RUN BOOK 2025
MAY 13TH
HARRAH'S/CAESARS HOTEL

CLICK TO JOIN THE LINKEDIN GROUP

A Cybersecurity Gumbofest !!

BSIDES NEWORLEANS 2025

Mixing the Right Ingredients for Resilience

7:30 AM	**Registration Opens**			
	Vieux Carré Ballroom			
9:00AM - 9:55AM	Opening Keynote Unleashing Your Inner Leader!!! *Dominic Vogel*			
	Track 1 (Main)	**Track 2 (Fulton I)**	**Track 3 (Fulton 3)**	**Track 3 (Satchmo)**
10:00AM-10:45AM	Cyber Werewolves: Rewriting the Rules to the Game Against Insider Threats *Roxey Davis*	Mental Health and Resilience *Derek "The Cyber Warrior" Scheller*	When the (Un)Expected Happens *Miriam Lorbert*	Android App Security (with a dash of LLM) *Vaibhav Agrawal*
10:45AM-11:10AM	**Networking Break and Technology Pavilion**			
	Track 1 (Main)	**Track 2 (Fulton I)**	**Track 3 (Fulton 3)**	**Track 3 (Satchmo)**
11:15AM - 12:00PM		Transforming Cyber Risk Assessments Through Continuous Validation *Irina Loktionava* and	LSU WiCS Breaking into Cyber *Arushi Ghildiyal / Jenah Mansour*	Breaking Down (and Breaking Into) PCI QSA: The Path, The Role, and Why It Matters

		Chris Oshaben			James Chad Oliver
	Vieux Carré Ballroom				
12:00PM-12:45PM	Lunch Keynote Real Consequences of Abstract [Security] Risk Decisions *Raf Los*				
12:45PM - 12:55PM	Community Announcements "Gumbo Guild" Women in Technology, ISACA Baton Rouge, ICS2 Gulf Coast, Louisiana Cyber Reserve, Infragard				
	Track 1 (Main)	**Track 2 (Fulton I)**	**Track 3 (Fulton 3) (Mini Tracks)**		**Track 3 (Satchmo)**
1:00PM - 1:45PM	Is your remote employee from North Korea? A discussion on North Korean IT workers FBI New Orleans Cyber Crimes Squad	Containers Won't Fix Your Code: Unraveling the Elaborate Fabric of Security Theater *Kat Fitzgerald*	1:00PM - 1:35 PM	Beyond lip service - how can Security become an enabler like Safety *Vivek Poneda*	A Quest for Active Fingerprinting Excellence *Aaron Ringo*
			1:35PM - 2:10 PM	Cyber Maturity's Final Boss: Open, effective Communication and Collaboration *Peter Tomis*	
1:50PM - 2:35PM	Playing Chess in Cyber Insurance *Sarah Anderson*	The Rise of Shadow AI *Josh Copeland*	2:10PM - 2:40PM	We Have CSPM at Home: Using DuckDB and SQL to discover your lab's Cloud Security Posture *Jared Gore*	Building a Digital Fortress: The Indispensable Role of Security Visibility *Hunter Ely*
2:35PM - 2:55PM	**Networking Break and Technology Pavilion**				
3:00PM - 3:55PM	Closing Keynote Evolve, Adapt, and Overcome. The Art and Science of Cybersecurity *Clint Bodungen*				
4:00PM - 4:45PM	Ask Me Anything! *Dominic Vogel* / *Clint Bodungen*				
4:50PM - 5:00PM	Closing Remarks - BSidesNOLA Planning Committee				

BRONZE

paloalto NETWORKS

FORTINET

netskope

SecureNation

AVEXON SECURITY

AXONIUS

SMARTAPPROACH ADVISORY

VARONIS

abstract.security

ultraviolet

Semgrep

LUNCH/BEVERAGE

BISHOPFOX

5:00PM - 7:00PM	Jazz Happy Hour – Sponsored By TEKsystems	

PRESENTATION SUMMARIES

Main Hall Sessions

UNLEASH YOUR INNER LEADER!!! – DOMINIC VOGEL

Back to Program Guide

Most IT and cyber professionals overlook their foundational people skills. The ability to inspire, to lead, to rally a team. These are skills that most technical professionals do not take the time to develop and strengthen. This talk will identify the hidden leadership traits (authenticity, vulnerability, empathy, and kindness. This talk will provide practical and actionable ways for you to start unleashing your hidden inner leader!

