★★★ BSIDESCHARM ★★★

DFIR & STORAGE ALMANAC

COMPLETE FORENSIC TECHNIQUES

2000 - 2050

THANKS TO OUR SPONSORS!

Morgan Stanley

flare

CLEAREDGE
people. technology. integrity.

BLACK HILLS
Information Security
• 2008 •

DTRSEC
REnigma

SANS
OFFENSIVE
OPERATIONS

Pixee

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

ThreatConnect.

augustschell
++

SILVEREDGE

ALTUS
CONSULTING

MetaCTF

WarCollar
industries

Reach

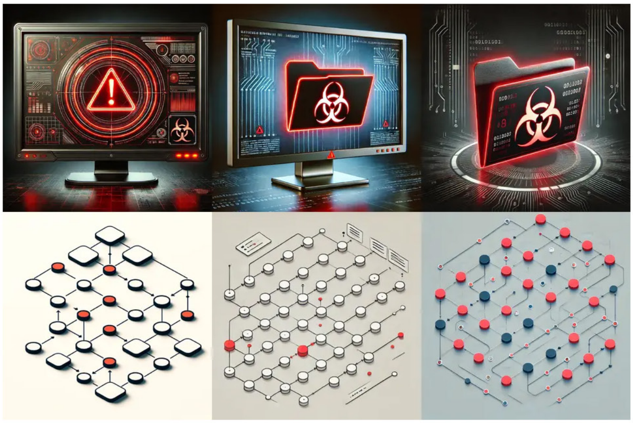
nDepth™
SECURITY

TABLE OF CONTENTS

DTRSEC REnigma

Record execution.
Replay perfectly.
See everything.
Get the root cause.
Validate your rules.

- Web GUI
- Python / Go API
- REST API



Record. Replay. Understand.

dtrsec.com youtube.com/@dtrsec sales@dtrsec.com

OPEN FOR CONSULTING

Black Hills InfoSec

SERVICES

- Penetration Testing
- Red Teaming
- ACTIVE SOC
- Blue Team Services
- Purple Teaming
- ANTISOC (Continuous Penetration Testing)
- Incident Response
- Consulting
- Training
- IR Tabletop Exercises
- AI Model Security Assessment
- Strategy, GRC (Governance, Risk, Compliance)and Privacy.

Learn More:

BLACK HILLS Information Security

CONTACT US

701-484-BHIS
consulting@bhis.co

WELCOME TO BSIDESCHARM 2025!

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 challenges. 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.

We'd also like to welcome this year's charities! Please visit Sober in Cyber, ISSA, WiCyS, and HTCIA, 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.

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 2025 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 BSidesCharm 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: Morgan Stanley, August Schell, SilverEdge, Atlus Consulting and John Hopkins University Applied Physics Laboraroty.

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!

Career Coaching and Resume Reviews

Time Slot	Event
1:00 PM – 2:15 PM	Career Coaching and Resume Reviews
2:15 PM – 3:00 PM	Breakout Talks
3:00 PM – 5:00 PM	Career Coaching and Resume Reviews

NEW THIS YEAR: Breakout Sessions with Jennifer Havermann and John Stoner, covering important topics like Reputational Impact on Career and Interview Strategy.

Attendees must visit all Hiring Village booths and collect a stamp from each one before visiting with the Career Coaches and Resume Reviewers.

Hiring Village Participating Companies

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SILVEREDGE

ALTUS
CONSULTING

augustschell

Morgan Stanley

Mental Health Hackers Village

2nd Floor Amphitheater, 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.

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

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

IoT Village

2nd Floor Duncan Room, Saturday and Sunday

Will be offering a different activity on each day

Saturday:

Packets, Protocols, and Pwnage: Assembling your own Packet Hacking Toolkit
Intercepting, analyzing and crafting specialized packets using a variety of applications (e.g. Browser Built-in Tools, Burp Suite, Linux tools like Curl/Wget, and Python3). We will provide a few stations, but we encourage attendees to bring their own laptops. This will run all day Saturday.

Sunday:

IoT Village Hackalong: This activity is designed for entry-mid level hackers. IoT Village has created a custom vulnerable web app that attendees will be guided through to discover vulnerabilities. You will work with the instructor and on their own to learn about how to adopt the “”think like a hacker”” mindset, and also poke around in a system that has over 40 vulnerabilities.

Aerospace Village

1st Warfields Ballroom, Saturday and Sunday

Will be offering two activities:

Bricks in the Air – A Hands-On Aerospace Cybersecurity Experience

Bricks in the Air is an engaging, interactive activity hosted by the Aerospace Village, designed to teach participants the fundamentals of low-level aerospace communication protocols. In this immersive experience, participants learn how to inject custom commands into avionics systems, mirroring real-world cybersecurity challenges in aviation. The commands issued are then reflected in real-time on a connected Lego aircraft, offering a tangible and visual demonstration of how cybersecurity vulnerabilities can affect aerospace systems.

By combining theory with practical application, Bricks in the Air equips participants with valuable skills in aerospace cybersecurity, problem-solving, and understanding the complexities of modern aviation systems.

Live ADS-B Data Demo – Understanding Vulnerabilities in Aviation Surveillance

The Live ADS-B Data Demo offers participants a real-time display of Automatic Dependent Surveillance–Broadcast (ADS-B) signals, commonly used for tracking aircraft position, speed, and other critical flight data. Through this demo, attendees can observe how ADS-B data is transmitted openly and unencrypted, providing an opportunity to discuss the potential vulnerabilities inherent in this widely-used aviation surveillance technology.

By showcasing live ADS-B transmissions, the demo highlights the ease with which anyone with the right equipment can intercept, manipulate, or spoof ADS-B signals. This serves as a valuable conversation starter on the risks posed by these vulnerabilities to aviation safety and security, and how they can be mitigated through better encryption, authentication, and monitoring solutions.”

Radio Frequency Hackers Village

1st Floor Warfields, Saturday and Sunday

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. 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 2025. 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 2025 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. We are the original creators of the WiFi Capture the Flag, 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

Cloud Village

2nd Floor Grason, Saturday and Sunday

Cloud village is an open space to meet folks interested in offensive and defensive aspects of cloud security. The village is home to various activities like talks, workshops, CTFs and discussions targeted around cloud services.

If you are a professional who is looking to gain knowledge on securely maintaining the cloud stack and loves to be around like-minded security folks who share the similar zeal towards the community, Cloud Village is the perfect place for you.

