Cyber security is everyone's business.

Join Leading Experts on Cyber Security

Conference Guide

Tuesday, Oct. 31, 2023
8 a.m.-4 p.m.

This conference is a partnership between
the state of Nebraska and Southeast Community College

NEBRASKA
OFFICE OF THE CIO
Information Security Office

Southeast
COMMUNITY COLLEGE

southeast.edu/ncsc

In today's world, we rely on technology and the Internet for a variety of transactions, communication and information – at home, in school and at the workplace. While we are familiar with the myriad of conveniences provided through Internet use, it is difficult to stay abreast of all the changes and the potential risks presented by the Internet. We are all "virtual neighbors" in cyberspace, and what we do, or don't do, can affect many others.

The Nebraska Cyber Security Conference will assist in raising our awareness of cyber security and help in protecting all of us in cyberspace. If we do our part individually, collectively we can have a tremendous positive impact on our state's cyber security.

This will be valuable time learning from skilled industry experts. The day will be filled with a variety of breakout sessions that will encompass different areas of information security and technology.

For more information, visit southeast.edu/ncsc.

Wi-Fi Login Information

Network: NU-Guest
Username: October31
Password: Innovate2023!

Keynote Speaker: René Agüero

Splunk

Threat Research Update

At Splunk, René has helped solidify Splunk's place among leading Cyber Security vendors by delivering more than 100 security assessments leading global teams and helping customers solve their most challenging security problems. Prior to Splunk he was at Rapid7 where he helped enterprise GTM, deployments and services ranging from Vulnerability Management, Penetration Testing, UBA. Prior to Rapid7, René worked in the financial sector in Southern California as a security manager where he won awards for the security program he built. René received a Master of Science in Business Administration with emphasis in IT security, IT audit and computer forensics from California Polytechnic University Pomona. René has appeared on Associated Press and their partner news agencies on topics like the End of XP and the Anthem healthcare breach.

			Track	Room
7:30 a.m.	**Check-in / Breakfast (provided)**			
8:15 a.m.	**Opening Remarks from State of Nebraska Officials and Southeast Community College**			Second Floor Banquet Hall
8:45 a.m.	**Break**			
9 p.m.	**Keynote**	***Threat Research Update***, René Agüero		Auditorium
10 a.m.	**Break**			
10:15 a.m.	**Breakout Sessions**	***Cyber Tatanka Panel,*** Tim Pospisil, Dustin Thorne and Dana Turner	E U M T	Auditorium
		Impact of Open Source Intelligence of Offensive Security and Investigative Practices, Md Rashedul Hasan	E U M T	Room A
		Network Threat Hunting and You! Two-Hour Workshop (Part 1), John Strand	E T	Room B
		When the Whole World is Watching - Enduring Security, Robert Palmer	E U M	Room D
11 a.m.	**Break**			
11:15 a.m.	**Breakout Sessions**	***AI and Its Transformative Potential in Business & Cyber Security: ChatGPT Makes a Terrible Search Engine,*** Gregory Richardson	E M T	Auditorium
		It's Okay to Walk Away, Karla Carter	E U M T	Room A
		Network Threat Hunting and You! Two-Hour Workshop (Part 2), John Strand	E T	Room B
		Security Risks of Generative AI, Jon Nelson	E U M T	Room D
Noon	**Lunch** (provided)			Second Floor Banquet Hall
1 p.m.	**Breakout Sessions**	***Out of Sight, Out of Control: Asset Intelligence,*** Michael A. Atkinson	M T	Auditorium
		Cloud Security Awareness, Jacob Charles	M T	Room A
		Antisyphon Open Exhibits		Room B
		Contingency Planning for a Rainy Day, AmyLynn Creaney	M	Room D
1:45 p.m.	**Break**			
2 p.m.	**Breakout Sessions**	***National Cyber Security Awareness Month and CISA Cyber Security Services,*** Nicholas Brand, Gregory Goodwater, and Warren Hagelstien	E U M	Auditorium
		Zero Trust ≠ Zero Risk, Ronald Woerner	U M T	Room A
		Antisyphon Open Exhibits		Room B
		Cybersecurity Priorities for Organizations, Ben Hall	E M T	Room D
2:45 p.m.	**Break**			
3 p.m.	**Breakout Sessions**	***Navigating the Digital Seas: Parallels between Pirates and Cyber Security Practitioners,*** Dana Turner	E U M	Auditorium
		The 90s Called and They Want Their Email Security Back!, Julie Paul	E M T	Room A
		Antisyphon Open Exhibits		Room B
		Defending Your Lan and Wireless Networks, Joseph Hall	E M T	Room D

Education End User Management Technical

AI and Its Transformative Potential in Business & Cyber Security: ChatGPT Makes a Terrible Search Engine

Gregory Richardson, Palo Alto Networks

The digital transformation era has seen the rise of various disruptive technologies, but none quite as influential as artificial intelligence (AI). It is reshaping business landscapes, offering unprecedented opportunities and compelling organizations to rethink their traditional modes of operation. Let's embark on a journey to explore the pivotal role AI plays in the modern business world.

