Track I: Policy Panels and Presentations

Policy, strategy, and governance-focused panels and presentations, including keynotes and fireside chats by leading government officials.

Location: 1001 Pennsylvania Avenue NW, floor 10, rooms 10CC5 and 10CC6

May 30, 10:00 AM:	*Conference Opening and Introduction* with **Bryson Bort**
May 30, 10:30 AM:	*Fireside Chat* with Congressman **Brad Finstad** and **Ron Gula**, President and Founder of Gula Tech Adventures
May 30, 11:30 AM:	*Operation Cyber Shield: Expanding Department of Defense Authorities to Safeguard U.S. Critical Infrastructure*

Moderator: Alison King, Forescout
Panel: HON **Lucian Niemeyer**, former DOD Assistant Secretary of Defense, BuildingCybersecurity.org**,** **Michael G. McLaughlin**, co-leader of the Cybersecurity and Data Privacy Practice Group and Principal Policy Advisor at Buchanan Ingersoll & Rooney PC, and **RADM Mark Montgomery (Ret.),** Foundation for Defense of Democracies**.**
This panel will discuss the need to expand DOD authorities and operations to actively defend US critical infrastructure in cyberspace. National security leaders have warned recently that the nature and target of attacks by Nation-State and affiliated actors has escalated from the collection of data and seizing/ransom of IT system and software to the placement of malware intended to sabotage, disrupt, or deny the operational technologies in essential services including power, water, communications, trade, and transportation systems. Recent cyber attacks to Texas water systems affirm the ability and intent to disrupt essential services. In response, the private sector owners of these systems are being urged to fund and apply advanced risk mitigations and to hunt for a wide range of malicious activities. Most of these system owners do not have the threat awareness, expertise, or resources to combat sophisticated State sponsors of cyber sabotage. At a time when USCYBERCOM is conducting hunt-forward missions in more than a dozen countries and deployments globally, it's time to mobilize and deploy a Cyber National Mission Force within a named USNORTHCOM Operation to work side by side with critical infrastructure owners and other federal agencies to actively protect U.S. citizen safety and health, defend against Nation State attacks, and establish a national cyber shield for North America.

The panel will explore the implications of categorizing Nation-state cyber attacks and sabotage action to infrastructure as Acts of War. They will assess the need for an operation formally designated by National

Command Authorities to direct DOD resources, funding, and the potential use of the Defense Production Act, to quickly implement capabilities and effects to identify risk, protect assets, detect breaches, and deter attacks. The panel will analyze relevant provisions in the NDAA to generate actionable insights and recommendations. These insights will contribute to the strengthening of US cyber defenses, the protection of critical infrastructure, and the evolution of international law in response to the challenges of cyberspace and the need to reshape the cyber ecosystem to achieve greater public health and safety outcomes.

May 30, 1:30 PM:

Adversarial Technomics: Identifying and Mitigating Economic and Intellectual National Security Threats When Commercializing High Tech Innovations

Moderator: Robert J. Shaughnessy, CEO, Psymetis, Inc.
Panel: Jeff Jones, Psymetis, Inc., **Jonathan Cook**, Idaho National Laboratory, and **David Aaron**, Perkins Coie LLP.
Why steal technology when you can simply own it? This talk and panel will discuss the current threat landscape to commercializing innovations in the US; including nation-state adversaries applying covert sovereign funds through US-based shell entities to make clandestine investments in US tech companies. We will approach the problem and talk through ways to deter and mitigate the threat with experts representing technology, legal, governmental, and commercial industries. This talk will touch on technology, law, policy, and contracting, and will help illuminate a significant hindrance to getting more truly cutting-edge capabilities into the market.

May 30, 2:30 PM:

The Evolving Threat Landscape for Critical Infrastructure

Moderator: RADM Mark Montgomery (RET.), Senior Director of the Center on Cyber and Technology Innovation, Foundations for the Defense of Democracy
Panel: Matt Hayden, Former Assistant Secretary of Homeland Security for Cyber, Infrastructure, Risk, and Resilience Policy, **Audrey Adams**, MITRE, **Col. Gerald Mazur**, Deputy Commander, 91st Cyber Division of the VA National Guard, and **Alexandra Seymour**, Staff Director, Cybersecurity and Infrastructure Protection subcommittee, House Homeland Security Committee.
This panel will provide an in-depth analysis of the rapidly evolving cyber threat landscape facing critical infrastructure sectors in the United States, specifically on the state level. As adversaries continue to enhance their offensive cybersecurity capabilities, they are increasingly targeting vulnerabilities in America's critical infrastructure systems with the aim of causing disruption and destabilization.

