GRIDSECCON 2021

NERC • E-ISAC • TEXAS RE

October 18–20, 2021

2021 GridSecCon Program Welcome Letter

Welcome to our tenth annual grid security conference, GridSecCon 2021! This is our first year in a completely virtual environment, but we are confident you will find it just as engaging and informative as our previous events. This year's event is co-hosted by NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), and Texas Reliability Entity, Inc. (Texas RE) as part of the Electric Reliability Organization (ERO) Enterprise's collaborative efforts to support industry in securing the North American bulk power system through information sharing, education, and collaboration.

Although we canceled GridSecCon 2020 due to the pandemic, the bad actors have not missed a beat. Since we last convened, we have witnessed multiple headline-grabbing compromises from ransomware to major hacks and physical breaches, making GridSecCon even more relevant as we come together to discuss threats and solutions to help enhance our security efforts. NERC's E-ISAC seeks to be an essential part of enhancing these efforts by helping to educate industry about threats and solutions and by working to strengthen the cyber and physical security of our grid.

Security and reliability are inextricably linked, and events like GridSecCon help industry plan and prepare for contingencies through training, information sharing, and lessons learned. To be successful, we are building a collective defense to avoid, mitigate, and solve our critical security challenges. It is clear from this year's record number of registrants that cyber and physical security remain a top priority in the industry's reliability efforts.

Our program this year is very exciting, and we are delighted that we will have a virtual conversation with U.S. Department of Energy (DOE) Secretary Jennifer Granholm on the second day. During the two days, industry leaders from Texas RE, Analysis and Resilience Center for Systemic Risk, Center for Strategic and International Studies, SolarWinds, and TAG Cyber will share insights into latest strategies and solutions.

The agenda also includes training, panel discussions, and breakout sessions on the Administration's 100-day plan, supply chain lessons learned, the current threat landscape, GridEx, and game-changing research and development. At the conclusion of GridSecCon 2021, we will announce the winner of the inaugural E-ISAC Electricity Security Service Award in honor of Michael J. Assante, who was instrumental in establishing the E-ISAC. The award recognizes individuals or teams that have made significant contributions to support the security of the North American electricity industry.

We know our industry takes security risks seriously, and we remain vigilant as our adversaries continue to develop more sophisticated campaigns that place the North American grid at risk. This is why a learning environment like GridSecCon is increasingly important. We cannot assure reliability without also assuring the security of the North American bulk power system. GridSecCon is one way that the ERO Enterprise fosters a learning environment that supports this common goal. We look forward to the discussions and a successful conference.

Jim Robb
President and Chief Executive Officer
North American Electric Reliability Corporation

Jim Albright
President and Chief Executive Officer
Texas Reliability Entity, Inc.

Agenda

Monday, October 18 | Training

11:00 a.m. – 3:00 p.m. **Training Sessions**

Training Topic	Training Provider
OT Cyber Risk Management	Waterfall Security Solutions
Cyber Physical Grid Training: Cyber-Physical Electric Grid Analysis of Threats, Impact and Defense	Texas A&M University
Sneak Peek at SANS ICS 418-ICS for Managers Course	SANS and Dragos
Building a Phishing Simulation Training Program Without Barriers	Curricula
5G Security 101: From Radio to Cloud	Deloitte
How to Build an Insider Threat Program	Carnegie Mellon Software Engineering Institute
Making Supply Chain Management Work for You	aDolus Technology, Inc.

4:00 – 7:00 p.m. **SANS and Dragos Industrial Control Systems Capture the Flag - DAY 1**

Tuesday, October 19 | DAY 1

11:00 – 11:15 a.m. **Welcome/Opening Remarks**
Manny Cancel – NERC Senior Vice President and CEO, E-ISAC

11:15 – 11:30 a.m. **Regional Entity Keynote**
Jim Albright – President and CEO, Texas RE

11:30 – 11:45 a.m. **Keynote**
Suzanne Spaulding – Senior Adviser, Homeland Security, International Security Program Center for Strategic and International Studies

11:45 – Noon **Keynote**
Bruce Walker – Head of Energy Risk Operations/Energy Chief Risk Officer, Analysis and Resilience Center for Systemic Risk

Noon – 12:15 p.m. **Transition/Break** *(sponsored by Dragos)*

12:15 – 1:15 p.m. **Concurrent Breakout Sessions**

Collective Cyber Defense for NY State Municipalities and Co-Ops
Vic Costanza – Senior Director and Deputy CISO, New York Power Authority
Shawn Wallace – VP Energy, IronNet

