6th Annual March 19-21, 2024 • Chicago

Utility Cyber Security Forum

www.utilitycybersec.com **Organized by:** SGO Smart Grid Observer

Organized by the Smart Grid Observer, the **6th Utility Cyber Security Forum,** March 19-21, 2024 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."
- Ramesh Reddi, CTO, CybSecBCML, Inc

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

Platinum Sponsor: Landis+Gyr **Gold Sponsors:** tenable DRAGOS

Silver Sponsors: NOZOMI NETWORKS ThinkGard Total Data Security SALVADOR TECHNOLOGIES IncSys ESENTIRE asimily

Organizations that have participated in prior editions include:

Acronis
AlertEnterprise
Arizona Public Service Co.
Awesense
Basler Electric Co.
BC Hydro
Black & Veatch
Blockchain Engineering Council (BEC)
Bonneville Power Authority
Burns & McDonnell
Calpine
Citrix
Cleco Corporation
Consolidated Edison
Control Infotech Pvt Ltd
Cordoba Corporation
CPS Energy
CSA Group
CybSecBCML, Inc.
Dispersive Networks
Dominion Energy
Doyon Utilities, LLC
Dragos, Inc.
Duke Energy
DynTek
EDF Renewables
Edison Electric Institute
Element
El Paso Water
EPRI
Exclusive Networks
Exelon Corporation
Finite State
Fortinet
GridBright
Guardtime Energy
Guernsey
Guidehouse Insights
HYAS
Illinois Commerce Commission
IncSys
Indegy
JPEmbedded LLC
JSC Institute of Information Technology
Kent Power
Lea County Electric Cooperative, Inc.
Los Angeles Dept of Water & Power
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 Co.
Pacific Northwest National Laboratory
Pepco Holdings
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 Coop.
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
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

Platinum Sponsor

Landis+Gyr is a leading global provider of integrated energy management solutions. We measure and analyze energy utilization to generate empowering analytics for smart grid and infrastructure management, enabling utilities and consumers to reduce energy consumption. Visit www.landisgyr.eu

Gold Sponsors

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Visit tenable.com

Dragos has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The Dragos Platform offers the most effective industrial cybersecurity technology, giving customers visibility into their ICS/OT assets, vulnerabilities, threats, and response actions. Visit www.dragos.com

Silver Sponsors

Nozomi Networks is the leader in OT & IoT security for critical infrastructure. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for fast, effective incident response. Customers around the world rely on us to minimize risk and complexity while maximizing operational resilience. Visit Nozomi Networks

ThinkGard is your public sector expert in data protection. This consists of both managed cybersecurity and backup & disaster recovery as a service. ThinkGard acts as an extension of your IT team, allowing your team to focus on other critical parts of your organization. Unlike other companies that include data protection & security as part of a large complex offering, at ThinkGard, data protection is all we do. Visit www.thinkgard.com

Salvador Technologies provides pioneer failover technology, enabling seamless continuity in ICS & OT systems. Our enterprise-level platform reduced downtime to only 30 seconds and is activated by a single click. Designed for critical infrastructures, it ensures the operational continuity of SCADA systems through a patented technology of air-gap protection. Visit www.salvador-tech.com

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 2000+ organizations in 80+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Visit www.esentire.com

Asimily provides proactive, efficient, and accessible cybersecurity solutions that empower businesses to safeguard their digital assets. Reliant on constant and precise monitoring, IIoT and OT devices give real-time information about grids, power distribution, water levels, chemical sensors, temperature levels and much more. Asimily's comprehensive device and attack database keeps defenses high and security-related downtime low. Visit www.asimily.com

For over 30 years, IncSys and PowerData have championed the development and implementation of simulation-based solutions for power system operators. The industry-leading PowerSimulator now gives all transmission operators, balancing authorities, reliability coordinators and generator operators affordable access to their own power system model for use in world-class simulations. Visit www.incsys.com

Agenda

NOTE: Subject to change

Tuesday, March 19, 2024

Pre-Conference Workshop

9:00 am - 4:00 pm

Preparing Cyber Defenders and System Operators for an Inverter-Centric Electric Grid

The 9/11 commission concluded "We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities and management. It is therefore critical to find a way of routinizing, even bureaucratizing the exercise of imagination."

