5th Annual

March 21-22, 2023 • Chicago

Utility Cyber Security Forum

www.utilitycybersec.com

Organized by: SGO Smart Grid Observer

Organized by the Smart Grid Observer, the **5th Utility Cyber Security Forum 2023,** March 21-22, 2023 in Chicago is an in-depth information sharing program intended for cyber security utility executives, strategists and practitioners. Key technology advances, regulatory requirements, and success strategies for effectively dealing with cyber security threats will be examined through a series of presentations and panel discussions. Ample time is reserved for one-on-one discussions with industry thought leaders and executives who are at the forefront of utility cyber security advances.

Topics to be Addressed Include:

- Implementing digital security in a utility environment
- Adapting cybersecurity to OT environments
- Bridging the IT / OT divide
- Protecting substations and distribution and transmission infrastructure from cyber attacks
- Dealing with advanced persistent threats that exploit flaws in industrial control systems
- Cyber security for operational technologies and smart systems
- Ensuring grid SCADA and PLC grid control networks cyber security
- What works, what doesn't, and what to put in place
- Next-gen technology advances for industrial control systems security
- The state of silicon-based cybersecurity functionalities for utilities
- Securing 'brownfield' devices
- Best practices in reducing human sources of vulnerability
- Managing cyber security challenges introduced by distributed energy resources

"The topics and speakers chosen are very relevant to what is happening in the industry. In fact, the presentations contents are state of the art. The conference is able to attract the utilities, which is always a challenge. Everything went well. "

- Ramesh Reddi, CTO, CybSecBCML, Inc

Platinum Sponsors:

Acronis INTEL471 network perception element matrix

Gold Sponsors: txOne networks DIRECTDEFENSE bpm ONAPSIS DARKTRACE

Silver Sponsors: POLYSWARM XONA

Participating Organizations Include:

AlertEnterprise
Annaba University | UBMA, Algeria
Arizona Public Service Company
Awesense
BC Hydro
Blockchain Engineering Council (BEC)
Bonneville Power Authority
Calpine
Citrix
Cleco Corporation
Control Infotech Pvt Ltd
Cordoba Corporation
CPS Energy
CybSecBCML, Inc.
Dispersive Networks
Doyon Utilities, LLC
Dragos, Inc.
Duke Energy
DynTek
EDF Renewables
Edison Electric Institute
Electric Power Research Institute
Exclusive Networks
Exelon Corporation
Finite State
Fortinet
GridBright
Guardtime Energy
Guernsey
Guidehouse Insights
Illinois Commerce Commission
IncSys
Indegy
JPEmbedded LLC
JSC Institute of Information Technology
Kent Power
LADWP
Lea County Electric Cooperative, Inc.
McAfee
Microsoft
Midcontinent ISO
MITRE Corporation
National Cybersecurity Center of Excellence, NIST
NES
Network Perception
Nevermore Security
Northern Indiana Public Service Co.
Norwegian University of Science and Technology (NTNU)
Nozomi Networks
NRG Energy
OASD HD&GS, Office of the Principal Cyber Advisor
OMICRON Electronics
OPSWAT
Pacific Gas and Electric
Pacific Northwest National Laboratory
POWER Engineers
Protect Our Power
Public Service Electric & Gas Company (PSE&G)
Puget Sound Energy
Pyramid Security Advisors
Quadra Applications & Technology
Resilience
RSI Security
S&C Electric Company
Sandia National Laboratory
Sargent & Lundy
Schweitzer Engineering Laboratories
Sempra / SDGE / SoCalGas
Southern California Edison
Southern Company
Synack
Tenable
The CSA Group
The Market Connection
Transformer Protector Corp.
Tri-County Electric Cooperative
Vectren Energy
West Monroe Partners
West Wing Advisory Services
XONA
XTec Inc.

