Session	Description	Date	Start	End	Speakers
International Reception: State-sponsored Cyberattacks	Join us at the International Reception to welcome our international delegates, visitors to the United States, and invited guests. Included as part of the VIP All Access Pass or available to purchase as an extra item. The global cyber threat environment is being shaped by a series of significant state-sponsored cyberattacks.	10/20/25	17:00	19:00	Dr. David Mussington,Sean Costigan
InfraGard Breakfast	Fuel up and find out why the FBI InfraGard is the nation's strongest information-sharing network for security professionals and critical infrastructure protection. Meet recently retired FBI Special Agents Doug Dvorak, Liz Lehrkamp and John Bonhage, this year's CSS Visionary Security Awareness Program Leader honorees.	10/21/25	7:00	7:50	John Bonhage,Lizabeth Lehrkamp,Elizabeth Stevens,Douglas Dvorak
MNIT Careers Breakfast: For Students & Seasoned Cyber Pros	Hosted by MNIT, home to the State of Minnesota IT Services team, this is the breakfast where students can get career insights and learn about the cyber role options in government. Not a student? Not to worry!! All are welcome.	10/21/25	7:00	7:50	Chris Luhman,John Israel,Jen VanDemmeltraadt
Cyber Sports Regional CTF Competition - Observer	The Cyber Sports Regional Capture the Flag competition brings high-stakes cyber challenges and high-speed gamification to the Summit for the second year in a row. Stop by for a few minutes to see top high school, college and pro teams redefine hyper-focus from log in to flag found. Today's teens are tomorrow's workforce, and Cyber Sports Limited requires technical tactics, strategic smarts and teamwork to get to the finish line.	10/21/25	8:00	15:15	Darla Lewandowski,Lise Rediske
Welcome to the Cyber Security Summit	Thanks to title sponsor Google Cloud Security and the strength of a community 25K strong, Summit producer Eileen Manning gives a retrospective lookback, and CSS15 Summit Co-Chairs Shawn Riley and Shayla Treadwell start off two days of cybersecurity excellence by defining the Fearlessly Forward theme, including the "IT" in FIND IT. FIX IT. FORTIFY IT. Capes optional.	10/21/25	8:00	8:15	Eileen Manning,Shawn Riley,Shayla Treadwell
Chart New Frontiers and Transform Business with AI, Cyber and Cloud	Paint a picture of your work, using a palette of new frontiers for a horizon that's harmonized. See the transformative impact that results when organizations integrate artificial intelligence, cybersecurity, and cloud technologies across business operations. AI-driven security has brought a sea change for cybersecurity methods, with increased automation and orchestration in cyber defense, and the cloud serves as a canvas for AI to enhance business practices. These developments result in improved operational resilience and more effective management, with real-time anomaly detection, automated threat response, and improved critical system resilience against increasingly sophisticated cyberattacks. This is the picture of enhanced automation across security operations that allows organizations to autonomously investigate alerts, correlate diverse data sources, and initiate response actions all in a Fearlessly Forward frame.	10/21/25	8:15	9:00	Shayla Treadwell

State of the Hack	With the barrage of cyber-attacks from criminals, insiders, hactivists and nation-state threat actors, it's important to stay on top of the latest tradecraft to be able to defend and respond to incidents. Jibran Ilyas will walk through the perpetrators' tactics, techniques, and procedures and today's threat landscape to help prioritize cyber defense security program and project expense allocations. Brought to you by CSS15 Title Sponsor Google Cloud Security.	10/21/25	9:00	9:30	Jibran Ilyas
All Other Identities Are Here, Whether They're Welcome or Not	Let's talk identity. Today we obsess over workforce IAM and lock down employee access like Fort Knox. But what about the others? Non-human identities, external partners, and customer identities run wild. If you don't pay attention, they'll introduce massive security gaps. This session breaks down the identity landscape beyond human users to include the service accounts, bots, and workloads that outnumber employees and beg for managed security. We'll touch on vendors, partners, and contractors that need access that's both speedy and controlled. Plus our top customer identity (CIAM) challenge: how to lock things down without driving customers straight into the arms of the competition? In sum, this is the "one ecosystem deserves a common strategic solution" session.	10/21/25	10:00	10:30	David Lee