This pre-conference Workshop is designed to build teamwork and cooperation between Cyber Defenders, Protection Engineers, System Planners and Inverter Control System Developers with input from NERC Certified System Operators. The lack of coordination between these different disciplines is leading to a power system that is vulnerable to systemic events with and without malicious actors.

This SIM-X Workshop is an innovative and unique training opportunity for Cyber Defenders to work with NERC Certified power system operators to understand in depth how to provide services and products that can prevent widespread damage to critical equipment and lead to massive long term power outages that could impact millions of people over many months.

The fundamental nature of power systems is changing: large rotating coal and gas fired synchronous generators that provide MW / frequency response, dynamic MVAr response, short circuit capacity for fault clearing and synchronizing / torques for grid stability are being retired. These are being replaced with wind, PV solar and battery systems with much less mechanical and thermal inertia - they respond to power and voltage swings averaged over several milliseconds with inverter-based resources that respond within a few microseconds.

As a result of barriers in communications between different disciplines, poorly designed PV solar farms and wind farms have been tripping inadvertently within a 300 mile radius of single phase faults at the terminals of synchronous generators.

The same hypothetical Cascadia Power System that is used to train NERC Certified System operators with organizations which are keeping the lights on for over 100 million people will be used in this workshop.

-- **To attend the training, participants will need to provide evidence that they work as employees of, or as product and service suppliers to, a NERC-registered entity.**

-- For NERC System Operators, 6 Hours of NERC Continuing Education Hours will be provided.

Fee: $495.00

Workshop facilitator:

Dr. Robin Podmore, IEEE Fellow, Member NAE

NERC Certified System Operator and President, **IncSys**

Wednesday, March 20, 2024

8:00 - 9:00 am

Welcome Coffee and Registration

9:00 - 9:45 am

Securing the Digital Energy Transition

The global transition to renewable energy sources is gaining momentum across various sectors. As we embrace this shift, it is crucial to address the security challenges that arise when integrating renewable energy into existing infrastructure. One major concern is the presence of adverse suppliers in the renewable energy supply chain. While expanding renewable energy is essential, efforts are underway to reduce dependence on these products due to cybersecurity risks. Protecting energy infrastructure during this transition requires a multifaceted approach to cybersecurity. Stakeholders must prioritize the development and implementation of robust cybersecurity measures. This involves securing communication networks and employing strict access controls to prevent unauthorized entry. Additionally, adopting secure software design principles, regularly updating and patching software systems and fostering a cybersecurity-aware culture among personnel involved in the renewable energy sector are crucial. This session will discuss the global challenges facing the renewable and utility space, along with some potential solutions for the future of the sector.

Emma Stewart
Chief Power Grid Scientist and Research Strategist
Idaho National Laboratory
profile

9:45 - 10:30 am

Making Progress: Focusing Your Limited Resources to Protect What Really Matters

In today's dynamic business landscape, the effective management of limited resources is crucial for safeguarding organizational assets. This presentation delves into a practical example of a risk management process tailored for Operational Technology (OT) environments. The discussion encompasses a comprehensive understanding of business impacts, providing insights into prioritizing strategic areas for resource allocation based on business risk. Attendees will gain valuable insights into streamlining their approach to protect what truly matters to their organization, fostering a proactive and resilient security posture in the face of evolving threats.

Jeremy Korger
Senior Solutions Architect
Dragos
profile

10:30 - 11:00 am

Networking Coffee Break

11:00 - 12:15 pm

Navigating Control System Vulnerabilities: Risk, Regulation, and Real-Time Solutions

The vulnerability landscape within control systems, especially in the electric sector, is fraught with challenges. Managing the high volume of emerging software vulnerabilities, often in the hundreds or thousands monthly, is a daunting task. Operational Technology (OT) environments complicate this further, as patching can lead to system downtime. This necessitates prioritizing patches based on risk assessment, a process hindered by the limitations of current tools which often overlook organizational operational contexts like existing firewall protections.

