Cyber security is everyone's business.

Join Leading Experts on Cyber Security

19th Annual

NCSC

Nebraska Cyber Security Conference

Conference Guide

Tuesday, Sept. 17, 2024
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: NUGuest
Username: September17
Password: Innovate2024!

Keynote Speaker: Tim Vidas

Amazon

Tim Vidas a Principal Engineer at Amazon Web Services (AWS) focused on Threat Intelligence and operational security. Prior to joining AWS, Tim collected decades of experience in a mix of academic, commercial and government settings. His endeavors span from being the development team lead for DARPA's Cyber Grand Challenge, to digital forensics research lead at CERT, to developing a high-assurance security kernel at NPS. Tim has a Ph.D. in ECE from Carnegie Mellon, and also is a DEF CON black badge holder. Tim also is a founder of both the local DC402 DEF CON group and the Kernelcon conference.

			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 a.m.	**Breakout Sessions**	***Designing a Successful Identity Security Program,*** Cullen Landrum & Dane Paulsen	Education, Management	Auditorium
		Navigating Privacy in the Age of Generative AI, Ross Coudeyras	Education, End User, Management, Technical	Room A
		Attack, Detect, Defend: Antisyphon Training (Part 1), Kent Ickler & Jordan Drysdale	Education, Technical	Room B
9:45 a.m.	**Break**			
10 a.m.	**Breakout Sessions**	***Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications,*** Audra Streetman	Education, Management, Technical	Auditorium
		Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, Md Rashedul Hasan	Education, End User, Management, Technical	Room A
		Attack, Detect, Defend: Antisyphon Training (Part 2), Kent Ickler & Jordan Drysdale	Education, Technical	Room B
10:45 a.m.	**Break**			
11 a.m.	**Breakout Sessions**	***Identifying the Adversary and Operationalizing Cyber Threat Intelligence,*** Richard Mendoza	Education, End User, Management, Technical	Auditorium
		Does Mr. Data Dream at Night?, Aamir Lakhani	Education, End User, Management, Technical	Room A
		Antisyphon Open Exhibits		Room B
11:45 a.m.	**Lunch** *(provided)*			
1 p.m.	**Keynote: Tim Vidas**			Auditorium
2 p.m.	**Break**			
2:15 p.m.	**Breakout Sessions**	***Accelerating the Evolution of Cybersecurity Using a Converged Approach,*** Chris Cruz	Management	Auditorium
		Securing Data in an AI Driven World, Patrick Wright	Management, Technical	Room A
		Antisyphon Open Exhibits		Room B
3 p.m.	**Break**			
3:15 p.m.	**Breakout Sessions**	***National Cyber Security Awareness Month and CISA Cyber Security Services,*** Nicholas Brand	Education, End User, Management	Auditorium
		Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, Karla Carter	Education, End User, Management	Room A
		Antisyphon Open Exhibits		Room B

Education End User Management Technical

Accelerating the Evolution of Cybersecurity Using a Converged Approach

Chris Cruz, Tanium

To defend against attacks & protect critical data, Government needs a paradigm shift for complex risk & technology issues. Local Government Chief Information Officers (CIO's) and Chief Information Security Officers (CISO's) have thousands of distributed assets to see and control, but most of them cannot capture how many endpoints they have, what applications run on them, or whether they have the right access controls across them. Tanium Public Sector Chief Information Officer (CIO) Chris Cruz will discuss the convergence of real-time decisions and remediation using one plane of glass/one source of truth, unified controls, a common taxonomy and how he developed a common cybersecurity plan as a former State and County government CIO. He will discuss the need for new generations of tools and new frameworks for them to address a unified cybersecurity approach.

Experience Level: Intermediate

Chris serves as Tanium's Public Sector CIO for SLED (State, Local, Education), bringing more than 31 years of government and public sector leadership to the role, including tenure asthe Director and CIO for the County of San Joaquin in Stockton, California. Prior to this position, he served as the State of California's Deputy CIO, and was the CIO for the California Department of Food and Agriculture, the Department of Health Care Services and was the first such leader for the Health Benefits Exchange, now referred to as Covered California. Chris earned a Bachelor of Science Degree in Business Management from California State University at Sacramento, and a certification from the UC Davis Master's Program in Leadership Excellence. He was recognized by StateScoop as one of the top 2024 SLED Industry Leaders of the Year, by Forbes on the CIO Next List for 2023, StateScoop as one of the 2020 County Executive Leaders of the Year and received national honors from the National Association of State Chief Information Officers (NASCIO) as the 2018 State Technology Innovator of the Year.

