25th Annual UNC Charlotte Cybersecurity Symposium

Are you ready for the next 25 years?

Presented On Campus // October 22-23, 2024

Tuesday, Oct 22, 2024

8:00-9:00 Continental Breakfast Student Activity Center Salons

9:00-12:00

Turning Network Metadata into GOLD! Corelight Capture the Flag using Zeek, Robert Henry, Corelight

[Room: Student Activity Center Salon D-E]

This will be a hands-on event for aspiring analysts and seasoned practitioners engaged in Incident Response/Handling, Threat Hunting and CSI: Cyber Security Investigations. The event will begin with a foundation discussion - Why NTA? Why NDR? Why NSM? Why Zeek & Suricata?. After foundations, we'll spend time on a data/logs deep dive to cover the top 4 logs - specifically conn, http, dns and notice logs. While doing a log deep dive, attendees will be able to follow along as we cover each of those logs, fields and data as well as how they can be used and leveraged across various security related use cases. We'll also cover how real world incidents/intrusions & compromises of the past to see how they have looked with NDR/Network Detection & Response data & protocol logging vs. packet analysis. For the remaining 1.5 - 2 hours, there will be a Capture the Flag style round of labs in Spunk for attendees to work through questions & answers to practice filtering, analysis, observations & analytics with Corelight data & logs.

Prerequisites/requirements: To participate in the labs, each attendee will need to bring their own laptops and have the ability to join the wifi guest network. While the labs/hands-on session is in a Capture the Flag style layout, this is not a capture the flag competition. No pressure, no time constraints - the goal is to provide an opportunity to work with our logs & data in a practical enterprise search and/or SIEM environment while subject matter experts with field *experience are there to answer questions, provide advice and guidance on best practices, etc.*

9:00-12:00

Cybersecurity Maturity: A Practical Workshop on the Cybersecurity Risk Framework Safeguards, Russell Eubanks, Cyverity

[Room: Student Activity Center Salon A]

Are you ready to strengthen your cybersecurity posture and protect your organization like never before? Join us and transform how you approach cyber defenses! This isn't just another cybersecurity session – it's your chance to take control and lead your organization to more robust defenses. You'll leave empowered, confident, and ready to implement your knowledge!

In this hands-on workshop, you will dive deep into the essential Cybersecurity Risk Framework (CRF) Safeguards, empowering you to drive real organizational change! Whether you are just starting or have years of experience, you'll gain practical tools and actionable insights to boost your cybersecurity program. This is your opportunity to evaluate your cybersecurity posture and walk away equipped to make an immediate impact.

Learning Objectives

By the end of this workshop, participants will:

1. Master the CRF Safeguards:
Get hands-on with CRF Safeguards, from basic measures to advanced, continuously monitored defenses. Learn to implement strategies that can make a difference today!
Website:
https://crfsecure.org/research/crf-safeguards/

2. Evaluate and Improve:
Use our free Excel-based tool to conduct a live self-assessment and gain clarity on where you stand. Identify gaps, prioritize actions, and make your program stronger!

3. Leave with Confidence:
Equip yourself with the tools and knowledge to communicate the current status of your cybersecurity program. Be the cyber leader your organization needs!

Workshop Agenda:

1. Introduction to the Cybersecurity Risk Framework Safeguards (CRF-S)
- *Time:* 45 minutes

- *Objective:* Discover how CRF Safeguards provide a robust framework to defend against cyber threats. From foundational steps to advanced, monitored defenses, you'll learn how to strengthen security at every level. Get ready to gain insights that will transform your approach!

2. Self-Assessment Session
- *Time:* 1 hour
- *Objective:* Let's roll up our sleeves and dive into a live self-assessment! You will leave this session with a clear understanding of how your organization measures up and the immediate steps you can take to improve.

3. Interactive Discussion: Addressing Common Challenges
- *Time:* 30 minutes
- *Objective:* This isn't just about learning; it's about action! Join an interactive discussion where we tackle real-world challenges together. Hear from peers and gain solutions to implement right away.

4. Next Steps and Actionable Insights
- *Time:* 30 minutes
- *Objective:* It's not over when the workshop ends! We'll provide you with specific, actionable next steps so you can confidently continue improving your cybersecurity program. Walk away empowered to make an immediate difference.

Target Audience

This workshop is designed for cybersecurity professionals, IT managers, and organizational leaders looking to supercharge their security efforts. Whether you're new to cybersecurity or a seasoned pro, you'll find practical, exciting insights to level up your program.