Job Titles:

Regional Sales Manager
Co-Founder
CEO
Global Enablement Engineer
Associate Professor of Energy
Engineering Manager
Engineer IV
Senior Cybersecurity Analyst
IT Infrastructure Manager
IT Manager
Technical Team Lead
Energy Cybersecurity
Research Engineer, Cyber Systems
Senior Security Architect
Director, Cybersecurity
Principal Product Manager
Executive Assistant
System Operations Manager
Director, IT
Senior Research Analyst
Consultant Substation Automation Engineer
Cybersecurity Architect - IoT
Senior Manager, Cybersecurity
Head of Business Development Power Utility Communication
Chief Cybersecurity Specialist
Application Engineer
Account Manager
Manager, Cyber Security Ops
Manager, Utility of the Future
IT Governance/ Enterprise Architecture Manager
VP, Technology Services
Senior Research Scientist
President
Manager Communications/IT
Senior Cyber Security Advisor
Senior Engineer
Manager, Real-Time Systems Security Engineering
VP-Power System Solutions
Sr. Director Product Dev
AI/ML Data Scientist
Cyber Defense Analyst
Solutions Architect
Manager - PdM & Performance Engineering

Sponsorship Packages

Platinum Level Sponsor

Value: $5,000

- Top-level logo recognition as Platinum-Level Sponsor
- Speaking slot on panel session or stand-alone
- Tabletop exhibit in networking break and reception area
- Booth in Virtual Exhibit – available 24/7/365
- 4 complimentary conference passes
- 25% off additional registrations
- Top logo positioning in Official Program Guide, event website, and email communications
- White paper or press release posted on event website, and in Smart Grid Observer
- Corporate description with hyperlink on event website
- Banner ad on SGO website for three months
- Top positioning of logo in on-site banners and signage
- Dedicated floor-standing banner (provided by sponsor)
- Company information or insert included in registration portfolios distributed to all attendees
- Attendee List provided one week prior to, and following the event

Gold Level Sponsor

Value: $4,000

- Logo recognition as Gold-Level Sponsor
- Tabletop exhibit in networking break and reception area
- Booth in Virtual Exhibit – available 24/7/365
- 3 complimentary conference passes
- 20% off additional registrations
- Top logo positioning in Official Program Guide, event website, and email communications
- Corporate description with hyperlink on event website
- Logo in on-site banners and signage
- Dedicated floor-standing banner (provided by sponsor)
- Company information or insert included in registration portfolios distributed to all attendees
- Attendee List provided one week prior to, and following the event

Silver-Level Sponsor

Value: $2,500

- Logo recognition as Silver-Level Sponsor
- Booth in Virtual Exhibit – available 24/7/365
- 2 complimentary conference pass
- 15% off additional registrations
- Logo positioning in Official Program Guide, event website, and email communications
- Corporate description with hyperlink on event website
- Logo positioning in on-site banners and signage
- Dedicated floor-standing banner (provided by sponsor)
- Attendee List provided one week prior to, and following the event

Bronze-Level Sponsor

Value: $1,500

- Logo recognition as Bronze-Level Sponsor
- 1 complimentary conference pass
- 10% off additional registrations
- Logo positioning in Official Program Guide and event website
- Corporate description with hyperlink on event website
- Logo recognition in on-site banners and signage

Platinum Sponsors

Network Perception was launched at the University of Illinois at Urbana-Champaign Research Park. Founded by a team of experts on network security and critical infrastructure protection, Network Perception delivers a pioneering solution that enables corporate compliance and cyber security managers to gain a complete view of their network security and to immediately determine if its configuration is in alignment with best practices and regulatory standards.

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT Professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus , backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment-from cloud to hybrid to on premises-at a low and predictable cost. Visit www.acronis.com

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using near-real-time insights into the latest malicious actors, relationships, threat patterns, and imminent attacks relevant to their businesses. The company's TITAN platform collects, interprets, structures, and validates human-led, automation-enhanced results. Clients across the globe leverage this threat intelligence with our proprietary framework to map the criminal underground, zero in on key activity, and align their resources and reporting to business requirements. Intel 471 serves as a trusted advisor to security teams, offering ongoing trend analysis and supporting your use of the platform. Learn more at https://intel471.com/.

