LEVEL ZERO

Zero Day Trainings

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

	Start time	End time	Event Title	Speaker(s)	Location	Abstract	Track
April 19	9:00AM	5:00PM	[0-102] Incident Response for OT	**Bryan Singer**, *Principal Director, Global OT Incident Response Lead* at Accenture, *Founding Faculty* at CambiOS Academy	Centennial	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	Expert
	9:00AM	5:00PM	[0-103] OT Monitoring & SOC	**Marc Visser**, *OT/IT Security Officer at Sec4OT, Founding Faculty* at CambiOS Academy **Vincent Seruch**, *Directeur associé at* Adamante cyber, *Founding Faculty* at CambiOS Academy	Home Park	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.	Mid-level
	9:00AM	5:00PM	[0-104] OT Security Essentials	**Mike Holcomb**, *Founding Faculty* at CambiOS Academy	Kirkwood	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	Mid-level
	9:00AM	5:00PM	[0-105] Cyber-Informed Engineering Training for Infrastructure Resilience	**Virginia "Ginger" Wright**, *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Laboratory **Jeremy Jones**, *Critical Infrastructure Security Analyst* at Idaho National Laboratory	Highlands	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.	Everyone
	9:00AM	5:00PM	[0-101] Assessing and Exploiting Control Protocols	**Justin Searle**, *Director of ICS Security* at InGuardians	Cabbagetown	Industrial control systems rely on a diverse ecosystem of communication protocols — many designed decades ago with reliability in mind, not security. This intensive 8-hour course gives practitioners the hands-on skills to identify, capture, decode, and ultimately exploit the protocols running across your OT environment. Beginning with the physical layer, participants work through serial communication standards including RS-232, TIA-422, and TIA-485, learning to capture and manually decode traffic before progressing to software-based tools. From there, the course moves into fieldbus protocol families and TCP/IP-based ICS protocols, using Wireshark, Zeek, and GrassMarlin for endpoint analysis, flow inspection, and deep dives into Modbus TCP. A structured overview of ProfiNet, EtherNet/IP, CIP, OPC, DNP3, IEC 104, IEC 61850, and ICCP rounds out the known-protocol landscape. Where the course distinguishes itself is in unknown protocol analysis — participants apply entropy analysis and behavioral heuristics to identify and characterize protocols without prior knowledge. The course then pivots to enumeration, where students repurpose engineering tools and write Python scripts to interact directly with PLCs using Modbus RTU and ctmodbus. The course concludes with protocol fuzzing and exploitation using boofuzz, with deliberate attention to the risks of fuzzing embedded devices in live environments. Participants leave with a repeatable methodology, practical toolchain experience, and a clear understanding of why ICS protocols present such a persistent attack surface. Certificate of completion included. Duration: 8 hours.	

