BLUE TEAM

20 CON 21

28–29 August 2021
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

While traveling around the country to various conferences, through a mix of observation, participation, and attendance of many talks it became quite clear a gap within the information security industry currently exists. When it comes to these industry standard conferences and gatherings, the information sharing network for red team and offense research and activities was very mature while those for blue team and defense are lacking.

There are a multitude of industry standard offerings ranging from small regional meetups to the much larger well-known conferences held at summer camp in Las Vegas. These information-sharing networks benefit all teams encompassed within information security but are limited in how much they can benefit defenders of the enterprise. This realization made evident a strong need for a conference specific to blue teams and defense to kick-start the maturation process of information-sharing on this side of the house. Enter 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. Our goal is to help organize that information in a fun and collaborative way while offering a platform for those that have figured it out to share their knowledge.

The conference audience will include students, professionals, executives, and sales personnel from all over the United States and potentially beyond. We limit the amount of each of these categories of attendees to ensure this conference contains actual information security practitioners that need to benefit from the knowledge-transfer contained within.

Welome to Blue Team Con!

Code of Conduct

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

Who is Our Code of Conduct For?

Blue Team Con aims to be a conference for EVERYONE. We expect all event attendees, speakers, sponsors, partners, vendors, facilities staff, committee, and board members to agree to and follow 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, non-binary, 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
- ✓ 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 the 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, off-site.

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

ALYSSA
Miller

alyssa@blueteamcon.com

@AlyssaM_Infosec

CARL
Hertz

carl@blueteamcon.com

@cillic

BECKY
Selzer

becky@blueteamcon.com

@BeckySecurity

FRANK
McGovern

frank@blueteamcon.com

@FrankMcG

STEL
Valavanis

stel@blueteamcon.com

@StelValavanis

CFP
Board Members

DANNY
Akacki

@dakacki

FRANK
McGovern

@FrankMcG

GARY
Tinnin

@GWi1s0n

JAMES
Arndt

@jcarndt

ALYSSA
Miller

@AlyssaM_Infosec

STEL
Valavanis

@StelValvanis

CARL
Hertz

@cillic

ERICH
Nieskes

@ErichNieskes

KATRINA

@pinkpushpop

CHRIS
Kubecka

@SecEvangelism

BRAD
Schaufenbuel

@bschaufe

ANONYMOUS

RICARDO
Lafosse

@cyclingciso

BECKY
Selzer

@BeckySecurity

ANONYMOUS

Schedule

All times are in CDT.

Hak4Kidz Village: Saturday from 10:30 AM to 5:00 PM, Sunday from 10:00 AM to 3:00 PM

Health & Wellness Village: Open during talk hours

Resume & Interview Workshop: Saturday from 11:00 AM to 5:30 PM

Unconference: Saturday at 11:00 AM to Sunday at 3:00 PM (Yes, all night)

Friday, August 27th

Registration: 6:00 PM to 9:00 PM

Saturday, August 28th

Registration: 7:00 AM to 3:00 PM
Swag: 11:00 AM to 3:00 PM

Saturday

	Talk Track 1 - 50 Minutes International Ballroom	Talk Track 2 - 30 Minutes Gold Room
9:00 AM	9:00 AM TO 9:30 AM Opening Ceremonies with Blue Team Con Advisory Board	
10:00 AM	9:35 AM TO 10:30 AM Keynote: "Into The Blue" with Sean Metcalf	10:40 AM TO 11:10 AM "Realigning From Chaotic Evil" with Joseph Schottman
11:00 AM	11:00 AM TO 11:50 AM "Betting Before the Breach: Applying Poker Theory to Cybersecurity Spending" with Karen Walsh	11:20 AM TO 11:50 AM "Shifting Security PEOPLE Left: A successful experiment embedding a security engineer in Sales to build empathy, trust, and [more] scalable RFI and incident response processes" with Jennifer Chermoshnyuk
12:00 PM		

Saturday

	Talk Track 1 - 50 Minutes International Ballroom	Talk Track 2 - 30 Minutes Gold Room
12:00 PM	**12:00 PM TO 12:50 PM** “Panel Discussion - Security Strategy for Small-Medium Business” with Russell Mosley, Amanda Berlin, Jim Nitterauer, and Heather Smith	**12:10 PM TO 12:40 PM** “Eliminating Alert Fatigue: Reducing False Positives Through Better Engineering” with Dana Baril
1:00 PM	**1:00 PM TO 1:50 PM** “Incident Communications 101 - Breaking the Bad News” with Dr. Catherine J. Ullman	**1:00 PM TO 1:30 PM** “Office365 Logging - Turning Attacker TTP’s into High-Fidelity Alerts” with Ryan Clark **1:40 PM TO 2:10 PM** “Analyzing Application Risk” with Chelsea Troy
2:00 PM	**2:00 PM TO 2:50 PM** “Shining a Light on Overprivileged Modern Applications – What are they, how to find them, what to do about it” with Mark Morowczynski and Bailey Bercik	**2:20 PM TO 2:50 PM** “When Dinosaurs Ruled the Blue Team: Quickly Retrieving Triage Images Via EDR” with Dan Banker
3:00 PM		**3:40 PM TO 4:10 PM** “Building an AWS Onramp: Maintaining Guardrails for Self-Service AWS” with Margaret Valtierra
4:00 PM	**4:00 PM TO 4:50 PM** “Compliance and Regulation: The Next Great Security Threat?” with John Orleans	**4:20 PM TO 4:50 PM** “Your Tax Dollars hard at work: how 800-53 and STIGS help in non-government space” with Gary Rimar
5:00 PM		