Digital Transformations and Precision Time Security – A Roadmap for Risk Mitigation *(sponsored by Keysight Technologies)*
Christine Hertzog – Principal Project Manager, Electric Power Research Institute
David Howard – Office of Electricity Delivery and Energy Reliability, DOE

How Do Your Trade Associations Help the Industry Become More "Cyber Secure"? *(sponsored by Dragos)*
Bridgette Bourge – Director, Legislative Affairs, National Rural Electric Cooperative Association (NRECA)
Fritz Hirst (moderator) – Director, Legislative and Regulatory Affairs, NERC
Alex Hoffman – Vice President, Technical and Operational Services, American Public Power Association
Leah Michalopulos – Director, Government Relations, Canadian Electricity Association
Hailey Siple – Manager, National Security Policy, Edison Electric Institute

Safe and Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E) *(sponsored by Network Perception)*
Adam Gormley – Control Systems Engineer, Chelan PUD
William Hofer – Cyber Security Engineer, Pacific Northwest National Laboratory

Security Concerns with DNP3
Jacob Brodsky – IT Specialist (INFOSEC), Federal Energy Regulatory Commission

Security Threats from Drones
Alex Benoliel – Director, Corporate Security, Southern California Edison
Benjamin Gibson – Senior Physical Security Analyst, E-ISAC
William "Tom" Hewitt – Chief, Unmanned Aircraft Systems Threat Integration Cell, U.S. Department of Homeland Security
Travis Moran – Vice President of Operations, Welund North America

1:15 – 1:30 p.m. **Transition/Break** *(sponsored by IronNet)*

1:30 – 2:30 p.m. **Concurrent Breakout Sessions**

A Year of Supply Chain Lessons

Brian Barrios (moderator) – VP of Cybersecurity and IT Compliance, Southern California Edison
Tim Brown – CISO and Vice President, Security, SolarWinds
Allan Liska – Senior Security Architect, Recorded Future
Andrew Serwin – U.S. Chair and Global Co-Chair, Data Protection, Privacy and Security Practice, DLA Piper
Zachary Tudor – Associate Laboratory Director, National and Homeland Security, Idaho National Laboratory (INL)

Advancing the Utility Industry's Cybersecurity with Essence

Phil Craig – Founder, BlackByte Cyber Security, LLC
Doug Lambert – Senior Principal, Grid Solutions, NRECA
Emma Stewart – Chief Scientist, NRECA

Best Practices for an Insider Threat Program

Margaret Fenner – Director, Threat Intelligence and Investigations, Enterprise Protective Services, Duke Energy
Greg Klein – Supervisory Special Agent, FBI
Brittany McBride – Insider Threat Fusion Center Team Lead, Southern Company
Jazmin Perez – Manager, Insider Risk and Intelligence Safety, Security and Business Resiliency/Corporate Security, Southern California Edison

Diversity and Inclusion in the Electricity Industry

(sponsored by Tripwire)
Stephen Brown – Director, Cyber and Physical Security, SERC Reliability
Lam Chung – Vice President and Engineer for Strategy, Innovation, and Finance, Midwest Reliability Organization
Joan Jacobs – Vice President, Learning and Inclusion, Con Edison
Janet Sena (moderator) – Senior Vice President, Policy and External Affairs, NERC
Tabice Ward – Area Vice President, Business Security Risk Advisory and Support Services, Xcel Energy

Secure Authentication and Discerning Control

Abdo Saad – Department Manager, Con Edison

The Five Electric Utility Languages

Brent Castagnetto – Senior Security Consultant, Archer
Nick Weber – Senior Security Consultant, Archer

2:30 – 2:45 p.m. **Transition/Break** *(sponsored by Tripwire)*

2:45 – 3:45 p.m. **General Session: Cybersecurity Risk Information Sharing Program (CRISP) Briefing**
Frank Honkus – CRISP Program Manager, E-ISAC
Carter Manucy – Director IT/OT and Cybersecurity, Florida Municipal Power Agency
Michael Toecker – CRISP Task Lead and +30 PM, DOE

3:45 – 4:00 p.m. **Closing Remarks**
Manny Cancel – NERC Senior Vice President and CEO, E-ISAC

