#ES17SUMMIT

17TH ANNUAL ENERGYSEC SECURITY & COMPLIANCE SUMMIT

July 18-20, 2022 | Disneyland Hotel | Anaheim, CA

THANK YOU to our SPONSORS!

Contents

General Conference Information

Venue:

Disneyland Hotel

1150 Magic Way, Anaheim, CA 92802

(714) 778-6600

Registration and Information Hours:

Magic Kingdom Ballroom East Foyer

Monday, July 18th - 8:00 - 5:00
Tuesday, July 19th - 7:00 - 4:00
Wednesday, July 20th - 7:00 - 10:00

Additional Conference Information:

www.energysec.org/energysec-summit

Networking Events...

Day 1 - Monday

Welcome Reception
05:00 PM - 07:00 PM
Sleeping Beauty Pavillion

Day 2 - Tuesday

Breakfast
(Full Conference Pass Attendees)
7:30 AM - 08:30 AM
Castle A-B

Catered Lunch
12:00 PM - 01:15 PM
Adventure Lawn

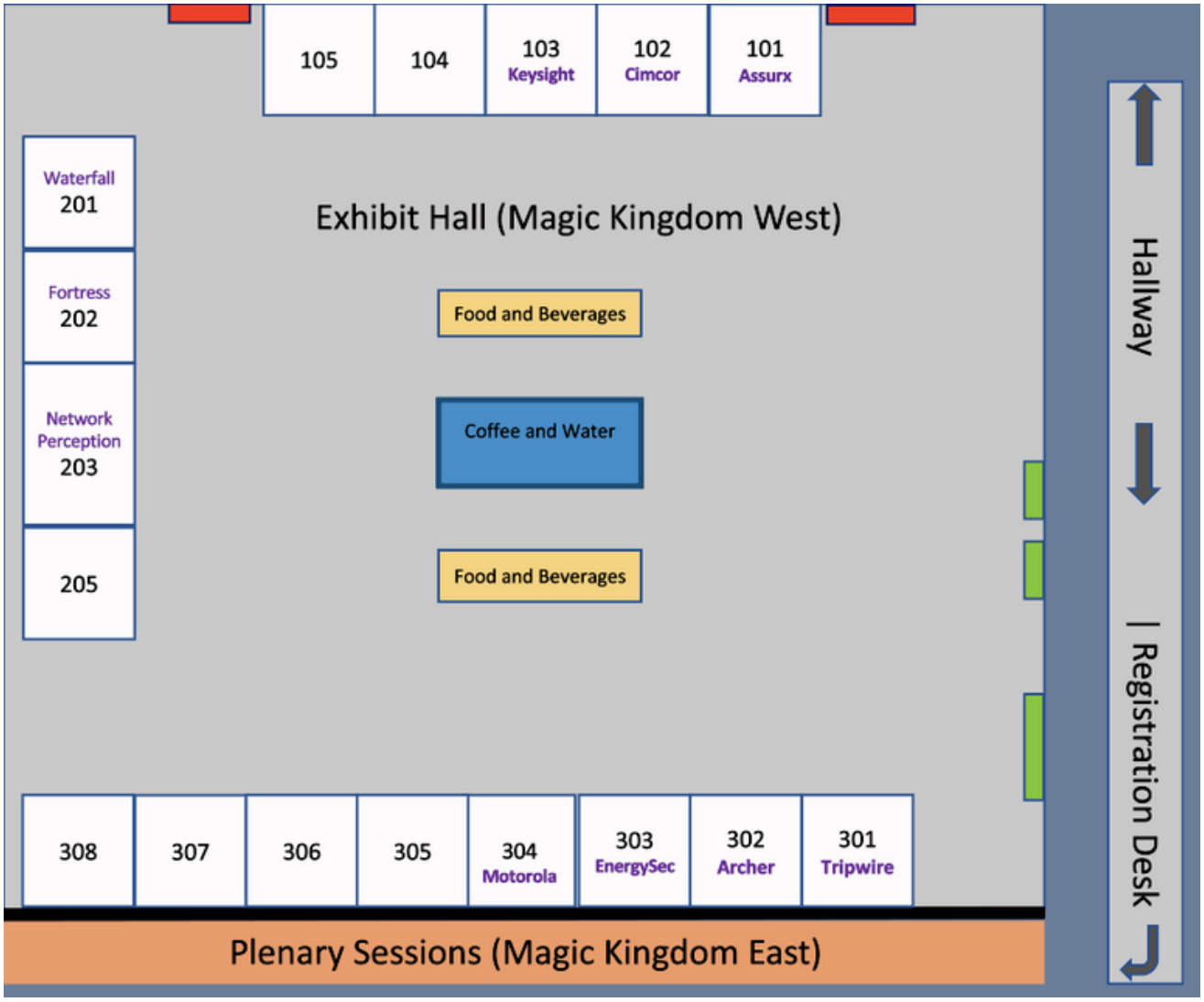
Exhibitor Showcase with Refreshments & Prizes
03:15 PM - 05:00 PM
Expo Hall - Magic Kingdom Ballroom West

Day 3 - Wednesday

Continental Breakfast
(All Attendees)
8:00AM - 09:00 AM
Expo Hall

Catered Lunch
12:00 PM - 01:15 PM
Adventure Lawn

Exhibitor Hall Map



Legend

101	Assurx-Bronze
102	Cimcor-Silver
103	Keysight Technoligies Bronze
104	
105	
201	Waterfall -Gold
202	Fortress - Gold
203	Network Perception-Platinum
205	
301	Tripwire- Bronze
302	Archer. 10x10
303	EnergySec- Host
304	Motorola 10x10
305	
306	
307	
308	

10 x 10 Expo Space

Emergency Exits

Exhibit Hall Entrance

Coffee & Water

Food & Beverages

network perception

Protecting Mission-Critical Assets

NP-View Software Solution

A Different Kind of Visibility & Understanding

Knowing Your Network
We can only defend what we know

Eliminating Blind Spots
Do we understand our attack surface?

