27-28 August 2022
Fairmont Chicago

@BlueTeamCon

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 second iteration of Blue Team Con.

The goal of Blue Team Con is to have talks that are almost exclusively focused on sharing information amongst defenders and protectors of organizations. This can span from SOC Analysts through CISOs and across the aisle to auditors and compliance personnel and application developers focusing on security. There are many professionals hard at work struggling to keep up with the vast amount of information in the cybersecurity space. There are also individuals working in technology who don't realize they're a part of our community. They're the local high school Information Technology staff or the small business technology guru in a rural town that helps out local small businesses install antivirus, update their machines, and remove malware. Our conference audience includes students, professionals, executives, and business folks from all over the world.

Our goal is to help organize cybersecurity information sharing in a fun and collaborative way by offering a platform for those that have figured it out to share their knowledge. Just as doctors don't know everything on their own, they complement their own knowledge by a network of specialists that they can quickly poll for information and insight. We work to cultivate a community atmosphere where you can build that personal network of specialists.

Blue Team Con is a choose-your-own adventure. If you want to stay and only see talks and leave, we hope you learn new information. If you want to make new friends by chilling in lobbycon, we hope you grow your personal network of specialists. If you want to do it all and stay up all night, please drink water and have a nap at least. In the end, it's up to you. Either way, we welcome you into our community. Thank you for being here and for what you do.

Welcome to Blue Team Con!

Frank McGovern
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

DANNY
Akacki

@dakacki

DEE
Muran-de Assereto

@DaemonObserver

GARY
Tinnin

@GWi1s0n

JAMES
Arndt

@jcarndt

JULES
Okafor

@julsmgmt

STEL
Valavanis

@StelValvanis

CARL
Hertz

@cillic

ERICH
Nieskes

@ErichNieskes

KATRINA
Roberts

@magynta

RICARDO
Lafosse

@cyclingciso

BRAD
Schaufenbuel

@bschaufe

AMBER
Welch

@MsAmberWelch

ELLEN
McCullough

BECKY
Selzer

@BeckySecurity

ANONYMOUS

Schedule

All times are in CDT.

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

Childcare Village: Saturday from 7:30am to 7:30pm. Sunday from 9:00am to 5:30pm

CTF Room: Saturday at 10:30am to Sunday at 1:00pm (Yes, all night)

Note: CTF Room Admin Availability Hours are* Saturday from 10:30am to 5:00pm and Sunday from 10:00am to 1:00pm

Hak4Kidz Village: Saturday from 10:00am to 5:00pm

Hand-On Village: Saturday from 10:30am to 6:00pm CDT. Sunday from 10:00am to 3:00pm CDT.

Unconference: Saturday at 11:00am to Sunday at 3:00pm (Yes, all night)

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

Friday, August 27th

Registration: 6:00pm to 9:00pm

Saturday, August 28th

Registration: 7:00am to 3:00pm Swag Hours: 11:00am to 3:00pm

Saturday

Talk Track 1 - 50 Minutes
International Ballroom

9:00 AM

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

10:00 AM

9:35am to 10:30am
Keynote: "The Best Offense is Defense: How Blue Teamers are at the heart of the security movement" with Tazin Khan

11:00 AM

10:45am to 11:35am
"Satisfying compliance requirements with passwordless credentials" with Ehud Itshaki

12:00 PM

12:30pm to 1:20pm
"Hacking (and Defending!) APIs" with Robert Wagner

Talk Track 2 - 30 Minutes
Gold Room

10:40am to 11:10am
"Preparing your IT SOC for OT Network Security Monitoring" with Wesley Lee

11:20am to 11:50am
"Going Atomic: The Strengths and Weaknesses of a Technique-centric Purple Teaming Approach" with Alfie Champion

Saturday

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 30 Minutes
Gold Room

12:00 PM

1:00 PM

12:50pm to 1:20pm
"A VEXing Question: Am I Affected or Not?" with Justin Murphy & Dr. Allan Friedman

1:30pm to 2:20pm
"Improving the security posture of MacOS and Linux with Azure AD" with Mark Morowcynski

1:30pm to 2:00pm
"Blue Team Social Impact: How to volunteer your cyberdefense skills without getting burned out" with Tom Costello

2:00 PM

2:10pm to 2:40pm
"Hunting down rogue Managed Identities" with Ram Pliskin

2:30pm to 3:20pm
"How to Win Over Executives and Influence the Board" with Alyssa Miller

3:00 PM

3:30pm to 4:00pm
"Formulating An Intelligence-Driven Threat Hunting Methodology" with Joe Slowik

3:40pm to 4:30pm
"Building Better Security Metrics" with Jake Williams

4:00 PM

4:10pm to 4:40pm
"Hey! Your database got owned" with Sarit Yerushalmi

4:40pm to 5:30pm
"Everyone Can Play! Building CTFs To Teach Non-Security Folks" with Joe Kuemerle

4:50pm to 5:20pm
"You, Only Better, or: Lessons in Transformational Leadership for Techies in the Workforce" with Carl Hertz

5:00 PM

5:30pm to 6:00pm
"Say Hi to the New Guy: How Diverse Backgrounds Can Mature Your Security Program" with Ross Flynn

5:40pm to 6:30pm
"Life beyond the SIEM - Take control of your SOC with Jupyter" with Pete Bryan & Ian Hellen

6:00 PM

Saturday

Talk Track 1 - 50 Minutes
International Ballroom

Talk Track 2 - 30 Minutes
Gold Room

6:00 PM

6:10pm to 6:30pm
"SaaSy detection: purple teaming Software-as-a-Service platforms"
with Nick Jones & Chris Philipov

7:00 PM

8:00pm to 10:00pm
Gameshow(s) (Gold Room)

8:00 PM

8:30pm to 10:30pm
3rd Floor Foyer
PianoBar Con with Gary Rimar
Laidback piano music listening that will transition into an optional sing-along.