	9:00AM	5:00PM	[0-107] Building AI Agent for ICS/OT Security	**Clint Bodungen**, *Founder / Chairman / Head of Product Innovation* at ThreatGEN	Little 5 Points	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.	Everyone
	9:00AM	10:30AM	[0-109] OT Awareness Bootcamp (Session 1 of 3)	**Donovan Tindill**, *Director of OT Cybersecurity* at DeNexus, *Founding Faculty* at CambiOS Academy	Old 4th Ward	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.	Entry
	10:20AM	10:30AM	BREAK				
	10:30AM	12:00PM	[0-209] OT Awareness Bootcamp (Session 2 of 3)	**Donovan Tindill**, *Director of OT Cybersecurity* at DeNexus, *Founding Faculty* at CambiOS Academy	Old 4th Ward	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.	Entry
	10:20AM	10:30AM	LUNCH ON YOUR OWN				
	1:00PM	2:30PM	[0-309] OT Awareness Bootcamp (Session 3 of 3)	**Rob Garry,** *Retired Executive Chief Engineer, VP Product Cyber Security* at GE Energy, *Founding Faculty* at CambiOS Academy	Old 4th Ward	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.	Entry
	2:30PM	5:00PM	[0-358] Intro to OT Regulations, Standards & Guidelines	**Donovan Tindill**, *Director of OT Cybersecurity* at DeNexus, *Founding Faculty* at CambiOS Academy	Old 4th Ward	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	Entry
	2:30PM	5:00PM	Vendor Expo Setup Begins		Midtown		
	2:30PM	2:45PM	**BREAK**				
	3:00PM	5:00PM	[0-401] Mini-Conference - GT Students & Faculty -	Host: **Derek Harp**, *Founder & Chairman* at (CS)²AI / Level Zero Conference, *Co-Founder* at CambiOS Academy Yosef Beck, Vice President of Cyber Security at CRH	Midtown	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.	Entry
	4:00PM	8:00PM	**Early Registration**				
	5:00PM	6:30PM	Informal Vendor Expo		Midtown	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.	
	5:00PM	9:00PM	**Pizza, Beer & Cocktails**				
	5:00PM	10:00PM	**[0-901] Game Night Social**	**Clint Bodungen**, *Founder / Chairman / Head of Product Innovation* at ThreatGEN	Midtown	After a full day of hands-on training, Level Zero kicks off conference week the right way — with a night built for the OT/ICS security community. Game Night Social brings together conference registrants for an evening of Cybersecurity and Hacker-themed board games, card games, puzzles, and activities designed to spark conversation and connection in a low-key, fun environment. The evening is as much about building relationships as it is about having a good time. Whether you're a seasoned ICS practitioner or attending your first security conference, this is the perfect way to meet the people behind the badges before the main event begins. Light refreshments available. Open to all conference registrants. No separate registration required.	

