UNIVERSITY OF NORTH CAROLINA CHARLOTTE | COLLEGE OF COMPUTING AND INFORMATICS

In collaboration with ISSA Charlotte Information Systems Security Association

2023 Cybersecurity Symposium

THANK YOU TO OUR SPONSORS

Presenting

Bank of America

Silver

Lowe's

ally

Wells Fargo

TIAA

dexian

DISYS SIGNATURE CONSULTANTS

CALYPSOAI

Bronze

VERACODE

Exhibitor

tavve

Consortium Networks

servicenow

tenable

Abnormal

Booz | Allen | Hamilton 100 YEARS

huntsource Pinpointing technology talent.

paloalto NETWORKS

Wednesday, Oct 18, 2023

8:00-9:00 Continental Breakfast

9:00-12:00 *Cyberbit live fire Attack Simulation workshop* (see description below), SALON C

Live Fire Cyber Range Attack Simulation Workshop hosted by Cyberbit. Using the Cyberbit Platform, workshop participants will be immersed in a hyper-realistic environment with enterprise grade networks, commercial security tools from Palo Alto Networks & Splunk and real-works cyber-attack scenarios. Attendees will work to detect and respond to a live attack. This Live Fire Exercise is designed for SOC and Incident Response Teams and qualifies for CPE Credit with (ISC)2. Must register.

Cyber Threat Solutions Delivery: Bank of America. SALON B

Join us to learn how to idealize and deliver end-to-end cyber security threat solutions. Workshop targets audiences that are technical and non-technical to navigate process and implementation steps together to deliver enterprise grade solutions.

Proofpoint Data Loss Prevention- Hands-on Discovery Lab SALON A

Remote work, combined with cloud adoption and unprecedented employee turnover, has created a perfect storm for organizations trying to protect their most strategic and sensitive data. Insider threats are the top cybersecurity concern among CISOs globally. As the Data Loss Prevention (DLP) and Insider Threat Management (ITM) markets converge, a people-centric approach is required to fuel your cybersecurity strategy. The primary objective of both sets of technology is to prevent data loss and misuse of data. DLP monitors file activity and leverages content scanning to determine whether users are handling sensitive data according to corporate policy. ITM monitors user activities such as application usage, user input/output, website access and file movement. It also captures screenshots of high-risk activity for visual evidence to accelerate investigations.

Join us at Proofpoint Discovery where you'll get hands-on experience with Proofpoint products. In this free workshop, you will learn:

- Best practices on how to protect people and defend data
- How to detect and respond to potential insider threats
- How to investigate insider threat and data loss incidents
- How to stop data loss through cloud sharing tools and personal webmail
- And much more!

Reminder: In order to participate in the hands-on lab, you will need to bring your own personal laptop.

12:00-1:00 Lunch
12:00-2:00 *Women in Cybersecurity Networking.* SALON A
1:00-4:00 *Cyberbit live fire workshop* SALON C

Thursday, Oct 19, 2023

8-8:50 Continental breakfast
8:50-9:00 Welcome
9:00-10:15 **Opening Keynote Session** (McKnight Auditorium)

AI, Security and your Future
Sam Curry (zscaler)
Generative AI and Security
Carrie Gates (BofA)
Perspectives on AI usage in Attack Operations
Lawrence Taub (Google Mandiant)

10:15-10:45 Break

10:45-11:30

AI and Cybersecurity Track

The Crossroads of AI & Application Security
Sohail Iqbal (Veracode), 210
AI Compliance panel, 111
Abby Mitchell (ISSA)
Frank DePaola – (Enpro Industries)
Jeff Crume – (IBM)
Allen ORourke – (Truist)
Nick Solimini – (Tenable)

Cyber Attack and Defense Track

Demystifying Zero Trust: Unveiling Reality Amidst Hype. McKnight

Thor Draper (Booz Allen Hamilton)