9:00 PM

9:00pm to 1:00am
International Ballroom

NETWORKING PARTY AND EVENT

DJ Cillic and
Benjamin Barnes Magic

Open Bar and Food

Sponsored by:

milton security

12:00 AM

1:00 AM

Sunday

Sunday, August 29th

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

Talk Track 1 - 50 Minutes
International Ballroom

10:00 AM

10:00am to 10:50am
"Protecting Application and Service Principal Permissions in Azure AD" with Eric Hall

11:00 AM

11:00am to 11:50am
"Becoming the Threat, The Making of A World Class Security Team" with Aaron Rosenmund

12:00 PM

1:00 PM

1:00pm to 1:50pm
"Holistic AWS Cloud Security Design for Organizations" with Cassandra Young (muteki)

2:00 PM

2:00pm to 2:50pm
"The Defender's Guide to Budgetless Endpoint Hardening" with Matt Coons

3:00 PM

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

4:00 PM

Talk Track 2 - 30 Minutes
Gold Room

10:00am to 10:30am
"Improving Alert Recall: miss fewer attacks through customizable ML anomalies" with Karishma Dixit & Ed Gardner

10:40am to 11:10am
"From Exceptionally Awful to Pretty Good: A Guide for New Security Leaders" with K R Bard

11:20am to 11:50am
"Breaking Boundaries, Securing Perimeters: A pragmatic approach to Attack Surface Management" with Katie Inns

1:00pm to 1:30pm
"Easy Defender Playbooks to Make Ransomware Criminals Cry" with Drew Hjelm

1:40pm to 2:10pm
"Why I Keep Building My Security On Open Source Year After Year" with Joe Gresham

2:20pm to 2:50pm
"From the Ground Up: Lessons Learned from Starting a Vulnerability Management Team" with Bryan Garcia

KEYNOTE SPEAKER

Tazin Khan

@techwithtaz

www.tazinkhannorelius.com

www.cybercollective.org

FOUNDER AND CEO
OF CYBER COLLECTIVE

THE BEST OFFENSE IS DEFENSE:

How Blue Teamers are at the heart of the security movement

In order to make change and inspire behavior, we must build movements. And whether we like to believe it or not, what we're doing in the security industry is building micro movements to influence a better world. The work of a Blue Teamer is very similar to that of someone looking to motivate and inspire change. As a Blue Teamer you must analyze existing systems, ensure security across sectors, conduct forensic investigations and most importantly - communicate to stakeholders on why they should not only care but fund and support the work that the Blue Team does.

This talk will cover:

- ✓ What it takes to inspire change and build movements
- ✓ How Blue Teamers sit at the heart of the cybersecurity industry
- ✓ How to leverage radical candor, compassion and communication skills to get buy in from key stakeholders on defense strategy

About Tazin

As a cybersecurity specialist of 10+ years with a focus on program compliance, third party risk management, and product mapping for Fortune 500 companies, she has an acute understanding of transforming problems into product solutions and translating product benefits into the customer's environment. This skill-set, paired with firsthand experiences of poverty, racial bias, gaslighting, and the all-too-common formalities that immigrant-American women in tech face, is what inspired her to educate people on the impact of their data and its effect on their real lives.

In 2019, Tazin mobilized her community and founded Cyber Collective in an effort to increase awareness of the importance of digital protection. Today, Cyber Collective is recognized by Forbes as "the only women of color owned and operated community-centered research organization that focuses on data ethics, privacy, and cybersecurity research." Tazin and her team at Cyber Collective are dedicated to creating approachable and interactive content, workshops, and resource guides for people to educate themselves and learn freely about these topics.

Talk Track One
50 MINUTES

Becoming the Threat, The Making of A World Class Security Team

Aaron Rosenmund

Are you cleverer than a Malware author? Do you feel like you are just waiting on someone or groups of someone's to make their next move and hoping that your defenses can manage? Of course, they don't always do they? And that is because, waiting for the threat to happen, means you are forever behind the power curve. I have created malware that can consistently morph to blow past defenses, but in this case, it is tamed, it doesn't actually cause harm, and stays within your control. Why would I do that? To test the defenses, I wanted to become the malware author so the threat I am working to beat is me! And I want to teach you to do the same. I will walk you through simulated ransomware with various techniques that can be launched in a test environment to test your defenses. Then I am going to show you where common security products fail, where humans fail, and where you can iterate to teach yourself to be different.

Building Better Security Metrics

Jake Williams

Let's face it: most of us don't like gathering and reporting metrics. But the boss says "that which isn't measured isn't managed." Of course there's the problem of users gaming metrics to paint unrealistic pictures to stakeholders. Good metrics should serve as a heuristic for stakeholders to understand a situation at a high level without needing to understand all the nuance of how the sausage is made. In other words, metrics should tell a story. Since you'll be generating security metrics anyway, shouldn't they tell the right story?

Beyond the obvious justification of "management says you have to," as an aspiring security leader you should be self-motivated to create and deliver better metrics. If there's one thing leadership abhors, it's uncertainty. Better metrics don't eliminate uncertainty, but they do promote better understanding, leading to better evaluation of risk.

In this presentation, you'll learn the principles of generating compelling metrics. We'll then cover examples of easy-to-gather metrics across a range of security disciplines, including SOC, cyber threat intelligence, threat hunting, and incident response. Come learn how to level up your metrics game in this session!

Everyone Can Play! Building CTFs To Teach Non-Security Folks

Joe Kuemerle

Most security practitioners are aware of the learning and fun that comes from participating in Capture the Flag competitions. Racing against other teams, solving brain-twisting challenges and seeing new ways to compromise systems teaches and entertains.

CTFs are also a great tool to give non-security folks a hands-on understanding of how security vulnerabilities enable criminal activities, reduce user privacy and degrade system reliability.

In this session you will learn to build interesting, educational and easy to use Capture the Flag events targeted at developers and other technical, non-security, users. We will cover specific considerations for each audience you target, how to create interesting (yet solvable) challenges, and how to make the overall experience friction free for the participants.

You will also learn tools and techniques to create easily repeatable, consistent events with minimal work. We will cover collaborative development, external system integration techniques, tooling and a fully automated deployment pipeline to make spinning up a new CTF as easy as pushing a button.

Hacking (and Defending!) APIs

Robert Wagner

APIs are a leading attack vector that often get pushed into production without proper security testing. In this presentation we will provide an overview of the OWASP API Security Top 10 vulnerabilities from an adversarial perspective. Then we will discuss how vulnerability management programs often use the wrong tools to test APIs and how to build an effective API security stack.

Holistic AWS Cloud Security Design for Organizations

Cassandra Young

Ditch the kale smoothie, it's time to go big picture. Your organization is moving to AWS, and you're in a panic. Which of the 42 billion AWS service offerings do you really need? How do you manage user and service accounts? What about those 7 different rogue AWS accounts you just found out about? We'll talk about securing, organizing and standardizing your AWS environment(s), managing authentication, protecting your applications, and we'll walk through a few key guardrails you can plan today. Throughout the presentation, we'll talk about balancing security with usability, how your existing architecture can work for you and against you, and how to identify and protect your attack surface in (and even out of) the cloud.