Experience Level: Beginner, Intermediate, Advanced

Gregory Richardson is a seasoned cybersecurity leader and serves as Advisory CISO supporting Palo Alto Networks' largest, most strategic clients. Having been an information security practitioner and having built and lead large teams tasked with securing several large multinational corporations for more than 30 years, Gregory understands the business of cybersecurity well.

Prior to joining Palo Alto Networks, Gregory was Chief of Staff for the Office of the CTO for a publicly traded US company, where he was responsible for overseeing operational efficiency for the office of the CIO and CISO respectively.

Fueled by his passion for security, Gregory studied threats and understands attacker ontology well. He spent a significant part of his career learning to think like the attacker, so as to preempt the attack and leverages this as a part of the value he adds to the defender conversation

Cloud Security Awareness

Jacob Charles, Bison Cloud Solutions

Prerequisite: Basic understanding of what the cloud is and the pay as you go pricing model.

Cloud security has unique challenges that need to be understood. This presentation provides an awareness of what security issues we are facing in the cloud, and provides a foundation on how to overcome these challenges.

Experience Level: Beginner, Intermediate

I've worked in the IT industry for more than eight years. I started my career as a software engineer and quickly grew into leadership positions. I've had the great opportunity to solve a variety of problems and grew a passion for security and infrastructure automation. Last year I turned my passion into a product that everyone can benefit from. I founded Bison Cloud Solutions in order to help others improve cloud security and infrastructure automation.

Contingency Planning for a Rainy Day

AmyLynn Creaney, State of Nebraska

Business continuity and contingency planning for cloud services. With more reliance on and integration with cloud computing, it's important for organizations to have business continuity and contingency plans for a disruption in vendor provided services. Let's face it, planning can be a chore that never seems to end. I'll breakdown the six questions any organization can use to determine if their existing plans adequately cover their cloud dependencies. And if you don't have a plan yet, you'll know where to start.

Experience Level: Beginner, Intermediate

AmyLynn is a certified Master Business Continuity Professional through the Disaster Recovery Institute International and the recipient of an honorary "Admiralship" from Governor Ricketts for her excellence in leadership in response to the COVID-19 pandemic. AmyLynn brings extensive professional experience in all aspects of emergency management and is recognized for her effective management of planning projects to develop business continuity plans, cyber incident response plans, contingency plans, and disaster recovery plans. She previously served as a government contractor providing EM/HS capabilities analysis, operational planning, and incident response support to Commander, Navy Region Midwest and FEMA Region 5 (Chicago, IL). Connect with AmyLynn on LinkedIn @AmyLynn Creaney, MBCP.

Cybersecurity Priorities for Organizations

Ben Hall, Heartland Business Systems

Building a strong security program for organizations doesn't need to be a daunting task and should align with your organization's business and regulatory objectives. Organizations across all industries are under pressure from regulators and customer needs for robust cybersecurity measures to safeguard sensitive data, ensure operational integrity, and uphold public trust. This presentation will highlight and focus on:

- Understanding the cyber threat landscape and prevalent cyber threats
- Emerging technologies and threats faced
- The importance of data privacy, security and compliance with regulations, and the potential legal, financial and reputational repercussions of data breaches
- Best practices for organizational cybersecurity offering practical guidance
- Incident Response and Disaster Recovery Processes

A security program isn't something you ever finish, rather it's continuously evaluated and added to as your business and risks change.

Experience Level: Beginner, Intermediate, Advanced

Ben Hall, CISA, CDPSE, Senior Information Security Consultant and Virtual CISO, is a Certified Information Systems Auditor (CISA) and a Certified Data Privacy Solutions Engineer (CDPSE) with more than 15 years of Governance, Risk, Compliance, Information Security, and Information Technology experience in the banking, financial, insurance and health care sectors. Prior to joining HBS, he held positions as Information Security Officer, Risk Manager, Lead IT Security and GRC Analyst, IT Operations Supervisor, and Systems Administrator. As a Senior Information Security Consultant for HBS, he works with clients to support their information security, risk management, and compliance efforts. Ben has expertise in third-party risk management, change management, access control, security operations, incident response, disaster recovery and business continuity, security and risk management, and security awareness. Additionally, he has experience in IT governance, risk and compliance.

Cyber Tatanka Panel Discussion

Dana Turner, Union Bank and Trust, Dustin Thorne, LES, and Tim Pospisil, Nebraska Public Power District
Moderator: Patrick Wright

Dana Turner, Dustin Thorne and Tim Pospisil will talk about outcomes and lessons learned from Cyber Tatanka.