Attack, Detect, Defend: Antisyphon Training

Kent Ickler & Jordan Drysdale, Antisyphon

In this session we will give an overview into what we call threat optics: auditing endpoints, centralizing logs and visualizing results.

Each student will leave the class having experienced a penetration test through three distinct perspectives, each building on the previous. These will include adversarial attacks, examination of defensive postures, and wrapped up with various detection methodologies using open-source or free industry threat detection and defenses.

Experience Level: Beginner

***Kent Ickler** started his Information Technology career working for an Internet Service Provider supporting the MidWest's broadband initiatives of the early 2000s. His interest in technology and business operations drove his career into working for multiple Fortune 500 companies and equipping their organizational leadership with business analytical data that would support their technology initiatives. With an understanding of Information Technology, System Administration, Accounting, and Business Law, Kent has helped businesses leverage technology for competitive advantage while balancing the risks associated with today's dynamic network environments. Kent has been with Black Hills Information Security for three years in security and administration roles.*

***Jordan Drysdale** has been with the Black Hills Information Security (BHIS) tribe since December 2015. He is a Security Analyst, as well as a member of the systems administration team. Jordan came to BHIS with a strong background, including many years in networking tech support and engineering for HP, UNi and Managed Services — he never stops learning and sharpening his skills.*

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment

Md Rashedul Hasan, University of Nebraska-Lincoln

Prerequisites: Application Security Analysis, VAPT, Different Vulnerability Types, Knowledge about Machine Learning, AI Usage

As cyber threats become more sophisticated, detecting software vulnerabilities earlier using artificial intelligence techniques can help secure interconnected systems. However, current commercial language models do not effectively address all criteria needed to identify and mitigate certain vulnerabilities. This talk discusses the deficiencies of language models to comprehensively assess software vulnerabilities. A comparative analysis evaluates the LLM model's performance through the usage of a benchmark data set. Results reveal limitations in providing resilient fixes for optimized vulnerability versions, often falling short in constructive suggestions. The goal is to address the criteria and limitations for diverse vulnerability properties and interactions beyond what current models can achieve. By consolidating the strengths of different models and techniques a resilience driven -based approach can be developed to detect security vulnerabilities.

Experience Level: Intermediate

Md Rashedul Hasan is a Ph.D. student at the University of Nebraska-Lincoln, currently pursuing a Ph.D. in Computer Science (since Spring 2022) while also serving as a Graduate Research Assistant at the School of Computing, University of Nebraska-Lincoln. He is a graduate of Software Engineering, having completed his Bachelor's Degree at Daffodil International Universityin Fall 2019. Additionally, he is an Information Security Researcher and OSINT Expert who has participated in various training programs in Bangladesh, Singapore, Indonesia, and Malaysia. He has been involved in information security since 2013, personally assisting different government organizations in Bangladesh in understanding cybercrime measures and countermeasures. In 2017, he began working at Detectify as a CrowdSource Researcher. His co-founded startup, CyberTrendz Inc., was selected in the top 27 in Grameenphone Accelerator Season 3 and progressed to the top 19. Cybertrendz Inc. has conducted numerous workshops, seminars and public consultations to raise awareness about cybersecurity, including events in Dhanmondi, Dhaka, Bangladesh, and seminars at BDjobs Training's corporate office. Rashed regularly engages in information security activities and has received numerous accolades, including hall of fames, bounties and responsible disclosures from various companies. He was the runner-up in a Capture The Flag competition named #Hacktag 2017 and was chosen as a Researcher in Zerocopter in 2018. In 2019, he received a fully-funded scholarship from ITS Indonesia to join Commtech: Community and Technological camp and participated in cybersecurity training in Malaysia and Singapore. Since 2019, he has been working as a core Researcher at Zerocopter, earning hall of fame listings from reputable companies such as T-Mobile, Twitter, Snapchat, the US Department of Defense (DoD), Mavenlink, Edmodo, TTS BBP, Mobidea, Envoy, Magento, and more. From 2020 to 2021, Rashed worked as an Assistant Maintenance Engineer with the Ministry of Defense of Bangladesh. He has diverse interests in Information Security Research, including Application and Mobile Security, Network Security, Cyber Physical Systems, and Malware analysis. In recent years, he has focused on AI and Software Engineering-centric research, participating in various workshops and programs such as the 12th Summer School on Formal Techniques by SRI in 2023 and, recently in 2024, being invited to ICANN 79 community forum as a NextGen Participant. Transitioning from an independent security researcher, Rashed aims to become a business associate and stakeholder in the IT industry in the future.