How to Win Over Executives and Influence the Board

Alyssa Miller

Stop me if you've heard these before (or maybe you've said them yourself), "Management just doesn't listen", "The executives don't care", "The board just doesn't understand". These exasperations can be very common for blue teamers. We know what needs to be done but we just can't seem to get the support of our organizational leadership. Even when CISOs or high-level security leaders break through and get time with the board, it's not uncommon to see them with their heads down looking at their phones. Well, this session is your master class in turning that around and making these conversations work for you.

Come learn from an experienced cyber security executive about what works and what doesn't when you're engaging with your leadership teams. Learn actual techniques you can employ tomorrow for effectively planning and delivering a presentation, recovering engagement from an audience that's tuned out, and overcoming some the skepticism and animosity that can derail your efforts. You'll see re-world examples from presentations that succeeded as well as from those that failed. Whether you're in an individual technical role or in the executive suite, this is a chance to up your game and start gaining the support you need.

Improving the security posture of MacOS and Linux with Azure AD

Mark Morowczynski

The majority of organizations have Windows, MacOS and Linux in their environment. Typically many of the security controls that are applied to Windows are not applied to MacOS or Linux, due to the size of the footprint and the difficulty of implementation. This can lead to holes in an organization's overall security posture as well as a poor end user experience.

Recently, Azure AD has released some new functionality to help improve the overall environment security posture for MacOS and Linux, both servers and clients. We'll discuss how these pieces work deep down and some best practices on deploying them.

In this session you'll learn how to reduce authentication prompts, further lockdown your Conditional Access policies, and leverage modern credentials like Passwordless on these platforms.

Talk Track One
50 MINUTES

Life beyond the SIEM - Take control of your SOC with Jupyter

Pete Bryan, Ian Hellen

The SIEM is the center-point for most SOC activity: providing tools for handling threat detection, incident investigation, threat hunting, and more. Even the best SIEM though, is only as capable as the features it includes. Analysts often have to develop processes and scripts to fit alongside it. What if it didn't need to be this way? What if there was a tech stack that allowed you to take control?

Jupyter is the solution that allows analysts to investigate threats, conduct hunts, and manage processes in a flexible, agile manner. Use visualizations, analysis techniques, data sources and workflows that your SIEM doesn't possess.

In this talk, we will look at the Jupyter ecosystem and how it can empower SOC analysts (from tier 1 to specialized hunters) in a wide range of tasks: from creating custom visualizations to automating triage and enrichment tasks.

We'll cover some Jupyter basics then dive deeper on how to use standard Python libraries and techniques to customize your analysis flow. Then look at using MSTICPy (Python InfoSec library) and how its data, enrichment and visualization features can speed up your workflow with generate elegant, low-code notebooks.

We will also show how you can deploy notebooks in your organization in a consistent, secure and reliable manner using tools like Docker and Git.

Finally, we will demonstrate how to use Jupyter to automate investigation and hunting, to drive great efficiency and consistency benefits for the SOC.

Protecting Application and Service Principal Permissions in Azure AD

Eric Hall

Do you know what your service principals are doing? Service principals represent non-human accounts in Azure AD. They're a big improvement over the on-premises service account model, but the permissions they are granted can introduce new risks. In this talk we'll explain the threats to the permission consent model posed by app sprawl and malicious actors. We'll show you how to discover what apps are in your environment and how to understand the risk associated with those apps.

Key topics we'll cover include:

- Understanding the service principal and application directory objects
- Evaluating the impact and blast radius of permissions
- Delegated (on behalf of a user) and application (without a user) permissions
- Identifying threats to your applications and service principals
- Managing requests from app developers

Based on our experience implementing an application permission security assessment model across Microsoft's internal IT environment, we'll share lessons learned, gotchas, and product features that can help you manage the security of service principals and applications in your Azure AD tenant.

Satisfying compliance requirements with passwordless credentials

Ehud Itshaki

Do you want to know how FIDO2 measures up against FedRamp High? Does it satisfy NIST Authentication Assurance Level 2 or 3? Learn how to interpret the standards and regulations and how you can map the various common credentials in the ecosystem to them, also learn how you can show compliance to your auditor when you use new passwordless credentials like FIDO2 keys.

Recent cyber-attacks are driving governments and regulated industries around the world to improve their Cybersecurity and ensure that baseline security practices are in place. Requiring MFA is no longer enough, there is a need to make sure it is a phishing resistant MFA. In this session we'll explain NIST Special Publication 800-63-3 "Digital Identity Guidelines" pivotal role in shaping Identity regulation in US and around the world, we'll dive into the requirements for meeting the various Authentication Assurance Levels and explain why not all MFA methods are created equal.

The Defender's Guide to Budgetless Endpoint Hardening

Matt Coons

Hardening the endpoint is one of the first and most effective measures implemented by defenders to protect organizations against attackers. The EDR, XDR and antivirus space is full of vendor solutions to detect and prevent malware, but what can a budget conscious blue team do to block malware without spending a dime?

This talk will dive into cost free hardening tools and techniques that can be implemented to better protect endpoints from attack. Hardening techniques like leveraging Windows Firewall to block unwanted outbound network traffic, implementing Windows Attack Surface rules, disabling unneeded endpoint services and more will be discussed throughout the interactive session.

Session participants will leave with zero cost, actionable, and easy to implement endpoint hardening measures that can be implemented in various types of computing environments.

Talk Track Two
30 MINUTES

A VEXing Question: Am I Affected or Not?

Justin Murphy, Dr. Allan Friedman

With recent events like Log4Shell, more attention is being paid to software security and the underlying components used in developing software. SBOMs (Software Bill of Materials) are a great tool in uncovering vulnerabilities in software components, and aid software providers in becoming fully transparent about the components that comprise their software products. As SBOMs become more widespread, many security advisories released by organizations could contain "false positives," when the underlying component contains a vulnerability, but that vulnerability is not exploitable. A key idea at the intersection of security advisories and SBOM is the "Vulnerability Exploitability eXchange" (VEX). A VEX allows software providers to explicitly communicate that they are NOT affected by a vulnerability, and software users (e.g., network defenders, developers, and services providers) to reduce effort and resources spent in investigating non-exploitable vulnerabilities that do not affect a product. VEX provides a machine-readable approach to support automation to help software users understand, am I affected or not?

This talk will give a brief overview of the SBOM concept and review the challenge of understanding when a vulnerability actually affects a product. We'll discuss the implementation of VEX in current standards, highlight future directions, and conclude with a call for participants to get involved.

