Event Agenda

2025 UNC Charlotte Cybersecurity Symposium

Tuesday, September 30, 2025

Registration and Continental Breakfast

8:00 AM – 9:00 AM

REGISTRATION

ADventuring in Active Directory

9:00 AM – 12:00 PM | Location: Student activity center salons C

ATTACK AND DEFEND

Workshop Description:

ADventuring in Active Directory is a four-hour workshop focused on common attacks used against Active Directory environments. Through a mixture of lecture and hands-on exercises, participants will discover ways to examine an Active Directory environment for a variety of common misconfigurations and then exploit these issues to pivot and escalate their access. Not only will the workshop cover the different attacks but also the details of why the attacks work and how an environment can be made resilient to them, making it useful to those looking to hone their offensive skills as well as those who are protecting networks.

Participants will be provided access to a lab but will need to bring a laptop that can connect to a Windows server through Remote Desktop. While attendees don't necessarily need any prior security experience to take this course, they will get the most out of it with a basic grasp of Windows operating systems and PowerShell.

Speaker

Eric Kuehn

Principal Security Consultant | Secure Ideas

Secure Agentic Development Workshop

9:00 AM – 12:00 PM | Location: Student activity center salons DE

AI AND SECURITY

Workshop Description:

AI agents bring power - and new attack surfaces. In this hands-on workshop, we'll map the core threats (prompt injections, data leaks, hallucinations, misalignment and approval bypass), then walk through how to design and deploy agents securely. Participants will understand basic agentic threat modeling, guardrails, auditing, and MCP deployment hardening. We'll explore why runtime guardrails alone fail, and show how to build multi-layer defenses with monitoring, HITL, and red-team style evaluations. The session closes with a live multi-agent CTF - where you'll exploit, patch, and harden your chatbots.

Outline

1. Agent Threat Landscape Intro
2. Emerging Attacks: phishing, hallucination exploits, prompt injections, approval bypass
3. Secure-by-design Agents - Components: threat modeling, testing, guardrails, auditability
4. MCP Security & Agentic Deployment hardening
5. Live Exercise: Spot Vulnerabilities in Agentic Code & MCP Tools
6. Beyond runtime guardrails - defense-in-depth controls
    1. Building Multi-Layer defenses
    2. Monitoring, HITL & Auditing
    3. Recommended Evaluation: Test-Suites & Red-Teaming Guidance
7. Live Multi-Agent CTF: Exploit chatbots for fun and profit

Speakers

Barak Sternberg

CEO | Tenet Security

Nevo Poran

CTO | Tenet Security

PwmPower

9:00 AM – 12:00 PM | Location: Student activity center salons AB

ATTACK AND DEFEND

Workshop Description:

The PwnPower workshop gives attendees hands-on experience with hardware hacking by converting IoT smart plugs into Wi-Fi

penetration testing implants. Participants will explore fundamental hardware concepts, common hardware protocols, soldering techniques, hardware exploitation, and red team operations. This session is designed to provide practical insight into offensive security through real-world hardware modification.

Speaker

Jacob Glenn

Founder of Offensive Appliances | Hak5

Lunch

12:00 PM – 1:00 PM | Location: Student Activity Center Salons

LUNCH

Stop Guessing, Start Governing: A Cyber Risk Workshop with the CRF GRC Roadmap

1:00 PM – 4:00 PM | Location: Student activity center salons DE

RISK MANAGEMENT

Turn uncertainty into clarity with a simple, seven-step roadmap for governing cyber risk that leaders can trust.

Abstract:

Too often, organizations “guess” their way through cyber risk decisions — leaving leaders uncertain and programs reactive. The CRF Governance & Risk Model (CRF-GRM) changes that by offering a clear, seven-step roadmap for governing cybersecurity in business terms.

In this interactive workshop, participants will move beyond theory and begin applying the CRF-GRM directly to their own organizations. Through guided instruction and practical exercises, attendees will draft the early stages of their governance roadmap, share insights with peers, and translate lessons into a 90-day action plan they can use immediately.

Whether you are new to governance or an experienced security leader, this session will equip you with the clarity, confidence, and tools to align cyber risk with business goals and communicate progress in a way executives can trust. You’ll walk away empowered to stop guessing — and start governing.

Workshop Overview:

Are you ready to stop guessing about cyber risk and start governing with confidence? This isn’t just another cybersecurity session – it’s your chance to transform how your organization manages risk. You’ll leave empowered, energized, and equipped to move from talk to tangible action.

In this hands-on workshop, you will dive into the seven-step CRF Governance & Risk Model (CRF-GRM), a free and open-source roadmap designed to help organizations align cybersecurity with business objectives. You won’t just learn the model — you’ll apply it to your own organization using practical worksheets and templates. Whether you’re new to governance or a seasoned leader, this session will give you clarity, confidence, and momentum to lead with purpose.