The panelists will discuss the latest cyber threats and tactics being employed by hostile nation-states and other malicious actors. They will also explore strategies for improving cyber threat intelligence sharing between government, both at the state and federal levels, and industry, as well as modeling techniques to better anticipate and defend against potential attacks. Additionally, the panel will delve

into the readiness capabilities for state-level officials to respond to the effects of cyberattacks on critical infrastructure such as the energy sector, water supplies, and the oil and gas industry.

May 30, 3:30 PM: *Fireside Chat* with **Deputy Homeland Security Advisor Caitlin Durkovich**, National Security Council and **Evan Wolff**, Partner, Crowell LLP

May 31, 10:00 AM: *Opening Remarks*, with **Bryson Bort**

May 31, 10:20 AM: *Raise the drawbridge! Rethinking critical infrastructure cybersecurity in an unstable world*

Moderator: Steve Kelly, Institute for Security and Technology
Panel: Chris Butera, Technical Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, **Kate Ledesma**, Head of Public Policy & Government Affairs, Dragos, **Bilyana Lilly**, RAND researcher, Warsaw Security Forum cyber chair, and NightDragon advisor, **Andrew Stewart**, Senior National Security Strategist, Cisco Systems, and **Virginia "Ginger" Wright**, Department Manager for Research Accelerator and Cyber-Informed Engineering Program Manager, Idaho National Lab.
The world is becoming less stable by the week, setting the conditions under which ransomware gangs and hostile foreign militaries are no longer deterred from positioning on, or even disrupting, essential public services. At the same time, critical infrastructure owners and operators are too often failing to implement the most basic cyber protections. Given the challenge of increasingly distributed assets, remote administration needs, and a dearth of cybersecurity expertise in small and midsize organizations, it is not hard to understand why so much operational technology is exposed to the public internet. What essential measures should organizations' take to keep critical assets beyond the reach of bad actors? And what preparations should organizations make to "raise the drawbridge" and fight through a bad day?

May 31, 11:30 AM: *NEXT STEPS – The Cybersecurity Posture of the United States*

Moderator: Alison King, Forescout
Panel: Bishop Garrison, INSA, **John Quigg**, JHU APL, **Chris Reid**, Elastic, and **Brian Schultz**, CyberAlphas.
The panelists will explore a multi-layered national defense strategy focusing on risk management, information sharing, and incident response coordination. They will do so in the context of the recent reports from the PCAST and the ONCD, providing a comprehensive understanding of the current cybersecurity posture of the United States.

May 31, 1:30 PM: *Press Views on Critical Infrastructure Reporting*

Moderator: Sam Sabin, Axios
Panel: Derek Johnson, CyberScoop, **John Sakellariadis**, Politico, and **Sara Friedman**, Inside Cybersecurity.

May 31, 3:30 PM:

Hacking CNI Risks with VCs?

Moderator: Pete Cooper, Former Deputy Cybersecurity at UK Cabinet Office
Panel: Anjana Rajan, Assistant National Cyber Director for Technology Security The White House**, Justin Label,** Inner Loop Capital, and **Dr. Emma Stewart,** Idaho National Labs.
The recent US Govt announcements regarding nation state threats to US CNI are driving critical conversations about what else can be done to increase security and resiliency. We need a significant and collaborative effort from everyone involved to make sure that the right cyber security capabilities and capacity is applied in the right way - we don't have the luxury of time and we need to scale fast. To do this will take prioritized and strategic investment and collaboration between those setting out the challenge, those building the cyber capabilities and those who help fund it - the VC community.

What's the challenge and how can founders, builders, defenders, government and the VC community work together for the common good? How best can we work together to grow what we need both now and in the future?

No matter where you sit in the ecosystem be it cyber defense, government or the VC community, this panel will have something that will be relevant to how you can contribute going forwards.