Making Informed Decisions
Do we understand context & dependencies?

"You cannot connect all the dots if you can't see all the dots"

[SANS ICS Summit - June 2022]

For more information visit:
https://network-perception.com

Schedule Overview

Day 1 - Monday July 18, 2022

Magic Kingdom Ballroom East Foyer

8:00-5:00 **Registration Open**

Event check-in, name badge pick-up, program guides and event assistance.

Day 1 Morning Breakout Sessions and Lunch are exclusive to Full Conference Pass Holders Only

Monorail A-C

9:00 - 12:00 ***Workforce Challenges & Solutions***

Small Utility Focus

Castle A-B

12:00 - 1:00 **Lunch**

Monorail A-C

1:00 - 4:30 ***Security Analyst***

Supply Chain Security

Sleeping Beauty Pavillion

5:00-7:00 **Welcome Reception**

Join us for our famous Welcome Reception. Bring a guest or the whole family to enjoy appetizers and refreshments, networking with friends and peers, and a photo opportunity with special Disney Characters!

Detailed Schedule

Day 1 - Morning Breakout Sessions

Monorail C — *Workforce Challenges & Solutions*

9:00 - 9:45	**Getting the cybersecurity passion into the K12 space** Nate Evans and Jessica Boersma, Argonne National Laboratory *This summer we will be hosting a version of DOE's CyberForce Competition to engage the K12 audience as a pilot and would like to report out the results as well as ways to potentially grow and engage the pipeline of students at an earlier and earlier age.*
9:45 - 10:30	**Hands-on Operational Technology Cybersecurity Community College Program** Dennis Skarr, Everett Community College and Hack the Capital
10:30 - 10:45	**Break**
10:45 - 12:00	**Launching EnergySec's Cybersecurity Apprenticeship for the Electric Sector** Twila Denham, EnergySec
12:00 - 1:00	**Lunch**

Monorail A — *Small Utility Focus*

9:00 - 9:45	**Cyber integration and information sharing solutions for small utilities** Emma Stewart, NRECA *Cybersecurity is a booming business, with all sizes of companies seeking to advance in OT/ICS security. As this business has increased, and our ability to protect and defend has accelerated, with public private partnerships and new research announced and published on a daily basis. Adversaries respond to this, increase their capabilities – and the business moves forward. The cybersecurity business creates profit on the adversaries improvements, and increases our need to defend. The social responsibility falls to the utilities to deploy and upgrade, but we designed a system in which defending against the latest adversaries, is unaffordable for small and not for profit locations who serve vulnerable communities. They are uniquely community driven and not for profit and the business models don't match. Industry responds with initiatives that provide downsized, or free services – but a small profit driven product, is not the same as something tailored to be used for these entities. This session will discuss the potential avenues for innovation and information sharing models for small utilities in the future.*
9:45 - 10:30	**EnergySec Services** Steve Parker, EnergySec
10:30 - 10:45	**Break**
10:45 - 12:00	**Roundtable Discussion** Steve Parker, EnergySec
12:00 - 1:00	**Lunch**

Detailed Schedule

Day 1 - Afternoon Breakout Sessions

Monorail C

Breakout Session: Security Analyst

1:00 - 1:45

The Case for Well-Structured Advisory Data

Kylie McClanahan, University of Arkansas

The National Vulnerability Database (NVD) is a consistent and centralized source of vulnerability information, provided in a machine-readable format. Contrast this with vendor advisories, which are rarely machine-consumable and must be manually found and read. While these advisories often contain additional useful information for security analysts and operators, the lack of machine-readable data limits attempts at automation; consequentially, many utilities perform this part of the CIP-007 requirements entirely manually. In this presentation, Kylie will demonstrate the difficulty in processing advisories programmatically, while ultimately making the case for a standardized reporting format.

1:45 - 2:30

Baseline Response Capabilities utilizing Structured Threat Information Expression JSON bundles

Manny Vazquez, Idaho National Laboratory

With cyber-attacks on the rise, information is one of the first lines of defense. Now more than ever, security experts and developers need efficient ways to detect and mitigate emerging threats. By generating a baseline based on custom scripts and open-source tools such as the Volatility Framework, security experts and developers can respond to out of norm activities and generate STIX2/JSON bundles that could be used to share valuable information. Security experts and developers can ensure that they know where to find what can go wrong with their systems before the hackers do.

2:30 - 2:45

Break

2:45 - 3:30

Automating and Codifying Attack Surfaces with Structured Threat Information Expression

Manuel Maestas, Idaho National Laboratory

Understanding your attack surface is crucial when trying to protect your systems and devices from cyber-attacks. An attack surface consists of all attack vectors and points of entry into a system, in which an unauthorized user can gain access to, and potentially compromise your system. For years, it has been difficult to create an attack surface as there is no industry "standard" as well as very little resources and documentation about how one should be built. This process can be also difficult as it should include software, firmware, and hardware elements, making attack surface creation time-consuming.