Learning Objectives:

By the end of this workshop, participants will:

1. Master the CRF Governance & Risk Model (CRF-GRM):

Walk step-by-step through the seven phases of the model—Initiate, Inventory, Select, Educate, Implement, Validate, and Communicate —and discover how each stage strengthens your organization.

Website: https://crfsecure.org/research/crf-governance-and-risk-model/

2. Apply the Roadmap in Real Time:

Use guided worksheets to begin drafting a governance roadmap tailored to your company, turning information into immediate application.

3. Learn from Peers:

Share insights and challenges with other professionals, gaining new perspectives and practical solutions to strengthen your approach.

4. Leave Empowered and Equipped:

Walk away with tools, templates, and a 90-day action plan you can start using right away to communicate your strategy and drive results. Workshop Agenda:

1. Introduction to the CRF Governance & Risk Model (CRF-GRM)

-Time: 45 minutes

-Objective: Discover how the CRF-GRM provides a clear, actionable roadmap for governing cybersecurity. Explore the seven steps and learn how to apply them to your organization.

2. Application Session: Build Your Governance Roadmap

-Time: 1 hour

-Objective: Roll up your sleeves and begin creating your own governance roadmap using the CRF-GRM worksheets. Work through the early steps (Initiate, Inventory, and Select) with practical guidance.

3. Interactive Discussion: Peer Insights and Challenges

-Time: 30 minutes

-Objective: Share your draft roadmap, discuss common governance challenges, and learn from peers tackling similar issues.

4. Next Steps and Actionable Insights

-Time: 30 minutes

-Objective: Translate your draft into a 90-day action plan with clear goals and metrics. Walk away empowered to communicate your progress and lead with confidence. Target Audience:

This workshop is designed for CISOs, cybersecurity leaders, IT managers, and organizational decision-makers who want to move from awareness to action. Whether you're building governance from the ground up or refining a mature program, you'll leave with fresh tools, a practical roadmap, and renewed confidence to lead.

Workshop Resources:

•Free CRF-GRM Worksheets & Templates (provided at the beginning of the session)

•Example 90-Day Action Plan Template

•Access to the open-source CRF Governance & Risk Model

Speaker

Russell Eubanks

Principal Consultant and Co-Founder | Cyverity

Cloud Capture the Flag

1:00 PM – 4:00 PM | Location: Student activity center salons AB

AI AND SECURITY

Exposing the Hidden Risks: Securing AI Workloads in the Cloud Era

As enterprises race to adopt generative AI and cloud-native technologies, many are unknowingly deploying AI workloads riddled with critical vulnerabilities and misconfigurations. In this session, we'll uncover insights from Tenable's 2025 Cloud AI Risk Report, revealing how AI-powered services—like AWS SageMaker, Amazon Bedrock, and Google Vertex AI—are being deployed with default permissions and public access that expose sensitive data and increase the attack surface.

We'll introduce Tenable AI Exposure, a new framework for managing AI-specific risks in cloud environments. Attendees will learn how to:

- Identify shadow AI and misconfigured AI workloads across cloud platforms
- Prioritize and remediate AI-specific risks such as prompt injection and model abuse
- Enforce governance and data protection policies for enterprise AI usage

Whether you're building AI solutions or securing them, this session delivers actionable strategies for protecting your organization's most intelligent assets—before they become your biggest liabilities.

Bonus: Capture the Flag (CTF) Workshop

Following the talk, join our interactive CTF workshop, where you'll apply what you've learned in a hands-on lab. Test your skills by identifying misconfigurations, uncovering over privileged accounts, exploiting insecure AI pipelines—and racing others to secure them.

Whether you're a cloud security engineer, AI architect, or red team enthusiast, this session offers both strategic insights and practical experience to help you defend your AI-powered future.

Speaker

Frank Passman

Account Manager, Cloud Security | Tenable

Binary Exploitation and Exploit Defense: A Hands-On Deep Dive

1:00 PM – 4:00 PM | Location: Student activity center salons C

ATTACK AND DEFEND

Abstract:

In this course, with all-new interactive visual demos of buffer overflows, you will learn low-level, binary exploitation skills; specifically how to exploit buffer overflows and "smash the stack". We will examine the various mitigations that have been put in place including NX and ASLR since exploits of this type of vulnerability were first published in 1988, as well as each of those defense's weaknesses. The skills taught in this course are critical for those in Offensive roles including Adversary Emulation and Exploit Writing; and Defensive roles including Reverse Engineering, Malware Research, and some Tier II and Tier III SOC Analyst roles. In order to accurately emulate the threats you face, you have to know how to be able to write them; and in order to effectively analyze the threats, one needs to know some of the common patterns in how they work. Finally, the course will show how to implement a new type of solution called "Consensus-Based Defense", and demonstrate why it puts an end to the attacks on our example binaries, due to the exploit string needing to satisfy a logical impossibility. We will also show how Consensus-Based Defense applied to Nginx and IIS webservers reduces the number of exploits faced in the past 10 years from over 20 to 0.