Breach Village

2nd Floor Burke, Saturday and Sunday

Breach Village features Hack the Case, a fast-paced, hands-on breach and hacking game. Participants can take on physical security challenges, such as lockpicking, sensor avoidance, and digital face spoofing, or attempt to hack the web application and backend systems connected to the case. The game loops every five minutes, with sound and visual cues signaling errors and failures.

The game is designed to be both fun and educational, showcasing real-world security concerns around deployable “fly-away” kits. Difficulty scales based on participant skill level, with entry-level and advanced lock challenges, as well as escalating digital hacking objectives. The cyber range Kleared4 will host cyber-focused participants, and a CTF challenge tied to this effort may also be available during BSides Charm.

Makerspace Village

1st Floor Warfields, Saturday and Sunday

The Makerspace Village features hands-on demonstrations and interactive displays covering a range of DIY and hacker-space projects. Stations include 3D printing, crafting, a Lockpicking CTF, and a Meshtastic demo, showcasing open-source mesh networking. Attendees will also find the UAS Trophy Table, highlighting past projects, and a sticker wall for adding their own contributions.

Equipment on display includes different types of 3D printers and a plasma speaker, but no soldering or high-temperature work is planned.
Meshtastic devices may be available for donation, with proceeds supporting Unallocated Space (UAS), a local non-profit hackerspace.

SANS Offensive Operations Village

2nd Floor McIntosh, Saturday Only

Join the SANS Offensive Operations Village to engage in a Capture the Flag (CTF) event that challenges your skills in network penetration testing, web, and binary exploitation, as well as programming and other offensive security disciplines.

Charities

WiCyS

The Women in Cybersecurity Mid-Atlantic Affiliate (WiCyS MAA) is a regional affiliate that covers these geographic areas: District of Columbia, Maryland, and Northern Virginia. As the first affiliate founded under WiCyS, we will undertake activities to promote, educate, recruit, retain, and advance women in cybersecurity. WiCyS MAA offers mentoring, learning, networking and career development to all professionals in various stages of their cybersecurity careers. Whether you are a student just considering a career in cybersecurity or an experienced leader in the cybersecurity workforce, WiCyS provides tangible benefits and a supportive community.

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

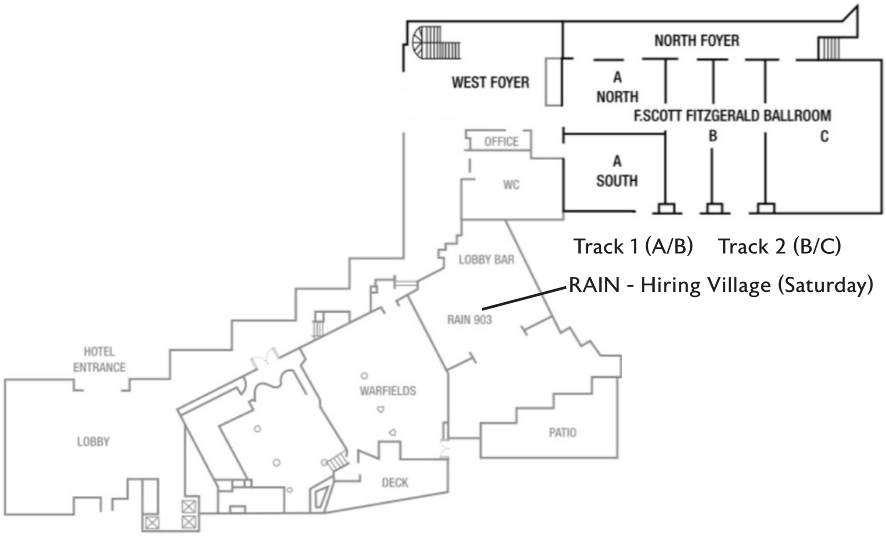
HTCIA

The High Technology Cyber Investigation Association (HTCIA) was founded more than 40 years ago to provide education and collaboration to our global members who are involved in cyber investigations. We are an organization that aspires to help all those in the cyber and high technology field by providing extensive information, education, collective partnerships, mutual member benefits, astute board leadership, and professional management. HTCIA is a registered not for profit association. Our chapter includes Maryland, DC and Virginia.

Sober in Cyber

Sober in Cyber is a volunteer-led nonprofit organization committed to creating alcohol-free events and building a community for sober and sober-curious individuals in cybersecurity. With a mission to provide a comfortable platform for professional networking without alcohol, the organization plays a vital role in fostering inclusivity within the cybersecurity industry. Join the movement at https://www.soberincyber.org/

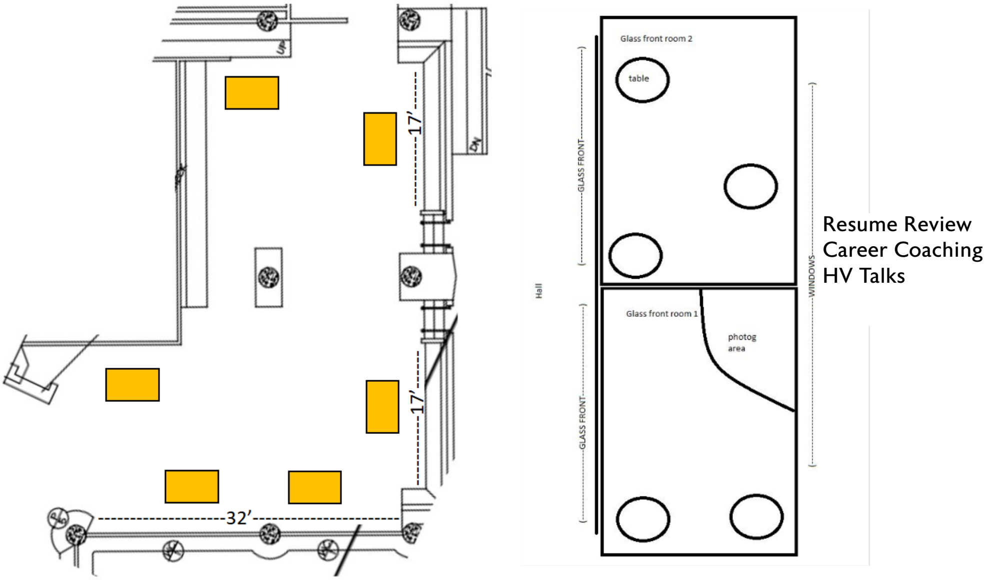
PLAZA LEVEL



Track 1 (A/B) Track 2 (B/C)