REAL CONSEQUENCES OF ABSTRACT [SECURITY] RISK DECISIONS – RAF LOS

Back to Program Guide

Security professionals make risk decisions every day - that's what we're paid to do. We assess, analyze, and advise - and then our business counterparts act. Unfortunately, far too often the people who make the (security) risk decisions are far too disconnected from the downstream effects of these decisions. This not only creates friction, but we create situations where doing the right thing for security can have a catastrophic downstream effect - and the worst thing is we're blissfully unaware.

How does preventing an unpatched system from accessing the Internet affect your company's ability to make revenue - and how does that come back all the way around to impact your ability to hire? We'll talk through the processes, risk decisions, and impacts to give you a broader perspective which our industry desperately needs.

EVOLVE, ADAPT, AND OVERCOME. - THE ART AND SCIENCE OF CYBERSECURITY - CLINT BODUNGEN

TBA

Back to Program Guide

From the first macro worms that clogged inboxes to today's AI-powered deep-fake heists, the threat landscape never stops mutating—but the defenders who thrive are the ones who evolve faster. In this high-energy closing keynote, Air-Force-veteran-turned-cyber-game-maker Clint Bodungen distills three decades on the cyber front lines into a story of constant reinvention. You'll rocket through a living timeline that links late-1990s macro-outbreaks, modern supply-chain mega-breaches, and evolving AI-powered hackers that can exploit systems now faster than ever. Borrowing examples from other big tech industries and the (mis)quoted Darwin insight that "survival favors the most adaptable", Clint shows how the mantra "adapt, evolve, overcome" becomes a playbook for modern cybersecurity teams. Learn about real-world, cutting-edge techniques that Clint and his colleagues are putting into practice, today, to adapt to rapidly evolving technology and threats. To cap it all off, be ready for an exciting, first time ever, announcement that will accelerate your own cyber evolution.

Talk Tracks (Alphabetical)

A QUEST FOR ACTIVE FINGERPRINTING EXCELLENCE – AARON RINGO

Back to Program Guide

Both offensive and defensive work roles need to know what services are exposed. This talk will introduce/compare what's out there and lead into a deep dive on a chosen open-source service fingerprinter. The focus will then be on adding functionality to improve the detection times and results with reasoning on why changes are being made. The integration of these changes and update to the tool will be pair-programmed with low/no code AI.

ANDROID APP SECURITY (WITH A DASH OF LLM) – VAIBHAV AGRAWAL

Back to Program Guide

There are over 3 billion android devices in use worldwide, which includes mobile phones, smart watches, TV to name a few. The threat landscape increases as more and more devices use the Android platform.

Whether you're building the next hit app or securing existing ones, this session will equip you with the knowledge to find and protect against some modern android app threats. We will also discuss how LLM can be leveraged to find bugs in Android apps and demonstrate an open source LLM tool to do so.

BEYOND LIP SERVICE - HOW CAN SECURITY BECOME AN ENABLER LIKE SAFETY – VIVEK PONEDA

Back to Program Guide

Critical infrastructure companies take Safety very seriously. Organizations with VPP Star facilities to People & Products with Safety Certifications to a Safety Culture of Best Practices, most would encourage their employees to “Do it safely or not at all”. That’s not the case with Security today. This presentation addresses the key issues (awareness, capabilities and resources) and offers suggestions (training, risk assessment and planning) to flip the script on Security to make it just as ‘natural’ as Safety in enabling the company’s bottom line.