Requirement:

Students should have both Windows and Linux available to run the binaries used in the course (with full admin rights), which can be in either a VM or on the host. Kali VM, preinstall Ghidra and note that 64-bit VMs are required to run the latest version of Ghidra. Dedicate 4 GB RAM and 2 processor cores to the VM.Also, students should have a Git client on the same system that has the JRE installed. Also, it is critical that students have a recent Java Runtime Environment installed, additionally, another requirement is 7-Zip.

Speaker

Parker Garrison

Startup Founder and CEO | Iguana Cyber

Wednesday, October 01, 2025

Registration and Continental Breakfast

7:30 AM – 8:30 AM | Location: Lucas/lobby

REGISTRATION

Exibition Hall

7:30 AM – 4:15 PM | Location: Lucas/lobby

EXIBITION HALL

Opening remarks

8:30 AM – 8:45 AM | Location: Cone McKnight

KEYNOTE

Vulna-palooza: Lessons Learned from a Half-Century of Vulns, 1983-2033 A Jaunty (but Practical) Romp Down Memory Lane

8:45 AM – 9:05 AM | Location: Cone McKnight

KEYNOTE

Speaker

Ed Skoudis

President | SANS Institute

Applying Lessons Learned in the Age of AI

9:05 AM – 9:40 AM | Location: Cone McKnight

KEYNOTE PANEL

Abstract:

As both attackers and defenders harness AI, our hard-earned cybersecurity lessons still apply—but their priority and expression change. This expert panel will examine possible failure patterns involving AI systems, and outline strategic controls that matter the most. Rather than chasing every new attack or feature, the goal is to operationalize discipline, so that AI capabilities accelerate the mission without expanding the attack surface, and defenders regain the initiative.

Speaker

Kristopher Fador

Chief Information Security Officer | Bank of America

Keynote Q&A

9:40 AM – 9:50 AM | Location: Cone McKnight

KEYNOTE

Break

9:50 AM – 10:05 AM | Location: Lucas/lobby

EXIBITION HALL

The Next Frontier - Generative AI & Cybersecurity Careers

10:05 AM – 10:50 AM | Location: Cone McKnight

CAREER DEVELOPMENT

Abstract:

Generative AI is transforming cybersecurity work, from automating tasks to reshaping required skills. This panel of experts will explore how AI aligns with cybersecurity structures and capabilities, highlight risks of overreliance, and share practical steps professionals can take to adapt. Attendees will gain fresh insights and actionable ideas to future-proof their cybersecurity careers.

Speakers

Todd Inskeep

Founder and Senior Director | Incovate Solutions

Ed Skoudis

President | SANS Institute

John Melton

Director of Product Security | Oracle Netsuite

Zscaler AI Guard: Redefining Threat Defense with Intelligent Detection and Response

10:05 AM – 10:50 AM | Location: Cone 210A

AI AND SECURITY

Abstract:

In an era where cyber threats evolve faster than ever, traditional security measures often lag behind. Zscaler AI Guard is at the forefront of innovation, leveraging artificial intelligence and machine learning to transform threat detection and response. This session will explore how AI Guard processes billions of data points across Zscaler's global Zero Trust Exchange to deliver real-time threat intelligence, predictive analytics, and automated mitigation strategies. Attendees will learn how AI Guard enables proactive defense against zero-day threats, increases operational efficiency by reducing alert fatigue, and enhances decision-making for security teams with contextual insights. Whether defending against ransomware, phishing, or insider attacks, Zscaler AI Guard equips enterprises to stay ahead of attackers and maintain a resilient posture in today's threat landscape.

Takeaways:

- Understand the core capabilities of Zscaler AI Guard in threat detection and response.
- Discover how predictive analytics and automated workflows reduce risk and save time.
- Learn actionable strategies for integrating AI-powered defenses into your security framework.
- Make informed, data-driven decisions by harnessing the power of Zscaler AI Guard for intelligent and agile threat management.

Speaker

Benjamin Corll

CISO in Residence | Zscalar

Beyond the Keys: Rethinking Crypto Security for a Mainstream Future

10:05 AM – 10:50 AM | Location: Cone 208

ATTACK AND DEFEND

Abstract

From "Not your keys, not your coins" to billion-dollar hacks, custody remains the defining challenge for digital assets. Kyriakos Skiouris, CTO and Co-Founder of Agingo, explores wallet models, human risk, and smart contract exploits while highlighting innovations like multi-party computation, zero-knowledge proofs, and social recovery. Looking ahead to AI scams and quantum threats, he asks: can crypto security ever feel as mature as online banking by 2030?