We believe people should be able to talk, via the internet, with the same level of privacy as a face-to-face conversation in their own home. Building on the Matrix open standard for decentralized communication, we enable anyone to talk with everyone. No walled gardens, no vendor lock-in. We've created a unique system that combines true end-to-end encryption, cross-signed device verification, an open decentralized network and digital self-sovereignty. We're in our element developing it; we hope you're in your element using it. Visit www.element.io

Gold Sponsors

TXOne Networks offers cybersecurity solutions that ensure the reliability and safety of industrial control systems and operational technology environments through the OT zero trust methodology. At TXOne Networks, we work together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. TXOne Networks offers both network-based and endpoint-based products to secure the OT network and mission-critical devices in a real-time defense-in-depth manner. Visit www.txone.com

Onapsis protects the business applications that run the global economy. The Onapsis Platform uniquely delivers vulnerability management, threat detection and response, change assurance, and continuous compliance for business-critical applications from leading vendors such as SAP, Oracle, and others. The Onapsis Platform is powered by the Onapsis Research Labs, the team responsible for the discovery and mitigation of more than 1,000 zero-day vulnerabilities in business-critical applications. Visit www.onapsis.com

DirectDefense is an information security services company that provides enterprise risk assessments, 24/7 managed services, penetration testing, and ICS/SCADA security services. Headquartered in Englewood, CO, with locations across the United States, we implement best-practice security programs that elevate our customers' security posture to a higher standard of protection and resiliency. Founded in 2012 on more than 50 years of combined experience in information security, DirectDefense provides continuous security solutions and managed services that help businesses and organizations protect their data and critical infrastructures against the most advanced threats and adversaries. Visit www.directdefense.com

BPM's CyberSecurity Assessment Services is an assessment-only team of offensive security experts, offering an independent perspective to our clients through exercises such as penetration testing, incident assessment, and related security assessment services. For over 20 years we have been performing penetration tests, and through that experience we understand the risks and challenges that modern organizations face. We have seen how the value of information security is often only recognized after a breach or incident has impacted a business's bottom line, and we work with our clients to proactively reduce their level of risk for costly attacks. Our reports are designed to provide stakeholders and system administrators with key information that will allow them to prioritize and mitigate risk effectively. Visit www.bpm.com/cybersecurity

Darktrace, a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Breakthrough innovations from the Darktrace Cyber AI Research Centre in Cambridge, UK and its R&D centre in The Hague, The Netherlands have resulted in over 125 patent applications filed and significant research published to contribute to the cyber security community. Darktrace's technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Visit www.darktrace.com

Silver Sponsors

Tap into PolySwarm's next-generation malware intelligence marketplace and get better, fresher insight faster. Cut through extraneous data and noise to detect, analyze, and respond to critical threats before they make an impact. Visit polyswarm.io

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and Zero Trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. Visit www.xonasystems.com

About the Organizer

The Smart Grid Observer is an online information portal and weekly e-newsletter serving the global smart energy industry. SGO delivers the latest news and information on a daily basis concerning key technology developments, deployment updates, standards work, business issues, and market trends worldwide. The publication serves a global readership of executives and practitioners in the electric power generation, transmission, and distribution industry. For a free subscription, visit www.smartgridobserver.com

Agenda

Tuesday, March 21, 2023

8:00 - 9:00 am

Welcome Coffee and Registration

9:00 - 10:00 am

Understanding the Impacts of Real-time Isolation and Empowering its Execution

Recent international conflicts and cybersecurity events have pushed utilities to bolster their response plans including procedures for isolating critical real-time systems. Confidence is critical during a cyber event. Teams must be confident in their actions, in their support, and in their responsibilities for continued operations. Newly mandated cybersecurity requirements for real-time systems, including recent TSA directives, have included language around developing isolation procedures and governance. This session will showcase how Exelon is going a step beyond defining the architecture, impacted systems, and needed steps for isolating real-time systems. IT, Cybersecurity, and Business leads across Exelon's utilities are working together to map out the downstream processes, and day-to-day operations that will be impacted during an isolation event in order to better plan and raise confidence in their team's response.

