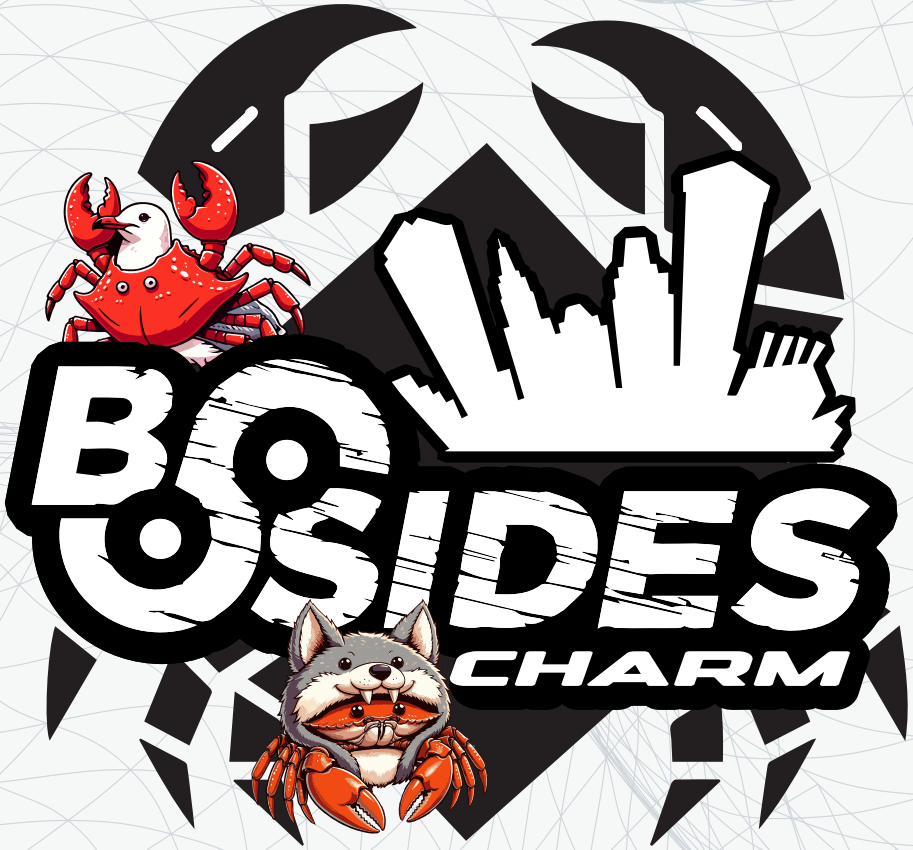

BSIDES
CHARM

THANKS TO OUR SPONSORS!

TABLE OF CONTENTS

WELCOME TO BSIDESCHARM 2024

Welcome to BSidesCharm 2024!

Whether you're a returning attendee or joining us for the first time, we're thrilled to have you with us for another exciting weekend of information security education and community building. As we gather for this year's event, we're mindful of recent tragedies. We've witnessed the incredible resilience of Charm City as we've come together to support each other with compassion. BSidesCharm embraces this spirit of unity to bring cybersecurity together with the power of community.

For those of you who have attended our events in the past, you will be thrilled to know that many of your favorite events, villages, and activities are returning this year. For those joining us for the first time, we extend a warm welcome and invite you to enjoy two days of cutting-edge talks, hands-on training courses, workshops, villages, CTFs, networking with local industry professionals, and a peek into various cyber career opportunities.

Our Hiring Village offers unlimited opportunities for you to discuss your career growth, fine-tune your resume, and help you pursue your professional passions. They will be available on Saturday, during the day, in Rain Restaurant between Registration and the hotel lobby.

In addition to the familiar faces of the Lockpick Village and the Radio Frequency CTF, we're excited to welcome back the IoT Village, Black Cybersecurity Association, and Mental Health Hackers. Plus, we're introducing the addition of the Graylog, Aerospace Village, and AI Village. You will also find three CTFs hosted by Radio Frequency Village, AI Village, and Graylog.

We'd also like to welcome this year's charities! Please visit Blacks in Cybersecurity, ISSA, Unallocated Space, and VetSec over the weekend.

Join us Saturday evening for the BSidesCharm Happy Hour, immediately following the last talk of the day. It's the perfect chance to unwind, catch up with old friends, and make new connections while enjoying some refreshments. And if you're up for more fun, stick around for our video game party on Saturday at 8 PM!

We couldn't make this event happen without the help of all involved. Special recognition and thanks to:

* All organizers and volunteers who have worked tirelessly to bring this weekend together

* Our awesome speakers, trainers, and villages who are graciously giving their time and knowledge this weekend

* Our amazing sponsors that made this year's event possible

* Our families who have supported the work and strain involved in putting BSidesCharm 2024 together

* And, especially to YOU! We thank you for being a valued part of our community. We work hard to bring this event together for you, and we hope that you leave this weekend with newly gained knowledge and, hopefully, new friends.

Code of Conduct

Our "Code of Conduct" is "Be Excellent to Each Other".

We expect the best behavior from our attendees, speakers, sponsors, staff, and other participants to create a safe and positive environment for everyone.

We have no tolerance for verbal, physical, or sexual harassments against any individual.

Speakers and presenters appreciate legitimate questions and alternate points of view. This is how we all learn. Asking questions of a speaker during their talk, to get clarity or debate a point, is acceptable and encouraged. However, heckling speakers, engaging in any disruptive behavior, or interfering with a presentation or training is unacceptable behavior and will be considered harassment which could become grounds for you being asked to leave the conference.

You will not engage in any form of harassing, offensive, discriminatory, or threatening speech or behavior, including (but not limited to) relating to race, gender, gender identity and expression, national origin, religion, disability, marital status, age, sexual orientation, military or veteran status, or other protected category.

If you witness activity that violates the letter or spirit of this Code of Conduct, please alert a staff member. Staff are designated as the Board, Organizers, and Volunteers.

If someone asks YOU to stop a certain kind of behavior, please stop.

BSidesCharm has the right, and duty, to remove any harmful influence from the event for the safety of others.

Content Limitations and Restrictions

BSidesCharm is an all-ages event. For any and all content provided by speakers, trainers, villages, and sponsors, the following rules apply:

- No inappropriate content related to any protected class
- No explicit nudity or sexual content
- No disclosure of a private person's personal identity, a.k.a. doxxing
- No classified content, regardless of if the content is previously leaked or publicly available

If content may violate one of these policies, but is very specifically integral to the content being presented, please contact your BSidesCharm Point of Contact to allow for Board review and approval.

Photography and Video Recording

Avoid any photography, video recording, or audio recording of attendees or other individuals without the expressed consent of all individuals included or portrayed in the recorded media. Using your best effort and judgment, please try to ensure you have permission from anyone you photograph or record. This includes, but is not limited to, anyone in the background of your shot. Similarly, please try to ensure you have permission from anyone you photograph or record to post their picture online, including to social media and personal websites. For these reasons, "crowd shots" from the front (facing the crowd) are strongly discouraged.

Some presentations are designated as not-recorded. Refrain from any attempts to take video or photos within these sessions. Content from these sessions should be considered Off the Record unless willingly provided with the express consent of the presenter.

We require press attendees to adhere to this policy as well.

Respect the privacy of any individuals at the BSidesCharm event. You may request appropriate contact information from individuals but cannot force the disclosure of an individuals personal identity for any reason, nor should you willingly disclose an individuals identity for any reason without express consent.

Hiring Village

Hiring Village - 1st Floor, Rain Restaurant
Saturday 1pm-5pm

Career Opportunities

Hiring Village offers an opportunity for BSides-Charm attendees to talk with companies about career opportunities. We have a fine assortment of small/medium/large companies from our local area that offer a mix of career opportunities. Come talk to our participating companies in a low-pressure environment and learn about what they have to offer!