			*Agenda is subject to change. Please check back regularly.			
	Start time	**End time**	**Event Title**	**Speaker(s)**	**Location**	**Abstract**
April 20	7:45AM	5:00PM	Registration			*Abstract*
	7:45AM	8:45AM	Light Breakfast			*Abstract*
	7:45AM	8:45AM	[1-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	Facilitated by: **Derrik Oates**, *OT Cybersecurity Senior Consulting* at UTSI	Midtown	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
	8:45AM	9:00AM	Transition			*Abstract*
	9:00AM	9:15AM	[1-101] Introduction	**Host: Derek Harp**, *Founder & Chairman* at (CS)^{2}AI / Level Zero Conference, *Co-Founder* at CambiOS Academy	Midtown	Opening remarks and welcome to Level Zero 2026
	9:15AM	9:30AM	[1-111] Welcome	**Host**: **Vivek Sakar,** *Founding Chair, School of Cybersecurity and Privacy* at Georgia Tech	Midtown	Welcome and Introduction to the School of Cybersecurity and Privacy
	9:30AM	10:00AM	[1-121] Keynote	**Megan Samford,** *Chief Security Officer - US National Security Agreements & US Federal Business* at Schneider Electric	Midtown	*Abstract*
	10:00AM	10:40AM	[1-131] Key Perspectives in OT Security Panel	**Host: Derek Harp**, *Founder & Chairman* at (CS)^{2}AI / Level Zero Conference, *Co-Founder* at CambiOS Academy **Panelists: Yosef Bec**k, *Vice President of Cyber Security* at CRH **Blake Gilson**, *Industrial Cybersecurity Manager* at ExxonMobil **Dee Kimata**, *Cybersecurity Thought Leadership Director* at Schneider Electric **Brad Willet**, *OT Security Infrastructure Architect* at UPS	Midtown	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.
	10:40AM	10:55AM	[2-202] OT Defense Workforce Roles and Training	**Daryl Haegley,** *Technical Director, Control Systems Cyber Resilience* at United States Department of Air Force	Midtown	"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?"
	10:55AM	11:45AM	[1-151] The Insurable Gap Panel: Why OT Security is the New Board Mandate	**Host**: Shaun Six, President and CEO, PMP, MSM, ITILv3 at UTSI International Corporation **Panelists**: **Joe Carroll**, *Chief Information Officer & Head of Cybersecurity* at CITGO Petroleum **Scott Kannry**, *Chief Executive Officer* at Axio **Nick Jennings**, *VP and Philadelphia Market Leader, Cyber Solutions* at Aon	Midtown	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.
	11:45AM	12:15PM	[1-141] View from the Board Room: Cybersecurity, Artificial Intelligence, and Geopolitics	**Host: Derek Harp**, *Founder & Chairman* at (CS)^{2}AI / Level Zero Conference, *Co-Founder* at CambiOS Academy **John Tien**, *Board Member at Union Pacific, Board Member* at SAIC, *former Deputy Secretary* at U.S. Department of Homeland Security	Midtown	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.
	12:15PM	12:30PM	[1-145] Recognition Ceremony	**Host: Derek Harp**, *Founder & Chairman* at (CS)^{2}AI / Level Zero Conference, *Co-Founder* at CambiOS Academy **John Tien**, *Board Member at Union Pacific, Board Member* at SAIC, *former Deputy Secretary* at U.S. Department of Homeland Security	Midtown	The Level Zero team is proud to recognize the many veterans and first responders in attendance at this year's conference.
	12:30PM	1:45AM	LUNCH		Midtown	Lunch is served — and so is the main stage. During today's lunch break, three industry guest speakers take the floor for a series of TEDx-style short talks: sharp, focused presentations designed to spark ideas, challenge assumptions, and connect the day's themes to real-world OT/ICS challenges. These fast-format talks are a highlight of the Level Zero experience — expert voices, minimal slides, maximum impact. Grab your plate, find a seat, and stay tuned to the main stage.
	12:45PM	2:10PM	[1-201] Continuous Risk Management In Flight	**Cody Scott**, *Senior Industry Analyst, Security & Risk* at Forrester, *former Chief Cyber Risk Officer* at NASA	Midtown	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.
	2:10PM	2:35PM	[1-221] Session with Fortinet		Midtown	
	2:35PM	3:30PM	[1-301] CISO Energy Panel	**Host: Chris Roche**, *CISO | Director - Energy/Critical Infrastructure Cybersecurity & Resilience* at CI-Discern, *former CISO* at GE Energy & NextEra Energy **Panelists: Dale Beauchamp,** Deputy CISO at *Amtrak* **Jonathan Tubb**, Industrial Cyber Security Officer at *Siemens Energy* **Alex Waitkus**, Principal OT Cybersecurity Architect at *Southern Company*	Midtown	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.
	3:30PM	4:20PM	Panel	**Host: Preston Futrell**, Partner, Cybersecurity Services / Global OT Security Offering Leader at IBM **Panelists:** Opswat **Tamir Margalit**, *Director of ICS/OT Security* at Sygnia	Midtown	
	4:20PM	4:45PM	[1-321] Closing Message	**Host: Derek Harp,** *Founder & Chairman* at (CS)^{2}AI / Level Zero Conference, *Co-Founder* at CambiOS Academy **Patrick Miller**, *CEO* at Ampyx Cyber, *Co-Founder* at CambiOS Academy	Midtown	Closing remarks for Day 1 and recognizing long-term community contributors.

	4:45PM	5:45PM	Cocktail Hour	Midtown	*Abstract*
	5:45PM	10:00PM	FULL DINNER, Open Bar & Planned Activities	Midtown	Monday night at Level Zero means dinner, open bar, and a little controlled chaos. The evening features an OT/ICS cybersecurity trivia competition — and an intermission that might be even more entertaining: a Shark Tank–style comedy pitch session where participants present a 5-minute pitch for a fictional OT cybersecurity product or service. Solo or team, scripted or spontaneous. The goal is simply to have fun and see what creative — and possibly ridiculous — ideas the community can dream up. Come ready to laugh, and maybe come ready to pitch.

