LEVEL ZER0

OT CYBER SECURITY CONFERENCE

Georgia Tech Exhibition Hall • 460 Fourth St. N.W., Atlanta, GA 30332

April 19 – 23, 2026

**Agenda is subject to change. Please check back regularly.*

CONFERENCE OVERVIEW

Level Zero 2026 • April 19–23 • Georgia Tech, Atlanta, GA

DAY 0

Sunday, April 19

Pre-Conference Training & Early Arrivals

In-Person Training
CambiOS Academy, INL, ThreatGen - OT/ICS security courses — multiple tracks

Mini-Conference
Georgia Tech students & faculty — hosted by Derek Harp

Evening Social
Conference registrants are invited to join a casual night of Cybersecurity & Hacker themed board games, card games, and a movie. Early check-in.

DAY 1

Monday, April 20

Main Conference — Opening Day

Main Stage
Keynotes, panels & fireside chats — opening ceremonies

Food & Beverage
Light breakfast, gourmet coffee & snacks, light sit-down lunch

Vendor Activity
TEDx-style talks during Lunch break

Evening Party
Cocktail hour, full dinner & activites with open bar

DAY 2

Tuesday, April 21

Main Conference — Full Day

Break-Out Rooms
Solo presentations, panels, fireside chats & workshops

Food & Beverage
Full breakfast, gourmet coffee & snacks, full sit-down lunch

Vendor Activity
Vendor Speed Dating — connect with sponsors during Lunch. Interact with Vendors at the Expo and win game points.

Evening
Enjoy your night networking with new friends in and around Atlanta

DAY 3

Wednesday, April 22

Main Conference — Closing Day

Break-Out Rooms
Solo presentations, panels, fireside chats & workshops

Food & Beverage
Full breakfast, gourmet coffee & snacks, full sit-down lunch

Vendor Activity
TEDx-style talks during Lunch break. Interact with Vendors at the Expo and win game points.

Closing Ceremony
Final closing and award ceremony

DAY 4

Thursday, April 23

Post-Conference Working Sessions

CIE Working Group
CIE Design Patterns Working Group — open to all, free, 4-hour session

FIRST FLOOR

Exhibition Hall — Main Conference Space

SECOND FLOOR

Exhibition Hall — Breakout Rooms

PARKING

Georgia Tech Campus — Visitor Areas

Parking

Student Center Deck

This visitor deck entrance is located off of Ferst Drive. The hourly rate is $2 and must be paid by card as you exit.

Parking Lot/Deck: **Visitor Area 3**
Parking Number: **W02 Deck**

Student Center Lot

This visitor lot entrance is located off of Ferst Drive. The hourly rate is $2 and must be paid when you park by either the Park Mobile application (ParkMobile App Zone 8631), or by the pay station located by the Smithgall building entrance.

Parking Lot/Deck: **Visitor Area 2**

SCAN FOR GOOGLE MAPS

Georgia Tech Exhibition Hall — Atlanta, GA

Hartsfield-Jackson Atlanta Intl (ATL)
Approx. 20 min drive • Uber/Lyft available at all terminals

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
7:30 AM	8:30 AM	**Course Registration on Main Floor**				
9:00 AM	5:00 PM	[0-102] Incident Response for OT	**Bryan Singer**, *Principal Director & Global Leader for Incident Response Services, OT* at Accenture	Incident Response for OT (OTSE-0403) is an intensive 3-day course that moves beyond IT data protection and containment strategies to focus on physical safety and operational resilience. Traditional IT playbooks can be catastrophic in an Industrial Control System (ICS) environment. When physical safety and operational uptime are the priorities, "unplugging" is rarely an option. Participants will learn from three OT cybersecurity pioneers how to manage the full IR lifecycle—from preparation to post-incident hardening and lessons learned - while maintaining mission-critical systems under fire. This will be a condensed 1-day version of the full course	CENT	Expert
9:00 AM	5:00 PM	[0-103] OT Monitoring & SOC	**Marc Visser**, *OT/IT Security Officer* at Sec4OT	OT Monitoring and SOC (OTSE-0203) builds on foundational OT and network architecture knowledge by providing best practices for deploying detection and monitoring sensors, extracting meaningful logs and security events from OT hardware and software, and aggregating this security context into an OT DMZ staging area. These logs, events and alerts can be forwarded to an IT, OT, or IT-OT SOC, either managed in-house or by a MSSP service provider. Key topics for this 1-day course include OT SIEM deployment, custom protocol signatures, IT/OT correlation, and SOC staffing models. Participants will also learn to utilize SOAR, threat feeds, and threat hunting to shift operations from a reactive to a proactive security posture.	HPRK	Mid-Level
9:00 AM	5:00 PM	[0-104] OT Security Essentials	**Mike Holcomb**, *Fellow of Cybersecurity and ICS/OT Cybersecurity Global Lead* at Fluor	OT Security Essentials (OTSE-0301) teaches students how to defend ICS systems. Students learn to design secure ICS architectures, implement proper firewall placement, position IDS/IPS systems effectively, deploy secure remote access, and implement centralized log aggregation and network monitoring solutions. The course emphasizes practical, vendor-agnostic security techniques that can be immediately applied in production environments.ing to shift operations from a reactive to a proactive security posture. This will be a condensed 1-day version of the full course	KIRK	Mid-Level
9:00 AM	5:00 PM	[0-105] Cyber-Informed Engineering Training for Infrastructure Resilience	**Virginia "Ginger" Wright**, *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Labs, *Faculty* at CambiOS Academy **Jeremy Jones**, *Critical Infrastructure Security Analyst* at Idaho National Labs, *Faculty* at CambiOS Academy	This 6-hour training introduces participants to the foundational principles and practical applications of Cyber-Informed Engineering (CIE), a transformative framework developed to embed cybersecurity resilience directly into the design of critical infrastructure systems. Unlike traditional cybersecurity approaches that focus on digital perimeter defenses, CIE empowers engineers and technicians to design systems that can withstand and mitigate the process impacts of cyber sabotage and digital technology failure. Participants will explore how CIE integrates engineered controls, consequence-focused design, and planned resilience to protect essential functions and reduce adversary opportunities for degrading them. The session will cover the 12 core CIE principles, illustrated through real-world use cases in energy, water, and manufacturing sectors. Attendees will engage in interactive exercises to apply CIE concepts to operational technology environments. Participants will receive access to tools to speed and focus the application of CIE for specific functions and a database of engineering controls to incorporate in their own designs.	HLND	Everyone
9:00 AM	5:00 PM	[0-101] Assessing and Exploiting Control Systems and IoT	**Justin Searle**, *Director of ICS Security* at InGuardians		CBTN	