This year our hiring companies who will be in the village to talk to you include: CYDECOR, augustschell, CLARITY, ALTUS CONSULTING.

Resume Review/Career Advice

Have career questions? Don't know how to break into the speciality area of your interest? Not sure what options might be a fit for you? Stop by! We will have volunteer mentors - subject matter experts in the domain that can help with career questions.

How dusty is your resume? Does it really reflect your skills, abilities and talents? What does it look like to someone reviewing you for a job? Everyone should have an up-to-date resume. Stop by and meet with volunteer resume reviewers to fine tune your resumes. You don't have to be job hunting to update your resume. Don't wait until you need it!

NEW THIS YEAR: Participants in our Resume Review and Career Coaching sessions get a FREE HEADSHOT from a professional photographer!

Hiring Village Participating Companies

ALTUS CONSULTING

augustschell

CYDECOR

CLARITY

Mental Health Hackers Village

2nd Floor Burke, Saturday and Sunday

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

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

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

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

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

Graylog

1st Floor Rain, Sunday

You don't want to miss Graylog's CTF event, where players will engage in thrilling challenges of wit and skill. Through a series of captivating puzzles, you'll navigate through intricate scenarios designed to both educate and evaluate your expertise in data analytics and cybersecurity. From beginners to seasoned professionals, our inclusive format accommodates all skill levels, fostering an environment of learning and friendly competition.

Don't miss out on the opportunity to showcase your talents and win exciting prizes!

IoT Village

2nd Floor Lindsay, Saturday and Sunday

IoT Village advocates for advancing security in the Internet of Things (IoT) industry through bringing researchers and industry together.
IoT Village hosts talks by expert security researchers, interactive hacking labs, live bug hunting in the latest IoT tech, and competitive IoT hacking contests. Over the years, IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees the opportunity to learn about the most innovative techniques to both hack and secure IoT.
IoT Village is organized by security consulting and research firm, Independent Security Evaluators (ISE), and Loudmouth Security.

Lockpick Village

1st Floor Warfields, Saturday and Sunday

The mission of The Open Organisation of Lockpickers (TOOOL) is to advance the general public knowledge about locks and lockpicking. By examining locks, safes and other such hardware and by publicly discussing our findings, we hope to strip away the mystery with which so many of these products are imbued.The more that people know about lock technology, the better they are capable of understanding how and where certain weaknesses are present. This makes them well-equipped to participate in sportpicking endeavors and also helps them simply be better consumers in the marketplace, making decisions based upon sound fact and research.

Visit TOOOL and learn how to pick a lock or work on refining your current skills!

Aerospace Village

2nd Floor Lindsay, Saturday and Sunday

The Aerospace Village is a diverse community of hackers, engineers, pilots, policy leaders and more from across both the public and private sectors. We believe the flying public deserves safe, reliable, and trustworthy air travel, which is highly dependent on secure aviation and space operations.

RADIO FREQUENCY CAPTURE THE FLAG

1st Floor Warfields, Saturday and Sunday

In this game capture the flag you will be presented with real configurations of real wireless and

Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at BSidesCharm. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question – ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

This contest is free and open to anyone and everyone. You can sign up and start playing any time during the conference. If you didn't bring your wireless gear don't worry, our virtual RFCTF environment is played over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: https://rfhackers.com/resources

Hybrid Fun

For BSidesCharm we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn, practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

THE GAME

To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct. Flags worth more points for the early solves, so don't sit on those flags. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself.
Play nice, and we might also play nice.

Who runs this thing?

RF Hackers Sanctuary is a group of all volunteers with expertise in radio security and various other related fields. Wireless Capture the Flag, and RF Capture the Flag. We are the original founders of the WiFi Village, Wireless Village, and RF Village. Often imitated, never duplicated.

TL;DR
Getting started guide: https://github.com/rfhs/rfhs-wiki/wiki

Helpful files (in-brief, wordlist, resources) can be found at https://github.com/rfhs/rfctf-files

Support tickets may be opened at https://github.com/rfhs/rfctf-support/issues

Our whole game is also open source and available at: https://github.com/rfhs/rfctf-container

Twitter: @rf_ctf and @rfhackers
Discord: https://discordapp.com/invite/JjPQhKy
Website: http://rfhackers.com – play with us
Github: https://github.com/rfhs
Official Support Ticketing System: https://github.com/rfhs/rfctf-support/issues

BLACK CYBERSECURITY ASSOCIATION VILLAGE

2nd Floor Duncan, Saturday and Sunday

The BCA Village is designed to be a dynamic hub for Black cybersecurity professionals to explore the latest in cybersecurity technologies, practices, and career opportunities. We are dedicated toward increasing the number of Black cybersecurity professionals and creating a space for Black people to call home.

At the heart of the BCA Village, attendees will find a series of interactive workshops, engaging talks, and hands-on challenges tailored to empower cybersecurity professionals and enthusiasts at all levels. Whether you're a seasoned expert looking to share your knowledge, or a newcomer eager to dive into the world of cyber defense, the BCA Village offers a unique space to connect with like-minded individuals, learn from industry leaders, and contribute to a more inclusive cybersecurity community.

Key Features of the BCA Village:

- Interactive Workshops and Panels: Covering a wide range of topics from ethical hacking and cyber defense strategies to career development and leadership in cybersecurity.
- Networking Opportunities: Connect with professionals, mentors, and companies dedicated to supporting diversity and inclusion in cybersecurity.
- Live Demonstrations and Challenges: Experience real-world cybersecurity scenarios through CTF (Capture The Flag) competitions, live hacking demonstrations, and more.
- Resource Sharing and Collaboration: Access valuable resources, share knowledge, and collaborate on projects aimed at solving pressing cybersecurity challenges.

Join us at the BCA Village to celebrate the strength of diversity in cybersecurity, forge new connections, and advance your skills in an inclusive and supportive environment. Together, we're building a stronger, more resilient cybersecurity future for everyone.

AI Village

2nd Floor Grason, Saturday and Sunday

AI Village is focused on teaching you what you need to know to both defend and break AI. Come learn how ChatGPT, StableDiffusion, malware detectors, ML firewalls, and other AI based products work and how to break them. We'll have demos that show you technical aspects of AI that you need to know as security professionals. We'll also have a CTF that will help train you in ML Security.

Charities

Unallocated Space

Unallocated Space is a 501(c)(3) charitable organization in Severn, Maryland. Their mission is to foster creative and technical growth through open collaboration by providing tools and resources within the greater Baltimore-Washington Metro area. Please learn more at https://www.unallocatedspace.org.

VetSec

Our mission is to create a world where no veteran pursuing a career in cybersecurity goes unemployed. VetSec is a US-based, 501(c)(3) non-profit accepting active-duty, reservists, and veterans from the United States and friendly nations into our community. We want to provide the nearly 200,000 people who transition out of the military in the United States every year with a path to employment in cybersecurity, if they desire. We provide a platform where our members can receive mentorship, resume and job assistance, and reduced-cost training.

ISSA

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners.

It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. For more information about the Central Maryland chapter, please visit our website at https://issa-centralmd.org

Blacks in Cybersecurity

Blacks In Cybersecurity, is a Cybersecurity conference series and all encompassing networking/development group for the Black community in Cybersecurity. BIC seeks to promote advancement, knowledge, education and culture in the Cybersecurity and greater STEM Community. Blacks In Cybersecurity™ is a meetup group and conference series to help highlight and elevate the Black community in Cybersecurity.