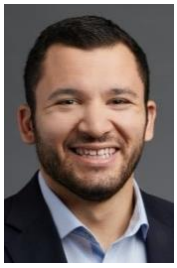
Key Takeaways:

- How to take proactive cybersecurity measures to protect utility real-time systems
- Why documentation and socialization of IT and business impacts of real-time isolation is important
- Which isolation governance procedures are needed to empower the proper stakeholders to make critical decisions around isolation

Theodore Johnson
IT Director - Real-Time Operations: SCADA, OMS, OT Cyber Security
Exelon
profile

Ryan Hoover
Principal IT Architect, Real-Time Systems
Exelon
profile

David Bower
Senior Manager IT
Exelon
profile



Michael Feula
Senior Consultant, Energy and Utilities Practice
West Monroe
profile

10:00 - 10:30 am

How to Survive a Penetration Test of an OT Network

Penetration tests provide an organization valuable insight into vulnerability exposure as well as a metric to quantify risk for an organization; however, penetration testing actions themselves can pose risk to even a mature network. Denial of service conditions can occur when basic systems get taken offline due to testing, such as phones not working, printers failing, and network outages, all due to standard penetration testing methods. Many Operational Technology (OT) networks running critical industrial control infrastructure never undergo a penetration test for fear of causing these types of service outages. Take the plunge, learn how to safely traverse the penetration testing process and understand the vulnerabilities and consequent risk associated with an OT network running critical infrastructure. Hear firsthand experiences of complete OT network penetration tests including initial scoping, establishing rules of engagement, active testing of OT infrastructure, reporting and more.

- Josh Schmidt, Director - Cyber Security Assessment Services, **BPM**
- Ryan Ferran, SCADA Penetration Test Team Lead, **BPM**

10:30 - 11:00 am

Networking Coffee Break

11:00 - 11:30 am

Five Steps Utilities Can Take to Defend Against Evolving Cyberthreats

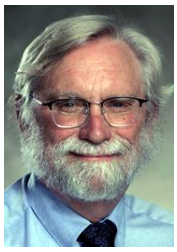
Utilities and other critical infrastructure operators are juicy targets for various cyber attackers, from hostile nation-states and their proxies to organized cybercrime gangs to malicious insiders. It's a full-time job to keep up with their evolving tactics to steal sensitive data, lock up critical systems for ransom, or just wreak general havoc for geopolitical ends. This session will examine the evolving cyberthreat landscape for utilities and explore the five proactive steps you can take to mitigate the impact of successful attacks on your critical systems and prevent them from happening in the first place.

Stephen Nichols
Director - Solutions Engineering, NAM
Acronis
profile

11:30 - 12:30 pm

Trusted Networking in Energy Systems

This session will cover topics related to how advanced networking support can be applied in the context of energy systems, such as substations and control systems. Technologies of particular interest and discussion include software-defined-networking, transparent and automated establishment of trust among devices, and network services with mathematically proven properties.



Prof. David M. Nicol
Director, Information Trust Institute
Herman M. Dieckamp Endowed Chair in Engineering
University of Illinois at Urbana-Champaign
profile

Sachin Shetty
Associate Director and Associate Professor, Virginia Modeling, Analysis and Simulation Center
Old Dominion University
profile

Philip Huff
Assistant Professor and Research Fellow, Emerging Analytics Center
University of Arkansas at Little Rock
profile

Dr. Atul Bohara
Research Engineer
Network Perception
profile

12:30 - 1:30 pm
Lunch Break

1:30 - 2:00 pm
Uncovering the Ugly Truth of OT Cybersecurity

The modernization of operational technology (OT) has brought about significant challenges. There's the complexity of securing these assets as connectivity increases, but there are also operational challenges unique to OT environments. This session will focus on use cases that deal with some of the most prevalent issues organizations encounter today, such as legacy systems, insecure protocols, and asset availability. Following this session, you'll be able to identify key differences in IT and OT cybersecurity strategies that maintain security defenses while keeping the operation running.

Jim Montgomery
Principal Solution Architect
TXOne Networks
profile

2:00 - 2:30 pm

The New TSO: Transforming Secure Operations

Utilities need secure, mission critical real time communications across their supply chain. Instead they have email which is insecure, brittle and slow. Of course there's Microsoft Teams or Slack; which are insecure and siloed to the point of being unusable across a supply chain. Or the likes of WhatsApp and Signal: free consumer-grade apps with zero corporate oversight and control. This session examines how Big Tech has made it so spectacularly difficult for a supply chain to communicate quickly and securely -- and an open standard for secure, decentralized real time communication designed to address this problem. We will discuss how the US Navy, US Marine Corps and US Space Force are adopting this same open standard and how European Transmission System Operators plan to do the same.

Karl Abbott
Product Manager
Element
profile

2:30 - 3:00 pm

Avoiding VTD's: Are Your Third-Party Vendors Equally as Protected as You?

