



GRIDSEC CON 2023
NERC • E-ISAC • NPCC

October 17–20, 2023

2023 GridSecCon Welcome Letter

Welcome to the 12th annual GridSecCon 2023. We are delighted to return once again to an in-person format. This year's event is co-hosted by the North American Electric Reliability Corporation (NERC), the Electricity Information Sharing and Analysis Center (E-ISAC), and the Northeast Power Coordinating Council (NPCC). It is part of the Electric Reliability Organization (ERO) Enterprise's collaborative efforts to support industry to secure the North American bulk power system through information sharing, education, and collaboration. This year's program leverages the unique opportunity of in-person engagement, trainings, networking events, vendor interface, panels of industry experts from asset owner and operator organizations and, most importantly, peer-to-peer learning.

During the past year in particular, the tactics, tools, and techniques of our cyber and physical security adversaries have caught the attention of the media, the public and lawmakers. Industry has prevented and responded to these threats with our collective defenses, information-sharing programs, supplier and partner coordination, and our healthy posture of innovation and preparedness. However, we cannot rest on our victories but must continue our vigilance and ability to adapt our security posture to face new threats on the horizon.

In addition, with the rapid introduction of new technologies embracing climate-responsive and secure-by-design engineering for the grid of the future, we recognize the need to readily share knowledge and ideas for protecting our evolving assets. As we continue to say, "Collaboration and coordination are fundamental to our ability to secure our critical infrastructure." Our program for 2023 encompasses this theme and backdrop.

We kick off our training day with physical security, cyber security, and hands-on training from E-ISAC staff, national labs representatives, and world-class industry educators. Our main program initiates with keynote speakers Charles Dickerson, president and chief executive officer (CEO), NPCC; and Mario Tanguay, Cybersecurity and Chief Information Security Officer, Hydro-Québec. Our keynote leaders also include Johanne Picard-Thompson, executive vice president, Customer and Corporate Services, AltaLink; Jim Robb, president and CEO, NERC; Nitin Natarajan, deputy director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security; and Mara Winn, deputy director, Preparedness, Policy, and Risk Analysis, Office of Cybersecurity, Energy Security, and Emergency Response. We are honored to have these accomplished colleagues share their insights with us.

Our agenda continues with additional training, panel discussions, roundtables, and breakout sessions on operational technology maintenance, physical security resources, cyber security and supply chain risk, physical security design improvements, activist threat, and a panel on the upcoming GridEx VII, among other topics.

At the conclusion of GridSecCon 2023, we will announce the recipient of the E-ISAC Electricity Security Service Award in honor of Michael J. Assante, who was instrumental in building the E-ISAC. The award recognizes individuals or teams who have made significant contributions to support the security of the North American electricity industry.

We cannot maintain reliability without also securing the North American bulk power system. As we face new challenges and considerations of an evolving threat environment and demands on our grid, we choose to look toward the future embracing the challenge, one ripe for partnerships and innovation to face them as a community. In this spirit, the ERO continues to host GridSecCon to facilitate learning, interpersonal connection, and thought leadership toward this common goal. We look forward to the presentations, discussions, and a successful conference.

Jim Robb



President and CEO
NERC

Manny Cancel



Senior Vice President, NERC
President and CEO, E-ISAC

Charles Dickerson



President and CEO
NPCC

Schedule at a Glance

Monday, October 16 | Pre-Conference

6:00 – 8:00 p.m. Evening Registration

Tuesday, October 17 | Training Day

7:00 a.m. – 5:00 p.m. Registration
 7:00 a.m. – 8:00 a.m. Buffet Breakfast
 8:00 a.m. – 12:00 p.m. Morning Training Sessions
 12:00 – 1:00 p.m. Lunch
 1:00 – 5:00 p.m. Afternoon Training Sessions
 5:00 – 7:00 p.m. **Welcome and Networking Reception**
 6:00 – 9:00 p.m. SANS Capture the Flag Challenge – DAY 1

Wednesday, October 18 | Day 1

7:00 a.m. – 5:00 p.m. Registration
 7:00 – 8:30 a.m. Buffet Breakfast
 7:30 – 8:30 a.m. Women’s Breakfast
 8:00 a.m. – 5:00 p.m. **Exhibit Hall Open**
 8:30 – 10:30 a.m. General Session
 10:30 – 10:45 a.m. AM Break
 10:45 a.m. – 12:15 p.m. General Session
 12:15 – 1:15 p.m. Lunch
 1:30 – 2:30 p.m. Concurrent Breakout Sessions
 2:30 – 2:45 p.m. PM Break
 2:45 – 3:45 p.m. Concurrent Breakout Sessions
 3:45 – 4:00 p.m. Transition to Next Session
 4:00 – 5:00 p.m. Concurrent Breakout Sessions
 5:30 – 7:30 p.m. **Evening Networking Reception**
 6:00 – 9:00 p.m. SANS Capture the Flag Challenge – DAY 2

Thursday, October 19 | Day 2

7:00 – 8:30 a.m. Buffet Breakfast
 8:00 a.m. – 3:30 p.m. **Exhibit Hall Open**
 8:30 – 9:30 a.m. Concurrent Breakout Sessions
 9:30 – 9:45 a.m. Transition to Next Session
 9:45 – 10:45 a.m. Concurrent Breakout Sessions
 10:45 – 11:00 a.m. AM Break
 11:00 a.m. – 12:00 p.m. Concurrent Breakout Sessions
 12:00 – 1:00 p.m. Lunch
 1:15 – 2:15 p.m. General Session
 2:15 – 2:30 p.m. PM Break
 2:30 – 3:30 p.m. GridEx VII Panel
 3:30 – 4:00 p.m. Closing Remarks/E-ISAC Award

Friday, October 20 | Threat Briefing Day

7:00 – 8:30 a.m. Buffet Breakfast
 8:00 – 9:30 a.m. Unclassified Threat Briefing
 10:00 – 11:00 a.m. National Assembly Parliament Building Tour
 10:00 a.m. – 1:00 p.m. Hydro-Québec Lévis Substation Tour
 10:00 a.m. – 1:00 p.m. Classified Briefing

*All times are Eastern. Agenda subject to change.

GridSecCon 2023 Agenda

**Agenda subject to change. All times are Eastern.*

[Hilton Québec City Hotel](#)

1100 Blvd. Rene-Levesque Est
Québec, Canada G1R 4P3

AND

[Delta Hotels by Marriott Québec](#)

690 Blvd. Rene-Levesque Est
Québec, Canada G1R 5A8

**All conference programming will take place at the Hilton*

Monday, October 16 | Pre-conference

6:00 – 8:00 p.m. **Evening Registration** (*Hilton, Grande Place Foyer*)

Tuesday, October 17 | Training Day

7:00 a.m. – 5:00 p.m. **Registration** (*Hilton, Grande Place Foyer*)

7:00 – 8:00 a.m. **Buffet Breakfast** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny*)

8:00 a.m. – 12:00 p.m. **Morning Training Sessions**

Training Name	Training Track	Training Provider	Location
Physical Security Training 1A	Physical Security	Electricity Information Sharing and Analysis Center (E-ISAC)	Hilton, Palais
ICS Pentest and Assessment Sneak Peek 2A	Cyber Security	SANS Institute	Hilton, St. Louis
Gaining Insight with Zeek 3A	Cyber Security	Leargas Security	Hilton, Dufferin
ICS4ICS Exercise Part 1 4A* *Must register with 4B	Cyber Security	BBA Engineering	Hilton, Lauzon
Cyber/Physical Resilience and Human Performance 5A	Special Topics	Resilient Grid, Inc. and Pacific Northwest National Laboratory	Hilton, Kent

**See page 11 for training descriptions*

12:00 – 1:00 p.m. **Lunch** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny*)

1:00 – 5:00 p.m.

Afternoon Training Sessions

Training Name	Training Track	Training Provider	Location
VISA Crash Course 1B	Physical Security	E-ISAC	Hilton, Palais
ICS Pentest and Assessment Sneak Peek 2B	Cyber Security	SANS Institute	Hilton, St. Louis
Security by Design: Building Security into Your Projects in the Design Phase 3B	Cyber and Physical Security	Burns & McDonnell	Hilton, Dufferin
ICS4ICS Exercise Part 2 4B* *Must register with 4A	Cyber Security	BBA Engineering	Hilton, Lauzon
Addressing High Risk Cyber Threats 5B	Cyber Security	Western Area Power Administration	Hilton, Kent
Reliability, Security, and Cloud Technology 6B	Cyber Security	Amazon Web Services and North American Electric Reliability Corporation	Hilton, Plaines

**See page 11 for training descriptions.*

5:00 – 7:00 p.m.

Welcome and Networking Reception *(Hilton, Grande Place Foyer)*

6:00 – 9:00 p.m.