Workshop Resources

- Free Excel-based CRF Safeguard Assessment Tool (provided at the beginning of the session)

9:00-12:00

Cloud Security - CNAPP, CIEM, CSPM - Deciphering the word soup of acronyms and how to focus on what is important, Thomas Gentsch, Tenable

[Room: Student Activity Center Salon B]

This course is designed to provide a comprehensive understanding of Cloud Native Application Protection Platform (CNAPP) solutions, including Cloud Workload Protection Platform (CWPP), Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and Just-In-Time (JIT) access.

By the end of this course, participants will:

- Understand the key components of CNAPP solutions.
- Understand how to configure and utilize CWPP, CSPM, CIEM, and JIT features.
- Understand how to Identify and mitigate cloud security risks effectively.
- Understand how to Implement best practices for cloud security and compliance.

Module 1: Introduction to - CNAPP
Module 2: Cloud Workload Protection Platform (CWPP)
Module 3: Cloud Security Posture Management (CSPM)
Module 4: Cloud Infrastructure Entitlement Management (CIEM)
Module 5: Just-In-Time (JIT) Access

9:00-12:00 *Resume workshop, Adrianne George*, MyCyberEec
[Room: Student Activity Center Salon C]

1:00-4:00 *Agentic AI and Distributed LLMs in Edge Computing Environments, Dr. Wolfgang Rohde , AiSuNe* [Room: Student Activity Center Salon D-E]

This tutorial examines the integration of Agentic AI Systems and Distributed Large Language Models (LLMs) within Edge Computing frameworks. We introduce novel approaches to partitioning and deploying LLMs across edge devices, addressing the challenges of resource constraints in these environments. We explore how Agentic AI enhances edge device autonomy and decision-making capabilities when coupled with distributed language processing. We analyze the technical challenges of implementing these systems, including model distribution, inference optimization, and maintaining context across distributed components. We provide insights into the practical applications of these technologies in various edge computing scenarios, offering a balanced view of their current capabilities and limitations.

1:00-4:00 *When Smart Bulbs Attack, Jacob Glenn (HAK5), Phish Club and Charlotte ISSA*
[Room: Student Activity Center Salon A]

This is a hands-on workshop where you will disassemble, solder and flash update a smart light bulb!

Wednesday, Oct 23, 2024

7:30-8:30 Continental breakfast [Room: Cone Lucas/lobby]

8:30 Welcome [Room: Cone McKnight]

8:45-9:30 *Cybersecurity: A 25-year journey. What's next?*

[Room: Cone McKnight]

Roger Callahan (Information Assurance Advisory, LLC)
Ron Green (Mastercard)
Sounil Yu (National Security Institute, Scalia Law School, GMU)

9:30-10:00 *Cloud Security: Verifying a digital identity when there are no secrets*

[Room: Cone McKnight]

Shawn Gunsolley (Bank of America)

10:00-10:30 Break [Room: Cone Lucas/lobby]

10:30-11:15 *Security by Default: Applying the brakes to go faster!*

[Room: Cone McKnight]

Jeffrey Dimuro (Service Now)

Future Proofing Cybersecurity Skills

[Room: Cone 113]

Dale Jones (TIAA)
Pete Murphy (TBD)
Carl Cahill (Ahold Delhaize)
Amy Braswell (TIAA)

Building Stronger Security through Effective Segmentation

[Room: Cone 210]

Nevin Absher (CISCO)

Adversarial Intelligence: Redefining Application Security Through the Eyes of an Attacker"

[Room: Cone 265]

Aviv Mussinger (Kodem)

Software Supply Chain Risk Management in the Enterprise

[Room: Library Halton Reading Room]

Derek McCarthy (Netrise)

UNCC Cyber Clinic

[Room: Cone 111]

Vinicius Da Costa (Bank of America)

Ending Cyber Risk Management Groundhog Day

[Room: Student Activity Center Salon D-E]

Jack Jones (Fair Institute)

How State and Local Governments are Approaching AI Implementation and Governance

[Room: Student Activity Center Salon B]

Randy Cress (Asst. County Manager & CIO, Rowan County)
Christie Burris (N.C. Department of Information Technology)
Torry Crass (N.C. Department of Information Technology)
Jason Skeen (Mecklenburg County NC)

Operational Technology (OT) Security Update

[Room: Cone 208]

Justin Pauler (Booz Allen)

Jack and Friends Talk Cyber Risk: Insights and Perspectives from Industry Leaders

[Room: Student Activity Center Salon A]

Jack Freund (Kovrr)
Jared Heintz (TIAA)
Diane McCarthy (TD Bank)
Kraig Corgan (Corning)
Jeffrey Edwards (Protego Trust)