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
9:00 AM	5:00 PM	[0-107] Building AI Agent for ICS/OT Security	**Clint Bodungen**, *Founder, CEO, Chairman* at ThreatGen	AI agents are transforming how we approach critical infrastructure security, but most teams are still using basic chatbots, not even realizing the full potential of what AI agents can really do. In this hands-on workshop, you'll build real AI agents that can reason about ICS/OT and cybersecurity, remember context across engagements, coordinate multi-step workflows, and more. You'll learn to do it safely and securely, and you won't believe how easy it actually is. No prior AI engineering or programming experience required, just a laptop and curiosity. You'll leave with a working agent framework you can customize for your own environment.	L5P	Everyone
9:00 AM	2:30 PM	[0-108] Intro to OT Regulations, Standards & Guidelines	**Donovan Tindill**, *Director of OT Cybersecurity* at DeNexus	This course provides an introduction to regulations, standards, and guidance that applies to OT environments, as well as the application of maturity and security levels. -Differences between Regulations, -Standards, and Guidelines -Overview of OT-specific and OT-applicable resources -NIST CSF Introduction and Concepts (Core, Tiers, Profiles) -IEC 62443 Introduction and Concepts (Zones, Security Levels, Roles, Lifecycle, Certification) -C2M2 introduction -Multiple regulations, standards, and guidelines -Introduction to capability Maturity Level (ML) -Introduction to technical Security Level (SL) -Applying security and maturity level to your OT cybersecurity program	SWAB	Entry
9:00 AM	10:30 AM	[0-109] OT Awareness Bootcamp (Session 1 of 3)	**Jonathan Pollet**, *Founder/Executive Director* at Red Tiger Security	OT Security Awareness (OTSE-0102) provides a high-level introduction to cybersecurity risks and considerations in operational technology environments. Derived from the fundamentals course content, it focuses on building basic security awareness around OT systems, without delving into deep technical implementation details. The course covers common OT security threats, basic risk factors, and fundamental security principles applicable to industrial control systems (ICS) and other operational technology (OT) environments.	O4W	Entry
10:10 AM	10:30 AM	**BREAK**				
10:30:00	12:00 PM	[0-209] OT Awareness Bootcamp (Session 2 of 3)	**Jonathan Pollet**, *Founder/Executive Director* at Red Tiger Security	Introduction to OT/ICS Fundamentals (OTCS-0103) serves as an awareness-level overview of what Operational Technology is and its role in industrial environments. Consisting of select segments of the complete 8-hour OT/ICS OT Fundamentals course, this introduction provides essential knowledge for understanding OT systems without deep technical detail. The course covers basic industrial control system concepts, the difference between IT and OT environments, and fundamental terminology and components.	O4W	Entry
12:00 PM	1:00 PM	**LUNCH BREAK (on your own)**				
1:00 PM	2:30 PM	[0-309] OT Awareness Bootcamp (Session 3 of 3)	**Rob Garry**, *former Executive Chief Engineer and VP Product Security* at GE power gen	Product Security Awareness (OTRC-0101) provides product development teams, engineers, and management about cybersecurity considerations in industrial product design and manufacturing. The curriculum covers secure development practices for OT products, common vulnerabilities in industrial devices, regulatory requirements for product security, and the business impact of security flaws in deployed products.	O4W	Leadership, Entry
2:30 PM	5:00 PM	Vendor Expo Setup Begins	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex		MTWN	
2:30 PM	2:45 PM	**BREAK**				