SANS Capture the Flag Challenge – DAY 1 *(Hilton, Kent/St. Louis)*

Wednesday, October 18 | Day 1

**See page 15 for breakout session descriptions*

- 7:00 a.m. – 5:00 p.m.** **Registration** (*Hilton, Grande Place Foyer*)
- 7:30 – 8:30 a.m.** **Buffet Breakfast** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny*)
- 7:30 – 8:30 a.m.** **Women’s Networking Breakfast – Registration Required** (*Hilton, Plaines*)
- 8:30 – 10:30 a.m.** **General Session** (*Hilton Ballroom*)
Opening Remarks (20 min): *Jim Robb, President & CEO, NERC*
- NPCC Regional Keynote (20 min):** *Charles Dickerson, President & CEO, Northeast Power Coordinating Council*
- Host Utility Keynote (20 min):** *Mario Tanguay, Cybersecurity and Chief Information Security Officer, Hydro-Québec*
- Keynote Panel (60 min):** *"Shields Up – Shifting North American Electricity Model Beyond Intelligence Sharing to Integrated Security Collaboration"*
Moderator: *Eóin Cooke, Partner, Energy Transition, Utilities and Cybersecurity, PwC*
Panelists: *Rajiv Gupta, Associate Head, Canadian Centre for Cyber Security*
Nitin Natarajan, Deputy Director, Cybersecurity & Infrastructure Security Agency
Johanne Picard-Thompson, EVP, Customer & Corporate Services, AltaLink
Jim Robb, President & CEO, North American Electric Reliability Corporation
- 10:30 – 10:45 a.m.** **AM Break/Transition to Next Session**
- 10:45 a.m. – 12:15 p.m.** **General Session** (*Hilton Ballroom*)
Keynote (30 min): *Francis Bradley, President & CEO, Electricity Canada*
- Keynote Panel (60 min):** *"Policy Impacts on Grid Security – A Look at Legislative, Regulatory, and Strategic Considerations for the Grid in 5 – 10 Years"*
Moderator: *Michael Powell, VP Government Relations, Electricity Canada*
Panelists: *Bridgette Bourge, President & CEO, Bridgette Bourge Security, LLC*
Mara Winn, Deputy Director, Preparedness, Policy, and Risk Analysis, Office of Cybersecurity, Energy Security, and Emergency Response
- 12:15 – 1:30 p.m.** **Lunch** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny, Plaines*)
- 1:30 – 2:30 p.m.** **Concurrent Breakout Sessions (60 min)**
Cyber: *ICS/OT Cyber Security: Current Threats and Vulnerabilities in the Electric Sector – Dragos*
Physical: *Violent Extremist Panel – E-ISAC*
Supply Chain: *Relying Upon the Work of Others for Supply Chain Risk Management – North American Transmission Forum*
Special Topics: *Maximizing the Intelligence Cycle – Southern California Edison*
- 2:30 – 2:45 p.m.** **PM Break/Transition to Next Session** (*Hilton, Grande Place Foyer*)

- 2:45 – 3:45 p.m.** **Concurrent Breakout Sessions (60 min)**
Cyber: Ransomware: Current Trends and Mitigation TTPs – *E-ISAC*
Physical: What's Unacceptable to You? – *SERC Reliability Corporation*
Supply Chain: Securing Software's Supply Chain – *Burns & McDonnell*
Special Topics: The Integrated Compliance Journey: Enhancing Our NERC Program through Collaboration and Technology – *Eversource Energy*
- 3:45 – 4:00 p.m.** **Transition to Next Session**
- 4:00 – 5:00 p.m.** **Concurrent Breakout Sessions (60 min)**
Cyber: Information Sharing – Can We Really Be Anonymous – *National Rural Electric Cooperative Association*
Physical: Gunfire Threats to the Grid and Potential Impacts – *E-ISAC*
Supply Chain: Operationalizing SBOMs for the Energy Sector – *Deloitte & Touche LLP*
Cyber II: Evolving Threats from Malicious Use of AI – *Vector9 Consultants, LLC*
- 5:30 – 7:30 p.m.** **Evening Networking Reception (Hilton, Grande Place Foyer)**
- 6:00 – 9:00 p.m.** **SANS Capture the Flag Challenge – DAY 2 (Hilton, Kent/St. Louis)**

Thursday, October 19 | Day 2

**See page 15 for breakout session descriptions*

- 7:30 – 8:30 a.m.** **Buffet Breakfast (Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny, Plaines)**
- 8:30 – 9:30 a.m.** **Concurrent Breakout Sessions (60 min)**
Cyber: Future-Proofing NERC CIP: An Impossible Dream? – *SANS*
Physical: Mitigating the Activist Threat – *Foresight*
Supply Chain: The Various Shades of Supply Chain: SBOM, N-Days – *Binarly, Inc.*
Special Topics: Data Sharing Programs – Their Maturity and Impact – *E-ISAC*
- 9:30 – 9:45 a.m.** **Transition to Next Session**
- 9:45 – 10:45 a.m.** **Concurrent Breakout Sessions (60 min)**
Physical: Physical Security Topics: Resource Roundtable – *E-ISAC*
Cyber II: Enhancing Cyber Security for Electric Utilities – *Finite State*
Special Topics: Aggregated DERs – Grid Security and Reliability – *Environmental and*
- 10:45 – 11:00 a.m.** **AM Break/Transition to Next Session**
- 11:00 a.m. – 12:00 p.m.** **Concurrent Breakout Sessions (60 min)**
Cyber: Power Grid Containment Test: Hydro Québec Achievement – *Hydro Québec*
Physical: Design Security into a Facility from the Beginning – *TRC Engineers*
Cyber II: Defending the Grid: Approaching AI Security – *KPMG US*
Special Topics: Security Challenges of the Future Grid – *E-ISAC*

- 12:00 – 1:15 p.m.** **Lunch** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny, Plaines*)
- 1:15 – 2:15 p.m.** **General Session** (*Hilton Ballroom*)
- Panel (60 min) Supply Chain Challenges: Managing Risk and Resilience**
Moderator: *Bluma Sussman, Director of Membership, E-ISAC*
Panelists: *Jeffrey Baumgartner, VP, Security & Resilience, Berkshire Hathaway Energy*
Vinod D’Souza, Head of Manufacturing and Industry, Office of the CISO, Google Cloud
Frank Harrill, VP of Security, Schweitzer Engineering Laboratories, Inc.
Brian Moss, Information Security Manager, Bruce Power
Jonathan Tubb, Director of Industrial Cyber Security, Siemens Energy
- 2:15 – 2:30 p.m.** **PM Break** (*Hilton, Grande Place Foyer*)
- 2:30 – 3:30 p.m.** **GridEx VII Panel** (*Hilton Ballroom*)
Moderator: *Jesse Sythe, GridEx Program Manager, E-ISAC*
Panelists: *Saad Ansari, Senior Specialist – Emergency Preparedness, IESO*
Ingrid Rayo, Senior Consultant/Governance, Risk, Cybersecurity, and Compliance, Burns & McDonnell
Erin Rowe, Director Incident Response, MISO Energy
Ashley Wemhoff, Incident Response Drill Coordinator, NPPD
- 3:30 – 4:00 p.m.** **Closing Remarks/E-ISAC Award** (*Hilton Ballroom*)

Friday, October 20 | Threat Briefing Day

- 7:00 – 8:30 a.m.** **Buffet Breakfast** (*Hilton, Beauport/Beaumont/Belair, Villeray/De Tourny*)
- 8:00 – 9:30 a.m.** **Unclassified Threat Briefing** (*Hilton, Palais Ballroom*)
- 10:00 – 11:00 a.m.** **National Assembly Parliament Building Tour** (*Walking distance from hotel, registration required*)
- 10:00 a.m. – 1:00 p.m.** **Hydro-Québec Lévis Substation Tour** (*Transportation provided, registration required*)
- 10:00 a.m. – 1:00 p.m.** **Classified Briefing** (*Location TBD, transportation provided, registration and SECRET level clearance required*)

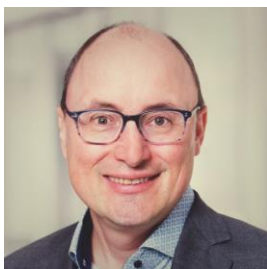
Featured Keynote Speakers

Charles Dickerson, President and CEO, Northeast Power Coordinating Council



Charles Dickerson serves as president and CEO for NPCC. He is a recognized industry thought leader with 30 years of experience in the energy sector. Most recently, Mr. Dickerson served as president, Utility Division of SUEZ North America, where he led its regulated utilities across the United States. His previous positions include having served as chief operating officer for Austin Energy where he led the generation, market operations, transmission, distribution, IT, technology, and strategic planning functions, and as President of National Grid, USA Business Services. Prior to National Grid, he worked for Exelon-Pepco Holdings Inc. for 27 years. In addition, Mr. Dickerson brings deep governance expertise as a past board of directors member for both the Seedling and RMEL organizations. Mr. Dickerson holds a Bachelor of Science in mechanical engineering and master's degree in applied management from the University of Maryland.

Mario Tanguay, Cybersecurity and Chief Information Security Officer, Hydro-Québec



Mario Tanguay has more than 30 years of experience at Hydro-Québec, where he has held positions of increasing responsibility in various fields. Over the course of his career, he has acquired in-depth knowledge about the company's digital technologies and operating activities as well as vast experience in technical architecture, innovation, cyber security, and management. Among other achievements, he spearheaded the deployment of Hydro-Québec's cyber security monitoring center and the development of its analytics foundation and launched the ITC infrastructure modernization project.