BREAKING DOWN (AND BREAKING INTO) PCI QSA: THE PATH, THE ROLE, AND WHY IT MATTERS – JAMES CHAD OLIVER

Back to Program Guide

Have you ever wondered what it takes to become a PCI Qualified Security Assessor (QSA)? In this talk, I’ll break down the path to QSA certification, including the prerequisite certifications you can choose from, and how they shape your knowledge in security and compliance. We’ll dive into the history of PCI DSS, why it exists, and how QSAs play a critical role in securing payment environments.

As a penetration tester, I’ll also highlight how red teamers and assessors collaborate to meet PCI DSS requirements—especially in areas like segmentation testing and vulnerability management. We’ll examine real-world breaches, including Magecart attacks, and how they led to key updates in PCI DSS 4.0. To keep things engaging, I’ll walk through some mock assessment scenarios, demonstrating tricky compliance requirements and what assessors look for when ensuring organizations are truly secure.

Whether you’re considering becoming a QSA, dealing with PCI compliance, or just curious about how security standards evolve, this talk will give you a practical and insightful look into the world of PCI DSS.

BREAKING INTO CYBER - ARUSHI GHILDIYAL / JENAH MANSOUR

Back to Program Guide

Cybersecurity is a rapidly growing and evolving field with a diverse range of career paths that go far beyond the stereotypical "hacker in a hoodie." This presentation is designed for students and aspiring professionals interested in breaking into cybersecurity but unsure where to start. We’ll explore the major domains of cybersecurity—offensive security (such as penetration testing and red teaming), defensive security

(including security operations, incident response, and threat hunting), and information security (governance, risk, compliance, and security awareness). Attendees will gain a clear understanding of the responsibilities, required skills, and real-world impact of each role. Additionally, we will highlight accessible resources such as hands-on labs, training platforms, mentorship opportunities, and certification pathways to help newcomers build skills and confidence. Whether you're a tech-savvy enthusiast or just beginning to explore the field, this session will demystify the landscape of cybersecurity and provide actionable steps to launch your journey.

BUILDING A DIGITAL FORTRESS: THE INDISPENSABLE ROLE OF SECURITY VISIBILITY – HUNTER ELY

Back to Program Guide

In today's interconnected world, organizations of all types face an escalating barrage of sophisticated cyber threats. The sheer volume and diversity of connected devices, from traditional IT infrastructure to burgeoning IoT and OT environments, create sprawling attack surfaces that traditional security measures struggle to defend. This talk examines why comprehensive security visibility is no longer a luxury, but a foundational requirement for robust cybersecurity.

CONTAINERS WON'T FIX YOUR CODE: UNRAVELING THE ELABORATE FABRIC OF SECURITY THEATER - KAT FITZGERALD

Back to Program Guide

In today’s cybersecurity world, it seems like everyone is chasing the next shiny object—whether it's the latest AI-driven defense tool or the newest, most complicated security gadget. Yet, despite all these fancy toys, breaches continue to rise faster than a teenager’s TikTok following. What gives? Have we lost our way?

This talk will take you on a journey through the history of IT, from the days when Sys Admins were the unsung heroes of the server room to today, where cybersecurity professionals juggle acronyms like WAF, EDR, and AI as if they were in a circus. Along the way, we’ll discover that the secret to stopping breaches isn’t found in the latest buzzword-laden product but in good old-fashioned basics. And yes, we’ll reminisce about “The Cuckoo’s Egg” while asking why anyone today would think a container is the magic bullet for insecure code. Spoiler alert: it’s not. By the end, you'll be ready to throw away the smoke and mirrors and focus on what really matters—the foundational practices that keep our digital world spinning.

CYBER MATURITY'S FINAL BOSS: OPEN, EFFECTIVE COMMUNICATION AND COLLABORATION– PETER TOMIS

Back to Program Guide

An organization can have a great executive and operations team and the most gifted IT/cyber security engineers the world has to offer, but without open collaboration and communication between these individuals the cyber program and subsequent security posture will be a poor reflection. By re-evaluating company culture, departmental boundaries, and learning the levels of communication required to appropriately tackle the cyber risks imminent in your organization, the road is to a secure tomorrow can be much shorter and more easily travelled.