Talk Track 1 - 50 Minutes

International Ballroom

Talk Track 2 - 30 Minutes

Gold Room

5:00 PM

5:00 PM TO 5:50 PM

"Stop talking nerdy to me: translating the value proposition of the blue team to the C-Suite"
with Jake Williams

5:00 PM TO 5:30 PM

"DFIR with Dinosaurs: Unearthing Artifacts and Host Hunting with Velociraptor"
with Wes Lambert

6:00 PM

7:00 PM

7:00 PM TO 9:00 PM

Gameshow

Time to Let Loose with
Blockbusters
Enjoy Fun Competition With
Your Friends and Colleagues

8:00 PM

9:00 PM

9:00 PM TO 1:00 AM

onShore SECURITY

Networking Party and Event

DJ's Cyber Tao Flow, Missy Poptart, Mr. Brad, and cillic

Open Bar and Food

1:00 AM

Sunday

Sunday, August 29th

Registration & Swag: 8:00 AM to 1:00 PM

Talk Track 1 - 50 Minutes

International Ballroom

10:00 AM

10:00 AM TO 10:50 AM
"How to successfully implement a Global Threat Hunting Program"
with Alberto Garcia

11:00 AM

11:00 AM TO 11:50 AM
"Star Wars: How an ineffective Data Governance Program destroyed the Galactic Empire"
with Micah Brown

12:00 PM

12:00 PM TO 12:50 PM
"The TIP of the Stinger: Efficiently Using Threat Intelligence With TheHive"
with Matthew Gracie

1:00 PM

1:00 PM TO 1:50 PM
"Oh FFS! : Practical Password Auditing for Windows Networks"
with AJ Van Beest

2:00 PM

2:00 PM TO 2:50 PM
"Automating Vulnerability Management from Scratch"
with Adam Schaal

3:00 PM

3:30 PM TO 4:30 PM
Closing Ceremonies with
Blue Team Con Advisory Board

Talk Track 2 - 30 Minutes

Gold Room

10:00 AM TO 10:30 AM
"Real World advice to stay sane while building a Security program"
with Lauren Rogers

10:40AM TO 11:10AM
"In the event of my demise, digital estate planning for the whole family"
with Carla Raisler and Matt Speer

11:20 AM TO 11:50 AM
"PhishCatch: Detecting Password Reuse from the Inside Out" with Tyler Butler and Eason Goodale

12:10 PM TO 12:40 PM
"Infosectual disfunction- how soft skills are helping bridge the gap between advocacy and infosec"
with Katelyn Bowden

1:00 PM TO 1:30 PM
"How to Persuade, Change, and Influence to deliver the Blue Team mission"
with Blake Regan

1:40PM TO 2:10 PM
"Writing Cybersecurity Policies: You Don't Have to be Michael Jordan"
with Frank McGovern

2:20 PM TO 2:50 PM
"Lessons learned from building your own Vulnerability Management Platform"
with Lee Berg

Talk Track One
50 MINUTES

Keynote - Into The Blue: Hacking Defense

Sean Metcalf - Founder & CTO, Trimarc

This talk kicks off the first ever Blue Team Con in 2021 and explores several concepts and themes that seem to pop-up from time to time.

Key items covered:

- ✓ "Defender's Dilemma" - do defenders have to be right 100% of the time? (no, watch this talk for the reasons why).
- ✓ Why Blue & Red are effectively 2 sides of the same coin & why we are all on the "Blue Team".
- ✓ Big wins matter - how focusing on big wins can improve security exponentially.
- ✓ Security doesn't need 100% solutions.
- ✓ Fundamental security items tend to matter most.

So, whether you are part of a Blue Team, Red Team, Purple Team, or another team, join me on this journey Into the Blue…

Automating Vulnerability Management from Scratch

Adam Schaal - Director of Enterprise Security, Contrast Security

Did you know that an average of 14,600 vulnerabilities are disclosed each year? How are you handling your discovered vulnerabilities? Vulnerability management is a difficult task, especially at a large organization. In fact, it takes an average of 100 days until known security vulnerabilities are remediated. Often times vulnerability management is implemented in segments, without a big picture vision. It can be also arduous and cumbersome, costing employees valuable time and effort. However, vulnerability management is a necessity in today's cyber security landscape.

In this talk, we discuss where vulnerability management programs fall short and how we can avoid such pitfalls. We will walk through a typical program and the pain points. Once we understand the problem, we will enhance the process through automating asset inventory and daily vulnerability collection. We will also demonstrate how using automation to search asset inventory for newly discovered vulnerabilities increases speed and efficiency of the team and helps to more quickly create action items from discovered vulnerabilities. In addition, our process will help teams determine which vulnerabilities are the riskiest and organize them by remediation priority.

The vulnerability management program is built from the ground up across a complex work environment using Python3, Jenkins, SQL, and a few extra tips and tricks. Proof-of-concept code will be open sourced at the conclusion of the discussion and attendees will leave this talk with the ability to implement similar automated vulnerability management solutions in their environments.