Recognized for his strong leadership and ability to listen, Mr. Tanguay prioritizes process optimization, innovation and the alignment of business strategies, and favors a collaborative approach aimed at reinforcing his team's know-how.

Francis Bradley, President and CEO, Electricity Canada



Francis Bradley is the President and Chief Executive Officer of Electricity Canada. Founded in 1891, Electricity Canada (formerly the Canadian Electricity Association) is the national voice for sustainable electricity for its members and the customers they serve as the country works towards a Net Zero by 2050 future.

Mr. Bradley is the co-chair of the National Cross-Sector Forum, overseeing Canada's Action Plan for Critical Infrastructure. He also sits on the Steering Committee for the Electricity Sub-Sector Coordinating Council (ESCC), the Board for the Energy Council of Canada (ECC), the Positive Energy Advisory Council, and is a founding Board member of the Canadian Transportation Alliance. At the NERC Member Representatives Committee and Board of Trustees meetings, Mr. Bradley represents

Electricity Canada and advocates strongly for its members in their activities related to the Electric Reliability Organization Enterprise, and its role in ensuring the reliability and security of the North American bulk power system.

Prior to being named CEO in June 2019, Mr. Bradley managed Electricity Canada’s day-to-day activities as chief operating officer since 2014. During that time, he also was a member of the National Advisory Committee of Canada’s Platform for Disaster Risk Reduction and was a co-chair with the Standards Council of Canada of the Smart Grid Standards Advisory Committee.

In 2019 Mr. Bradley created and continues to host “The Flux Capacitor” podcast, featuring discussions about the future of electricity with CEOs, regulators, political figures, and leaders from civil society.

Keynote and General Session Panels

Wednesday, October 17: 9:30 – 10:30 a.m.

Shields Up – Shifting North American Electricity Model Beyond Intelligence Sharing to Integrated Security Collaboration *(Hilton Ballroom)*

Eóin Cooke – Partner, Energy Transition, Utilities and Cybersecurity, PwC (moderator)

Rajiv Gupta – Associate Head, Canadian Centre for Cyber Security

Nitin Natarajan – Deputy Director, Cybersecurity & Infrastructure Security Agency

Johanne Picard-Thompson – EVP, Customer & Corporate Services, AltaLink

Jim Robb – President & CEO, North American Electric Reliability Corporation

Join senior leaders from industry and government as they share their perspectives on how the increasing cyber threat landscape, physical attacks from domestic violent extremists, and Russia's invasion of Ukraine have resulted in a “shields up” posture as the new normal. The panel will discuss systemic national level risks, coordination during an event, and collaboration between industry and government across borders.

Wednesday, October 17: 11:15 a.m. – 12:15 p.m.

Policy Impacts on Grid Security – A Look at Legislative, Regulatory, and Strategic Considerations for the Grid in 5–10 Years *(Hilton Ballroom)*

Michael Powell – VP Government Relations, Electricity Canada (moderator)

Bridgette Bourge – President and CEO, Bridgette Bourge Security, LLC

Kathleen Miller – Deputy Director, Natural Resources Canada

Mara Winn – Deputy Director, Preparedness, Policy, and Risk Analysis, Office of Cybersecurity, Energy Security, and Emergency Response

This panel of experts will examine and discuss the various legislative and policy-focused initiatives that are currently being discussed at the federal levels in both Canada and the United States.

Thursday, October 18: 1:15 – 2:15 p.m.

Supply Chain Challenges: Managing Risk and Resilience

Bluma Sussman – Director of Membership, E-ISAC (moderator)

Jeffrey Baumgartner – VP, Security and Resilience, Berkshire Hathaway Energy

Vinod D'Souza – Head of Manufacturing and Industry, Office of the CISO, Google Cloud

Frank Harrill – VP, Security, Schweitzer Engineering Laboratories, Inc.

Brian Moss – Information Security Manager, Bruce Power

Jonathan Tubb – Director of Industrial Cyber Security, Siemens Energy

Panel discussion with leading electricity industry and vendors on the increasing complexities of the supply chain and how vendors and utilities are coming together to manage supply chain risk management and identify solutions.

Thursday, October 18: 2:30 – 3:30 p.m.

GridEx VII Panel

Jesse Sythe – GridEx Program Manager, E-ISAC (moderator)

Saad Ansari – Senior Specialist – Emergency Preparedness, IESO

Ingrid Rayo – Senior Consultant/Governance, Risk, Cybersecurity, and Compliance, Burns & McDonnell

Erin Rowe – Director Incident Response, MISO Energy

Ashley Wemhoff – Incident Response Drill Coordinator, NPPD

With GridEx VII right around the corner, this panel of past participants and experienced exercise planners will get you energized and ready to collect those lessons learned and action items that make GridEx so valuable to the electricity industry. Our panel will walk through their process of preparing for GridEx VII, discuss their best practices for exercise evaluation and feedback collection, and tell their own stories of how they've seen the GridEx program measurably improve the resilience of the bulk power system.

Training Descriptions

Tuesday, October 17: 8:00 a.m. – 12:00 p.m.

Morning Training Sessions

Physical Security Training – 1A

(Hilton, Palais)

Part 1: Physical Security Incidents, Tactics Used in Significant Incidents, and Workshop on Categorizing Incidents

Lauren Alexander-Binns – Physical Security Analyst, E-ISAC

Kristen Bove – Manager, Physical Security, E-ISAC

Samantha Lee – Senior Physical Security Analyst, E-ISAC

This session is to cover how the E-ISAC analyzes incidents as they come, as well as how incidents are processed and analyzed with the Severity Level Model.

Part 2: Indicators of Malicious Intent (Physical and Digital)

Lauren Alexander-Binns – *Physical Security Analyst, E-ISAC*

This session focuses on best practices for assessing whether an incident that has occurred is part of a concerted attempt to disrupt the grid as well as on assessing threats in the digital space.

Part 3: How to Design Ballistic Testing

Mark Maney – *Manager of Economic Development and Governmental Affairs, Southern Company*

This session focuses on best practices for assessing whether an incident that has occurred is part of a concerted attempt to disrupt the grid.

Sneak Peek at SANS ICS 613 – ICS Penetration Testing and Assessments – 2A

(Hilton, St. Louis)

Fred Alvarez – *Instructor, SANS Institute*

Don Weber – *Principal Consultant and Founder, Cutaway Security, LLC*

The ICS613 course introduces information and operational security professionals to the tactics, techniques, and procedures for conducting penetration testing and security assessments in networks with active processes. Penetration tests in business environments are structured to avoid outages primarily because of the monetary impacts on the organization. However, outages within industrial control networks are more concerned with the consequences of an outage. These consequences potentially include loss of life and injury to personnel and could also have a dangerous environmental impact. This situation is exacerbated by fragile equipment and protocols in these networks.

Get a sneak peek into the new SANS ICS613 course – ICS Penetration Testing and Assessments. While the full 5-day course will be released late in 2023, this is an opportunity to join the course authors and get a glimpse of the course.

Gaining Insight with Zeek – 3A

(Hilton, Dufferin)

Patrick Kelley – *Founder, Leargas Security*

Zeek is a great open-source tool that allows you to monitor your network and analyze events within it. This course will teach you about this tool as well as how to configure and use it within your network to suit your needs.

Zeek is a network event-based monitoring and analysis tool used by many organizations around the world. It enables users to see the traffic going through their networks and respond to it in several different ways.

This course will teach the user how to configure, use, and customize this tool to discover attackers on the network, perform in-depth forensic investigations, and resolve network issues.

ICS4ICS Exercise Part 1 – 4A

(Hilton, Lauzon)

Brian Peterson – *ICS4ICS Program Manager, LOGIIC Program Manager, International Society of Automation*

Pierre Janse van Rensburg, GCIH – *Senior Consulting Expert, ICS Cybersecurity, BBA*

ICS4ICS is designed to reduce the impact of cyber security incidents that impact Industrial Control Systems by providing a consistent orderly approach to managing an incident.

This demonstration of an exercise will enable participants to learn about the Incident Command System for industrial control systems and understand the various ICS4ICS roles. Participants will play key roles on the ICS4ICS team. Others will be able to observe the exercise so they can learn about ICS4ICS and prepare to use the processes in their companies or organizations.

Cyber/Physical Resilience and Human Performance – 5A

(Hilton, Kent)

Michael Legatt, Ph.D. – Chief Executive Officer | Founder, Resilient Grid, Inc.

Mark Rice – Electrical Power Systems Researcher, Engineer, Pacific Northwest National Laboratory

Around the moment of the "bang" during a blended cyber/physical attack, groups that haven't had to work together much before (e.g., system operators, EMS support engineers, IT analysts, media relations, legal) suddenly must start communicating and collaborating in the most effective, high-bandwidth way possible along with increased use of their tools. This training session brings together research in diverse domains, such as human performance, neuroscience, resilience engineering, systems engineering, and human factors, including work done by the Resilient Grid team with control from and SOC/NOC operators to build a practical set of changes you can bring to your organization to improve readiness and outcomes.