Security and privacy are everyone's responsibility, but how do we protect our enterprises when we are surrounded by networks, many not our own? It is nearly impossible to run a business today without network interconnectivity. Vendor risk and third-party risk management have become an increasingly important part of any enterprise risk management framework. The larger your organization, the more vendor, supplier, and partner relationships you're likely to have, and the greater your risk. Are you protecting your organization from "vendor-transmitted diseases"?

Key Takeaways:

- Learn the importance and necessity of auditing your vendor security to protect your ecosystem
- Security attacks become more sophisticated each year, and most IT architectures weren't designed to withstand today's sophisticated security threats
- System owners, managed third-party partners, and information-sharing mechanisms are all at risk

Christopher Walcutt
Chief Security Officer
DirectDefense
profile

3:00 - 3:30 pm
Networking Coffee Break

3:30 - 4:00 pm
Exploit-Centric Intelligence Approach

Exploit-centric intelligence approach shifts the focus from adversary precursors to exploitation. The cyber underground ecosystem is a hotbed of pernicious infrastructure framework offerings that break down into illicit products, goods and services enabling threat actors to strategically arm their operations for eventual exploitation. With the evolution and expansion of attack surfaces, intelligence analysts and response teams often struggle to effectively prioritize vulnerabilities discovered in the wild. Without visibility into the cyber underground marketplace, analysts do not have the threat intelligence necessary to predictively analyze threat actors, initial access brokers and RaaS affiliate groups exploits as they leverage commodities to monetize their targeted campaigns. These exploits and productized kits pose significant risk to organizations worldwide, particularly the grave impact a successful cyber attack may have on critical infrastructure when compromised or damaged.

In this discussion, we will cover instances of cybercrime exploitation impacting critical infrastructure targets around the globe. These include initial access and data brokers, hacktivism, ransomware attacks, vulnerabilities and supply chain attacks.

Key Takeaways:

- Adversary precursors to exploitation
- Real-world instances of cybercrime exploitation impacting critical infrastructure targets
- Patch prioritization keys to mitigation and risk reduction

Kris Palmer
Vice President, Intelligence Solutions
Intel 471
profile

4:00 - 4:30 pm

Keep The Lights On: Securing Business-Critical SAP Applications

Recent cyberattacks are a grim reminder that the utilities industry is a vulnerable target for hackers. The interconnection of information networks such as information technology systems and operational technology increases the vulnerability for cyberattacks like ransomware with a strong potential for widespread system outages. Most utilities companies have taken steps to protect their infrastructure, but recent attacks demonstrate that business-critical applications are still vulnerable. This session will examine how a leading gas and electric utility to took familiar security best practices and extended them to their SAP landscape. Key Takeaways:

- Hear why SAP security matters and understand how to reduce and mitigate risk to the business' most important assets
- Learn how you can use security as a tool to manage your business, not as an obstacle
- Gain recommendations for what you should be doing now, short-term, and long-term in regards to your company's digital transformations

Aleck Brailsford
VP Americas Solution Architects
Onapsis
profile

4:30 - 5:00 pm

Leveraging Cyber AI to Increase Cyber Resilience & Reduce Operational Risk

The OT IT convergence point is not just an area located on a network but a living convergence point between the IT directors and OT engineers. Innovative technology strategies enable action to be taken on the IT side of the house and bring a granular level of visibility and protection to the OT side of the house. In the face of skyrocketing cyber risk, organizations must take proactive steps to prevent threats before they happen, and to recover if compromised. In this session, Darktrace unveils an ambitious new approach to security, with core engines powering AI technologies to prevent, detect, respond, and ultimately heal from attacks across all areas of their digital environment. Together, these engines combine to strengthen utilities' security posture in a virtuous AI feedback 'loop,' which provides powerful end-to-end, bespoke, and self-learning solutions unique to each organization.