CYBER WEREWOLVES: REWRITING THE RULES TO THE GAME AGAINST INSIDER THREATS – ROXEY DAVIS

Back to Program Guide

Insider threats don't kick down the front door — they walk in with an ID badge. Whether it's a rogue employee, an accidental misconfiguration, or a malicious threat actor inside our virtual walls, organizations must anticipate, detect, and mitigate risks before they escalate.

People learn often by experience, this interactive, scenario-driven session will dive into Threat-Informed Defense (TID) and how it can fortify security policies while proactively identifying insider risks. Using real-world threat intelligence, the MITRE ATT&CK framework, and behavioral analytics, we'll map adversary behaviors to policy decisions in real time.

Attendees will step into the shoes of a security team, investigating a simulated insider threat, analyzing data artifacts, and collaboratively updating security policies to prevent future incidents.

IS YOUR REMOTE EMPLOYEE FROM NORTH KOREA? A DISCUSSION ON NORTH KOREAN IT WORKERS – FBI NEW ORLEANS CYBER CRIMES SQUAD

Back to Program Guide

Over the past years, the FBI has seen an increase in North Korea actors acquiring remote jobs at US-based companies, conducting malicious activity and earning money to fund the DPRK. This presentation will discuss North Korean cyber activity and how they target companies, recent trends on the activities they conduct when hired, and mitigation steps to consider when hiring remote individuals for your company.

MENTAL HEALTH AND RESILIENCE - DEREK "THE CYBER WARRIOR" SCHELLER

Back to Program Guide

The importance of mental health and resilience for not only cybersecurity but life in general. This will also include ways to improve mental health, motivation, discipline, and resilience.

PLAYING CHESS IN CYBER INSURANCE - SARAH ANDERSON

Back to Program Guide

This presentation teaches you how to buy and recoup all available benefits under cyber insurance plans by identifying the competing motivations of the insured, the insurer, and the panel vendors. From an attorney's perspective, the audience learns to battle insurers in an effective manner that maximizes all available benefits to transform a crisis into opportunity.

THE RISE OF SHADOW AI – JOSH COPELAND

Back to Program Guide

As artificial intelligence continues to transform industries, the emergence of Shadow AI—unauthorized or unsanctioned AI applications and systems—presents new challenges and opportunities for organizations. This presentation explores the dual nature of AI's growth, highlighting the benefits of sanctioned AI while shedding light on the risks posed by Shadow AI. Attendees will gain insights into the factors driving the rise of Shadow AI, including the increasing accessibility of AI tools and the pressure to innovate rapidly. We will also discuss strategies for identifying, managing, and mitigating the risks associated with Shadow AI, ensuring that organizations can harness the power of AI responsibly and securely. Join us as we navigate the AI frontier and uncover the hidden forces shaping the future of technology.

TRANSFORMING CYBER RISK ASSESSMENTS THROUGH CONTINUOUS VALIDATION - IRINA LOKTIONOVA AND CHRIS OSHABEN

Back to Program Guide

Traditional cyber risk assessments often provide limited value. They rely on subjective ratings, compliance checklists, and infrequent evaluations that fail to drive actionable security improvements. This session introduces a modern approach to make risk assessments more timely, relevant, and actionable by increasing assessment frequency, focusing on real-world threats, and building a continuous feedback loop to validate control effectiveness.

Attendees will learn a structured methodology integrating threat intelligence, asset inventory, vulnerability analysis, prioritized controls, and ongoing validation. The talk will also provide real-world examples of continuous control validation methods, such as leveraging Micro-Purple Testing to continuously validate SIEM detections and using automated configuration monitoring tools to ensure endpoint detection and response protections remain effective. This session will help security practitioners shift from compliance-driven assessments to dynamic risk management that continuously improves cyber resilience.

WE HAVE CSPM AT HOME: USING DUCKDB AND SQL TO DISCOVER YOUR LAB'S CLOUD SECURITY POSTURE - JARED GORE

Back to Program Guide

At work we have Wiz, at home we can't afford a pot to piss in. That doesn't stop us from wanting to learn, play, and hack in our own personal cloud environments.

