



CASE STUDY

Strengthening OT/ ICS Cybersecurity in European Electric System Distribution Operations with Industrial Defender

A Case Study on Best Practice Implementation of
CIS Controls and NIS Directive Standards

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



BACKGROUND

An electric distribution system operator (DSO) responsible for the power network that keeps the lights on for 8 million customers across 3.9 million homes and businesses in Europe. Their grid covers an area of 25,000 square kilometres and consists of more than 63,000 substations and around 96,000 kilometres of overhead line and underground cables.

This leading DSO is playing a key role in the region's transition towards a sustainable future. To achieve their vision of a flexible and reliable digital energy network, the company has embarked on a digital transformation journey. Their digitalisation roadmap aligns with their plan to meet the zero-carbon challenge, guided by the following principles:

- Improving system resilience and reliability through increased data visibility and transparency across the energy network. The company has set a goal to enhance data practices for improved data sharing.
- Maintaining their industry-leading status in cybersecurity by proactively detecting and protecting against cyber threats. The company recognizes the importance of robust data practices to safeguard their digital infrastructure.

OBJECTIVES

When they approached Industrial Defender, this leading DSO set forth the following objectives to ensure the success of their digital strategies and continued compliance with industry regulations:

- Establish an “Analytics Function” team to extract value from data and generate insights
- Implement a unified cybersecurity approach across operational technology (OT) and information technology (IT)
- Enable data integration with third parties through open APIs

At the center of their digitalisation journey was a requirement to comply with best practices and requirements laid out by the **CIS Critical Security Controls** and the **European Network and Information Security (NIS) Directive**. To ensure effective implementation of these controls, continuous monitoring for compliance, and the ability to prove it, the DSO turned to Industrial Defender for help managing their cybersecurity program.

To ensure effective implementation of these controls, continuous monitoring for compliance, and the ability to prove it, the DSO turned to Industrial Defender for help managing their cybersecurity program.

THE SOLUTION: THE INDUSTRIAL DEFENDER PLATFORM

Since 2012, the company has been using Industrial Defender to manage and monitor their Advanced Distribution Management System, which includes over 200 assets such as firewalls, servers, and client workstations across their primary and backup data centers, control centers, and regional distribution management centers. To enhance their cybersecurity measures, they decided to upgrade to the full Industrial Defender Platform, which is a comprehensive centralized platform for managing all OT asset data that could meet their CIS and NIS Directive needs.

The Industrial Defender Platform provides advanced policy compliance capabilities, with easy-to-use drop-down menus and out-of-the-box reports specifically for CIS and NIS Directive requirements (among other leading frameworks), giving the company greater confidence in their ability to meet, maintain, and demonstrate on-going compliance. They felt further assurance with the white glove support offered by Industrial Defender's team of engineers, who provide consulting and training to ensure that the company stays ahead of any potential threats.

INDUSTRIAL DEFENDER SERVICES

The team provided training and documentation to the company specifically to support the DSO's goals. They also set up customised dashboards, reports, and periodic report subscriptions such as:

- Unauthorised device connections
- Firewall rule changes that alter the visibility of servers
- Software inventory changes
- Changes made to the critical assets (e.g. SCADA) configurations such as patches installed, ports and services, user accounts, and device audit policies
- Unauthorised user access attempts
- All user activity for remote access (jump servers)
- Use of portable media such as USB drives

The Industrial Defender team also validated and certified the platform's cyber security control requirements and configured it to interface with the DSO's SIEM. They also provided hands-on training to the cyber security analysts for identifying risks and vulnerabilities.

RESULTS

The operator gained the following capabilities to manage their systems according to CIS Controls and NIS Directive standards:

◆ Asset Inventory Management

- Automated asset inventory discovery
- All equipment acquisitions automatically updated in the system

◆ Software/Firmware and Patch Management for Computers, Network and Process Control Devices

- Devised authorized software list by system type
- Deployed software inventory tools for each OS type
- Tracking OS versions and installed applications
- Maintaining latest security updates on all network devices

◆ Critical File Integrity Checking

- Deployed file integrity checking tools to verify critical system files haven't been altered

◆ Automated Configuration Monitoring for Computers, Network and Process Control Devices

- Implemented and tested automated configuration monitoring to detect unauthorized changes, such as new listening ports, users, policy object changes, and new services
- Ensured only necessary ports, protocols, and services are running on each system
- Compared firewall, router, and switch configurations against standard secure configurations for each device type used in the organization

◆ User Account Monitoring

- Automated tools used to inventory all admin accounts
- Configured systems to issue alerts for admin group changes
- Reviewed system accounts and disabled unassociated ones
- Monitored and enforced account expiration dates

◆ Security Event Monitoring for Computers, Network and Process Control Devices

- Systems configured to log and alert on unsuccessful login to admin accounts
- Biweekly anomaly reports run and actively reviewed by security and system admins
- SIEM/log analytic tools deployed for log aggregation, consolidation, and correlation
- Automated tools employed to continuously monitor devices with anti-virus, anti-spyware, personal firewalls, and IPS
- External device use monitored and auto anti-malware scan configured

◆ Network Intrusion Detection including Industrial Control Systems with Proprietary Protocols

- Network-based anti-malware tools used to identify and filter out malicious content in network traffic
- Network-based IDS sensors deployed on DMZ systems and networks to detect unusual attack mechanisms and system compromise

◆ Firewall Rules Configuration Monitoring

- Successfully documented and recorded all new configuration rules beyond a baseline-hardened configuration
- Ensured that this documentation applies to rules allowing traffic to flow through network security devices such as firewalls and network-based IPS

THE INDUSTRIAL DEFENDER DIFFERENCE

Industrial Defender is a global leader in providing deep-level asset data and endpoint information for addressing cyber risks across the operational technology (OT) environment. Our customers rely on us as a single source of truth for all operational asset information, enabling them to achieve key goals in OT asset management and policy compliance. The Industrial Defender difference is in our best-in-class approach to data collection, with integrated methods for completeness and depth of OT asset information. Our mission is to protect our customers' reputations and competitive edge as the cyber-physical landscape evolves. 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