Experience Level: Beginner, Intermediate

***Dana Turner**, CISSP, is addicted to everything Infosec and has been since before it was cool. He has more than 35 years' experience in IT and Information/Network Security and is the Network Security Officer for Lincoln, NE-based Union Bank and Trust Company. Dana is passionate about helping to align IT with business objectives, while effectively managing risk and not just meeting compliance requirements, but exceeding them. He also leads the critical incident response team at UBT aided by more than a decade of operational and tactical experience as a volunteer first responder in the fire/ems service, dealing with incident and crisis management. As an information security practitioner, Dana enjoys giving back to the community by volunteering in a technical and/or information security advisory capacity for non-profit organizations. Most weekends you can find him working on metal or wood craft projects, studying up on the latest covert entry techniques or doing something motorcycle related with his wife Candice.*

***Timothy Pospisil** was recently assigned the role Nebraska Public Power District's (NPPD) Director of Security Technology Outreach and Chief Security Officer (CSO), with responsibility for guiding and influencing the electric industry and governmental agencies at the federal, state and local levels related to all matters both in physical and cyber security. Tim is NPPD's designated North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIP) Senior Manager. Prior to his current assignment, he led NPPD's NERC CIP implementation projects and launched the security operations team as the Corporate Security Director. He joined NPPD in 1999 at Cooper Nuclear Station and served as a Procurement Engineer where he was the stations Environmental Qualification (EQ) engineer after working previously for Motorola Semiconductor as an Equipment Engineer and Test & Packing Section Manager. He is active in many industry groups, including the Large Public Power Council (LPPC) Cyber Security Task Force where he is the current Chairman, the North American Transmission Forum Security Practices Group, as well as other state and local security groups. He completed the U.S. Department of Energy (DOE) Operational Technology (OT) Defender Fellowship Program in 2022. Tim graduated from the University of Nebraska-Lincoln in 1989 with a bachelor's degree in Electrical Engineering. He holds certifications from ISACA as a Certified Information Security Manager (CISM), SANS – GIAC Security Leadership Certification (GSLC), SANS – GIAC Critical Infrastructure Protection (GCIP), and CompTIA – Security +.*

Defending Your Lan and Wireless Networks

Joseph Hall, Nile

Deep dive into mitigating local threats and protecting local assets.

Experience Level: Beginner, Intermediate, Advanced

Joe Hall, a cybersecurity expert with more than 20 years of experience in network security and risk mitigation, now Head of Security Services at Nile. Prior to joining Nile, Hall held numerous security engineering positions at Fortinet, Sophos, Symantec PGP, Dell Sonicwall, American Express, and Solera Networks. As a forward-thinking leader at these large companies, Hall's experience includes supporting the launch of Dell's SuperMassive Next-Gen Firewall Series and training hundreds of support technicians on various enterprise security product lines. He also was responsible for deploying the worlds largest GCP network as well as protecting the 2016 Olympics in Rio. Joe and his wife Christine live in Paradise Valley, Arizona with their four teenagers and two dogs. You will find them doing something active like riding One Wheels, mountain biking, paddle boarding, or racing in triathlons. Hall is a serial entrepreneur with a hunger to build and innovate.

Impact of Open Source Intelligence of Offensive Security and Investigative Practices

Md Rashedul Hasan, University of Nebraska-Lincoln

Prerequisite: Basic knowledge of information security

OSINT, or open source intelligence, is the practice of collecting information from published or otherwise publicly available sources. OSINT operations, whether practiced by IT security pros, malicious hackers or state-sanctioned intelligence operatives, use advanced techniques to search through the vast haystack of visible data to find the needles they're looking for to achieve their goals—and learn information that many don't realize is public. Open source in this context doesn't refer to the open source software movement, although many OSINT tools are open source; instead, it describes the public nature of the data being analyzed. See how OSINT is being utilized on cyber security practices on a regular basis and how counter intelligence are utilizing this to mine information for investigative purposes.

Experience Level: Beginner, Intermediate, Advanced

Md Rashedul Hasan is a current student pursuing a Ph.D. in Computer Science at the School of Computing at the University of Nebraska-Lincoln. He completed his Software Engineering Bachelor's degree from Daffodil International University in the Fall of 2019. He also is an Information Security Researcher and OSINT expert. He has participated in various training programs in Bangladesh, Singapore, Indonesia, Malaysia, and the United States. Rashed is working as a graduate research assistant at the School of Computing at UNL. His research involves Large Language model-based development of efficient and resilient software systems.

It's Okay to Walk Away

Karla Carter, Bellevue University

Prerequisites: An interest in the human factors of cybersecurity.

The ability to say "no" is an underemphasized yet critically important skill. This presentation delves into the psychological aspect of disagreeableness from the Five Factor Personality Model, linking it to key decision-making processes in cybersecurity. The talk identifies five principal areas where the power of "no" is most directly relevant: Social Engineering, Hardware and Software, Vendor Relationships, Product Development, and Data Collection. By focusing on real-world examples, this presentation will argue that being able to decline, defer, or walk away is not just a personal trait but a professional necessity. Note: Elephants not included. Honey Badgers sold separately.

Experience Level: Beginner, Intermediate, Advanced

Karla Carter is an Associate Professor of Cybersecurity in the College of Science and Technology at Bellevue University, in Bellevue, NE. Armed with an MS in Cybersecurity, Security+ and SANS Security Awareness Professional certifications, and drawing on more years than she should admit to of information technology experience, she teaches undergraduate and graduate courses in cybersecurity operations, social engineering and human factors, security awareness, web security, technology ethics, and—in a plot twist you didn't see coming—occasionally history and civics. Karla is a Member-At-Large and Student Activities Committee Chair on the Nebraska Section IEEE executive committee, as well as being involved with the IEEE Computer Society and ACM Committee on Professional Ethics. She is curious, intense and irreverent and often sends coded messages through her accessories.