11:15-12:20 Lunch [Room: Cone Lucas/lobby]
12:20-1:00 Dissert [Room: Cone Lucas/lobby]

1:00-1:30 Lessons in Responsible AI from and Industry Pioneer

[Room: Cone McKnight]

Igor Jablokov (Pryon)

1:30-2:00

Securing the Grid Now and Into the Future

[Room: Cone McKnight]

Martin Strasburger (Duke Energy)

2:00-2:15 Break [Room: Cone Lucas/lobby]

2:15-3:00 *Securing the Grid Now and Into the Future: A Deeper Dive into OT Network Protection*

[Room: Cone 208]

Liz Holland (Duke Energy)

Change is the Only Constant: Building Resilient Security Strategies in a Rapidly Evolving Digital World

[Room: Cone 210]

Matthew Haschak (stratascale)

Neurodiversity and Language Skills - The New Superpowers in Generative AI and Prompt Engineering

[Room: Cone 113]

Rick Doten (Centene)

The next 25 years of Cryptography: Anticipating the Challenges and Embracing the Opportunities

[Room: Cone McKnight]

Sam Phillips (Incovate Solutions)
Anne Dames (IBM)
Yongge Wang (UNC Charlotte)
Dale Miller (Cinnamon Bay Advisors LLC)

Future of Programming

[Room: Cone 111]

John Melton (Oracle, NSBGU)
Adrian Wood (Dropbox)
Kristian Lund (Github)

Revolutionizing Cybersecurity: The Role of Enterprise Browsers in Modern Security Architectures

[Room: Cone 265]

Scott Montgomery (Island)

Annual cybersecurity legal review

[Room: Library Halton Reading Room]

Allen O'Rourke (Truist)
Patrick Hymas (Wells Fargo)
Kellen Dwyer (Alston & Bird's National Security & Digital Crimes Team)

3:00-3:15 Break [Room: Cone Lucas/lobby]

3:15-4:00 *Board Strategy & Practices for Governing Cybersecurity*

[Room: Cone 208]

Todd Inskeep (Incovate Solutions)
George Bell (United Community Bank)
Lance Drummond (Freddie Mac Board)

Securing Tomorrow: The Evolution and Future of Security Operations Centers

[Room: Library Halton Reading Room]

Matthew Snyder (Booz Allen Hamilton)
Jared Heinz (TIAA)
Rick Doten (Centene)

Securing AI: Managing Risk Without Slowing Progress

[Room: Cone 210]

Ryan Powell (Metlife)
Elissa McKinley (Advocate Health)

Confused Learning: Supply Chain Attacks through Machine Learning Models

[Room: Cone 113]

Adrian Wood (Dropbox)

Identity Perimeter in Cloud Native: A CIEM Focused Approach to CNAPPs

[Room: Cone McKnight]

Frank Passman (Tenable)

The Future Cybersecurity Professional

[Room: Cone 265]

Brent Bigelow (ISSA)

Oliver Stalenget (AvidExchange)
Madeline Sides (Ally Financial)
Nia Luckey (Infosys Limited)
Jack Jones (Fair Institute)

Introducing Consensus-Based Defense: Creating 1 Secure Web Server from 2 Vulnerable Web Servers

[Room: Cone 111]

Parker Garrison (Startup Founder)

4:00-4:15 Break [Room: Cone Lucas/lobby]

4:15-5:00 **Closing Keynote Session**

*CISO panel*s

[Room: Cone McKnight]

Todd Inskeep (Incovate Solutions)
Chase Carpenter (Honeywell)
Marc Varner (Lowe's)
Amit Metha (Wells Fargo)

Abstract

8:45-9:30 *Cybersecurity: A 25-year journey. What’s next?*

Addressing cybersecurity challenges the past 25 years has been a moving target and a difficult operational challenge. Ron Green, a Mastercard Fellow and Sounil Yu, co-founder and Chief AI Safety Officer at Knostic will discuss insights learned over their extensive careers, and their views on some of the new challenges facing the community. What’s today’s prominent challenges and how will Artificial Intelligence (AI) affect cybersecurity practitioners and organizations going forward?