LEVEL ZERØ

*Agenda is subject to change. Please check back regularly

	Start time	End time	Event Title	Speaker(s)	Location	Abstract	Track
April 21	7:30AM	8:50AM	FULL BREAKFAST			*Abstract*	
	8:00AM	12:00PM	Vendor Expo: Game Points			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.	
	8:00AM	10:00AM	[2-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	Facilitated by: **Derrik Oates**, *OT Cybersecurity Senior Consulting* at UTSI	Midtown	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	Everyone
	8:50AM	9:00AM	TRANSITION				
	9:00AM	9:50AM	[2-101] Considering Cyber Conservative Operations	**Virginia "Ginger" Wright**, *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Laboratory	Centennial	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.	Everyone
	9:00AM	11:00AM	[2-109] Getting Started in ICS/OT Cybersecurity: (2 hrs)	**Justin Searle,** *Director of ICS Security* at InGuardians	Highlands	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.	Entry
	9:25AM	9:50AM	[2-102] Beyond Technology: Building Cyber Resilience beyond the Security Team	**Dee Kimata,** *Cybersecurity Thought Leadership Director* at Schneider Electric	Home Park	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.	Everyone
	9:50AM	10:00AM	TRANSITION				
	10:00AM	10:50AM	OT Cyber Warrior Work Role	**Daryl Haegley,** *Technical Director, Control Systems Cyber Resilience* at United States Department of Air Force	Home Park	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 system and its interconnections are secure in support of mission operations. It's the only cyber work role focused on Operational Technology (OT) systems, i.e. power, water, building automation, airfield lighting, fuel, manufacturing, logistics, security, fire life safety, etc.	Everyone
	10:00AM	10:50AM	[2-201] "Accelerate" for OT: What Actually Translates?	**Josh Ross,** *Co-Founder and CEO* at Ironloop	Centennial	"Accelerate", the landmark DevOps study, transformed how IT measures software delivery performance. But what actually translates to OT? In this interactive BoF session, participants will examine the four DORA metrics (Deployment Frequency, Lead Time, Change Failure Rate, MTTR) through an OT lens. Using an "Adopt, Adapt, or Avoid" framework, small groups will debate which DevOps practices work in industrial environments and co-create an OT DevOps self-assessment guide to take back to their teams.	Entry
	10:00AM	12:00PM	[2-203] Living off the Land, and Delivering Over the Air (2 hr Workshop)	**Marc Visser,** *OT/IT Security Officer* at Sec4OT, *Founding Faculty* at CambiOS Academy **Bryan Singer,** *Principal Director, Global OT Incident Response Lead* at Accenture, *Founding Faculty* at CambiOS Academy	Kirkwood	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	Mid-level

9:00AM	11:00AM	[2-109] Getting Started in ICS/OT Cybersecurity: (2 hrs)	**Justin Searle**, *Director of ICS Security* at InGuardians	Highlands	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.	Entry
10:50AM	11:00AM	TRANSITION				
11:00AM	11:50AM	[2-401] Grid Time Travel Panel: Navigating Greenfield, Brownfield, and Legacy Technologies in the Modern Utility	**Host: Rob Garry,** *Retired Executive Chief Engineer, VP Product Cyber Security* at GE Energy, *Founding Faculty* at CambiOS Academy **Panelists: Jacob Kitchel**, *Sr. Manager OT for Transmission Operations* at Invenergy **Carter Manucy,** *Director, Cybersecurity* at National Rural Electric Cooperative Association **Cole Oursler**, *Director of Information Services* at Mountain View Electric Association	Centennial	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.	Everyone
11:00AM	11:50AM	[2-402] OT Security Crossroads - Engineering x Hacking	**Vivek Ponnada**, *SVP of Growth & Strategy* at Frenos	Home Park	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.	Everyone
11:00AM	11:50AM	[2-403] Cognitive Architectures for Critical Infrastructure: When Your AI Analyst Never Forgets	**Clint Bodungen**, *Founder / Chairman / Head of Product Innovation* at ThreatGEN	Highlands	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.	Everyone
12:00PM	1:30PM	LUNCH				
12:10PM	1:00PM	[2-451] Vendor Speed Dating			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!	
1:30PM	2:20PM	[2-501] PANEL	Panelists: Copia, Netwrix	Centennial		
1:30PM	2:20PM	[2-502] Meandering No More: Escaping the Firefighter Trap in OT Security (Talk + Working Session)	**Christian Harter,** *BISO OT & Director of OT Security and Engineering* at UPS	Home Park	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.	Leadership