Betting Before the Breach: Applying Poker Theory to Cybersecurity Spending

Karen Walsh - CEO and Founder, Allegro Solutions

Karen Walsh, CEO and Founder of Allegro Solutions, is a data-driven compliance expert and CMMC Registered Practitioner focused on cybersecurity and privacy who believes that securing today's data protects tomorrow's users. Karen has been published in the ISACA Journal experience in cybersecurity centers around compliance. Her work includes collaboration with security analysts and ghostwriting for c-suite level security leaders across a variety of internal and external vulnerability monitoring solutions. As a lawyer, she is deeply knowledgeable about security and privacy laws and industry standards including GDPR, CCPA, and ISO. She is currently under contract with Taylor& Francis and is writing a book about cybersecurity for small and midsized businesses.

Talk Track One
50 MINUTES

Compliance and Regulation: The Next Great Security Threat?

John Orleans - Cloud Infrastructure Security

Most security tools, policies, and processes were created before the advent of consumer protection laws, such as those implemented by the EU, New York State, and California. Many organizations may be surprised to discover that their in-place solutions may be in violation of the law or a critical security risk.

In this session, participants will get tips regarding the overall principles of privacy regulations, what to look for, how to find them, and perhaps learn ways to improve their security stature while maintaining compliance.

How to successfully implement a Global Threat Hunting Program

Alberto Garcia - Global Cyber Threat Intelligence Consultant and Adjunct Professor of Cyber-security, Maryville University

First, this talk is about my last five years of experience implementing a global threat hunting program in two Fortune 500 companies. In this talk, I will introduce the threat hunting concept and explain the following topics: what is threat hunting and what is not threat hunting, how to define/sync threat hunting process between Incident Response process, how to use Cyber Kill Chain, Pyramid of Pain, MITRE Att&ck Framework to develop your threat hunting mission, what are the recommended data sources you need to start your threat hunting program, what are the techniques you can use during your threat hunting engagement and a demo of threat hunting engagement to how to identify Data Exfiltration. I am available to offer a hands-on threat hunting workshop too

Incident Communications 101 - Breaking the Bad News

Dr. Catherine J. Ullman - Researcher & Senior Information Security Analyst, University at Buffalo

Enabling better communications between geeks and management. As humans we have had 60,000 years to perfect communication, but those of us working in IT, regardless of which side (Blue or Red Team), still struggle with this challenge. We have done our best over the centuries to yell “FIRE!” in a manner befitting our surroundings, yet today we seem utterly incapable of providing that very basic communication capability inside organizations. This talk will endeavor to explain HOW we can yell “FIRE!” and other necessary things across the enterprise in a language both leadership, managers and end-users understand.

Panel Discussion - Security Strategy for Small-Medium Business

Russell Mosley - CISO
Amanda Berlin - Co-Author, Defensive Security Handbook
Jim Nitterauer - Senior Security Engineer, AppRiver
Heather Smith - Principal Consultant DFIR, CrowdStrike

Russell Mosley will moderate a panel discussion with blue teamers experienced at organizations of a range of sizes and security budgets, from startups and universities, to government contractors, cloud vendors, and large enterprises - and all of whom worked at Small-Medium Businesses (SMB.) They will discuss SMB capabilities and constraints, blue team organization and leadership, disparate threat models, compliance, and the impact of cloud at SMB compared to larger organizations.

Oh FFS! : Practical Password Auditing for Windows Networks

AJ Van Beest

“Password1!” is a terrible password, right? Surely no one would be foolish enough to use that in your organization, right? RIGHT???

Not *only* is someone almost certainly using “Password1!,” when they next change their password, you _know_ it’s going to be “Password2!” unless it’s “Winter2019.”

In this session, get an (very!) brief overview of gauging password strength, then take a deep--ish dive into exactly how to audit the strength of the live passwords in your Windows environment.

Things you’ll get from this session:

✓ Chuckles over real-life tales of woe;
✓ A sense of urgency around auditing the passwords in your org;
✓ A set of custom scripts and recommended tools you can use;
✓ Playbooks for different kinds of password validation strategies;
✓ Examples of targeted, educational “communications” to send to users;
✓ High-fives from your boss and team for being a “proactive security go-getter!”

Shining a Light on Overprivileged Modern Applications – What are they, how to find them, what to do about it

Mark Morowczynski - Principal Program Manager, Microsoft
Bailey Bercik - Program Manager, Microsoft

App developers have frequently requested more permissions than required. This is not a new problem. As applications modernize and move to the cloud this problem is still occurring, and it’s still your problem as a defender. Some malicious apps are also using similar TTPs to maintain persistence and read and extract data. In this session you will get a crash course on how modern apps request and use permissions, how to find these overprivileged apps, and what you as the defender can do about them.

Talk Track One
50 MINUTES

Star Wars: How an ineffective Data Governance Program destroyed the Galactic Empire

Micah Brown - Vice President, Greater Cincinnati ISSA Chapter

The Galactic Empire in Star Wars Episode 4 was destroyed not by a farmboy from Tatooine, but by an ineffective Data Governance Program. Regardless if you are a traditionalist and follow the original story of Kyle Katarn stealing the Death Star plans out of the Danuta base form Star Wars: Dark Forces or if you believe the new cannon established in Rogue One where Jyn Erso and her team transmits the Death Star plans to the Rebel Alliance ships overhead the planet of Scarif the results is the same. Bad Data Governance practices allowed the Rebel Alliance to blow up the Death Star and ultimately survive the battle of Yavin and go onto eventually topple Emperor Palpatine. This talk will be 100% vendor agnostic and will focus on tools, techniques, and strategies that attendees may take back and implement leveraging either tools that they already own or tools that will be new to their environment. We will discuss aligning Incident Response and Data Governance to ensure proper stewardship of critical and regulatory data. Hopefully after this talk you will not 'find my lack of regular expressions disturbing.