Speaker

Kyriakos Skiouris

Co-Founder and CTO | Agingo

Governing Ethical Drift In Agentic AI: A Relational AI Ethics Framework for Safe Human-AI Co-evolution

10:05 AM – 10:50 AM | Location: Cone 113

AI AND SECURITY

Speakers

Wolfgang Rohde

Exec. Director of Innovation and Strategy | AiSuNe

Rick Doten

VC and Startup Advisory Board Member, AI Governance and Ethics Researcher | Multiple Companies

Reducing Randomness: Creating the Next Generation of Identity Professionals

10:05 AM – 10:50 AM | Location: Cone 111

CAREER DEVELOPMENT

Abstract:

In the Identity Professionals Skills Survey published by IDPro, one consistent theme to emerge over the years is that digital identity professionals come from a broad variety of backgrounds. In some respects, this reflects both a strength of the community in its diversity and is part of a critical challenge in finding and retaining talent. But what if we could provide a catalyst to speed up some of that development in a classic setting, such as higher education?

In this session, we will discuss the current challenges in finding and developing talent, propose a path that attempts to enhance what most higher-ed curriculums are trying to achieve and offer a 'call to arms' to support this critical effort on a number of fronts: publishing knowledge, searching beyond the narrow scope of security, development of curriculum, and teaching.

Speaker

Lance Peterman

Manager, Identity & Access Management | Dick's Sporting Goods

Packets Don’t Lie: Revealing Threat Actor TTPs

10:05 AM – 10:50 AM | Location: Cone 210B

ATTACK AND DEFEND

Abstract:

Packets don’t lie; they are the source of truth for an organization’s network. Threat actors, on the other hand, “lie”; threat actors like LockBit and Volt Typhoon exploit organizations and hide in the noise of daily operations. The uncomfortable truth is that many organizations already have threat actors operating inside. This session will discuss how the OODA Loop (Observe, Orient, Decide, Act Loop) applies to both threat actors and cybersecurity defenders. It will also provide insights on threat actor TTPs as well as how cybersecurity professionals can use network detection and packet analysis to discover these TTPs. By illuminating threat actor behavior in a timely manner, cyber defenders can disrupt the threat actor’s OODA Loop, impact their maneuver, and deny them the ability to achieve their objective.

Speaker

Chad E. LeMaire

Chief Information Security Officer | ExtraHop

Fake IT workers

10:05 AM – 10:50 AM | Location: Library Halton Reading Room

GRC

Speakers

Brian Russell

Lead Info Sec Threat Hunting Specialist | TIAA

Seth Hagan

Cyber Threat Hunter | TIAA

Dawn M. Haley

Senior Manager, Threat Management | Duke Energy

William E. Galipeau

Sr. Vice PresidentHead of Truist Enterprise Insider Threat Program | Truist

AI-Driven Cyber Risk Intelligence Across the Supply Chain

10:05 AM – 10:50 AM | Location: Cone 112B

ATTACK AND DEFEND

Abstract:

The future of cyber risk management lies in automation. Traditional risk assessments are often resource-intensive, slow, and lack the dynamic context required for timely decision-making. In this session, explore how Black Kite innovatively embeds AI into the core of its Third-Party Cyber Risk Management platform to transform cyber risk assessments from manual, static processes into real-time, automated, and defensible intelligence.

Speakers

Jefferson Pike

Information Security Director | Lowe's

Conor Coveney

Senior Account Executive | Black Kite

Mitchell Wahl

Strategic Alliances leader | Black Kite

Two Jacks, One Standard: Cyber Risk Quantification

10:05 AM – 10:50 AM | Location: Cone 112A

GRC

Abstract:

Cybersecurity leaders are under pressure to explain risk in business terms, justify investments, and meet regulatory expectations. In this fireside chat, Jack Jones and Jack Freund, coauthors of Measuring and Managing Information Risk, discuss how the FAIR model and FAIR-CAM bring rigor to cyber risk measurement. They will explore how quantification improves decision making, where automation and AI fit into the picture, and why moving beyond qualitative guesswork has become essential for modern cyber governance.

Speakers

Dr. Jack Freund

Head of Technology Risk | Accrisure

Brent Biglow

President | Charlotte ISSA

Jack Jones

Strategic Advisor | Safe Security

Break

10:50 AM – 11:05 AM | Location: Lucas/lobby

EXIBITION HALL

Securing the Future: The Interplay of Global Politics, Regulation, and Infrastructure Resilience

11:05 AM – 11:50 AM | Location: Cone McKnight

ATTACK AND DEFEND

Abstract:

The global cybersecurity landscape is being reshaped by rapidly evolving geo-political forces and an increasingly complex regulatory environment. As organizations expand across borders and digital threats become more sophisticated, ensuring robust infrastructure resilience while meeting regulatory compliance is more challenging—and more critical—than ever.