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
3:00 PM	5:00 PM	[0-401] Mini-Conference - GT Students & Faculty -	Host: **Derek Harp**, *Founder & Chairman* at CS²AI / Level Zero Conference **Yosef Beck**, *VP of Cyber Security* at CRH	This two-hour invite-only session brings together Georgia Tech students who are actively pursuing careers in cybersecurity — not an intro course, but a focused dialogue with industry practitioners. Attendees will explore the real challenges shaping the OT/ICS security landscape, emerging threat vectors that will define the next decade, and the career pathways available to those ready to step into this critical field. Come prepared to engage.	MTWN	Entry
4:00 PM	8:00 PM	**Early Registration for Level Zero Conference**				
5:00 PM	6:30 PM	Informal Vendor Expo	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex	Earn Game Points! The Vendor Expo provides a dedicated space for you to explore the latest industry tools and solutions through interactive demonstrations and expert consultations. It is designed to be a one-stop shop where you can engage directly with multiple service providers to compare technologies and discover new ways to optimize your operations.	MTWN	
5:00 PM	9:00 PM	**Pizza, Beer & Cocktails**				
5:30 PM	10:00 PM	Evening Social	**Clint Bodungen**, *Founder, CEO, Chairman* at ThreatGen	Conference registrants are invited to join a casual night of Cybersecurity & Hacker themed board games, card games, and a movie. Early check-in.	MTWN	

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
7:45 AM	9:00 AM	**REGISTRATION + LIGHT BREAKFAST**				
7:45 AM	8:45 AM	[1-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	**Derrik Oates**, *Information System Security Officer* at Bureau of Engraving and Printing	UTSI will be facilitating a specialized Tabletop Exercise (TTX) utilizing ThreatGen technology and featuring a custom scenario. The TTX will run across three morning sessions, concluding with a final summary and awards presentation during the Level Zero closeout. This TTX can be used as part of the items needed for Type 3 or Type 4 ICS4ICS Credentials	HPRK	Everyone
8:45 AM	9:00 AM	**TRANSITION**				
9:00 AM	9:15 AM	[1-101] Introduction	**Derek Harp**, *Founder & Chairman* at CS²AI / Level Zero Conference	Opening remarks and welcome to Level Zero 2026	MTWN	Everyone
9:15 AM	9:30 AM	[1-111] Welcome	**Vivek Sakar**, *Dean, College of Computing* at Georgia Tech	Welcome and Introduction to the School of Cybersecurity and Privacy	MTWN	Everyone
9:30 AM	10:05 AM	[1-121] Keynote			MTWN	Everyone
10:05 AM	10:55 AM	[1-131] Key Perspectives in OT Security Panel	Host: **Derek Harp**, *Founder & Chairman* at CS²AI / Level Zero Conference **Preston Futrell**, *Partner, Cybersecurity Services / Global OT Security Offering Leader* at IBM Security **Brad Willet**, *OT Security Infrastructure Architect* at UPS **Yosef Beck**, *VP of Cyber Security* at CRH **Blake Gilson**, *Industrial Cybersecurity Manager* at ExxonMobil	This session explores the CS2AI-KPMG Control System Cybersecurity Annual Report, highlighting key trends from the last three years of survey data. Drawing on insights from over 500 global professionals, the presentation covers the most pressing challenges and priorities in OT security, while comparing these findings to recent public market analysis to identify where industry perspectives converge or diverge.	MTWN	Everyone, Leadership
10:55 AM	11:45 AM	[1-151] The Insurable Gap Panel: Why OT Security is the New Board Mandate	Host: **Shaun Six**, *President and CEO* at UTSI International Corporation **Joe Carroll**, *Chief Information Officer & Head of Cybersecurity* at CITGO Petroleum **Nick Jennings**, *Vice President and Philadelphia Market Leader, Cyber Solutions* at Aon **Scott Kannry**, *Chief Executive Officer* at Axio	Cybersecurity risk has evolved from merely an IT issue to a core strategic and operational challenge, especially due to the convergence of IT and vulnerable, legacy Operational Technology (OT) systems. Recent, high-impact attacks (Colonial Pipeline, MWAA, Volt Typhoon) on critical infrastructure demonstrate that disruptions are inevitable and lead to severe financial, operational, and reputational costs, risking national economic stability.	MTWN	Everyone, Leadership
11:45 AM	12:25 PM	[1-141] View from the Board Room: Cybersecurity, Artificial Intelligence, and Geopolitics	**Derek Harp**, *Chairman & Founder* at CS²AI / Level Zero Conference **John Tien**, *Board Member* at Union Pacific & SAIC, [former Deputy Secretary]	The Honorable John Tien, Deputy Secretary of the U.S. Department of Homeland Security, 2021-2023, will discuss how the topics of cybersecurity, artificial intelligence, and geopolitics are dominating discussions in Fortune 500 boardrooms.	MTWN	Everyone, Leadership
12:25 PM	12:35 PM	Recognition Ceremony	**Derek Harp**, *Chairman & Founder* at CS²AI / Level Zero Conference **John Tien**, *Board Member* at Union Pacific & SAIC, [former Deputy Secretary]	The Level Zero team is proud to recognize the many veterans and first responders in attendance at this year's conference.	MTWN	Senior
11:45 AM	12:15 PM	**LUNCH + TEDx speakers**				
1:25 PM	1:45 PM	[1-201] Continuous Risk Management In Flight	**Cody Scott**, *Senior Analyst* at Forrester, [former Chief Cyber Risk Officer at NASA]	Cody tackles the common shift from reactive risk assessments to a model of Continuous Risk Management. You will learn the blueprint for ditching "check-the-box" programs in favor of real-time risk intelligence that catches vulnerabilities before they become incidents. By the end of the session, you'll have the tools to transform security from a business blocker into a strategic advantage.	MTWN	Everyone