Stop Talking Nerdy to Me: Translating the Value Proposition of the Blue Team to the C-Suite

Jake Williams - CTO and Co-Founder, BreachQuest

There are no shortage of C-Suite executives that don't understand why there is any need for a blue team. After all, isn't the blue team "just" cyber defense? Obviously you know better, but how do you communicate that to the C-Suite? Unfortunately, this is easier said than done. The C-Suite needs to understand value proposition, but they can only do that when we stop talking like a bunch of geeks. We must be business bilingual.

In this session, Jake will share his battle-tested methods for explaining blue team topics to executives. Whether you need to explain why you need that new EDR or justify more retention for the SIEM, this talk is for you.

The TIP of the Stinger: Efficiently Using Threat Intelligence With TheHive

Matthew Gracie - Information Security Engineer, BlueCross BlueShield of Western New York

There are many sources of threat intelligence out there - so many that it can easily become overwhelming. This talk covers a set of open source tools (including MISP, Security Onion, and TheHive) that can be leveraged to organize, normalize, and distribute threat intelligence in your environment for efficient threat hunting and response.

Talk Track Two
30 MINUTES

Analyzing Application Risk

Chelsea Troy

Unit tests help us us drive out intra-class functionality and build confidence in our incremental changes. Integration tests help us ensure that our inter-class and inter-app configuration works as a system.

But neither of these test types presents a panacea for helping us save time and avoid worry: unit tests are relatively slow to drive out, and they tend to end up micro-managing our implementation choices. Integration tests give us a long feedback loop, and they tend to produce a lot of false positives for problems.

Instead, we can consider the risks present in our system as a whole, then write a test harness that mitigates the largest risks and communicates those risks to the rest of the team. This risk-focused perspective, over time, makes it easier for you and your teammates to spot and preempt the kinds of bugs that could become headaches later.

Building an AWS Onramp: Maintaining Guardrails for Self-Service AWS

Margaret Valtierra - Program Manager, Morningstar

More than 130 teams at Morningstar use AWS in some capacity. To encourage teams to follow security best practices our central cloud team had to get creative. We set firm guardrails yet offer a self-service ownership. First, we will review the foundations of a strong account set up and network security based on the AWS Shared Responsibility Model. With that strong foundation in place, we will review how the cloud team enables application teams to take ownership for security best practices. Empowered builders are fully understand their AWS environments and share knowledge across teams. Rigid IAM policies can inhibit innovation. We encourage developers to understand AWS and security best practices.

Finally, we will review how to scale the guardrails to the entire organization and nudge teams to follow security best practices.

We centrally ensure cloud security through two scanning systems: event based and time based scanners. Scanners use custom scripts, Lamdba functions, jira tickets, and SES. Currently we report on public S3 buckets, resources without backups, unpatched instances, and non-standard AMIs. This talk will delve into our scanner architecture as well as how we enforce cloud security across business units. This balance of a self-service approach with automated security checks enables teams to quickly adopt AWS but stay secure.

DFIR with Dinosaurs: Unearthing Artifacts and Host Hunting with Velociraptor

Wes Lambert - Principal Engineer, Security Onion Solutions

This presentation will discuss how security teams can perform multi-platform host-based artifact collection, processing, and hunting using a completely free and open-source tool called Velociraptor. Designed to be simple, yet powerful, Velociraptor allows for security practitioners to quickly and easily build their own detections and gain context around events during an investigation, or while performing routine endpoint monitoring. Attendees should walk away from the presentation with a general knowledge of how they can start using Velociraptor in their environment to enhance their enterprise security monitoring and incident response strategy.

Talk Track One
30 MINUTES

Eliminating Alert Fatigue: Reducing False Positives Through Better Engineering

Dana Baril - Security Research Architect, Microsoft

False Positive alerts (FPs) are the bane of blue teams everywhere. Countless hours are lost as Security Operation Center (SOC) analysts attempt to separate the wheat from the alert chaff to find the real indicators of an attack. Reducing FPs is thus a critical goal for any security platform. Yet reducing FPs at the expense of missing the signs of an actual threat is inviting disaster. The solution to this conundrum lies in better engineering: building the right tools to accurately assess alerts at scale.

In this talk, we explore our approach at Microsoft Defender Advanced Threat Protection (MDATP) to reducing alert FPs. Our engineering-driven methodology evaluates logical units along the entire alert generation and monitoring process, identifies potential high-volume FPs, prototypes viable solutions, and delivers new tools that directly reduce FPs. These tools implement a variety of advanced techniques, including clustering, supervised learning, real-time analysis and sampling optimization.

This approach has proven highly effective at improving alert quality, driving significant enhancements to our customers' investigation experience and making the entire process more efficient. This work is highly applicable to blue teams faced with scaling up to meet increased demands on their limited resources.