9:30-10:00 *Cloud Security: Verifying a digital identity when there are no secrets*

10:00-10:30 Break

10:30-11:15 *Security by Default: Applying the brakes to go faster!*

Future Proofing Cybersecurity Skills

Bring your Vulnerability Management beyond compliance

Almost every compliance framework or standard mentions vulnerability management in some capacity. In this session we will review a few of the most common ones and learn how to simply achieve it by 'checking the box' then how to go beyond it for a truly robust and mature vulnerability management program

Building Stronger Security through Effective Segmentation

Effective segmentation is something that companies have been working towards for years, but always seem to fall short. Understanding the foundational elements necessary for effective segmentation and how they contribute to a secure, resilient environment is something that we'll cover in this session - along with where we see it going in the future.

Adversarial Intelligence: Redefining Application Security Through the Eyes of an Attacker"

Software Supply Chain Risk Management in the Enterprise

All companies rely on software to power their business. However, software development pressures and the corresponding enterprise software sprawl is driving up software supply chain risks. These risks are much greater than most security professionals understand. In fact, the software risk data most rely on today is only the tip of the iceberg and misses many of what should be considered the highest priority software risks that exist in the enterprise. However, we see that understanding the true software supply chain risks starts with building a detailed inventory and control of software assets (including a full SBOM of all the software components) which organizations struggle with today. According to Sonatype's ninth annual State of the Software Supply Chain report, the supply chain of open source and proprietary libraries is so complex that only 7% of organizations interviewed have even attempted to review their supply chain risks. In this presentation, we will illustrate the issues of building supply chain visibility and tackling the risks associated with that new visibility.

UNCC Cyber Clinic

Ending Cyber Risk Management Groundhog Day

How State and Local Governments are Approaching AI Implementation and Governance

The next 25 years of Cryptography: Anticipating the Challenges and Embracing the Opportunities

Jack and Friends Talk Cyber Risk: Insights and Perspectives from Industry Leaders

1:00-1:30

Securing the Grid Now and Into the Future

1:30-2:00 *Lessons in Responsible AI from and Industry Pioneer*

2:15-3:00

Securing the Grid Now and Into the Future: A Deeper Dive into OT Network Protection

Change is the Only Constant: Building Resilient Security Strategies in a Rapidly Evolving Digital World

> In a digital world where change is constant, security leaders must navigate the rapid evolution of technology while staying grounded in fundamental security practices. This presentation will offer practical insights and real-world examples of how to balance innovation with proven strategies, ensuring that new tools like AI and cloud technologies are harnessed effectively and securely. We'll explore current industry challenges, highlight the importance of a risk-based approach, and discuss how to prioritize what truly matters in evolving your security programs. The goal: to build resilient strategies that keep your organization secure amidst constant change.

Neurodiversity and Language Skills - The New Superpowers in Generative AI and Prompt Engineering

Operational Technology (OT) Security Update

Future of Programming

Revolutionizing Cybersecurity: The Role of Enterprise Browsers in Modern Security Architectures

In the face of evolving cyber threats, enterprise browsers are emerging as a critical component of modern cybersecurity strategies. This presentation will cover: What is an Enterprise Browser anyway? Common Use Cases for an Enterprise Browser. Seamless Integration: The ease of integrating enterprise browsers with existing IT infrastructure and security tools. Risk Mitigation: Strategies for using enterprise browsers to reduce exposure to web-based threats and vulnerabilities. Regulatory Compliance: How enterprise browsers help organizations meet stringent regulatory requirements and maintain compliance. Live Demonstration of an Enterprise Browser Join us to explore how enterprise browsers are revolutionizing cybersecurity and providing organizations with a strategic edge against emerging threats.

Annual cybersecurity legal review

3:00-3:15 Break

3:15-4:00 *Board Strategy & Practices for Governing Cybersecurity*

In this discussion, we'll talk about how board members should be thinking about cybersecurity, including asking the right questions, understanding issues around ransomware and other threats, and understanding overall cyber risks programmatically versus looking at metrics from security tools. We expect a great discussion with time for questions from the audience.

Securing Tomorrow: The Evolution and Future of Security Operations Centers

"Securing Tomorrow: The Evolution and Future of Security Operations Centers" is a panel discussion focused on the evolving challenges and opportunities for SOCs, focusing on both immediate and long-term needs. The discussion will explore how SOCs can leverage automation, AI, and threat intelligence for faster threat detection while addressing the crucial role of personnel in managing these tools. The panel will examine the need for upskilling and adapting the workforce to meet the demands of emerging technologies and evolving threats, ensuring that SOC professionals remain a critical asset in both current operations and future strategies. Attendees will gain insights into the skillset development required to maintain an agile, effective SOC team in the face of future cybersecurity challenges.