3:30 - 4:30

Compliance, does NOT mean Security – Strengthen your network infrastructure with applicable cybersecurity measures

Mariam Coladonato, Phoenix Contact

Hindsight is always at least 20/20, but is the electric sector really learning from the past? Recommendations from influencing organizations like DHS/CISA, down to NERC CIP and IEC62443 often are so watered down lacking both realistic security controls, management capabilities and any actionable intelligence. This topic will look at the best of both worlds: the NERC CIP standards, specifically those that impact network communications and equipment hardening. Together with complementary ISA/IEC 62443, focusing on the foundational concept of identification and implementation of security Zones and Conduits. The session will showcase hardening recommendations for industrial network infrastructure devices, following Defense in Depth concept and an example of putting it all together in a secure implementation for people, data and networks.

Detailed Schedule

Day 1 - Afternoon Breakout Sessions

Monorail A

Breakout Session: Supply Chain Analyst

1:00 - 2:30 **This afternoon session will be an interactive discussion of issues around supply chain security and compliance requirements.**
Karl Perman, EnergySec and Wally Magda, Senior Standards Instructor

2:30 - 2:45 **Break**

2:45 - 4:30 **Supply Chain Session Continued**

Notes

Detailed Schedule

Day 2 - Tuesday July 19, 2022

Magic Kingdom Ballroom East Foyer

7:00-5:00 **Registration Open**

Event check-in, name badge pick-up, program guides and event assistance.

Castle A-B

7:30 - 8:30 **Breakfast - *Full Conference Pass Exclusive***

Buffet Style Breakfast. This breakfast is exclusive to Full Conference Pass holders only.

Magic Kingdom Ballroom

8:30 - 9:15 **Opening Keynote**

Steve Parker, President, EnergySec

Magic Kingdom Ballroom

9:15 - 10:00 **The Two Sides of Network Visibility**

Robin Berthier, Network Perception

Gaining accurate visibility of OT networks is fundamental to protect critical assets and to ensure that networks are correctly segmented. A comprehensive network visibility solution combines traffic monitoring (what is connecting to what) with network architecture analysis (what can connect to what). This presentation will show a case study to augment traditional intrusion detection with firewall review in order to eliminate blind spots and develop relevant contextual information to better mitigate cyber threats.

Expo Hall

10:00 - 10:30 **Networking Break**

Visit the exhibitor hall for light refreshments and snacks.

Magic Kingdom Ballroom

10:30 - 11:15 **Three Ways Ransomware Impacts Operations**

Andrew Ginter, Waterfall Security Solutions

95% of cyber incidents causing physical downtime in the last two years were ransomware. This presentation introduces the ICSStrive OT incident repository and series of incident analysis reports. We dig into the three ways that ransomware can trigger shutdowns and other consequences. And we look at how cybersecurity programs can prevent these consequences when ransomware hits IT networks.

Magic Kingdom Ballroom

11:15 - 12:00 **Cyberattacks Resulting from the Russian/Ukrainian Conflict**

Bill Nelson, Global Resilience Federation

The Russian invasion of Ukraine has resulted in significant physical damage to Ukrainian critical infrastructure and has impacted the global supply chain. It has also resulted in an uptick in sophisticated and destructive cyberattacks against Western nations, including attacks against the energy sector. In this session, attendees will learn about current and potential Russian cyber threats and how to defend against them. Mr. Nelson will provide an overview of the Operational Resilience Framework (ORF) that provides a roadmap and set of rules for immutable recovery of data, systems, networks, devices, and applications resulting from destructive wiperware attacks that have been launched by Russian adversaries.

Detailed Schedule

Day 2 - Tuesday July 19, 2022

Adventure Lawn

12:00 - 1:15 **Catered Lunch**

Magic Kingdom Ballroom

1:15 - 1:45 **Fireside Chat: Current Trends in OT Security**

Dennis Skarr, Everett Community College/Hack the Capital

Magic Kingdom Ballroom

1:45 - 2:15 **CISA and the Energy Sector**

Dan Strachan, CISA and JCDC

This presentation will talk about the Cybersecurity & Infrastructure Security Agency ("CISA"). How it came to be, its role in the defense of critical infrastructure, and its interactions with the energy sector. Detailed information will be shared about information sharing offered to the energy sector by CISA, the new Joint Cyber Defense Collaborative, and what cybersecurity precautions the sector needs to take now.

Magic Kingdom Ballroom

2:15 - 3:15 **Lightning Talks:**

CIMCOR **Remove the Guesswork: Continuous NERC-CIP Security & Compliance**

Justin Quevedo, Tacoma Power

In this presentation, we will hear from Tacoma Power and their continued use of Cimcor's file and system integrity monitoring software CimTrak, in regards to NERC-CIP Security and Compliance.

Expo Hall - Magic Kingdom Ballroom West

3:15 - 5:00 **Exhibitor Showcase with Refreshments & Prizes**

Join your peers for refreshments in our Expo Hall and explore solutions to your security and compliance needs.

Notes

Detailed Schedule

Day 3 - Wednesday July 20, 2022

Magic Kingdom Ballroom East Foyer

7:00-10:00 **Registration Open**

Event check-in, name badge pick-up, program guides and event assistance.

Expo Hall - Magic Kingdom Ballroom West

8:00 - 9:00 **Continental Breakfast**

Magic Kingdom Ballroom

9:00 - 10:00 **A Review of the Policies Framing the Cyber Defenses of Tomorrow**

Sharla Artz, Xcel Energy

If there has been one constant in the cybersecurity and critical infrastructure space it is how quickly and increasingly the threats continue to evolve. The consistent interest from advanced persistent threat actors in critical infrastructure and industrial control systems, the growing interconnectivity of operational environments, and the current geopolitical tensions have elevated government focus on the national security impacts from attacks on utility systems.