Blue Team Social Impact: How to volunteer your cyberdefense skills without getting burned out

Tom Costello

Want to give back to your community by volunteering your blue team skills, but don't want to turn into a small nonprofit's 24/7 unpaid on-call helpdesk? We'll explore ways you can maximize your happiness & social impact by taking your blue team talents into the volunteer space. You'll learn how to avoid re-inventing the wheel when it comes to blue team charity work, along with many lessons learned on avoiding volunteerism burnout due to a busy dayjob. When done properly, volunteering your technology skillset or helping to train/mentor others interested in your occupation can have a gigantic positive impact both to your community and your mental wellbeing! When done poorly, you might burn bridges and find yourself more stressed out than necessary due to a volunteer situation gone wrong. Don't do that to yourself; attend this talk and let's make the world a better place one blue team volunteer opportunity at a time!

Breaking Boundaries, Securing Perimeters: A pragmatic approach to Attack Surface Management

Katie Inns

Security teams can often become overwhelmed by large lists of vulnerabilities that affect their systems and have trouble knowing which to prioritise first when it comes to remediation. This can lead to ineffective vulnerability management processes that focus on addressing issues from a top-down approach and do not reflect real-world exploitation or the risk to the organisation. This becomes more problematic when organisations don't fully understand their attack surface and their systems that may be at risk.

This talk will discuss how organisations can adopt a more pragmatic approach to attack surface management, by understanding the assets at risk, how to prioritise remediation and how to adapt based on emerging threats.

Easy Defender Playbooks to Make Ransomware Criminals Cry

Drew Hjelm

The last few years of continuous assault by ransomware gangs against businesses and organizations have left a large mess in their wake. The onslaught makes it seem like the adage “the attackers only have to be right once” holds some truth, even if it is wildly inaccurate.

Let’s talk about what we can do as defenders to flip the script and give the bad guys a hard time. These are architecture patterns and tactics you should bake into your policies, procedures, and runbooks that would have stopped literally hundreds of ransomware attacks. And best of all, most are free and/or easy to implement.

Formulating An Intelligence-Driven Threat Hunting Methodology

Joe Slowik

Consultants and marketing departments refer to “threat hunting” as a desired position for network defenders. By adopting this mindset, defenders can take an active role pursuing intrusions. Yet precise methodologies for threat hunting are hard to come by, making the concept something amorphous. In this discussion, we will explore a methodology to standardize the threat hunting process, using an intelligence-driven, adversary-aware approach to drive investigation. This discussion will reveal a series of concrete steps or operational techniques that defenders can leverage to produce a measurable, repeatable, sustainable hunting process. To illustrate the concept, we will also look at several recent examples of malicious activity where an intelligence-driven hunting process allows defenders to defeat fundamental aspects of adversary tradecraft. Audiences will emerge with a roadmap for building a robust threat hunting program to improve the defensive posture of their organizations.

From Exceptionally Awful to Pretty Good: A Guide for New Security Leaders

K R Bard

Drawing on 25 years of experience, this narrative-driven presentation walks through proven strategies for all aspiring security leaders who may be wondering: how can I have fun and profit whilst hacking the typical systemic challenges that block better security outcomes? The four sections of this talk outline people-driven and culture-conscious methodologies that will enable you to do just that! First, you will learn how to choose the right leadership opportunity that aligns with your professional career goals and your amazing life purpose. Second, you will explore how to harness your “new role energy” to do two simultaneous jobs: making good on your highly visible “30/60/90 day plan” that aligns with the business of security; also an in-depth investigation into what is holding back the security program you just inherited. Third, you will discover how to rebuild your security program step-by-step, including a commitment to excellent security experiences, fostering healthy team culture, and partnering with others in your security ecosystem. And to round out your journey, you will uncover how to deal with inevitable entropy and change in a fast-paced industry through the power of reflection, storytelling, and gratitude.

Talk Track Two
30 MINUTES

From the Ground Up: Lessons Learned from Starting a Vulnerability Management Team

Bryan Garcia

As the Cybersecurity field continues to mature and vulnerability numbers increase, there is a growing need to form specialized teams to handle dedicated areas of Cybersecurity. From the Ground Up shares the lessons learned from the creation of a dedicated Vulnerability Management team, the successes and struggles the team faced, the impact and value the team would bring to the company, and what choices could be made to help others be more effective in their decision-making to create an efficient Vulnerability Management team.

Going Atomic: The Strengths and Weaknesses of a Technique-centric Purple Teaming Approach

Alfie Champion

Atomic purple teaming, i.e. testing individual permutations of offensive techniques outside of a scenario-based exercise, offers an approach that can maximise kill chain coverage and provides a means to benchmark a SOC's detective capability.

Initially, the methodology for atomic testing will be presented, alongside example results from a typical engagement. We'll evaluate the significant data set that such testing can produce - e.g. which test cases produce telemetry, which produce alerts, which were prevented - and consider its application in informing SOC strategy, demonstrating Return on Investment, and providing insight into general security posture.

This empirical, data-driven approach is invaluable in developing a bottom-up view of our defenses, i.e. understanding how our detection stack fares when faced with the tactics, techniques and procedures of legitimate actors, but it is not a one-stop shop for adversary emulation. As such, this talk will consider the limitations of such an approach, and how other supplementary collaborative testing can offer a more complete view of detective capability.

Hey! Your database got owned

Sarit Yerushalmi

A data breach is an organization's worst nightmare.

Your databases can be used as a pivot to infiltrate the organization or may be the target to exfiltrate sensitive data.

In this talk we will explore different exploitation techniques used by attackers to attack databases.

We will dive into practical real life examples captured by our honeypots around the world and present advanced detection approach to identify attacks such as: ransom and crypto mining campaigns, malware deployment, distributed brute-force attacks, evasion techniques and slow & low exfiltration.

Hunting down rogue Managed Identities

Ram Pliskin

Usage of Cloud managed-identities is on the rise in all cloud providers. But are they really as secure as we assume them to be?

Recently, more and more attacks have been leveraging legitimate usage of managed identities to advance the attack and pivot across multiple resources. Managed identities are the latest phase in the evolution of protecting secrets, but without being properly protected, they themselves can serve as double edged swords introducing new risks and vulnerabilities. Powered by OAuth 2.0, Cloud managed identities blur the distinction between Identity protection and Endpoint solutions leaving crucial terrain unclaimed.

OAuth 2.0 introduces an authorization layer and separates the role of the client from that of the resource owner. In this session I will dive into delegation flows and together we will understand how they are related to ghost managed identities which pop-up on a compromised network. Together, we will extract Cloud-unique aspects out of known attacks, isolating managed identities as overlooked soft spots.

We will wrap-up with several high-fidelity detections giving every blue-side attendee, practical tools to implement in their own environment.