CLEAREDGE IT SOLUTIONS

ClearEdge's Mission is to empower customers in government and industry with innovative data driven solutions. We achieve this by investing in our employees, technology, and improving our communities.

Intelligence Solutions

- Software Engineer
- Systems Engineer
- DevOps Engineer
- Systems Administrator

Cyber

- Embedded Software Engineer
- Vulnerability Researcher
- CNO Engineer
- IoT / ICS Engineer

- 10% Employer 401k Contribution
- 11 Holidays & Up to 25 Days PTO
- 100% Employer Paid Healthcare
- Annual $500 Health & Tech Allowance
- $10,000 Education, Training, & Conference Allowance

ClearEdgeit.com/careers

@ClearEdge IT Solutions
@ClearEdgeIT
@ClearEdgeIT

CORELLIUM®

Virtualize iOS & Android devices

Mobile Security Research
Vulnerability research and introspection.

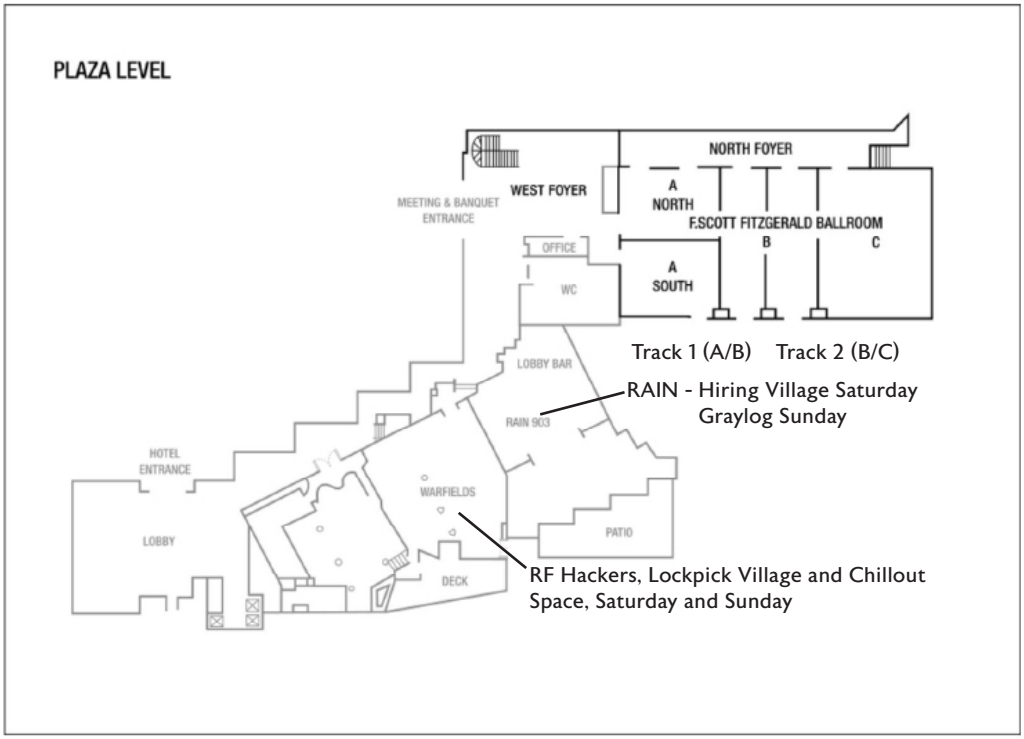
Mobile App Pentesting
App security and penetration testing.

Mobile App DevOps
Continuous security testing for DevSecOps.

Malware Research
Mobile malware and threat hunting.

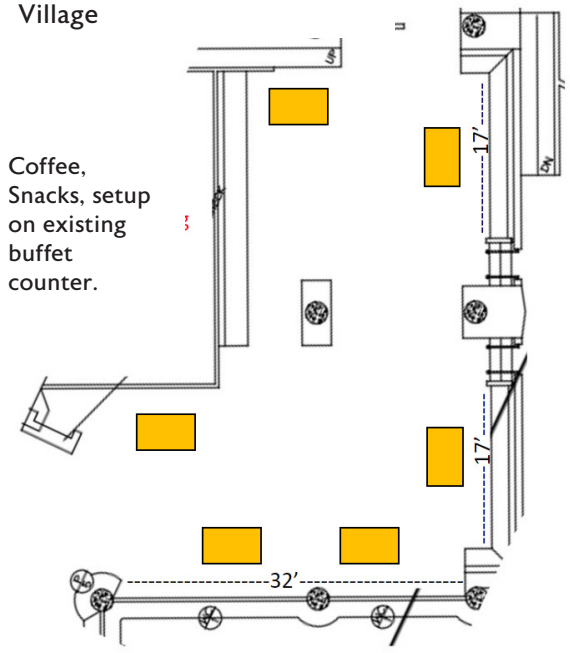
Security Training
Virtual learning platform for professors and trainers.

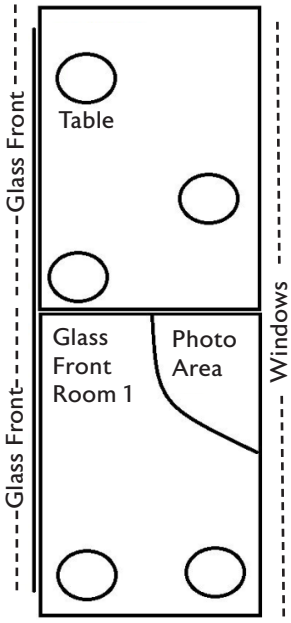
Free trials at **Corellium.com**



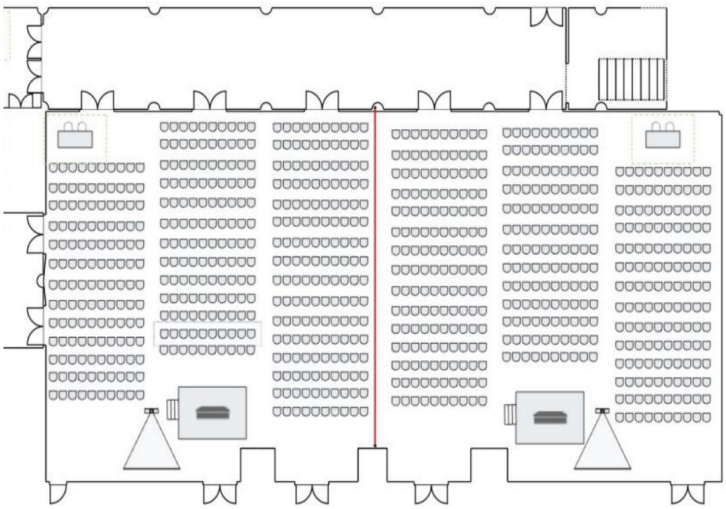
Rain (Restaurant) - Hiring Village

Coffee, Snacks, setup on existing buffet counter.

