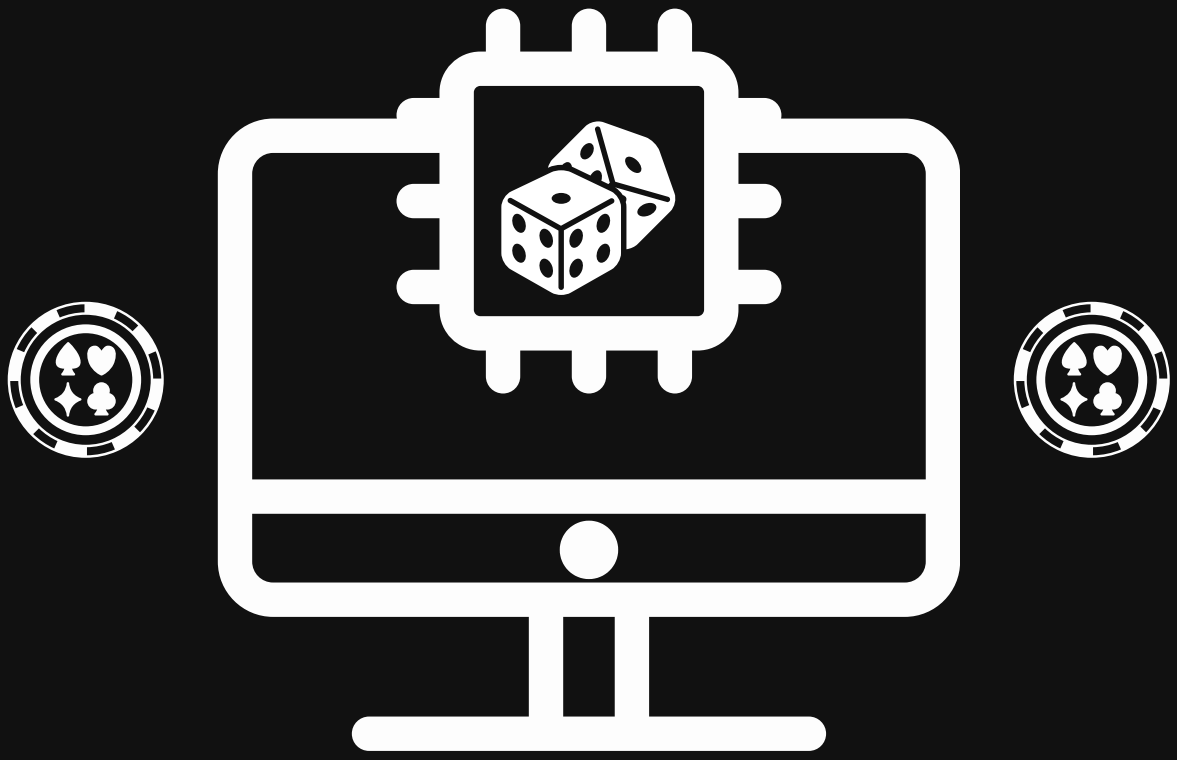
Live! CASINO • HOTEL PHILADELPHIA

Friday December 6, 2024

900 Packer Ave.,
Philadelphia, PA 19148



Conference Zine

BSIDES PHILADELPHIA

Hosted by and for the Information Security Community
https://bsidesphilly.org

VIP SPONSOR

Since 2010 Security Risk Advisors has been a highly-specialized consulting firm with solutions to cybersecurity's emerging problems. We are technical and engaging. We have a passion for recruiting and training the next generation of cybersecurity practitioners

- **Purple Teams:**
  Obtain your Threat Resilience Benchmark and sharpen your defenses with our VECTR platform.
- **Red Teams:**
  Conduct expert adversary simulations and test your network, applications, cloud, and OT environments.
- **XDR & CyberSoc:**
  24x7 services using our Microsoft-based SCALR platform or staffing in your bespoke SOC environment.
- **OT Security:**
  Build resilience in your ICS, XIoT, or IoMT environments
- **Cloud Security:**
  Assess and secure your Azure, Google, and AWS infrastructure and applications

Visit us at **https://sra.io** to learn more about other services we can provide!

BSIDES PHILLY

CONFERENCE PAMPHLET

Thank you for attending BSidesPhilly!

BSides Philly is an annual security conference that supports the Philadelphia region, drawing over 1,000 information security practitioners and leaders from Pennsylvania, New Jersey, Delaware, New York, and Maryland. Our goal is to provide an affordable, high-value conference open to everyone, fostering a space for security experts, IT professionals, and newcomers to share ideas, exchange concepts, and build relationships within the community.