Track II: The Boardroom

A series of half-hour individual sessions, each of which will dive deep into leading issues in ICS security. Topics include the corporate, legal and regulatory environment, and specific technical or operational details.

Location: 1001 Pennsylvania Avenue NW, floor 9, rooms 9E and 9F

May 30, 10:00 AM: *Global Humanitarian ISAC–Defending the Vulnerable on the Front Line*

Presenter: Mike Clauser, Ark
Humanitarian organizations like OxFam, Doctors Without Borders, and IFRC work on the front lines of conflict zones and destabilized regions providing relief to the war ravaged, refugees, and the impoverished. These regions are often politically sensitive, like Ukraine and Gaza. Direct support with local populations puts non-profits squarely in the crosshairs of malicious cyber attackers. But non-profit rating agencies count cybersecurity spend as “overhead” limiting necessary investments and leaving them largely undefended. Efforts are underway to constitute a Global Humanitarian Information Sharing & Analysis Center (ISAC) to give these organizations a fighting chance at cyber defense and the US Government can play a crucial role.

May 30, 10:30 AM: *Defensive Tensions in Critical Infrastructure Defense*

Presenter: Joe Slowik, MITRE
Critical infrastructure defense faces a significant, but often overlooked, issue in terms of delineating what precisely is "critical" - and what infrastructure elements are not. In this presentation, we will take a "critical" eye to examining infrastructure, attacks, and defense to separate out what is "simply important" in economic and strategic terms, and what items should (unfortunately) be deprioritized in allocating scarce defense and response resources. As part of this discussion we will also examine what the entities left outside strategic support can meaningfully do to shore up defense, resilience, and recovery in a contested landscape.

May 30, 11:00 AM: *Respond! Recover! Understanding OT Cyber Incidents in Manufacturing*

Presenter: Dr. Lynette F. Wilcox and **Stephanie Saravia**, NCCoE/MITRE
Cybersecurity incidents in manufacturing facilities present unique problems not found in IT environments which can have significant physical impacts. This session will delve into Operational Technology via video demo of the NIST manufacturing lab and speakers sharing technologies, risk decisions, planning and communications for response and recovery. Techniques can be applied to OT environments.

May 30, 11:30 AM: *The In(sights) and Out(comes) of OT Security Program Build Outs*

Presenter: Jonathan Schoelwer, OT/ICS Cyber Security Analyst
An argument for priorities when building out an OT Security Program as well as Lessons Learned from 5 Program Buildouts. This talk seeks to provide actionable direction for properly securing OT environments while being cognizant of risk tolerance, budget, regulation and other differences across companies and industry sectors.

May 30, 12:00 PM: *How Hackers Send Input to Policymakers like the Pros*

Presenter: Harley Geiger and **Casey Ellis**, Venable LLP
This workshop will demonstrate how anybody can submit official, on-record comments to regulations and legislation. Federal agencies have formal channels for receiving written feedback on policy proposals, and this feedback is an important part of the record for policymaking. These channels are open to the public, but many people do not know how to access or use them.

This workshop will walk participants through how to use regulations.gov and congress.gov to find open commenting opportunities related to security. The workshop will culminate in the drafting and submission of comments - live from the stage, with audience participation! Make your voice heard!

May 30, 2:00 PM: *Bridging the Cybersecurity Skills Gap: Empowering the Next Generation with ICS/OT Expertise*

Presenter: Eric Belardo, Raíces Cyber Org

May 30, 2:30 PM: *Tales from the Front Lines: Ukraine, GPS, and The Struggle to Keep a Power Grid Resilient in a War*

Presenter: Joe Marshall, Cisco Talos
In 2023, Cisco and a multinational, multi-company alliance united to solve a difficult problem in Ukraine: Electronic warfare was disrupting GPS services vital to running a transmission grid. This presentation is the story of the problem, how it was solved by passionate volunteers, and the profound difference it has made on Ukrainian grid stability. This has also opened the conversation on how resilient an American or global power grid would survive GPS disruptions.