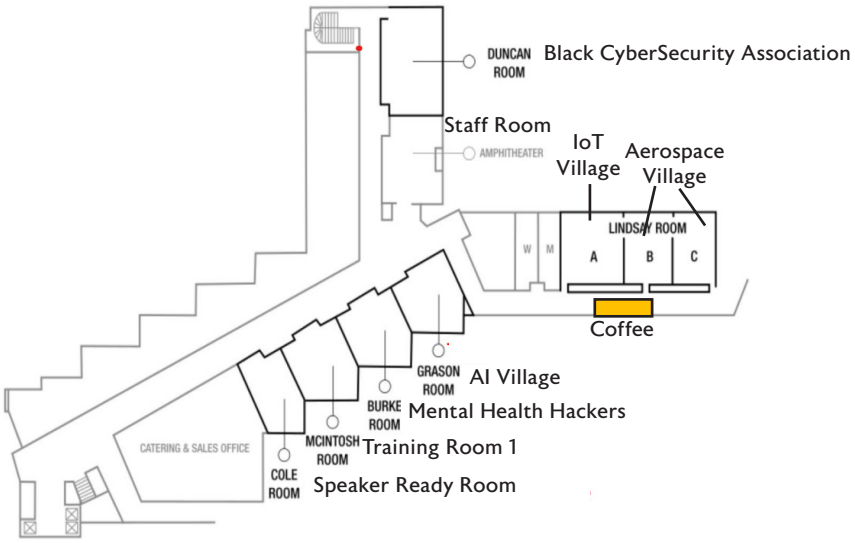




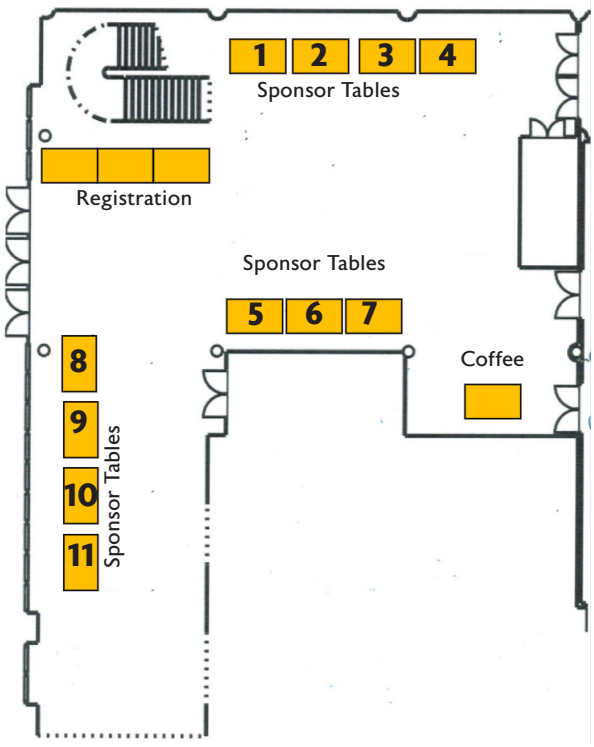
Fitzgerald Ballroom



SECOND LEVEL



West Foyer



Sponsors Village tables key

1. **Trimarc**
2. **Sealing Tech**
3. **Black Hills Information Security**
4. **Johns Hopkins Applied Physics Laboratory**
5. **Corellium**
6. **Capitol Technology University**
7. **Turngate**
8. **Clear Edge IT**
9. **Cydarm**
10. **Flare Systems**
11. **Pixee**

TALK SCHEDULE

SATURDAY

Time Slot	Track 1	Track 2
08:30 - 10:00	Registration Opens	
10:00 - 11:00	Keynote - Caroline Wong	
11:00 - 11:30	Visit Our Sponsors and Villages	
11:30 - 12:00	Generative AI for Blue Teams - Chris Wheeler	Defenders can use ATT&CK! Oh really? - Lex Crumpton
12:00 - 13:00	The Problem with Identity Security & How to Fix It - Sean Metcalf	Hackers in Jurassic Park: When Attackers Find a Way - Kevin Johnson
13:00 - 14:00	Lunch on Your Own	
14:00 - 15:00	Network Segmentation without a Network Engineer - Mike Burns	Scaling the Security Wall: Agile Threat Modeling for Complex Systems - Vineeth Sai Narajala
15:00 - 16:00	Identifying and Securing Psychologically Vulnerable Users - Ira Winkler	Everything You Didn't Want to Know About CVE - Paul Asadoorian
16:00 - 16:50	The Fellowship of the Ring0 - Dana Behling	Cloud IAM Strategy for Multicloud and Hybrid Environments: Risks and Gaps - Cassandra Young, Christian Nicholson
16:50 - 17:00	Registration Closes at 5pm	
17:00 - 17:30	Graph Activity Logs for Incident Responders - Pallav Gurung	CI/CD talent development pipeline- Chris Foulon
17:30 - 18:00	Top Ways I Still Hack Your Company (and How to Defend Against Them) - Bennet Warner	Beyond Booze: Rethinking Networking Events for a Healthier Security Culture - Jen VanAntwerp
18:00 - 20:00	BSidesCharm Happy Hour	
20:00 - 23:00	BSidesCharm Party	

SUNDAY

Time Slot	Track 1	Track 2
09:00 - 10:00	Registration Opens	
10:00 - 11:00	Keynote - Melanie Ensign	
11:00 - 11:30	Visit Our Sponsors and Villages	
11:30 - 12:00	From Aspire to Hire: Navigating Your First Cyber Job - Sully Vickers	Securing generative AI: threats, old and new - Adam Swanda
12:00 - 13:00	Protect Your Most Sensitive Users With This One Weird Trick! - Jake Hildreth	Getting Started in ICS - Tyler Jansen
13:00 - 14:00	Lunch on Your Own	
14:00 - 14:50	Using Bloodhound as a Defender: Tips from the Red Team - Andrew McNicol	Sysmon or it Didn't Happen - Gerard Johansen
14:50 - 15:00	Registration Closed	
15:00 - 16:00	Who's going to secure the code our army of robots are going to be writing? - Arshan Dabirsiaghi	Purple Teaming 301 - Free attack simulation and control validation using At - Jason Wright
16:00 - 16:30	Closing Ceremony	

TRAINING SCHEDULE

SATURDAY

Time Slot	Training
11:30 - 17:30	SECURITY AI - Imani Palmer

SUNDAY

Time Slot	Training
11:30 - 13:30	Threat Actors: Gotta Catch Them All! - Marcelle Lee
14:00 - 17:00	Securing the Cloud with Cloud Threat Intelligence and Open Source Security - - Natalie Simpson

KEYNOTE SPEAKERS

Caroline Wong

Caroline Wong is the Chief Strategy Officer at Cobalt. As CSO, Caroline leads the Security, Community, and Pentest Operation teams at Cobalt. She brings a proven background in communications, cybersecurity, and experience delivering global programs to the role. Caroline's close and practical information security knowledge stems from her broad experience as a Cigital consultant, a Symantec product manager, and day-to-day leadership roles at eBay and Zynga.

Caroline also hosts the Humans of InfoSec podcast, teaches cybersecurity courses on LinkedIn Learning and has authored the award-winning textbook Security Metrics, A Beginner's Guide. Caroline holds a bachelor's degree in electrical engineering and computer sciences from UC Berkeley and a certificate in finance and accounting from Stanford University Graduate School of Business.

Melanie Ensign

Melanie Ensign is the Founder and CEO of Discernible Inc, a specialized communications consultancy for security and privacy teams. After managing security, privacy, and engineering communications for some of the world's most notable brands including Uber, Facebook, and AT&T, she now coaches teams around the world to increase their influence with business leaders and reduce risk. She counsels executives and technical teams alike on how to cut through internal politics, dysfunctional inertia, and meaningless metrics. Previously,

Melanie led the press department for DEF CON as a volunteer for 10 years. A certified rescue scuba diver, she brings lessons from navigating unexpected, high-risk underwater incidents to her professional work.

SATURDAY PRESENTATIONS

Generative AI for Blue Teams - Chris Wheeler

This talk is an introduction for defensive cybersecurity practitioners and blue teams to Generative Artificial Intelligence (AI). It will review generative AI terminology and concepts, show practitioners how to get started with free and minimally paid resources, and demonstrate use cases in defensive cybersecurity.

Chris is a Blue Team Lead in the financial services sector, currently specializing in SOAR and Incident Response. In his 14 year career he has also led Threat Intelligence, Automation, and Operations teams at Resilience Insurance, Arbor Networks, and the US Navy. He enjoys running, home networking, and joining too many fantasy football leagues.