Resilience Refreshed: Break It Down to Build It Up	Cybersecurity work is often about disruption (ideally, preventing, but often, responding) and resilience is that word that permeates conversations like the 'win-win' of yesteryear. It's a business imperative, but what exactly is it, and what does it take to build and sustain it? Learn from candid discussion with industry leaders who have navigated through uncertainty, adapted to rapid change, and emerged stronger. We'll break it down to see what resiliency actually looks like across people, processes, and technology. Get strategies that strengthen organizational and technical resilience. Get insights on leading through change and fostering a collective culture of adaptability.	10/21/25	10:30	11:15	Corey West,Noam Perel,Dan Cunningham
Embracing the Cloud(s) Doesn't Have to Stop the Sun from Shining	Follow Castlelake's global technology and security transformation journey to a cloud-only environment. From the offices to the data centers to a portfolio of SaaS/PaaS/IaaS solutions and the build-out of a 24x7 support desk and security operations center, very little was left untouched, including re-working most of an existing Azure tenant and deploying a new cloud-centric security architecture. We'll discuss how and why the Castlelake/Avanade team designed and deployed the various elements of the solution and the many issues dealt with along the way. Finally, we'll touch on the pros and cons, lessons learned and how the firm is now positioned for growth, resilience, and flexibility now and into the future.	10/21/25	11:15	11:45	David Notch,John Orleans,Lynette Seminara

CISO Luncheon - Security that Drives Growth and Velocity	Explore how strong security foundations can accelerate delivery and business growth, rather than slow them down. Learn the steps to position your program in a positive light and elevate C-Suite perceptions. Leave with leverage and be seen as trusted enabler for innovation, customer confidence, and market expansion. The CISO Luncheon is sponsored by Chainguard. For C-level and senior executives, Summit Think Tank members and 2025 Visionary Leadership Award honorees. Select ADD TO WAITLIST to indicate interest prior to selecting "next". CISO Luncheon registration list will be vetted prior to the Summit. Check the Summit APP after October 20 or stop by the registration desk onsite to confirm your CISO Luncheon or Networking Lunch.	10/21/25	11:45 13:00	Quincy Castro
Safeguarding the Bioeconomy: Biotechnology Needs a Security Patch...Badly	The bioeconomy promises profound, beneficial impacts in the areas of health, agriculture, renewable energy, and additive manufacturing. However, when it comes to security, biological threats have historically focused on emerging infectious diseases or the possibility of engineering a virus to start a zombie apocalypse. As biotech converges with the cyber, AI, quantum, and telecom realms, new security challenges will arise. This presentation will highlight the need to radically redefine what we consider biological and cyber threats for the US and internationally.	10/21/25	13:00 13:40	Edward You
Ransomware Attack - The City's Detection and Response to Interlock	Join the City of St. Paul security team for a review of the recent ransomware attack initial access and detection phases. The brief will focus on the "drive-by download" technique used for initial access, and the endpoint detection and response (EDR) that signaled the City to take immediate response actions. Using the July 22, 2025 joint FBI	CISA	HHS	MS-ISAC Cybersecurity Advisory - #StopRansomware: Interlock we will highlight access techniques and methods, as well as critical identity and device protection and monitoring program elements.	10/21/25	13:40 14:30	Stefanie Horvath,Sherina Gant
Tackle Threats with New Teams and Non-Technical Tools	This interactive facilitated session, led by noted intelligence expert Chris Tatarka (35+ years with the FBI and U.S. Army), highlights the non-technical factors that often make or break security efforts. We'll examine how cognitive biases and underlying human-centric tendencies can quietly derail cyber security practices and responses. Through case studies and discussion we'll examine practical, non-technical tools to sharpen your ability to spot pitfalls, strengthen your practices and decision-making, and walk away with research-based ideas to move forward in enhancing security.	10/21/25	15:00 15:30	Christopher Tatarka