Improving Alert Recall: miss fewer attacks through customizable ML anomalies

Karishma Dixit, Ed Gardner

In the ongoing game of cat and mouse between attackers and defenders, attackers continually find new ways to evade detection. Whilst high fidelity security detections tend to have high precision, they can sometimes have low recall, therefore some new attack techniques can go undetected. Anomalies on the other hand are much noisier but can capture attacks that would otherwise be missed. Anomalies don't necessarily indicate malicious behavior on their own. But when combined with other anomalies or alerts their cumulative effect is much stronger.

In this talk, we explore our approach at Microsoft Sentinel to provide the user with customizable anomaly rules. Our engineering methodology uses a PySpark backend to implement a variety of ML techniques including both supervised and unsupervised learning. We deep dive into the ML behind one of our customizable anomalies and then demonstrate the ease at which the rules can be configured by the user. Lastly, we demonstrate, via simulated attacks, how anomalies and alerts can be combined at various stages of the kill chain to produce high quality incidents.

Thus, we can see how customizable anomaly rules improve recall while reducing the noise of traditional anomalies via machine learning and customization.

Talk Track Two
30 MINUTES

Preparing your IT SOC for OT Network Security Monitoring

Wesley Lee

OT and IT convergence is here. One of the biggest push in OT/ICS is the implementation of better visibility and increased network security monitoring. No matter if you have a fully in-house or hybrid Security Operation Center augmented with Managed Security Services. If you don't have the funding or time to implement a separate OT Security Operations Center dedicated to monitoring your OT environment. This talk will discuss strategies, tactics, people, processes, and lessons learned in effectively integrating your OT NSM program into you IT SOC. This talk will lay out a flexible roadmap and walk you through the process of the before, during, and after steps that should be done in order to integrate your OT NSM program in your IT SOC, how to integrate, mature, response, and measure your OT NSM program within your IT SOC without losing the focus and critical aspect with better OT NSM monitoring within your organization.

SaaSy detection: purple teaming Software-as-a-Service platforms

Nick Jones, Chris Philipov

This talk will present an approach to developing attack detection capability across cloud-based Software as a Service (SaaS) solutions. This approach is drawn from real world experience across a wide variety of enterprise environments and focuses on the use of purple team methodologies to identify and execute likely attack paths, evaluate telemetry and build effective detections.

Historically cloud security research has focused on cloud infrastructure providers, but the use of SaaS solutions has increased dramatically, and become deeply ingrained in how organizations operate day-to-day. Microsoft 365, GitHub, and Slack are good examples of SaaS solutions used by the majority of organizations today. The fast-paced development of these new technologies has seen a divergent approach to security within the solutions themselves. Perhaps more notably, organizations' rapid adoption of these technologies has seen engineering efforts far outpace security development and understanding.

Over the past 18 months the presenters have been helping organizations understand what attacks against SaaS look like and building an approach for building and validating detection through emulation of these threats. The dynamic nature of SaaS solutions and the cloud environments they inhabit mean that building an effective long-term framework for keeping up with these changes is more important than the individual detections themselves.

Attendees will leave the talk with a clearer understanding of:

- What real-world SaaS attacks look like
- How SaaS detection differs from more conventional detection
- How to approach designing, implementing and evaluating their SaaS detection capability

Say Hi to the New Guy: How Diverse Backgrounds Can Mature Your Security Program

Ross Flynn

In a sea of candidates, why should you consider hiring a teacher as a SOC analyst? In what world would you hire a salesperson as a pen tester? As the need for more holistic security professionals grows, the Infosec field has a unique opportunity to address security concerns by leveraging the unprecedented number of converts from seemingly unrelated field.

The bad guys will always continue to develop and evolve their techniques, so strategic organizations are finding success pulling from more diverse backgrounds. Fresh thinking and function-specific experience can help these diverse defenders protect data and the basic human right to security and privacy.

Let's talk about the influx of new blood, strategic positioning, and how qualified professionals from other industries can leverage their experiences to benefit your security team.

Session attendees will leave with:

1. Advice on qualities to look for when searching for non-traditional team members – what can we give HR to help them help us find the right people?
2. Tips for supporting employees with non-traditional backgrounds in demonstrating their strengths
3. Real world examples of diverse backgrounds uniquely benefiting security programs

Why I Keep Building My Security On Open Source Year After Year

Joe Gresham

After 15 years of developing a network sensor, log analyzer, and SIEM, based primarily on open-source tools, the future still points to open source. Something is inherently different about open source that makes it more viable for security analysis. Too many analysis processes need to run narrowly and in parallel, or sometimes serial. These require rich interconnections and openness between each specialized tool. The open source community has provided these with thousands of developers working on the projects they are passionate about and fulfilling a function, narrowly, and extremely well. This is what's lacking in the closed source world where vendors keep out the competition in an attempt to provide a "complete security stack" which has ruined more than a few initially powerful open source tools.

In this talk the presenter recalls his 15-year journey to build and continuously improve his company's detection platform. His experience with integrating software tools like Bro/Zeek, Snort, and ELK, and with low-level performance tuning of multi-core CPUs and network interfaces provide insight into the powerful advantage of open source. Using the specific example of modifying open-source full packet capture systems to add indexing, Joe demonstrates how just having a decent API is not enough. Open source gives you the total flexibility needed to build a rich cybersecurity SOC platform. Besides, you can't afford to "test" the non-free stuff.