Defenders can use ATT&CK! Oh really?- Lex Crumpton

As a defender, what does "I use ATT&CK" really mean? In this talk, we will share how defenders like you can translate the adversary perspective provided by ATT&CK into knowledge on how to detect and protect against cyber threats. We will also explore using ATT&CK to identify defensive gaps, develop analytics, and measure/improve your SOC maturity.

Alexia "Lex" Crumpton is a Principal Cybersecurity Engineer – SOC and Blue team for the MITRE Corporation. Lex is a multi-functional leader whose current work spans across various exciting efforts involving security operations and research, specializing in defensive countermeasures and heuristic behavior analysis. She leads teams that help shape and deliver cyber analytics, mitigations, and detections within MITRE ATT&CK®, the Center for Threat-Informed Defense, and ATT&CK Evaluations. Lex previously worked as an Exploitation Developer, Windows Blue Team/Threat Hunter analyst, Malware Reverse Engineer, and lead DFIR analyst. Lex holds a M.S. in Cybersecurity from University of Maryland, Baltimore County (UMBC) and a B.S. in Computer Science from Bowie State University. Her personal mission is creating defensive solutions for the everyday user to understand and showing representation of technical women within the cybersecurity field to make a positive impact on youth.

The Problem with Identity Security & How to Fix It - Sean Metcalf

We have an Identity problem and not the kind you think of when you look in the mirror. Attacks have shifted from the perimeter to the endpoints and now attackers have their sights on identity. This talk explores the issues with Identity security specifically the two most popular identity systems, Active Directory & Azure AD

("Entra ID" for those who read Microsoft's press releases). These Identity security issues lead to compromise of systems that leverage the identity system for authentication/authorization.

Explored during this talk are the most common ways attackers compromise Identity systems, well-known breaches related to these issues (including the recent MGM breach), and the best ways to mitigate them. Attendees will leave this talk with a better understanding of attacker techniques to compromise Active Directory & Azure AD (Entra ID) as well as methods to best mitigate these attacks.

Sean Metcalf is founder and CTO at Trimarc (TrimarcSecurity.com), a professional services company which focuses on improving enterprise security. He is one of about 100 people in the world who holds the Microsoft Certified Master Directory Services (MCM) Active Directory certification, is a former Microsoft MVP, and has presented on Active Directory, Azure AD, & Microsoft Cloud attack and defense at security conferences such as Black Hat, BSides, DEF CON, DerbyCon, & BlueHat.

Hackers in Jurassic Park: When Attackers Find a Way - Kevin Johnson

In the talk 'Hackers in Jurassic Park: When Attackers Find a Way', Kevin Johnson of Secure Ideas delves into the world of cybersecurity, through the lens of real-life hacking stories. Just as 'Jurassic Park' unveiled the unforeseen consequences of bringing dinosaurs back to life, this presentation uncovers the unexpected and often ingenious methods used by cyber attackers to breach seemingly impregnable digital fortresses. Our journey takes us through a series of true tales from the front lines of cybersecurity, where penetration testers navigate the complex jungle of code and cybersecurity measures.

Each story in the talk is carefully selected to demonstrate a unique aspect of cyber attacks – from social engineering feats that mirror the cunning of a Velociraptor, to sophisticated attacks that target applications and APIs with the ferocity of a T-Rex on the loose. Attendees will not only get an insider view of the tactics and thought processes of attackers but will also grasp the critical importance of proactive defense strategies. This session aims to enlighten, entertain, and educate, offering vital insights into the ever-evolving threat landscape. By the end, participants will have a heightened awareness of the risks lurking in the digital world and be inspired to think like a seasoned hacker to better defend their digital realms.

Kevin Johnson is CEO of Secure Ideas, a consulting company dedicated to security testing and training. Kevin passionately advocates for cybersecurity through his work with Secure Ideas, as a global board member for OWASP and as a faculty member at IANS. During his over 30 years in the industry, Kevin acted as an instructor and author for the SANS institute. He also contributed to a number of open-source projects, including OWASP SamuraiWTF (a web pen-testing training environment), Laudanum (a collection of injectable web payloads) and Yokoso (an infrastructure fingerprinting project) and was the founder and lead of the BASE project for Snort. Kevin has served as an expert witness in court cases involving cybersecurity. Kevin began his IT career in system administration and application development. He went on to build incident response and forensic teams, architect security solutions for large enterprises and pen test everything from government agencies to Fortune 100 companies. He is the author of three SANS Institute classes: SEC542: Web Application Penetration Testing and Ethical Hacking, SEC642: Advanced Web Application Penetration Testing, and SEC571: Mobile Device Security. In 2010 Kevin established Secure Ideas, LLC. Kevin understands that the path to security is through education and information sharing. As a result, Kevin participates in various podcasts and training activities. He is regularly invited to keynote cybersecurity events like ISSA, GrrCon, and ShowMeCon. He has also spoken at many conferences including RSA, DEF CON, OWASP, DerbyCon, ShmooCon, and BlackHat. When not immersed in consulting, testing, and educating, Kevin loves spending time with his daughters and exploring woodworking and costuming with the 501st Legion.

Underground Insights: Criminal Exploitation of Multi-Factor Authentication

Adam Bumgarner

As organizations increasingly deploy or modify existing multi-factor authentication (MFA) techniques, cybercriminals are increasingly exploiting MFA. Regardless of whether organizations' use of MFA requires SMS messages, authentication applications, or hardware-based security keys, Accenture Cyber Threat Intelligence (ACTI) is observing malicious actors buying and selling MFA bypass techniques, in addition to actors sharing and seeking information on the topic. In this talk, ACTI examines the underground activity focused on bypassing MFA, as well as threat actors buying and selling services to bypass MFA, including modified versions of publicly available tools, mobile malware, credential stealers, SIM swapping, Signaling System 7 (SS7) exploits, and services for bypassing MFA to hack cryptocurrency wallets.

Adam Bumgarner currently works as an intelligence analyst at Accenture Security and brings nearly 15 years of experience in researching and analyzing financially-motivated cybercrime. Adam focuses primarily on English and Russian-language cybercrime research and analysis, including researching threat actors and groups, emerging trends and tactics, techniques and procedures (TTPs).

Adam has also conducted a great deal of research focused on hacktivism. Additionally, Adam possesses an in-depth knowledge of the evolution of criminal forums and markets.

Network Segmentation without a Network Engineer - Mike Burns

Network Segmentation is a defense-in-depth security methodology that has a proven track record of making it difficult for attackers to laterally move throughout networks in their attempts to escalate privileges, gain access to sensitive systems, and in some cases to deploy ransomware. Traditionally, network segmentation strategies have been designed and deployed by Network Engineers. The first step in the process typically requires designating security zones. Then using a series of internal firewalls, Virtual LANs (vLANs) and routers, communication between zones is limited by access lists and routing rules. These kinds of projects tend to be very resource intensive and met with many challenges.
As the abstract describes, centrally managing the Windows Host-Based Firewall and Active Directory Security Groups can over come those challenges.

Mike Burns is a Senior Technical Architect that has helped many organizations implement recommendations for enhancing detections, hardening environments, and bolstering security governance during Incident Response and proactive engagements. Mike has experience performing assessments for network architecture, Microsoft technologies (Active Directory, PKI), and cloud services (Microsoft 365, Azure, Amazon Web Services). Mike has served as a leader to develop, implement, and manage organizational vision and strategy to reduce risks, improve incident response capabilities, and enhance enterprise networks defensive resiliency.