4:00 – 7:00 p.m. **SANS and Dragos Industrial Control Systems Capture the Flag Challenge DAY 2**

Wednesday, October 20 | DAY 2

11:00 a.m. **Welcome**
Manny Cancel – NERC Senior Vice President and CEO, E-ISAC

11:00 – 11:30 a.m. **Keynote: Virtual Conversation with the Honorable Jennifer Granholm**
The Honorable Jennifer Granholm – Secretary of Energy, DOE
Jim Robb – President and CEO, NERC

11:30 – 11:45 a.m. **Keynote**
Ed Amoroso – CEO and Founder, TAG Cyber LLC

11:45 – Noon **Keynote**
Tim Brown – CISO and Vice President, Security, SolarWinds

Noon – 1:00 p.m. **Concurrent Breakout Sessions**

Incident Response Preparedness Assessment Tool (IRPAT)
Bheshaj Krishnappa – Program Manager, Resiliency and Risk, ReliabilityFirst
David Sopata – Principal, Reliability Consultant, ReliabilityFirst

Ransomware "Are You Ready"? – The Importance of an Integrated IT/OT Defense
(sponsored by Attivo Networks)
Greg Baker – Senior Associate, Incident Response, Booz Allen Hamilton
Kyle Miller – OT Cybersecurity Practice Lead, Booz Allen Hamilton
Bridget Quinn Choi – Director, Incident Response, Booz Allen Hamilton
Juan Villarreal – Senior Associate, Booz Allen Hamilton

Security Regulations: Are We Giving Away the Blue Team Game Plan?
Jason Christopher – Principal, Cyber Risk Advisor, Dragos
Eóin Cooke – Vice President, Security and Information Systems, AltaLink
Lonnie Ratliff – Senior Manager, Cyber and Physical Assurance, NERC
Betsy Soehren-Jones – Director, Cyber and Physical Security Strategy, Exelon

Situational Awareness and Collaboration in Blended IT/OT Events *(sponsored by Nozomi Networks)*
Michael Legatt – CEO and Founder, ResilientGrid
Jodi Heintz Obradovich – Chief Research Scientist, ResilientGrid

The Cybersecurity for the Operation Technology Environment (CyOTE) Methodology
Sam Chanoski – Technical Relationship Manager, INL

The Enemy Within: How to Protect Yourself from a Third Party Breach *(sponsored by Fortinet)*
Jeffrey Sweet – Director, Security Assessments, American Electric Power

1:00 – 1:30 p.m. **Transition/Break** *(sponsored by IronNet, Tripwire, and Dragos)*

1:30 – 2:30 p.m. **General Session: A Decade of GridEx**
Caitlin Durkovich – Special Assistant to the President and Senior Director for Resilience & Response, National Security Council
Kate Ledesma (moderator) – Resilience and Policy Manager, E-ISAC
Adam Lee – Vice President and Chief Security Officer, Dominion Energy
Brock Long – Former Administrator of the Federal Emergency Management Agency, and Hagerty Consulting's Executive Chairman
Mark Weatherford – Chief Strategy Officer and member of the board at the National Cybersecurity Center; Chief Information Security Officer, AlertEnterprise; Founding Partner of Aspen Chartered

2:30 – 3:30 p.m. **General Session: Joint Presentation on 100-Day Plan**
Manny Cancel – NERC Senior Vice President and CEO, E-ISAC
Rob Lee – CEO, Dragos

3:30 – 3:35 p.m. **General Session: E-ISAC Electricity Security Service Award in Honor of Michael J. Assante, Capture the Flag Competition Winners, and Closing Remarks**
Manny Cancel – NERC Senior Vice President and CEO, E-ISAC

GridSecCon 2021 Sponsor Listing

ABLOY USA Critical Infrastructure
6005 Commerce Drive#330
Irving, TX, 75063
800.367.4598
www.abloyusa.com
Jerry Burhans
Jerry.Burhans@assaabloy.com

Archer Energy Solutions, LLC
12042 SE Sunnyside Road
Suite 292
Clackamas, OR 97015
503.347.0052
www.archerint.com
Mark Brahmstadt
m.brahmstadt@archerint.com

Armor Text
1751 Pinnacle Drive Suite 600
McLean, VA 22102
202.800.2074
www.armortext.com
Matt Calligan
matt.calligan@armortext.com