How to Persuade, Change, and Influence to Deliver the Blue Team mission

Blake Regan - Manager of Information Security - Global CERT, Equinix, Inc

Psst….want to learn how to social engineer your way into CAB approval at your Change Advisory Board meetings? At the end of the day, CAB stakeholders have to meet their objectives, just like the next person. The most important objective is usually maintaining production uptime at all costs. This can make it difficult to make changes to the environment, like security hardening, anti-virus upgrades, and unfortunately security patching falls into that category as well. Learning how to use the objectives of others as part of your plan is the way to succeed when seeking to influence change and earn buy-in to make configuration changes of any type in a production environment. Together, we will cover a five step process to consistent CAB approval, even in the largest of production environments, under the most unforgiving of timelines. There is no trickery involved, rather a methodology built on open communication, trust, defined expectations, follow through, and accountability.

Infosectual Disfunction - How Soft Skills are Helping Bridge the Gap between Advocacy and Infosec

Katelyn Bowden - CEO and Founder, BADASS

Many orgs dedicated to fighting domestic violence and sexual abuse lack the proper security knowledge to adequately help victims protect themselves from online abuse. Yet, the "soft skills" they desire to learn are often explained in ways that are too complicated for the average user to understand. How can we, as an industry, help bridge this gap, and assist those who need this knowledge?

In the Event of My Demise, Digital Estate Planning for the Whole Family

Carla Raisler - Security Architect, Matt Speer - Penetration Tester

Have you ever received an email from a dead relative? It happens when spammers take over email and social media accounts of deceased contacts. It's just as frustrating as it is creepy if you don't have the means to access the account and stop the hack. Digital estate planning is essential today for both digital immigrants and digital natives alike. Do you have a Digital Executor? You should and so should the rest of your family. When a friend or loved one pass, they leave behind a digital trail of email, social media, online storage, websites, gaming accounts, and intellectual property. Some of this digital property has monetary value, and some of it is their legacy; good and bad. Put your defender skills to good use and protect you and your loved ones' digital assets through administrative, technical, and physical controls.

Lessons learned from Building Your Own Vulnerability Management Platform

Lee Berg - Product Manager - InfoSec, Atlassian

Software Supply Chain Security is an increasingly significant challenge for many organizations, large and small. In this session, we will talk all about the homegrown Vulnerability Management Platform build inside Atlassian. Atlassian makes multiple software products used by thousands of teams worldwide and needed a way to stay on top of vulnerabilities to protect ourselves and our customers. This session will focus on the Why, How, Challenges, Lessons Learned, Wins, and Road bumps of building a Vulnerability Management Platform presented by Atlassian's own Information Security Team.

Office365 Logging - Turning Attacker TTP's into High-Fidelity Alerts

Ryan Clark

This presentation will incorporate actionable alerts found from Office365 logging. These focus on empowering small-mid tier organizations who do not have extensive security staffing. These alerts are often for malicious use, but are noted in unique ways. Each alert presented is defined not by what it finds, but by the attackers TTP. A good example is changing inbox rules. A half dozen different TTPs involve this log, but each requires a different alert query to both find and verify the alert proactively. Alerts will be generated by multiple data points, including UUIDs for Extension and Modified fields, user agents *extensively*, and refinement to take analysis to the next level.

Talk Track One
30 MINUTES

PhishCatch: Detecting Password Reuse from the Inside Out

Tyler Butler - Security Evangelist, Palantir,
Eason Goodale - Application Security Engineer, Palantir

Does fear of a password leak keep you awake at night? Worried that your MFA implementation might not be comprehensive, that passwordless authentication remains out of reach for your org, or that your best-in-class network traffic inspection platform does nothing while off VPN? Concerned your users will remain prone to phishing regardless of how much training they receive? Spurred by the global shift to remote work, the Palantir InfoSec team set out to address these issues in a robust, scalable, low-friction, and highly-actionable new tool.

PhishCatch is an open-source, identity-provider-agnostic browser extension for both Chrome and Edge, which evaluates use of corporate passwords on non-corporate resources in a more robust and versatile manner than similar tools that have come before. PhishCatch features both local and remote alerting (via an optional API server), enterprise management via Group Policy and/or Jamf Pro profiles, no admin dashboards, consistent detections regardless of VPN status, and - most importantly - an invisible, no-action-required addition to the end user's web browsing experience. PhishCatch has revolutionized Palantir's password reuse detection, and we believe it will revolutionize yours too.

Realigning from Chaotic Evil

Joseph Schottman - Security Researcher

The talk uses AD&D (Advanced Dungeons and Dragons) as a metaphor for problems created by corporations and other organizations by having incorrect metrics and incentives for different teams and the need to realign to solve them.

The AD&D theme provides a variety of jokes and clip art throughout the talk but enough background on the game is given that the audience does not need to be familiar with it to understand.

The first part of the talk examines common incentives/goals for offensive and defensive security staff as well as other groups they often interact with such as developers and operations, some of the common ways that they end up working against each other to the detriment of security, and how to fix it.

The second part of the talk delves into using individual sections of the MITRE ATT&CK framework to create manageable, granular tests that offensive and defensive teams can work together on in order to affect a positive change in a unified way.