Tuesday, October 17: 1:00 – 5:00 p.m.

Afternoon Training Sessions

VISA Crash Course (Physical Security Training) – 1B

(Hilton, Palais)

Ross Johnson – President, Bridgehead Security

Rob Siefken – Chief Operating Officer, Safeguards3

This is a short introduction on how to use and apply the Vulnerability of Integrated Security Analysis method to effectively assess the vulnerabilities of a site's critical assets. This methodology, which has been used successfully since the 1970s, will provide the necessary framework and tools for asset owners and operators to make informed risk-based and cost-effective decisions on the effectiveness of their physical protection systems as well as provide justification to support targeted upgrades.

Sneak Peek at SANS ICS 613 – ICS Penetration Testing and Assessments – 2B

(Hilton, St. Louis)

Fred Alvarez – Instructor, SANS Institute

Don Weber – Principal Consultant and Founder, Cutaway Security, LLC

This is a repeat of Session 2A. The ICS613 course introduces information and operational security professionals to the tactics, techniques, and procedures for conducting penetration testing and security assessments in networks with active processes. Penetration tests in business environments are structured to avoid outages primarily because of the monetary impacts on the organization. However, outages within industrial control networks are more concerned with the consequences of an outage. These consequences potentially include loss of life and injury to personnel and could also have a dangerous environmental impact. This situation is exacerbated by fragile equipment and protocols in these networks.

Get a sneak peek into the new SANS ICS613 course – ICS Penetration Testing and Assessments. While the full 5-day course will be released late in 2023, this is an opportunity to join the course authors and get a glimpse of the course.

Security by Design: Building Security into Your Projects in the Design Phase – 3B

(Hilton, Dufferin)

Joseph Bonventre – Department Manager, Burns & McDonnell, GRCC

Eric Smith – Senior Cyber Security Reliability Consultant, Burns & McDonnell, GRCC

Security by design (or secure by design) is an approach to product development that considers cyber security at the onset. It does away with the “let’s cross the bridge when we get there” outlook on cyber security and makes software or hardware more secure. It is similar to designing a house and ensuring that it is earthquake-resistant and hurricane- or typhoon-proof. Security by design ensures that security controls are built into a product’s design rather than as an afterthought. Such an approach reduces the likelihood of cyber security breaches and has become common in product development.

ICS4ICS Exercise Part 2 – 4B

(Hilton, Lauzon)

Brian Peterson – ICS4ICS Program Manager, LOGIIC Program Manager, International Society of Automation
Pierre Janse van Rensburg, GCIH – Senior Consulting Expert, ICS Cybersecurity, BBA

ICS4ICS is designed to reduce the impact of cyber security incidents that impact Industrial Control Systems by providing a consistent orderly approach to managing an incident.

This demonstration of an exercise will enable participants to learn about Incident Command System for Industrial Control Systems and understand the various ICS4ICS roles. Participants will play key roles on the ICS4ICS team. Others will be able to observe the exercise so they can learn about ICS4ICS and prepare to use the processes in their companies or organizations.

Addressing High Risk Cyber Threats – 5B

(Hilton, Kent)

Eric Cardwell – Vice President of Professional Services and Cyber Risk Engineering, Axio
Shannon Hughes – Cybersecurity Business Operations Manager, Department of Energy
Barry Jones – Cybersecurity, Western Area Power Administration
Jamison Jangula – Cybersecurity Analyst, University of North Dakota
Dr. Prakash Ranganathan – Associate Professor of Electrical Engineering and the Director for the Center for Cyber Security Research, University of North Dakota

Join the Western Area Power Administration, Department of Energy, Axio, and University of North Dakota School of Electrical Engineering and Computer Sciences (SEECs) for a discussion of cyber and physical risks to the Bulk Electric System operational technology and industrial control systems. This panel will tie risk program areas together to discuss and spotlight examples, methods and tools to identify, quantify, mitigate and monitor risks to electric sector operations, engineering and supply chain as well as future considerations for protecting key assets.

Reliability, Security, and Cloud Technology – 6B

(Hilton, Plaines)

Ranjan Banerji – Principal Partner Solutions Architect, Amazon Web Services
Kristine Martz – Industry Specialist, Energy & Utilities, Amazon Web Services
Sean Murray – Senior Partner Solutions Architect, Amazon Web Services
Maggie Powell – Principal Industry Specialist, Energy & Utilities, Amazon Web Services

Modern society relies on the utility industry for safe, secure, reliable, and resilient electric energy. Cloud technology is increasingly supporting business, analytics, and operations, providing significant benefits. As an emerging and widely used technology, cloud technology has significant benefits that can improve upon existing business use cases – from offline tools, to near-real-time assessments, to online applications. This session helps you put into perspective a wide range of requirements including business, engineering, security and compliance, and how cloud technology can help.

Breakout Sessions Descriptions

Wednesday, October 18: 1:30 – 2:30 p.m.

Cyber Security: ICS/OT Cyber security: Current Threats and Vulnerabilities in the Electric Sector

(Hilton, Kent)

Jose Avila-Gomez – Industrial Consultant, Dragos

The industrial cyber threat landscape constantly changes with new adversaries, vulnerabilities, and attacks that put operations and safety at risk. During this presentation, Jose Avila-Gomez summarizes what you need to know about current threats targeting electric companies, including: cyber events that dominated the headlines, the current ICS/OT threat landscape, threat groups targeting electric, findings from incidents and threat hunts, impact of ransomware, and trends in ICS/OT vulnerabilities.

Physical Security: Violent Extremist Panel*

(Hilton, Palais)

Lauren Alexander Binns – Physical Security Analyst, E-ISAC

Fred Hosling – Senior Intelligence Analyst, Public Safety Canada

Ross Johnson – President, Bridgehead Security

Andrea Van Peteghem – Program Manager, Senior Corporate Security Department, Pacific Gas and Electric Company

Discussion on the state of violent extremism in Canada and the United States as well as the intelligence frameworks and methods being used to combat this.

This session is closed to media and will not be recorded

Supply Chain: Relying Upon the Work of Others for Supply Chain Risk Management*

(Hilton, Saint Foy/Portneuf)

Valerie Agnew – General Counsel, NATF

Jennifer Couch – EMS Compliance and Quality Assurance Manager SCS Transmission, Southern Company

Christopher Fitzhugh, CISSP, GICSP, GCIP – Industrial Cybersecurity Lead, Siemens

Tony Hall – Manager, CIP and Federal Regulatory Compliance, LG&E and KU Energy

Frank Harrill – VP, Security, Schweitzer Engineering Laboratories, Inc.

Michael Pyle – Director of Product Cyber Security for the Energy Management Business Unit, Schneider Electric

A panel of electric industry supply chain risk management subject matter experts and representatives from key suppliers of bulk power system products and services will discuss how entities and suppliers can rely upon and optimize the work of others while avoiding potential pitfalls.

NATF staff will convene and moderate the panel, opening with an overview of how relying upon the work of others is integrated into the NATF Supply Chain Security Assessment Model, the NATF Supply Chain Security Criteria, and the Energy Sector Supply Chain Risk Questionnaire. The overview will be followed by the panel discussion on how industry, suppliers, and third-party assessors can work together to leverage third-party assessments and certifications to optimize approaches to understanding and managing supply chain security risks.

This session is closed to media and will not be recorded

Special Topics: Maximizing the Intelligence Cycle for a More Secure Grid

(Hilton, St. Louis)

Amanda Olson – Senior Advisor | National Security and Emerging Risk, Southern California Edison

This session will focus on attributes of a mature intelligence cycle and equip attendees to self-appraise and improve their own intelligence program. Attendees should walk away from the session with a clear set of opportunities to tighten up processes and key relationships to better protect critical infrastructure from cyber and physical threats.

Wednesday, October 18: 2:45 – 3:45 p.m.

Cyber Security: Ransomware: Current Trends and Mitigation TTPs

(Hilton, Kent)

Aurora Johnson – CISA JCDC Partnerships, U.S. Cybersecurity and Infrastructure Security Agency

Ransomware remains one of the major threats to cyber and critical infrastructure across North America. Recent years have highlighted the need for private industry and government collaboration to mitigate and respond to the growing number of ransomware attacks. The proposed panel will discuss both the CISA and CCCS-observed ransomware trends, mitigation measures, and the tactics, techniques, and procedures used in real-life incident response scenarios.

Physical Security: What's Unacceptable – to You?

(Hilton, Palais)

Travis Moran – Senior Reliability & Security Advisor, SERC Reliability Corporation

CIP0-014 can seem irrelevant for many smaller entities; however, the process used to comply is useful for entities at all levels. Unacceptable consequences apply to every utility system at every level. This session will help entity physical security personnel identify what unacceptable consequences are to their system and the process to understand, protect, and mitigate threats.