Joseph O'Shei
Director of Critical Infrastructure
Darktrace
profile

5:00 - 6:30 pm

Networking Drink Reception at Monk's Pub

Wednesday, March 22, 2023

8:00 - 9:00 am

Morning Coffee

Note: Attendance at any of the workshops is included in registration fee

ROOM A

9:00 - 11:00 am

Workshop: Network Cyber Hygiene to Strengthen Resiliency

Learning objectives:

1. Foundational knowledge of networking concepts, firewalls, and risks
2. Step-by-step cyber hygiene workflow and technology to verify firewall policies
3. Most frequent firewall policy risks and how to prevent them
4. Clear understanding of NERC CIP requirements: CIP-003 and CIP-005

Description:

The size and complexity of networks that are providing connectivity to the bulk electric system keep increasing. Protecting mission-critical assets requires constant vigilance and a robust cyber hygiene workflow to ensure that networks are correctly segmented and configured at any point in time. This hands-on workshop will provide the knowledge and technical understanding to build a best-in-class CIP firewall verification workflow as part of network cyber hygiene practice. Attendees will gain a clear understanding of CIP-003 and CIP-005 requirements and learn how to establish an automated and independent policy verification process. Through access to a realistic network environment and the NP-View platform, attendees will be able to practice ruleset review scenarios to learn how to identify and document the most frequent risks, including:

- Lack of egress access control
- Lack of correct justification
- Overly permissive rules and insecure services
- Overly complex access lists

The workshop will also provide step-by-step instructions to prepare clear reports and to measure progress through a set of risk-based cybersecurity and compliance maturity indicators.

Workshop Schedule and Outline:

9:00 - 10:00 am

1. Introduction and training objectives
2. CIP-003 and CIP-005 requirements
3. Networking concepts and how firewalls work
4. Accessing the NP-View training platform

10:00 - 11:00 am

1. Hands-on practice: reviewing firewall access rules
2. Identifying the most frequent firewall policy risks
3. Verifying interactive remote access with path analysis
4. Reporting template and preparing for a NERC CIP audit

Dr. Robin Berthier
CEO
Network Perception
profile

Joseph Baxter
Director, Solutions Engineering
Network Perception
profile

11:00 - 11:30 am
Coffee Break

ROOM A
11:30 am - 1:30 pm
Workshop 2: The Auditor's Perspective

Learning Objectives:

1. Philosophy - Understanding the auditor's restrictions and responsibilities
2. Process - Audit stages, inventories, sampling, data collection, additional requests, etc.
3. Problem - What constitutes quality evidence to sufficiently demonstrate compliance
4. Preference - Clean artifacts, clear evidence, and an exacting culture of compliance

Description:

Create an advantage in every audit by understanding the process, practices, and evidence from the perspective of the auditor. Each entity in the critical infrastructure space understands regulation, but often that understanding does not extend the legal and ethical responsibilities their auditors face to find sufficient evidence of compliance.

This workshop will teach a simple compliance framework, hierarchically down from Program, Policy, Process, Procedure, and Practice. Attendees will complete group strategy exercises, breaking down a single real-world regulatory requirement into a workable and universal process designed to create

compliance artifacts at each stop. Attendees will use their new process to analyze sample procedures created by two fictitious business units, ensuring that each procedure produces all the compliance artifacts required.

With this greater understanding of process and procedural audit, attendees will be able to create an "approval rubric" for use in conjunction with their process. Then, armed with this rubric, the workshop attendees will become the auditors - comparing sample data to the compliance requirement and determining the sufficiency of evidence. Is there evidence of compliance? Or is there a potential non-compliance finding to report?

Workshop Schedule and Outline:

11:30 - 12:30 pm
1. Introduction and Agenda
2. Five-P Compliance Structure
3. Idealized Audit Process - Internal, Independent, External (Regulator)
4. Better Processes Mean Better Compliance
5. Exercise: Example Requirement - CIP-005 Requirement 1.2
6. Accessing the NP-View Training Platform

12:30 - 1:30 pm *(working lunch)*
1. Be the Auditor: Procedures 1 and 2
2. Rubrics Should Be Documented
3. Exercise: Approval Rubric Creation
4. Be the Auditor: Review firewall justifications for quality
5. How to document and discuss audit findings
6. Operationalizing a process in a compliance program

Joseph Baxter
Director, Solutions Engineering
Network Perception
profile

ROOM B
11:30 - 12:45 pm
Supply Chain Cyber Security and NERC CIP-013 Compliance for Electric Utilities

This session will focus on the issues related to cyber securing the supply chains of electrical utilities. Specifically, it will cover the NERC CIP-013 reliability standard and its requirements. The requirements are: Develop, Implement and Continuously Monitor the supply chain cyber security risk management plans for high and medium impact BES Cyber Systems.