The talk closes with a brief detour into the terminology of video game terminology to use the concept of tanking (players whose characters take the brunt of damage but often are relegated to the not so exciting parts of games) to talk about how junior SOC analysts often do a substantial portion of actually keeping companies secure and how security as an industry should do a better job of respecting and supporting them.media accounts of deceased contacts. It's just as frustrating as it is creepy if you don't have the means to access the account and stop the hack. Digital estate planning is essential today for both digital immigrants and digital natives alike. Do you have a Digital Executor? You should and so should the rest of your family. When a friend or loved one pass, they leave behind a digital trail of email, social media, online storage, websites, gaming accounts, and intellectual property. Some of this digital property has monetary value, and some of it is their legacy; good and bad. Put your defender skills to good use and protect you and your loved ones' digital assets through administrative, technical, and physical controls.

Real World Advice to Stay Sane While Building a Security Program

Lauren Rogers - Defensive Security Programs

There are lots of theories about how to build a SOC in a perfect world, many written by consultants who do great work but don't live in the less than perfect world after their perfect suggestions.

I will discuss common sense approaches based on my 10 years in security and my 20 in IT. I will reference the painful but still useful resources online and why this is not as daunting as it feels and sounds and how real world solutions do exist.

Shifting Security PEOPLE Left: A Successful Experiment Embedding a Security Engineer in Sales to Build Empathy, Trust, and [more] Scalable RFI and Incident Response Processes

Jennifer Chermoshnyuk - Sr. Manager, Customer Security and Trust Engineering, GitHub, Inc.

What do you get when you take a nearly burned-out security engineer with a foot-at-the-door but trying one last "plan c" to save a budding security enablement program, mix in some extremely supportive and creative solutions engineers, and add a healthy dose of an executive sponsor with a gift for identifying value and an appetite for "we can do better"? You have a recipe for a silo-busting experiment of "shifting security [people] left" and after two years some excellent lessons learned.

This talk is both a retrospective on GitHub Revenue's welcoming of an embedded security engineer, as well as "Do try this a home" how to on building customer trust, scaling security RFI response, multiplying a company's incident response capabilities, and above all increasing security awareness in and empathy for sales teams.

Spoiler alert: As all security blue team members know in our heart of hearts, we are not just a cost center to protect the business and ARR: we can actually grow revenue through tighter partnerships and empowering stakeholders. This experiment proves it AND brought enthusiasm and hope back to a cynical security engineer.

When Dinosaurs Ruled the Blue Team: Quickly Retrieving Triage Images Via EDR

Dan Banker - Threat Response Team Lead, Motorola Solutions

With the recent rise in users working remotely, many security-related processes have had to adapt. One of these is capturing a forensic image for analysis. Acquiring a bit-for-bit copy of a full disk over the network is impractical, and obtaining the physical drive may introduce unacceptable delays. I will outline a process for using EDR to deploy the Velociraptor standalone executable and capture a triage image under 500MB in size. This can be done in under 30 minutes, and will hand your team the most important forensic artifacts to start the investigation.

Talk Track One
30 MINUTES

Writing Cybersecurity Policies: You Don’t Have to be Michael Jordan

Frank McGovern - Cybersecurity Architect, StoneX & Co-Founder, Blue Team Con

Cybersecurity policies are often viewed as the pinnacle of what a mature business represents. They are often created and pushed out during late stage development because of how much time and emphasis must be given to them. This is a fallacy; mainly due to the fact that when you are looking at people, process, and tools, the process comes before tools. You won’t know what tools you need until you outline and agree on a set of processes, which are dictated by policy. In addition to the word policy, there are standards, guidelines, regulations, procedures, controls, control objectives, metrics, influences, risks, and regulations...It’s no wonder smaller shops are completely lost!

In this talk, we will start off by working through the terminology together and then walk through the hierarchy of how they connect. With that out of the way, we can now discuss how you do not have to “Be Like Mike” (Michael Jordan) when writing policy. Too often, we are scared to implement something unless we can perfect it on the first round. Policies are a continual maturation process. Simply getting some basics down counts as a written policy! In this talk, we will go over how you can get started immediately after Blue Team Con, on Monday, with writing your corporate cybersecurity policy.

Your Tax Dollars Hard at Work:
how 800-53 and STIGS help in Non-Government Space

Gary Rimar - Risk Management Executive Function Support

As a newly-minted IT director, I knew enough about Information Assurance/INFOSEC/Cybersecurity to know that I didn’t know enough, and smartly hired it out. I wished that I had known of good study materials to help me understand what security risks needed to be met, and step-by-step instructions to harden my systems. Years later, I was exposed to Risk Management Framework (RMF) and learned about Security Technical Implementation Guides (STIGS) and NIST 800-53 (security controls handbook). Had I known about these back then, I would have been a much better IT director. I am sure that there are those working in non-government space that don’t know what these are. This talk is to provide a tour of NIST 800-53, STIGS for non-governmental employees, to help them see how to protect their networks, what levels of control implementation are appropriate, and a basic hands-on how-to guide.

Last Minute CTF

Welcome to the Last Minute CTF, a friendly, beginner-oriented, introduction to Capture The Flag (CTF) competitions. As you may be able to tell from the name, we're doing this all very last minute to try and 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. The understanding is that most, if not all, of the challenges should be easy to people who have participated in CTFs in the past (mostly due to the very last-minute nature). 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. 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.

