant to the security industry.*
- ✓ *We'll also accept security-adjacent books, coding books, and textbooks as long as they're applicable to modern cloud environments. (We know you love your Perl and COBOL books, so we encourage you to hang on to those!)*
- ✓ *Drop off a book or two to swap or donate at the Book Swap table in the Hands-On-Village on Saturday between 10am and 2pm and receive a Blue Star ticket. Swing by the booth between 2pm on Saturday and noon on Sunday to "shop" for another book with your ticket.*
- ✓ *If you are not a student, we ask that you hold off your shopping excursion until after 3pm Saturday so that students will have first crack to swap their books, then the booth will open for all.*
- ✓ *After noon on Sunday, we will not take any new donations and all 'shopping' will be free—no ticket required.*

We're really excited about the opportunity to share some knowledge, swap some books, and save the environment a little bit, too. Any books not claimed or swapped by Sunday at before closing ceremonies will be distributed or donated by Blue Team Con.

We're looking forward to seeing you in a few weeks, so check your bookshelves and toss a book in your backpack to swap!

Thanks to Bat recommending we bring this event to Blue Team Con!

2023 ULTIMATE + TRAINING SPONSOR

Sponsors

PLATINUM SPONSOR

Sponsors

BLUE TEAM CON 2023
FOUNDING SPONSOR

onShore SECURITY

GOLD SPONSORS

LIMA CHARLIE

gravwell

Quest

AIRLOCK DIGITAL

TALK TRACK 1 SPONSORED BY VULCAN.

SILVER SPONSORS

SUBLIME

datatheorem

elastic

Security Onion SOLUTIONS

RAPID7

OCC THE FOUNDATION FOR SECURE MARKETS

StoneX

QUADRANT INFORMATION SECURITY

BRONZE SPONSORS

Focivity

no starch press

impart

PDA PRIVATE DIRECTORS ASSOCIATION® Creating Value Through Board Excellence

TECHNOLOGY SEMINAR SERIES

Sponsored by NineStar Connect.

MANNING

Venture in Security

BADGE SPONSOR

Material

Foodstuffs

Coffee Fix

Dunkin
233 Michigan Ave

Stan's Donuts & Coffee
181 Michigan Ave

Starbucks
300 E Randolph St

Starbucks
200 N Michigan Ave

Quick Bites

Chipotle
316 N Michigan Ave

Burrito Beach
233 N Michigan Ave

Potbelly Sandwich Shop
190 N State Street

Roti(Mediterranean)
80 E Lake St

Nandos Peri-Peri
117 E Lake St

Wildberry Pancakes & Cafe
130 E Randolph St

McDonalds
233 N Michigan

5 Guys Burgers & Fries
180 N Michigan Ave

Burger King
151 E. Randolph St

Subway
333 E Benton Pl #107

Taco Fresco
151 N Michigan Ave Ste C17

Chick-fil-A
177 N State St Suite 1A

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.

BLUE TEAM CON 2023

Thank You

For Attending Blue Team Con 2023!


BLUE TEAM
CON