Scaling the Security Wall: Agile Threat Modeling for Complex Systems - Vineeth Sai Narajala

This talk explores the urgent need for a paradigm shift in threat modeling to address the complexities of large-scale systems. Adding more security bottlenecks to the development process is not only expensive but also risks losing developers' trust. However, identifying security issues later in the Software Development Life Cycle (SDLC) or after launch proves to be even more expensive. Threat modeling provides an ideal and cost-effective approach to incorporating security into the development process, ensuring it does not impede the rate of progress. The first part of the presentation delves into the challenges presented by cloud architectures, microservices, and rapid development practices, highlighting the shortcomings of traditional threat modeling approaches like STRIDE and DREAD. It also presents ways to integrate a fast and scalable threat modeling stage into the SDLC.

Following that, the talk unveils strategies for effective threat modeling at scale, emphasizing the importance of automation, secure design principles, and the integration of builder-focused security tools into agile and DevOps practices. It includes dissection of real-world case studies that offer concrete insights into organizations that have successfully implemented threat modeling at scale. Furthermore, this talk examines the overcoming of challenges, the fostering of a cultural shift towards security, and the assurance of efficient resource allocation.
Attendees will leave with a clear understanding of the critical need for threat modeling at scale and practical insights to enhance security in their large-scale systems.

As an Application Security Engineer at Amazon Web Services (AWS), I specialize in core Data Analytics services such as EMR, Athena, and LakeFormation. Prior to my current role, I held positions in Pentesting and Threat Intelligence. Additionally, I gained valuable experience in Business Recovery and Disaster Recovery, particularly in mitigating ransomware attacks during my tenure at Nordstrom.

Identifying and Securing Psychologically Vulnerable Users - Ira Wrinkler

Studies show that 85-95% of attacks start with an exploited user. Also, studies indicate that a small number of users create most of the losses. One study found that 4% of users cause 80% of damage. As a potential attacker or defender, you clearly want to find those most vulnerable users. The question is, how do we find those 4%? Then how do we either target those users or better secure the organization against them? Attackers, including red teams, perform spear phishing to targets without regard to levels of susceptibility. Defenders don't differentiate the levels of controls applied to users, which results in wasteful efforts that aggravate otherwise aware users. To identify users highly susceptible to phishing attacks, a study was performed, partially funded by the US National Institute of Standards and Technology, where subjects were administered a variety of psychological assessments and were then sent a series of phishing messages over several months. Based upon those phishing messages, user susceptibility was determined. Personality traits of the subjects was then compared to their level of phishing susceptibility.

were indicative of phishing susceptibility; low locus of control and high levels of neuroticism as measured on the Big 5 personality test. Machine learning techniques were then applied to classify phishing susceptibility, with 100% accuracy, based on 5 personality traits: locus of control, depression, self-discipline, communications, and anxiety. While attackers (or even cybersecurity programs) can't administer psychological assessments, there are social media indicators of these traits. Indicators include, Frequent negative posts, Indications of social isolation, Sleep disturbances as demonstrated by posting at late hours, High levels of personal disclosure, and Posting many selfies. This information is rarely considered in attacks.

Ira Winkler, CISSP is the Field CISO for CYE Security, former Chief Security Architect at Walmart, and author of You Can Stop Stupid, Security Awareness for Dummies, and Advanced Persistent Security.

Everything You Didn't Want to Know About CVE - Paul Asadoorian

In the past year (or so), many events have highlighted issues with vulnerability disclosure and CVE. This makes the defender's jobs difficult as evaluating and prioritizing remediation for vulnerabilities is a complex and time-consuming task. In this talk, I will discuss in detail several different events that exemplify the shortcomings of vulnerability disclosure and specifically the CVE process

Paul Asadoorian is currently the Principal Security Evangelist for Eclypsium, focused on firmware and supply chain security awareness. In 2005 Paul founded Security Weekly, a weekly podcast dedicated to hacking and information security. In 2020 Security Weekly was acquired by the Cyberrisk Alliance. Paul is still the host of one of the longest-running security podcasts, Paul's Security Weekly, he enjoys coding in Python & telling everyone he uses Linux.

The Fellowship of the Ring0 - Dana Behling

The Common Vulnerability Scoring System (CVSS) is a widely recognized framework utilized by professionals to quantitatively assess the risk associated with known software vulnerabilities. However, risk is inherent to all components of any interconnected system, not just those with Common Vulnerabilities and Exposures (CVEs). Most notably, it is easy to see how "living off the land" binaries and particularly vulnerable drivers increase exposure, but there is no current method of quantifying risk for these. Drivers in particular and by their nature require privileged access to the protected parts of the operating system and underlying hardware, so should be included in risk assessments. The site loldrivers.io exists to address this issue and provides a list of drivers with known vulnerabilities or malware associations, but scrolling down the length of the list immediately brings to mind additional questions. Which of these drivers pose the greatest threat? Should they all be added to the blocklist?

Introducing Driver Risk Score (DRS) – a simple score that quantifies exposure. DRS takes into account seven characteristics that include the driver's security attributes and real-world prevalence metrics. Each characteristic is assigned an easy-to-understand score, ranging from 0 (indicating no risk) to 5 (signifying the highest degree of risk), which are combined and evaluated to achieve the DRS. This holistic appraisal score makes plain the security implications of a driver, eliminating the need for guesswork and facilitating informed decision-making.

Dana Behling is a cyber security researcher at Carbon Black by day, and a science fiction and fantasy enthusiast by night. With a keen eye for digital threats and a passion for exploring otherworldly realms through literature, Dana thrives on the cutting edge of technology while escaping into imaginative worlds beyond. Whether decoding complex cyber puzzles or unraveling the mysteries of distant galaxies, Dana brings a unique blend of analytical prowess and creative insight to every endeavor. Join Dana on a journey through the digital frontier and beyond.

Cloud IAM Strategy for Multicloud and Hybrid Environments: Risks and Gaps - Cassandra Young, Christian Nicholson

In this talk, we'll discuss the multicloud threat landscape and walk through strategic, process and technical gaps in Identity and Access Management. From the provisioning and management of privileged accounts, to determining privilege and creating efficient logging and monitoring, you'll come away with a better understanding of how to secure IAM to protect your multicloud environment.

For those in the hacking community, having awareness of the security implications of these environments is an important part of incident response, particularly because of the recent increase in cloud-savvy threat actors.

Cassandra (aka muteki) works full time in cybersecurity consulting, specializing in proactive cloud security technical assessments for Azure and GCP. She holds a master's degree in Computer Science, focusing on cloud-based app development and academic research on serverless security and privacy/anonymity technology.As one of the directors of Blue Team Village, she also works to bring free Blue Team talks, workshops and more to the

broader security community.

Cybersecurity veteran, multi-cloud maestro, passionate problem solver. Christian's career has been a relentless pursuit of security excellence, spanning every realm from consultancy owner and educator to Fortune 5 leader and architect, and spanning across offense, defense, intelligence, and secure design and architecture domains, Christian has honed their skills by diving headfirst into diverse assessments, no challenge too big or too small. Currently Owner and Partner at Indelible Security LLC.

Graph Activity Logs for Incident Responders - Pallav Gurung

Recently, threat actors like Storm-0558 and APT-29 have been identified for misusing OAuth applications via Graph API roles. Additionally, the Solarwinds incident highlighted instances where actors exploited Entra ID applications to access sensitive data. Given this evolving threat landscape, it becomes imperative for investigators to understand identity management practices, recognize the significance of Microsoft Graph, and explore new sources for incident response (IR) purposes. This paper examines essential Azure log sources crucial for organizational security. Notably, MailItemsAccessed logs within the OfficeActivity table have proven instrumental for investigators, offering valuable insights into accessed and potentially exfiltrated data by the aforementioned threat actors. Furthermore, the introduction of Microsoft Graph activity logs has been positively received by the community. These logs enable users to monitor all requests to Microsoft Graph within their tenant, facilitating enhanced visibility and comprehension of environment activities. The research also delves into how attackers exploit environments using familiar tools and the traces they leave behind.