Over the past couple of years, there has been considerable public private partnership activity – from the White House 100 Day Initiative, from TSA Security Directives, to joint collaborative environment developments. Add in legislation on Capitol Hill and regulatory developments at the federal and state level, and it becomes a tremendous amount of activity that impacts business plans, investment decisions, and security priorities.

During this session, Xcel Energy's Security and Resilience Policy Area Vice President will share information regarding current government policies, interests, and trends, utility efforts to support those activities, and how suppliers and asset owners are working together to reduce risk. Attendees will learn how they can help shape these activities in order to enhance our collective, strategic path forward in protecting critical infrastructure from all hazards.

Magic Kingdom Ballroom

10:00 - 10:30 **Understanding Why Geopolitical Risk Matters**

FORTRESS
Critical Infrastructure. Secured.

Tobias Whitney, Fortress Information Security

The shifting geopolitical landscape creates additional risks and threats that can impact business continuity. Geopolitical risks include political upheaval, economic instability, corruption, natural disasters and wars. How do you determine the degree to which they pose a threat to business continuity? Which of your suppliers have manufacturing and other physical locations, ownership, or even cyber presence in the affected countries or regions? How do you respond to them? How do you prepare for compliance regulations emerging in reaction to them? How do you digest the data you have and present it in a way that is actionable for your organization's stakeholders and leadership?

Expo Hall

10:30 - 11:00 **Networking Break**

Enjoy coffee and tea served in the expo hall.

Detailed Schedule

Day 3 - Wednesday July 20, 2022

Magic Kingdom Ballroom

11:00 - 11:30

Engineering vs Cybersecurity - Advanced OT Risk Management

Andrew Ginter, Waterfall Security Solutions

To keep a boiler from blowing up in your face, which would you prefer? A longer password for the PLC? Or a spring-loaded over-pressure valve? And - if a cyber attack works once, and exactly the same attack is launched at exactly the same target a second time, will it work again? If attacks are deterministic, then what, really, does "likelihood" mean in our cyber risk matrices? OT cyber risk management is maturing as a discipline - likelihood is going away, and eliminating consequences and attack vectors entirely is becoming easier to justify than a continuous spend on cybersecurity . "Due care" expectations from insurance providers are following suit. Join us to look at how our industry is evolving - both in terms of understanding risk and of doing something about it.

Magic Kingdom Ballroom

11:30 - 12:00

Energy Sector Threat Landscape and Recent Lessons Learned from the Field

Dr. Jacob Benjamin, Dragos, Inc.

Dr. Jacob Benjamin will provide an update on emerging cyber threats to the energy sector and industrial control systems. The session will discuss threat activity groups targeting the energy sector and recent lessons learned from the front lines of service engagements in the energy sector.

Adventure Lawn

12:00 - 1:15

Catered Lunch

Magic Kingdom Ballroom

1:15 - 1:45

Building an Exercise Program that Sticks

Nick Weber, Archer

Have you struggled with building and sticking to an effective exercise routine? Ever wanted to participate in a large coordinated exercise like GridEx but didn't know where to start? Join Nick Weber as he walks attendees through tried and true tactics to developing a holistic security exercise program that will challenge participants and drive visible results in your security program.

Too often security response and recovery exercises rely on notional components, rehash the same scenarios, only work in a vacuum, and leave participants more confused than they started. A well-planned security program includes a variety of exercise type, scope, and duration with capability-driven scenarios and objectives. Nick will lay out the foundation for this program and discuss ways to take your exercises from a "necessary evil" to a critical value adding component of your security program. - You'll leave this session with the knowledge and tools to make your security exercise the next "can't miss" event!

Magic Kingdom Ballroom

1:45 - 3:15

Townhall Discussion - A Look Ahead
Closing Comments & Final Prize Drawing

"See you real soon!" - Mickey Mouse

FORTRESS

Discover, prioritize, and monitor cyber supply chain risk.

A2V Data Exchange

Discover, prioritize, and monitor third-party risks.

Cyber Risk Management

Manage your entire ecosystem OT and IT vendors.

Tools & Services

Access a complete toolkit of supply chain risk solutions.

Stop by and visit us at booth #202

Platinum Sponsor

NETWORK PERCEPTION

www.network-perception.com

Booth # 203

Since 2014, Network Perception has set the standard for best-in-class OT network cybersecurity audit and compliance solutions. With intuitive, mapping-centric visualization and independent verification for network segmentation, Network Perception instantly and safely ensures compliance and protection.

Network Perception's technology platform and products range in functionality from essential network auditing technology to continuous and proactive visualization of OT network vulnerabilities, with the intent of improving network security and heightened cyber resiliency for critical infrastructure companies.

Protect the mission-critical assets we all depend on today. With Network Perception, you know your risk now and always and protect your critical networks.

Gold Sponsors

FORTRESS INFORMATION SECURITY

www.fortressinfosec.com

Booth # 202

Fortress Information Security provides cyber risk management solutions for mission critical supply chains and critical infrastructure including services for vendor risk management, asset risk management, product security, file integrity, procurement, continuous monitoring, assessments, and remediation to support overall zero trust supply chain cyber security and integrity.