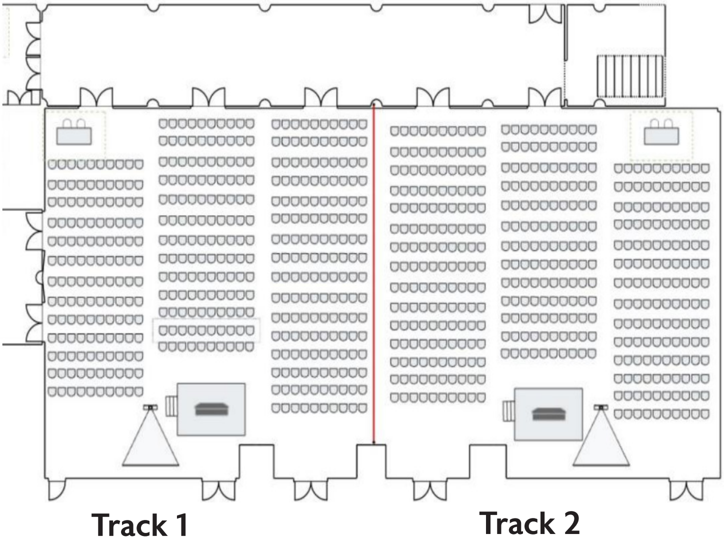
RAIN - Hiring Village (Saturday)

Rain (Restaurant) - Hiring Village

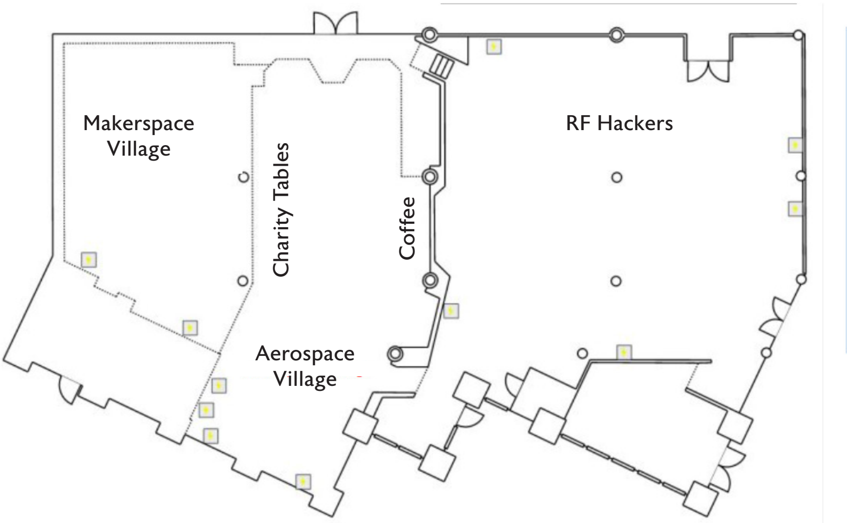


Resume Review
Career Coaching
HV Talks

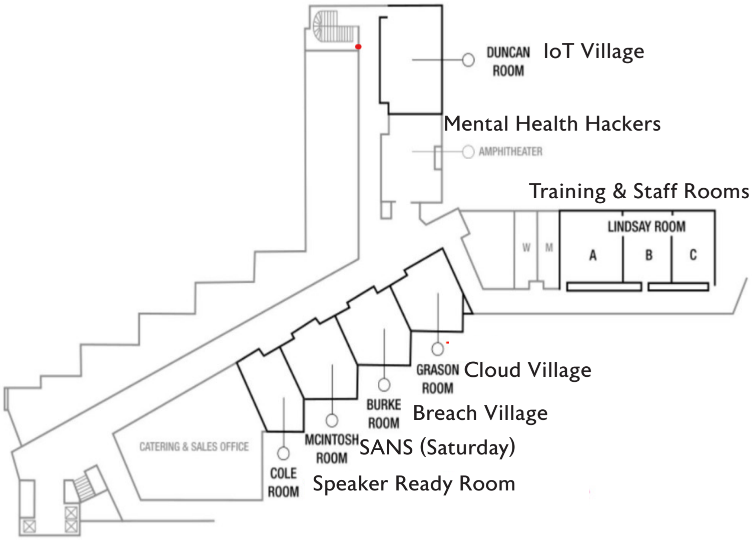
Fitzgerald Ballroom



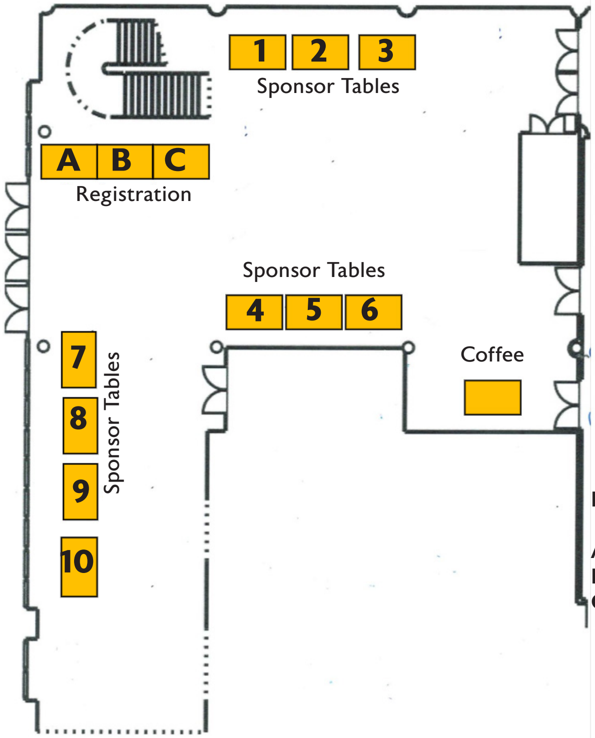
Warfields Ballroom



SECOND LEVEL



West Foyer



Sponsors Village tables key

1. **Black Hills Information Security**
2. **Johns Hopkins Applied Physics Laboratory**
3. **Clear Edge IT**
4. **Pixee**
5. **Flare Systems**
6. **Morgan Stanley**
7. **Deterministic Security**
8. **SANS OffSec**
9. **Threat Connect**
10. **Aikido Security**

Registration Key:

A. Attendee Registration
B. Attendee Registration
C. Sponsor Registration

Harry Coker

KEYNOTE SPEAKER

Harry Coker was appointed by MD. Governor Wes Moore as Secretary of the Maryland Department of Commerce in January 2025. Prior to this appointment, Coker served as the United States National Cyber Director from 2023-2025, serving as principal advisor to the President of the United States on cybersecurity strategy and policy.