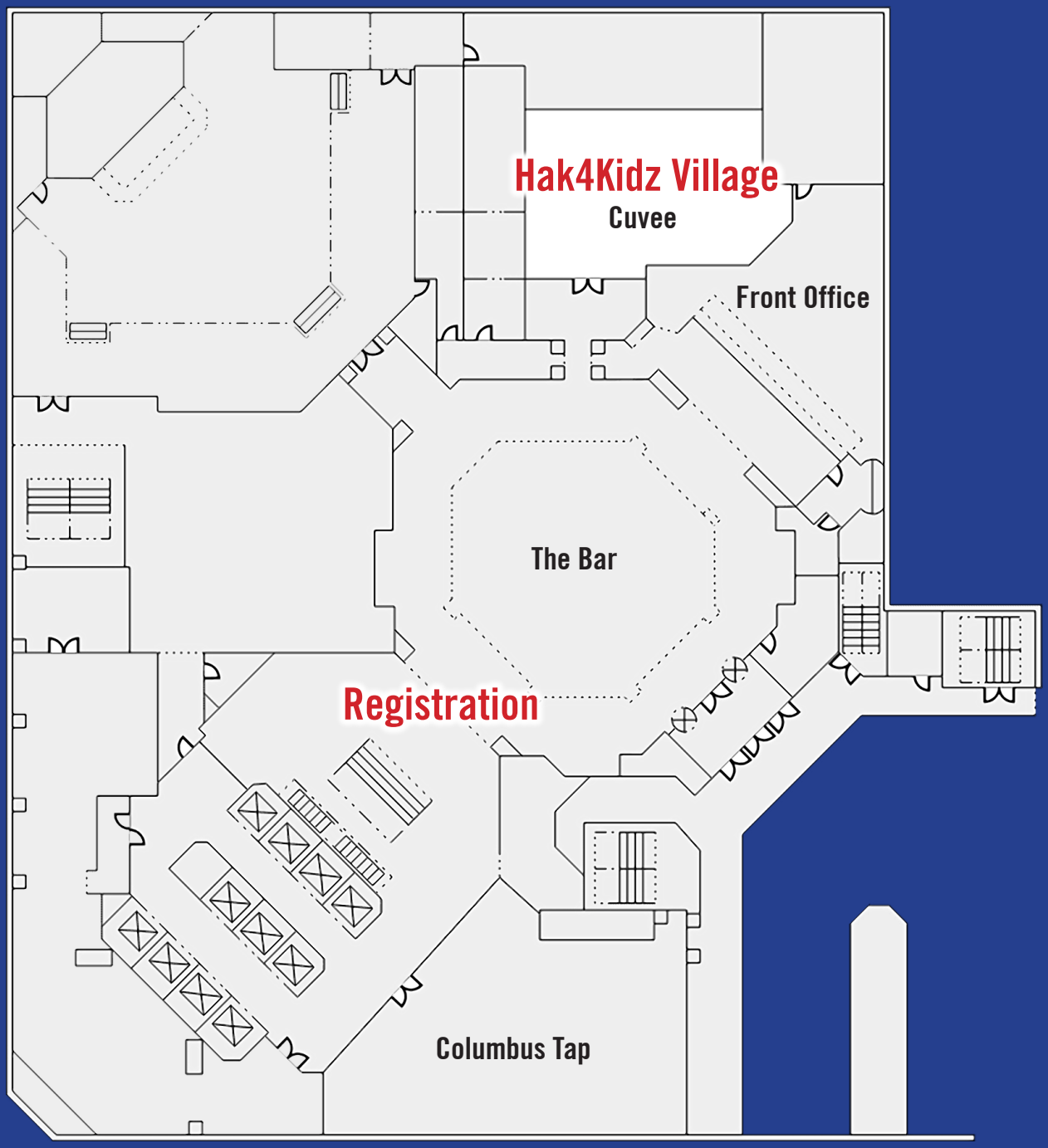
You, Only Better, or: Lessons in Transformational Leadership for Techies in the Workforce

Carl Hertz

tl;dr: Most techies have transactional business relationships with each other and their management in the workspace. I will present a list of skills and behaviors that will help people become transformational leaders as employees and managers.