Fortress guides complex enterprises to discover, prioritize, and monitor third-party supply chain cyber risks. We are the only company offering software integrated into a customizable platform to manage OT, IT and third-party technology threats into a single end-to-end solution.

WATERFALL SECURITY SOLUTIONS

www.waterfall-security.com

Booth # 201

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable enterprise-wide visibility for operations, with disciplined control. Waterfall products represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases, and protocols in the market.
For more information, visit www.waterfall-security.com.

Silver Sponsors

CIMCOR

www.cimcor.com

Booth # 102

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

Bronze Sponsors

ASSURX

www.assurx.com

Booth # 101

AssurX exists to provide the most configurable, adaptable and easy to use software platform that helps professionals effectively run their daily business. We do this by delivering complete solutions developed with a deep understanding of our clients' needs and an honest dedication to our customers' success. Our vision is to do for businesses what the mobile OS has done for people with a smartphone—keep the enterprise connected, informed, and coordinated. We intend to be the one software platform that empowers professionals to make informed decisions and easily orchestrate evolving business activities based on live intelligence from across the company.

TRIPWIRE

www.tripwire.com

Booth # 301

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. As the pioneers of file integrity monitoring, Tripwire delivers top critical security controls, including asset discovery, secure configuration management, vulnerability and log management.

KEYSIGHT TECHNOLOGIES

www.keysight.com

Booth # 103

Keysight's Network Visibility Solutions (NVS) deliver complete access to both OT and IT networks. Complete, real-time visibility starts with "tapping" networks to capture and copy traffic used in performance and security monitoring, incident response, forensics, and analysis. Keysight's Network Packet Brokers aggregate, process, and deliver traffic data to OT security tools, filtering out traffic not relevant to SCADA security (such as CCTV video over IP traffic). The Vision series of packer brokers and OT security tools can be integrated with security information and event management (SIEM) and other systems to establish automated threat response to indicators of compromise (IoCs). More information is available at www.keysight.com.

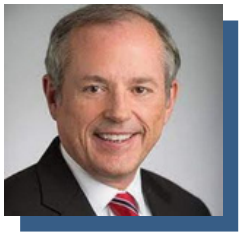
SPEAKERS' BIOGRAPHIES

Industry, Academia, and Experts

Andrew Ginter

VP Industrial Security, Waterfall Security Solutions

At Waterfall, Andrew leads a team of experts who work with the world's most secure industrial enterprises. Before Waterfall, Andrew led the development of industrial control system products, of IT/OT middleware products, and of the world's first industrial SIEM at Industrial Defender. Andrew is the author of two textbooks on industrial security and a co-author of the Industrial Internet Consortium Security Framework. He co-hosts the Industrial Security Podcast, is a lecturer at the Industrial Security Institute, and contributes regularly to industrial security standards and best-practice guidance.



Bill Nelson

Chair, Global Resilience Federation

Bill Nelson is the Chair of the Global Resilience Federation (GRF), a multi-sector non-profit association dedicated to helping ensure the resilience and continuity of organizations against cyber and physical threats, incidents and vulnerabilities. GRF is headquartered in Herndon, Virginia.

At GRF, Nelson has led the growth of information sharing communities within their respective sectors and on a cross-sector basis. This results in faster detection and actionable response and mitigation of those threats. GRF serves many sectors around the world including three communities in the energy sector plus financial services, K12 school districts, manufacturing, law firms, retailers, utilities, operational technology, energy, healthcare, and accounting/consulting firms. Nelson also formed and now serves on the board of the Operational Technology Information Sharing & Analysis Center (OT-ISAC). OT-ISAC's mission is to protect global operational technology assets of multiple sectors including maritime, energy, shipping, manufacturing, and others.

Dan Strachan

Senior Industry Engagement Lead, CISA and JCDC

Dan Strachan has worked at CISA as a Senior Industry Engagement Lead since July, 2021.

Dan's background includes 16 years as Director of Industrial Relations at the American Fuel & Petrochemical Manufacturers (AFPM). At AFPM, Dan helped start and run the association's Cybersecurity Committee, which is one of the best voices in Washington on cybersecurity in the Energy sector. A native of Quincy, Massachusetts, Dan has a BA in Political Science from the University of Central Florida and an MBA from The Johns Hopkins University.

Dennis Skarr

IT Instructor/Industrial Cybersecurity, Everett Community College

Dennis Skarr is tenured faculty at Everett Community College (EvCC) where he teaches Information Technology. Dennis enjoys creating classes for his students which include tabletop and capstone exercises replicating real world experiences in cybersecurity, misinformation, and ethical hacking. His teaching endeavors resulted in receiving the 2019 Exceptional Faculty Award from EvCC. Dennis is currently building an Industrial Security Program for EvCC that includes classes, workshops, and Capture the Flag competitions.

Dennis has an extensive background in performing security assessments on a variety of industrial control systems. While Dennis was with the National Guard he created a two-week training program for cyber operators to receive special qualifications for missions involving cyber-physical systems. Dennis spent over 10 years performing assessments for the National Guard on critical systems that included building automation systems, electrical utilities, and voting systems. In 2016, Dennis' work at the Guard contributed to US Secretary of Defense Ash Carter visiting his unit for a briefing on their capabilities and achievements.

Emma Stewart

Chief Scientist, NRECA

Emma Stewart, Ph.D. is chief scientist of the National Rural Electric Cooperative Association (NRECA) where she works to expand the leadership of NRECA and electric co-ops in the scientific and engineering communities. She leads the Business & Technology Strategies team to further advance research into grid resilience and reliability, transmission and distribution, cybersecurity and more.