Hear from Cisco experts Matt Fussa, Megan Inman, and XYZ provide a holistic perspective on these converging trends. The session will examine how shifting geo-political dynamics are driving new compliance requirements and influencing corporate security strategies. Attendees will gain practical insights on:

- The current and emerging geo-political forces shaping the global cyber threat and regulatory landscape

- Key trends in global compliance and the implications for multinational organizations

- Strategies for building resilient infrastructure that can adapt to regulatory changes and withstand cyber threats

This session will offer valuable global insights and feature actionable guidance to help organizations future-proof their security posture amid ongoing global uncertainty.

Proposed Agenda (45 minutes)

- Introductions (3 min)

- Geo-Political Landscape (Megan Inman 7-8 min)

- Global Compliance Trends & Challenges (Matt Fussa, 9-10 min)

- Building Infrastructure Resilience (TBC 8-9 min)

- Panel Discussion & Audience Q&A (15 min)

Speakers

Matt Fussa

Vice President, Trust & Compliance Officer | CISCO

Jeff Schutt

Principal Engineer | CISCO

Should the U.S. Military Defend Corporate Enterprises from Cyber Attacks by Domestic and Foreign Actors?

11:05 AM – 11:50 AM | Location: Cone 210A

ATTACK AND DEFEND

Speakers

Jeffrey DiMuro

Deputy Chief Security Officer | ServiceNow

Madison Horn

Senior Director, National Security Strategy & Policy, World Wide Technology | World Wide Technology

Dr. Jack Freund

Head of Technology Risk | Accrisure

Resilience Beyond the Firewall: Leadership Lessons from a Cybersecurity Journey

11:05 AM – 11:50 AM | Location: Cone 208

CISO

Abstract:

Cybersecurity has always been about resilience—but resilience isn't just about systems, it's about leaders. In this keynote, Amy Bogac shares lessons from over 20 years on the frontlines of security leadership, weaving together career-defining moments with insights on navigating uncertainty, reclaiming narrative, and staying anchored to purpose.

Through five phases of her own journey—finding what matters, bringing clarity in times of chaos, leading when control is gone, taking back the narrative, and sustaining passion—Amy shows how resilience is built not by avoiding disruption, but by how leaders respond to it.

Attendees will walk away with:

- Practical ways to ground themselves in purpose during change.
- Strategies for clear, credible communication in high-pressure situations.
- Inspiration to reframe setbacks and reclaim the story of their careers.
- A reminder that passion—not fear—is the ultimate driver of resilience.

This talk is designed for cybersecurity professionals, IT leaders, and anyone seeking to evolve their leadership in a world defined by constant disruption.

Speaker

Amy Bogac

Chief Information Security Officer | Baker Tilly

AI Insider Threat

11:05 AM – 11:50 AM | Location: Cone 113

AI AND SECURITY

Speakers

Patrick Nord

CISSP | ArchetypeSC

Frankie Warren

ArchetypeSC

From AI Adoption to AI Risk: Building Resilient Enterprises in the AI Era

11:05 AM – 11:50 AM | Location: Cone 111

AI AND SECURITY

Abstract:

From defending with AI to securing AI itself, Tenable helps organizations reduce risk across the modern attack surface. This session explores practical strategies for visibility, risk prioritization, and governance that security leaders can act on today.

Speaker

Damien Lim

Sr. Product Marketing Manager | Tenable

AI in OT Security: Hype vs. Reality

11:05 AM – 11:50 AM | Location: Cone 210B

ATTACK AND DEFEND

Abstract:

As artificial intelligence (AI) continues to influence cybersecurity, its role in Operational Technology (OT) environments raises both promise and concern. This joint session from Duke Energy and Nozomi Networks offers a dual perspective—strategic and technical—on how AI is shaping OT security.

Duke Energy will explore where AI can enhance OT capabilities and where its limitations introduce risk. Topics include governance, open-source vs. proprietary models, and how to critically assess vendor claims to avoid unrealistic expectations.

Nozomi Networks will provide a transparent look at how AI is implemented in their platform—beyond the buzzwords. They'll share how their models support threat detection, how performance is validated, and what success looks like in real-world industrial deployments.

Whether you're researching the future of AI in critical infrastructure or deploying solutions in the field, this session offers grounded insights to help you navigate the complexity with clarity.