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
1:45 PM	2:10 PM	[1-211] Session TBD			MTWN	Everyone
2:10 PM	2:30 PM	[1-221] Session TBD			MTWN	Everyone
2:30 PM	2:40 PM	**BREAK**				
2:40 PM	3:30 PM	[1-301] PANEL TBD	**Blake Gilson**, *Industrial Cybersecurity Manager* at ExxonMobil		MTWN	Everyone
3:30 PM	3:55 PM	[1-311] Session TBD			MTWN	Everyone
3:55 PM	4:10 PM	[1-321] Closing Message	**Derek Harp**, *Co-Founder* at CambiOS Academy **Patrick Miller**, *CEO* at Ampyx Cyber	Closing remarks for Day 1 and recognizing long-term community contributors.	MTWN	Everyone
4:10 PM	5:20 PM	**Cocktail Hour and Beer ISAC**				
5:20 PM	10:00 PM	**Full Dinner w/ Open Bar & Planned Activities**				

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
7:30 AM	8:00 AM	**FULL BREAKFAST**				
8:00 AM	13:00:00	Vendor Expo: Earn Game Points!	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex	Earn Game Points! The Vendor Expo provides a dedicated space for you to explore the latest industry tools and solutions through interactive demonstrations and expert consultations. It is designed to be a one-stop shop where you can engage directly with multiple service providers to compare technologies and discover new ways to optimize your operations.	MTWN	
8:00 AM	10:00 AM	[2-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	**Derrik Oates**, *Information System Security Officer* at Bureau of Engraving and Printing	UTSI will be facilitating a specialized Tabletop Exercise (TTX) utilizing ThreatGen technology and featuring a custom scenario. The TTX will run across three morning sessions, concluding with a final summary and awards presentation during the Level Zero closeout. This TTX can be used as part of the items needed for Type 3 or Type 4 ICS4ICS Credentials	MTWN	Everyone
9:00 AM	9:50 AM	[2-101] Considering Cyber Conservative Operations	**Virginia "Ginger" Wright**, *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Labs	Cyber threats are driving the need for robust resilience strategies. This talk introduces the concept of Cyber Conservative Operations, a proactive approach to manage risk and maintain resilience in the face of imminent, but not yet occurring, cyber events. Leveraging Cyber-Informed Engineering (CIE), with the practice of conservative operations, this approach for planning and deploying protections and controls ahead of an incident ensures quick and efficient recovery from cyber threats.	CENT	Everyone
09:25:00	9:50 AM	[2-102] Beyond Technology: Building Cyber Resilience beyond the Security Team	**Dee Kimata**, *Cybersecurity Thought Leadership Director* at Schneider Electric	While cyber resilience is often framed as a technical problem, it is truly shaped by decisions made across operations, supply chains, and external partnerships. This session presents a practical framework for expanding cybersecurity influence beyond the technical domain by building trust and transparency across the entire business ecosystem. Attendees will learn how to translate complex cyber risks into actionable insights that align investment and accountability among IT, OT, and executive leadership. By the end of the presentation, you will have a clear blueprint for turning shared understanding into a measurable business advantage.	HPRK	Everyone
9:00 AM	11:00 AM	[2-109] Getting Started in ICS/OT Cybersecurity: (2 hrs)	**Jonathan Pollet**, *Founder/Executive Director* at Red Tiger Security	Getting Started in ICS/OT Cybersecurity: Protecting critical infrastructure becomes more important each day as the frequency of cyber attacks and the number of attackers continues to grow. State adversaries are no longer the only ones targeting these specialized environments. Today's attackers include ransomware groups, hacktivists, cyber mercenaries, and more. ICS/OT cyber security can seem complicated and even daunting at first, but it does not have to be. This workshop will help participants understand how to get started in ICS/OT cyber security and provide a path for getting up to speed quickly! Whether brand new to ICS/OT cyber security or a seasoned professional, this session will offer something for everyone.	HLND	Entry
9:50 AM	10:00 AM	**BREAK**				
10:00 AM	10:25 AM	[2-201] Session with Fortinet	**Speaker TBD**, *TBD* at Fortinet		CENT	Everyone
10:00 AM	10:25 AM	[2-202] OT Defense Workforce Roles and Training	**Daryl Haegley**, *Technical Director, DAF Cyber Resiliency Office for Control Systems (CROCS)* at U.S. Air Force & Space Force, Pentagon	NEW DoD Cyber Work Role "Control Systems Security Specialist." Responsible for device, equipment, and system-level cybersecurity configuration and day-to-day security operations of control systems, including security monitoring and maintenance along with stakeholder coordination to ensure the system and its interconnections are secure in support of mission operations. How many are needed in operational testing? How many needed to defend against OT cyber-attacks? Is training sufficient?	HPRK	Everyone