The conference is made possible through the generous support of our sponsors and **Live! Casino Hotel Philadelphia**, covering significant event costs like the venue, A/V, meals, and materials.

Managed by Bsides Philly LLC, a 501c3 non-profit organization, all proceeds go towards future local BSides events or technology-related charities such as Hackers for Charity. Our team is entirely volunteer-based, and we are committed to supporting and growing the information security community in our region.

www.bsidesphilly.org

info@bsidesphilly.org

900 Packer Ave., Philadelphia, PA 19148

SUMMARY OF BSIDES PHILLY

What is BSides?

BSides is a community-driven platform designed to foster events by and for information security professionals. It aims to broaden the scope of discussions beyond traditional settings, creating an environment that encourages collaboration and innovation.

BSides events are dynamic, featuring interactive discussions, demos, and participation that drive forward-thinking conversations. The primary goal is to break down barriers, offering more opportunities for speakers, diverse topics, and engaging events within the information security community.

BSides was created in 2009 when quality speakers were turned away from a mainstream conference due to limited space and time. Recognizing the need for more opportunities, BSides aims to break these constraints by offering additional options for speakers, topics, and events.

BSIDES HISTORY

2009
Launched in the United States

2010
First European event

2011
More than 20 events in US, Europe, India, Hong Kong, & Australia

2012
More than 25 events worldwide with new events in both Africa and Brazil.

2013
40 events worldwide and over 100 events total since

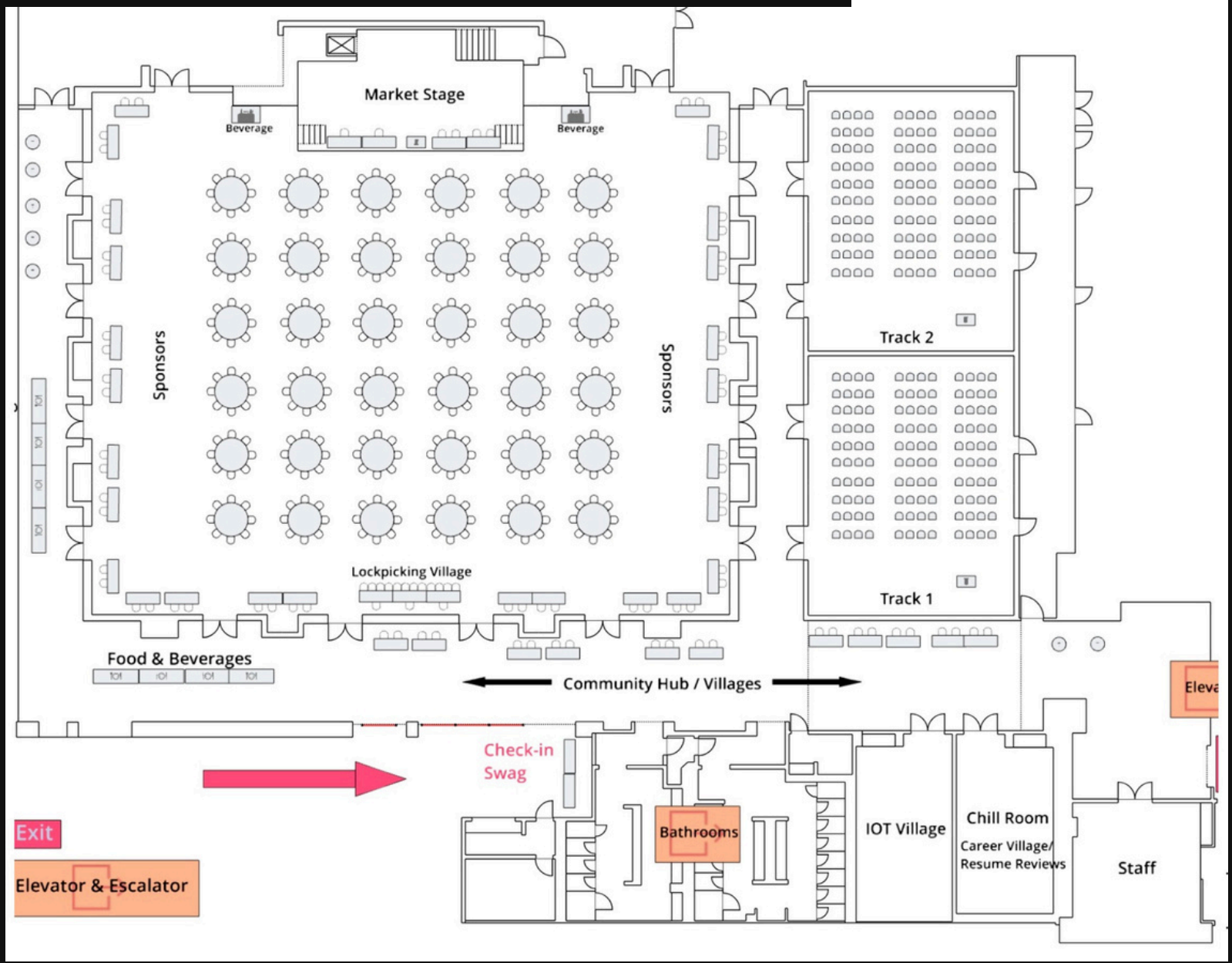
2015
20 countries, 300 cities, 6 continents