Supply Chain: Securing Software's Supply Chain

(Hilton, Saint Foy/Portneuf)

Krista Koors – Lead Cyber Security Analyst, Burns & McDonnell

Securing the supply chain is a complex topic, not only due to the uptick in cyber attacks and the release of executive orders and other federal guidance, but also due to the constantly changing regulatory compliance environment. Additionally, with specific ramifications in the electric utility industry if vulnerabilities in the supply chain are left unaddressed, there is added pressure to identify and mitigate these vulnerabilities in a timely manner. Software supply chain attacks continue to be a concern for utilities as risks continue to grow and evolve. To address these risks across the software supply chain of our power grid, this session dives into learning how to identify and mitigate vulnerabilities in the software supply chain, understanding challenges related to securing the software supply chain, and recognizing methods to secure open-source software and cloud-based software.

Special Topics: Efficiency Unleashed: Eversource's Journey to Integrated Process Management and Data Visualization

(Hilton, St. Louis)

Jonathan Kitchin – Vice President of Solutions and Service Delivery, Karta

Vicki O'Leary – Director – NERC Reliability and Compliance, Eversource Energy

In 2021, Eversource sought a re-imagining of its approach to project team coordination and evidence management. Limitations to existing software tools and the challenge of coordinating cross-functional activities cost the organization hundreds of man-hours. Leadership felt that the time spent chasing evidence requests and approvals could be redirected into efforts that better

contribute to the resiliency and security of the organization by deploying a user-friendly, automated tool. In partnership with Karta, a consulting organization focused on the utility sector, Eversource deployed a solution built on the Archer Integrated Risk Management platform. This solution centralized a variety of processes and reduced the manual effort in preparing for audits and tracking potential noncompliance. Through integrated data visualizations and increased stakeholder awareness, leadership was positioned to make wiser investments in the future. This session provides an overview of how to drive successful process change and lessons learned throughout implementing an integrated risk management platform.

Wednesday, October 18: 4:00 – 5:00 p.m.

Cyber Security: Evolving Threats from Malicious Use of AI

(Hilton, Kent)

Dennis Gilbert, Jr. – Founder & CEO, Vector9 Consultants, LLC

Artificial intelligence (AI) and machine learning capabilities are growing at an unprecedented rate and will have many widely beneficial applications, but less attention has been paid to the ways in which AI can and will be used maliciously by both advanced cyber threat actors as well as the novice. During this breakout session, the discussion will highlight that as malicious use of AI capabilities becomes more mature and widespread, the threat landscape the electricity sector will face will change as well with the expansion of existing threat, the introduction of new threats, and changes in tactics and techniques of threat actors.

The presentation will then pivot to focus on three specific areas that will be of concern for the electricity sector and provide representative examples, which are IT and OT security, physical security, and corporate security.

The session will close by providing attendees with actionable insight regarding means to forecast, prevent, and (when necessary) mitigate the potentially significant impacts to the grid due to the malicious use of AI.

Physical Security: Gunfire Threats to the Grid and Potential Impacts*

(Hilton, Palais)

Dr. Henry Chu – Scientist and Engineer, Idaho National Lab

Frank Gauthier – Critical Infrastructure Protection and Compliance, Pacific Gas and Electric Company

Mark Maney – Manager of Economic Development and Governmental Affairs, Southern Company

Rob Siefken – Chief Operating Officer, Safeguards3

In this session, we will take a look at specific ballistic trends impacting the electric grid and strategies for mitigation.

This session is closed to media and will not be recorded

Supply Chain: Operationalizing SBOMs for the Energy Sector

(Hilton, St. Louis)

Emily Fesnak – Senior Consultant, Deloitte

Joseph Price – Senior Manager | Specialist Leader, Deloitte

Major events like SolarWinds, Log4j, and ongoing advanced persistent threat groups exploiting known vulnerabilities that target sectors worldwide, including the energy sector, have highlighted the threats unhandled software vulnerabilities pose to the global supply chain. The damaging impacts of these hacking events have prompted companies to innovate their Cyber Security Supply Chain Risk Management programs to include the verification of software integrity. A valuable source of data that can help fortify software supply chains is the Software Bill of Material (SBOM). While some may consider SBOMs a box to check on a list of regulatory requirements, when used effectively, SBOMs are key tools for enhancing transparency and security within the supply chain. Operationalizing SBOMs by using predictive analytics and vulnerability trend data shifts software supply chain security to be more innovative and proactive. Attendees will leave with an understanding of what emerging SBOM standards and

solutions means for organizations, how SBOMs can increase software supply chain security, and use cases for making SBOMs work within their organization's supply chain.

Cyber Security: Information Sharing – Can We Really Be Anonymous?

(Hilton, Saint Foy/Portneuf)

Frank Honkus – Director, Cybersecurity Risk Information Sharing Programs, CRISP, E-ISAC

Danielle Jablanski – OT Cybersecurity Strategist, Nozomi Networks

Carter Manucy – Senior Manager, Cybersecurity, NRECA

Mara Winn – Deputy Director, Preparedness, Policy, and Risk Analysis Division, Office of Cybersecurity, Energy Security, and Emergency Response

In this session, the panel will explore the importance of responsible data collection and effective information sharing. It will highlight various organizations and their missions in this field along with current trends and efforts to promote anonymous information sharing. The panelists will highlight the entities that seek information, including DOE, CISA, NRECA and the E-ISAC. The panelists will also dive into the missions of different efforts, such as ETAC, CRISP, and NRECA's TAC.

The panel will discuss the pros and cons of anonymized information sharing and the new approach offered by ETHOS as well as the current trends in information sharing.

Thursday, October 19 – 8:30 – 9:30 a.m.

Cyber Security: Future-Proofing NERC CIP: An Impossible Dream?

(Hilton, Kent)

Jason Christopher – Certified Instructor, SANS

We've heard it before: "regulation will always lag behind threat actors." This long-held belief has driven continued iterations of the NERC CIP standards, but what if it was not true? What if there was a way to futureproof the NERC CIP requirements? What if it's already been done with other global cyber security regulations that we can use as a model for growth? That's right, the future-proofing of OT security programs has happened elsewhere, and it happened recently. 2022 saw the largest growth in ICS security standards, laws, and regulations ever. A majority of these efforts shared the same themes, security controls, and goals: keep bad guys out of critical infrastructure. Dating back to Order No. 706, FERC and others have always expressed an interest in learning from other standards and best practices. As such, NERC CIP professionals need to be aware of how 2022 has already shaped the ICS/OT security programs of 2032 (and how to prepare for potential changes in NERC CIP as a result). Join Jason D. Christopher, SANS Certified Instructor and Author, as he provides a meta-analysis of this exponential growth in ICS security regulations and guidelines. Learn what your NERC CIP program needs to plan for today to be better prepared tomorrow. The future is already here.

Physical Security: Mitigating the Activist Threat

(Hilton, Palais)

Harris Stephenson – Chief Analyst, FORESIGHT Reports

Activism poses a range of physical security threats to utilities and overall grid security. From high-profile substation attacks to protests targeting assets or people, activism presents persistent challenges. The ability to understand the motivations and goals behind activist campaigns as well as an awareness of the diversity of tactics employed by activists from mainstream campaigners to extremists is essential to securing utilities and the grid. This is especially important as utilities transition to renewables, exposing them to novel threats and issues. This session will provide a solid understanding of the physical risks posed by activism to utilities and the security of the grid, as well as techniques for how to assess these risks. This will include a checklist to assess threats and recommendations for how to monitor, prepare for, and mitigate them.

Supply Chain: The Various Shades of Supply Chain: SBOM, N-Days

(Hilton, Saint Foy/Portneuf)

Alex Matrosov – CEO and Founder, Binarly, Inc.

Over the past two years, attacks on multiple targets in the semiconductor industry have consistently led to leaks of firmware source code. A compromised developer device could potentially give an attacker access to the source code repository, adding a major gap in the security of the software supply chain. There are multiple policies in place to improve transparency in the firmware supply chain in general, but implementing and adopting them will take years.

The technology industry is in the midst of active discussions about the use of "software bill of materials" to address supply chain security risks. To implement supply chain security practices, there must be better transparency on software dependencies. Previously, any piece of software shipped as a black box without providing any information related to software dependencies and third-party components. Firmware has largely been looked at in the same way.

We already discussed in our previous talks the multiple levels of complexity in the UEFI firmware ecosystem and supply chain taxonomy and the firmware supply chain complexity topics regarding the firmware update delivery and how the timing plays a negative role to give an attackers advantage to adopt already known vulnerabilities (N-days) to their attacks in last year's research "The Firmware Supply-Chain Security Is Broken: Can We Fix It?" The silicon vendor reference code vulnerabilities are always the worst since they impact the whole industry and all the device vendors have used the same chips on their devices. When it comes to applying mitigations, how does the industry take advantage of them, and who controls their adoption in the firmware? Those are all good questions, but unfortunately, no positive news can be shared.

The system firmware attack vectors will be discussed in this talk from the perspective of attacking the operating system or hypervisor. The nature of these attacks breaks the foundation of confidential computing and often creates problems for the entire industry. This talk will focus on practical examples of such attacks and how they are dangerous.