Designing a Successful Identity Security Program

Cullen Landrum, SailPoint, & Dane Paulsen, Flatwater Services

In this session, we will discuss what it takes to have a successful Identity Security program. Identity Security is fundamental to any organization to meet audit, zero trust and more. Dane will describe what it took for his organization to decide on a solution and what it took to get a program going. Also, we will discuss his decision to migrate to a SaaS solution and what was involved in that decision.

Experience Level: Beginner

With 20+ years of experience in Identity and Access Management, ***Cullen Landrum*** *is a Senior Sales Engineer at SailPoint. Cullen specializes in the area of Identity Security. Prior to joining SailPoint, Cullen worked for several software companies, including Aegis Identity, Oracle and Sun Microsystems supporting higher education, federal, state, and local. Prior to that Cullen worked at EDS where he spent 10+ years as a developer on everything from mainframes to Tandem to Java. Cullen holds a Bachelor of Arts in Computer Science and Mathematics from the University of Colorado, is a Certified Information Systems Security Professional (CISSP) and is a member of Information Systems Security Association (ISSA).*

As a leader of people and enterprise technologies, ***Dane Paulsen*** *brings 20+ years experience in program development and strategy. Dane is an industry-respected subject matter expert in Identity and Access Management (IAM) and Governance (IGA) programs leadership. Known for cultivating collaborative partnerships, he has a reputation for building highly engaged teams and achieving business objectives through accountability, creative resource management and agile methodologies. Dane currently serves as the Director of Identity and Access Management at ProofID, a global services firm dedicated to every facet of Identity Security and building the best possible identity solutions for businesses. He also is a Principal Advisor at Flatwater Services providing fractional technology leadership to enterprises, small businesses, non-profits, and individuals looking to strategically improve their operations. Dane is grateful for the relentless support and adoration of his wife Cindy, an elementary school teacher, and their five amazing children. Outside of work you often find Dane chasing kids to activities, coaching high school theater or serving in his faith community. Dane is a sucker for pop-music and deep conversations about big ideas over coffee or cocktails.*

Does Mr. Data Dream at Night?

Aamir Lakhani, Fortinet

We may fantasize about the days of Star Trek and Terminator where artificial intelligence might be able to help us accomplish impossible tasks or perhaps, we are worried it may destroy us. The reality is AI within cybersecurity is much more nuanced than most people realize and the everyday mistakes it can cause can exponentially harm the way we protect organizations. Cybersecurity and AI researcher Lakhani will discuss how AI solutions within cybersecurity actually work, how they can help solve problems against modern threat actors and nation states, and issues and problems cybersecurity professionals have to look out for when implementing these solutions. Learn about real-world attack scenarios that Aamir is developing and solving using AI tools to combat denial of service attacks, ransomware and phishing related attacks.

Experience Level: Beginner

Aamir Lakhani is a leading senior security strategist. He is responsible for providing IT security solutions to major enterprises and government organizations. He is a member of the AI and Cybersecurity advisory boards for the World Economic Forum, Cyber Threat Alliance, MITRE, and Cybersecurity and Infrastructure Security Agency (CISA).

Lakhani creates technical security strategies and leads security implementation projects for Fortune 500 companies. Industries of focus include healthcare providers, educational institutions, financial institutions, and government organizations. Aamir has designed offensive counter-defense measures for the Department of Defense and national intelligence agencies. He also has assisted organizations with safeguarding IT and physical environments from attacks perpetrated by underground cybercriminal groups.