This panel brings together experts from academia, security solutions, and the electric utility industry to explore advanced, automated technologies for context-aware vulnerability risk assessment. These innovations link vulnerabilities with firewall policies for accurate risk evaluation and streamlined patch management. Discussions will focus on the challenges of asset protection, regulatory compliance, and how emerging technologies aid in making swift, effective cybersecurity decisions in the electric utilities sector.

Philip Huff
Assistant Professor and Director of Cybersecurity Research, Emerging Analytics Center
University of Arkansas at Little

Azi Cohen
Executive Chairman
Salvador Technologies
profile

Kylie McClanahan
Director of Engineering
Bastazo, Inc
profile

Robin Berthier
Co-Founder and CEO
Network Perception
profile

12:15 - 1:15 pm

Lunch Break

1:15 - 2:00 pm

Top 10 OT Security Risks in Utilities and How to Build End-To-End Cyber Security

The digitization of critical infrastructure has made industrial processes of energy production and distribution a target for cyber attacks. Adversaries can utilize a vast array of attack vectors on Operational Technology (OT) typically overlooked by firewalls:

- Spill-over from enterprise IT
- Exploit of misconfigurations, zero-day or unpatched vulnerabilities

- Exploit of stolen / phished credentials
- Trespass in remote substations and undetected access to cyber-physical systems

In this session we will examine "real-world" security risks and vulnerabilities uncovered by Landis+Gyr security company Rhebo through OT risk analyses and OT monitoring at energy companies in 2023. We will show how energy utilities can create visibility in their OT, detect vulnerabilities and attack activities in real time. Finally, Chad the session will look at how utilities can establish end-to-end OT security from the control room to the head-end system to edge devices like smart meters and renewable energy installations.

Todd Wiedman
Chief Security Officer
Landis+Gyr
profile

Zeek Muratovic
Director of Security Solutions
Landis+Gyr
profile

2:00 - 2:45 pm
Securing Power Grids & Water Systems: 5 Essentials of a Solid IT/OT Security Program

From cyber attacks to cyber regulations, the pressure is on for security teams to stay vigilant of their networks and operations. But securing utilities from power grids to water systems cannot only focus on the same IT networks we've been securing for decades - OT systems are at risk, too. It's time to build a robust IT/OT security program that recognizes the importance of protecting systems without disrupting supply in the process. Key Takeaways:

- The key steps for safeguarding the OT environments of utility operators
- Considerations to ensure security activities don't lead to downtime
- Why bridging IT and OT silos can reduce the attack surface
- How to implement effective best practices to enhance overall security program efficiency

Marty Edwards
Deputy CTO, OT/IoT
Tenable
profile

2:45 - 3:15 pm
Networking Coffee Break

3:15 - 4:30 pm

Security and Risk Considerations in Deploying Generative AI Technology at Utilities in the United States

During this session, Ramesh Reddi will present on innovative Generative AI technology and its risk for utilities. Elizabeth Escobar led the research and development to understand the business value of Generative AI technology at Duke Energy. She will speak on Generative AI benefits for utilities and the guardrails needed to deploy this technology at Duke Energy, starting with an Enterprise Generative AI Chatbot that can retrieve high quality answers from diverse and siloed data sources.

Key Takeaways:

- Learn the difference between Generative AI and other types of AI
- Understand the risk and benefits of Generative AI deployment in US utilities
- Learn about security controls needed to deploy Generative AI in the energy and utilities industry

Liz Escobar, CISSP
Sr. IT Manager
Duke Energy
profile

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

4:30 - 5:15 pm

Crossing the Chasm from Compliance to Cybersecurity

We all hear (and likely agree) that compliance is not security. The underlying negative connotation is that most people only have the time and energy to focus on the compliance aspects of security at the expense of actually securing their organizations based on risk. That chasm between compliance and security can be crossed (figuratively) with a bit of planning and lot of groundwork. This presentation will highlight three key aspects of that process: 1) Platform Approach 2) Scalability and 3) Partnerships.