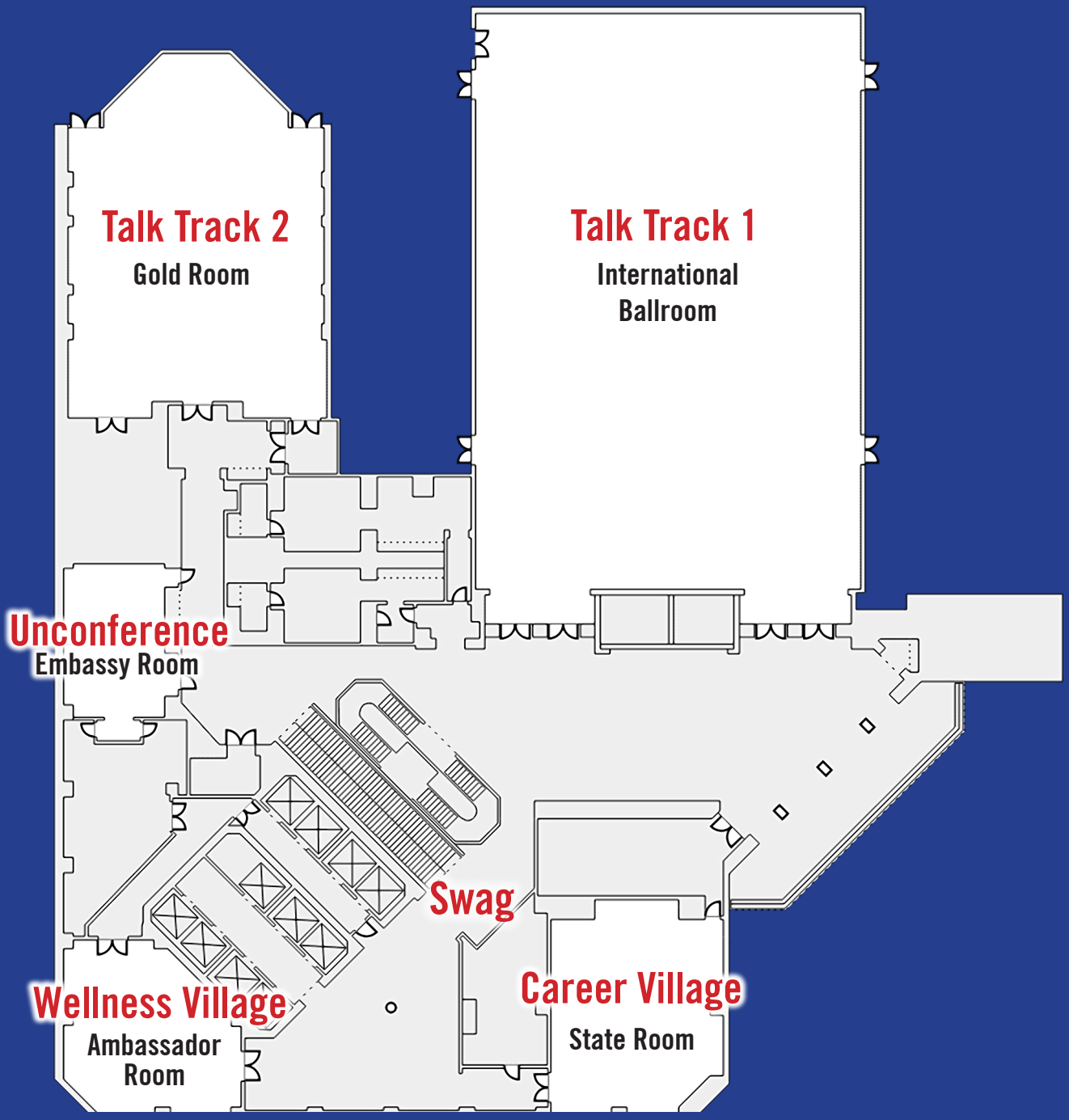
Venue

Level ONE



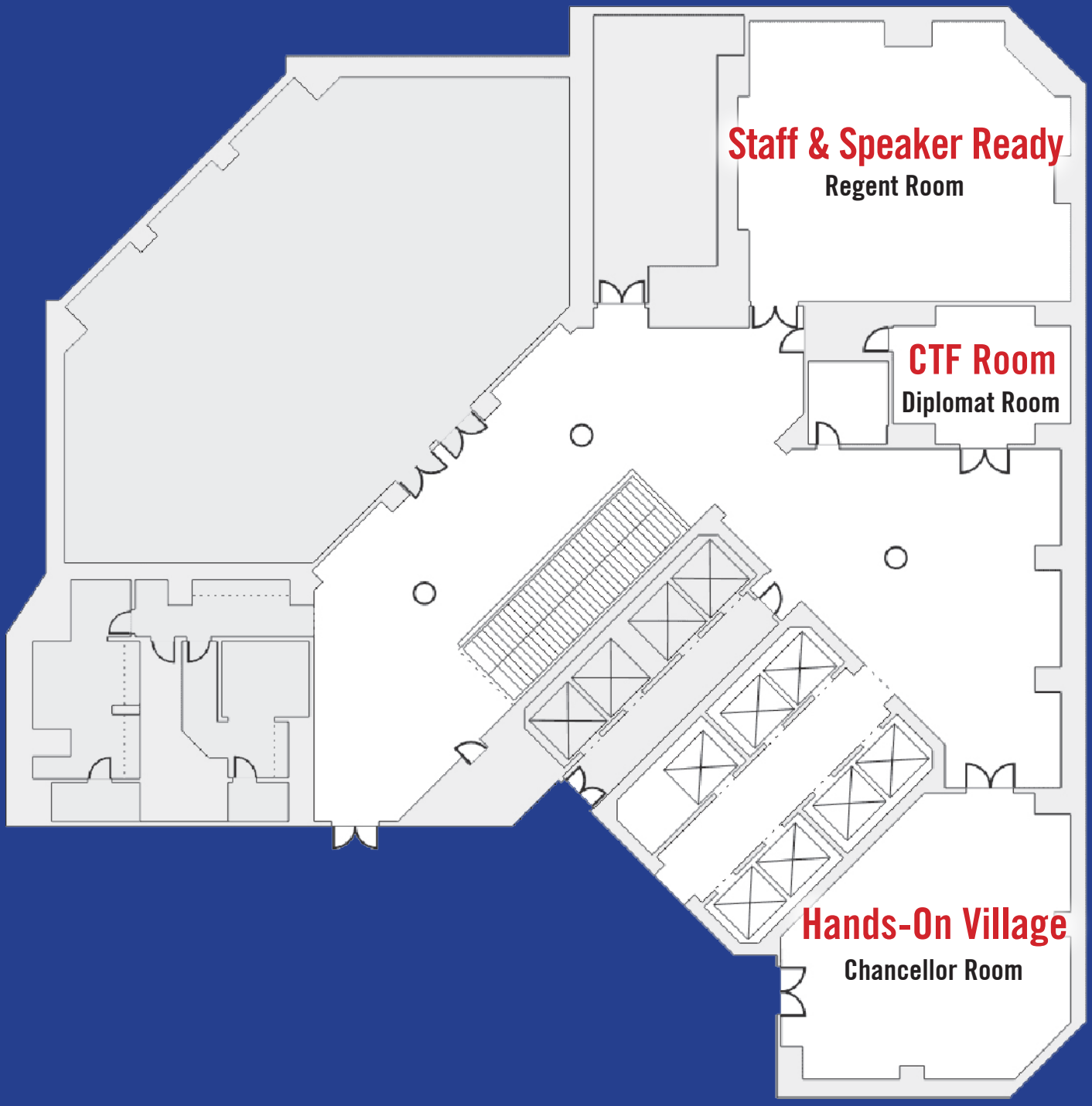
Venue

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

yearup®

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. We're looking to bring another beginner-friendly CTF competition. As we were happy to announce last time around, this was originally a very last minute thing. This time, not quite so late, but still pretty last minute. However we aim to provide 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.

Our goal is to create somewhat friendly introduction to CTF-style challenges and being very accessible to users of all skill levels. We have reworked and rebuilt how we want to start the competition in effort to help show newer CTF players a bit of what we have going on. To this end, the competition requires you to complete two introductory challenges that walk you through some important information and will hopefully help get you into the spirit of the competition. 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, as we did last year, is that the Last Minute CTF wants to see you document your work and provide write-ups for each of the challenges. This is totally not because we're doing this at the last minute and don't want to do it ourselves... However, 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 Hours:
Saturday, August 27th: 10:30am to 5:00pm
Sunday, August 28th: 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 26th, at 6:00pm CDT.

The rest of the challenges and the competition will begin Saturday, August 27th, at 10:30am CDT until Sunday, August 28th, at 1:00pm CDT.

Visit: blueteamcon.com/2022/ctf/

Villages

Career Village

Saturday from 10:30am to 12:00pm 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.

Childcare Village *Village Restricted to Children and Parents Only*

Saturday: 7:30am to 7:30pm CDT
Sunday: 9:00am to 5:30pm CDT

The Childcare Village is a free childcare offering to parents on a first come, first serve basis. Seats are limited. The Childcare Village is setup to help watch all children from the ages of 3 through 12 while the parents enjoy the conference or go network with peers.

The vendor College Nannies will be providing this service through Blue Team Con. College Nannies is a registered and insured company. All sitters go through a thorough vetting process including reference checks, a background check, and several in-person interviews. Many of their sitters have extensive experience with group settings, such as camp, daycare, and in the classroom.

NOTE: Any child that is capable to receive COVID-19 vaccination is required to have their full vaccination as per CDC guidelines.

"Last Minute" CTF Room

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

Note: CTF Room Admin Availability Hours are* Saturday from 10:30am to 5:00pm and Sunday from 10:00am to 1:00pm.
***These hours are subject to change.**

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/2022/ctf/***

Sponsored by:

GitHub Unconference

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

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 fish bowl about knitting - have at it! It's an Unconference!

The Unconference Village will have SOME structure to it, in that we will have different formats at different times.