Identifying the Adversary and Operationalizing Cyber Threat Intelligence

Richard Mendoza, Google

In this session, we will explore the critical process of identifying adversaries and their TTPs to enhance your defense mechanisms. We'll discuss methods for effectively analyzing and understanding potential threats, transforming this intelligence into actionable strategies. Attendees will gain insights into integrating these practices within their security operations to proactively defend against the latest cyber threats.

Experience Level: Intermediate

Richard E. Mendoza is an accomplished cybersecurity expert, having earned an MBA with a degree concentration in Information Assurance adhering to The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. He holds a CISSP and is a Google Professional Certified Security Cloud Engineer. His career experience includes AT&T, Mandiant Consulting and is currently a Security Architect within Google Public Sector. Richard positions have included Digital Forensic Investigation and Incident Response. His speciality is Operationalizing Cyber Threat Intelligence within the Security Operations Center.

National Cyber Security Awareness Month and CISA Cyber Security Services

Nicholas Brand, 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.

Navigating Privacy in the Age of Generative AI

Ross Coudeyras, Remesh

Join us for an insightful exploration into the privacy implications surrounding the surge of Large Language Model (LLM) generative AI technology. In the wake of OpenAI's ChatGPT 3.5 release, the landscape of AI-powered innovation has evolved rapidly, prompting critical questions about data security and privacy safeguards. In this presentation, we'll delve into a real-world case study of a SaaS B2B tech company's journey to leverage this cutting-edge technology responsibly. Learn first hand how they successfully navigated the complex terrain of privacy concerns while collaborating closely with enterprise-level customers. From implementing robust data protection measures to forging secure partnerships with AI providers like OpenAI, discover actionable strategies to safeguard sensitive information without compromising innovation.

Experience Level: Intermediate

With 16+ years in software and technology, Ross Coudeyras is a recognized authority in cybersecurity and data privacy. Currently heading Security and Compliance, as well asserving as Data Protection Officer at Remesh, he is known for his practical approach to securing digital landscapes. At Remesh, Ross Coudeyras leads security and compliance efforts, ensuring the organization aligns with regulations while staying resilient against cyber threats. His real-world insights bridge the gap between security measures and compliance needs. As an adjunct instructor at Doane University, Ross Coudeyras imparts hands-on knowledge to future cybersecurity professionals, leveraging his industry know-how to prepare students for real challenges. Ross also is into Dune. Fear is the mind-killer.

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity

Karla Carter, Bellevue University

Prerequisite: An interest in the topic - suitable for all levels of cybersecurity experience

["Oh, no," the audience gasps, getting that sinking feeling . . . "it's Professor Karla again . . . and she's wearing that Titanic dress . . ."] Yes! We are journeying back to the Titanic! This time, in "Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity," we dive into how varying interpretations of the same policy led to drastically different outcomes. We will explore how these historical lessons can buoy your present-day cybersecurity efforts, keeping your organization sailing smoothly. Well-anchored procedures and policies, when executed consistently across all levels of your organization, can steer you in the right direction. However, procedural discrepancies in cybersecurity practices can scuttle your defenses, leaving your organization vulnerable to threats. All aboard!

Experience Level: Intermediate

Karla Carter is an Associate Professor of Cybersecurity in the College of Science and Technology at Bellevue University, in Bellevue, NE. Drawing on more years than she should admit to of information technology experience, she teaches undergraduate and graduate courses in cybersecurity operations, social engineering, human factors, security awareness, white-collar crime, information warfare, technology ethics, and — in a plot twist you didn't see coming — occasionally history and civics. Additionally, she serves on the IEEE Nebraska Section Executive Committee and ACM Committee on Professional Ethics. Curious, intense, and irreverent, Carter lives by the question, "what if...?" and has a low tolerance for the phrase "because that's the way we've always done it." She might even surprise you with a Melville quote that didn't make it into Star Trek II: The Wrath of Khan.

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications

Audra Streetman, Splunk

Large language models are all the rage right now, but do you have the visibility to detect exploitation of the top LLM vulnerabilities? To address threats such as prompt injection attacks, sensitive information disclosure and others, the SURGe research team at Splunk collected and analyzed LLM prompt and response data for real-time threat detection. Join this talk to learn how this research overlaps with the OWASP Top 10 for LLM Applications. We'll show some methods created using Splunk as a detection layer for LLM data to help you better defend against emerging threats.