May 30, 3:00 PM: *After the Gates have Fallen: The Potential of a Cybersecurity Breach at a Wastewater Facility*

Presenter: Andrew Krapf, Loudoun Water
In an era dominated by advancing cyber threats, critical infrastructure sectors face unprecedented challenges in safeguarding their systems against malicious actors. This presentation delves into the consequences of cybersecurity breaches within wastewater facilities, emphasizing the potential ripple effect that extends into the cyber-physical realm.
The discussion unfolds by examining a few of the "crown jewel" processes of a modern wastewater system and the reliance on digital technologies. By focusing on what can happen after an intrusion, this presentation explores the cascading implications of a breach as it relates to cyber-physical systems, as well as physical, environmental, and health concerns.

May 30, 3:30 PM: *Getting Started in Industrial (ICS/OT) Cyber Security*

Presenter: Mike Holcomb, Fluor
Getting started in the world of ICS/OT can be confusing, frustrating and daunting for many. And yet, it doesn't have to be that way! This presentation highlights the lessons learned from years of trying to decipher how to get started, and continually improving, in the field.

May 30, 4:00 PM: *Product Security or: How I Learned to Stop Worrying and Love the SBOM*

Presenter: Kyle McMillian, Siemens AG
Are you looking forward to knowing the software "ingredients" baked into your ICS components? The "Software Bills of Materials" promised by changes in Federal Acquisition Regulations and legislation in Europe are intended to give the blue team a leg up in defending systems and mitigating vulnerabilities in common software components without the help of their vendors. Instead, these SBOMs will further complicate the already tricky landscape of OT cybersecurity risk management and the missions of our OT defenders. This presentation looks at the pitfalls we must avoid as a community and how we can turn these mundane documents into actionable information.

May 30, 4:30 PM:

Stop Assessing, Start Addressing: Priorities for Critical Infrastructure Cybersecurity in 2024

Presenter: Chuck Weissenborn, Dragos
Since 2017, there have been reports, investigations, hundreds to thousands of assessments, and policy discussions focused on protecting our Nation's and the Department of Defense's critical infrastructure. Those activities all highlighted the need to take action to protect critical infrastructure from cyber-attacks. Our adversaries have shown placement, access, capability, and intent to attack critical infrastructure essential to the lives of our citizens. We are out of time and need to take precise and decisive action in the face of determined adversaries. During this talk, we will explore those actions at the policy, regulatory, and tactical levels.

May 31, 10:00 AM:

Cooperation for the Flag: Innovating Cyber Exercise Approaches

Presenter: Flavio Costa, Inter-American Defense Board
In contrast to conventional Capture the Flag (CTF) competitions, our unique model, crafted under the auspices of the Inter-American Defense Board, is designed to cultivate a spirit of collaboration among participants. Unlike traditional contests, our approach eliminates the scoreboard, encouraging teams to exchange information about challenges to collectively advance. This methodology does not aim to replace existing exercise formats but rather to foster a culture of cooperation essential for addressing real-world cyber threats. By prioritizing collaborative problem-solving, we believe this innovative approach will enhance participants' readiness for real-world cybersecurity challenges.

May 31, 10:55 AM:

Critical Infrastructure Intelligence Challenges

Presenter: Chris Sledjeski, MITRE
This presentation will discuss the enhancements needed to improve cyber threat warning for critical infrastructure across process, tools, capability and integration.

May 31, 11:30 AM:

Achieving Memory Safety Now

Presenter: Joe Saunders, RunSafe Security
As FBI Director Christopher Wray and CISA Director Jen Easterly presented before Congress's Select Committee on PRC, China has gained access to US Critical Infrastructure and could administer a simultaneous cyber attack when it conducts military action on Taiwan by 2027-2030. At the root of this

threat lurks memory-based vulnerabilities exposing embedded systems to exploitation. This presentation will offer an overview of memory safety, what the government has done thus far to help achieve it, practical ways you can implement memory safety protections, what to do about open source software with memory-based vulnerabilities, and the implications for national security.

May 31, 12:30 PM: *Managing Cyber Risk in OT Networks*

Presenter: Michael Frank, Boston Consulting Group / USMCR

May 31, 2:30 PM: *Policy Hacking as Market Hacking: The Future of Product and OT Security Policy as a Case Study*

Presenter: Dr. Amit Elazari, OpenPolicy

Track III: Technical Talks

Also known as the Beer-ISAC, this featured series of half-hour individual sessions is dedicated to peer-to-peer information sharing.