2017
500 global events

2023
650 conferences globally!

ABOUT THE VENUE

Live! Event Center on 2nd Floor (All Ages)



Must be 21 or older to access casino floor on 1st floor

THIS YEARS
BADGES & SWAG!

2024'S BADGE

2024’s badge takes inspiration from the humble poker chip which has evoked so many feelings since it’s ancestors were created in the 1700s. Joy, despair, murderous rage; you’ll experience at least one of these emotions while at the convention. Hit the chill out room and recenter if you find yourself towards the latter half of the spectrum.

- Attendees = Red eyes
- Sponsors = White eyes
- Speakers = Green eyes
- Volunteers = Blue eyes
- Staff = Dichromatism eyes

THANK YOU

2024 Sponsors!

Gold Sponsor

Trace your data to protect it like never before. Cyberhaven detects and stops the most critical insider risks to your most important data.

Learn more at **https://www.cyberhaven.com**

SCHEDULE

POWERED BY HACKER TRACKER

https://bsidesphilly.org/conference

https://hackertracker.app/schedule/?conf=BSIDESPHILLY2024

Phillip Wylie

Keynote

Title: Optimal Offensive Security Programs
Time: Fri, Dec 6, 09:10 - 09:50 EST
Room: Market Ballroom Stage

Abstract:
Offensive security is vital for identifying and exploiting system vulnerabilities. However, current practices have gaps that reduce test effectiveness. This presentation will address these gaps and suggest strategies to enhance offensive security assessment efficacy.

Details:
Offensive security, a critical component of cybersecurity, aims to identify and exploit vulnerabilities in information systems. Despite its importance, several gaps exist in current practices that can undermine the effectiveness of these tests. This presentation will address these gaps and propose strategies to enhance offensive security assessment efficacy.

Topics discussed in this presentation:

- Offensive security introduction
- Offensive security types
- Gaps in pentesting
- Overcoming the gaps and optimizing your offensive security program

Bio:
Phillip Wylie is an offensive security with over 20 years of industry experience. He is a former Dallas College Adjunct Instructor. Phillip has diverse experience in multiple cybersecurity disciplines, including network security, application security, and pentesting. As an offensive security professional with over a decade of experience, he has conducted pentests of networks, Wi-Fi networks, applications, red team operations, and social engineering.

Phillip's contributions to the cybersecurity industry extend beyond his work as a pentester. He is the concept creator and co-author of "The Pentester Blueprint: Starting a Career as an Ethical Hacker," a highly regarded book inspired by a lecture he presented to his class at Dallas College, which later became a conference talk. Phillip hosts "The Phillip Wylie Show" and previously "The Hacker Factory Podcast."

Zach Malinich

Speaker

Discord OSINT: Using the Power of Empathy Banana

Time: Fri, Dec 6, 10:00 - 10:50 EST
Room: Rittenhouse (Track 1)

Open-source intelligence in Discord may seem surface level. Some techniques include searching through chat history using search operators similar to Google dorking and reviewing a user's profile to look for any linked accounts tied to their Discord account. Going beyond this and analyze the servers that a user is a part of, you would be able to make more assumptions and inferences based on those servers. I applied what I saw and experienced with Student Hubs and applied it to cybersecurity within Discord. The information from knowing what cybersecurity servers a person is in informed me of what their experience level was, the type of field they were interested / worked in, and potentially even where they lived.

