Radiflow **Case Study**

Enhancing Data Center Cybersecurity and Operational Resilience with Integrated OT Monitoring

Overview

Data centers are among the most complex facilities to secure, blending advanced IT systems with operational technology that controls critical functions such as cooling, power, and environmental management. Recognized as **Critical National Infrastructure (CNI)** in many jurisdictions, these facilities are prime targets for cyber attacks.

A leading data center operator in the EMEA, managing several mission-critical facilities, experienced disruptions stemming from vulnerabilities in the convergence of its IT and OT networks. Although equipped with a high-end Building Management System (BMS) that provides 24/7 monitoring, the integration with the IT network exposed significant cyber risks. In response, the operator launched an urgent cybersecurity initiative focused on **IT/OT network segmentation**, **comprehensive OT asset mapping**, and **real-time anomaly detection** to safeguard its critical infrastructure and ensure uninterrupted operations.

Objectives

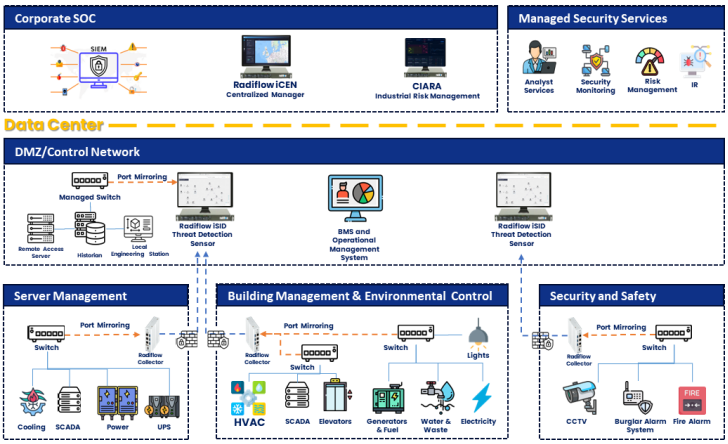
- Protect BMS systems for cooling, power, and environmental controls.
- Achieve real-time visibility through comprehensive OT asset mapping.
- Isolate IT and OT networks to reduce cyber risks.
- Ensure compliance with CNI and industry standards.

Challenges

- Vulnerabilities from unsupervised third-party maintenance.
- Increased attack surface due to IT/OT convergence.
- Risk of operational disruptions and downtime.
- Limited specialized OT security expertise.

Solution and Process

- Built a digital OT network model using passive data capture (recording firmware, open ports, protocols) without disrupting operations.
- Mapped assets and established a baseline with an advanced threat detection platform.
- Refined the model with expert input to create a visual OT network map with logical segmentation.
- Automatically segmented the BMS into key subsystems (power, lights, UPS, HVAC, water, fuel, fire sprinklers).
- Configured rule-based alerts to rapidly detect anomalies (sensor fluctuations, controller changes, unauthorized devices).



Key Features & Results

Radiflow's integrated solution, using **iSID** for digital asset mapping and real-time anomaly detection along with **iCEN** for unified IT/OT monitoring — improved **network security**, ensured **CNI compliance**, reduced chances of **downtime**, and optimized **resource allocation**.

Radiflow

Radiflow develops OT Security and Risk Management solutions that ensure operational resilience and compliance, and optimize cybersecurity expenditure while minimizing risk. Radiflow's solutions enable local or centralized deployment, and integrate with leading technology-partner platforms. Now part of the Sabanci Group, Radiflow protects over 8,000 sites worldwide. Visit us at www.radiflow.com