Key Takeaways:

- There are things to consider while implementing cyber security solutions that can both help achieve compliance and improve the overall security posture based on your organizational risk
- Partnerships are key at several levels (internally within the organization, as well as with external parties including vendors)
- Planning for one site/situation is not the same as planning for the whole organization, so scalability should always be a key consideration

Vivek Ponnada
Technical Solutions Director
Nozomi Networks
profile

5:15 - 6:45 pm

Networking Drink Reception

Thursday, March 21, 2024

8:00 - 9:00 am

Welcome Coffee

9:00 - 9:45 am

Cybersecurity Operational Resilience for the Electric Utility

This session will cover security by design, consequence-driven and cyber informed engineering, including how to identify the emerging threat landscape, the best approach to creating a sustainable cyber resilience program, and the key differences between new and outdated systems to cyber resiliency.

Key Takeaways:

- Understanding the changing landscape
- Significance of "Security By Design"
- Operational Resilience -- How to withstand and recover
- Physical and cybersecurity measures to help reduce risk; while understanding that engineering risk out, helps with resiliency
- Navigating regulatory compliance

Michael Welch
Managing Director, Critical Infrastructure Sector
Morgan Franklin Cyber
profile

Aaron Crow
Senior Director
Morgan Franklin Cyber
profile

9:45 - 10:30 am

"You need your business and I need my money" -- Voicemail from a Hacker

This session presents an educational case study of a real-world scenario that occurred with a ThinkGard client. There are many presentations about organizations that are behind the times and not prepared for the cyber threats of today, but in this case, the client had all of the layers of protection they should have needed but one checkbox made the difference between complete protection and getting completely owned. Unfortunately for them, it was the latter. This will be a deep dive into what happened, why it happened and how it could have been avoided. The goal is for you to take something away from this situation that can be applied in your environment and will help keep you better protected moving forward.

- Gain a better understanding of the complex and dynamic nature of the current cybersecurity landscape

- Understand how to develop a more hardened approach within your organization to better protect it from breaches
- Learn how bad actors can take advantage of the smallest vulnerabilities to move laterally within your IT security and gain access to your most sensitive systems

Kevin Fuller
Co-Founder, President and Chief Technical Officer
ThinkGard
profile

10:30 - 11:00 am
Networking Coffee Break

11:00 - 11:30 am
Cyber Security of DERs in an Increasingly Decentralized Energy Grid

An ever-expanding collection of public reports of attacks on DER systems describe how adversaries exploit vulnerabilities in products, networks, and cloud infrastructure; deface EV chargers; compromise local DER products and cloud infrastructure; prevent visibility and control of 100s of megawatts of DER assets; and maliciously update firmware on DER systems to prevent operation. Near-daily disclosures indicate that threat actors are escalating their attacks on DER systems as they become more important to the grid. This session will provide 1) provide a real-time update of the risks facing DER- and grid operators, 2) the specific threats operators face using real-world examples, and 3) steps that owners and operators can take to protect their assets and operations.

Key takeaways:

• DER proliferation, including EV chargers and solar+storage systems, is expanding the attack surface of critical energy infrastructure. Recent incident reports bring this reality into sharp focus.

• The responsibility for protecting DER assets and the grid is shared by all stakeholders. No single entity (e.g. a utility grid operator) is in total control and yet all stakeholders have a vested interest actively protecting their parts of the system. A Zero Trust approach is indicated.

Tom Tansy
CEO, **DER Security Corp**
Chairman, **SunSpec Alliance**
profile

11:30 - 12:00 pm

Risk-Based Assessment of Cyber-Physical Power Grid

Interconnectedness of control areas within an interconnection poses a risk of cascading outages caused by a potential cyber attack. Hence, Risk-Based Compliance Monitoring and Enforcement Program (CMEP) activities, Regional Entity oversight and enforcement, and certification are introduced with a statistically driven, risk-based approach that can be discerned from the cyber assets (CA). The foundation of this process for Inherent Risk Assessments (IRAs) and Internal Control Evaluation (ICE) should be based on physics-based modeling and anomalies of data coming from cyber assets. The risk-based CMEP should be widely promoted, and its methodologies should introduce stochasticity of foul play that deviates from normal activities. Contingency analysis is performed on an N-1 basis, but the cyber-informed framework may not have been combined into potential associated impacts to substations, generation that could introduce instability indices for the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) risk assessment framework. This presentation provides the methodological introduction on how NERC CIP 005 and 007 are introduced with quantitative and qualitative examples and the basic calculation of risks that will enable efficient spot checks, voluntary reporting that can help enhance audit reports. Key Takeaways:

- The interconnected control areas in power systems are at risk of cascading outages due to cyber attacks, underscoring the critical role of Risk-Based Compliance Monitoring and Enforcement Programs (CMEP) and Regional Entity oversight
- Cyber asset (CA) risk assessment relies on physics-based modeling and anomaly detection, necessitating robust methodologies within CMEP
- Integration of cyber-informed frameworks with traditional contingency analysis improves grid stability, vital for NERC CIP compliance by identifying potential impacts on substations and generation
- These metrics can quantify hypothesized cyber attack impacts, informing cybersecurity technology investments to bolster grid resilience and safeguard critical infrastructure

Prof. Chee-Wooi Ten
Professor, Electrical and Computer Engineering
Michigan Tech
profile

12:00 - 12:30 pm

Digital Twins for Imagineering Grid Cyber-Physical Defenses

- Generic power system models
- Specific power system models and protecting CEII
- Simulating Digital Control Systems and Networks
- Instructor and Drill management methods and systems
    - Creating realistic black swan events
    - Knowledge capture and transfer
- Massive multi-user simulations of continental power systems

- Transient stability simulations for defending Aurora attacks
- Electro-magnetic transient simulations for preventing SSR and cracked generator shafts

Dr. Robin Podmore
IEEE Fellow, Member NAE and NERC Certified System Operator
President, **IncSys**
profile

12:30 - 1:30 pm
Lunch Break

1:30 - 2:00 pm
GridTrust: Electricity Grid Root-of-Trust Decentralized Supply Chain Cybersecurity

Traditional supply chain protections include physical labels, patents, and information stored in a device's non-volatile memory, all of which are vulnerable to tampering. This session examines recent advances in mitigating supply chain attacks via physics-based device authentication. One such advancement is GridTrust -- a cybersecurity technology developed by Georgia Tech researchers. It employs semiconductor chip fingerprints and cryptographic techniques to safeguard electrical utilities from supply-chain cyber attacks. Tested successfully in a power substation, GridTrust is designed to prevent unauthorized software alterations and offer multi-layered security for the electricity grid, ensuring both authenticity and proper authorization before updates are installed.

Key Takeaways:

- Semiconductor Fingerprint Security: Relying on unique chip fingerprints to fortify utility equipment against cyberattacks targeting control device software updates
- Collaborative Testing: The project involved Georgia Tech researchers, the City of Marietta, Sandia National Laboratories, and Protect Our Power in a three-year supported by the U.S. Department of Energy
- Enhanced Protection: By combining cryptographic technology with physically unclonable functions (PUFs)

Santiago Grijalva
Georgia Power Distinguished Professor of Electrical and Computer Engineering and Director, Advanced Computational Electricity Systems (ACES) Laboratory
Georgia Tech
profile

2:00 - 2:45 pm
Securing the GOOSE: A Real-World Test Case and Post-Quantum Path to Secure Sub-Millisecond Latency for Time-Sensitive Protocols

Many OT/ICS/IoT systems components require low latency communication to operate. As a result, these

systems have been left to communicate in an unencrypted format making our power grid a prime target for APTs and nation state adversaries. For the first time publicly disclosed, this session will present a real-world test case involving ground-breaking quantum resilient hardware that was leveraged to secure lightweight protocols like Generic Object Oriented Substation Event or GOOSE/ IEC 61850, which requires latency of less than 4 milliseconds to communicate successfully. The test case was completed with hardware encryption devices that provide secure UDP or TCP point-to-point communication with an average latency of 0.07ms while leveraging encryption that is $8.636 * 10^{434}$ more powerful than AES-256, proving the possibility of eliminating all site-specific IT/OT technical debt with the installation of a single hardware encryption device.

We now live in a sub-millisecond latency, power-over-ethernet post-quantum encryption reality.