Special Topics: Data Sharing Programs – Their Maturity and Impact to the North American Grid from an Industry Perspective

(Hilton, St. Louis)

Frank Honkus – Director Cybersecurity Risk Information Sharing Program, CRISP – E-ISAC

William Lu – Director, Independent Electricity System Operator (IESO)

For the past decade, the United States and Canadian governments have identified the need to safeguard critical infrastructure from persistent and sophisticated threats. Data sharing programs on OT and IT utility environment involving government enrichment is a key collective defense tool to assist utility organizations. This panel will discuss current available programs that a utility member can join, discuss the need of these complimentary programs, and the information sharing collaboration required between government and industry.

Thursday, October 19: 9:45 – 10:45 a.m.

Cyber Security: Enhancing Cyber Security for Electric Utilities: A Comprehensive Approach to Safeguarding Critical Infrastructure

(Hilton, Kent)

Sean Tomecko – Lead Security Researcher, Finite State

The electric utility industry faces a growing number of cyber threats, making it essential to protect critical infrastructure and the software supply chain. Join cyber security expert Jason Ortiz for an in-depth discussion on the latest challenges facing the electric utility sector and how SBOMs can help, both in detecting vulnerabilities and supporting vulnerability management programs. This session will provide valuable insights into the current cyber security landscape with a focus on the electric utility industry. We will explore why attackers love the huge attack surface presented by operational technology, the key pain points facing

stakeholders in today’s electric-sector software supply chains, and effective industry best practices that can contribute to the overall resilience of our critical infrastructure. Additionally, we will discuss the emerging importance of software bill of materials in ensuring software supply chain security. By incorporating these essential tools and strategies, electric utility professionals can confidently address and mitigate the ever-evolving cyber threats facing their industry. Join us to enhance your understanding of the latest cyber security measures and best practices that will empower your organization to strengthen its resilience and secure the future of America’s electric utilities.

Physical Security: Resources Roundtable

(Hilton, Palais)

Kristen Bove – Manager, Physical Security, E-ISAC

Adam Deluca – Director of Security Operations, E-ISAC

Ross Johnson – President, Bridgehead Security

Rob Siefken – Chief Operating Officer, Safeguards 3

This session is to provide a brief but substantive overview of the types of resources currently available to members; including what their strengths and use cases are and how they can follow up to access the full content.

This session is closed to media and will not be recorded

Special Topics: Aggregated DERs – Grid Security and Reliability

(Hilton, Saint Foy/Portneuf)

Sharon Brown – President and CEO, EOSS

FERC Order 2222 was approved in September 2020. The rule requires that U.S. Independent System Operators and Regional Transmission Organizations develop plans that give distributed energy resources access to wholesale energy markets. This order, coupled with the Inflation Reduction Act of 2022, has spurred significant investment in distributed energy resources (DER), including aggregated DERs. In addition, Canadian demand response best practices and technology deployments are also being shaped with the help of energy market participants. Aggregated DERs/distributed energy resource management systems (DERMS) and virtual power plants have the ability to enhance and the potential to undermine the reliability of the bulk power system. Traditional application of NERC Reliability Standards to evolving demand response technology is not practical; consequently, a robust conversation about protecting inordinately large volumes of telemetered data between VPP/DERMS participants is essential. Likewise, power electronics and secure data movement warrant deep technical discussions when applied to various energy use cases. This session will focus on emerging technologies/best practices to securely and reliably navigate the intersection of distributed computing and data analytics with distributed energy.

Thursday, October 19 – 11:00 a.m. – 12:00 p.m.

Cyber Security: Power Grid Containment Test: Hydro Québec Achievement

(Hilton, Kent)

Mario Tanguay – Senior Director, Cybersecurity and Chief Information Security Officer, Hydro Québec

With the number of cyber attacks on energy companies on the rise around the world, Hydro-Québec performed a great achievement when it successfully carried out an electrical containment test. To assess its systems in real time, the government-owned corporation completely isolated itself from the web and Internet for four hours without interrupting service. Meticulous planning and unprecedented coordination made the operation possible. **This presentation will be held in French (translation available).**

Physical Security: Design Security into a Facility from the Beginning

(Hilton, Palais)

Larry Fitzgerald PG, CPTED, PSP, CPP – Director of Security & Emergency Management, TRC Engineers, Inc.

Jim LaPrade, NCARB/RA, CPP – Manager/Senior Consultant, TRC Engineers, Inc.

Facilities like primary control centers and transmission substations are often solely designed for engineering, architectural functionality, and space needs. In this session, our security consulting team will discuss how engaging security experts early in the design process helps to minimize vulnerabilities. We will share numerous examples of the benefits of designing security in from the beginning to ensure facilities as secure as possible as efficiently as possible. You won't want to miss this session as we address the ideal location for critical assets, sightline strategies, defining and enforcing the active perimeter, ballistic considerations, access control, and situational awareness.

Cyber Security: Defending the Grid—Approaching AI Security

(Hilton, Saint Foy/Portneuf)

Katie Boswell – Managing Director, KPMG US

Kristy Hornland – Director, KPMG US

AI adoption has accelerated, and it is increasingly important to consider the expanded threat landscape and what it can mean for organizations that support critical infrastructure. Our speakers, Katie Boswell (National Leader of KPMG U.S. AI Security Services) and Kristy Hornland (KPMG U.S. AI Security Services Director) will share lessons learned from the development of a securing AI practitioners and leadership guide, leveraging insights from public sectors initiatives (CISA, NIST), academia, research bodies, private sectors (ISACs/Trade associations), and public companies (including the utility sector) in defining critical AI security threats and developing a strategy and roadmap to protect these organizations. Throughout this session, our speakers will embed real world examples of adversarial AI techniques to build attendees' awareness as to potential threat vectors their organizations should be considering as they begin to plan for overall strategy and governance.

Special Topics: Security Challenges of the Future Grid

(Hilton, St. Louis)

Kristen Bove – Manager, Physical Security, E-ISAC

Stephen Crutchfield – Principal Technical Advisor and Coordinator for the RSTC, NERC

Frank Gauthier – Critical Infrastructure Protection and Compliance, Pacific Gas and Electric Company

Calvin Ramos – Senior Cyber Threat Intelligence Analyst, E-ISAC

Discussion of NERC's grid reliability reports, and the security challenges raised during periods of grid vulnerability. Review of NERC's long-term reliability forecast and what this means for cyber and physical security.

