

Scaling OT Cybersecurity Practices Across Substations

Protecting the bulk electric system goes beyond securing our largest power generating facilities. The attack surface continues to evolve across the broader electric grid, with threats of disruption emerging at substations and low-impact facilities throughout the network.

While the industry has advanced cybersecurity practices in very critical areas, the evolving threat landscape requires heightened situational awareness across substations and other distributed assets.

Scaling OT Cybersecurity Efforts Across the Grid

Increasingly, utilities are recognizing the need to monitor and manage OT security beyond their generating sites. In one example, a major utility responsible for powering over 1.4 million customers, collaborated with Industrial Defender to enhance their OT asset management program. This covered more than 35 substations across a significant portion of the state. Their ambition was to gain in-depth visibility into these OT environments, with regularly updated asset database detailing software versions, firewall rules, and intricate configuration specifics. With this data, they wanted to stay on top of any system changes and ensure configuration states adhered to their policies.

With the Industrial Defender platform, the utility has a comprehensive and up-to-date view of more than 2,500 assets distributed across their substations.

35 SUBSTATIONS **2,500** ASSETS

Assets managed include the following, of various makes and manufacturers:

- Servers
- Workstations
- Network Devices
- Firewalls
- Meters
- SIEM Appliances
- RTUs
- Ruggedized HMI Servers
- Gateway and Port Servers
- Relays, Measurement, I/O and Protection Devices

Easy Access to Critical OT Asset Data

Industrial Defender safely and effectively automates comprehensive depth of data collection resulting in deeper insights, minimizing manual efforts. Manual effort is especially a challenge for substations that are geographically distributed. With Industrial Defender's automated solution, teams no longer need to travel to various sites to manually update asset information in spreadsheets—an approach that is not only prone to errors but also quickly becomes outdated.

Industrial Defender gets deeper data through its proven integrated data collection approach, employing a blend of strategies including manual data ingestion, passive and active data collection, agent-based and agentless monitoring, native polling, and direct database integrations. Since 2006, Industrial Defender has proven this integrated approach to be operationally safe and effective for managing even hard-to-reach and/or offline assets.

Getting Ahead of Potential Low-Impact Compliance Requirements

It remains to be seen whether all NERC CIP requirements will eventually extend to low impact assets. However, recent updates like the Reliability Standard CIP-003-9—which mandates “vendor electronic remote access security controls” at low impact sites—suggest a growing emphasis on applying security best practices throughout the electric system. Regardless of whether compliance is mandated, having comprehensive and reliable OT asset data, along with insights into any changes, is foundational to maintaining system integrity and enforcing security posture. The Industrial Defender automates reporting for easy assessment, whether for external audits or internal governance.

Trustworthy OT Asset Data is Foundational to Securing the Bulk Power System

Scaling OT cybersecurity practices across substations is imperative in today's rapidly evolving threat landscape, and Industrial Defender is dedicated to partnering with utilities to enhance their security posture across the entire electric grid. By delivering in-depth visibility, comprehensive asset management, and automated data collection, we empower utilities to proactively manage and secure their OT environments, including substations and distributed assets across the bulk power system.

Ready to enhance OT security across your substations? Get an Industrial Defender demo today.

[Schedule a demo](#)

About Industrial Defender

Industrial Defender is the single best source of OT asset data needed to protect industrial operations and meet compliance. Established in 2006 and headquartered in the United States, Industrial Defender is the leader in providing deeper-level asset data and vital endpoint information, along with historical context and change monitoring capabilities, for addressing cyber risks across the OT environment.

1 (877) 943-3363
(617) 675-4206
info@industrialdefender.com
225 Foxborough Blvd
Foxborough, MA 02035

[industrialdefender.com](https://www.industrialdefender.com)

© 2023 iDefender, LLC