ISC2 CHAPTER CHARLOTTE METRO

ISACA® Charlotte Chapter

AGENDA

SEPTEMBER 17, 2024

UNC Charlotte Marriott Hotel & Conference Center
9041 Robert D. Snyder Rd., Charlotte, NC 28262

Resilient Security in the Age of Intelligent Threats: Building, Championing, and Securing AI & AWS

Times are approximations. The agenda may be adjusted as necessary.

7:30AM **Light Breakfast**

8:00AM **Welcome & Opening Remarks**

8:15AM **"Audit Techniques for Workloads Hosted in Amazon Web Services (AWS)",**
Denis Volkov, Forvis Mazars, Manager IT Risk & Compliance

The training is designed for the audit, risk and controls professionals to get familiar with available cloud industry audit programs, best practices and frameworks to assist auditors in planning, scoping and executing audit engagements for Amazon Web Services (AWS) cloud hosted environments. The learner will get familiar with approaches for manual auditing of AWS hosted workloads with a focus on security criteria and general security controls. In addition, the training will shed light into improving efficiency of performing security auditing by utilizing native AWS services and strengthening the IT control environment over AWS hosted environments. The training is mid-level complexity and may require prior familiarity with AWS and cloud technologies. The training is primarily designed for internal and external IT auditors, however, may be useful for IT professionals in charge of AWS cloud management.

9:05AM **"Implementing Compliance, Assurance, and Auditing on AWS",**
Brian Benscoter, AWS Area Principal Solution Architect

In this session, learn how to continuously assess, manage, and maintain compliance for formalized standards such as those required by the Federal Risk and Authorization Management Program (FedRAMP), the National Institute of Standards and Technology (NIST), among others.Learn about various auditing options, including auditing privileged access across services like Amazon S3 and Amazon DynamoDB. Dive deep into how you can achieve governance and compliance using preventative and detective guardrails and other AWS offerings.

10:00AM Morning Break

10:10AM **"Responsible AI on AWS: Transforming Responsible AI from Theory into Practice",**
Joe Losinski, AWS Senior Solutions

As organizations increasingly adopt AI systems, IT auditors play a critical role in ensuring their development and deployment adhere to ethical principles and regulatory compliance. This presentation equips IT auditors with a comprehensive framework to audit responsible AI practices, covering governance structures, bias mitigation techniques, explainability measures, and data privacy safeguards. Attendees will gain actionable insights to assess AI systems' alignment with organizational policies, industry standards, and societal values, enabling them to provide assurance on the ethical and trustworthy use of AI technologies.

11:00AM **“Cybersecurity Services for Building Cyber Resilience”,**
Robert Main, Cybersecurity and Infrastructure Security Agency (CISA)

During this presentation, attendees will be provided an overview of CISA as the nation’s premier risk manager. Next, the current state of our risk landscape will be covered, to include real-world examples of direct North Carolina impacts. That leads to a deep-dive into the no-cost cyber resilience services and capabilities CISA provides its critical infrastructure stakeholders. Finally, we’ll talk about the importance of information sharing and incident reporting.

12:00PM **Lunch & Networking**

12:45PM **Sponsor Remarks**: Hackerone

1:00PM **CISO & Industry Leaders Panel Discussion facilitated by Rick Doten**
“Reducing Risks with Security Champion Programs”
Panelists: Jonathon Robin, CISSP & Shawn Robinson, CISSP

1:45PM **“Adversarial AI - Lying Chatbots, Deep Fakes and more …”,**
Jeff Crume, PhD, CISSP (IBM)

This presentation will explore the potential dangers of adversarial AI, lying chatbots, and deep fakes. We will discuss how these technologies are becoming more sophisticated and how they can be used to deceive people, spread disinformation, and even cause harm. Through real-world examples and demonstrations, we will explore the implications of these technologies for society in order to gain a better understanding of these emerging technologies and the risks they pose.

2:45PM **Afternoon Break**

3:00PM **”Securing Artificial Intelligence using Zero Trust”,**
Cindy Green-Ortiz, CISSP, CSSLP, CISM, CRISC, PMP, CSM, BS-CIS, AS-CIS (CISCO)
The rapid evolution of Artificial Intelligence (AI) has brought about significant advancements in various sectors, from healthcare to finance. However, with these advancements come new security challenges. As AI systems become more integrated into critical infrastructure, the need to secure these systems against potential threats becomes paramount. One of the most effective strategies for securing AI systems is the implementation of Zero Trust principles. This session will explore the application of Zero Trust principles to AI security, referencing key frameworks such as NIST 800-207, NIST AI Risk Management Framework (AI RMF), and the EU AI Act.

4:00PM **“OSC&R in the Wild — How to Start Making Sense of Your Supply Chain Security”***,*
Katie Teitler-Santullo (Ox Security)

Software is the foundation on which today’s businesses operate. From standard enterprise applications to custom-built applications, every organization relies on software. As reliance grows, so does its attractiveness to cyber criminals. The ubiquity of applications across companies, the prevalence of reused code, and abundant code vulnerabilities make software a prime cyber attack target.

But companies don’t have to accept high risk. OX Security has conducted extensive research on software supply chain risk (SSCR) and has identified the most common and concerning exposures.

Join OX Security to hear what researchers learned from analyzing over 100 million software supply chain security alerts, and how using OSC&R — the industry's only attack reference for SSCR — can help you reduce software-related risk.

You will learn:

- *The state of the software supply chain attack surface*
- *Where in the attack lifecycle software is most vulnerable*
- *What is OSC&R — a free resource, and how can you use it to become your company's supply chain savior?*

4:50PM	**Closing Remarks**
5:00PM	**Networking Hour**

Thank you to our sponsors:

Ox Security, HackerOne

ISACA®

Charlotte Chapter

OX

hackerone