However, you can only reach a certain point by joining servers within Discord. This type of approach can only be done at scale and this presents its own set of problems. Scaling this seemed unlikely to happen until a service known as Spy.pet was publicly disclosed in April this year. Spy.pet was marketed as a data broker that was inadvertently a very capable OSINT tool that could be used for Discord. Knowing that it would be available for a short time before it got shut down, I was able to access Spy.pet to use and document what capabilities it had. I will cover Spy.pet and its capabilities as well as my approach with Discord OSINT at scale. I also include some OPSEC tips and tricks.

Bio:
Zach a.k.a "UberZachAttack" is a PSU alum with a focus in offensive security and currently works as a pentester for a small cybersecurity company in Pittsburgh.

https://www.linkedin.com/in/zmalinich
https://uberzachattack.xyz/

Edan Cohen

Speaker

Persona Management - A practical guide on safely infiltrated and engaging while going undercover on the underground

Time: Fri, Dec 6, 10:00 - 10:25 EST
Room: Liberty (Track 2)

Cybersecurity professionals know that threat hunting on underground environments is necessary, but they don't know the most crucial step to beginning the process. How do you access the deep and dark web? How do you gain a threat actor's trust? These are the most commonly asked questions of cybersecurity professionals preparing a proactive threat hunt.

Navigating the underground requires dedication to persona management and setting up a safe and secure environment to ensure one does not expose themselves to malicious actors. I will demonstrate how to set up a secure environment (dirty machine) using Tails, how to find sources in the dark web, best practices when creating your first persona, communicate with threat actors, and of course, how to seek out threats once you gain access to the sources where threat actors plan, play, and profit. All while using real examples that attendees can try for themselves.

Bio:
Edan Cohen is the Solution Architect at Cybersixgill. Previously, he worked in Corporate Security at the World Bank Group, where he analyzed geopolitical events while identifying threats to staff and business operations globally. He has experience working at security consulting firms in both the US and Israel and served in the IDF. Talk to him about ransomware-as-a-service operators and biking.

https://www.linkedin.com/in/edan-cohen-a8a74551

atlas OfdOOm

Speaker

Alcohol, Blood, Sweat, and Creativity: Reversing an Obfuscated Car Mod Tool

Time: Fri, Dec 6, 11:00 - 11:50 EST
Room: Rittenhouse (Track 1)

Reversing can feel uber powerful... like you hold God's honest truth within your hands... most humans don't understand what you can see and comprehend. Until someone tries to hide the truth from you... limit your knowledge... keep you from your glorious purpose!

Obfuscated code can be a real downer.

This talk focuses on the story of how i took on an interesting obfuscated target (an automotive modder's toolset with ability to flash firmware and tweak engines), in fun and exciting ways. We'll discuss several problems with obfuscated code, the approach i took (and tooling), play in the guts of machine code, and customizations to binary analysis tools that came out of the journey...
there will be much hex, disassembly, green on black, total carnage.

You will walk away with nifty ideas and new tools to help you in your pursuit of truth. you will be entertained, enriched, and more educated. instead of thinking that "atlas is smart" my goal is you feeling, and being, more powerful.:sh

Bio:
chief pwning officer

https://x.com/at1as

Sheshananda Reddy Kandula

Speaker

Hacking OAuth: An Attacker's View of Your OAuth Flows

Time: Fri, Dec 6, 10:30 - 10:55 EST
Room: Liberty (Track 2)

OAuth is widely adopted and used in all industries like Tech, Finance, Social Media, SaaS providers, E-Commerce, Retail etc. OAuth provide enhanced security, user experience, seamless integrations and control of the data shared with other apps. But small misconfigurations lead to critical vulnerabilities. In this presentation, I would like to give quick introduction to OAuth then talk about vulnerabilities in OAuth. Then few demos and vulnerabilities discovered recently several organizations.

Bio:
Sr Security Engineer, Adobe

https://www.linkedin.com/in/sheshanandak

Stephen Bondurich

Speaker

Next-Gen Deception: Exploring the Evolution of Social Engineering

Time: Fri, Dec 6, 11:00 - 11:25 EST
Room: Liberty (Track 2)

My presentation discusses the constantly evolving nature of social engineering attacks and how threat actors are adapting their techniques to overcome our conceptions of what social engineering attacks look like. I reveal the most successful modern approaches to social engineering that I have been using against real people during penetration tests. I also discuss the application of AI and the novel attack vectors that are now possible. Finally, I describe ways to identify social engineering attacks and steps individuals and organization can take to protect themselves. I hope to educate people about how attackers are becoming more advanced and believe in their social engineering attacks, what the impact is, and how they can protect themselves in both a personal and professional setting.