This talk introduces an alternative approach using DuckDB—a lightweight, embeddable analytical database—combined with SQL to create a flexible, cost-effective security monitoring solution. We demonstrate how DuckDB's native integrations with cloud storage platforms (AWS S3, Azure Blob Storage, Google Cloud Storage) enable direct querying of audit logs, network flow data, and configuration files without expensive intermediaries. Attendees will learn how to implement automated scripts for collecting cloud resource configurations, storing them in DuckDB, and writing SQL queries that detect security misconfigurations, compliance violations, and potential threats. Through practical examples, we'll show how this approach can provide comparable visibility to commercial CSPM tools while offering greater customization and significant cost savings. This session is ideal for students and security professionals seeking pragmatic solutions to cloud security monitoring challenges in budget-constrained lab environments.

WHEN THE (UN)EXPECTED HAPPENS - MIRIAM LORBERT

Back to Program Guide

Experience and participate in an interactive, real-life OT/ICS tabletop exercise!!

BIOS

AARON RINGO

Back to Program Guide

Over a decade of experience in communications and computer network operations. Proven work performance in high stress no fail environments.

CHRIS OSHABEN

Back to Program Guide

Chris Oshaben is a Senior Security Auditor at Delta Dental of California, specializing in cybersecurity risk management, internal controls, and compliance assurance. With extensive experience auditing security programs against frameworks such as NIST CSF, SOC 2, ISO 27001, HIPAA, PCI DSS, 23 NYCRR 500, and CIS CSC, Chris partners closely with organizational stakeholders to identify critical risks, enhance security maturity, and validate effective controls. He is adept at translating complex technical risks into clear, actionable insights that drive strategic decision-making. Chris holds professional certifications including CISA, CRISC, CISM, CCSK, and CDPSE, reflecting his deep commitment to cybersecurity excellence, risk-informed decision making, and continuous security improvement.

CLINT BODUNGEN

Back to Program Guide

Clint Bodungen is a globally recognized ICS cybersecurity professional and thought leader with 30 years of experience (focusing primarily on industrial cybersecurity, red teaming, and risk assessment). He is the author of two best-selling books, "Hacking Exposed: Industrial Control Systems" and “ChatGPT for Cybersecurity Cookbook.” He is a United States Air Force veteran and has worked for notable cybersecurity firms like Symantec, Booz Allen Hamilton, and Kaspersky Lab, and is currently the Founder/Head of Product Innovation at ThreatGEN® as well as the Director of Cyber Innovation at MorganFranklin Cyber. Renowned for his creative approach to cybersecurity education and training, Clint has been at the forefront of integrating gamification and AI applications into cybersecurity training. He created “ThreatGEN® Red vs. Blue”, the world's first online multiplayer computer designed to teach real-world cybersecurity and “AutoTableTop”, which uses the latest generative AI technology to automate, simplify, and enhance IR tabletop exercises. As AI technology continues to evolve, he hopes to help revolutionize the cybersecurity industry using gamification and generative AI.

DEREK “THE CYBER WARRIOR” SCHELLER

Back to Program Guide

Derek "The Cyber Warrior" Scheller is a retired army veteran who started in helpdesk and IT in 2004. He pivoted to cybersecurity in 2008 and hasn't looked back since. After retiring from the military in 2017, he entered the private sector as a blue team specialist, working a few jobs in offensive security as well. He now works in leadership and has worked extensively to help people stay motivated and find their path in cybersecurity. He hosts a weekly show called Security Happy Hour on YouTube, has a 50-episode self-improvement podcast called Walk With Me, and consistently posts short-form content to help people stay disciplined, motivated, and take ownership of their lives.

DOMINIC VOGEL

Back to Program Guide

Dominic Vogel is a well-respected cyber security thought leader appearing on media news outlets across the world. As a veteran cyber security expert and thought leader, Dominic holds a proven track record across multitude of industries (financial services, logistics, transportation, healthcare, government, telecommunications, and critical infrastructure).

Dominic is a firm believer in delivering sustainable security that supports and protects business goals. Having worked within large and globally diverse organizations he has extensive security experience that has been forged over the past two decades as an information security professional.