Hands-On Village

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

Black Hills Information Security: BHIS will be playing Backdoors & Breaches, an Incident Response Card Game with conference attendees. Backdoors & Breaches contains 52 unique cards to help you conduct incident response tabletop exercises and learn attack tactics, tools, and methods. TRAIN YOUR TEAM OR YOUR STUDENTS… WHILE HAVING FUN! Feel free to read How to Play ahead of time.

CompTIA: CompTIA will have representatives from different internal groups (Community/ISAO, Tech Academy (CTCA), Certifications, etc.) to converse with attendees and show what our industry association can do around cybersecurity for you and your organization. We will also be running games of Jenga themed 'Cybersecurity is a Team Sport'.

Trimarc: Darryl Baker (@dfirdeferred) is proudly presenting Trimarc's all new Identity Security Village along with other members of the Trimarc team. We hope AD admins, security professionals, and all interested in AD security will walk away from the village with a deeper understanding of modern Tactics, Techniques, and Procedures used by attackers, as well modern defense techniques and configurations to combat these attacks.

HAK4KIDZ

Saturday: 10:00am to 5:00pm 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 bring the benefits of white hat hacking to the children and young adults at the conference. Hak4Kidz accomplishes 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 enables 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. **www.hak4kidz.com**

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

Sponsored by:

GitHub *Wellness Village*

Presented by:

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

YOGA
7:30-8:30 Sat
9-10 Sun

The Health and Wellness Village will be run 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 are 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. **www.mentalhealthhackers.org**

The following talks are taking place at this village:

Saturday, August 27th

12:00pm to 1:00pm CDT

You're Not Broken...Just Different: Don't Let Undiagnosed Neurodivergence Ruin Your Life

Warnings: Topic includes Substance Abuse, depression, anxiety, ADH

Chris Culling

Have you ever felt that there's something different as to how your brain works, but you can't quite put a finger on it? That you excel in some parts of life, but fall behind in others?The type of person drawn to InfoSec seems to include a lot of folks from the neurodivergent side of the tracks. Autism, ADHD, anxiety, depression, dyslexia, Tourette's, bipolar disorder, and OCD are some of the more common types of neurodivergence. However, many folks are unaware of their own neurodiversity and how to live with it. If left undiagnosed and untreated, it can cause untold harm to them, their families, and their careers.I was undiagnosed...and I fell into addictive behaviors and substance abuse to self-medicate away the pain of not knowing what was different about me. But I found help. And after finding the right medication, along with therapy, I can mostly function these days...and without the substance abuse.This short presentation will explain neurodiversity and show some of the issues that undiagnosed neurodivergents face and how they can be overcome...using my own life as a case study.

1:30pm to 2:30pm CDT
12-Step Programs - Not Just for Addicts

Gary Rimar

12-step programs such as Alcoholics Anonymous and Al-Anon have existed for many years. While participation in a 12-step program doesn't guarantee successful addiction management, many people that benefit from these programs and improve their life quality.

As hackers, we find alternate ways to use tools and methods others create to accomplish our goals. This talk will explain the essence of how 12-step program principles can be applied to the lives of non-addicts for a positive effect, regardless of any belief or disbelief in religion and/or spirituality.

3:00pm to 3:45pm CDT
Gaslighting and Cognitive Dissonance
Warning: Topic can trigger individuals that have experienced abusive relationships.

Priscilla Aubrey

Gaslighting is probably one of the most overlooked forms of emotional abuse. It is easy to wave away as an overreaction or misunderstanding. Individuals that rely on gaslighting to control their loved ones count on that reaction. How do you recognize gaslighting and what is it? Does gaslighting have long-term effects? Physical? Mental? Gaslighting is much more than a few harshly placed words in the heat of the moment. Gaslighting is one of the cruelest forms of abuse because the person experiencing the abuse is not even sure if it's happening. Let's shed some light on how to detect it and options for countering it.

4:15pm to 5:15pm CDT
Rebalance every 10,000 miles

Wolfgang Goerlich

Careers are long. Jobs are short. One day, things are going well and in balance. The next day, there's twenty hours of work to do. Pull back some and it is more of the same. The first half of the year, things were great. Then change came and chaos reigned and burn out followed. Pull back even further, and the demands of work and life over decades comes into sharp relief. This session presents strategies to maintain your mental health over the long haul. Handle imposter syndrome and stress. Know when to stick it out but recognize the signs when it is just not worth it. Fail and recover gracefully. Pulling on personal lessons and anecdotes from mentoring others, the presentation provides a career owner's manual.

Main Sponsor of Blue Team Con 2022

Microsoft Security

BLUE TEAM CON

Want to play with some cool tech?

Microsoft spends $1 billion dollars
a year to make Defenders successful.

〉 aka.ms/free-security-trials

Sponsors

PLATINUM SPONSORS

Trimarc's Active Directory Security Assessment, Microsoft Cloud Security Assessment, & Virtual Infrastructure Security Assessment provide actionable information enabling you to quickly resolve critical issues.

TrimarcSecurity.com
ADSecurity.org

SentinelOne®

**One platform.
Unprecedented speed.
Infinite scale.**

SentinelOne's mission is to keep the world running by protecting and securing the pillars of modern infrastructure. SentinelOne is a pioneer in delivering autonomous cybersecurity to help organizations secure all of their assets. SentinelOne customers include 3 of the Fortune 10, hundreds of the Global 2000, and many governments, healthcare providers, and educational institutions.

@SentinelOne

www.sentinelone.com

Sponsors

BLUE TEAM CON 2022
FOUNDING SPONSOR

onShore SECURITY

@onShoreSecurity

onshore.com

GOLD SPONSORS

onShore SECURITY

QUADRANT INFORMATION SECURITY

SILVER SPONSORS

Blumira

COFENSE

Gigamon®

GitHub +VILLAGES SPONSOR

LimaCharlie

milton security +PARTY SPONSOR

red canary

StoneX®

tines

TrustedSec

BRONZE SPONSORS

Focivity

K9SECURITY

MOORE RECRUITING

no starch press

BADGE SPONSOR

SPECTEROPS

Foodstuffs

Coffee Fix

Dunkin
233 Michigan Ave

Stan's Donuts & Coffee
181 Michigan Ave

Starbucks
300 E Randolph St

Starbucks
225 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 N Michigan Ave

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)

2023

NOW WITH TRAINING SESSIONS!

BLUE TEAM CON

AUGUST 25-27

WWW.BLUETEAMCON.COM

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

Thank You

For Attending Blue Team Con 2022!

BLUE TEAM CON


BLUE TEAM
CON