National Cyber Security Awareness Month and CISA Cyber Security Services

Nicholas Brand, Gregory Goodwater, Warren Hagelstien, Cybersecurity & Infrastructure Security Agency

Updates from the Department of Homeland Security Cybersecurity & Infrastructure Security Agency. Learn about resources available for your organization.

Experience Level: Beginner, Intermediate

Nicholas Brand *serves as a Cybersecurity Advisor/Cybersecurity Coordinator for Nebraska in Region 7 (IA, KS, MO, and NE) for the Cybersecurity & Infrastructure Security Agency (CISA), Integrated Operations Division. Based in Lincoln, NE, he supports the Department of Homeland Security's (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure. His programs coordinate cyber preparedness, risk mitigation and incident response. He provides Cybersecurity resource briefings, Cybersecurity assessments and Incident Response planning to the nation's sixteen critical infrastructure sectors and state, local, tribal, and territorial government entities. Prior to joining CISA, Brand was the Director of Information Systems for the City of Fremont, Nebraska, Department of Utilities for nine years. He advised local government officials and Utility management on IT, cybersecurity and physical security related projects; coordinated and implemented all cybersecurity programs and training; and led the planning and day to day operations for the IT department to include continuity of operations. In addition, He also served previously as a federal technician, System Administrator, for Data Processing for six years in Lincoln, NE, in support of the NEARNG USPFO mission. Brand was a member of the Nebraska Army National Guard from 1997 until 2017 and retired after 20 years of military service. While in uniform he acquired a wide range of experience from positions that included 25B40 Senior Information Systems Specialist. Mr. Brand has a Bachelor of Science degree in Computer Information Systems from Wayne State College. He is a member of ISACA and has obtained a Certified Information Security Manager (CISM) certification.*

Gregory C. Goodwater *serves as the Protective Security Advisor (PSA) for Nebraska. As a PSA, he directly contributes to the development of the national risk picture by assisting with the identification, assessment, monitoring, and minimizing of risk to the nation's critical infrastructure. He engages as a technical and physical security advisor with federal, state, local, tribal, and territorial (FSLTT) government mission partners and members of the private sector stakeholder communities. In this capacity, Greg serves as the critical infrastructure stakeholder's link to Department of Homeland Security (DHS) infrastructure protection resources; security and resiliency assessments, training, and as a vital link for information sharing in steady-state and during incident response. Greg joined DHS in February of 2022 and has more than 18 years of combined experience in law enforcement, security, antiterrorism, infrastructure protection, and emergency operations. He has a background working with and leading tactical, operational, and strategic security and protection programs with federal, state, and local organizations/agencies. Prior to working for DHS, Greg was in law enforcement and is currently serving in the Nebraska National Guard as the Security Forces Commander with military experience in both the security and logistic officer career fields. In these capacities, Greg has served in a variety of federal, state, and local operational missions. Greg earned a Bachelor's Degree from the University of Nebraska, Lincoln, and a Master's Degree from the United States Army War College.*

Warren Hagelstien *serves as a Cybersecurity Advisor for Region 7 (IA, KS, MO, and NE) for the Cybersecurity & Infrastructure Security Agency (CISA), Integrated Operations Division. Based in Omaha, NE, he supports the Department of Homeland Security's (DHS) mission of partnering with industry and government to understand and manage risk, strengthening the security and resilience of the nation's critical infrastructure. Hagelstien provides cyber preparedness assessments and protective resources, working group support, leadership, partnership in public-private development, and coordination and support in times of cyber threat, disruption or attack to the nation's sixteen critical infrastructure sectors and state, local, tribal, and territorial government entities. Prior to joining CISA, he was the Director of Information Systems for the City of Fremont, Nebraska, for one year. Before his tenure with the City of Fremont, Nebraska, Warren spent six years with the Department of Defense where he held several positions to include Chief, Vulnerability Management for United States Strategic Command, Chief, Cybersecurity for the Air Force Weather Program Management Office, and Information System Security Manager for the Air Force Weather Program Management Office. Hagelstien spent time on active duty in the United States Air Force from 1998 until 2007. After his military service, Warren held multiple positions as a Department of Defense contractor with positions focusing on information security and information assurance. During the time following military service, he also spent three years as Director, Information Security for First National Technology Solutions in Omaha, NE. He holds a Master of Science in Cybersecurity and a Master of Business Administration from Bellevue University. He also holds a Bachelor of Science degree in Management Information Systems from Bellevue University. He is a member of (ISC)2 and is a Certified Information System Security Professional (CISSP) in good standing for the past 12 years and recently obtained the Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Control (CRISC) certifications from ISACA.*

Navigating the Digital Seas: Parallels between Pirates and Cyber Security Practitioners

Dana Turner, Union Bank and Trust

Arr matey! This here presentation be drawin' likenesses betwixt pirates and cyber security mateys to shine a light on the common traits and trials they be facin'. It be crucial to be notin' the moral disparities 'twixt these two crews, makin' it clear that cyber security professionals be sailin' within the bounds of law and ethics.