Speakers

Jonathan Mora

Lead OT Cybersecurity Analyst | Duke Energy

Ben Callaway

Regional Sales Director | Nozomi Networks

Tim Pierce

Senior Technical Sales Engineer | Nozomi Networks

Annual cybersecurity legal review

11:05 AM – 11:50 AM | Location: Library Halton Reading Room

GRC

Speakers

Allen O'Rourke

SVP & Chief Cyber Counsel | Truist

Patrick Hymas

Assistant General Counsel – Vice President | Wells Fargo

Zach Courson

Assistant General Counsel | Bank of America

Real Applications of AI in the SOC

11:05 AM – 11:50 AM | Location: Cone 112B

AI AND SECURITY

Abstract:

SOC teams have long been placed under constant pressure to scale, respond faster, and deal with analyst fatigue, all while managing increasingly complex cloud environments. It is no shock to anyone that AI will increase the number of these risks, and while AI as a blue-team cure-all is enticing, the reality is much more complicated. AI can accelerate triage, and modern tools can enrich or even automate investigations, but AI will likely never replace humans entirely. This is even more true for highly regulated industries dealing with private company information or needing to navigate complex regulatory environments. This talk will discuss the limits of current AI approaches in the SOC, particularly for the modern enterprise... as well as where AI helps, where it fails, how to evaluate AI tooling, and most importantly, how to adopt AI for regulated financial systems.

Using a collection of real-world anonymized cases from my time building Sentinel, as well as Fortune 100 companies we currently work with, we'll discuss the potential risks and opportunities provided by advancements in AI through the context of SOC teams. We'll walk through a practical method for how teams can maintain their current playbooks, tools, and workflows while leveraging the contextual judgment capabilities of AI to scale their team.

Speaker

Ryan Rowcliffe

Field CTO | Legion Security

Credential Compartmentalization

11:05 AM – 11:50 AM | Location: Cone 112A

ATTACK AND DEFEND

Abstract:

Keep Active Directory afloat in the sea of cyber threats! This talk will cover credential compartmentalization, a smart way of organizing your accounts into different tiers based on security needs. Credential compartmentalization is like having multiple watertight compartments in your ship. Even if one gets breached, the others stay dry and safe. Learn how to build resilient defenses that keep your AD infrastructure sailing smoothly, no matter what storms may come your way!

Speaker

Eric Kuehn

Principal Security Consultant | Secure Ideas

Lunch

11:50 AM – 12:50 PM | Location: Student activity center salons

LUNCH

Dessert and Networking

12:50 PM – 1:20 PM | Location: Lucas/lobby

EXIBITION HALL

Post Quantum Cryptography

1:20 PM – 1:45 PM | Location: Cone McKnight

KEYNOTE

Speaker

Colin Soutar

Global Quantum Cyber Readiness Leader | Deloitte

Economics of SBOM

1:45 PM – 2:15 PM | Location: Cone McKnight

KEYNOTE

Abstract:

The Software Bill of Materials (SBOM) is a list of components that can be used to identify any documented vulnerability associated with the enumerated dependencies. Analogies have been made to safety, as with materials safety data sheets, or with allergens listed in general nutrition labels. How can such a simple document play a role in securing the software supply chain? We argue that SBOMs have the potential to significantly resolve the security lemons problem. I introduce the SBOM and illustrate how it can be used to support decision-making in procurement and in code development. I frame this argument using summaries of empirical results; first showing that information in SBOMs aligns with purchaser interest. Second, we illustrate that SBOM contains data that purchasers of software find important. This implies that developers may have an incentive to use SBOMs to create more secure code. Third, we step back and discuss consumer preferences. If the lemons market were resolved, would consumers pay for security? We close with a quick summary of results showing that security-aware consumers will pay more for security in this case leveraging the U.S. Cyber Trust Mark.

Speaker

L. Jean Camp

Bank of America Distinguished Professor | UNC-Charlotte

Break

2:15 PM – 2:30 PM | Location: Lucas/lobby

EXIBITION HALL

Cybersecurity in the Boardroom: What Directors Think

2:30 PM – 3:15 PM | Location: Cone McKnight

CISO

Abstract:

Cybersecurity isn't just a technical challenge—it's a governance priority. This panel brings together board and governance leaders to share how directors think about cyber risk, what they expect from CISOs, and how to bridge the gap between technical detail and strategic oversight. Attendees will gain practical insights into what boards want to see, what they don't, and how to frame cybersecurity in terms that drive effective governance and informed decision-making.

Speakers

Todd Inskeep

Founder and Senior Director | Incovate Solutions

George Bell

Board member | United Community Bank

Tom Wilson

Managing Partner | DecisionPoint Advisors

AI in the SOC – Use Cases, Lessons Learned, and Readiness

2:30 PM – 3:15 PM | Location: Cone 210A

AI AND SECURITY

Abstract:

Security Operations Centers (SOCs) provide the most opportunity for artificial intelligence to deliver measurable impact—accelerating detection and triage times while driving greater operational efficiency. This panel will explore practical use cases of AI in the SOC, from threat detection and incident response to automation and predictive analytics. Panelists will share insights of AI-driven SOC solutions, highlighting both successes and challenges. The discussion will also focus on what organizations need to do to prepare for AI adoption in the SOC, including workforce readiness, data strategy, and governance. Attendees will gain actionable insights to help guide their own AI journeys in cybersecurity operations.