Location: 1001 Pennsylvania Avenue NW, floor 9, room 9C

May 30, 10:00 AM: *OT SecOps and Unveiling New Critical Developments in Our Critical Infrastructure Threat Landscape*

Presenter: Adam Robbie, Palo Alto Networks

May 30, 10:30 AM: *Whose Role Is It Anyway? Public perceptions on CI defense*

Presenter: Mark Bristow, MITRE
While critical infrastructure risks, vulnerabilities and incidents seem to make daily news in cybersecurity circles, not much is understood about how the public perceives this risk and, more importantly, what we can do about it. This presentation goes over the key takeaways from the recent MITRE-Harris poll examining public perceptions of the risk and responsibilities to secure national critical infrastructure. The presentation will conclude with some possible policy options to close some of these gaps.

May 30, 11:00 AM: *Navigating the Maze: Prioritization and Reporting in Critical Infrastructure Cyber Recovery*

Presenter: Paul Shaver, Mandiant | Google Cloud
With an ever growing landscape of connected devices and expanding threat landscape asset owners should work to build detect and respond capabilities that facilitate rapid investigation and remediation processes that allow them to return to normal operations as quickly as possible.

May 30, 11:30 AM: *OT Asset Inventory Methodologies and Why it Matters*

Presenter: Roya Gordon, Hexagon

Asset inventory tools play a vital role in capturing and maintaining accurate information about an organization's OT assets, which is the foundation of OT security. Being that the methods used to gather this information can vary, organizations should understand the differences between these methods to determine which tool (or combination of tools) best suits their environments. By choosing the appropriate method, organizations can achieve more accurate and comprehensive asset inventories, enabling them to make informed decisions regarding asset utilization, security controls, vulnerability management, and regulatory compliance.

May 30, 12:00 PM: *Secure by Design, What it Means, and What It Takes*

Presenter: Mehdi Tarrit Mirakhorli, University of Hawaii at Manoa
Secure by Design (SbD) is becoming a mainstream development approach to ensure security, privacy, and cyber-resiliency. But what does SbD really mean? What does it take to achieve that? What expertise, tools, and best practices are required? In this talk, I will present the concept of Common Design Weakness Enumeration funded by DHS, and share the empirical study results on common design flaws in industrial control systems. I will discuss some of the benefits we expect to gain from the emergence of Secure by Design as a major discipline, including software certification, liability, and redefining the concept of critical software.

May 30, 1:30 PM: *The Power of AI-Enabled Defensive Documentation*

Presenter: Jace Powell, Fortress Information Security
This presentation showcases the role of AI in transforming traditional documentation into an active element of cybersecurity strategies, with a particular emphasis on Industrial Control Systems (ICS). It introduces a documentation maturity model, showing how advanced documentation practices can enable AI to enhance cybersecurity operations, incident response, and other strategic initiatives. We will examine how AI can streamline the documentation process, improving an organization's defensive and operational capabilities.

May 30, 2:00 PM: *Glaring Vulnerabilities in the Automotive Ecosystem: Hacking Everything from a Car to a Country's EV Infrastructure*

Presenter: Ayyappan Rajesh, Zscaler
This talk focuses on the glaring vulnerabilities discovered in the automotive ecosystem, everything from hacking a car , IoT devices that go into them, as well as the entire EV charging infrastructure of a country's biggest provider.

May 30, 2:30 PM: *"Go Away or I Will Replace You with a Very Small Shell Script": AI-assisted Cyber Targeting*

Presenter: Sarah Freeman and **Walker Dimon**, MITRE
As noted by Microsoft Threat Intelligence in early 2024, "Over the last year, the speed, scale, and sophistication of attacks has increased alongside the rapid development and adoption of AI." Security researchers and defenders fear that AI will reduce adversary development and operational costs, enabling them to modernize their weapon systems and develop cyber capabilities at a pace that challenges critical infrastructure defense. But how difficult is it to create an AI-assistant to support cyber operations? This presentation will introduce the approach for developing such a system, as well as identify some of the challenges, pitfalls, and considerations for design.