	1:30PM	2:20PM	[2-503] Putting the E in P.A.C.E.: When Satcom Is Not Enough	**Mark Bristow**, *Director, Cyber Infrastructure Protection Innovation Center (CIPIC)* at MITRE	Kirkwood	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).	Everyone
	2:20PM	2:30PM	TRANSITION				
	2:30PM	2:55PM	[2-601] Session with IBM Security	Speaker IBM Security	Centennial	*Abstract*	Everyone
	2:30PM	3:20PM	[2-602] Trust, Transparency, and Treachery	**Marcus Sachs**, *Senior Vice President and Chief Engineer* at Center for Internet Security	Home Park	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.	Everyone
	2:30PM	3:20PM	[2-603] OT Asset Discovery at Massive Scale	**Brad Willet,** *OT Security Infrastructure Architect* at UPS	Kirkwood	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.	Entry
	2:55PM	3:20PM	[2-651] Session with UTSI Intl	**Shaun Six**, *President and CEO* at UTSI International Corporation	Centennial		Everyone
	3:20PM	3:30PM	TRANSITION				
	3:30PM	4:20PM	[2-701] Behind the Curtain: A Practical Guide to NERC Audit Success	**Chase Snuffer,** *Chief Information Officer* at Rayburn Electric Cooperative	Centennial	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.	Mid-Level
	3:30PM	4:20PM	[2-702] OT Risk Quantification for BESS	**Katherine Hutton**, *Product Manager, Cybersecurity* at Fluence	Home Park	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.	Entry

	3:30PM	4:20PM	[2-703] People, Process and Pragmatic OT Security	**David Ong**, *Founder, CEO* at Attila Cybertech	Kirkwood	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.	Everyone
	3:20PM	3:30PM	TRANSITION				
	4:30PM	5:20PM	[2-801] Applying Financial Quantification of Risk in ICS/OT Cybersecurity Decision-Making	**Donovan Tindill,** *Director of OT Cybersecurity at DeNexus*	Centennial	An introduction to the various ICS/OT standards, regulations, and guidelines relevant to owners, consultants, etc. across various verticals.	Entry
	4:30PM	5:20PM	Zero Trust Security: Cyber Resilience for OT Systems with Microsegmentation	**Justin Heyl,** *Modernization and Integration Principle* at Navigator Solutions, Inc.	Home Park	Across critical industries, cyber threats are escalating in scale and sophistication, leveraging advanced intrusion and lateral movement techniques to disrupt core operations. As these attacks target critical industries, such as energy and manufacturing, the impact extends beyond IT downtime to degraded OT. In this context, traditional perimeter-based defenses and OT security methodologies are no longer sufficient, making microsegmentation a foundational control for modern cyber-resilience.	Mid-level
	4:30PM	5:20PM	[2-803] Building a Resilient, Intelligent Digital Railway: Cybersecurity Strategies for the Broadway Subway SkyTrain Project	**Rahim Othman**, *Systems and Programs Leader* at Parsons	Kirkwood	Explore Parsons' Security by Design approach to safeguarding operational technology (OT) in critical infrastructure projects like Vancouver's Broadway Subway Project. This session delves into defense-in-depth strategies, lifecycle cybersecurity integration, and practical solutions for addressing the unique attack surface of automated, driverless transit systems where safety-critical OT, enterprise IT connectivity, and vendor remote access converge.	Entry
	4:30PM	6:30PM	Vendor Expo: Earn Game Points!		Midtown	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.	
	5:30PM	6:30PM	DINNER ON YOUR OWN IN ATLANTA			*Abstract*	

LEVEL ZERO

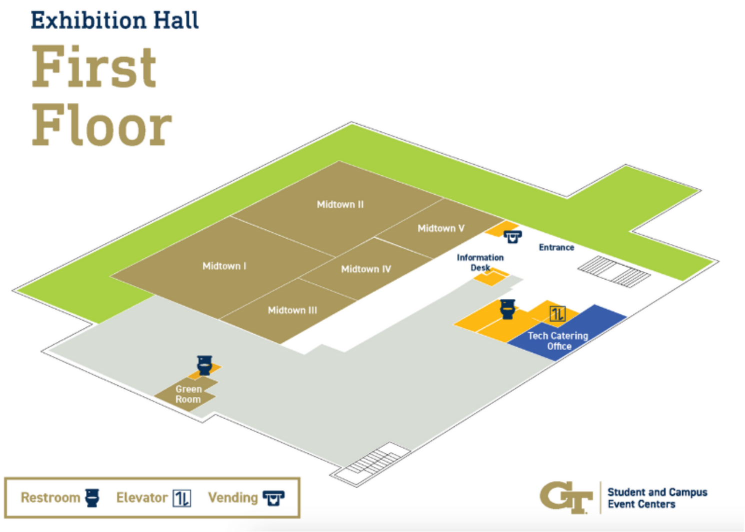
*Agenda is subject to change. Please check back regularly.