Rethinking Resilience: Don't Bounce Back, Forge Forward	What does it take to lean Fearlessly Forward and face the risk, speed, and daily disruption of the cyber sphere? And when things go really wrong, how do you forge ahead to lead others through turbulence? We've heard Be resilient - bounce back! but what if it's too late when you get back? Author, TedX speaker and former cybersecurity CEO Tissa Richards has found a dangerously incomplete definition and a fatal flaw in our traditional views on resilience. She'll share that gaping hole and more importantly how to build a better model that fills in the holes. Shifting resilience from a crisis comeback skill to a carefully constructed capability, she shares the secret sauce that supports adaptability, growth, and innovation. You'll lead through change rather than merely react to it, and respond faster and smarter in high-stakes environments. Most powerfully, you'll have the transformational confidence boost, clarity, and competitive edge that come from Rethinking Resilience. EXPO Reception Book Signing: meet author Tissa Richards and get a signed copy of her second book, Rethinking Resilience: Fueling Your Competitive Advantage.	10/21/25	15:30	16:15	Tissa Richards,Rob Slaughter
Visionary Leadership Awards	The 2025 Cyber Security Summit Visionary Leadership Awards recognize thirteen people behind the outstanding work that improves security and makes a difference. Nominated by peers and colleagues, the Visionary Leadership Award honorees will take the stage as we recognize and celebrate their Fearlessly Forward contributions.	10/21/25	16:15	17:00	David Notch, Christopher Buse
State of MN Department of Military Affairs Awards	State of Minnesota Department of Military Affairs Awards Major General Stefanie Horvath will present the 2025 Minnesota Achievement Ribbon, Minnesota Commendation Medal, and Minnesota Medal for Merit awards. These mission-focused awards recognize the exemplary service provided by soldiers and airmen during the response to the 2025 City of St. Paul cybersecurity incident. See page 27 for awards detail.	10/21/25	17:00	17:15	Mary Gleich-Matthews
VIP Dinner	The Summit's foundational strength is found in the fantastic community we've built over fifteen years. Check the box to attend Tuesday's VIP Dinner where you'll meet more people and discuss the day's highlights.	10/21/25	18:15	20:00	Jeremy Hehl
CISO Breakfast: Ally or Adversary? Rethinking AI in Cyber Defense	AI is rewriting the rules of cybersecurity are you ahead or already behind? From architecture to automation, it's time to rethink how we govern, detect, and defend. Join Avanade for a fast-paced, high-impact Breakfast Think Tank and dive into the strategies that matter most when resilience is non-negotiable. The CISO Breakfast is sponsored by Avanade. For C-level and senior executives. Select ADD TO WAITLIST to indicate interest prior to selecting "next". CISO Breakfast registration list will be vetted prior to the Summit. Check the Summit APP after October 20 or stop by the registration desk onsite to confirm your CISO Breakfast.	10/22/25	7:00	7:50	

Fuel Up & Stay Secure: Breakfast Bytes	Start your conference day right! Join us for a delicious breakfast session featuring flaky croissant sandwiches, hearty whole wheat wraps, and your favorite Caribou Coffee. Network with peers, recharge, before sessions kick off. Great food, great company, and smart security talk await!	10/22/25	7:00	7:50	
AM Cyber 101 - Session 1: Building Blocks: Developing a Comprehensive Cybersecurity Program	Learn how to build a strong cybersecurity program through standards, governance, and strategic alignment. This session covers risk mitigation, accountability frameworks, and oversight processes to help organizations enhance resilience, protect assets, and align cybersecurity efforts with business goals in today's evolving threat landscape.	10/22/25	8:00	9:15	Catherine Scott,Ron Olsen
MT - Welcome to the MedTech Seminar	In today's hyper-connected world, cybersecurity is no longer just a technical priority; it's a matter of patient safety. Nowhere is this more evident than in the healthcare industry, where a vulnerable medical device or a mis-configured system can impact operations and human lives. This MedTech Seminar is laser-focused on one mission: fortifying cyber resilience in healthcare and medical devices.	10/22/25	8:00	8:30	Mary Diner,Michelle Greeley
PS - Public Sector Seminar Welcome	The Public Sector Seminar brings a full day focus to the broad range of persistent cyber threats that challenge government at all levels - in Minnesota and beyond. We'll look at the many critical infrastructure efforts that reduce risk. Learn how law enforcement is prioritizing digital crimes, proactively and compassionately. We'll talk about the programs, processes and projects that support continuous improvement, and we'll find new ways to work together and bolster our collective security posture.	10/22/25	8:00	8:15	Jen VanDemmeltraadt