To compete in the CTF: https://btcon.link/CTF

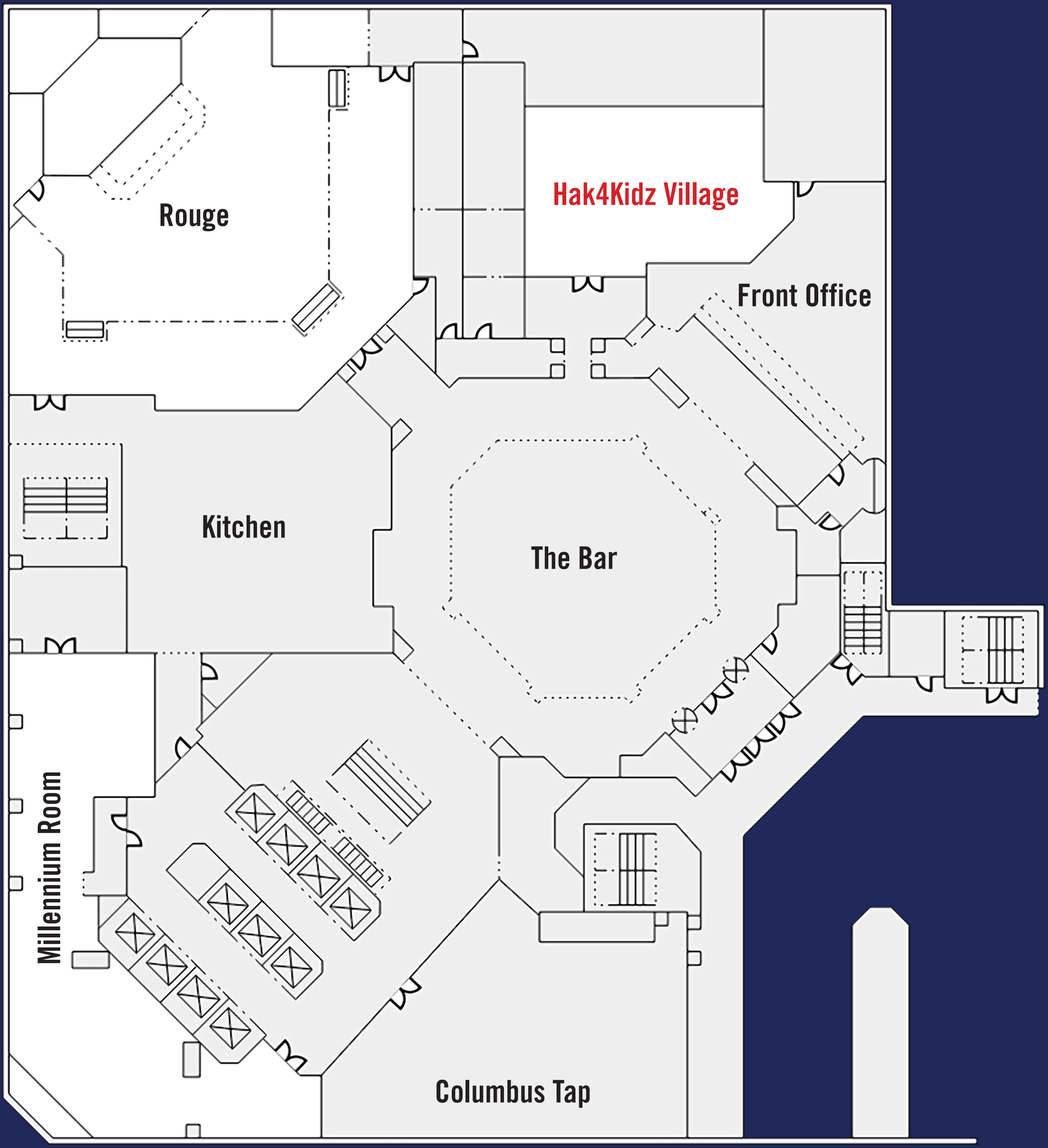
Help and Assistance: Join Blue Team Con Slack and then the #btc2021-ctf channel

More information, as well as competition updates, will be provided directly via the CTF homepage. And no, this is not a flag.

CTF Hours: Friday from 6:00 PM CDT until Sunday at 12:00 PM CDT

CTF winners will be announced at the closing ceremonies!