Bio:
Security Consultant at SEVN-X

https://www.linkedin.com/in/stephen-bondurich-sevnx

Chris Glanden

Speaker

Algorithmic Fate

Time: Fri, Dec 6, 11:30 - 11:55 EST
Room: Liberty (Track 2)

It’s damn near 2025, and it seems as though if you detect a system, software, or person is NOT leveraging AI… it’s an anomaly. Algorithms have leveled up from simple code to powering systems that shape everything around us. They’re influencing how we make decisions, how businesses run, and even more importantly, how society moves forward.

From systems built for saving lives to systems designed to destroy lives….. AI is driving innovation, but also driving the destiny of generations to follow.

This talk dives into "Algorithmic Fate" and how the algorithms we build today are deciding our future.

Key Takeaways:

- Explore how system algorithms, code, and AI models are shaping decision-making in critical sectors.
- Examine the ethical and security risks of relying on AI and algorithms to drive societal and business outcomes.
- Mention real world examples of algorithmic impact and how they can shape public policy, security, privacy, mental health, and physical safety.
- Learn strategies to secure and govern AI models, mitigating the risks associated with algorithmic decisions.
- Discuss how to maintain control over the future as AI algorithms become more integral to daily life.

Bio:
Founder and CEO of Barcode Security

https://www.linkedin.com/in/chrisglanden

Cyber Circus Network

Live Podcast

This interactive show will include crowd interaction and practical takeaways designed to help attendees break through the security career forcefield, whether they are students, career transitioners, or professionals simply looking to grow their expertise.

Bio:
Security Consultant at SEVN-X

https://www.linkedin.com/in/stephen-bondurich-sevnx

Cyber Circus Network Podcast: Breaking Into Cybersecurity

Time: Fri, Dec 6, 13:00 - 13:50 EST
Room: Market Ballroom Stage

Those interested in launching a cybersecurity career or seeking guidance on navigating the path ahead are invited to attend a live recording of the Cyber Circus Network (CCN) Podcast. This high octane session hosted by industry professionals, provides sound advice as well as onsite interviews with recruiters and hiring managers who share their expertise and personal experiences to support success in a field more “in-demand” than ever. The session will encompass:

- Cybersecurity Career Paths: An overview of typical roles such as SOC analyst, pentester, and threathunter, along with recommended entryways. In addition, the a-typical roles that often get overlooked and why they shouldn’t.
- Building a Strong Foundation: Tips on developing essential skills like networking, programming, and operating system fundamentals, the core skills that will help accelerate your journey.
- Industry Insights: Advice from frontline recruiters and hiring managers on standing out as a candidate, writing an impactful resume, and succeeding in the interview process.
- Networking and Practical Experience: Guidance on building connections, gaining real life experience through internships and passion projects, and recommended, proven platforms to boost skills.
- Soft Skills, Uncommon Attributes, and Future Trends: Insights into the importance of communication, teamwork, and adapting to advancements like AI and zero-trust security. The secret skills you won’t find in an instructional manual will be revealed.

Josh Mason

Speaker

How to Win Trust and Stop Hackers: Using Social Engineering for Good in Cybersecurity

Time: Fri, Dec 6, 13:00 - 13:50 EST
Room: Rittenhouse (Track 1)

We often focus on technical defenses in cybersecurity, but the most significant challenges are human. Convincing people to take security seriously without sounding pushy or annoying is an ongoing struggle for many professionals. In this talk, I'll share how we can use principles of influence—drawn from social engineering, psychology, and personal experience—to persuade people to make smarter security choices ethically. From getting buy-in for crucial initiatives to managing crises, this session will equip you with practical tools to influence your colleagues, leadership, and clients for the greater good. Learn how to build trust, foster cooperation, and ultimately create a culture where security is everyone's responsibility.

Bio:
Joshua Mason is a cybersecurity expert with a unique blend of military, training, and sales experience. As a former U.S. Air Force pilot and cyber warfare officer, Josh mastered the art of influence and leadership in high-pressure situations. He later transitioned these skills into cybersecurity, where he developed training programs, advised organizations on security strategies, and coached teams on how to build trust and cooperation within their companies.