Pallav is a cyber security professional with 10 years of experience in the financial services industry. Started his career as an info sec analyst and has worked in different roles like threat hunt, detection engineering and DFIR. Currently he focuses on Cloud security and holds the CCSP. He recently moved to the US and loves to travel and attend security conferences.

CI/CD talent development pipeline - Chris Foulon

Using the CI/CD pipeline analog, let us apply it to the concept of talent development and pipelining new candidates to integrate into the workforce as we continuously develop others. This concept can be used at both the micro stages of particular companies or the macro stages of workforce development at the state or national level.

Christophe Foulon, founder and cybersecurity coach at CPF Coaching LLC, brings over 15 years of experience as a vCISO, information security manager, adjunct professor, author, and cybersecurity strategist, and a passion for customer service, process improvement, and information security. He has also spent over ten years leading, coaching, and mentoring people.

As a security practitioner, Christophe is focused on helping businesses tackle their cybersecurity risks while minimizing friction, resulting in increased resiliency, and helping to secure people and processes with a solid understanding of the technology involved. He gives back by producing a podcast, "Breaking into Cybersecurity," focused on helping people transition into the cybersecurity industry by sharing the stories of those who have done it in the past five years to inspire those looking to do it now. He also co-authored "Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level" and "Hack the Cybersecurity Interview: A Complete Interview Preparation Guide for Jumpstarting Your Cybersecurity Career".

Top Ways I Still Hack Your Company (and How-to Defend Against Them) - Bennet Warner

In this technical deep-dive, we explore the landscape of current vulnerabilities and weaknesses based on extensive field experience penetration testing. This session focuses on persistent vulnerabilities that continue to challenge application and network security defenses into 2024. We'll dissect common penetration test successes, shedding light on enduring issues like authentication/authorization

Bennett Warner is the Penetration Testing Practice Leader at RISCPoint. His expertise is built on a foundation of experience working in both software development and penetration testing with concentration in application security. Prior to RISCPoint, Bennett worked in the defense industry as a software engineer and taught cybersecurity as an adjunct instructor for the University of Pennsylvania.

Beyond Booze: Rethinking Networking Events for a Healthier Security Culture

Working in security can be stressful, and substances are often used as coping mechanisms. This is especially prominent at networking events, which almost always involve alcohol. But it doesn't have to be that way. I'll share tips for employers and event organizers who want to make their events more inclusive, and some un-scary steps individuals can take to move towards a more sober lifestyle.

Jen VanAntwerp is the founder of Sober in Cyber, a nonprofit on a mission to provide alcohol-free events and community-building opportunities for sober individuals working in cybersecurity. She is deeply passionate about breaking the stigma surrounding addiction recovery. As the owner of JVAN Consulting, she provides marketing consultation to cybersecurity startups. Jen also enjoys sewing, volunteering, and working on her beloved '65 Ranchero.

SUNDAY PRESENTATIONS

From Aspire to Hire: Navigating Your First Cyber Job - Sully Vickers

Begin your cybersecurity journey! Learn tips for landing your first job, master self-marketing, excel at networking, and stand out in the job market. Gain insights on vital skills and certifications to kickstart your career. Whether a recent grad, career switcher, or student, this session offers actionable steps to transform your dreams into reality.

Sully Vickers, a committed Cyber Researcher and Developer at Leidos, is currently in their first year as a Bachelor's Degree student at WGU. Sully's deep passion for cybersecurity and cyber education is unmistakable, demonstrated through active participation in speaking engagements and podcasts, showcasing a dedication to advancing knowledge in the field.

Securing generative AI: threats, old and new - Adam Swanda

Attacks on AI systems can generally occur in two ways; attacking the model or attacking the infrastructure and applications built to support and/or use the model. While infrastructure and application threats are more commonly known, models can introduce unique vulnerabilities specific to AI systems such as data poisoning, bias, adversarial attacks, and more. Developing applications around the models also has the potential to increase the attack surface with issues like insecure plugin design and indirect prompt injection. While more eyes have been on these issues as of late, especially with regards to Large Language Models, it's important for cybersecurity professionals to have an understanding of the unique threats presented, how they are similar or different from traditional cybersecurity, as well as where we can apply or expand on existing techniques and frameworks for defense and monitoring.

Adam Swanda is a threat researcher with over 10 years working in cybersecurity, largely focusing on tactical and strategic threat intelligence. Adam is currently working as an AI Security Researcher at Robust Intelligence. He recently released the open source project "Vigil", a Python library implementing various LLM defense measures for prompt injection and jailbreak detection.

Protect Your Most Sensitive Users With This One Weird Trick! - Jake Hildreth

Presenting that "One Weird Trick" of Active Directory security: The Protected Users Group (PUG)! It's been lingering in Windows Server since 2012 R2, but it's the undercover legend few have heard of —

This talk shines a spotlight on the PUG's impressive protections used to shield sensitive accounts from common attacks. Picture it as a crash course on how PUG thwarts attackers, complete with demos that'll make you want to cheer. Yet, it's not all heroics; we'll explore the PUG's quirks and constraints, because even powerful tools have their limits. Stay tuned for the ultimate guide on slipping your VIPs into this exclusive club, using a not-so-secret approach. Wrapping up the talk will be a chat about PowerPug, the trusty sidekick that guides admins through the process of adding users to the Protected Users Group safely.

Jake Hildreth is a man of many roles – devoted husband, fun-loving dad, seasoned IT expert. With 20+ years entrenched in IT, he currently leads Trimarc's Active Directory (AD) Security Assessment. Jake's daily mission involves bolstering the digital fortifications of major corporations, ensuring their AD security is rock solid. His creations, Locksmith and BlueTuxedo, attempt to alleviate the burden on overworked AD admins while his CISSP certification demonstrates his wide-ranging experience.

.

Using Bloodhound as a Defender: Tips from the Red Team - Andrew McNicol

Network defenders are often not armed with the right information to fix critical permission issues and general misconfigurations within Active Directory (AD). Many of these flaws lay dormant in the network for 10+ years until either an attacker or pentester takes advantage of the flaw. The reason for this is that these flaws don't show up in security checklists, or vulnerability scanners, which alone can be a daunting task to handle for a large enterprise. We often get in this mindset of "need to fix what the tool tells me" and if it's not a critical or high impact flaw coming out of a vulnerability scanner it just isn't addressed. When I take over an entire network I don't use a vulnerability scanner, or data the it provides.

This talk is aimed at providing defenders with an attacker perspective into their Active Directory (AD) environment. As part of the talk a tool will be released that automates numerous complex queries going through BloodHound data via Neo4j cypher queries.

Ad-recon is a tool designed to quickly triage BloodHound data (~2-4 seconds to run without pathing queries enabled) and will identify numerous security issues within the AD environment.

The talk will walk through each query the tool covers, why the data is interesting, discuss what could an attacker do, and what can a defender do to secure it. Ad-recon also supports printing out all these queries and descriptions to allow the user to modify them and make use in their own code, Neo4j interface, Cypher-Shell query, or BloodHound GUI.

Andrew McNicol has over 13 years of experience performing offensive serves as BreakPoint Labs (BPL) Chief Technology Officer (CTO). He holds dozens of industry recognized certifications (OSCP, OSCE, etc.), a B.S. from Towson University, M.S. degree from Capital Technology University. He's worked in DoD, Federal, Law Enforcement, and commercial sectors performing red teaming and penetration testing.