Experience Level: Intermediate

Audra Streetman is a member of SURGe, Splunk's security research team. Before arriving at Splunk, Audra worked as a reporter, producer and news anchor at local TV stations across the U.S. In her current role, Audra produces and co-hosts a podcast called The Security Detail, which examines the cyber threat landscape in different industries. She was nominated for the SANS Difference Makers Awards in 2022 and spoke at RSA Conference in 2023 and WiCyS Conference in 2024 about hiring career changers for cybersecurity roles.

Securing Data in an AI Driven World

Patrick Wright, State of Nebraska

This session will explore the unique challenges and innovative solutions for securing data in an era increasingly dominated by artificial intelligence.

Experience Level: Advanced

Patrick Wright is the State of Nebraska's Chief Information Security and Privacy Officer and is responsible for overseeing data security and privacy for the state government. His position includes strategic cybersecurity vision, statewide cybersecurity initiatives, cybersecurity and privacy operations, incident response, compliance under federal requirements, Federal and State law, and industry standards. Patrick is an information security professional who has worked in both the public and private sectors and holds multiple industry certifications, with a bachelor's degree in information technology and a master's degree in public policy and administration. He also has attended the Harvard Kennedy School of Government Cybersecurity: Intersection of Policy and Technology workshop. He has many years of experience at operational and strategic information security levels. Patrick is a member of the MS-ISAC Executive Committee under the Center for Internet Security. He develops and guides the State of Nebraska security policy and initiatives by chairing the Security Architecture Workgroup under the Nebraska Information Technology Commission and the Cybersecurity Grant Committee for the State and Local Cybersecurity Grant Program. Beyond state government, Patrick also chairs the Cybersecurity Workgroup for Network Nebraska, providing cybersecurity counsel to the K-12 and higher education communities within the State of Nebraska.

EDUCATION

9 a.m. Session

Attack, Detect, Defend: Antisyphon Training (Part 1), *Kent Ickler & Jordan Drysdale*

Designing a Successful Identity Security Program, *Cullen Landrum & Dane Paulsen*

Navigating Privacy in the Age of Generative AI, *Ross Coudeyras*

10 a.m. Session

Attack, Detect, Defend: Antisyphon Training (Part 2), *Kent Ickler & Jordan Drysdale*

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *Md Rashedul Hasan*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *Audra Streetman*

11 a.m. Session

Does Mr. Data Dream at Night?, *Aamir Lakhani*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence, *Richard Mendoza*

3:15 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *Karla Carter*

END USER

9 a.m. Session

Navigating Privacy in the Age of Generative AI, *Ross Coudeyras*

10 a.m. Session

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *Md Rashedul Hasan*

11 a.m. Session

Does Mr. Data Dream at Night?, *Aamir Lakhani*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence, *Richard Mendoza*

3:15 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *Karla Carter*

MANAGEMENT

9 a.m. Session

Designing a Successful Identity Security Program, *Cullen Landrum & Dane Paulsen*

Navigating Privacy in the Age of Generative AI, *Ross Coudeyras*

10 a.m. Session

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *Md Rashedul Hasan*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *Audra Streetman*

11 a.m. Session

Does Mr. Data Dream at Night?, *Aamir Lakhani*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence, *Richard Mendoza*

2:15 p.m. Session

Accelerating the Evolution of Cybersecurity Using a Converged Approach, *Chris Cruz*

Securing Data in an AI Driven World, *Patrick Wright*

3:15 p.m. Session

National Cyber Security Awareness Month and CISA Cyber Security Services, *Nicholas Brand*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *Karla Carter*

TECHNICAL

9 a.m. Session

Attack, Detect, Defend: Antisyphon Training (Part 1), *Kent Ickler & Jordan Drysdale*

Navigating Privacy in the Age of Generative AI, *Ross Coudeyras*

10 a.m. Session

Attack, Detect, Defend: Antisyphon Training (Part 2), *Kent Ickler & Jordan Drysdale*

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *Md Rashedul Hasan*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *Audra Streetman*