Experience Level: Beginner, Intermediate

Dana Turner, CISSP, is addicted to everything Infosec and has been since before it was cool. He has more than 35 years' experience in IT and Information/Network Security and is the Network Security Officer for Lincoln, NE-based Union Bank and Trust Company. Dana is passionate about helping to align IT with business objectives, while effectively managing risk and not just meeting compliance requirements, but exceeding them. He also leads the critical incident response team at UBT aided by more than a decade of operational and tactical experience as a volunteer first responder in the fire/ems service, dealing with incident and crisis management. As an information security practitioner, Dana enjoys giving back to the community by volunteering in a technical and/or information security advisory capacity for non-profit organizations. Most weekends you can find him working on metal or wood craft projects, studying up on the latest covert entry techniques or doing something motorcycle related with his wife Candice.

Network Threat Hunting and You! Two-Hour Workshop

John Strand, Antisyphon Infosec Training

Abstract: Fantastic malware and how to find it on your network. For free while grooving with a pict.

Experience Level: Intermediate, Advanced

John Strand has consulted and taught thousands of classes and hundreds of organizations in the areas of security, regulatory compliance and penetration testing. He is a coveted speaker and much-loved former SANS instructor and course author. John is a contributor to the industry shaping Penetration Testing Execution Standard and 20 Critical Security Controls frameworks. In 2008, John founded Black Hills Information Security (BHIS), a pentesting company that strives to understand its clients from a holistic perspective, emphasizing collaboration and education over stunt hacking. Since then, BHIS has grown to become a "tribe of companies" that includes Antisyphon Infosec Training, Active Countermeasures (ACM), Wild West Hackin' Fest (WWHF), and more.

Out of Sight, Out of Control: Asset Intelligence

Michael A. Atkinson, Armis

Prerequisites: An open mind and a willingness (among some of them, preferably) to ask questions and make this more of a discussion and less of a lecture.

We discuss the changed IT asset landscape and how asset intelligence is key to understanding what you have, where it is, and what vulnerabilities and other risks are associated with those assets. This is particularly important for those organizations in state government, local government and education as they never or nearly never know what kinds of unagentable devices are on their networks, much less where they are or what they're doing.

Experience Level: Beginner, Intermediate, Advanced

Mike Atkinson is a veteran cybersecurity practitioner and speaker, currently serving as the Principal Engineer for the Public Sector team at Armis. He lives in a far suburb of Chicago and believes that when he dies, if he was bad, that he will end up at O'Hare for his afterlife.

Security Risks of Generative AI

Jon Nelson, InfoTech Research Group

Prerequisite: Knowledge of Gen AI tools such as ChatGPT, Bard and Bing Chat is useful.

In this presentation we review InfoTech's approach to the security risks of generative AI. We start with a brief history of Gen AI, an overview of how it works and why it is so different than classic computing. We the discuss privacy and confidentiality risks of inputting data into AI; integrity attacks of how output from Gen AI can be misused and finally how AI technology can be used to augment and enhance existing phishing/whaling attacks. We then discuss InfoTech's approach to dealing with these threats; namely tackling Gen AI head on and establishing an acceptable use policy and then educating your users on the policy and the risks.

Experience Level: Beginner, Intermediate, Advanced

Jon Nelson is a Principal Advisory Director in the Security & Privacy practice. A seasoned security professional, Jon is passionate about helping clients improve their security practices and capabilities. Jon has more than 25 years of experience in IT and cybersecurity, primarily within the fintech industry. Most recently Jon served as an Information Security Risk Officer for a Fortune 500 Fintech responsible for core banking and payment systems, moving trillions of dollars each day. In this role Jon led a team of risk managers and analysts responsible for vulnerability management, governance, app sec assurance and enterprise architecture. Jon also has been tasked to lead an app sec red team that employed shift-left principles such as Threat Modeling, Abuse Case Development, and STRIDE methodology to software lifecycle development. This team was also responsible for app sec fundamentals such as Static Analysis Security Testing (SAST), Dynamic Analysis Security Testing (DAST), and Open Source.

The 90s Called and They Want Their Email Security Back!

Julie Paul, Check Point Software Technologies

How to keep your business flowing and the importance of a modern API-based email security.

Experience Level: Beginner, Intermediate, Advanced

For the past 28 years Julie has worked with security as a primary focus around the world. She started her career in the USAF as a Communications Computer Operator. She served at Kadena AB Okinawa Japan, Prince Sultan AB Saudi Arabia during Desert Shield and was at Offutt AFB Nebraska. During her 11 ½ years of service she encountered some interesting security issues such as the "Melissa" virus that took down the Air Combat Command network. She was instrumental in developing a plan of attack and orchestrated several security changes at Offutt AFB. Since leaving the Air Force, she has worked in several extremely complex networks. At her last position as a Global Network Security Architect she designed and created the network audit program. Julie has a Bachelor's degree in Networking and a Masters of Security Management degree from Bellevue University. Currently she works at Check Point Software Technologies as the Security Engineering Manager for the The Heartland area.

When the Whole World is Watching - Enduring Security

See page 13 for details.