May 30, 3:00 PM: *Liberty Eclipse: The Value of Immersive Cyber Defense Exercises*

Presenter: Michael Toecker, Department of Energy
DOE CESER Michael Tocker conducts Liberty Eclipse exercise with partners in the energy sector on testbed systems that approximate substation and control center environments. DOE partnered with DARPA on the Rapid Attack Detection, Isolation, and Characterization Systems (RADICS) program from 2018 through 2021, which focused on developing tools and capability to enable black start recovery of the power grid amidst a cyberattack on US energy infrastructure.

Inspired by RADICS, the Liberty Eclipse is a yearly, hands-on-keyboard, red-team/blue-team full-scale exercise that brings together federal partners, and operational technology (OT) and cybersecurity experts from the energy sector to validate cyber security of their cyber defense measures and exercise their plans, policies, and procedures, in a scaled environment.

The proposed presentation would be on how the exercise has been structured since taking it on in 2022, the hands on capabilities, partnerships, and exercise goals and objectives. Additionally, we'd be giving a preview of how the 2024 exercise will contribute to larger energy sector efforts on OT security and critical infrastructure defense, getting lessons learned from this live fire exercise out to energy sector owners and operators.

May 30, 3:30 PM: *How to Develop a CTF*

Presenter: Kate Vajda, Dragos, and **Kenny Warren**, Grimm
In this talk, Kate and Kenny will walk the audience through the process of creating a CTF for DEFCON. We'll discuss constraints, how to tap into creativity, design and organization for the players, and the technology

required to execute. At the end of this talk, you'll feel empowered to run your own CTF, or at the very least, you will be excited to participate in one.

May 30, 4:00 PM: *Bridging the Gap: Enhancing OT Cybersecurity in Critical Infrastructure*

Presenter: Aaron Crow, MorganFranklin Cyber
As digital transformation accelerates, OT systems in critical infrastructure face a widening security gap, notably in asset inventories and network understanding. Hindered by inadequate funding and a misunderstanding of OT's unique needs, alongside a lack of specialized training, the focus on technology alone falls short. A holistic approach, valuing people and processes equally with technology, is imperative. This conference seeks to bridge the knowledge gap for government staff and policymakers, advocating for informed decisions to bolster our nation's critical infrastructure resilience against cyber threats. Our collective action is crucial for a secure, shared future.

May 30, 4:30 PM: *How Resilience Has Changed – Chaos Engineering for Critical Systems*

Presenter: James Cabe, ZPE Systems
A resilience system provides all the infrastructure, tools, and services necessary to continue operating, if in a degraded state, during major incidents. It begins with immutable data and infrastructure. A blends moving target defense for everything needed to recover data, rebuild systems, perform security testing, and continue delivering core business functionality. A resilience system is the core of chaos resilience and the secret sauce of many large corporations and services. It is typically isolated from the production systems, preventing adversaries and resistant to disasters from reaching and compromising it. Allowing teams continuous access even if the primaries go down.

May 31, 10:00 AM: *Watts at Stake: Understanding Cybersecurity Risks to Virtual Power Plants*

Presenter: Nik Urlaub, National Renewable Energy Laboratory
Rooftop solar and other renewable Distributed Energy Resources (DERs) are being deployed at breakneck speed to meet our nation's climate goals. This presentation provides an overview of DERs and Virtual Power Plants (VPPs), highlighting their increasing significance to modern electric grids. It explores their role in enhancing grid flexibility and efficiency, while also delving into the cybersecurity risks they introduce. By fostering a deeper understanding of DERs, VPPs, and associated cyber threats, this session aims to empower attendees with the knowledge needed to understand these new components of the US's critical energy infrastructure.

May 31, 10:30 AM: *ICS4ICS: Incident Response Program Overview*

Presenter: Erik Peterson, Idaho National Lab and ICS4ICS
Learn how to enhance your organization's capabilities and processes to mitigate cyber incident impacts. Craft a business case for executive support to implement the Incident Command System for Industrial Control Systems (ICS4ICS) in your company. This initiative will allow your company to access mutual aid resources, enhancing cyber incident management. Start planning the deployment of ICS4ICS with the goal of strengthening your cybersecurity posture.