This session is closed to media and will not be recorded

Thank You to our GridSecCon 2023 Sponsors

Platinum Sponsor



Gold Sponsors



Silver Sponsors



Critical Infrastructure Protection



Bronze Sponsors



GridSecCon 2023 Sponsors

Translation Sponsor



Wi-Fi Sponsor



Wednesday Lunch Sponsor



Lanyard Sponsor



Keycard Sponsor



Critical Infrastructure Protection

Women's Breakfast Sponsor



Thursday Breakfast Sponsor



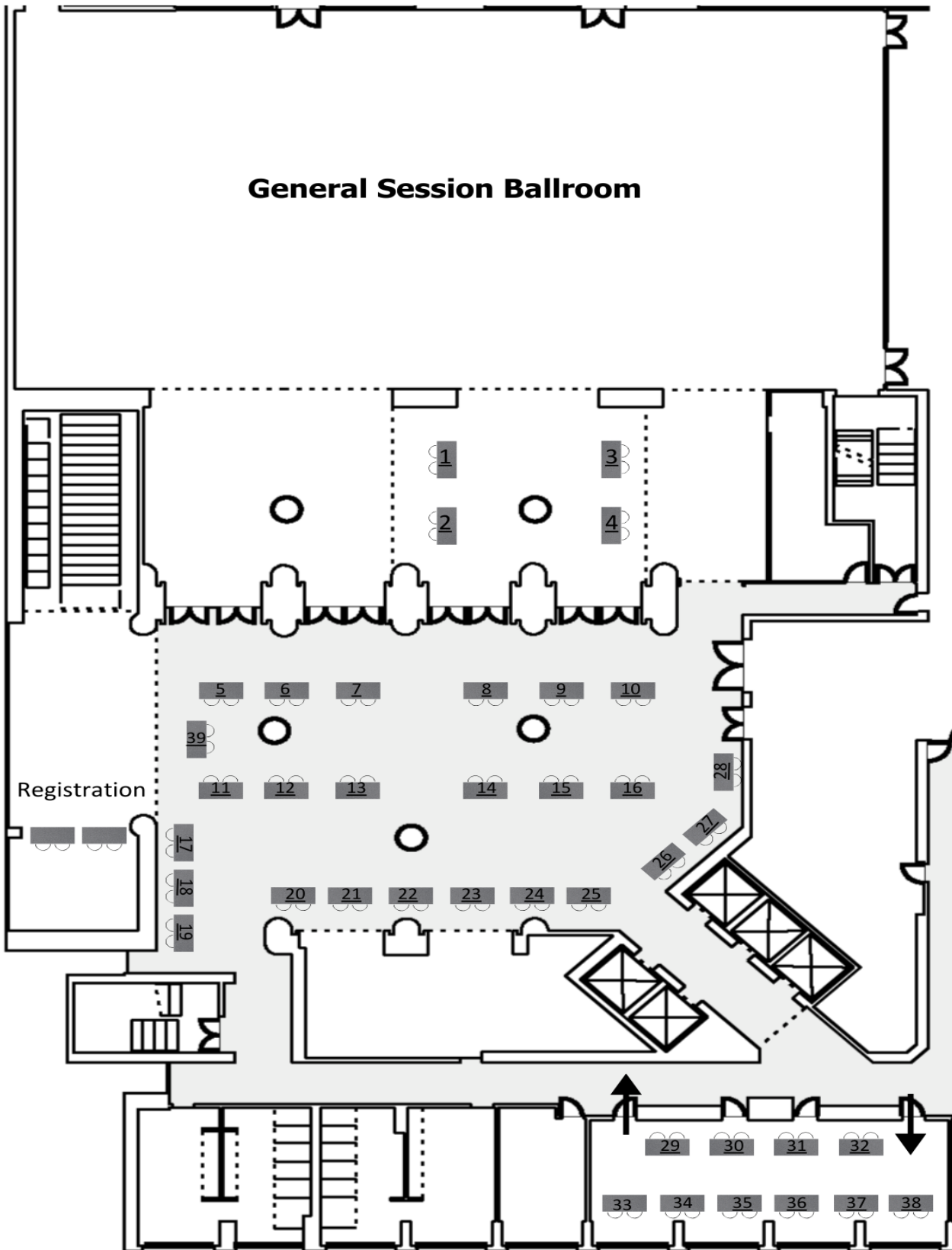
Thursday Break Sponsor



Cyber Track Sponsor



Exhibit Hall Map



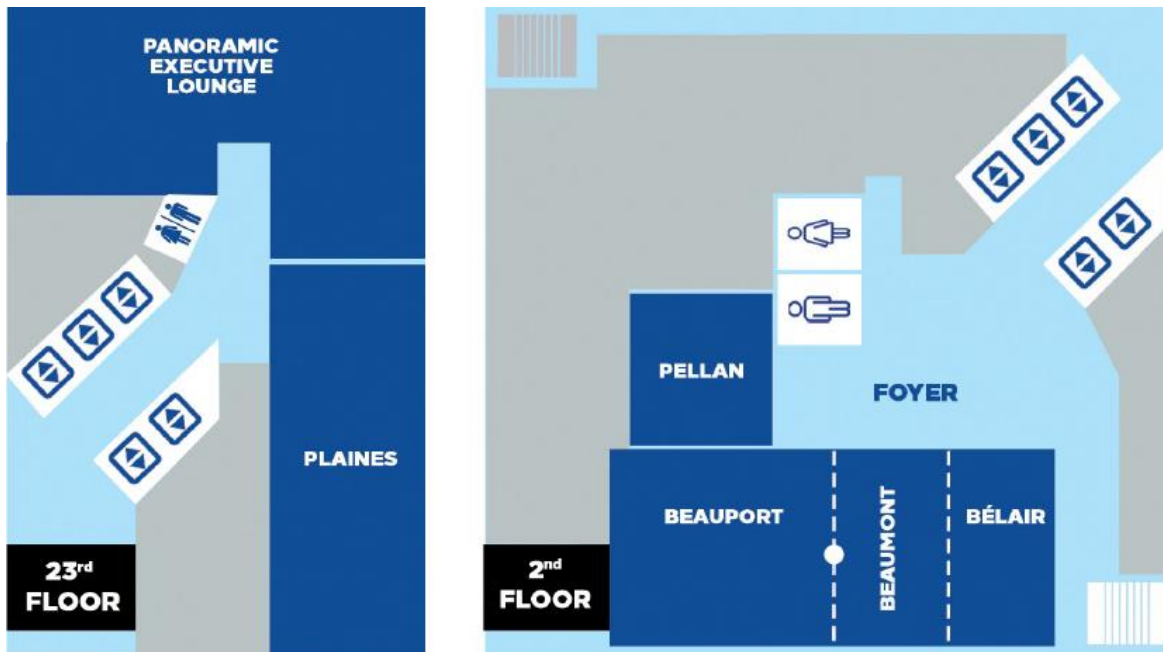
Exhibitor and Sponsor Booth Listing

<u>Company Name</u>	<u>Booth #</u>	<u>Company Name</u>	<u>Booth #</u>
ArmorText	1	Motorola Solutions	20
Clearforce	2	Motorola Avigilon	21
SANS Institute	3	Xtec	22
Waterfall Security	4	Operant Networks	23
Verve Industrial	5	LUNA Innovations- OptaSense	24
Ameristar Perimeter Security	6	Assurx	25
ITEGRITI	7	Dragos	26
Siemens Energy	8	Karta Corp	27
Network Perception	9	Archer Integrated Risk Management	28
Fortinet	10	IPKeys Cyber Partners	29
1898 & Co.	11	EnergySec	30
Burns & McDonnell	12	E-ISAC CRISP	31
Finite State	13	E-ISAC	32
Cyware	14	UND School of Electrical Engineering and Computer Sciences	34
AMICO Security	15	Deloitte	36
Industrial Defender	16	3bProtection	37
Fortra	17	Subnet Solutions	38
Electric Power Engineers	18	Archer Energy Solutions	39
Bosch Security Systems	19		

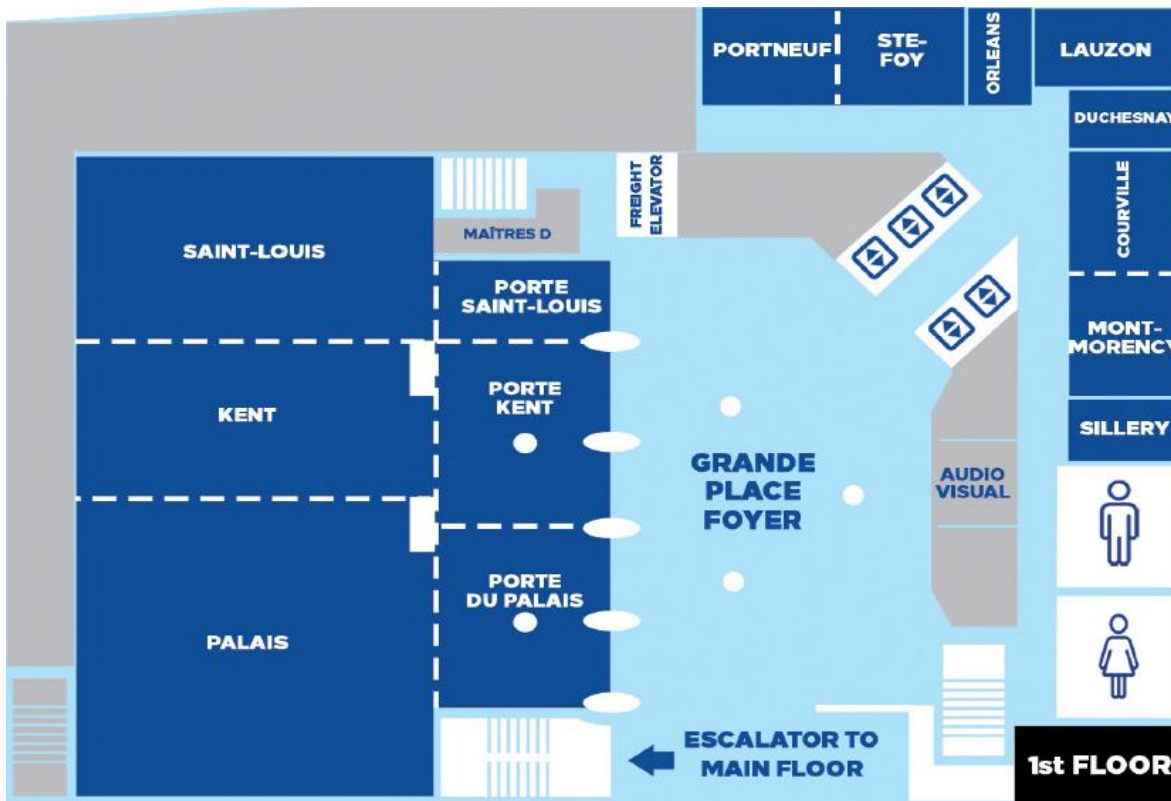
Thank You to our GridSecCon 2023 Exhibitors