Zero Trust ≠ Zero Risk

Ronald Woerner, Forrester Research

Zero Trust is the buzzword of the 2020s. Vendors are selling it, the U.S. Federal Government requires it and organizations are implementing it. But what does it really mean (I mean really beyond the hype)? In this session, you'll hear what Zero Trust really means in 2023 from a technical member of the organization that started it all. You'll also learn why Zero Trust is needed to combat threats and how to accelerate your cybersecurity program. We'll take a deep dive into the Zero Trust pillars (or components): Identity, Device, Workloads, Network, Data, Visibility and Analytics, and Orchestration and Automation. We'll also talk about technologies that make Zero Trust possible and how to use them to accelerate your cybersecurity program such as Identity and Credential Access Management (ICAM), Policy Decision Points (PDP) and Policy Enforcement Points (PEP). Zero Trust ain't going away so prepare yourself and your organization in this session.

Experience Level: Advanced

Ron Woerner, Senior Security and Risk Consultant at Forrester has more than 20 years of IT and security experience as a noted consultant, keynote speaker, educator, blogger, and podcaster. At Forrester, he focuses on building cybersecurity and Zero Trust programs for large organizations and US Federal Agencies. Ron also teaches at Bellevue University, an NSA Center of Academic Excellence. He is a member of the ISC2 North American Advisory Committee, the RSA conference program committee, has numerous technology degrees, and is passionate about building the next generation of cyber professionals.

EDUCATION

10:15 a.m. Session

Cyber Tatanka Panel, *Tim Pospisil, Dustin Thorne and Dana Turner*

Impact of Open Source Intelligence of Offensive Security and Investigative Practices, *Md Rashedul Hasan*

Network Threat Hunting and You! Two-Hour Workshop (Part 1), *John Strand*

When the Whole World is Watching - Enduring Security, *Robert Palmer*

11:15 a.m. Session

AI and Its Transformative Potential in Business & Cyber Security: ChatGPT Makes a Terrible Search Engine, *Gregory Richardson*

It's Okay to Walk Away, *Karla Carter*

Network Threat Hunting and You! Two-Hour Workshop (Part 1), *John Strand*

Security Risks of Generative AI, *Jon Nelson*

2 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand, Gregory Goodwater, and Warren Hagelstien*

Cybersecurity Priorities for Organizations, *Ben Hall*

3 p.m. Session

The 90s Called and They Want Their Email Security Back!, *Julie Paul*

Defending Your Lan and Wireless Networks, *Joseph Hall*

Navigating the Digital Seas: Parallels between Pirates and Cyber Security Practitioners, *Dana Turner*

END USER

10:15 a.m. Session

Cyber Tatanka Panel, *Tim Pospisil, Dustin Thorne and Dana Turner*

Impact of Open Source Intelligence of Offensive Security and Investigative Practices, *Md Rashedul Hasan*

When the Whole World is Watching - Enduring Security, *Robert Palmer*

11:15 a.m. Session

It's Okay to Walk Away, *Karla Carter*

Security Risks of Generative AI, *Jon Nelson*

2 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand, Gregory Goodwater, and Warren Hagelstien*

Zero Trust ≠ Zero Risk, *Ronald Woerner*

3 p.m. Session

Navigating the Digital Seas: Parallels between Pirates and Cyber Security Practitioners, *Dana Turner*

MANAGEMENT

10:15 a.m. Session

Cyber Tatanka Panel, *Tim Pospisil, Dustin Thorne and Dana Turner*

Impact of Open Source Intelligence of Offensive Security and Investigative Practices, *Md Rashedul Hasan*

When the Whole World is Watching - Enduring Security, *Robert Palmer*

11:15 a.m. Session

AI and Its Transformative Potential in Business & Cyber Security: ChatGPT Makes a Terrible Search Engine, *Gregory Richardson*

It's Okay to Walk Away, *Karla Carter*

Security Risks of Generative AI, *Jon Nelson*

1 p.m. Session

Out of Sight, Out of Control: Asset Intelligence, *Michael A. Atkinson*

Cloud Security Awareness, *Jacob Charles*

Contingency Planning for a Rainy Day, *AmyLynn Creaney*

2 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand, Gregory Goodwater, and Warren Hagelstien*

Zero Trust ≠ Zero Risk, Ronald Woerner

Cybersecurity Priorities for Organizations, *Ben Hall*

3 p.m. Session

The 90s Called and They Want Their Email Security Back!, *Julie Paul*

Defending Your Lan and Wireless Networks, *Joseph Hall*

Navigating the Digital Seas: Parallels between Pirates and Cyber Security Practitioners, *Dana Turner*

TECHNICAL

10:15 a.m. Session

Cyber Tatanka Panel, *Tim Pospisil, Dustin Thorne and Dana Turner*

Impact of Open Source Intelligence of Offensive Security and Investigative Practices, *Md Rashedul Hasan*

Network Threat Hunting and You! Two-Hour Workshop (Part 1), *John Strand*

11:15 a.m. Session

AI and Its Transformative Potential in Business & Cyber Security: ChatGPT Makes a Terrible Search Engine, *Gregory Richardson*