11 a.m. Session

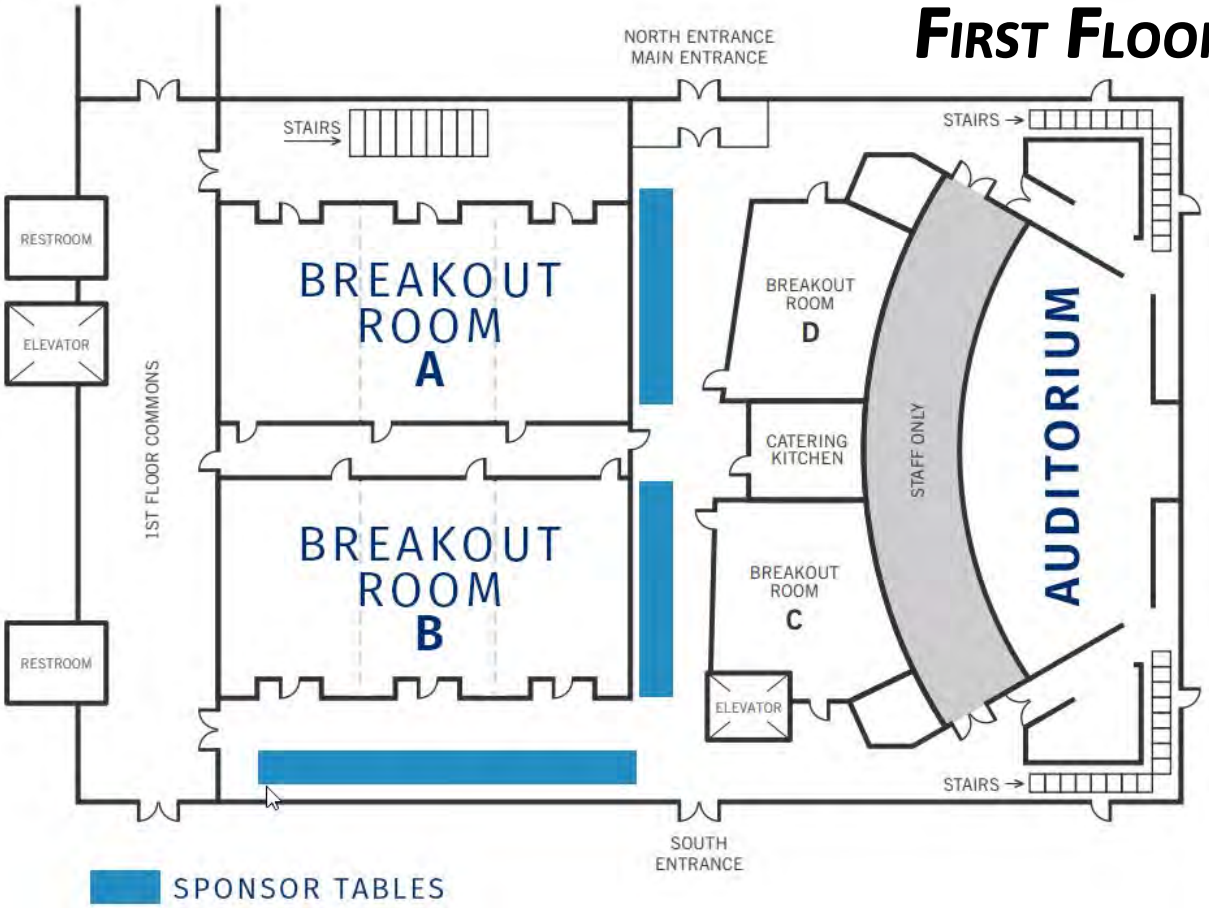
Does Mr. Data Dream at Night?, *Aamir Lakhani*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence, *Richard Mendoza*