	Start time	End time	Event Title	Speaker(s)	Location	Abstract	Track
April 22	7:30AM	8:50AM	**FULL BREAKFAST**			*Abstract*	
	8:00AM	12:00PM	Vendor Expo: Game Points			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.	
	7:45AM	8:45AM	[2-001] Incident Response Table Top Exercise using FEMA's NIMS Incident Command System	Facilitated by: **Derrik Oates**, *OT Cybersecurity Senior Consulting* at UTSI	Midtown	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	Everyone
	8:50AM	9:00AM	TRANSITION				
	9:00AM	9:50AM	[3-101] PANEL	Panelists: Foxguard & KASM	Centennial		Everyone
	9:00AM	9:50AM	[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	Home Park	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.	Mid-level
	9:00AM	9:50AM	[3-103] Oil & Gas Fireside Chat	Host: **Bemi Anjous**, *OT CISO* at Noble Corporation **Jeevan Sakti,** *Global ICS Security Engineering Supervisor* at ExxonMobil	Kirkwood	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.	Everyone
	9:50AM	10:00AM	TRANSITION				
	10:00AM	10:25AM	[3-201] Securing a UNS Workshop	**Jeff Smith**, *Chief Technology Officer* at Dynics	Centennial	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.	Mid-Level
	10:00AM	10:25AM	[3-202] Fortinet		Home Park		Everyone
	10:00AM	10:50AM	[3-203] Cyber Resilience Quantification Workshop	**Eric Cardwell,** *Vice President of Professional Services* at Axio **Shawn Bilak**, *OT Cybersecurity at Southern Company, former Risk & Compliance Analyst Specialist* at Southern Company	Kirkwood	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.	Mid-Level
	10:25AM	10:50AM	[3-301] Journey to OT Visibility	**Alex Waitkus**, *Principal OT Cybersecurity Architect* at Southern Company	Centennial	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.	Mid-level
	10:25AM	10:50AM	When Expectations Meet Reality: The Anatomy of Cyber Incidents Affecting OT Organizations	**Kyle Alexander**, *Director of Cyber Security Services* at Sygnia **Tamir Margalit,** *Director of OT Security* at Sygnia	Home Park	Real world incident response experience shows that many attacks against OT centric organizations unfold differently than expected. There are several key reasons why reality diverges from initial assumptions, and understanding these gaps offers critical lessons for strengthening operational resilience.	Entry
	10:50AM	11:00AM	TRANSITION				
	11:00AM	11:50AM	[3-401] OT Cyber Entrepreneurs Panel	Host: **Derek Harp**, *Founder & Chairman* at (CS)²AI / Level Zero Conference, *Co-Founder* at CambiOS Academy **Christophe Bourel**, *President* at TYREX	Centennial		Everyone
	11:00AM	11:50AM	[3-402] OPSWAT		Home Park		Everyone
	11:00AM	11:50AM	[3-403] Securing the Skies: Cybersecurity Challenges and AI-Driven Threats in Drone Operations	**Saman Zonouz**, *Associate Professor, Schools of Cybersecurity and Privacy (SCP) & Electrical and Computer Engineering (ECE)* at Georgia Tech	Kirkwood	As the role of drones in critical infrastructure expands, so does the attack surface, making them prime targets for cyber-attacks. Drawing from real-world incidents and cutting-edge research, we will explore adversarial tactics, nation-state attack strategies, and the cyber-physical implications of drone compromise. Leave with insights into innovative defense mechanisms, including AI-powered intrusion detection and resilient control algorithms tailored for drone security.	Everyone
	12:00PM	1:30PM	LUNCH			The final lunch of Level Zero keeps the main stage alive with another round of TEDx-style guest speaker talks — three sharp, presentations from leading voices across the OT/ICS cybersecurity landscape. Fast-format, high-signal content during a meal break: this is Level Zero's signature way of making sure every hour of the conference counts. Grab your lunch, find a seat, and catch the last round of big ideas before the closing sessions.	
	1:30PM	4:30PM	Vendor Expo Breakdown			*Abstract*	