It's Okay to Walk Away, *Karla Carter*

Network Threat Hunting and You! Two-Hour Workshop (Part 1), *John Strand*

Security Risks of Generative AI, *Jon Nelson*

1 p.m. Session

Out of Sight, Out of Control: Asset Intelligence, *Michael A. Atkinson*

Cloud Security Awareness, *Jacob Charles*

2 p.m. Session

Zero Trust ≠ Zero Risk, *Ronald Woerner*

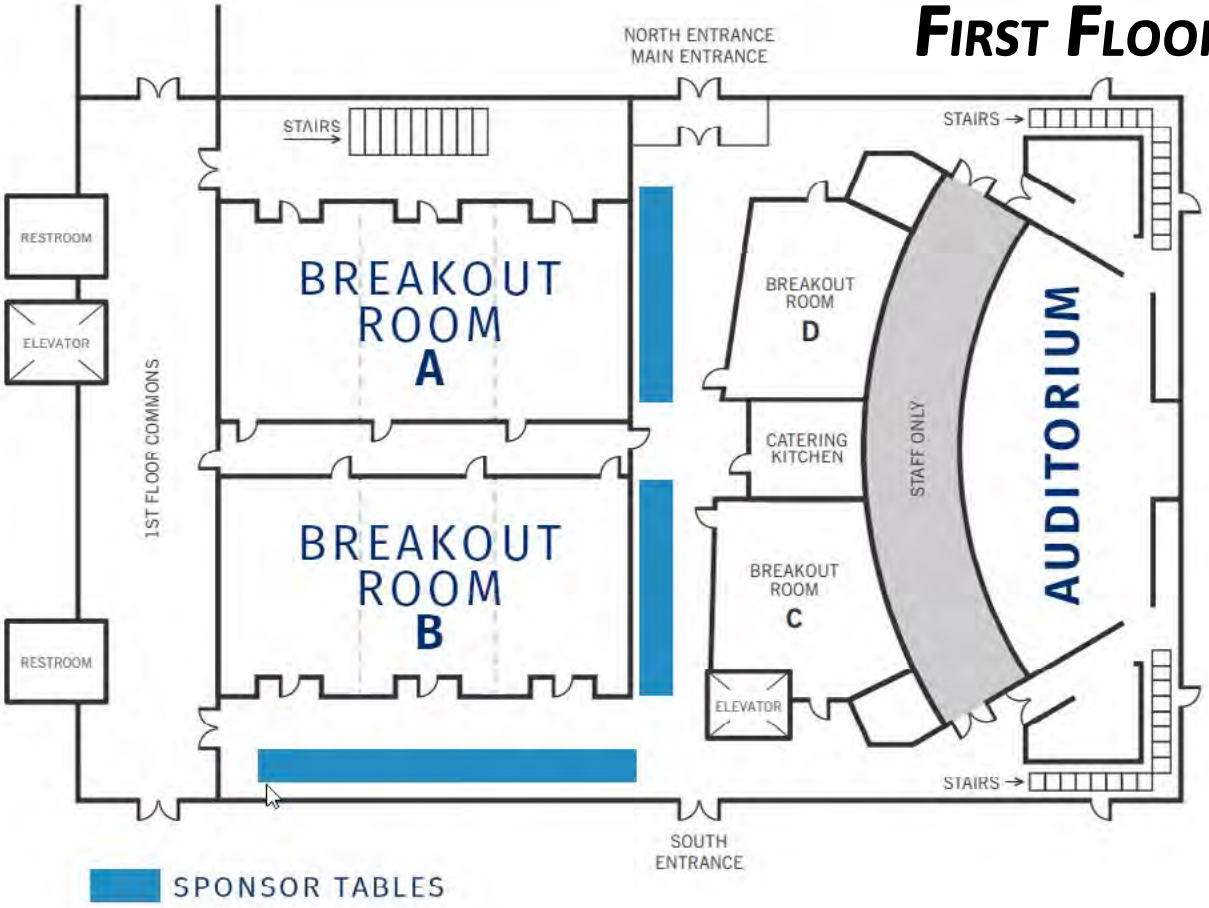
Cybersecurity Priorities for Organizations, *Ben Hall*