Coker is a graduate of the United States Naval Academy, the Naval Postgraduate School, and Georgetown University Law Center. After serving nearly 20 years as a naval officer, retiring in 2000 with the rank of commander, Coker joined the United States Central Intelligence Agency, spending 17 years in leadership posts in the agency's Directorate for Digital Innovation and Directorate of Science and Technology. In addition, he served as the agency's director of the Open Source Enterprise and deputy director of the CIA's Office of Public Affairs. From 2017-2019, Coker served as executive director of the United States National Security Agency—the agency's third-highest ranking post—and was responsible for supporting the strategic and day-to-day leadership of the NSA.

Coker's distinguished service and leadership within the national intelligence community has earned him a number of awards, including the National Intelligence Distinguished Service Medal, the NSA Director's Distinguished Service Medal, the Presidential Rank Award, and the CIA's prestigious Don Cryer Award.

TALK SCHEDULE

SATURDAY

Time Slot	Track 1	Track 2
08:30 - 17:00	Registration Open	
10:00 - 11:00	Keynote	
11:00 - 11:30	Visit Our Sponsors and Villages	
11:30 - 12:00	Beyond Tor and VPN: Protect Your Privacy With Decentralized Mixnet	Cyber Deception in GCP with Generative Traps
12:00 - 13:00	Fight Stealth with Stealth: Detecting post-breach activity in the Cloud	Closing the Visibility Gap: Threat Hunting with Hawk in the Microsoft Cloud
13:00 - 14:00	Lunch on Your Own	
13:00 - 17:00	Hiring Village Open in RAIN	
14:00 - 15:00	Career Campaigns: Changing Your Professional 'Class' for an InfoSec Role	Building Against a Breach.... Out of a disclosure?
15:00 - 16:00	When The Fall Is All There Is – How to Lose a Gig Without Losing Your Mind	Tinker Tailor LLM Spy: Investigate & Respond to Attacks on GenAI Chatbots
16:00 - 17:00	Beyond the Breach: Securing Political Parties in the 2024 U.S. Election	A Theme of Fear: Hacking the Paradigm
17:00 - 17:30	AI Agents Could Be Running Your SOC To Prevent Cyber Attacks	Filling Gaps in AI Governance: How ISO/IEC 42001 Shapes the Future of AI Ri
1730 - 1800	How to Build Authentic Sock Puppets with Your Neighbors' Yard Sale Junk	How to plan for your security career advancement
18:00 - 20:00	BSidesCharm Happy Hour	
19:00 - 21:00	PianoCon	
20:00 - 23:00	BSidesCharm Party	

SUNDAY

Time Slot	Track 1	Track 2
09:00 - 14:30	Registration Open	
10:00 - 10:30	JMP Into Malware Analysis	Starting a SBOM Programme - The Pain Is Probably Temporary
10:30 - 11:30	What's in the Cloud?	Red Teaming: A New Perspective for Intern Projects
11:30 - 12:00	Threat Modeling Meets Model Training: Web App Security Skills for AI	Think You're Stealthy? How to Detect Attacks in AD
12:00 - 13:00	A Grounded Approach to AI and LLM Security	Supercharge Your Workflow: Using WhiteRabbitNeo for AI-Powered Analysis
13:00 - 14:00	Lunch on Your Own	
14:00 - 15:00	SQL injection is a thing of the past, and other lies we tell ourselves	A Tale of Two Incidents: Responding to Akira Ransomware
15:00 - 16:00	Inch By Inch: a Case Study in Maintaining & Scaling a Modern XDR Product	Past, Present and Future of Automatic Code Remediation
16:00 - 16:30	Closing Ceremony	

TRAINING SCHEDULE

SATURDAY

Time Slot	Training - Lindsay Room
10:00 - 18:00	AD Security 101

SUNDAY

Time Slot	Training - Lindsay Room
10:00 - 13:00	Career Campaigns: A Tabletop RPG Workshop
13:30 - 16:30	Web Application Penetration Testing

Rose-Gaëlle
Technology

SATURDAY PRESENTATIONS

Beyond Tor and VPN: Protect Your Privacy With Decentralized Mixnet - Alexis Ciao

The internet is filled with prying eyes. While several well-established tools including TOR and VPNs offer certain degrees of privacy, they all have limitations that could leave users vulnerable to advanced attacks. In this talk, I'll discuss the foundations of a decentralized mixnet, how it performs against Tor and VPN, and how you can use it to protect your privacy.

Alexis Cao is a senior at Johns Hopkins University studying computer science. Her research interests include privacy and secure communication. She has volunteered at TraceLabs OSINT search party to find missing persons since 2021, and she has also volunteered at Physical Security Village, Red Team Village, and AppSec Village at DEFCON.

Cyber Deception in GCP with Generative Traps - Matt Maisel

Cyber deception is a ruse to mislead or disrupt adversaries by exploiting their cognitive biases. Traps— lures that detect adversary interaction— reinforce the seams in detection surfaces monitored by security operations teams. But deception management and orchestration is painful in practice. Cloud environments provide an opportunity to overcome some of these pitfalls. This talk defines cloud deception stratagems for the Google Cloud Platform. Each stratagem is motivated with the release of an open-source, deception management tool that programmatically generates cloud-native traps tailored to an organization's target personas, orchestrates engagements with specific stratagems, and sets up observability for detections.

Matt Maisel is a cybersecurity builder with over fourteen years in security operations, software engineering, and machine learning. His work spans data science and product development roles in cybersecurity startups. He's currently the Head of Research at Reach Security.

Fight Stealth with Stealth: Detecting post-breach activity in the Cloud - Jenko

Advanced and evolving cloud attacks (Blizzard) make breach seem inevitable. We describe a deception detection approach using canaries, with a bit of honey and razors, to implement stealthy tripwires to provide low-FP detections for post-breach lateral movement and privilege escalation. To move the security needle, we need to take a fresh look at defensive techniques that utilize red approaches like stealth and are based on the design of the target environments such as: restricted admin roles not used by valid users; honey resources (buckets, files) with detections to flag access; cached honey credentials; detection of enumeration of IAM permissions and resources. When properly applied to defenses, we can improve signal fidelity for detection of post-breach activity.