Key Takeaways:

- Encryption capabilities now exist that are efficient enough to secure even the most lightweight UDP or TCP protocols
- Post quantum encryption cannot be algebra-based in order to be truly secure
- Variable Word Length (VWL) is a post-quantum secure encryption protocol to consider for secure point-to-point transmission where either latency or power consumption matter (addresses SNDL attacks directly)
- Leveraging a HW component in front of otherwise vulnerable devices/technical debt can provide a great mitigation option

Brian Penny
Founder & CEO
Kloch
profile

Paul J. Malcomb
Director of Threat Intelligence
Kloch
profile

2:45 - 3:30 pm

The Power of Time: Enhancing Grid Stability Through Redundancy

This session explores the critical role of timing across the power grid, discussing GPS and the Precision Time Protocol (PTP) as key tools in maintaining stability. We will delve into the need for redundancy in these systems to ensure resilience against potential disruptions. Highlighting a real-life application, we will examine the work spearheaded by Joe Marshall from Cisco Talos to protect the Ukrainian power grid from GPS jamming. This case study emphasizes the importance of diversified timing solutions in securing power grid operations.

Kam Chumley-Soltani
Technical Solutions Architect, Industrial Internet of Things
Cisco
profile

Event Venue:

Chicago 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.

>> Directions in Google Maps
>> Nearby Hotels

Media Partners:

Utility Business Media, Inc. (UBM) is the utility industry's leading publisher and producer of utility safety and leadership-focused content and education. UBM was founded by Carla Housh in 2004 as a newsletter and has rapidly grown into a multi-faceted media and education organization. Visit utilitybusinessmedia.com

GlobalPlatform is a technical standards organization that enables the efficient launch and management of innovative, secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity and convenience to users. It achieves this by providing standardized technologies and certifications that empower technology and service providers to develop, certify, deploy and manage digital services and devices in line with their business, security, regulatory and data protection needs. Visit www.globalplatform.org

Published in Fremont, California, CIOReview (www.cioreview.com) is one of the leading print magazines in the US. It is the knowledge platform where C-suite executives deliberate on critical market challenges and current technological trends across industries. We are a unique magazine because all of our contributors are senior executives from the industry. Visit www.cioreview.com

Guidehouse Insights is a premier market intelligence and advisory firm covering the global energy transformation with a focus on emerging resilient infrastructure systems. Our goal is to present an objective, unbiased view of market opportunities across dozens of industry verticals. Guidehouse Insights is not beholden to any special interests and is thus able to offer clear, actionable advice to help clients manage transformation, unfettered by technology hype, political agendas, or financial influences that are inherent in emerging technology markets.
Visit www.guidehouseinsights.com

The OSGP Alliance is the global non-profit association dedicated to promoting the adoption of the Open Smart Grid Protocol (OSGP) and infrastructure for smart grid applications towards a future proof modern smart grid. With a key focus on security, smart metering, smart grid, grid analytics, distribution network management and smart cities our members, including utilities, hardware manufacturers, service providers and system integrators, all share a common goal and vision: promoting open standards for energy demand side management, smart grid and smart metering systems. Visit www.osgp.org.

Since 2012 we've published our Cybersecurity Conference directory - which has now become the 'go-to' place to discover where, when and what events are taking place in our community. Visit www.infosec-conferences.com

Registration:

Standard Rate – Main Conference
Equipment and software vendors, services providers, consultants $895.00

Standard Rate – Main Conference plus Workshop $1,390.00

Special Rate – Main Conference $795.00
(Utilities, Academic, Government and Non-Profit Organizations.
Note - .edu, .gov or .org email address required)

Special Rate – Main Conference plus Workshop $1,290.00
(Utilities, Academic, Government and Non-Profit Organizations.
Note- .edu, .gov or .org email address required)

Workshop Only $595.00

Register securely online at https://www.utilitycybersec.com/register.htm

Sponsorship Packages:

Platinum Level Sponsor

Value: $10,000

- 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: $6,000

- 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: $4,000

- Logo recognition as Silver-Level Sponsor
- Tabletop exhibit in networking break and reception area
- 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: $3,000

- 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

About the Organizer:

The Smart Grid Observer is an online information resource 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. SGO produces several conferences each year on topics such as microgrids, grid modernization, energy storage, EV charging, V2G, demand response, distributed energy resources, and more. Visit www.smartgridobserver.com