Public Sector Village: Hands-on Learning and Demos	For free resources and expert support that's NOT too good to be true - take a walk around the Public Sector Village to explore hands-on cybersecurity tools and shared services available to Minnesota's public entities. See how local governments, schools, and utilities can leverage no-cost and discounted resources for system hardening, detection and response, and incident support. Hosted by National Guard C3 and MNIT, the Village offers demos, walkthroughs, and real experts (no sales here!) sharing real tools in use across the state.	10/22/25	8:00	16:00	Nicolette Weis,Matthew Harberts,Marco Riley

TS 1A -Death by PowerPoint: Resurrecting Cybersecurity Training from the Grave	Let's face it cybersecurity training has long suffered from the curse of monotony: endless slides, robotic voiceovers, and quizzes that feel like they were written by ghosts of compliance past. In this spirited session, we'll explore how to breathe life back into global cybersecurity education programs using creative, culturally resonant, and interactive approaches that actually engage employees. From gamified learning and storytelling to regionally tailored content and spooky seasonal campaigns (yes, even Halloween-themed phishing simulations), we'll share tricks and treats to make training not just effective but unforgettable. Come for the laughs, stay for the lessons, and leave with ideas that won't haunt your workforce.	10/22/25	8:00	8:50	Lev Frayman
TS 1B - From Actors to Action: Cyber Threats and How to Defend Against Them in the Food and IT Sectors	The Food and Ag-ISAC and IT-ISAC jointly maintain playbooks on over 300 adversaries and have collected information on over 12,000 ransomware incidents and counting. Using analysis from these data sets and blending it with intelligence from their members and strategic partners, the ISACs have built individual sector-specific threat reports that provide a clear picture of their risk environment. This session will unpack the findings of these reports, delivering an overview into the threat landscape for the food and IT sectors. We'll connect the dots between adversary campaigns, evolving TTPs, and ransomware trends, while exploring the actors behind the attacks including their operations and motivations. Attendees will gain insight into best practices and actionable defenses that can be used to strengthen resilience and stay ahead of the adversaries.	10/22/25	8:00	8:50	Jonathan Braley
PS - Rebuilding Digital Trust: When and How to Use IAL2	As digital interactions become the default, establishing and maintaining trust has never been more critical. This session explores the role of NIST Identity Assurance Level 2 (IAL2) in combating fraud, meeting regulatory requirements, and protecting sensitive transactions. We'll discuss where IAL2 is the right fit, where it may create unnecessary friction, and how alternatives like componentized services or IAL1+ can provide the right balance of security and user experience. Attendees will walk away with practical insights on aligning assurance levels with business risk, reducing onboarding drop-off, and building adaptive trust frameworks that scale across industries.	10/22/25	8:15	8:45	Spencer Crane

MT - Overcoming Cyber Defensiveness: Real World Lessons From a 15-Year Security Transformation	Look inside the 15-year product cyber security transformation at Medtronic, a global health tech company. After the medical device industry was called out for vulnerable devices at a hacker conference, this leading manufacturer took bold steps to reshape its cybersecurity strategy. Hear the full story, from the initial public disclosure to the decision to use it as a catalyst for critical change. Learn about the process that included building partnerships with the hacker community to embed operational cyber resilience along with other program moves unique to the risks of connected healthcare technologies. Whether starting from scratch or strengthening an existing program, this real-world example includes some universally applicable challenges and lessons learned.	10/22/25	8:30	9:00	Nancy Brainerd
PS - Cyber Risk Insurance - Policy to Preparedness	This session explores cyber risk insurance and its role within a comprehensive cybersecurity strategy - and why it can't be the entire cybersecurity strategy. Get an understanding of key policy components and multiple cyber risk considerations. Whether you're evaluating a new policy or renewing an existing one, or wondering how insurance could possibly impact your (non-insurance focused) job, this session offers practical guidance to support informed policy decisions and strategic response preparedness.	10/22/25	8:45	9:30	Christian Torkelson
MT - Future-Proofing Healthcare: Tackle IoMT Security, Patching, and Device Diversity Challenges	Healthcare's digital core is growing fast as is the risk. In Future-Proofing Healthcare, experts explore how to remediate health systems vulnerabilities when patching is not feasible. By deploying risk-based remediation, healthcare can shift from reactive to resilient through context-aware risk modeling. Walk away with scalable strategies to secure even the most fragmented device ecosystems.	10/22/25	9:00	9:30	William Scandrett,Samuel Maeder,Joe Vanhoorik,Christopher Warren