Jenko Hwong heads threat research at WideField Security, focusing on identity-based attacks and abuse. He's spent time in engineering and product roles at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

When The Fall Is All There Is – How to Lose a Gig Without Losing Your Mind - Danny Akacki & Jeff Man

Jeff Man and Danny Akacki bring decades of experience—and their own battle scars—to explore not just the why behind job loss, but how to navigate its emotional and practical fallout. From the shock of that final paycheck to the long weeks and months that follow, this session will offer real talk, resilience strategies, and a much-needed reminder: when the fall is all there is, how you land matters.

Jeff is a respected Information Security advocate, advisor, hacker, evangelist, mentor, teacher, international keynoter, speaker, former host of Security & Compliance Weekly, co-host on Paul's Security Weekly, Tribe of Hackers (TOH) contributor, including Red Team, Security Leaders, and Blue Team editions, and a member of the Cabal of the Curmudgeons. Jeff currently serves as a PCI QSA and Trusted Advisor for Online Business Systems, also a Grant Advisory Board Member for the Gula Tech Foundation, Advisory Board Member for the Technology Advancement Center (TAC), and is the Director of Diversity, Equity, and Inclusion for Hak4Kidz NFP. Over 40 years of experience working in all aspects of computer, network, and information security, including cryptography, risk management, vulnerability analysis, compliance assessment, forensic analysis and penetration testing. Certified National Security Agency Cryptanalyst. Designed and fielded the first software-based cryptosystem ever produced by NSA. Inventor of the "whiz" wheel, a cryptologic cipher wheel used by US Special Forces for over a decade currently on display at the National Cryptologic Museum. Honorary lifetime member of the Special Forces Association. Previously held security research, management and product development roles with the National Security Agency, the DoD and private-sector enterprises. Pioneering member of the first penetration testing "red team" at NSA. For the past twenty-eight years has been a pen tester, security architect, consultant, QSA, and PCI SME, providing consulting and advisory services to many of the nation's best known companies. (https://darknetdiaries.com/episode/83/)

Danny's career has run the gamut of cyber security. From hands-on-keyboard to positions in leadership, he's been on the outside looking in and the inside looking out. The horrors persist on both sides, but so does he.

Career Campaigns: Changing Your Professional 'Class' for an InfoSec Role - Stryker

Hack your way into a new cybersecurity career during this gaming-inspired interactive session, during which we'll transform your current resume's "character sheet" into a freshly reskilled or dual-classed hero, ready to take on any cybersecurity hiring process for your next – or first! – infosec campaign.

Stryker is a threat intelligence analyst at a major insurance company, where she translates technical research and qualitative intelligence into the "so what?" and "what now?" solutions that keep more people safe and secure. Feel free to say hi on LinkedIn or in the Lonely Hackers Club (LHC) Telegram chat, where she once (in)famously ranted about how commercial gun safes are insufficient for secure off-site data storage. Stryker lives in the Baltimore-DC area, growing parsley for swallowtail butterfly caterpillars and algae for neocaridina shrimp.

Red Teaming: A New Perspective for Intern Projects - Mia Hagood, Kenyan

Red teaming is an important consideration when training new software professionals, ultimately creating a generation of adversarial-minded engineers. We will present how this perspective was integrated in the Praxis internship project, enabling us to unveil vulnerabilities, research mitigations, and strengthen the resiliency of AI solutions.

Mia graduated from Virginia Tech majoring in computer science in May 2024. She was a summer intern at Praxis Engineering in 2023 and 2024 and worked on projects in data science, machine learning, and reverse engineering. Now, Mia is working as a full time Software Engineer for Praxis.

Tinker Tailor LLM Spy: Investigate & Respond to Attacks on GenAI Chatbots - Allyn Stott

It's coming, and you aren't ready—your first generative AI chatbot incident. GenAI chatbots, leveraging LLMs, are revolutionizing customer engagement by providing real-time, automated 24/7 chat support. But when your company's virtual agent starts responding inappropriately to requests and handing out customer PII to anyone that asks nicely, who are they going to call? You.

You've seen the cool prompt injection attack demos and may even be vaguely aware of preventions like LLM guardrails; but are you ready to investigate and respond when those preventions inevitably fail? Would you even know where to start? It's time to connect traditional investigation and response procedures with the exciting new world of GenAI chatbots.

In this talk, you'll learn how to investigate and respond to the unique threats targeting these systems. You'll discover new methods for isolating attacks, gathering information, and getting to the root cause of an incident using AI defense tooling and LLM guardrails. You'll come away from this talk with a playbook for investigating and responding to this new class of GenAI incidents and the preparation steps you'll need to take before your company's chatbot responses start going viral—for the wrong reasons.

Allyn Stott is a senior staff engineer at Airbnb where he works on the InfoSec Technology Leadership team. He spends most of his time working on enterprise security, threat detection, and incident response. Over the past decade, he has built and led detection and response programs at companies including Delta Dental of California, MZ, and Palantir. Red team tears are his testimonials.

Allyn has previously presented at Black Hat (Europe, Asia, MEA), Kernelcon, The Diana Initiative, Blue Team Con, Swiss Cyber Storm, SecretCon, Texas Cyber Summit, and BSides around the world. He received his Master's in High Tech Crime Investigation from The George Washington University as part of the Department of Defense Information Assurance Scholarship Program.

In the late evenings, after his toddler ceases all antics for the day, Allyn writes a semi-regular, exclusive security newsletter that you can subscribe to at meoward.co.

A Theme of Fear: Hacking the Paradigm - Dr. Catherine J. Ullman

The InfoSec industry was born out of fear. But fear is hard to manage: too much fear breeds paralysis, and too little fear breeds complacency. We will explore this history, consider how it shaped the industry, and how it's now in the way. Finally, we'll consider what the new paradigm could be, and most importantly – how to enable a security-minded culture without using fear.

Dr. Catherine J. Ullman is a security researcher, speaker, author, and Principal Technology Architect, Security, at the University at Buffalo with over 25 years of highly technical experience. In her current role, Cathy is a digital forensics and incident response (DFIR) specialist, performing incident management, intrusion detection, investigative services, and personnel case resolution in a dynamic academic environment. She additionally builds security awareness among faculty and staff which educates and informs users about how to prevent and detect social engineering threats, and how to compute and digitally communicate safely. Cathy has presented at numerous information security conferences including DEF CON and Blue Team Con. Cathy is a contributor to the O'Reilly title 97 Things Every Information Professional Should Know and the author of the Wiley title The Active Defender. In her (minimal) spare time, she enjoys visiting her adopted two-toed sloth Flash at the Buffalo Zoo, researching death and the dead, and learning more about hacking things to make the world a more secure place.