3 p.m. Session

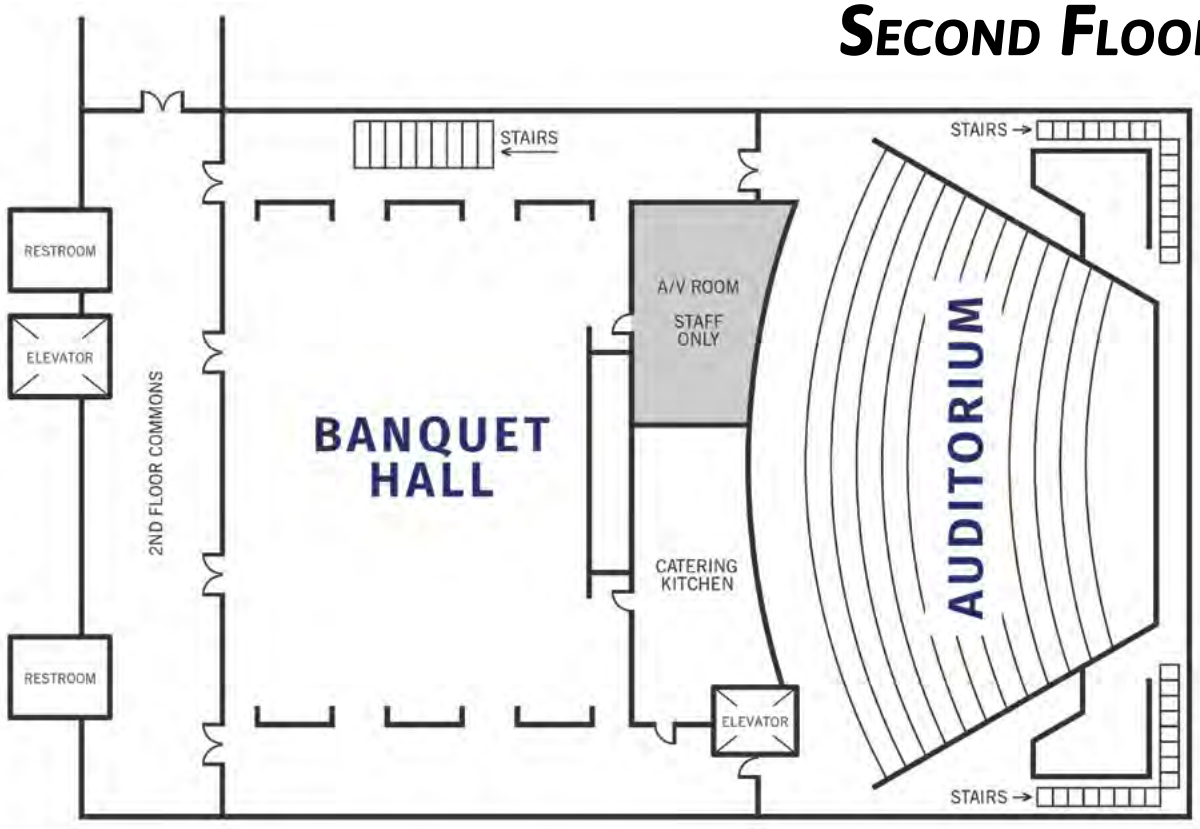
The 90s Called and They Want Their Email Security Back!, *Julie Paul*

Defending Your Lan and Wireless Networks, *Joseph Hall*

FIRST FLOOR



SECOND FLOOR



Continental Breakfast

Breakfast Frittata Casserole

Assorted Danish

Mini & Medium Donuts

Mini Bagels & Cream Cheese

Market Fresh Seasonal Fruit

Ice Tea, Water and Coffee

Afternoon Snack

Traditional Chex Mix Snack Mix

Ice Tea, Water, Coffee, and Assorted Pepsi Products

Lunch

Barbecue Shredded Chicken Sandwich

Brioche Slider Roll

Dill Pickle Slices

Gourmet Macaroni & Cheese

Baked Beans

Kettle Chips

Cookies

Ice Tea, Water, Coffee, and Assorted Pepsi Products

For those who requested dietary considerations, alternate meals have been prepared. Items are limited, so please only take one if it was requested.

Meals are prepared in a shared kitchen.

Catering provided exclusively by: Premier Catering

Allo FIBER
2003 — 20 YEARS — 2023

Americom nile

AXONIUS

CHECK POINT™

elastic

FORTINET®

HBS

paloalto® NETWORKS

ABSOLUTE®

antisyphon training

ARMIS

IBM Security

OPTIV®

rubrik SLED

splunk>

tenable®

tyler technologies

GREAT SEAL OF THE STATE OF NEBRASKA MARCH 1ST 1867

NEBRASKA OFFICE OF THE CIO

Southeast COMMUNITY COLLEGE

U.S. DEPARTMENT OF HOMELAND SECURITY

Agenda

10:15 a.m.	**Breakout Sessions**	***Cyber Tatanka Panel,*** Tim Pospisil, Dustin Thorne and Dana Turner		Auditorium
		Impact of Open Source Intelligence of Offensive Security and Investigative Practices, Md Rashedul Hasan		Room A
		Network Threat Hunting and You! Two-Hour Workshop (Part 1), John Strand		Room B
		When the Whole World is Watching - Enduring Security, Robert Palmer		Room D

Additional Breakout Session

When the Whole World is Watching - Enduring Security

Robert Palmer, Mandiant, Now Part of Google Cloud

Experience Level: Beginner, Intermediate

Robert Palmer is the Director of Mandiant-Google Public Sectors "Incident Response and Proactive Services" teams, providing services to state, local government, higher education, and federal agencies. Robert has been with Mandiant for eight years, specializing in Incident Response. Prior to joining the Mandiant team, Robert was provided the opportunity to hold roles specific to incident response, cyber threat hunting and malware reverse engineering. Robert additionally has a background with the 1st Marine Special Operations as a team level combat communicator. Robert's role with Mandiant affords him the opportunity to lead incident response efforts against the most complex and impactful cyber security attacks across the globe. Leading a team of dedicated Incident Response consultants, Roberts' team is regularly on the forefront of compromises conducted by advanced, nation-funded threat actor organizations, developing methodologies for detection, investigation, and eradication and facilitating a stronger cyber security posture for his clients.