Dr. Stewart most recently served as Associate Program Leader, Defense Infrastructure, at Lawrence Livermore National Laboratory in California. She also managed the Grid Integration Group at Lawrence Berkeley National Laboratory, led the distribution planning, modeling and analysis consulting group at BEW Engineering, a DNV Company, and performed research on hydrogen fuel cells and other hydrogen programs at Sandia National Laboratory. She earned her Ph.D. in Electrical Engineering and Master of Engineering degree from the University of Strathclyde, Glasgow, Scotland.

SPEAKERS' BIOGRAPHIES

Industry, Academia, and Experts

Dr. Jacob Benjamin

Director of Professional Services, Dragos, Inc.

Jacob Benjamin is Director of Professional Services, at the industrial cyber security company Dragos, Inc. Prior to joining Dragos, Dr. Benjamin was a cybersecurity researcher at Idaho National Laboratory and a cybersecurity specialist for Duke Energy. Jacob has substantial cybersecurity experience with operational technology at domestic and international critical infrastructures.

Jessica Boersma

K-12 Cybersecurity Educational Development, Argonne National Laboratory

Ms. Jessica Boersma received her bachelor's of science degree from St. Xavier University in 2009. She has held positions working in a special education classroom as well as in elementary education. For the past eight years, she has been teaching 2nd grade at Maya Angelou Elementary in Harvey, IL and has received her Special Education endorsement from Governors State University. She currently supports K-12 cybersecurity educational development for Argonne National Laboratory and co-owns her own K-12 cybersecurity education company.

Justin Quevedo

Engineer
Tacoma Power

Justin Quevedo has worked for Tacoma Public Utilities for 20 years supporting operation control systems including Automated Metering and Energy Management Systems. Justin is a key contributor to the development and execution of Tacoma Public Utilities' CIP program in the areas of security configuration and change management.

Kylie McClanahan

PhD Student, University of Arkansas

Kylie McClanahan is a doctoral student in the Computer Science and Computer Engineering department at the University of Arkansas and a senior developer for Bastazo, Inc.; she holds a BS in physics and a BS in computer science. Her graduate work centers on the cybersecurity of critical infrastructure, including projects funded by NSF and DOE. Her research explores the automation of vulnerability analysis and remediation, drawing from her knowledge of machine learning and her professional experience with CIP compliance processes.

Karl Perman

EnergySec Board Member

Mr. Perman has held security leadership positions in the energy sector including Exelon Corporation and Southern California Edison. Karl developed a security practice during his service as the first Director of Security for the North American Transmission Forum. He served in law enforcement roles at the municipal and federal levels prior to entering the private sector. He also served in military intelligence and military police units in the U. S. Army Reserves. Mr. Perman has a Master's Degree in Public Safety Administration from Lewis University and a Bachelor's Degree in Public Law and Government from Eastern Michigan University.

Manuel Maestas

Software Analyst, Idaho National Laboratory - Critical Infrastructure Protection & Resilience

Manuel is a software analyst for Critical Infrastructure Protection & Resilience at Idaho National Laboratory. Participating in his first EnergySec Summit, he will be presenting his research on automating and codifying attack surfaces by expressing them in Structured Threat Information Expression (STIX) and utilizing Structured Threat Information Graph (STIG) and Auto Discover, open-source tools.

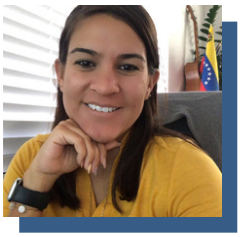
SPEAKERS' BIOGRAPHIES

Industry, Academia, and Experts

Manny Vazquez

Critical Infrastructure Security Researcher, Idaho National Laboratory - Critical Infrastructure Protection and Resiliency

Previous EnergySec 2021 presenter, Manuel Vazquez graduated with a BS in Information Systems and Technology with a minor in Computer Science from California State University, San Bernardino in 2020. He has since worked with Idaho National Laboratory finding ways that can help protect critical infrastructure through research in machine learning, securing software and analyzing binaries. Manuel has experience conducting tests on systems that have an impact on our daily lives. This includes scanning and enumerating networks, devices, services and generating STIX 2 (Structured Threat Information Expression)/JSON (JavaScript Object Notation) bundles that can depict information that make it easy for security experts to understand.



Mariam Coladonato

Sr. Cybersecurity Product Specialist, Phoenix Contact

Mariam Coladonato from Phoenix Contact has over 10 years of experience in OT/ICS Cybersecurity with a dedicated focus around industrial networking and defensive controls. She is blue team engineer by experience and heart, her motto is “prevention the gold standard of security, detection and remediation are equally important to overall defense capabilities for any industry”. Mariam is the technical liaison, SME for all things cybersecurity within an industrial, electronic and automation manufacturer. Her day-to-day consists in competition analysis, understanding market needs, providing valuable input to R&D that creates future roadmaps, creating documentations, articles, and security best practices for most of the networking technology available. Additionally, Mariam is the main point of contact for technical support, pre-post sales cybersecurity opportunities and conversations where the needs for basic assessments, secure network design, recommendations and best practices are needed, either by following industry standards like NERC CIP, ISA/IEC62443, NIST 800-82, NIST CSF or internal security policies. The mission and vision statement for industrial cybersecurity is to collaborate with any interested party and be able to implement best solution and remediation strategy that will meet the client's expectations and satisfaction.