Sysmon or it Didn't Happen - Gerard Johansen

Out of the myriad of evidence sources, one that has gained traction as a solid go-to is Windows System Monitor. Providing insight into program execution, registry writes and DNS queries, Sysmon has quickly become the threat responder's friend. This session focuses on how to leverage Sysmon logs during an incident investigation to determine what actions a threat actor took on a system.

Gerard Johansen is a cyber security professional with over a decade of experience in Incident Response, Digital Forensics, Security Operations and Cyber Threat Intelligence. During his tenure in the cyber security field, Gerard has served as both a digital forensics and instruction analysis professional as well as an Incident Commander, managing large scale network intrusions and ransomware cases. Currently Gerard works within a Managed Detection and Response vendor where he works directly with customers providing consultation and guidance around forensics, log management and incident resolution. A frequent speaker, Gerard has presented at various conferences including SANS DFIR and Wild West Hackin' Fest. He is also completing a fourth edition of his book; Digital Forensics and Incident Response.

Who's going to secure the code our army of robots are going to be writing? - Arshan Dabirsiaghi

Large Language Models (LLM) are writing a significant portion of our code through tools like Copilot, and now promising new companies like Sweep are starting to write wholesale features for us. The LLMs are trained on the vulnerable code we've already written, so of course multiple studies have now confirmed that they offer the same vulnerability density. Security today is often already outnumbered by developers at rates like 1000:1. When we started to add LLMs to the developer toolchain, we began barreling towards a comically hopeless situation where the ratio of code developed vs. code secured is no longer tenable. There are too many humans involved in critical chokepoints that have no hope of meaningfully securing the deluge of code that is coming. I'd like the opportunity to make the case that the only way to keep up is with virtual security engineers, powered by a mix of LLMs and traditional technologies.This talk will illustrate the scale of the issues we are facing, new research into automated remediation and review, and include the demonstration and release of open source tools for building your own virtual security engineers.

Arshan is a security researcher pretending to be a software executive, with many years of experience advising organizations on code security. He has spoken at conferences like Bluehat, Blackhat and OWASP, and definitely wrote his own bio. He is also a co-founder of Contrast Security, a cybersecurity unicorn focused on vulnerability discovery through runtime instrumentation. He now serves as CTO of Pixee where he's done finding and asking about security issues -- he's just fixing it for you.

Purple Teaming 301 - Free attack simulation and control validation using At - Jason Wright

This presentation will be a technical demonstration. It will showcase how to leverage a completely free utility, Atomic Red, to run attack simulations safely in your own organization. Many organizations are puzzled at whether or not they are obtaining the most out of their in house SecOps / SOC teams, Managed Security Service Providers, or MDR/EDR suites. Atomic Red Team is an open-source library of tests that security teams can use to simulate adversarial activity in their environments. These tests map to the MITRE framework to validate control operation and verify alarms through detection mechanisms. Creating local accounts, domain accounts, Process Inject/Hollowing via Powershell and Obtaining Credentials from Password Stores. This presentation will cover why to run this type of simulation, the principles of purple teaming, the technical prerequisites to achieve this in a lab environment (great for students!) or a dev environment, the architecture of the lab in this use case, several Atomic Red simulations via recorded demos and finally how to use this information to improve an organizations detection and response program and get the most out of one's MSSP.

Jason Wright is an IT and Cybersecurity Professional with over a decade of experience across several industries, such as critical supply chain and financial sectors. Jason primarily serves as a Senior Security Engineer for Convera, a global finance organization, specializing in security operations.

Jason also serves as Adjunct Faculty at Chesapeake Community College in the Computer Science and Technology. Jason possesses several industry certifications, such as the CISSP and Sans GIAC GCIH among others. Jason currently lives in Delmar, Delaware with his wife.

TRAINING EVENTS

SecurityAI - Saturday

Trainer: Imani Palmer

Welcome to SecurityAI. The goal of this course is to inform on how artificial intelligence is becoming one of the major tools in our security arsenal. The problem is that, unless mom you have a specific type of degree, you are at the mercy of product vendors,collaborators, ChatGPT, or search engines to understand these concepts. This course demystifies artificial intelligence and its relationships.

This is an interactive course, with the goal of teaching security professionals how to implement AI in order to obtain valuable insights. This course will encompass various topics including: machine learning (ML), natural language processing (NLP), and large-language models (LLMs). The combination of AI and security allows the security community to move our assumptions, opinions and beliefs into knowledge.

No previous experience is necessary. Background understanding programming is very helpful, specifically Python.

Imani Palmer, a visionary in security data science, boasts a decade of honed expertise. Graduating from the University of Pittsburgh for undergrad, she pursued her passion, earning a Ph.D. in Computer Science from the esteemed University of Illinois at Urbana-Champaign. With an unwavering drive to fuse security and data science, Imani stands at the forefront of innovation, reshaping the landscape of security.

Threat Actors: Gotta Catch Them All! - Sunday

Trainer: Marcelle Lee

How do we quantify threat actor activity? There are many ways to do this, but I like mapping to various frameworks and models. In this session we will use tools such as MITRE ATT&CK, Diamond Model, Pyramid of Pain, and more in an effort to categorize threat activity. While not a workshop, we will talk through practical application.

As a security researcher who regularly examines tactics, techniques, and procedures (TTPs) of threat actors, I have learned the value of applying frameworks. This will be an interactive session where audience members can chime in with their experiences.

Marcelle Lee is a principal information security engineer and the lead for threat research and operations at Equinix. She is also an adjunct professor and training consultant. She specializes in security research and digital forensics and has worked in both the government sector and private industry. She has been involved with many industry organizations, working groups, and boards, including the Women's Society of Cyberjutsu, the NIST Cyber Competitions Working Group, and the Cybersecurity Association of Maryland Advisory Council. She also both builds and participates in cyber competitions. Marcelle has earned the CISSP, GCFA, GCIA, GCIH, GPEN, GISF, GSEC, GCCC, CIHFI, CIEH, CSX-P, CCNA, PenTest+, Security+, Network+, and ACE industry certifications. She holds four degrees, including a master's degree in cybersecurity. She has received the Chesapeake Regional Tech Council Women in Tech (WIT) Award and the Volunteer of the Year award from the Women's Society of Cyberjutsu. Marcelle frequently presents at conferences and training events and is an active volunteer in the cybersecurity community.

Securing the Cloud with Cloud Threat Intelligence and Open Source Security - Sunday

Cloud cyberattacks targeting enterprise environments have nearly tripled this past year, and cloud misconfigurations have become an open door to threat actors. Understanding cloud threat actors and how they are breaching misconfigured cloud environments will help security professionals defend cloud environments.

This workshop will showcase the cloud-conscious adversary and how to run cloud security assessments using open source tools Prowler and ScoutSuite. We will provide a demo on how to use these tools, and then train participants to conduct their own cloud security assessment using our test environment. We will review the output of the Prowler and ScoutSuite assessments, and identify vulnerabilities that cloud-conscious adversaries are known to target.

Trainer: Natalie Simpson & Nivu Jejurikar

Natalie Simpson is a Consultant at CrowdStrike where she assists customers with optimizing Falcon applications to enhance their security program. Natalie is certified as a CrowdStrike Cloud Specialist (CCCS), and helps customers deploy Falcon Cloud Security to secure and manage their cloud environment.

Nivu Jejurikar is a Senior Consultant at Mandiant within Google Cloud where she focuses on proactively helping clients identify and mitigate cyber risks. Prior to joining Mandiant, Nivu worked with customers of varying size and industry vertical through CrowdStrike's proactive services team. Nivu holds the Security+, CEH, Splunk Core Certified Power User, and AWS Cloud Practitioner certifications. She loves to spend time outdoors and read fiction novels in her spare time.

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES