



CASE STUDY

Electrical System Distribution Operator

Following Best Practice Standards
for the 20 CIS Controls and EU NIS
Directive

INDUSTRIALDEFENDER.COM





COMPANY PROFILE

An electrical grid system operator in the EU that supplies gas and electricity to millions of homes and businesses spanning thousands of kilometers and tens of thousands of substations.

THE SITUATION

The client formed a digitalisation roadmap to become a digital energy network as part of their approach to meeting the challenge of the new zero carbon landscape. Their vision is to develop their role as their region's distribution systems operator (DSO) for their network to be a trusted and neutral platform, able to optimise their energy system and underpin the transition to carbon-free electricity, transport and heat for all their customers. By utilising all available digital tools and technologies, they planned to transform their infrastructure and their business to support a flexible, reliable, and resilient energy network.

To ensure the right outcomes, their plan to deliver digital transformation is underpinned by a set of clear design principles, which include:

- Focus on delivering outcomes like system resilience
- Drive efficiencies within the business to reduce costs and ensure affordable services
- Improve visibility of data to drive new, more productive ways of working
- Deliver industry-leading, future-proofed cybersecurity performance

CUSTOMER REQUIREMENTS

The client's intention was to leverage data analytics to improve system resilience and reliability by promoting data sharing across the wider energy network to detect and prevent threats at an early stage. Example initiatives included:

- Creation of a Security Data Research Team
- A Common Cyber Function Across OT and IT
- Open APIs for Data
- A "Digital System Map" Using Asset Data

"THEY PLANNED TO TRANSFORM THEIR INFRASTRUCTURE AND THEIR BUSINESS TO SUPPORT A FLEXIBLE, RELIABLE, AND RESILIENT ENERGY NETWORK."

THE SOLUTION: INDUSTRIAL DEFENDER

The client chose the Industrial Defender solution to manage and monitor their Advanced Distribution Management System, including over 200 assets such as firewalls, servers, and client workstations within the client’s primary and backup Advanced Distribution Management System data centers, control centers and regional distribution management centers.

Organisations often use multiple frameworks to guide their cybersecurity strategy, and this client engaged Industrial Defender to help them align with the 20 CIS Controls and the NIS Directive principles because their solution provides functionality that directly satisfies these chosen regulations and best practices, with out-of-the-box reports aligned to both the 20 CIS Controls and NIS Directive requirements. Industrial Defender’s engineers also provided consulting and training to help them manage compliance with tailored dashboards and reporting that aligned to specific requirements, including:

- Unauthorised device connections, or added to the network
- Firewall rule changes that alter the visibility of servers protected by the firewall Software inventory changes
- Changes to critical asset’s configurations such as patches installed, ports & services, user accounts, and audit policies
- Unauthorised user access attempts
- All user activity for remote access (jump servers)
- Use of portable media such as USB drives

Goals	Results
• Creation of a “Digital System Map” • Adoption of the 20 CIS Controls for processes and policies • Comply with the European NIS Directive	• Automated asset inventory for all systems on their network • Centralised patch management for software/firmware • Easier compliance with the 20 CIS controls and NIS directive

THE RESULTS: STREAMLINED STANDARDS COMPLIANCE

The client performed validation testing to certify that Industrial Defender met their cybersecurity control requirements. They used the API-enabled integrations to feed data into their enterprise SIEM, to achieve the OT/IT collaboration they were striving for. Industrial Defender also helped them to create their “Digital System Map” and align with both the 20 CIS Controls and the NIS Directive Principles to build a future-proofed cybersecurity program.

Some of the use cases they continue to support with Industrial Defender include:

- Asset Inventory Management
- Software/Firmware Patch Management
- Critical File Integrity Checking
- Automated Configuration Monitoring
- User Account Monitoring
- Security Event Monitoring
- Network Intrusion Detection
- Firewall Rules Configuration Monitoring

“INDUSTRIAL DEFENDER PROVIDED FUNCTIONALITY THAT DIRECTLY SATISFIED MULTIPLE OT SECURITY REGULATIONS, STANDARDS AND FRAMEWORKS, SPECIFICALLY CIS AND NIS.”

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

© 2020 Industrial Defender. All Rights Reserved.