Nathaniel Evans

Program Lead, Cybersecurity Research, Argonne National Laboratory

Nate Evans is the Cybersecurity Program Lead for Argonne National Laboratory’s Strategic Security Sciences Division. He also serves as a Vector Lead in Cybersecurity for Argonne’s National Security Programs. Prior to joining Argonne, Nate managed cybersecurity and cyber defense activities at several private-sector companies. He is considered a key asset by the Department of Homeland Security (DHS) for the development of a cybersecurity vulnerability assessment for field use, analysis of cybersecurity consequence and threat studies, and leading the pilot cyber-physical regional assessment. Evans was involved in the development of a patented, R&D 100 award winning operational instance of moving target defense (MTD), and has worked in a variety of other cybersecurity research areas, including transportation, satellite communications, social engineering, workforce development and offensive cybersecurity. He has taught computer networking and cybersecurity issues to students in Senegal, Africa, through the African Institute for Mathematical Sciences (AIMS) Next Einstein Initiative and is an adjunct professor at University of Chicago and Moraine Valley Community College. He also led the development of DOE’s CyberForce Competition™, drawing college students from across the Nation, in the defense of realistic attacks on simulated critical infrastructure. Dr. Evans received a B.S. in Computer Engineering and a Ph.D. in Computer Engineering with a specialty in Cybersecurity from Iowa State University.

Nick Weber

Managing Partner, Archer

Nicholas (Nick) Weber is a seasoned security leader who has been in military and security leadership roles since 2002. He is a Critical Infrastructure Protection (CIP) professional who has held a Top Secret/Secret Compartmentalized Information (TS/SCI) Clearance. He has served in physical and cyber security management roles at Grant Public Utility District, Western Electricity Coordinating Council (WECC), the US Department of Homeland Security, and the US Army. He has been recognized for his leadership with accolades such as the Security Systems News 20 Under 40 award and the Bronze Star Medal.

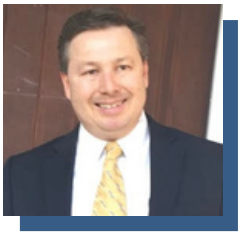
SPEAKERS' BIOGRAPHIES

Industry, Academia, and Experts

Robin Berthier

CEO & Co-Founder, Network Perception

Dr Robin Berthier is the co-founder and CEO of Network Perception. He has over 15 years of experience in the design and development of network security technologies. He was part of the University of Illinois research team that originally developed the technology that drives the Network Perception platform. He received his PhD in the field of cybersecurity from the University of Maryland College Park before joining the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign (UIUC) as a Research Scientist.



Ralph Ising

Sales Manager, Cimcor

For 30+ years Ralph has been a trusted adviser to executives across multiple industries worldwide helping them leverage innovative and disruptive technologies to lower costs, mitigate risk, and improve stakeholder value. For the last 3 1/2 years, Ralph has been responsible for direct sales, channel sales, and government sales worldwide for all of Cimcor's Cyber Security & Compliance Products.

Sharla Artz

Security and Resilience Policy AVP, Xcel Energy

Sharla Artz serves as the Security and Resilience Policy Area Vice President where she works with utilities, government partners, and industry stakeholders to develop policies that enhance the resilience of critical infrastructures. Previously, she served as the Senior Vice President of Government & External Affairs at the Utilities Technology Council, where she focused on bringing attention to cross sector interdependencies in critical infrastructure protection efforts. Ms. Artz was formerly the Director of Government Affairs at Schweitzer Engineering Laboratories, Inc. (SEL), where she established close working relationships with government officials, contributed insight for sound policy decision making, and was an advocate on the role of technology in grid resilience. Prior to joining SEL, Ms. Artz was the vice president of legal and government affairs for Genscape, Inc., developing business relationships for the company with federal entities. SMs. Artz was the assistant general counsel for the National Association of Regulatory Utility Commissioners, serving the 50 state utility commissioners on energy regulatory matters pending before the federal government. *Cont...*

After receiving her juris doctor from Georgetown University Law Center, Ms. Artz spent four years on Capitol Hill, working on energy policy for a former member of the House Energy and Commerce Committee. Ms. Artz has a bachelor's degree in sociology and psychology from the University of Tulsa, Oklahoma. She lives in Alexandria, Virginia, with her husband and two children.

Tobias Whitney

VP of Strategy and Policy, Fortress Information Security

Tobias Whitney is a recognized leader in control systems security solutions with over 20 years of critical infrastructure security experience. For six years, Whitney led the compliance and standards for NERC's Critical Infrastructure Protection program. Most recently, Whitney spent two years as Technical Executive at the Electric Power Research Institute (EPRI), evaluating risks in supply chain cybersecurity for utilities, developing solutions to address security architecture for utility cloud-based solutions, as well as researching emerging technologies, such as electric vehicle charging and supply chain security.

Wally Magda

Senior Standards Instructor & Advisor, WallyDotBiz LLC

Wally Magda brings his passion and energy to the Summit as an internationally recognized security expert for Industrial Control Systems (ICS). His deep security experience spans military nuclear missile command and control systems, intelligence agencies, enterprise security and industrial control systems. Wally's involvement with the NERC CIP standards goes back to the Urgent Action Cyber Security standards of 2003. As a former WECC NERC CIP auditor he has performed over 100 NERC CIP on and off site audits in the roles of Audit Team Lead and team member. He started out in the utility business from the ground up as an Instrumentation, Control and Electrical Tech. He then progressed to managing ICS as a process control engineer. Seeing the need for experienced security professionals to assist Information, Operations and Physical Technology business units, he stepped into the enterprise level security realm. Wally is an active member of the NERC Supply Chain Working Group and Security Integration and Technology Enablement Subcommittee. He holds several professional certifications including ISA Certified Automation Professional (CAP), SANS GIAC Global Industrial Cyber Security Professional (GICSP), ASIS Physical Security Professional (PSP), ISC2 Certified Information Systems Security Professional (CISSP) and ISACA Certified Information Systems Auditor (CISA).