Perhaps the biggest cybersecurity risk today is the risk posed by supply chain cyberattacks. SolarWinds and the Log4j attacks are two well-known examples, but there are many more. Software supply chain attacks are at least doubling every year. According to HelpNet Security, "..in 2022, supply chain attacks surpassed the number of malware-based attacks by 40%." Electric utilities are faced with a special challenge, because of their need to comply with NERC CIP-013.

The big challenge of supply chain cybersecurity is that, in principle, the utility has to secure not only its own environment but the environments of all its suppliers of software and intelligent devices. This can be accomplished through an effective risk management program. We will discuss how electrical utilities can implement NERC CIP-013 standard through developing, implementing, and continuously monitoring such a risk management program. However, our methodology will cover full spectrum of supply chain cyber security.

Ramesh Reddi
President and Chief Technology Officer
CybSecBCML, Inc.
profile

Tom Alrich
Principal Consultant
Tom Alrich LLC
profile

12:45 - 1:45 pm
Lunch Break

ROOM A
1:45 pm - 3:45 pm
Workshop 3: Why Two Sides of Visibility Matter More Now Than Ever

Learning Objectives:

1. Philosophy -- How adding network access visibility can bolster your incident response efforts and increase cyber resiliency.
2. Process -- Enhancing Network Visibility, Incident Response Plans, Post Incident, etc.
3. Problem/Solution -- Traditional intrusion detection systems (IDS) may contain visibility gaps from a network access (firewall/router) perspective. Be better equipped to respond to incidents that are detected in your OT networks by enhancing IDS with network access modeling.
4. Take Away - Leveraging network access modeling to enhance your incidence response procedures.

Description:

Our OT network has been breached!!! Do we know where the threat can pivot to next? Is the network correctly segmented? How many steps away from hitting our crown jewels? These are questions that traditional intrusion detection systems have a hard time answering. We may be able to understand what has been compromised and what anomalous behaviors threat actors are exhibiting, however, in order to be resilient to breaches, knowing the answer to these key questions can greatly reduce the risk (and stress) of handling a network incident. How do we accomplish that? By layering in Network Access Modeling.

In this workshop we will go over two complimentary sides of network visibility -- Network Traffic Monitoring & Network Access Modeling -- and how to create strategies and incident response plans around these two to better respond to OT network intrusion incidents and build a more cyber resilient program. A case study will be reviewed on how these two controls could have helped prevent one of the most widely known incidents: The Colonial Pipeline Shutdown.

Attendees will have the opportunity to go through a table top exercise and use Network Access Modeling to be better respond to a theoretical breach and gain a better understanding and appreciation of how the Two Sides of Network Visibility will help your team build resiliency during incidents!

Kes Jecius
Senior Solutions Engineer
Network Perception
profile

David Carmona
Regional Sales Manager
Network Perception
profile

Registration

Includes access to all sessions, lunches, workshops, networking coffee breaks, and drink reception on Tuesday, March 21 and Wednesday, March 22. Also includes presentation PDFs and attendee list.

Standard Rate -- Equipment and software vendors, services providers, consultants	$895.00
Utilities, Academic, Government and Non-Profit Organizations *NOTE: .edu, .gov or .org email address required*	$795.00

Register securely online at

https://www.utilitycybersec.com/register.htm

"Just the right size. Excellent industry participants, excellent speakers, excellent networking."
- Dr. Robin Podmore, President, IncSys

"Well organized and very informative. The panels of experts were well selected. Excellent presentations - well done!"
- Anita Bhat, Principal Member of Technical Staff, Sandia National Laboratories

"Really enjoyed the conversations. The presentations were extremely useful. Very relevant."
- April Morelock, Lead, Cyber Security Operations Team, Midcontinent ISO

Event Venue

Executive Conference Center

205 W. Wacker Drive, Chicago, Illinois 60605
2nd Floor

Located in downtown Chicago's Loop, the Conference Center is steps away from the city's magnificent lakefront with world-renowned Millennium and Grant Parks, marvelous museums, restaurants and retail shopping.