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
10:00:00	12:00:00	[2-203] Living off the Land, and Delivering Over the Air (2 hr Workshop)	**Marc Visser**, *OT/IT Security Officer* at Sec4OT **Bryan Singer**, *Principal Director, Global OT Incident Response Lead* at Accenture	Hacking factories with AI, leveraging AI to execute pentests followed by using Mesh to communicate offgrid (and no one can trace you) Hands-on Fun	KIRK	Mid-Level
9:00 AM	11:00 AM	[2-109] Getting Started in ICS/OT Cybersecurity: (2 hrs)	**Jonathan Pollet**, *Founder/Executive Director* at Red Tiger Security	Getting Started in ICS/OT Cybersecurity: Protecting critical infrastructure becomes more important each day as the frequency of cyber attacks and the number of attackers continues to grow. State adversaries are no longer the only ones targeting these specialized environments. Today's attackers include ransomware groups, hacktivists, cyber mercenaries, and more. ICS/OT cyber security can seem complicated and even daunting at first, but it does not have to be. This workshop will help participants understand how to get started in ICS/OT cyber security and provide a path for getting up to speed quickly! Whether brand new to ICS/OT cyber security or a seasoned professional, this session will offer something for everyone.	HLND	Entry
10:35 AM	11:00 AM	[2-301] Session with IBM Security	**Speaker TBD**, *TBD* at IBM Security		CENT	Everyone
10:35 AM	11:00 AM	[2-302] Session TBD			HPRK	
11:00 AM	11:10 AM	**BREAK**				
11:10:00	12:00:00	[2-203] Living off the Land, and Delivering Over the Air (2 hr Workshop)	**Marc Visser**, *OT/IT Security Officer* at Sec4OT **Bryan Singer**, *Director, Global OT Incident Response Lead* at Accenture	Hacking factories with AI, leveraging AI to execute pentests followed by using Mesh to communicate offgrid (and no one can trace you) Hands-on Fun	KIRK	Mid-Level
11:10 AM	12:00 PM	[2-401] Grid Time Travel Panel: Navigating Greenfield, Brownfield, and Legacy Technologies in the Modern Utility	Host: **Jacob Kitchel**, *Senior Manager* at Invenergy **Rob Garry**, *Retired Executive Chief Engineer, VP Product Cyber Security* at GE Energy **Cole Oursler**, *Director of Information Services* at Mountain View Electric Association **Carter Manucy**, *Senior Director, Cybersecurity* at National Rural Electric Cooperative Association (NRECA)	Utilities rarely start from scratch. New technologies must be integrated into environments that include decades-old infrastructure and evolving operational needs. This panel explores how utilities navigate greenfield builds, brownfield upgrades, and legacy systems while introducing modern capabilities. Panelists will share lessons learned and discuss what the future grid may realistically look like.	CENT	Everyone, Leadership
11:10 AM	12:00 PM	[2-402] OT Security Crossroads - Engineering x Hacking	**Vivek Ponnada**, *SVP, Growth & Strategy* at Frenos	OT Security is still a young discipline that's evolving. While everyone understands that OT is different from IT, the OT Security responsibilities are driven by or inherited from IT Security. Therefore the purpose-built products for OT Security try to meet IT Security's expectations while avoiding a conflict with operations or causing downtime. E.g., a vulnerability scan could disrupt operations so a 'hack' would be a passive monitoring solution that can also provide assets & vulnerabilities information. Or another 'hack' for letting OT protocols stay unencrypted is to put the communication behind a Secure gateway for remote access. Besides such hacks, several engineering driven approaches are gaining traction. E.g., focus on resilience and reducing consequence - from a regulatory path such as Europe's CRA, methodologies like cyber-informed-engineering, and the growth of standards (ISA/IEC 62443). So, which of these paths "Engineering" or "Hacking" will help us 'solve' OT Security? This presentation unpacks the nuances including timelines, budgets and practical risk considerations at the proverbial crossroads that OT Security is at.	HPRK	Everyone

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
11:10 AM	12:00 PM	[2-403] Cognitive Architectures for Critical Infrastructure: When Your AI Analyst Never Forgets	**Clint Bodungen**, *Founder, CEO, Chairman* at ThreatGen	This session addresses the critical loss of institutional memory in ICS/OT environments by introducing AI agents capable of persistent, multi-year knowledge retention. Using the "MindStone" three-tier memory architecture, we explore how cognitive systems can move beyond simple RAG or fine-tuning to maintain contextual reasoning across teams and sessions. A live demonstration will showcase an agent answering questions about past engagements without a fresh briefing, highlighting practical applications for compliance and threat monitoring. Attendees will leave with a framework for building AI that survives personnel turnover, ensuring the future of security isn't just smarter, but remembers.	HLND	Everyone
12:00 PM	1:25 PM	**LUNCH**				
12:15 PM	1:00 PM	Vendor Speed Dating	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex	This high-energy speed dating session allows you to connect with every event sponsor through a series of rapid, five-minute face-to-face meetings. Simply remain at your table while our sponsors rotate to you, providing a streamlined way to discover new solutions and professional opportunities. It is a time-efficient networking format designed to help you vet potential partners and build industry leads before the lunch hour ends. Earn Challenge Coin points!	MTWN	
1:25 PM	2:15 PM	[2-501] CISO Energy Panel	Host: **Chris Roche**, *CISO | Director - Energy/Critical Infrastructure Cybersecurity & Resilience* at CI-Discern **Alex Waitkus**, *Principal OT Cybersecurity Architect* at Southern Company **Jonathan Tubbs**, *Industrial Cyber Security Officer* at Siemens Energy **Dale Beauchamp**, *Sr Director Cyber Security Focused Operations* at AMTRAK	This panel brings together cybersecurity leadership from critical infrastructure and energy sectors to discuss the evolving relationship between corporate cyber teams and the broader business. Experts will explore strategies for effective cross-functional collaboration, focusing on how security can move beyond a siloed function to become a true partner in operational success.	CENT	Everyone, Leadership
1:25 PM	2:15 PM	[2-502] Meandering No More: Escaping the Firefighter Trap in OT Security (Talk + Working Session)	**Christian Harter**, *Director of OT Security and Engineering and the BISO for OT Security* at UPS	OT security succeeds when engineering, operations, and security share a destination—and a realistic path to get there. This interactive session helps attendees move from reactive work to a strategy that respects uptime, safety, and legacy constraints while still improving security outcomes.We'll begin with a rapid overview of why OT programs slip into firefighting (misaligned incentives, unclear decision rights, and "tool-first" approaches). Then we'll collaborate on building a practical, lightweight strategy using five pillars: governance/ownership, asset visibility, access control, data protection, and resiliency/recovery. Participants will leave with a one-page plan, a draft ownership model, and a prioritized 90-day action list—plus a roadmap outline that can be expanded into a formal program plan back at work. Designed for OT engineers and OT security leaders who want a strategy they can execute without disrupting operations.	HPRK	Leadership