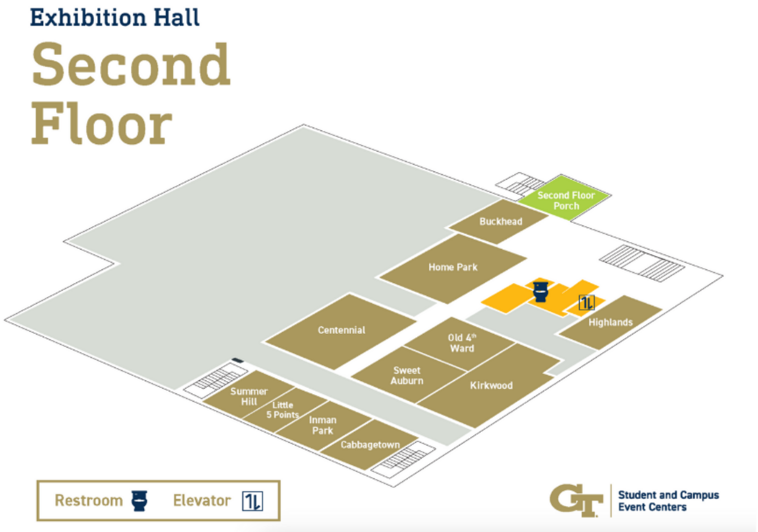
	1:30PM	2:20PM	[3-501] Lessons Learned: Incident Response Exercise using FEMA's NIMS Incident Command System	Facilitated by: **Derrik Oates**, *OT Cybersecurity Senior Consulting* at UTSI	Centennial, Midtowr	This interactive session brings together facilitators from the morning's three concurrent Incident 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.	
	1:30PM	2:20PM	A Tale of Two Grids: Poland, Iberia, and the Future of Energy Stability.	**Closeout Keynote:** **Emma Stewart**, *Director, Center for Securing Digital Energy Technology* at INL (Idaho National Laboratory)	Home Park		
	2:20PM	3:00PM	[3-601] FINAL CLOSING CEREMONY	**Host:** **Derek Harp**, *Founder & Chairman* at (CS)²AI / Level Zero Conference, **Co-Founder** at CambiOS Academy	Centennial, Midtowr	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.	Everyone

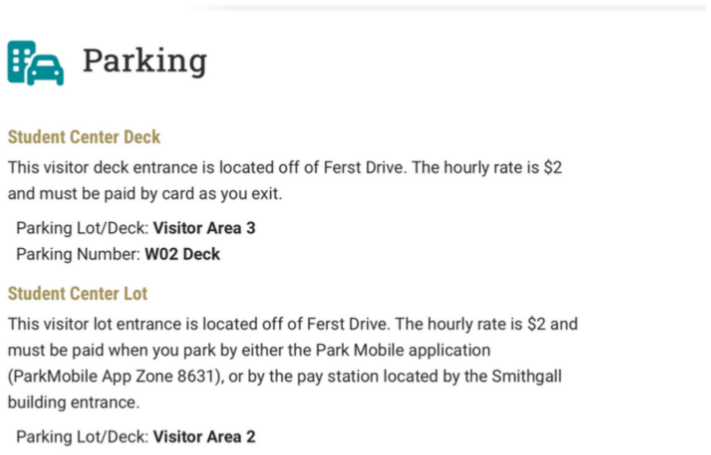
LEVEL ZERO			*Agenda is subject to change. Please check back regularly.			
	Start time	End time	Event Title	Speaker(s)	Location	Abstract
April 23	8:00AM	12:00PM	[4-101] CIE Design Patterns Working Group	**Virginia "Ginger" Wright,** *Program Manager, Cyber-Informed Engineering (CIE)* at Idaho National Laboratory and **Benjamin Lampe**, *Instrumentation and Control Engineer* at Idaho National Laboratory		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

First Floor



Second Floor





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**