Protecting Critical Infrastructure Across Borders

Building a Bi-National IT-OT SOC for a Scandinavian Energy Provider

A cross-border energy provider in Norway and Denmark sought to protect critical infrastructure from nation-state threats. Krish Services Group deployed a dual-purpose SOC covering IT and OT environments, with capabilities tailored to industrial control systems and energy-specific regulations.

CLIENT BACKGROUND

This major utility organization operates energy production and transmission assets across Scandinavia. With national infrastructure at stake, including hydro and grid systems, the client needed advanced SOC capabilities that bridged IT, OT, and regulatory compliance.

BUSINESS VALUE

Blocked ICS Intrusion Attempt:

Detected Modbus traffic from IT to ICS network. Contained threat within hours via workstation isolation and firewall hardening.

Cross-Team Collaboration:

Coordinated drills and playbook updates improved incident response across IT and OT teams.

Resilient, Compliant Infrastructure:

Achieved real-time threat detection and met regulatory expectations with automated reporting.
for financial risk management.

PROBLEMS

- **Nation-State Threats to Critical Systems:** Legacy SCADA systems lacked modern defenses, raising concerns over OT intrusions.
- **Siloed Teams and Monitoring:** IT and OT systems were monitored separately, limiting visibility and cross-domain threat correlation.
- **Compliance Challenges:** Meeting standards like NERC CIP and ISO 27019 required specialized reporting and response protocols.

SOLUTIONS

- **Dedicated Cross-Domain SOC Team:** Included OT experts, SOC analysts, and a compliance lead with specialization in SCADA protocols like Modbus and DNP3.
- **Modern Threat Detection Stack:** Implemented Azure Sentinel SIEM, Defender EDR, Nozomi/Dragos ICS monitoring, and SOAR automation for both IT and OT.
- **Process Alignment with NIST:** Developed NIST 800-61 aligned playbooks and performed quarterly red teaming for OT segmentation tests.

TECHNOLOGIES

SOAR

Final Perspective

Krish Services Group enabled the client to proactively defend critical infrastructure across regions, unifying threat detection and response across both IT and OT environments.