Attivo Networks
46601 Fremont Boulevard
Fremont, CA 94538
510.623.1000
www.attivonetworks.com
Helena Kuly
helena@attivonetworks.com

Burns and McDonnell Engineering Company, Inc.
9400 Ward Parkway
Kansas City, MO 64114
314-944-8974
www.burnsmcd.com
Jarome Farquharson
jfarquharson@burnsmcd.com

Cooper Compliance
1745 Dorado Ridge Trail
El Dorado Hills, CA 95762
678.788.2956
www.coopercompliance.com
Michael Gabriel
info@coopercompliance.com

DeNexus
1 Harbor Drive
Suite 300
Sausalito, CA 94965
443.480.5052
https://www.denexus.io/
jc@denexus.io

Dragos, Inc.
1745 Dorsey Road
Suite R
Hanover, MD 21076
855.372.4670
www.dragos.com
info@dragos.com

Fortinet
899 Kifer Road
Sunnyvale, CA 94086
408.235.7700
www.fortinet.com
Cheryl Hatlevig
chatlevig@fortinet.com

Green IT Energy Applications
1201 N. 3rd Street
#227
Philadelphia, PA 19122
800.275.5870
www.greenitea.com
Glenn McConnell
glenn@greenitea.com

Hagerty Consulting
1618 Orrington Avenue
Suite 201
Evanston, IL 60201
847.492.8454
www.hagertyconsulting.com
development@hagertyconsulting.com

Industrial Defender
225 Foxborough Boulevard
Suite 202
Foxboro, MA 02035
617.675.4206
www.industrialdefender.com
info@industrialdefender.com

IronNet Cybersecurity
7900 Tysons One Place
Suite 400
McLean, VA 22102
215.768.5981
www.ironnet.com
Christine Baker
Christine.baker@ironnetcybersecurity.com

Keysight
1400 Fountaingrove Parkway
Santa Rosa, CA 95403
800.829.4444
www.keysight.com
Eric Floyd
Eric.floyd@keysight.com

Network Perception
20 N Wacker Drive
Suite 1200
Chicago, IL 60606
872.245.4100
www.network-perception.com
info@network-perception.com

Nozomi Networks
575 Market Street
Suite 3650
San Francisco, CA 94105
800.314.6114
www.nozominetworks.com
info@nozominetworks.com

Tripwire
308 SW 2nd Avenue
Suite 400
Portland, OR 97204
503.276.7500
www.tripwire.com
Nikki Holt
nholt@tripwire.com

Verve Industrial Protection
1640 McCracken Boulevard
Paducah, KY 42001
650.793.3885
www.verveindustrial.com
Jessica Howard
jhoward@verveindustrail.com