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
1:25 PM	2:15 PM	[2-503] Putting the E in P.A.C.E.: When Satcom Is Not Enough	**Mark Bristow**, *Director* at Cyber Infrastructure Protection Innovation Center (CIPIC) at MITRE	What happens to your situational awareness when both the grid and your networks go down and stay down for weeks? MITRE's Critical Infrastructure Risk-Informed Decision Analysis Platform (CIRIDAP) is designed to fill the current gap: there is no national Common Operating Picture (COP) for critical infrastructure in prolonged "dark sky" conditions, when power and IP-based, cellular, satellite, and landline communications are largely unavailable. Traditional P.A.C.E. planning assumes some power and limited comms will return within days, and today's civilian COP tools (e.g., WebEOC) are not built to support shared, cross-jurisdictional visibility and decision-making when digital infrastructure is mostly offline. In 2025, MITRE designed and built a CIRIDAP prototype, including a graph database based on an all-hazards data model, a unified map-based dashboard, integrated long and short-range wireless links, and multiple field devices assembled from COTS components, with requirements shaped by state agencies, industry partners, and asset owners through interviews, a concept workshop, and a SIMEX. In a live demo in late 2025, CIRIDAP ran without grid power or public communications and still delivered near-real-time visualization of a simulated cascading critical infrastructure failure. This talk will cover how the system works, what we learned about improving ICS resilience and decision-making during extended outages, and options for scaling CIRIDAP into an operational capability for long-duration, large-scale disruptions.This session will include a live demonstration of the technology (which is not for sale but we are looking for testing partners/industry feedback).	KIRK	Everyone
2:15 PM	2:25 PM	**BREAK**				
2:25 PM	3:15 PM	[2-601] Assessing and Exploiting Control Systems in IoT	**Justin Searle**, *Director of ICS Security* at InGuardians		CENT	
2:25 PM	3:15 PM	[2-602] Trust, Transparency, and Treachery	**Marcus Sachs**, *Senior VP and Chief Engineer* at Center for Internet Security, Inc	A Cold War handshake that compromised global cryptography - and a modern reminder that in connected systems, unverified trust is the most dangerous vulnerability of all.Through the lens of the Friedman-Hagelin cryptographic agreement, this talk explores how a secret handshake led to decades of compromised encryption, and what Cold War deception can teach today's OT and ICS engineers about trust, transparency, and supply chain integrity in connected systems.Program DescriptionFollowing the popular session "Encryption, Engineering, and Errors," this new talk examines how a quiet handshake between American cryptographer William Friedman and Swedish engineer Boris Hagelin set the stage for one of the longest-running intelligence operations in history. Their "gentleman's agreement" secretly weakened commercial encryption for decades. This decision offers striking parallels to today's industrial cybersecurity challenges. Through a historical lens, attendees will explore how hidden dependencies, opaque supply chains, and unverified trust relationships can undermine modern OT and ICS systems, and how traditional engineering principles can help us design transparency, verification, and ethical integrity into connected infrastructure.	HPRK	Everyone
2:25 PM	3:15 PM	[2-603] OT Asset Discovery at Massive Scale	**Brad Willet**, *OT Security Infrastructure Architect* at UPS	From package delivery to healthcare to logistics, UPS operates thousands of facilities worldwide. Over 118 years as a company and almost half a century of utilizing ICS systems, UPS continues to grow and innovate. With that growth comes an increasing need for OT security and a solid asset inventory. How do you safely discover OT assets at this scale without disrupting operations? This session covers what worked for us, what didn't, and the lessons learned along the way.	KIRK	Entry