Closing the Visibility Gap: Threat Hunting with Hawk in the Microsoft Cloud - Jonathan Butler, Paul Navarro

Security teams often face the challenge of navigating complex cloud environments with limited visibility into potential threats. Commercial log aggregation and investigation solutions can be costly, putting a strain on budgets while still leaving gaps in coverage. Hawk bridges this gap by providing a free and open-source solution that automates the collection of essential logs from Microsoft Cloud environments. This talk will demonstrate how Hawk reduces investigation time, flags high-risk behaviors, and enables defenders to hunt for threats across the Microsoft cloud ecosystem.

Jonathan Butler is an active-duty Marine with over 20 years of experience in cybersecurity, specializing in cloud security, security automation, and threat hunting. As a core contributor to Hawk, his work enables security teams to streamline investigations and reduce reliance on costly commercial solutions. His background in software development and cybersecurity allows him to build automation-driven security tooling that enhances visibility and detection capabilities in complex cloud environments.

Paul Navarro, a Marine Corps veteran and Cybersecurity Chief Architect at Microsoft, is one of Hawk's core maintainers. He brings firsthand experience in Microsoft Cloud forensics and operationalizing security in cloud environments for customers. He has played a key role in shaping Hawk's development with a focus on detecting high-risk activities across Microsoft cloud services for cloud customers who need a place to start from. Paul's passionate about helping anyone who has an interest in security get into the workforce.

Beyond the Breach: Securing Political Parties in the 2024 U.S. Election - Andrew Schoka, Veronica Merril

In 2021, we presented at BSides Charm on the vulnerabilities plaguing state-level political party domains across the country. This year, we're back to share the evolution of that work into a non-partisan nationwide election cybersecurity initiative that discovered and shared thousands of vulnerabilities in political campaigns and party offices before the 2024 Election.

Andrew Schoka is a former U.S. Army Cyber Warfare Officer and is currently a graduate student at the University of Virginia. He served in a variety of offensive cyber operations assignments with the Election Security Group at U.S. Cyber Command, and later with U.S. Special Operations Command. Andrew is the co-founder of an election cybersecurity startup and teaches a graduate course on cybersecurity at the University of Virginia School of Engineering.

He holds a bachelor's degree in systems engineering from Virginia Tech, a master's degree in cybersecurity from Georgia Tech, and a number of industry security certifications.

Veronica Merril earned a double major in architectural history and music from the University of Virginia. She is pursuing her JD degree at the same institution, rendering her a "super Hoo." Through her work with Voterguard, she's solved the age old question, "how many engineers does it take to write a clear report?" Answer: None— there's always an editor involved.

AI Agents Could Be Running Your SOC To Prevent Cyber Attacks - Keyur Rajyaguru

It is becoming increasingly complex to defend against zero- to low-cost attacks generated by Threat Actors (TA) as they leverage sophisticated Generative AI (Gen AI)-enabled infrastructure. An orchestrated Workflow with a team of AI Agents presents an opportunity to respond better. To avoid burnout and alert fatigue of SOC analysts, a shift in strategy is required by automating routine tasks.

Keyur currently works with Walmart Global Tech as Lead Intrusion Analyst, and has keen interest in the safe use of AI systems. He is a mentor for future workforce on his webpage, www.topmate.io/kpr. Last year, SANS named him as a finalist in Rising Star Category of Difference Maker Awards 2024. He supports the infosec community by volunteering at local conferences, actively contributing to open source bodies (OWASP, Atomic Red Team, CoSAI), and as a panel member of Globee Cybersecurity Awards.

How to Build Authentic Sock Puppets with Your Neighbors' Yard Sale Junk - Tim Pappa

This industry cyber deception practitioner's short talk demonstrates how to build authentic online sock puppets using the cheap nostalgic junk we buy at yard sales to project the storyline and cultural depth of your sock puppet for defensive cyber deception.

Tim Pappa is an Incident Response Engineer – Cyber Deception Strategy, Content Development, and Marketing, with Walmart Global Tech's cyber deception team. Before Walmart, Tim was a Supervisory Special Agent and certified profiler with the FBI's Behavioral Analysis Unit (BAU), specializing in online influence and cyber deception. Tim is also a Senior Behavioral Consultant with Analyst1 and a Strategy and Statecraft Fellow with the Center for Strategic and International Studies.

A Grounded Approach to AI and LLM Security- Lucas Tamagna-Darr

With the emergence of Large Language Models, there has been a rapid acceleration in the development of AI capabilities. This brings with it many questions for security teams on how they should be thinking about AI security. While care should be taken on the development of LLM prompts, it is critical to not lose sight of the fundamentals to establish secure best practices.

In his role as a Senior Director of Engineering and Research Solutions Architect, Lucas Tamagna-Darr leads the automation and engineering functions of Tenable Research. Luke started out at Tenable developing plugins for Nessus and Nessus Network Monitor. He subsequently went on to lead several different functions within Tenable Research and now leverages his experience to help surface better content and capabilities for customers across Tenable's products.

Think You're Stealthy? How to Detect Attacks in AD - Rachit Arora, Sai Sathvik Ruppa, Aakash Raman

As Active Directory attacks rise, red teamers often focus on "pwning" systems, but real-world engagements require understanding the artifacts these tools leave. In " Think You're Stealthy? How to Detect Attacks in AD", we'll explore the workings of commonly used AD pentest tools and the artifacts they leave behind. Ideal for anyone looking to deepen their knowledge of defense in AD environments.

We're a team of three—one a University of Maryland alum (Aakash Raman), one a current student studying there (Rachit Arora), and another from Carnegie Mellon University (Sai Sathvik Ruppa) —coming together for our first talk at BSidesCharm.

After attending as volunteers in February 2024, we decided to face our fears and tackle imposter syndrome by sharing what we've learned. Two of us have earned OSCP, while one of us naturally gravitates toward blue teaming. Combining our mindset and research

SUNDAY PRESENTATIONS

Threat Modeling Meets Model Training: Web App Security Skills for AI - Breanne Boland

New specializations have emerged in this AI-adoring age, but where does that leave security practitioners? Good news: if you know web application security, you can secure AI applications too! This talk explores common web app security concerns that are relevant to any LLM-based app—and the handful of issues unique to AI—guiding the audience through ways to detect and mitigate them.