Secure Power Systems Cybersecurity Technician

Why Cybersecurity Technician?

Total job postings in 2020: 8,919*
Average Starting Salary: $78,200*
Median Salary: $83,200*

*Burning Glass and CompTiaTech statistics

What is a Secure Power Systems Cybersecurity Technician?

This is the first of several Secure Power Systems job roles being developed to train incumbent workers to become Secure Power Systems Professionals.

Technician - a person skilled in the practical application of work processes related to technical equipment

Cybersecurity - Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks.

Power Systems - the electric grid, a vital part of our critical infrastructure

Secure Power Systems Cybersecurity Technician - A technician with cybersecurity skills and related knowledge specific to the needs of electric power generation, transmission, and distribution operations.

Why EnergySec?

Deep industry experience *which provides decades of collective security experience in security roles within the energy sector.*

Independent, Non profit. *Our purpose has always been to serve industry. Our apprentice program is designed to further our mission of assisting industry to secure its critical systems.*

National breadth. *As a national organization, we can execute a nationwide workforce development program, including apprenticeships, to benefit the entire industry.*

Cybersecurity is our mission. *Our apprenticeship program is central to our one mission: security.*

We've already started. *As an intermediary, EnergySec is working with employers to implement the Secure Power Systems Cybersecurity Technician throughout the industry. We are in the process of registering our apprenticeship as a national program.*

Reasons to Not Participate:

- *I already have a job.* *Great! Let's use those skills to advance your position!*
- *I'm too old to start as an apprentice.* *Apprenticeship doesn't mean starting over. You are adding to the skills you already possess.*
- *I'm happy where I'm at.* *Great! But learning brings earning benefits!*

Why should I do this program?

The program will prepare you to move up the career ladder into cybersecurity positions with greater responsibility and higher compensation. You will gain skills and knowledge that can be applied to current roles and increase the security and protection of the electric sector.

How long does the program last?

This is a competency-based program. You may already have some of the skills required so you can advance through the program as quickly as your skills and time allow. For IT-centric workers, we provide OT courses and OJT that is directly related to your utility's operational technology. For OT-centric workers, we provide IT courses and OJT to understand your IT environment.

How do I join the program?

Express an interest to your employer through your supervisor or human resources department.
Complete the online registration form.
EnergySec will secure an Employer Agreement form with your utility and facilitate your training with an onsite mentor .
EnergySec will track your progress to completion of the program.

Scan the QR code to be directed to our sign-up page

or visit www.energysec.org.

EnergySec
SECURING CRITICAL INFRASTRUCTURE

CompTIA
Apprenticeships for Tech

Secure Power Systems Cybersecurity Technician Apprenticeship Opportunity

EnergySec has been talking workforce development… and now we are delivering what we promised — a cybersecurity apprenticeship specifically designed for the electric sector. Based on the PNNL Secure Power Systems research, we have combined IT and OT components to create a unique program for utilities, large or small, to use to train an ever-growing need for talent in our industry.

Why should we participate as an organization?

- Develop a highly-skilled tech workforce
- Diversify your talent pipeline
- Amplify employee engagement and retention
- Increase productivity and deliver better results
- It's time— think Capacity Building - you have staff — use the program to train them for future cybersecurity openings. Start now.

Why EnergySec?

Deep industry experience *which provides decades of collective security experience in security roles within the energy sector.*

Independent, Non profit. *Our purpose has always been to serve industry. Our apprentice program is designed to further our mission of assisting industry to secure its critical systems.*

National breadth. *As a national organization, we can execute a nationwide workforce development program , including apprenticeships, to benefit the entire industry.*

Cybersecurity is our mission. *Our apprenticeship program is central to our one mission: security.*

We've already started. *We are in the process of registering our apprenticeship as a national program.*

We are partnering with CompTia. *This partnership aligns our apprenticeship to the National Standards that are approved through the Department of Labor. It also provides discounts to apprentices who wish to obtain CompTia certifications.*

A tech apprenticeship?

Why not? Utilities have apprentices for linemen, relay technicians, substation operators, etc. The model is there because it works! Imagine passing on the technical knowledge of your senior staff to your technical apprentices—knowledge of your specific needs can be directly passed on through mentorship. The work-as-you-learn model gives the employer the immediate benefit of a skilled employee.

Why EnergySec as an intermediary?

We can:

- Help you fast-track your program
- Build and deliver your training program
- Sponsor apprentices and assist with administration and reporting requirements.
- Assume responsibility for apprentices' success

Apprenticeships are *not*…

Limited to the construction or manufacturing trades or only for big companies.

How do I get started?

Complete an Employer Agreement Form.
Identify interested staff.
Enroll staff through EnergySec into the program.

Scan the QR code to be directed to our sign-up page

or visit www.energysec.org.

EnergySec
SECURING CRITICAL INFRASTRUCTURE

CompTIA
Apprenticeships for Tech

“It's kind of fun to do the impossible.” —Walt Disney

Not a part of our Community?

To join our community, go to energysec.org and register under the tab - Join our Community. Start enjoying the benefits of Community today!

www.energysec.org