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
3:15 PM	3:25 PM	**BREAK**				
3:25 PM	4:15 PM	[2-701] Behind the Curtain: A Practical Guide to NERC Audit Success	**Chase Snuffer**, *CIO* at Rayburn Electric Cooperative	In this session, we'll pull back the curtain on our 2025 audit. We'll walk through the specific strategies we used to organize our initial evidence submittals to minimize downstream friction and how we managed the weeks of RFI's (Request for Information) leading up to the off-site/on-site. Passing a NERC audit is rarely about the audit itself, it's about the 36 months that precede them. This is our story.	CENT	Mid-Level
3:25 PM	4:15 PM	[2-702] OT Risk Quantification for BESS	**Katherine Hutton**, *Product Manager for Cybersecurity* at Fluence	As Battery Energy Storage Systems (BESS) take on mission-critical grid roles, organizations need better ways to understand and communicate OT cyber risk. This session explores how Cyber-Informed Engineering (CIE) can be used to structure credible cyber scenarios, guide mitigations, and support early-stage risk quantifications. Attendees will gain practical frameworks for translating cyber risk into engineering, operational, and leadership-relevant decisions.	HPRK	Entry
3:25 PM	4:15 PM	[2-703] People, Process and Pragmatic OT Security	**David Ong**, *CEO* at Attila Cybertech	From the lens of a control systems professional grounded in functional safety, this presentation explores how cybersecurity in Operational Technology (OT) must remain pragmatic, not prescriptive. True resilience arises when people, process, and technology are integrated around operational realities—where safety and reliability cannot be compromised. The session examines practical lessons from industrial environments where IT-style controls disrupted production, and contrasts them with workable approaches such as passive monitoring, process behavioural understanding, and safety-aligned governance. It advocates a unified mindset where cybersecurity complements—not conflicts with—functional safety, ensuring secure, reliable, and sustainable operations in an increasingly connected industrial world. Practical examples of pitfalls will also be shared.	KIRK	Everyone
4:15 PM	4:25 PM	**BREAK**				
4:25 PM	5:15 PM	[2-801] Session TBD			CENT	
4:25 PM	5:15 PM	[2-802] Session with Tyrex	**Speaker TBD**, *TBD* at Tyrex		HPRK	Everyone
4:25 PM	5:15 PM	[2-803] Session TBD			KIRK	
4:15 PM	6:30 PM	Vendor Expo: Earn Game Points!	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex	Earn Game Points! The Vendor Expo provides a dedicated space for you to explore the latest industry tools and solutions through interactive demonstrations and expert consultations. It is designed to be a one-stop shop where you can engage directly with multiple service providers to compare technologies and discover new ways to optimize your operations.	MTWN	
6:30 PM		Close out for evening				

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
7:30 AM	7:45 AM	**FULL BREAKFAST**				
7:45 AM	8:45 AM	[3-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	**Derrik Oates**, *Information System Security Officer* at Bureau of Engraving and Printing	UTSI will be facilitating a specialized Tabletop Exercise (TTX) utilizing ThreatGen technology and featuring a custom scenario. The TTX will run across three morning sessions, concluding with a final summary and awards presentation during the Level Zero closeout. This TTX can be used as part of the items needed for Type 3 or Type 4 ICS4ICS Credentials	MTWN	Everyone
8:00 AM	1:30 PM	Vendor Expo: Earn Game Points!	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex	Earn Game Points! The Vendor Expo provides a dedicated space for you to explore the latest industry tools and solutions through interactive demonstrations and expert consultations. It is designed to be a one-stop shop where you can engage directly with multiple service providers to compare technologies and discover new ways to optimize your operations.	MTWN	
8:45 AM	9:00 AM	**BREAK**				
9:00 AM	9:50 AM	[3-101] Applying Financial Quantification of Risk in ICS/OT Cybersecurity Decision-Making	**Donovan Tindill**, *Director of OT Cybersecurity* at DeNexus	An introduction to the various ICS/OT standards, regulations, and guidelines relevant to owners, consultants, etc. across various verticals.	CENT	Entry
9:00 AM	9:50 AM	[3-102] Beyond the Fence Line: Securing the OT/Consumer Interface in the Age of DERs	**Brian Foster**, *Grid Security - Enterprise Sr Advisor* at Southern California Edison	Your OT perimeter is gone. It wasn't breached by hackers; it was dismantled by EV chargers and smart inverters. As we connect critical infrastructure to consumer-grade IoT, the attack surface is expanding faster than we can patch. This session offers a survival guide for the decentralized grid. We'll ditch the buzzwords to provide practical architectures for isolating "hostile" DERs, securing 3rd-party aggregators, and preventing load-shedding attacks. Secure the edge before it breaks you.	HPRK	Mid-Level
9:00 AM	9:50 AM	[3-103] Oil & Gas Fireside Chat	**Bemi (Shola) Anjous**, *Head of Global InfoSec/OT* at Noble Corporation **Jeevan Sakti**, *Global ICS Security Engineering Supervisor* at ExxonMobil	Participate in a high-level discussion on the strategic challenges facing the modern energy landscape. Together, they will share personal insights on navigating market volatility, driving operational efficiency, and the long-term future of traditional energy in an increasingly digital world.	KIRK	Everyone
9:50 AM	10:00 AM	**BREAK**				
10:00 AM	10:25 AM	[3-201] Securing a UNS Workshop	**Jeff Smith**, *Chief Technology Officer* at Dynics	This will be a working session where the participants suggest ideas for OT Cybersecurity concerns related to Unified Namespace (UNS) and then work through solving those. Depending on the time allotted, we will start with the top 5, and go from there.	CENT	Mid-Level
10:00 AM	10:25 AM	[3-202]			HPRK	Everyone
10:00 AM	10:25 AM	[3-203] Cyber Resilience Quantification Workshop	**Eric Cardwell**, *Vice President of Professional Services & Cyber Risk Engineering* at Axio **Shawn Bilak**, *Founder & Lead Assessor* at Bilak Security Solutions, [former Risk & Compliance Analyst Specialist at Southern Company]	An organization's resilience hinges on its financial capacity to endure challenges. This workshop will teach participants to model cyber risk in financial terms through hands-on exercises. Bring your laptop; each participant will receive a SaaS account for exercises and report development. A complimentary test-drive subscription to the software will be available for post-conference use. Participants will model and report on at least one risk for their or a fictitious organization.	KIRK	Mid-Level
10:25 AM	10:35 AM	**BREAK**				