The ISA Global Cybersecurity Alliance, in collaboration with the DHS Cybersecurity and Infrastructure Security Agency (CISA) and over 50 other companies, is adopting FEMA's Incident Command System. This globally recognized system, regularly used by first responders for managing emergencies such as natural disasters and industrial accidents, is now being tailored to enhance response structures, roles, and interoperability for cybersecurity incidents affecting industrial control systems and critical infrastructure worldwide. The ICS4ICS program aims at bolstering global cybersecurity defenses within this domain.

May 31, 11:30 AM: *The Mystical OT Security Budget and Where to Find It*

Presenter: Dr. Tomomi Aoyama, Omny
In asset owner organizations, the budget for operational technology (OT) security is often fragmented. While OT security funds typically fall under IT budgets, additional resources may be dispersed across departments such as Governance, Risk, and Compliance (GRC), operations, safety, and quality management. How can we effectively utilize these diverse resources?

This talk explores the dynamics of OT security budget allocation, focusing on cybersecurity and operations teams. We'll discuss steps for mobilizing operational involvement, reframing OT security to address operational issues, and the pivotal role of leadership in enabling organizational change."

May 31, 12:00 PM:

Engineering-In Cyber

Presenter: Virginia “Ginger” Wright, Idaho National Laboratory
This presentation will describe Cyber-Informed Engineering and how CIE is leveraging standard engineering practices, similar to those used to manage safety risk or ensure process performance to limit the impact of cyber attacks on Operational Technology. Together, we will examine specific engineering protections and how they limit the range of options for an adversary, understand how engineers can provide context to inform cyber protection actions, and discuss how engineers, operators, and cyber defenders should practice together to sharpen cyber defenses.

May 31, 1:30 PM: *MITRE EMB3D: Combating Threats to Critical Infrastructure* Devices

Presenter: Jack Cyprus, MITRE

May 31, 2:00 PM: *Threat Hunting Does Not Have to be Hard*

Presenter: Don Weber, Cutaway Security, LLC
Threat hunting to find EVIL can be a difficult endeavor, if you let it. Many people think that they are using threat hunting to find the bad guys in the network. Threat hunting can identify malicious insiders and hackers but it most often identifies misconfigured applications, servers and network devices. It can also provide context around normal and abnormal user and administrative behaviors. Whether you are a medium-sized shop, small shop, or a one-person IT / network / cybersecurity staff, your team can use threat hunting to improve operations while also reducing risk. In this talk, Don will simplify threat hunting activities. The goal will be to provide a repeatable process that can be used by your administrators to understand what is really happening on the network. The process will also provide the basis for justifying equipment and work hours to make this important process successful. All of this will, in turn, dramatically reduce the time it takes your team to respond to a compromise.

May 31, 2:30 PM: *Simple Mental Models for Better Cybersecurity Policy and Comprehension*

Presenter: Sounil Yu, Knostic

May 31, 3:00 PM: *Secure PLC Coding – are we there yet?*

Presenter: Vivek Ponnada, Nozomi Networks
Industrial Control Systems (ICS also referred to as OT or Operational Technology, consisting of SCADA, PLC, DCS etc.) have historically been insecure by design. Several years into customizing and applying best practices from IT gave rise to secure protocols, use of encryption, network segmentation & isolation etc. However,there has not been much focus on using the characteristic features in the PLCs and DCS for security, or how to code/program PLCs with security in mind. The Top 20 Secure PLC Coding Practices project – inspired by existing Secure Coding Practices for IT – fills that gap. The aim of this project is to provide guidelines to engineers that are creating software (ladder logic, functional charts etc.) to help improve the security posture of Industrial Control Systems, by leveraging the natively available functionality in the PLC/DCS/SCADA. Little or no additional software tools or hardware is needed to implement these practices. They can all be fit into the normal PLC programming and operating workflow. More than security expertise, good knowledge of the PLCs to be protected, their logic, and the underlying process, is needed for implementing these practices. Nearly 4 years on, there's been increasing awareness and some direct feedback. But the key question, is Secure PLC Coding happening?


HACK THE CAPITOL
May 30-31, 2024 | Washington, DC