Risk/policy Track

Cyber Risk Metrics that Matter

Larry Pfeifer (Consortium) 112

Leadership/Career Development Track

Cyber Security in Mergers and Acquisitions, Halton Reading Room

Todd Inskeep (Incovate Solutions)
Margaret White (Truist)
Pat McMahon (TIAA)
Sam Phillips (Incovate Solutions)

11:30-11:45 Break

11:45-:12:30

AI and Cybersecurity Track

Securing your Applications in the Age of AI

Kristian Lund (GITHUB), Cone 111

Cyber Attack and Defense Track

SASE Implementation, McKnight

Matthew Snyder (Booz Allen Hamilton)
Ben Agner (Truist)
Rick Doten (Centene)
Thor Draper (Booz Allen Hamilton)

Risk/policy Track

Risk/policy Track

Legal updates, 112

Allen O'Rourke (Truist)
Erin Frazer-Schardt (Truist)
John Ghose (VeraSafe)
Kellen Dwyer (Alston & Bird)

Leadership/Career Development Track

Metrics for board, Halton Reading Room

Michael Piacente (Hitch Partners)
Amy Braswell (TIAA)
Bill Belk (Sonic Automotive)
Ben Corll (Zscaler)

Bird of Feather

Obfuscation in Plain Sight 113

Jonathan Chaipis (Wells Fargo)

12:30-1:30 Lunch
1:30-2:15 Coffee, desert and networking
1:30-3:00 Job fair interviews

2:15-3:00

AI and Cybersecurity Track

The Weaponization of AI in Cybersecurity, McKnight
Richard Ford (Praetorian)
How behavior patterns can be used for better cyber security, 210
Vinicius Da Costa (Bank of America)
Alan Calvitti (Bank of America)
Kenneth Longshaw (Bank of America)
Kathleen Schaumberg (Bank of America)

Cyber Attack and Defense Track

Supply Chain Security: Addressing the Absence of Basics, 112
Brian White (Wells Fargo)
Frederick Dicks (Wells Fargo)
Cyber Risk Management Panel 111
Jack Freund (Kovrr)
Ian Lassonde (Wells Fargo)
Jeffrey Edwards (Protego Trust)
Kimberly Trapani (American Tire Distributors)

Leadership/Career Development Track

What the Board expects from the CISO and what the CISO needs from the Board, Halton Reading Room
Michael Piacente (Hitch Partners)

Bird of Feather

Threat intelligence; practical uses vs confusion over what it is, 113
Rick Doten (Centene)

3:00-3:15 Break
3:15-4:00

AI and Cybersecurity Track

AI SecOps: Better and Faster, Or Mere Fantasy? 210
Kevin O'Brian (Deepkeel)

Harmony & Discord: Navigating the Dual Nature of GenAI
Jeffrey DiMuro (ServiceNow), 208

Using AI to Detect and Prevent Fraud and Scams 112
Chris Hart (Vectari)
Alex O'Rourke (Vectari)

Cyber Attack and Defense Track

My 10-year Journey: Solving Alert Fatigue with AI that thinks like a cyber analyst 111
Jon Bagg (Salemcyber)

Risk/policy Track

Third Party Risk Management, McKnight
Jefferson Pike (Lowes)
Doug Rambo (Ally)
Patrick Butterfiled (Lowes)
Brian Cyprian (FBI)

Bird of Feather

Zero Trust isn't a product: A discussion that explores the different components that contribute to a Zero Trust strategy, and how to implement them 113
Thomas Obarowski (SiteOne Landscape Supply)

Leadership/Career Development Track

Managing neurodivergent individuals Halton
Rick Doten (Centene)

4:00-4:15 Break

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

CISO panel, McKnight
Todd Inskeep (Inovate Solutions)
Chase Carpenter (Honeywell)
Carla Sweeney (Redventures)
Amy Braswell (TIAA)

CHARLOTTE CYBERSECURITY SYMPOSIUM

UNC Charlotte Cybersecurity Symposium Cyber Range Workshop

October 18th, 2023
UNC Charlotte Campus / Charlotte, NC

Agenda

cyberbit

9:00 – 9:30 AM: Cyberbit Cyber Range Platform Overview & Demo

9:30 – 10:30 AM: Lab 1
"Common Attack Types – Analyzing Phishing"
45 min / .75 CPE Credit
Learn to identify and investigate phishing attacks
Hands-on experience analyzing HTML code