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
10:35 AM	11:00 AM	[3-301] Journey to OT Visibility	**Alex Waitkus**, *Principal OT Cybersecurity Architect* at Southern Company	OT environments face escalating cyber threats that outpace traditional defenses. This presentation outlines how enhanced OT visibility—through network monitoring, behavioral analytics, and threat-informed approaches—strengthens detection, resilience, and compliance, forming the foundation of modern critical-infrastructure cybersecurity.	CENT	Mid-Level
10:35 AM	11:00 AM	[3-302] Session with Sygnia	**Kyle Alexander**, *Director of Cyber Security Services* at Sygnia **Tamir Margalit**, *Director of OT Security* at Sygnia		HPRK	Everyone
10:35 AM	11:00 AM	[3-303] Session TBD			KIRK	
11:00 AM	11:10 AM	**BREAK**				
11:10 AM	12:00 PM	[3-401] OT Cyber Entrepreneurs Panel	**Derek Harp**, *Founder & Chairman* at CS²AI / Level Zero Conference **Christophe**, *Co-Founder* at CambiOS Academy		CENT	Everyone
11:10 AM	11:35 AM	[3-402] Session with OPSWAT	**Speaker TBD**, *TBD* at OPSWAT		HPRK	Everyone
11:10 AM	12:00 PM	[3-403] Session TBD	**Saman Zonouz**, *Associate Professor, Schools of Cybersecurity and Privacy (SCP) & Electrical and Computer Engineering (ECE)* at Georgia Tech		KIRK	Everyone
11:35 AM	12:00 PM	[3-412] Session with UTSI International	**Speaker TBD**, *TBD* at UTSI International		HPRK	Everyone
12:00 PM	1:30 PM	**LUNCH + TEDx speakers**				
1:30 PM	4:30 PM	Vendor Expo Breakdown	UTSI International, Fortinet, OPSWAT, CambiOS Academy, IBM, Sygnia, Foxguard, KASM, Dynics, Netwrix, Tyrex		MTWN	
1:30 PM	2:20 PM	[3-501] Lessons Learned: Incident Response Exercise using FEMA's NIMS Incident Command System	**Derrik Oates**, *Information System Security Officer* at Bureau of Engraving and Printing	This interactive session brings together facilitators from the morning's three concurrent Incident Response Tabletop Exercises to share key findings, themes, and lessons learned. Drawing on participant responses and real-time observations from each TTX track, the panel will highlight common gaps, surprising outcomes, and actionable takeaways that attendees can bring back to their organizations. Audience participation is encouraged — come ready to compare notes.	MTWN	Everyone
2:20 PM	2:25 PM	**TRANSITION**				
2:25 PM	3:00 PM	[3-601] FINAL CLOSING CEREMONY	**Derek Harp**, *Founder & Chairman* at CS²AI / Level Zero Conference	Acknowledgements, awards, and appreciation for our attendees, speakers, sponsors, vendors and staff for making the 2026 Level Zero conference a success for the OT Cybersecurity community.	MTWN	Everyone

START	END	SESSION / EVENT	SPEAKER(S)	COURSE ABSTRACT	ROOM	TRACK
8:00 AM	12:00 PM	[4-101] CIE Design Patterns Working Group	**Virginia "Ginger" Wright**, *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Labs	This working group meeting will focus on reviewing and enhancing guidance for creating Cyber-Informed Engineering (CIE) design patterns that integrate engineered controls and the larger body of CIE principles into engineered architectures and technologies within oil and natural gas, advanced nuclear, power delivery, and other critical infrastructure systems. The effort aims to define criteria, decisions, and constraints that guide engineering design to ensure safety, reliability, and performance while under cyberattack conditions. The approach will be validated through testing and analysis and mapped with the Engineering Controls Database recently released by the Idaho National Laboratory's CIE program (GitHub - idaholab/CIE_EC_Database: Cyber-Informed Engineering addresses how cyberattacks on engineered systems threaten physical safety and reliability beyond data loss. This database provides guidance on defining and applying engineered controls, explaining their distinction from information security measures and their integration into system design.). Building on the database of over 62,000 examples of engineered controls across national critical sectors, this initiative seeks to identify recurring patterns that help organizations reduce digital risk. As stated, while engineered controls represent one of twelve CIE principles, incorporating insights from all principles will enable the creation of this comprehensive catalog of design patterns—a powerful tool for national resilience conversations. This workshop invites participants to engage in this Thursday discussion and review the current efforts toward defining this catalog. Key activities include: Reviewing existing design patterns and technologies across targeted energy sectors. Creating any new design patterns that embed engineered controls into system architectures to enforce safety and operational requirements despite digital risks. Linking guidance to opportunities identified in the Engineering Controls Database.		Everyone