Breanne Boland is a product security engineer at Gusto. She's also done vendor security at Salesforce and spent time in the infra mines. Before that, she had a whole other career in online content, and she may never recover. When she's not encouraging engineers to do things a little differently than planned, she's writing speculative fiction novels, taking long walks around New York City, or saying hi to your pet on Zoom. She lives in Brooklyn, and you can find her @ toxoplasmosis@mastodon.social

Supercharge Your Workflow: Using WhiteRabbitNeo for AI-Powered Analysis - Bailey Williams

Pair hacking with WhiteRabbitNeo, an uncensored, open-source LLM trained on red team data, speeds up your process and reduces the tedium inherent in most security roles. Learn how WhiteRabbitNeo can help you harden your source code and improve configuration security while reducing hours of DevSecOps tasks to minutes.

Bailey is a cybersecurity and political science student at Old Dominion University and a contributor to the WhiteRabbitNeo open-source project. She is passionate about cybersecurity education and is excited about the growing integration of AI into cybersecurity.

JMP Into Malware Analysis - Katelin Grogan

We all know that the daily life of a cybersecurity analyst often requires you to branch out into left field and learn a completely new skill on the fly. Join me as I introduce you to today's go-to tradecraft for static, dynamic, and code-level malware analysis so that you can begin analyzing artifacts of interest with ease. At the end of the day, any threat actor has a goal to accomplish, and what we call malware is someone else's tooling. This presentation will walk you through how to characterize samples and identify indicators of compromise.

A junior cybersecurity analyst, graduate of Auburn University, and GIAC certification holder with 3 years of professional experience. When I'm not asking you about your home network or cringing at bad password policies, I'm probably exploring the DMV or sitting on a beach somewhere.

Past, Present and Future of Automatic Code Remediation - Arshan Dabirsiaghi

Recently, the landscape of tools used to change code saw explosive growth. Several open source code mutation frameworks have emerged, allowing expressive code transformations. LLMs have also jumped into the picture, promising power and delivering "cool" – but also towing chaos. We'll explore the capabilities of these tools all towards answering "are we ready to automatically fix code issues?

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.

Filling Gaps in AI Governance: How ISO/IEC 42001 Shapes the Future of AI Ri - Kartik Khurana

In this presentation, we will explore the emerging gaps in AI governance and how the newly released ISO/IEC 42001 framework addresses these critical issues. As AI technologies evolve rapidly, organizations face increasing challenges in managing risks related to ethics, security, transparency, and accountability. This talk will provide an in-depth analysis of ISO/IEC 42001's role in mitigating thes

Kartik Khurana is a cybersecurity professional specializing in Governance, Risk, and Compliance (GRC). Currently pursuing a Master's in Cybersecurity at Penn State University, he has gained experience through five internships in penetration testing, auditing, and cloud security. Joining NVIDIA's GRC team in February 2025, Kartik is committed to advancing security practices, enhancing compliance frameworks, and safeguarding digital infrastructures.

Quantum Computing: The Coming Revolution in Security and Cryptography - Shalini Menon

Quantum computing threatens current encryption. Post-quantum cryptography (PQC) is developing new algorithms and key distribution methods like QKD to secure data in this new era. IT professionals and developers must adapt to these changes to ensure a secure digital future.

Starting a SBOM Programme - The Pain Is Probably Temporary - Grey Fox

In my 3rd week working for a Fortune 500 company, I was tasked with designing and rolling out a programme to churn out software bills of material for our high inherent risk products. 5 months later, we're on the right side of the forthcoming supply chain security regulatory and compliance world. It wasn't easy, but it was sure worth the effort. I even made some friends along the way.

Grey Fox, the callsign assigned to him by a DHS colleague, is a Product Security Engineer for a Fortune 500 critical infrastructure manufacturing and operations company. He recently retired from the U.S. military after 20 years of service as a Digital Network Intelligence Analyst and Special Operations Cyberspace Mission Leader. Having deployed eight times supporting front line combat teams, his experience ranges from offensive cyberspace operations planning and execution to military information support operations. Along the way, Grey Fox acquired multiple creds, including GCTI, GASF, GAWN, and CWNA. When not breaking ICS apps, he instructs Digital OPSEC for the U.S. Departmernt of Defense, as well as software-defined radio foundations and Wi-Fi hacking for several community cybersecurity groups.

Building Against a Breach.... Out of a disclosure? - Liz Wharton

Metadata from incident response and business communications can leak sensitive information, aiding threat actors. External legal and crisis management teams may unintentionally expose data. Explore how to leverage AI/ML analysis of regulatory disclosures such as SEC 8-K filings and past incidents to build pre-incident cross-team partnerships and mitigate future leaks.

Liz, founder of Silver Key Strategies, brings 20 years of experience advising researchers and organizations on legal, business, information security, risk, and privacy matters. She has led operations at threat research startups and served as Sr. Assistant City Attorney for Atlanta's airport, aiding on the City's ransomware incident IR team. Liz also volunteers as a mentor and serves on startup, non-profit, and educational advisory boards.

SQL injection is a thing of the past... and other lies we tell ourselves - Mackenzie Jackson

Despite being older than internet explorer injection attacks like SQLi, Command Injection, and XSS remain prominent. Our research found SQLi alone accounts for 6.7% of open-source vulnerabilities and 10% in closed-sourceprojects. This session reveals why these attacks persist and how modern solutions can help.

Mackenzie is a security researcher and advocate with a passion for code security. He is the former CTO and founder of Conpago, where he learned firsthand the importance of building secure applications. Today, Mackenzie works for Aikido security to help developers and DevOps engineers build secure systems. He also shares his knowledge as a contributor to many technology publications like DarkReading, Financial Times, and Security Boulevard along with appearing as an expert in TV documentaries and interviews.

A Tale of Two Incidents: Responding to Akira Ransomware - Eno Dynowski, Dylan Watson

Akira, one of the most prolific RaaS groups today, is responsible for millions in ransom payments, and has proven themselves as a formidable opponent. Also tracked as PUNK SPIDER, they specialize in compromising edge devices, encrypting hypervisors, and extorting victims. Join us for an investigation of two PUNK SPIDER intrusions and gain insight into the life of an incident response consultant.

Eno Dynowski is an Incident Response Consultant at CrowdStrike. He has investigated dozens of nation state espionage, ecrime, and insider threat engagements with clients across industry verticals. Previously, Eno was a Professional Services Intern at CrowdStrike, and a Platform Security intern at Tesla. He is a graduate of Loyola University Chicago, and is currently based in Chicago, IL. When he's not stomping Threat Actors, Eno loves hiking, fine dining, and open world RPGs.