Thank you to our GridSecCon 2021 Sponsors

Platinum Sponsors

Gold Sponsors

Silver Sponsors

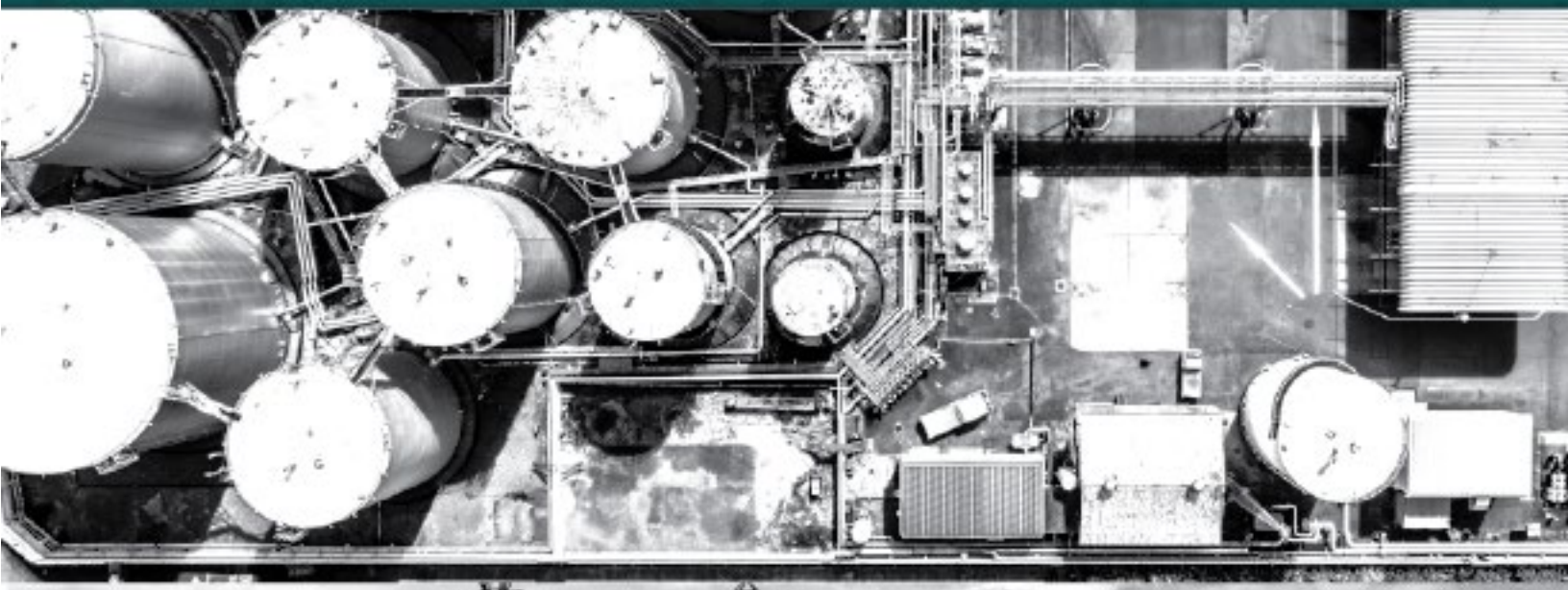
Bronze Sponsors

Partner Sponsors

DRAGOS

THE **INDUSTRIAL CYBERSECURITY** PLATFORM, EXPERT, AND ALLY.

DRAGOS.COM



IronNet

Collective Cyberdefense for NY State Munis and Co-Ops

OCTOBER 19 | 12:15 PM - 1:15 PM ET

Shawn Wallace, IronNet and Vic Costanza, NYPA

NYPA and IronNet have partnered to address a unique challenge: how to provide advanced cybersecurity and collective defense to munis and co-ops. After addressing the need and outlining benefits to stakeholders, we will share the program plan, schedule, and outreach package. We will discuss challenges, lessons learned, and the issues we encountered. Leveraging the results of the pilot, we will plan for ways to improve other future efforts and advance overall sector cybersecurity.

TRIPWIRE® STATE ANALYZER

AUTOMATED "WHY" REPORTING FOR SECURITY & AUDIT EFFICIENCY

With Tripwire State Analyzer you can:

- Define records in centralized allowlist configuration files that contain approved configuration items (e.g., network ports, services, local users, etc.)
- Automate the validation of detected system configurations against your allowlist configuration files
- Generate detailed system configuration reports of authorized and unauthorized configurations

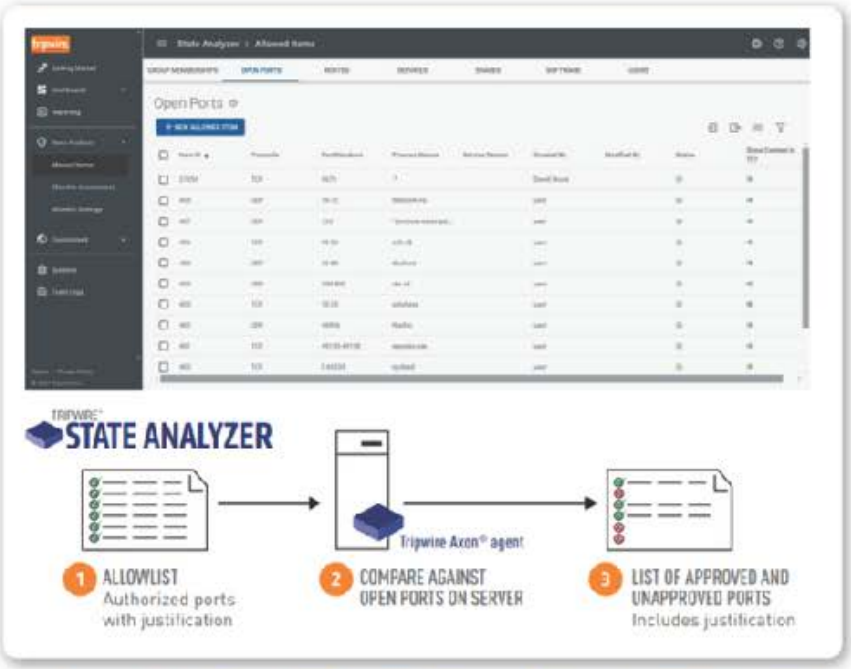


Fig. 1 Overview of Tripwire State Analyzer's process flow in the context of network port allowlisting.
Step 1: User defines an allowlist of authorized network ports
Step 2: Tripwire State Analyzer interrogates the system and compares any open ports to the list of authorized ports
Step 3: Report is generated, listing authorized and unauthorized open ports