Speakers

Brian White

Head of Cyber Threat Management | Truist

Mahesh Gopalakrishnan

Principal Consultant | Infosys Americas

Denny Deaton

Palo Alto Networks - Unit42

Beyond the Firewall: Protecting Executives in a Hybrid Threat Landscape

2:30 PM – 3:15 PM | Location: Cone 208

ATTACK AND DEFEND

Abstract

In today's interconnected world, executive protection can no longer be confined to bodyguards and secure cars. The digital and physical threat landscapes have converged — where a leaked password can be as dangerous as a protest outside headquarters, and a convincing deepfake can spark reputational crises in seconds. Drawing on real-world intelligence and case studies, ZeroFox will explore how adversaries are exploiting online exposure, social engineering, and disinformation to target high-profile leaders and the organizations they represent. Participants will gain a clear understanding of these evolving risks, practical strategies to safeguard executives across both cyber and physical domains, and immediate steps any organization can take to strengthen its protective posture in an increasingly complex environment.

Speaker

Fabio Barbalace

Manager of the Services & Analysis Team | ZeroFox

Tabletop exercise - The Exec Files: A Cyber Crisis Experience

2:30 PM – 3:15 PM | Location: Cone 113

CISO

Abstract:

The truth is out there. And today so is your client data - spilled onto the dark web by attackers who are still lurking in your network. The day starts normal. Then, a call comes in that changes everything. Where do you start? What do you do? No right or wrong answers here - only consequences.

Speakers

Chris Horner

Information Security Consultant | Rebyc Security

Connor Lawless

Penetration tester | Rebyc Security

Brent Biglow

President | Charlotte ISSA

From Ukraine to Utilities: Lessons in OT Threats from Global Conflicts

2:30 PM – 3:15 PM | Location: Cone 111

ATTACK AND DEFEND

Abstract:

Cybersecurity has become a frontline of modern conflict. Attacks on Ukraine's power grid and ransomware that shut down U.S. pipelines proved one thing: operational technology (OT) isn't just an IT problem — it's a national security and business survival issue. When OT is targeted, the fallout goes far beyond systems. It can disrupt economies, fracture public trust, and reshape geopolitical dynamics.

This session will cut through the comfort of "it can't happen here" and get straight to what leaders need to know:

- What global conflicts reveal about how adversaries weaponize OT.
- Why the boardroom is directly in the blast radius when critical operations fail.
- How innovation can become a liability when legacy infrastructure collides with AI, cloud, and automation.
- The hard questions boards should be asking right now to test their true resilience.

This isn't a technical talk. It's a wake-up call — a clear-eyed look at OT as both a strategic vulnerability and an opportunity for stronger governance, smarter investment, and real resilience in an era where cyber risk and global conflict are inseparable.

Speaker

Madison Horn

Senior Director, National Security Strategy & Policy, World Wide Technology | World Wide Technology

Beware the Hyde in Your Coding Assistant

2:30 PM – 3:15 PM | Location: Cone 210B

AI AND SECURITY

Abstarct: AI coding assistants are rapidly becoming a standard part of software development. They promise faster delivery and greater productivity, but they also introduce new security risks. Recent studies show that while adoption continues to grow, developers remain concerned about the accuracy and safety of the code these tools generate.

The risks, however, extend beyond LLM outputs. The larger challenge lies in how AI tools are integrated, governed, and trusted within development workflows. This talk will examine the current security landscape of AI-assisted coding, highlight the vulnerabilities that emerge, and provide practical guidance on how teams can mitigate these risks while still benefiting from the productivity gains these tools offer.

Speaker

Jan Nunez

Security Engineer | Dropbox

Real Solutions to Defend Against Third-Party Cyberattacks

2:30 PM – 3:15 PM | Location: Library Halton Reading Room

ATTACK AND DEFEND

Abstract:

In today's hyper-connected world, 3rd party Cyber risk is rapidly growing as there has been a significant increase in breaches in recent years. Join us as we discuss why, share challenges in managing risk, highlight AI impacts in the marketplace, and provide concrete actions to help minimize this risk.

Speakers

Pat McMahon

Director – Third Party andSubsidiary Cyber Risk | TIAA

Heather Hendershott

Senior Vice President – Head ofThird-Party Risk | First Citizen's Bank

Brad Davidson

Director – Third Party Cyber Risk | Ally

Branding Cybersecurity at Lowe's. How Marketing and Branding can make security a business priority

2:30 PM – 3:15 PM | Location: Cone 112B

GRC

Abstract:

While technical defenses are critical, cybersecurity's true impact depends on how it's perceived across the business. Too often, security initiatives struggle with executive buy-in and organization-wide adoption. This session explores how branding and marketing strategies can help security leaders reposition cybersecurity as a business priority, drive engagement, and foster a security-first culture that resonates at every level of the organization.