With over 15 years in the field, Josh has helped organizations apply principles of influence to improve security outcomes, whether through training programs or convincing leadership to prioritize cybersecurity. A frequent speaker at industry conferences, he's passionate about using social engineering for good—helping teams work together to build a culture of security and trust.

https://linkedin.com/in/joshuacmason

Jeremy Fuchs

Speaker

Browse Securely: Eliminate Barriers to Learning on the Web

Time: Fri, Dec 6, 13:00 - 13:25 EST
Room: Liberty (Track 2)

K-12 student emails have been fairly successfully locked down, allowing students of all ages to communicate with teachers safely. The web? Not so much. Kids are understanding how to get around existing security controls. And now, they've begun to use generative AI tools. Security becomes a concern, both in terms of their online safety, but also the safety of the school's data. We'll discuss new innovations in browser-based security that keep outside threats at bay, and allow students to learn in a safe, secure and productive environment.

Bio:
Security Analyst, Check Point

Jake Meltzer

Speaker

Bridging AI Innovation with Data Security: An Architectural Approach

Time: Fri, Dec 6, 13:30 - 13:55 EST
Room: Liberty (Track 2)

The primary goal of my presentation is to bridge the gap between AI system architects and information security professionals. In many organizations, there is an understated divide between those who, at an IT level, design and implement AI-driven solutions, and the security teams tasked with protecting data and ensuring regulatory compliance. This separation often stems from differences in priorities, communication challenges, and organizational silos. By addressing these issues and presenting realistic, technically-driven solutions and controls, my aim is to foster collaboration and mutual understanding between job functions and departments, ensuring that data security and compliance are integral components of not only AI architecture, but the overarching IT sphere from the ground up.

Bio:
Global Information Security Analyst & AI Implementation Lead at Crown Holdings (Crown Cork & Seal)

https://linkedin.com/in/jakemeltzer

Cory Wolff

Speaker

How to Train Your Llama: Lessons Learned from Finetuning Llama 3.1 on Thousands of Threat Actor Telegram Messages

Time: Fri, Dec 6, 14:00 - 14:50 EST
Room: Rittenhouse (Track 1)

Training and fine tuning LLMs is an incredibly complex process, but thanks to different libraries and frameworks we can easily find our own data and fine tune open source models like Llama 3.1.

This talk will be the story of how I scraped Telegram channels operated by threat actors and used this data to fine tune Llama 3.1. It will give attendees an easy way to fine-tune their own models and demonstrate what steps to take and what pitfalls to avoid.

Bio:
Director of Offensive Security at risk3sixty

https://links.corywolff.com/

Len Noe

Speaker

2024: A Cyborg Odyssey

Time: Fri, Dec 6, 14:00 - 14:50 EST
Room: Liberty (Track 2)

Transhumans, individuals enhanced with technological augmentations, are no longer just a concept from science fiction—they exist and walk among us today. Historically, these individuals have been perceived either from a medical standpoint, with enhancements designed to aid those with disabilities, or as full cyborgs, a notion confined to the realms of speculative fiction. However, with the advent of Brain-Computer Interfaces (BCI), SMART technologies, and consumer products, the boundary between the physical and biological is rapidly disappearing, transforming the landscape of human capability and interaction.

Today's headlines increasingly reflect scenarios reminiscent of science fiction movies, highlighting the profound implications of these advancements for cybersecurity. Augmented humans, with their integrated technological enhancements, pose a significant cyber threat to modern security controls. These transhumans can perform sophisticated cyber attacks such as URL redirections, phishing, smishing, and even man-in-the-middle (MiTM) attacks, all executed from technology embedded beneath their skin. The integration of such advanced tech within the human body renders traditional security measures inadequate, necessitating a rethinking of our defensive strategies.

We are living in a future world today, and it is crucial to recognize and acknowledge this reality to ensure our security. The presence of transhumans necessitates a paradigm shift in our approach to cybersecurity, calling for the development of new strategies and technologies to defend against the unique and evolving threats they present. This presentation aims to illuminate with multiple demonstrations including implant initiated MiTM attacks, Phishing, Smishing, and full automated Linux attacks. The expanding landscape of cyber threats posed by transhumans is a real. The urgent need for complimentary and layered security solutions to safeguard our society in this new era of human evolution is already here.