TS 2A - Hack My Brain: How Threat Actors Exploit Human Nature	Cybercriminals aren't just targeting your systems they're targeting your mind. In this eye-opening session, Proofpoint shares the latest threat research and uncovers the psychological tactics attackers use to manipulate, deceive, and exploit human behavior. While threat actors take advantage of technology that's advancing at the speed of light, social engineering remains a major factor in their attacks. Join us as we explore real-world attack scenarios, dissect the cognitive biases and emotional triggers that make users vulnerable, and reveal how threat actors evolve their methods to stay ahead.	10/22/25	9:00	9:50	Molly McLain Sterling,Katlyn Ostrom
TS 2B - Â "Man the (Fire)walls!" Strategies, pitfalls, and lessons learned in expanding our exposure management practice	Beazley Security Labs was presented with a unique opportunity when tasked with expanding our exposure management product. The process of adding timely and targeted vulnerability advisories, client network inventory discovery, and sensible but concise risk assessment to our existing attack surface management product has come with all kinds of unexpected struggles. This talk will discuss the various strategies and pitfalls we encountered, and some of the lessons learned along the way.	10/22/25	9:00	9:50	Bobby Venal

Session	Description	Date	Start	End	Speakers
AM Cyber 101 - Session 2: Cybersecurity Appetizers: Bite-Sized Challenges to Prepare for a Crisis	Engage in quick, real-world cyber scenarios to strengthen crisis response readiness. This session promotes critical thinking, communication, and collaboration through challenges focused on data breaches, ransomware, and incident planning equipping participants with practical strategies to improve preparedness, resilience, and stakeholder trust during cyber incidents.	10/22/25	9:30	10:45	Jennifer Lotze,Christopher Gabbard
PS - Local Threat Landscape: Modernizing Security with NGSIEM	Join CrowdStrike experts for an essential briefing on the evolving threat landscape facing State and Local Government organizations. Learn how sophisticated adversaries are targeting public sector entities and discover how Next-Generation SIEM capabilities can transform your security operations. This session includes a live demonstration of CrowdStrike's innovative NGSIEM solution, showcasing real-time threat detection, automated response capabilities, and operational efficiency gains.	10/22/25	9:30	10:00	Evan Emskamp,Rob Reynolds,Matt Singleton
MT - Addressing Risk in Medical Technologies	Vetting and managing the multitude of IoMT that populate unique span-of-care environments is a big deal. From procurement to asset management, how do policymakers, manufacturers, administrators, and healthcare professionals all benefit from a common model? Medical technology has evolved in a sophisticated manner, and the industry is calling for considerations that promote patient safety, data privacy, and operational integrity. How do security practitioners balance forward thinking strategies while simultaneously addressing legacy technical debt?	10/22/25	10:00	10:30	Michael DePorter
PS - CJIS & CJDN Compliance: Adapting to Policy and Technology Changes	Minnesota agencies that access FBI and BCA criminal justice information must comply with the FBI CJIS Security Policy and the BCA CJDN Policy. Recent policy updates and rapid shifts in technology -- such as cloud adoption and AI have created new compliance challenges. This session offers an overview of the two policies, highlights recent changes, and explores practical strategies for implementation. Attendees will gain insight into overcoming common obstacles and aligning their agency's practices with current security and regulatory expectations.	10/22/25	10:00	10:50	Tom Miller,Jodie Monette
TS 3A - The New Privileged User: Agentic AI and Machine Identity Risks	As Agentic AI systems gain autonomy in enterprise environments, they introduce new identity and access risks. This session explores how to secure AI agents from both the builder and buyer perspectives, covering machine identity governance, least-privilege enforcement, and real-world strategies to manage and mitigate AI-driven identity threats.	10/22/25	10:00	10:50	Shurouq Hijazi
TS 3B - The New Attack Surface: Protecting AI Systems from Exploitation	Accelerating AI adoption brings both opportunity and risk. Explore how a platform approach to security empowers organizations to secure their AI environments with confidence.	10/22/25	10:00	10:50	Andy Brogan