Securing AI: Managing Risk Without Slowing Progress

Artificial intelligence (AI) is driving advancements in every industry and function. From healthcare to finance, AI helps organizations unlock new efficiencies, better understand their data and improve their competitive edge. But as exciting as AI is, it comes with significant security risks. If you’re implementing AI solutions, protecting these systems is critical—not just for your organization’s success, but to safeguard the sensitive data they handle. This panel will explore this in depth. As AI becomes more powerful, adversaries are also using AI to act smarter. Let’s take a closer look at the specific threats AI faces and how you can address them without slowing down progress.

Confused Learning: Supply Chain Attacks through Machine Learning Models

All across the world, everyone is pedal-to-the-metal on machine intelligence, almost as though we're still assembling the plane mid-flight. With that being said, there's a lot about machine learning models that might surprise you and definitely surprises many ML and security engineers. For example, models can contain malware and still give accurate results. Did you know you can administer the ML repos for household names and just have their engineers hand you over their models, training sets, and more? As it stands today, ML is a great place for an attacker to operate in, because these environments have access to your data 'crown jewels' by necessity. No lengthy or complicated pivoting and privesc processes are needed. Simultaneously, tools to assess models proactively for safety, DFIR understanding of ML constructs, and how to analyze models suspected to be malicious are all few and far between. This presentation demonstrates how we have distributed malware using undocumented, novel techniques to compromise some of the largest companies in the world, one of which we discovered entirely unintentionally! Additionally, we will show you how to write ML malware, how to distribute it, and how to loot the environments after gaining access. You'll learn both how I developed a technique to allow me to avoid detection and what you can expect to find post-compromise. Finally, we'll discuss some techniques and tools available to analyze models, and we'll talk through threat hunting we've conducted to look for machine learning malware in the wild. All the work done will be released as open source code. We hope to not only help you do what we've done (so you can try out your own ideas and to help secure your organization) but also provide advice on mitigation and prevention.

Identity Perimeter in Cloud Native: A CIEM Focused Approach to CNAPPs

The Future Cybersecurity Professional

Introducing Consensus-Based Defense: Creating 1 Secure Web Server from 2 Vulnerable Web Servers

"Zero-day web server exploits are notoriously difficult to detect, and attackers will always be able to find a way around exploit detection solutions whether they are based on traditional signatures, AI, or the latest buzzword. However, my research has made use of an opportunity, namely that high-impact exploits against a web server on one OS have never coexisted with high-impact exploits against a different web server on a separate OS, as supported by Project Zero data. So what if we were able to take an incoming HTTP request, and poll the results of 2 or more web servers, such as Apache on Linux, and IIS on Windows, to see if anything's different with one of the responses before returning a final response?

Part 1 of the presentation, which requires very little technical background, will introduce the concept of Consensus-Based Defense as applied to web servers: issuing the same request to a group of 2 or more web servers, normalizing the responses, and comparing them for equality. Even if one of the web servers was exploited and sent back sensitive data, the difference in the responses will be detected and the result is only that the attacker will see an error page. If the responses for a benign user match as expected, they won't even know that this defense is in place.

If the responses do not match, this solution gives the SOC a high-likelihood alert that an actual exploit against one of their systems has taken place, rather than a generic scan or failed exploit attempt, and allows the organization's security team to take action including updating or replacing the impacted vulnerable server.

Much of the outlook in cyber has moved to ""Assume Compromise"", exemplified by Zero-Trust models, which enables after-the-fact detection of some breaches. However, we can realize an even larger security gain -- prevention of attacker tactics instead of just detection -- if we move to ""Assume Available Exploit"" as is done in a Consensus-Based Defense - as an exploit leads to a breach, if we are able to assume that every transaction over the network could be an exploit, we can prevent any Action on Objectives by the attacker. This is because, if at least 1 of the subordinate backend web servers behind the Consensus-Based reverse proxy is secure, the traffic from the secure web server will not match with the traffic from the vulnerable server, so the proxy will block any attacker's response traffic from leaving the server.

In Part 2 of the presentation, we'll dive into how one of today's most common class of attacks work, stack buffer overflow exploits, with live exploit writing demos; then show how to bypass common defenses such as Stack Canaries and ASLR. I will then show how a Consensus-Based Defense prevents any of these mainstay exploits and exploit bypasses from working.

Actionable takeaways are understanding the shortcomings and blind spots of existing defense mechanisms, such as IPS, IDS, and EDR; and how a consensus-based defense allows an organization to move beyond ""Assume Compromise"" as in Zero-trust (detection) to ""Assume Available Exploit"" (up-front prevention)."

4:00-4:15 Break

4:15-5:00 **Closing Keynote Session**

CISO panel, McKnight