Bio:
Len Noe, a Technical Evangelist, White Hat Hacker, and Transhuman at CyberArk Software, is a dynamic and influential speaker on the international security circuit. With an impressive track record of delivering impactful presentations in over 60 countries and at renowned security conferences worldwide, Noe's expertise leaves a lasting impression. Notably, he has graced the stage at the prestigious World Conference in The Hague, C.E.R.T. EU, and has been invited to address multiple governments.

https://www.linkedin.com/in/len-noe/
https://twitter.com/hacker_213

Alex Holden

Speaker

Decoding the Digital Canvas: Safeguarding Against Visual Data Leaks

Time: Fri, Dec 6, 15:00 - 15:50 EST
Room: Rittenhouse (Track 1)

The analysis of images and videos is not only crucial for identifying external cyber threats but also for uncovering internal and sensitive information inadvertently leaked by companies. From ransomware attacks to the identification of threat actor identities, trolls, and the dissemination of fake news, visual data holds the key to detecting and thwarting a wide array of threats.

In this presentation, we'll explore the transformative potential of harnessing AI for advanced image and video processing techniques to derive cyber threat signals. By searching for patterns within visual content, we can uncover threats that often go unnoticed by traditional threat intelligence sources. Moreover, our focus extends to detecting and preventing the accidental leakage of internal and sensitive information within images and videos, providing organizations with proactive measures to safeguard their data.

Join us as we delve into the cutting-edge techniques and strategies for leveraging image and video processing to enhance cyber threat detection and response, ultimately fortifying organizations against a rapidly evolving threat landscape.

Bio:
Alex Holden is the founder and CISO of Hold Security, LLC. Under his leadership, Hold Security played a pivotal role in information security and threat intelligence, becoming one of the most recognizable names in its field. Mr. Holden researches minds and techniques of cyber criminals and helps our society to build better defenses against cyber-attacks.

https://twitter.com/HoldSecurity

Nathan May

Speaker

Advanced Phishing Tradecraft

Time: Fri, Dec 6, 15:00 - 15:50 EST
Room: Liberty (Track 2)

Discuss techniques used to phish effectively in 2024, bypassing protections and exploiting common misconfigurations. Topics include proofpoint bypasses, smtp relays, proxying to capture session tokens, breaking okta verify from capturing your phishing page, etc.

Bio:
Penetration Testers at UltraViolet Cyber

VILLAGES — COMMUNITY HUBS

VILLAGE

TOOOL

BLACKS IN CYBER

#LITLIKEB.I.C

Women in Cybersecurity
WiCyS
DELAWARE VALLEY AFFILIATE

Temple University
College of Liberal Arts

Cybersecurity in Application, Research and Education Lab

VILLAGES — COMMUNITY HUBS

City of Philadelphia

THE DIANA INITIATIVE

BELIEVE & ACHIEVE—TOGETHER

(ISC)²

BOOKS

Voices Cyber

PHILLY TECH COUNCIL

Hispanic, Latino, Latina & LatinX International Association In Cybersecurity

Silver Sponsors

HackerOne is the global leader in human-powered security, harnessing the creativity of the world's largest community of security researchers with cutting-edge AI to protect your digital assets. The HackerOne Platform combines the expertise of our elite community and the largest vulnerability database to pinpoint critical security flaws across your attack surface.

Learn more at **https://www.hackerone.com**

Data Protection in the AI and Quantum Era. RSec is a multinational cybersecurity firm dedicated to safeguarding over 200 million users across the Americas. We offer comprehensive services and solutions that assist businesses in various industries to mitigate cyber risks and enhance productivity. Our expertise spans strategic and technical consulting, implementation and integration of security controls, threat management, and managed services. In partnership with IBM, we deliver industry-leading data protection and tailored solutions, helping businesses mitigate risks and enhance productivity.

Learn more at **https://rsecgroup.com**

Silver Sponsors

Savvy Security specializes in simplifying digital protection for businesses, offering accessible and scalable solutions for cyber risk management. From threat detection to compliance, Savvy Security makes cybersecurity achievable for all.