Dylan Watson currently works as an Incident Response Consultant at CrowdStrike. Having worked on a large number of active eCrime and APT engagements, Dylan specializes in hypervisor forensics, large-scale event triage, and intelligence coordination. Outside of work, Dylan is pursuing a master's degree in Security Studies at Georgetown University, and he also coaches high school robotics at a local high school.

Inch By Inch: a Case Study in Maintaining & Scaling a Modern XDR Product - Jessica David

Delivering security products to millions of users is a monumental task. From building & deploying to mitigating performance issues & false positives, securing systems requires constant coordination between multiple teams of researchers, engineers, and other stakeholders. This session will highlight lessons learned from our experience as an effective cross-functional team building an XDR product.

Jessica David is a Principal Data Engineer on the Security Intelligence Team at Elastic. With a background in software engineering and data warehousing, she brings her expertise to the security researchers & detection engineers around her by building data pipelines & services for processing first- and third-party threat intelligence.

What's in the Cloud? - Kai Lyer

The talk will outline detection and threat hunting strategies that could be easily adopted by a mature SOC to look for threats in their Cloud (Azure and AWS) environment. Session will use Jupyter notebook containing detections mapped to the MITRE ATT&CK framework and threat hunting methodologies backed by unsupervised machine learning to hunt for anomalies and visualize them.

Security Engineer at Amazon's Enterprise Protection Program and a GIAC Certified Security Professional with extensive experience leading security engineering and applied machine learning teams to deploy production-scale, near-real-time threat hunting models. Passionate about leveraging advanced technologies to solve complex cybersecurity challenges, with a proven track record in areas such as purple teaming and incident response. Actively contributes to the cybersecurity community through conference talks and open-source projects, fostering collaboration and knowledge sharing.

Active Directory Security 101 - Saturday

Active Directory (AD) is OLD in tech years, but this 25-yr-old identity platform is still deployed all over. This course focuses on understanding AD to build foundational defenses against common attacks and misconfigurations. Through guided lectures, instructor demonstrations, and hands-on labs participants will explore key AD security components and best practices for hardening AD environments.

Each student will have access to a dedicated lab environment to ensure practical, hands-on experience. The labs are designed to replicate real-world scenarios and as such will have common misconfigurations in place to discover and remediate.

Requirements:

Students will need a functioning laptop with the ability to connect to conference internet. The laptop must have a modern web browser. It would be beneficial if the students have a method to take notes, either pen and paper or on their laptop. A basic understanding of Active Directory is helpful. A basic understanding of basic networking like TCP/IP is required.

Trainer: Jim Sykora & Darryl G. Baker

Jim Sykora is a security researcher and consultant focused on identity security. Jim started his sysadmin path in 3rd grade & did a bunch of gigs before starting to blend operational experience & rampant curiosity with security knowledge. Loves following rabbit holes.

Darryl G. Baker is a security consultant at Trimarc Security, where he conducts in-depth security assessments against Active Directory and Entra ID. He is also the Principal Instructor for all Trimarc Attack and Defense courses. He has developed multiple tools and scripts,as well as written whitepapers on Active Directory security. When he is not presenting at conferences, he enjoys radio engineering. Find him on the 12m band!

Career Campaigns: A Tabletop RPG Workshop - Sunday

Join us for a tabletop roleplaying game (RPG) with real-world wins! Participant-players seeking their first role in cyber or simply transitioning to a new specialization will transform their current resume's "character sheet" into a freshly reskilled or dual-classed hero, ready to take on any cybersecurity hiring process for your next infosec campaign.

Requirements:

No hardware or software required. Copy of resume. Background in RPGs helpful but optional.

Trainer: Stryker

Stryker is a threat intelligence analyst at a major insurance company, where she translates technical research and qualitative intelligence into the "so what?" and "what now?" solutions that keep more people safe and secure.

Feel free to say hi on LinkedIn or in the Lonely Hackers Club (LHC) Telegram chat, where she once (in)famously ranted about how commercial gun safes are insufficient for secure off-site data storage. Stryker lives in the Baltimore-DC area, growing parsley for swallowtail butterfly caterpillars and algae for neocaridina shrimp.

Web Application Penetration Testing - Sunday

This 4-hour Web Application Penetration Testing Training Session provides a hands-on introduction to web application security, focusing on identifying and exploiting common vulnerabilities. The session begins with an overview of web application security, highlighting real-world breaches and the OWASP Top 10 threats. Participants will then set up a testing environment and familiarize themselves with essential tools like Burp Suite, SQLMap, and Nmap.

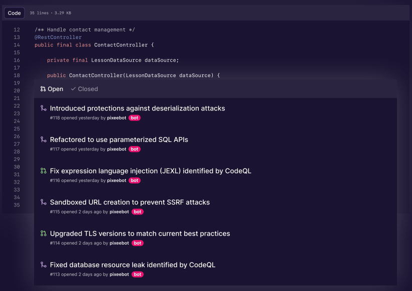
The core of the training covers practical exploitation techniques for vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Cross-Site Request Forgery (CSRF), and Security Misconfigurations. Each section includes real-world attack scenarios and hands-on exercises to reinforce learning.

Requirements:
Laptops with admin/root permissions are required. Basic knowledge of how web application works/build is recommended

Trainer: Sheshananda Reddy

Mr. Sheshananda Reddy Kandula is a seasoned Application Security professional with 15 years of experience, currently working at Adobe, where he specializes in securing web, mobile, and API ecosystems. His expertise lies in identifying and mitigating vulnerabilities in alignment with OWASP Top 10 security standards. He holds industry-recognized certifications, including OSWE, OSCP, and CISSP, and has extensive hands-on experience addressing real-world security challenges. Prior to his role at Adobe, he contributed to global security initiatives at Mastercard, leading efforts in vulnerability management and secure software development.

Passionate about advancing cybersecurity, Mr. Kandula actively contributes to the security community by sharing insights on secure coding, threat modeling, and application security best practices. His commitment extends to mentorship, technical leadership, and research, fostering a security-first mindset across organizations and professionals. Through his work, he strives to empower security practitioners, promote awareness, and strengthen digital resilience in an evolving threat landscape.



NOTES

NOTES

NOTES

BSIDES CHARM PARTY

CHILL OUT

RETRO VIDEO GAMES

BOARD GAMES

PERFORMANCE BY

DJ SYNTAX

STARTS AT 8 PM

TRACK 1