Speakers

Kalee Strawbridge

Sr. Manager, Information Security | Lowe's Companies, Inc

Andrew Withers

Sr. Manager Information Security | Lowe's Companies, Inc

Emerging Technology Trends: A Governmental Perspective

2:30 PM – 3:15 PM | Location: Cone 112A

GRC

Abstract:

As the impact of artificial intelligence and the threat landscape continue to evolve, hear how the State of North Carolina is addressing the state's cyber mission, the biggest opportunities ahead, and how to strengthen our state's ecosystem.

Speakers

I-Sah Hsieh

Deputy Secretary for AI & Policy | North Carolina Department of Information Technology

Bernice Russell-Bond

Chief Information Security Officer | North Carolina Department of Information Technology

Break

3:15 PM – 3:30 PM | Location: Lucas/lobby

EXIBITION HALL

Agentic AI Governance - The Cyborg Era

3:30 PM – 4:15 PM | Location: Cone McKnight

GRC

Abstract:

Postponing AI adoption is no longer an option. As Agetic AI quickly spreads among both legitimate industries and the threat actors that target them, financial services companies are under increased pressure to deploy agentic AI systems for critical functions like cyber defense, fraud and scam prevention, and AML. When faced with relentless, ever-iterating agentic threats, using only pre-GenAI protection techniques is the equivalent of bringing a cease-and-desist letter to the proverbial gun fight.

However, AI agents create their own risks. They combine the challenges of model governance with the trickiest aspects of managing human agents, with whom they share the ability to autonomously plan, decide, execute tasks, and adapt their strategies in real time. For governance purposes, these agents are the equivalent of cyborgs, combining unmatched capacity and complexity with human-like foibles and flaws. This novel set of challenges requires a creative and proactive approach to the operation, oversight, and optimization of agentic systems.

This session will explore practical agentic oversight mechanisms specifically tailored for financial services environments, including real-time monitoring of decision chains, establishing kill switches for autonomous workflows, and developing audit trails that satisfy both internal risk management and regulatory compliance requirements.

Speaker

Alexandra Villarreal O'Rourke

CEO | Credytu

A new approach to Automated Vulnerability Management Remediation

3:30 PM – 4:15 PM | Location: Cone 210A

ATTACK AND DEFEND

Speaker

Rick Doten

VC and Startup Advisory Board Member, AI Governance and Ethics Researcher | Multiple Companies

Tabletop exercise - The Exec Files: A Cyber Crisis Experience

3:30 PM – 4:15 PM | Location: Cone 113

CISO

Abstract:

The truth is out there. And today so is your client data - spilled onto the dark web by attackers who are still lurking in your network. The day starts normal. Then, a call comes in that changes everything. Where do you start? What do you do? No right or wrong answers here - only consequences.

Speakers

Chris Horner

Information Security Consultant | Rebyc Security

Connor Lawless

Penetration tester | Rebyc Security

Brent Biglow

President | Charlotte ISSA

UNC Charlotte talks

3:30 PM – 4:15 PM | Location: Cone111

ATTACK AND DEFEND

The Evolving Agentic Threat Landscape: lessons from attacking agents & building future defenses

3:30 PM – 4:15 PM | Location: Cone 210B

AI AND SECURITY

Abstract:

Agent security is moving fast. In this talk, Nevo & Barak will distill what they've learned breaking real agents and hardening production systems. We'll map how prompt injections become data exfiltration, how sanctioned chatbots can be steered into insider-threat behavior, and why naive "guardrails only" strategies fail. Case studies include: a Copilot Chat prompt-injection leading to exfil via rendered links, a public incident where Air Canada was held liable for chatbot misinformation, and research reporting Lenovo's Lena chatbot could be coerced into leaking session cookies- turning a helpful bot into an enterprise foothold. We'll close with a defense-in-depth blueprint for agents: layered detection and policy enforcement, least-privilege containment for tools and actions, and business-level alignment so approvals actually mean something. Attendees leave with concrete patterns to reduce blast radius now - and a mental model for the next wave of attacks.

Speaker

Nevo Poran

CTO | Tenet Security

CISO role

3:30 PM – 4:15 PM | Location: Cone 112B

CISO

Speakers

Amy Braswell

Deputy Chief Information Security Officer | TIAA

Rick Scot

Global CISO | Elevate Textiles

Todd Inskeep

Founder and Senior Director | Incovate Solutions

CISO panel

4:20 PM – 5:00 PM | Location: Cone McKnight

KEYNOTE

Speakers

Martin Strasburger

VP, Chief Security & Information Security Officer | Duke Energy

Michale Adams

Docusign

Rick Scot

Global CISO | Elevate Textiles

Rick Doten

VC and Startup Advisory Board Member, AI Governance and Ethics Researcher | Multiple Companies