Learn more at **https://www.savvy.security**

Securely Built specializes in developing robust software solutions with a focus on cybersecurity and privacy. Their expertise spans secure software design, secure coding practices, and advanced application security services to help businesses safeguard their digital assets. Committed to empowering organizations, Securely Built delivers innovative, reliable, and secure technology tailored to the ever-changing threat landscape.Description goes here

Learn more at **https://www.securelybuilt.com**

Bronze Sponsors

https://www.accessitgroup.com

https://buckhornconsulting.com

https://www.checkpoint.com

https://www.contrastsecurity.com

https://www.crowdstrike.com

https://www.extrahop.com

Bronze Sponsors

https://www.horizon3.ai

https://www.legitsecurity.com

https://owasp.org/www-chapter-philadelphia

https://www.mimecast.com

https://www.sectri.com

https://www.uvcyber.com

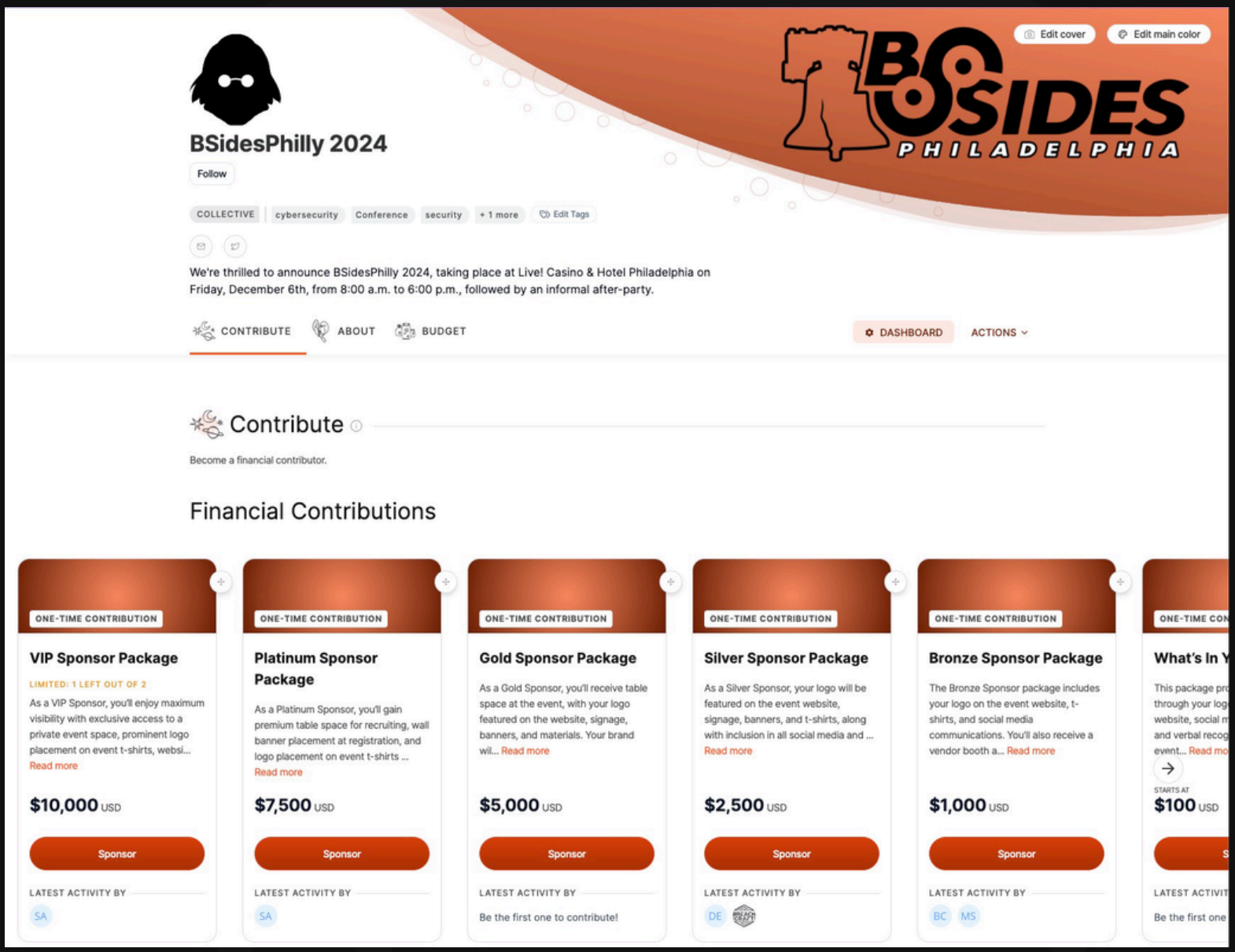
What's in Your Pocket

CraftedSecure

DONATIONS

How to make donations?

https://opencollective.com/bsidesphilly



THANK YOU, AND WE HOPE TO COLLABORATE WITH YOU IN THE FUTURE.

BSIDES PHILADELPHIA

www.bsidesphilly.org

900 Packer Ave.,
Philadelphia, PA 19148