MT - Large Language Models in Healthcare: Balancing Innovation, Privacy, and Security Risks	Large Language Models (LLMs) have become essential tools for improving clinical workflows, from medical record-keeping to providing decision support. However, in 2025, they present new challenges, such as ensuring the security and privacy of patient data, preventing model manipulation, and dealing with the potential for AI-generated misinformation. These risks require careful planning and governance to ensure that the implementation of LLMs does not compromise patient safety or data privacy.	10/22/25	10:30	11:00	Vitaly Herasevich
AM Cyber 101 - Session 3: Incident Response Planning: Templates, Best Practices & Key Considerations	This interactive workshop guides participants in creating effective incident response plans using state templates and CISA playbooks. Attendees will learn to define roles, assess readiness, ensure continuity, and align with emergency frameworks gaining practical tools to strengthen cyber response and organizational resilience.	10/22/25	11:00	12:00	Jennifer Lotze,Christopher Gabbard
Super Glue Strength and Special Powers: The Magic of a Multi-Government Defense Strategy	Escalating cyber threats, shrinking budgets, and rising expectations for secure digital services make isolated defense a losing strategy. This conversation explores the urgent need for governments at all levels state, local, tribal, territorial, and educational to come together through shared cybersecurity resources, infrastructure, and intelligence. From Joint Cyber Security Operations Centers (JCSOCs) to cross-agency incident response teams and multi-jurisdictional data-sharing agreements, this presentation will highlight the strategic value, cost-efficiency, and resilience that comes with collaboration. Attendees will learn how shared governance models can bridge resource gaps, reduce duplication, and create a united front against emerging threats while building smarter, safer, and more sustainable public sector ecosystems.	10/22/25	11:00	11:45	Shawn Riley
Confident Leadership: Be the Calm in the Eye of the Cyberstorm	Anomaly, breach, and C-level crisis are the top of the alphabet when cybersecurity goes upside down. The SEV-1 pings and a batphone rings, so you step into the phone booth and fasten that cape of courage! Even with a well-practiced playbook and process, layered stress comes from bosses and board executives, media inquiries and arguing attorneys. You've got technical skills and a top team but not core confidence. Shayla and Tina will share the TTPs that translate to critical incident command capabilities. You'll lead for the long haul when that career-defining bell rings, with strength that inspires trust and a voice that keeps the calm.	10/22/25	11:45	12:55	Shayla Treadwell,Tina Meeker

C101W Lunch & Learn: Level Up Your Cyber Game With K-12 Pathways & Resources	Level Up Your Cyber Game: K-12 Pathways & Resources! Description: Ready to turn your students into cyber superheroes? The need for cyber education is urgent so tackle the talent gap with a blast! See curriculum options like TestOut, with hands-on simulations for certifications including Security+ and Ethical Hacker Pro; Teach Cyber, focused on foundational concepts and big ideas like ethics and risk management, and Project Lead The Way (PLTW) cybersecurity that emphasizes problem-based learning and real-world scenarios. Discover thrilling career paths, epic certifications, and how to build a rock-solid K-12 cybersecurity roadmap that preps students for high-demand, high-impact futures.	10/22/25	12:00	12:50	Tabitha Senty,Jennifer Lotze,Kate Granlund
PS - The Impact of Synthetic Intelligence on Government and SLED	Explore the power of synthetic intelligence in the public sector. This session helps leaders navigate AI confidently with real-world insights for an immediate impact. Learn to manage potential AI risks and implement it safely, regardless of your organization's size or budget. We'll introduce the 'Organizational Mind' model for ambient intelligence and workforce enhancement. This session is about building a smarter public sector, equipping you with strategies to develop AI skills and understand the importance of clear goals.	10/22/25	12:30	13:30	Scott Klososky
MT - Global Compliance Journey: Pitfalls and Successes	Navigating global compliance requirements is a journey that requires planning. Solventum shares their efforts to map out and meet a variety of needs, plus a few pitfalls. Hear how they optimized controls and frameworks for success while simultaneously aligning the needs of their customers and minimizing negative operational impacts.	10/22/25	12:45	13:15	Amy Brown