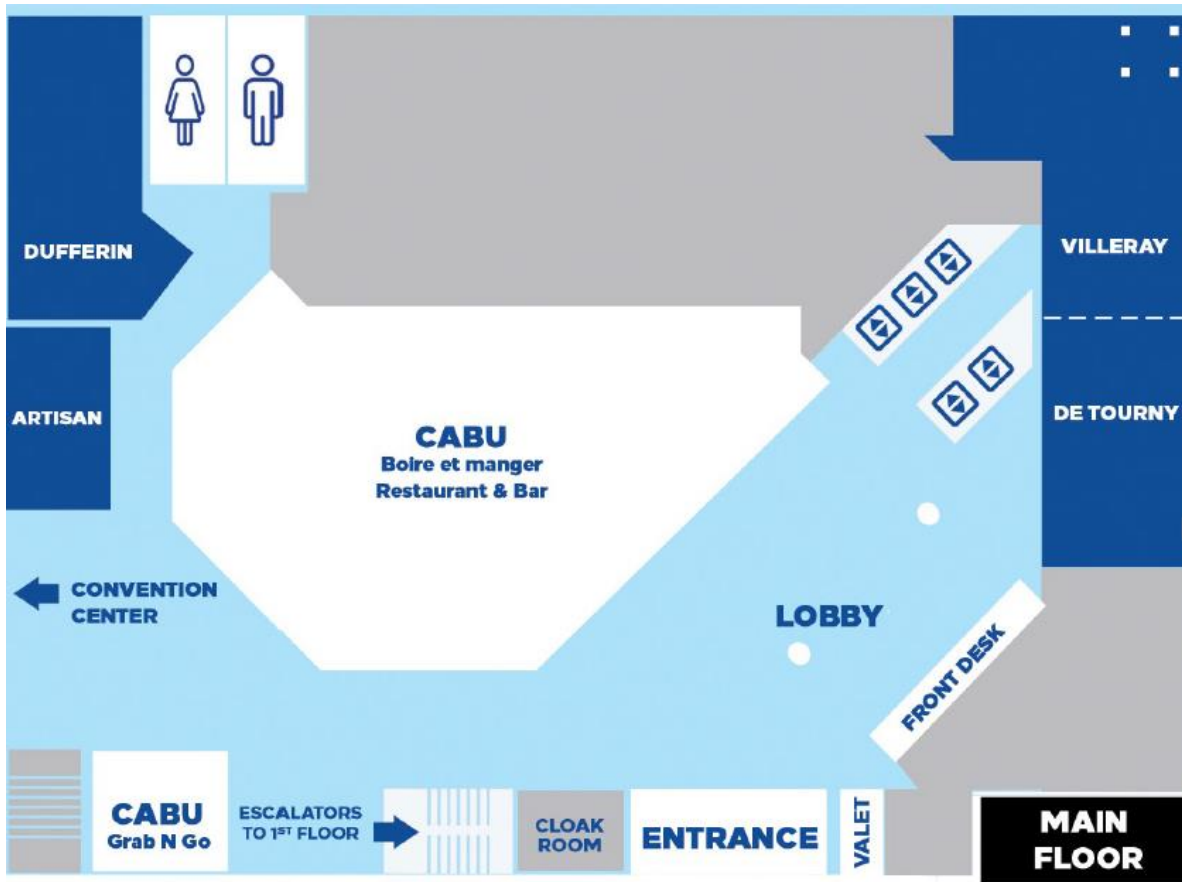
Hilton 23rd and 2nd Floor



Hilton First Floor



Hilton Main Floor





CYBER FUSION for Energy

Only Cyware brings it all together

Threat Intelligence
Management

Security
Collaboration

Orchestration &
Automation

Cyber Fusion from Cyware brings together threat intelligence, AI-automation, incident response, and security collaboration to break down silos and elevate your SOC.



1898  **CO.**

GAIN OPERATIONAL RESILIENCY
**THROUGH MANAGED OT/ICS
THREAT PROTECTION.**

— • •



SIEMENS
energy

Chance of OT
cyberattack
100%

Learn more about our Manage, Detection & Response solution for mission critical operations.

Visit us at booth #8



VERVE

**DETECT & RESPOND
IN ONE PLATFORM**

Speed to remediation for true
OT cybersecurity progress

info@verveindustrial.com

www.verveindustrial.com



ITEGRITI

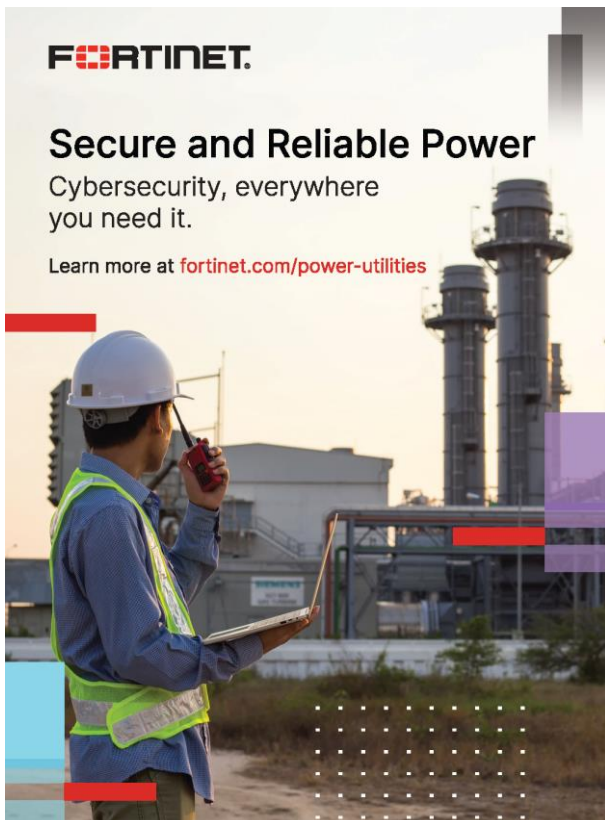
CRITICAL INFRASTRUCTURE
Cybersecurity + Compliance + Managed Services

Since 2008, the ITEGRITI team has completed NERC CIP projects in all regions across the U.S. and Canada, supporting utilities, generation, transmission, municipalities, and cooperatives.

- ▶ CIP and TSA SD02 program and compliance assessments
- ▶ CIP audit and SME preparation
- ▶ Asset inventory and site walkdowns
- ▶ NIST CSF security assessments

Visit our booth to meet the Leadership Team!


itegriti.com

FORTINET.

Secure and Reliable Power
Cybersecurity, everywhere you need it.

Learn more at fortinet.com/power-utilities



FINITE STATE

Securing the Software Supply Chain of Today's Electric Utilities

Gain continuous visibility into your software supply chain while increasing the efficiency of penetration testing and vulnerability management

Learn more at finitestate.io



Cybersecurity Risk Information Sharing Program (CRISP)

CRISP is a private-public partnership with the U.S. Department of Energy (DOE), Electricity Information Sharing and Analysis Center (E-ISAC), and the participating members in the energy sector. CRISP is the bilateral sharing of information where it deploys information sharing device(s) (ISDs) to the ingress/egress points of the corporate network and the internet. The participating members share four sets of metadata to the Pacific Northwest National Laboratory (PNNL) for joint classified and unclassified analysis with the DOE’s Office of Intelligence and Counterintelligence, PNNL, and E-ISAC. Reporting is then generated and provided to members.

Member Benefits

- CRISP provides cyber intelligence and members benefit from:
- Focusing on unusual activity within the members’ network
 - Understanding threat actor motivations and intent
 - Highlighting cyber, physical, and insider threats
 - Reporting that is actionable and informed

Products

- CRISP provides a variety of reports and analytics:
- Weekly and biweekly cyber activity snapshots
 - Biweekly geopolitical nation-state threat reporting
 - Indicators associated with identified threat actors and anomalies
 - Trend analysis and participant-wide analytics
 - Reconnaissance analysis and supply chain research



Cost

Membership cost depends on organization size, network data volume, and the number of information sharing device(s) (ISDs) at the organization. Contact CRISP for a free estimate.

Membership

CRISP is a fee-based service open to asset owners and operators in the electricity, oil, and natural gas subsectors, as well as ancillary Energy Sector support organizations.

Attributes

CRISP has several attributes that are unique from those provided by other commercially available cyber risk monitoring services:

- Members own their data and the hardware used to collect it
- Collaborating and partnering opportunities with DOE on government informed data enrichment
 - Integrating cyber related threat information gathered from the information sharing device(s) (ISD) installed at the members’ network perimeter
- Identifying correlations and trends across the members within the electricity sector
- The CRISP community shapes the trajectory of the program

Information about the program and membership:
crisp@eisac.com
<https://www.eisac.com/s/crisp>



E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Vendor Affiliate Program

TLP: CLEAR - Disclosure is not limited

The electricity threat landscape continues to evolve with new security vulnerabilities, changing technologies, extreme weather, and bold adversaries. The E-ISAC Vendor Affiliate Program allows qualified manufacturers and cyber and physical security solutions providers the opportunity to join the E-ISAC community to collaborate and share information directly with E-ISAC utility members. The E-ISAC is looking for the vendor community to join in sharing and exchanging information with the E-ISAC and its members, and promote collective defense across the sector.

- The Vendor Affiliate Program is open to:
- Electricity industry original equipment manufacturer suppliers
 - Cyber and physical security solutions companies
 - Providers of other related technology, product, or information services to electricity and/or other critical infrastructure stakeholders

The E-ISAC Vendor Affiliate Program is focused on facilitating information sharing and best practices in a trusted environment for member and partner organizations

Please visit the Vendor Affiliate Program webpage to learn more. Questions? Contact vendorprogram@eisac.com.

Program Benefits

- **Connect with Members:** Engage with E-ISAC members at events such as GridSecCon, the Industry Engagement Program, working groups, and more
- **Serve as an Industry Leader:** Provide subject matter expertise on critical vulnerabilities and security solutions through monthly security briefings and special topic webinars
- **E-ISAC Portal Access:** Obtain the latest industry threat information and analysis



GRIDSEC CON 2023
NERC • E-ISAC • NPCC