Dominic is a 2x founder who has focused on providing unbiased actionable cyber security strategic guidance and advice to startups and small businesses across North America.

Dominic is the President at Vogel Coaching & Leadership Services, a Vancouver-based leadership advisory company specializing in cyber security, and hosts the Cyber Security Matters Podcast, a highly regarded podcast that explores the intersection between cyber security and business.

He is also a self-professed positive troll and professional hype man and believes in the power of uplifting others through his high-energy coaching practice.

HUNTER ELY

Back to Program Guide

Career dedicated to supporting the mission of education. Faced a pivotal moment at 19, nearly leaving LSU due to tuition costs. Fortunate internship led to over a decade supporting LSU as a network administrator, forensics examiner, and security engineer. Transitioned to Tulane as the institution's first full-time Chief Information Security Officer. At Tulane, spearheaded the creation of a security operation, developed programs aligning with academic, research, and operational goals, and implemented a security approach prioritizing community needs for effective and user-friendly solutions. Following nearly eight years at Tulane, moved to the private sector, continuing to support education. Driven by a passion to advance teaching and research.

IRINA LOKTIONAVA

Back to Program Guide

Irina Loktionova is a seasoned Senior Cyber Risk Management Architect at Delta Dental of California with over a decade of experience in incident response, threat intelligence, and proactive threat hunting. Leading 24/7 cybersecurity operations, Irina

specializes in leveraging the MITRE ATT&CK framework for continuous security improvement, developing sophisticated detection methods, and conducting digital forensic investigations. Certified by HarvardX in Cybersecurity Risk Management and as a Proofpoint Certified Email Authentication Specialist, Irina is dedicated to enhancing organizational resilience by integrating cutting-edge detection capabilities with real-world threat scenarios.

JAMES CHAD OLIVIER

Back to Program Guide

James Chad Olivier is an information security consultant with over 25 years of experience. He began his career as a developer before shifting his focus to security, where he spent the majority of his career as a penetration tester. Throughout his career, he has led teams in identifying and exploiting security weaknesses across industries and organizations of all sizes.

In his current role as Director of Technical Audits, James continues to lead penetration testing engagements while also conducting PCI DSS assessments for major corporations in insurance, equipment manufacturing, and finance—including one of the major card brands. His expertise spans offensive security, compliance, and technical risk assessment, making him a trusted advisor in securing critical systems against evolving threats.

JARED GORE

Back to Program Guide

Jared is a Cloud Security Engineer at Paychex who loves golang and spends his days f#%!king (up production) and fighting (burn out). He holds a CISSP, is 5x GIAC and AWS Security certified - will do dirty things for a CPE or AMF.

JOSH COPELAND

Back to Program Guide

Joshua Copeland is a battle-tested cybersecurity expert with a wealth of experience in the field. He is a 20 -year veteran of the Air Force and has served in leadership roles with Crescendo AI, Quadrant Security, Bose, AT&T, and GDIT, focusing on security operations, governance, and the cloud. He is a sought-after guest speaker at prestigious conferences such as BlackHat, BSides, and RSAC, and his expertise makes him a highly coveted guest for podcasts and webinars. Joshua is also a member of the adjunct faculty at Tulane University, teaching cybersecurity and leadership.

Joshua holds a Master of Science in Cybersecurity Management from Tulane University and a Bachelor of Science in Information Systems (with Honors) from Charter Oak State College. His dedication to professional growth is evident through his impressive

collection of over 80 certifications from esteemed organizations such as ETA-I, CompTIA, ISC(2), EC-Council, and the Air Force. Furthermore, Joshua has made substantial contributions to the field, serving as a co-author for ETA's Network Systems Technician since 2016 and Information Technology Security since 2020. He also served as the technical editor for the book titled "The Art and Math of Cryptography: A Practical Guide for Cybersecurity Professionals." Joshua's expertise extends to publishing articles in esteemed publications like High Tech News and Cyber Security Review, where he delves into various topics related to cybersecurity and IT/cybersecurity leadership.

