



CASE STUDY

Multi-National Gas & Electrical Distribution

Monitoring Transmission and Distribution Networks



INDUSTRIALDEFENDER.COM





COMPANY PROFILE

This customer is a European multi-national electricity and gas utility company providing transmission and distribution of power. Its principal activities span multiple countries with an annual revenue in the tens of billions.

THE SITUATION

This customer needed to monitor their critical assets and control system networks, including Schneider Electric and GE SCADA systems, for natural gas and electricity supply to improve the reliability and cybersecurity of the grid.

CUSTOMER REQUIREMENTS

- Monitor events and network activity in their systems, including new communications or potential attacks.
- Detect arbitrary status or configuration changes in assets in their environments.
- Ensure that production operation computing assets of the same type are built correctly and adhere to a configuration standard.

**“ASSET
MANAGEMENT
AND NETWORK
INTRUSION
DETECTION
CAPABILITIES
GIVE THIS
UTILITY THE
ABILITY TO
MONITOR
SUSPICIOUS
NETWORK
TRAFFIC
ACROSS BOTH
ELECTRIC AND
GAS SCADA
NETWORKS.”**

THE SOLUTION: INDUSTRIAL DEFENDER

The customer deployed the Industrial Defender platform to achieve their goals, including monitoring and managing a variety of Linux and Windows endpoints and their associated authentication events. Industrial Defender lets them easily see if anyone is abusing or misusing their user privileges. Using the ID Event Search, they can quickly and easily find any event irregularities and monitor invalid and failed log on attempts.

Asset baselining is another feature that has proven highly useful to the client. They rely upon Industrial Defender's detection and display of exceptions from the asset details, software, patches and critical files in the baseline and check it daily to make sure any exceptions are either expected or investigated.

After tuning their passive network monitoring events, the customer can now detect any suspicious network traffic. Once detected, the suspicious traffic is investigated by the network team and IT group to validate the existence of the activity. Industrial Defender provides detailed data about traffic type, source, destination, and a time-stamp.

THE RESULTS: CONTINUOUS MONITORING OF TRANSMISSION & DISTRIBUTION NETWORKS

Their gas and electricity networks are completely isolated, and are managed and monitored by different groups. However, both systems are very similar, each consisting of one primary and one backup system. To provide strong security for the environment without unnecessary complexity, Industrial Defender gives them a single system where they can monitor their assets and network activity.

Some of their key use cases include:

- **Network Alerting and Easy Issue Investigation** – On a few occasions, the client had issues that suggested they were under attack. In one case, they were alerted of unusual network activity of a certain traffic type, and they started an investigation. They used the ID Events Search extensively to correlate the sequence of the events. After investigating the network activity details and mapping valid log ins to certain machines, and related hardware events, they concluded that a vendor was using a USB stick that had not been scanned for viruses. At that point, the client told Industrial Defender, "Your solution just paid for itself."
- **Easy Issue Investigation** – On another occasion, the client noticed a failure in one of their systems that was caused by an incorrect PLC setting. Of course, they were worried about a possible attack. Using Industrial Defender to examine the events over the previous week, they were able to determine that it was human error, not an attack.

- **Adherence to Configuration Standards** – To ensure that certain operational servers are built correctly and identically, the client uses ID Reports. They have multiple servers configured as “Operator Workstations” and use ID Reports to make asset to asset comparisons, and make sure the software installed, their versions, patches, and so forth, are identical. If not, the reports are used to submit a configuration correction to the IT department, which builds the machines. This saves significant time for the client as the detailed asset to asset comparison is accomplished with a few clicks and presented in a clear, well-formatted report.

“USING INDUSTRIAL DEFENDER’S EVENTS SEARCH FUNCTIONALITY, THE CUSTOMER DETERMINED THE SOURCE OF SUSPICIOUS NETWORK ACTIVITY AND SYSTEM FAILURE FOR ONE OF THEIR PLC’S.”

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. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

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

© 2021 iDefender. All Rights Reserved.