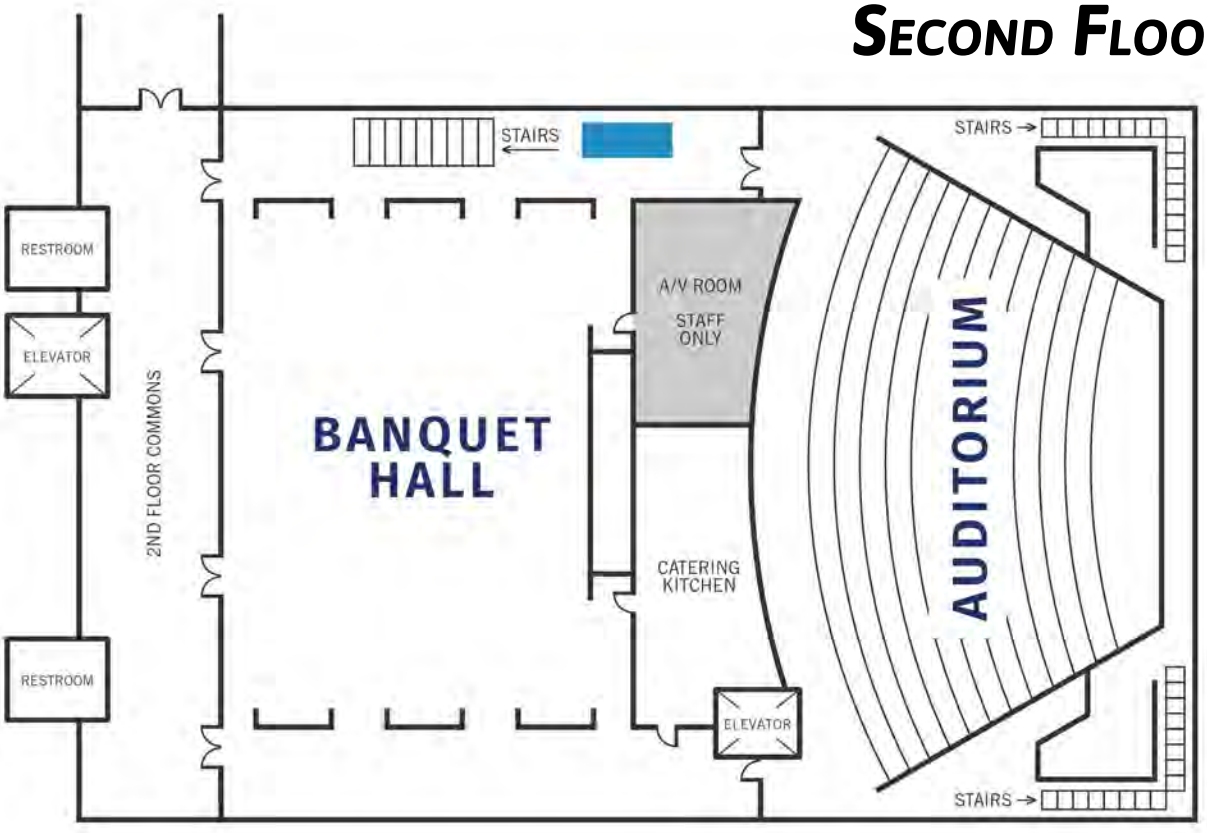
2:15 p.m. Session

Securing Data in an AI Driven World, *Patrick Wright*

FIRST FLOOR



SECOND FLOOR



Continental Breakfast

Breakfast Frittata Casserole

Assorted Danish

Mini & Medium Donuts

Mini Muffins

Mini Bagels & Cream Cheese

Market Fresh Seasonal Fruit

Afternoon Snack

Traditional Chex Mix Snack Mix

Assorted Pepsi Products

Lunch

Fried Chicken

Penne Rigatte Pomodoro

Oven Roasted Rosemary Potatoes

Chef's Vegetable Mix

Premier Salad

Broccoli & Bacon Pasta Salad

Macaroni

Sour Dough & Wheat Berry Rolls

Assorted Cookies

Assorted Pepsi Products

Available All Day

Ice Tea, Water, Coffee

**For those who have special dietary requests,
please talk to staff for options.**

Meals are prepared in a shared kitchen.

Catering provided exclusively by: Premier Catering

TANDEM

Google Cloud

Americom Cribl

CROWDSTRIKE CLOUDFLARE PUBLIC SECTOR FORTINET HBS

SailPoint STERLING tenable

antisyphon training GUIDEPOINT SECURITY OPTIV

paloalto NETWORKS splunk> a CISCO company TANIUM

TEKsystems Global Services tyler technologies Empowering people who serve the public verterent TIME TO START A NEW DAY

NEBRASKA OFFICE OF THE CIO Southeast COMMUNITY COLLEGE