PM Cyber 101 - Session 1: Building Blocks: Developing a Comprehensive Cybersecurity Program	Learn how to build a strong cybersecurity program through standards, governance, and strategic alignment. This session covers risk mitigation, accountability frameworks, and oversight processes to help organizations enhance resilience, protect assets, and align cybersecurity efforts with business goals in today's evolving threat landscape.	10/22/25	13:00	14:15	Catherine Scott,Ron Olsen
TS 4A - Rapid AI Prototyping	The age-old complaint in security engineering is that "big ideas die in the backlog." Lengthy discovery, design, and coding cycles smother urgency especially when threats are evolving faster than releases. Enter AI-first development, where language models collapse friction at every step of the SDLC and let small teams translate concept into running code in hours, not quarters. This talk tells the inside story of how we built a working AI Assisted Alert Agent & an Insider Threat & Fraud Detection module in a couple afternoons then generalized the method into a repeatable playbook any security team can copy.	10/22/25	13:00	13:50	Beth Glowacki

TS 4B - Don't Fall Victim to the Third Party Sucker Punch	Third-party breaches account for 63% of security incidents, often striking as an unexpected sucker punch. This session exposes how hidden vulnerabilities across vendors and even their vendors create a sucker punch effect that can catch organizations off guard, leading to operational disruption, regulatory consequences, financial loss, and reputational damage. We'll highlight common failures and share practical strategies that help CISOs build resilience and stay ahead of the next hit.	10/22/25	13:00	13:50	Michael Smilanich
MT - Blue Team Budo: Developing Your Cyber Defense Skills Like a Martial Artist	This session is a journey that aligns martial arts lessons learned with InfoSec career experience, incorporating principles that include getting good at falling and shape learning with growth and leadership from cybersecurity. First, Fundamentals: Like a karateka mastering basics, build core capabilities to include scripting (Bash, PowerShell, Python), and gather governance, risk, and response knowledge while embracing mistakes as learning opportunities. Second, Skill Refinement: Apply knowledge under pressure through hands-on labs, incident response simulations, and tactical teamwork tests. Third, Leadership: Transition from execution excellence to mentorship, project management, and strategic thinking. Leave ready to build your own InfoSec dojo that evolves and endures.	10/22/25	13:15	13:45	Abraham Judisch
PS - LEO-Led Crime Prevention: Social Media Safety Outreach	Cybercrime continues and people pay, with 2025 losses projected at 10.5 trillion. 2022 FBI stats had 800,944 complaints and 422 million victims. Bad actors use the internet, social media, and human behavior to make off with millions. Good news: law enforcement is leveraging social media awareness and outreach to prevent losses. This session covers high-value content: privacy and security settings, telltale signs of social engineering, scam stories, with the identity theft, doxxing and AI deepfake details that keep communities safe.	10/22/25	13:30	14:10	Jay Haapala
MT - What is a Red Team Anyway?	Today, red team operations are a hallmark for any mature cybersecurity program, but the related value hinges on timing and organizational readiness. Drawing from real-world assessments, this session demystifies red teaming and explores the strategic boost that results when these efforts are aligned with business priorities. Attendees leave with a red team success framework that outlines organizational prerequisites, core red team functions and tactical timing requirements, plus best practices on translating assessment findings into meaningful risk reduction outcomes.	10/22/25	14:15	14:45	David Dobrotka
PM Cyber 101 - Session 2: Cybersecurity Appetizers: Bite-Sized Challenges to Prepare for a Crisis	Engage in quick, real-world cyber scenarios to strengthen crisis response readiness. This session promotes critical thinking, communication, and collaboration through challenges focused on data breaches, ransomware, and incident planning equipping participants with practical strategies to improve preparedness, resilience, and stakeholder trust during cyber incidents.	10/22/25	14:30	15:45	Jennifer Lotze,Christopher Gabbard

PS - Behind the Screen: Cybercrime's Psychological Impact on Today's Youth	Cybercrime grows more sophisticated and the emotional and psychological toll to young people is a critical public safety and health concern. This session will explore how cyberbullying, sextortion, identity theft, and exposure to other harmful content affects our kids' mental health, self-esteem, and behavior. Learn the warning signs, how to report concerns, and how to collaborate in ways that support kids, parents, and communities with safer digital environments.	10/22/25	14:30 15:45	Tracy Habisch-Ahlin