tripwire®

HAGERTY

www.hagertyconsulting.com

Helping clients prepare for,
respond to, and recover from disasters.

@HagertyConsult

@HagertyConsulting

/company/52065

CLIQ™

The strongest locking system around is also the most flexible.

PROTEC² CLIQ™ is an advanced locking and access management solution for electric power operators. A smartphone connects the server and the key, and the key verifies access rights. The software gathers access registers for every key, which can be updated at any time. All told, CLIQ Connect reduces risks from lost keys and ensures efficient key control for securing critical infrastructure.

To learn more, contact us at 800.367.4598 or visit ABLOYUSA.com

ABLOY

An ASSA ABLOY Group brand ASSA ABLOY

KEYSIGHT TECHNOLOGIES

Don’t let cyber threats put your LIGHTS OUT

Learn more at our booth

network perception

Protecting Critical Assets is Your Top Priority

86% of security specialists don't have a best-in-class network security compliance program

Visit Our Virtual Booth to Learn More About Securing Your Network & NERC-CIP Compliance

network-perception.com

FORTINET

Secure and reliable power, everywhere you need it.

Protect the possibilities with Fortinet.

Learn more at fortinet.com/power-utilities

Innovative Technologies to Solve Cybersecurity Electricity Industry Business Challenges

Attivo NETWORKS.

- Lack of threat detection solutions that can run on OT devices
- Increasing exposure from IT/OT integration and remote connectivity
- Susceptibility to zero-day attacks with no available patches
- Economic repercussions from cyber-terrorism attacks on critical infrastructure

www.attivonetworks.com

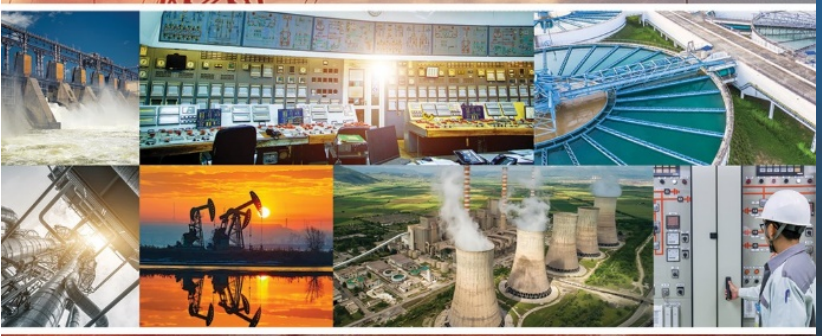
NOZOMI NETWORKS

Securing OT & IoT in Utilities

Protect your power generation, transmission & distribution networks while improving operational visibility and reliability.

Learn More →

nozominetworks.com



SECURITY • COMPLIANCE • RESILIENCE
www.archrint.com • 1 (800) 805-7411
contact@archerint.com • 2201 NE Columbia Blvd, Suite 2101B

Mobilize defenses and minimize disruptions from cyberattacks.

Utilities face unprecedented threats from cybercriminals. Early detection and defense strategies are key to protecting your most vital resources.

LEARN MORE

BURNS McDONNELL

INDUSTRIAL DEFENDER®

THE LEADER IN OT CYBERSECURITY & COMPLIANCE

OUR OT CYBER RISK MANAGEMENT PLATFORM PROVIDES:

- Comprehensive asset inventory and management
- Vulnerability and patch management from a single screen
- Network and endpoint anomaly detection capabilities
- NERC CIP compliance

LEARN MORE AT INDUSTRIALDEFENDER.COM

VERVE INDUSTRIAL PROTECTION

Over 25 Years of Comprehensive OT Security Solutions

The Verve Difference

- 100% Software Solution
- 360° Asset Risk Management
- Closed-Loop Platform
- Think Global, Act Local
- Open Platform for Integration

VERVE

www.verveindustrial.com