KAT FITZGERALD

Back to Program Guide

Chicago-based and proudly a natural creature of winter, I thrive on snow, OSS, and just the right amount of chaos. Whether sipping Grand Mayan Extra Añejo or warding off cyber threats with a mix of honeypots, magic spells, and a very opinionated flamingo named Sasha (the BSidesChicago.org mascot), I keep things interesting. Honeypots and refrigerators rank among my favorite things—though my neighbors would likely disagree.

MIRIAM LORBERT

Back to Program Guide

Miriam is a Senior Manager within Accenture Security, where she helps lead the OT Security practice. With over 10 years of experience in the industrial cybersecurity space, Miriam is an Industrial Cybersecurity subject matter expert applying firsthand experience in understanding industry challenges and protecting critical infrastructure.

PETER TOMIS

Back to Program Guide

Peter happened to be given a PC with an internet connection far earlier than any of his peers. Resulting from a lifetime of watching technology shape the world around him for better and worse, he discovered a deep passion for safeguarding individuals and digital infrastructures against evolving threats. Currently he applies his knowledge and experience thereof as a Systems Engineer at the most trusted Cyber Security company in America, Fortinet.

RAFAL LOS

Back to Program Guide

Rafal is an industry veteran and founder and host of the industry's longest-running security podcast - the Down the Security Rabbithole Podcast. Rafal's journey in cybersecurity spans over 25 years and has focused on building and optimizing professional and managed services, cross-functional problem-solving, and a wide range of customer-facing roles. His passions are his family, outdoor

adventuring, ice hockey and using his gifts to make a positive impact on the world around him. Rafal is a speaker, a writer, a well-known podcaster, and industry personality.

ROXEY DAVIS

Back to Program Guide

Currently, Roxey serves as a key player in the cybersecurity space at FNBO, where her focus is on proactive threat detection and response. With advanced skills in tools like Splunk and SentinelOne, she excels in identifying and mitigating security risks before they escalate, contributing to the development of robust threat intelligence and security policies. Her work is instrumental in strengthening defenses and creating a safer digital environment.

SARAH ANDERSON

Back to Program Guide

Sarah W. Anderson founded SWA Law LLC and LegallyCyber.com, representing public and private entities on cyber incident response, regulatory compliance, the implementation of enhanced cybersecurity practices, artificial intelligence integration, and contract negotiations involving technology products and services. Sarah teaches seminars on cybersecurity law across the United States, for non-profits, trade associations, corporate entities, and government entities. In less than 3 years, Sarah expanded SWA Law LLC from a solo practice to three (3) attorneys, with one (1) Certified Information Privacy Professional/US.

VAIBHAV AGRAWAL

Back to Program Guide

From software developer to seasoned security engineer, brings over ten years of experience safeguarding digital assets. Core expertise lies in the security of web, API, mobile, and LLM applications. Complementing this, academic and industry background provides a strong foundation in infrastructure, cloud, and Windows Active Directory security and privacy.

VIVEK PONEDA

Back to Program Guide

Vivek Ponnada is an Operational Technology (OT) Security practitioner with global experience and currently serves as SVP of Growth & Strategy at Frenos, the first Autonomous OT Security Assessment Platform. Having started his career in Industrial Control Systems (ICS) as a Technician, Vivek became a Controls Engineer and commissioned Gas Turbines in Europe, Middle-East, Africa and South-East Asia. Post MBA, Vivek held multiple roles including Sales, Marketing & Business Development and Services covering ICS and OT

Security solutions for Critical Infrastructure industries (Power, Oil & Gas, Water, Mining etc.) at GE, XenonCyber Dynamics and Nozomi Networks. He is the co-lead for the Top 20 Secure PLC Coding Practices Project and his recent talks/contributions include ICS Cybersecurity Conference in Atlanta (Security Week), Industrial Security Conference in Copenhagen, several BSides and others. Vivek has a C.Eng from I.E. India, MBA from The University of Texas at Austin and GICSP certification from GIAC. He is a member of the ISA, ISACA, Public Safety Canada ICS Security Symposium Advisory Committee and is a CS2AI Fellow.