



CASE STUDY

Combined Cycle Power Plants

NERC CIP Compliance &
Security Monitoring for
SCADA, DCS, Transformer &
Substation Assets



INDUSTRIALDEFENDER.COM





COMPANY PROFILE

A Fortune 500 power utility company transitioning from traditional coal power generation to cleaner fuel sources, including LNG, solar and wind.

THE SITUATION

This customer was looking for a mature platform to gather NERC CIP compliance data and perform cybersecurity monitoring of assets on its industrial control system (ICS) networks. This platform needed to be vendor-neutral and deliver automated NERC CIP compliance. Besides traditional servers and workstations, they also needed to monitor relay gateways, GPS time sync servers, Programmable Logic Controllers (PLCs), HMIs and industrial switches.

CUSTOMER REQUIREMENTS

They needed to monitor multiple vendor systems to handle functionality across multiple control systems, including:

- Distributed Control Systems (DCS)
- Vibration Monitoring System (VMS)
- Aux Boiler
- Fuel Gas Compressor (FGC)
- Continuous Emissions Monitoring System (CEMS)
- Water Treatment
- Steam and Combustion Turbine Generators
- Medium Voltage Step-Up
- Transformer Switchgear
- Remote Intelligent Gateway (RIG)

**“BESIDES
TRADITIONAL
SERVERS AND
WORKSTATIONS,
THEY ALSO
NEEDED TO
MONITOR RELAY
GATEWAYS,
GPS TIME SYNC
SERVERS,
PROGRAMMABLE
LOGIC
CONTROLLERS
(PLCS), HMIS
AND INDUSTRIAL
SWITCHES.”**

THE SOLUTION: INDUSTRIAL DEFENDER

The customer chose the Industrial Defender platform to achieve their goals. The Industrial Defender engineers worked hand-in-hand as part of the plant commissioning team with the prime contractor, SCADA supplier, DCS vendors, and the plant owner's engineering and cybersecurity team members. Together they designed and built a robust cybersecurity program by:

- Integrating Industrial Defender within the plant to monitor every asset
- Providing technical assistance to network engineers and device vendors to configure the assets for integration with Industrial Defender
- Consulting on NERC CIP requirements and how to automate compliance with Industrial Defender
- Performing validation testing for each asset, in accordance with NERC CIP requirements
- Identifying outages and misconfigurations to assist DCS engineers
- Configuring user interfaces and reporting subscriptions to meet the end user's needs
- Tuning of the data collected and processed by Industrial Defender to make the information meaningful and actionable
- Delivering hands-on training to end users

THE RESULTS: AUTOMATED NERC CIP COMPLIANCE AND SECURITY MONITORING

The Industrial Defender platform provided them with simplified NERC CIP compliance reporting, asset and policy management, and continuous cybersecurity monitoring. In addition to gathering data from higher-level traditional servers and workstations, Industrial Defender also helps them collect data from lower-level endpoints, such as PLCs, GPS clocks and relay devices, using a CIP collector. This allowed them to tremendously reduce manual data collection efforts for NERC CIP compliance.

“INDUSTRIAL DEFENDER WORKED AS PART OF THE PLANT COMMISSIONING TEAM TO PROVIDE AUTOMATED COMPLIANCE ACROSS A NUMBER OF NERC CIP CATEGORIES AND SIGNIFICANTLY REDUCED MANUAL DATA COLLECTION PROCESSES FOR LOW-LEVEL ENDPOINTS.”

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.