



CASE STUDY

US Green Energy Provider

OT Asset & Configuration Management,
Cybersecurity Monitoring and Alignment
with Best Practice Frameworks



INDUSTRIALDEFENDER.COM



COMPANY PROFILE

This Industrial Defender customer provides carbon-free electricity to its customers and is transforming their grid to be more flexible and renewable to fight climate change. The company owns over 60 power generation facilities and more than 22,000 miles of transmission and distribution lines.

THE SITUATION

Technology and innovation continue to transform their power distribution system into a smart grid built on a platform of software-centric services. Coincidentally, so does the complexity of cyberattack sources and mechanisms, dramatically increasing the risk to the security of operations and grid infrastructure.

To mitigate these cybersecurity risks, the company uses many of the controls recommended by three key risk mitigation and management frameworks:

- The NIST Cybersecurity Framework (CSF)
- The Center for Internet Security (CIS) Controls
- The ISO/IEC 27001 Security Standards

With these frameworks as a guide, the company's cybersecurity program has evolved significantly. It employs several key processes and technologies to detect, defend, and respond to a wide variety of technical attack methods. As a crucial aspect of their cybersecurity program, the company sought an all-in-one solution to protect and monitor their critical operational technology (OT) infrastructure.

“Technology and innovation continue to transform their power distribution system to a smart grid built on a platform of software-centric services.”

THE SOLUTION: INDUSTRIAL DEFENDER

The company implemented the Industrial Defender (ID) platform to meet their needs for OT cyber resilience and alignment with best practice frameworks. The ID platform captures data from multiple sources, including endpoint devices (servers, workstations, and network equipment) and the IT/OT network traffic in remote (field) locations. The data is then normalized to empower the security and engineering teams with events, alerts and reports that provide actionable intelligence, without data overload.

Industrial Defender passively discovers and identifies devices communicating on the network and onboards assets for inventory management using the Network Traffic Analysis (NTA) system. Deep-packet inspection uncovers anomalies with signature-based pattern matches, as well as abnormal messages within the control system network traffic between intelligent electronic devices and HMIs/servers.

Events are collected from endpoint syslogs, anti-virus application logs, and application logs (e.g. control systems software). Event processing logic is used to notify users of risk exposure, vulnerabilities and anomaly issues. Firewall rules, software inventory, user accounts and device configuration state data are also collected from endpoints, and users are immediately notified of any changes.

ID users consume this data via email alerts for high priority events and with report subscriptions that summarize important information. The team uses the web-based UI for investigative analysis, along with dashboard-based situational awareness.

	Asset Management	Configuration Management	Software Security & Vulnerability Management	User Account Management & Access Control	Event Management	ICS Network & Perimeter Defense	Other: • Media Use • File Integrity • Backups
NIST Cybersecurity Framework	ID.AM-1 ID.AM-3 PR.DS-3	ID.AM-2 PR.IP-1 PR.IP-3	ID.AM-6 DE.CM-8 DE.CM-7 PR.IP-12	PR.PT-3 DE.CM-7	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-4 RS.AN-1	DE.CM-1 DE.CM-7	PR.PT-2 PR.IP-4
CIS Critical Security Controls (CSC)	CIS CSC 1	CSC 2 CSC 3 CSC 9 CSC 11	CSC 2 CSC 4 CSC 18	CSC 5 CSC 14 CSC 16	CSC 6 CSC 8	CSC 11 CSC 12	CSC 10 CSC 13
ISO/IEC 27000 series	27019 part 8 27001 Annex A category A.8 27002 clause 8	27019 12.2	27019 12.5	27019 9 27019 11 27002 clause 9	27019 12.2 27019 12.4	27019 13	27019 12.3 27019 17

Best Practices Customer Implements with ID

THE RESULTS

Anomalies and Threats Discovered by ID

BACnet traffic found in control system network traffic. Building management systems (BMS) should be detached from the substation control system network. This was a network misconfiguration exposing the substation network through the BMS.

DNP3 traffic mode change operations which were causing buffer overflow were identified. After an investigation, the customer found these were caused by a configuration error and realized they had to increase the related event size on their server settings.

The customer now relies on the ID platform for:

◆ Asset and Configuration Management

- Hardware inventory, including descriptive information about each device
- Software inventory, including versions, patches and known vulnerabilities
- Configuration information, including ports and services, interfaces, software installed, audit settings, and firewall rules.
- Configuration state changes
- Policy monitoring for settings, OS/software version and patch inventory, configuration settings, firewall rules, and/or user accounts that are not in compliance with corporate policies.

◆ Access Control and User Account Security

- Monitoring of firewall rules
- User account monitoring and reports for auditing
- Removable media monitoring

◆ Cybersecurity Monitoring and Reporting

- OT Endpoint Monitoring for:
 - Syslogs
 - Anti-virus application logs and UTM firewalls
 - Application logs, such as SCADA software error logs

- Network Monitoring
 - VLANs
 - Device communications
 - Signature-based patterns to check for known vulnerabilities
 - NetFlow to visualize the network communications topology
 - PCAP replay within the ID system
- Information Reporting
 - Event streams processed with logic and correlation rules and assigned priorities of significance
 - Email notification alerts to engineers/analysts for specific events of significance
 - Periodic reports automatically delivered as subscriptions

◆ Professional Services

- Maintain the ID system and perform upgrades
- Continuously configure, tune and optimize to maximize ROI
- Consult and advise on cybersecurity best practices

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Learn more at www.industrialdefender.com.

Planning an OT Security Project?

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com

225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com