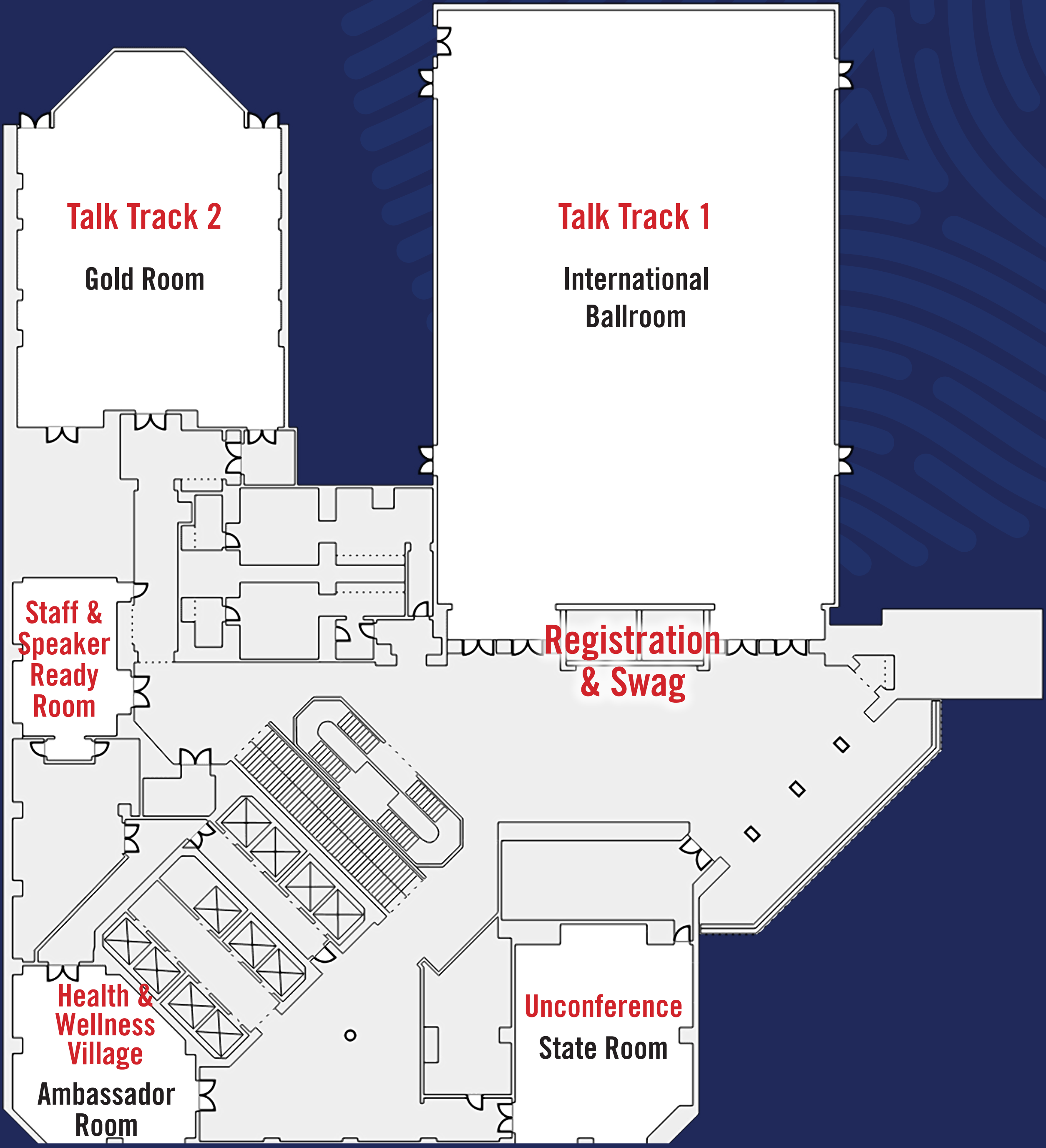
Venue


Rouge
Hak4Kidz Village
Front Office
Kitchen
The Bar
Millennium Room
Columbus Tap

Level TWO

Venue

Resume & Interview Village
37th Floor Boardroom



Villages

HAK4KIDZ

Hours: Saturday from 10:30 AM to 5:00 PM, Sunday from 10:00 AM to 3:00 PM

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 include the Cisco Cyber Defense Clinic, jrCTF, and more. If participating, please have kids bring a laptop with Wireshark installed and tested. Please note that the CDC and jrCTF are limited to ages 12 through 17.

www.hak4kidz.com

MENTAL HEALTH HACKERS

Sponsored By:

GitHub

Open during Talk Hours

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

scope

Resume & Interview Workshop

Hours: Saturday from 11:00 AM to 5:30 PM

A resume and interview workshop will take place that involves hiring managers and business professionals.

Learn how to effectively highlight your knowledge, experiences, and abilities on your resume and during interviews and become better prepared for interview settings that employers are utilizing today. You will be able to hear insider tips from real recruiters and hiring managers for rocking the interview and crafting your resume, then practice your skills and get direct feedback so you can feel more confident in your job search.

REDLEGG Unconference

Hours: Saturday at 11:00 AM to Sunday at 3:00 PM (Yes, all night)

One of our villages is an Unconference. Open during the entirety of the conference (even through the night). 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 by using the paper easel placed right outside the village's door. 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! It's an Unconference!

✓ Presentation/Participation
✓ Sounding Board
✓ Ignite talks
✓ Fishbowl
✓ Learn How to do X
✓ UnCon After Dark (have your stand-up or improv skills ready!)

Sponsors

FOUNDING SPONSOR

onShore SECURITY

@onShoreSecurity

www.onshore.com

GOLD SPONSOR

TRIMARC

@TrimarcSecurity

www.trimarcsecurity.com

SILVER SPONSORS

GitHub

@github

www.github.com

Palantir

@PalantirTech

www.palantir.com

red canary

@RedCanary

www.redcanary.com

StoneX®

@StoneX_Official

www.stonex.com

TREND MICRO™

@TrendMicro

www.trendmicro.com

TrustedSec

@TrustedSec

www.trustedsec.com

BRONZE SPONSORS

REDLEGG

scope

Raytheon Intelligence & Space

tines

cyber popup

Blue Team Labs™

Security Onion SOLUTIONS

OPTIV

FORETRACE

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)

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 2021!

BLUE TEAM CON

BLUE TEAM

CON