MT - Healthcare Network Segmentation for a Safer Tomorrow	This technical talk addresses the nuts and bolts of network security and brings tactical clarity to two big challenges. First, how to address sprawling hospital networks without creating chaos, and second, how to build a unified framework across a global organization. You'll leave with core concepts and plug-and-play content to share with your team and drop in playbooks.	10/22/25	14:45 15:15	Timothy Walsh
TS 5A - Thinking Like a Hacker in the Age of AI	Coming soon…The advent of robust AI is a genuine inflection point for our society. The impact is like the internet squared except the pace of adoption is much higher. We don't have decades to figure this out. We need to understand AI, what's here and what's coming, at a deep level. "Thinking Like a Hacker in the Age of AI" is not about how AI works. The focus is on the approaches we need to adopt to work with AIs with a fuller understanding of the symbiotic relationship between human and machine intelligence. It's about thinking differently. It's about expanding our consciousness. It's about thinking like hackers.	10/22/25	15:00 15:50	Richard Thieme
TS 5B - Securing AI Agents and MCP Servers for the Enterprise	The rise of Shadow AI has introduced a new wave of opportunity and risk within enterprises. Without robust authorization mechanisms for AI agents and MCP servers, organizations face a trade-off: enable innovation at the expense of security, or enforce controls that stifle agility. This session explores the emerging field of Agentic Identity, touching on how to secure access to business resources for your agents and sharing best practices for secure and scalable MCP deployments.	10/22/25	15:00 15:50	Rohit Ganguly
MT - Innovating Safely in a World of Embedded Devices	The closing panel, Smart Security: Protecting Embedded Medical Devices talks to challenge of securing devices that are often invisible yet mission critical. Expect discussion on lightweight encryption, secure boot, and lifecycle resilience tools that form the future-proof foundation of trustworthy care.	10/22/25	15:15 15:55	Phil Englert,Odutola 'Tola' Amusan,Shayana Vasichek,Kyle Erickson,John Kelcher
PS - Beyond the Badge: Supporting Cybercrime Victims and Sustaining Case Momentum	Digital crimes come with negative impacts that linger beyond the initial incident. Identity theft, nonstop ransomware calls, and romance scams create financial devastation, familial distrust, embarrassment, and other psychological damage. Today's law enforcement response adds victim support on top of investigation efforts, with best practices that include regular, transparent updates to maintain case visibility. From intake to resolution, cybercrime priorities are reinforcing public confidence.	10/22/25	15:45 17:00	Marit Peterson

PM Cyber 101 - Session 3: Incident Response Planning: Templates, Best Practices & Key Considerations	This interactive workshop guides participants in creating effective incident response plans using state templates and CISA playbooks. Attendees will learn to define roles, assess readiness, ensure continuity, and align with emergency frameworks gaining practical tools to strengthen cyber response and organizational resilience.	10/22/25	16:00	17:00	Jennifer Lotze,Christopher Gabbard
Winning While Fearlessly Forward	The pace of cyber change is relentless, and the work required to secure systems and protect people can be overwhelming. Some workers are fighting on against the storm, others are fleeing the industry, and a few have just stopped still, having succumbed to the changestorm's mind-numbing freeze. Learn from 40 years' experience at the intersection of IT and security to go Fearlessly Forward and embrace new technologies. We'll break down a logical troubleshooting process that uses generative AI as a first step - to identify and apply existing, effective solutions that remain relevant. Having narrowed the scope, step two lets us focus on the unique security challenges that need our attention. Wrap up the 15th Annual Summit with a practical and tactical approach to managing new technologies, securely.	10/22/25	16:00	16:30	Tim Crothers
Fearlessly Forward and Beyond: CSS15 Finale	We're ready to move Fearlessly Forward - enjoy a recap as Shawn and Shayla wrap up the 15th Annual Cyber Security Summit.	10/22/25	16:30	16:45	Shawn Riley,Shayla Treadwell
CXO Dinner: War Stories and Future Wins	Small tables make for the honest and open discourse that matters. SentinelOne will facilitate a discussion that weaves executive SOC experiences with today's improved options, including the AI, ML and Automation Curated Networking needed for the future.	10/22/25	17:15	19:00	Dave Gold