10:30 – 11:30 AM: Lab 2
"Identify Files Using File Explorer"
40 min / .75 CPE Credit
Gain experience investigating recently modified files to identify malicious activity
Hands-on with Windows CLI, Explorer, and File System Structure

11:30 – Noon: Lab Assessment Results & Debrief

Noon – 1 PM: Lunch (Served in Lobby)
Attendees log out of Labs and log in to Live Fire Exercise

1:00 PM – 4:30 PM: Live Fire Range Ransomware Attack Simulation
"DragonFly Malware"
4 Hr Live Fire / 4 CPE Credit
Gain hands-on experience investigating malicious PowerShell Scripts
Exposure to sophisticated attack techniques for lateral movement, privilege escalation, and data exfiltration
Enterprise Network with Windows 10, Palo Alto, McAfee, and Splunk

(Description & CPE Credits).

4:30 – 5:00 PM: Attack Debrief and Q&A

Register Here . . .

Participant Requirements

- For Labs and Live Fire Exercises, please bring your laptop with HTML5 Compliant Web Browser and headsets for Zoom breakout rooms.
- Connectivity test e-mail will be sent to registered attendees 1 week prior to the workshop to ensure successful access to the Cyberbit Cyber Range.
- For the Threat Hunting Lab and Live-Fire Ransomware Attack Simulation, if you have an (ISC)2 ID, your credits will be automatically uploaded to your account and will appear in your (ISC)2 account within 4 weeks of completing the exercises.

Event Overview

Join the Charlotte, NC ISSA Community on October 18th, 2023 for a Live Fire Cyber Range Attack Simulation Workshop hosted by Cyberbit. Using the Cyberbit Platform, workshop participants will be immersed in a hyper-realistic environment with enterprise grade networks, commercial security tools from Palo Alto Networks & Splunk and real-works cyber-attack scenarios. Attendees will work to detect and respond to a live attack. This Live Fire Exercise is designed for SOC and Incident Response Teams and qualifies for CPE Credit with (ISC)2.

Cyberbit Overview

Cyberbit was founded to address an acute issue: Cybersecurity teams are not prepared to deal with cyberattacks. Conventional cyber training forces teams to learn on the job with no clear measurement of progress and very real repercussions. With disproportionally large investments into cybersecurity tools, cybersecurity teams lack the knowledge, skills, and experience to effectively deploy their toolsets, leading to a continued increase in breaches, regardless of technology investments.

To address this issue, Cyberbit developed the first-ever hyper-realistic cyber skilling platform, ensuring that cybersecurity professionals have the right knowledge, skills, and experience to excel. The Cyberbit Skills Development platform includes cyber labs, commercial tool training (Palo Alto Networks, Cisco, Crowdstrike, Splunk, Microsoft& more) with attacker context, and live-fire cyber range exercises aligned to industry best standards (NICE Framework, MITRE ATT&CK, NIST) to ensure your team develops into top-tier cybersecurity professionals. Performance-based assessment using advanced network sensors validate your team's skills giving you the confidence that your digital assets are fully protected. Cyberbit contains the world's largest catalog of on-demand simulated attacks including Ransomware, DDoS, SQL Injections, Worms, Fileless Attacks, and more.

Cyberbit is used by leading organizations around the world including Fortune 500 companies, MSSPs, governments, and academic institutions to transform their cyber practitioners into elite cyber defenders.

Organizations use Cyberbit to create a better SOC team by upskilling their cyber professionals, validating incoming candidate skillsets, rapidly onboarding new hires, and validating incident response playbooks. Cyberbit delivers over now million hours of training annually across 5 continents.

More information on Cyberbit and to register for free custom Cyberbit Live Fire Attack Simulation Workshop here: https://www.cyberbit.com/