Radiflow

CASE STUDY

Securing a Large Financial Enterprise

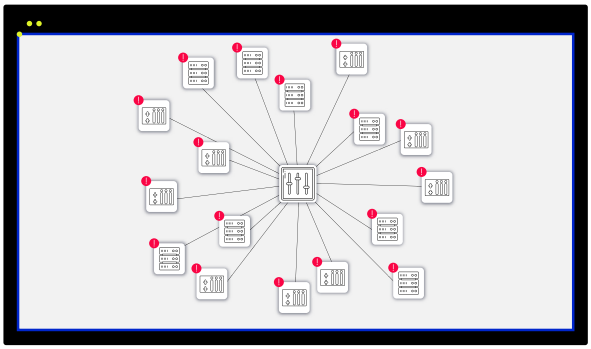
Overview

A leading financial enterprise has built a new campus with the goal of consolidating all their companies and activities into one place. This type of set-up involved the integration of multiple vendors into one Building Management System (BMS).
It is extremely challenging to provide proper protection, real time network visualization, and cybersecurity insights to such a complex. The challenge is further compounded by the growing reliance on internet-based automation & remote operations. This enterprise has made a decision to implement a best-in-class OT security for their Building Management Systems (BMS), as an integral part of this new infrastructure project, led by their CISO.

Objectives and Challenges

Radiflow's comprehensive cybersecurity solution suite, specifically designed for Industrial (OT) networks, provides BMS operators the correct toolkit to safely protect, visualize, and maintain their complex systems:

- Securing critical BMS systems (using DPI for ModBus, Profinet & BACnet protocols): electrical, HVAC, High Voltage and water
- Protecting the high voltage power supply systems (securing the IEC 61850 protocol)
- Hardening the IT-OT barrier
- Installing procedures for lifecycle management
- Installing procedures for securing/logging maintenance operations



iSID's Map View graphically displays all assets, business processes and connections, and enables users to drill down to each asset's properties and threats

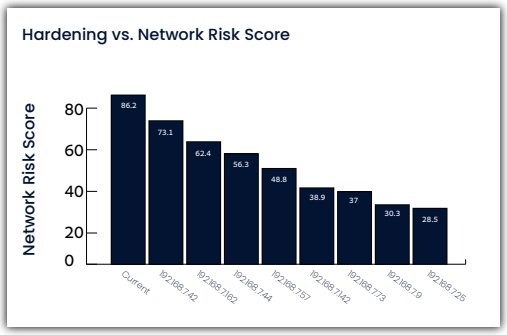
Solution and Process

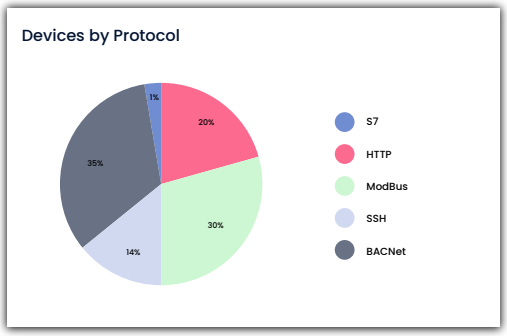
The first step in the campus BMS security project was determining the customer's needs and objectives. This was done over a meeting between facility personnel and Radiflow's OT security experts.
Next, a network model (digital image) of the OT network was created.

This was done using the iSID threat detection & monitoring platform, by analyzing a representative amount of data traffic, recorded using a parallel data stream (as to not disrupt operations) from the campus main data switch. Once completed, iSID was able to provide a detailed network model, including all assets, firmware, ports, open connections and protocols and vulnerabilities/risks associated with different assets. When complete, the iSID-generated digital image was reviewed by Radiflow's cyber experts, in tandem with the customer, and modified to reflect network attributes that couldn't be detected programmatically.

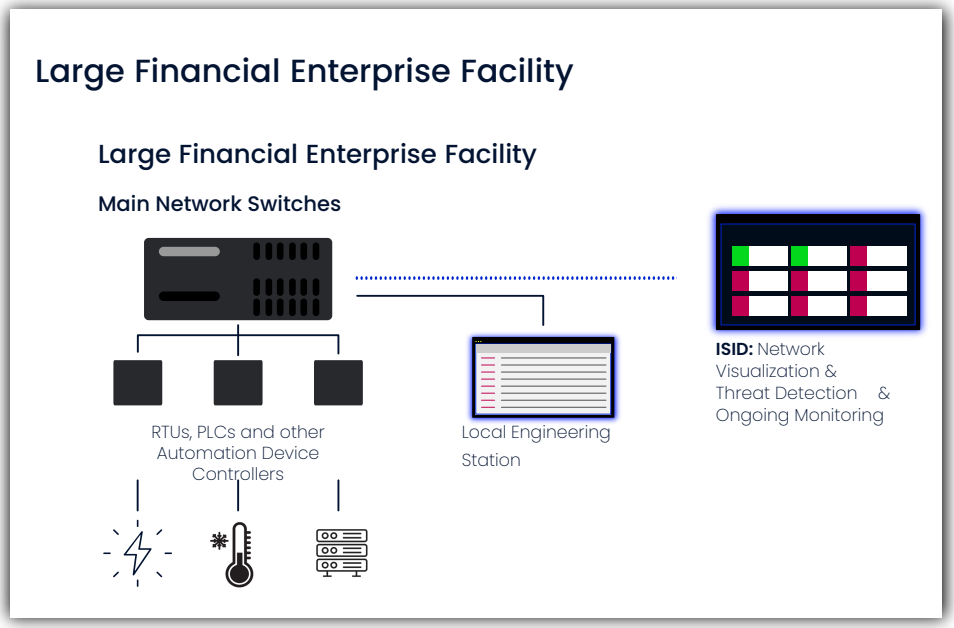
Once all unnecessary open ports and unnecessary protocols were handled, the model was deemed complete and suitable for reflecting the network's baseline activity, as well as for use as a visual network map, down-drillable to each and every device's full properties, links and vulnerabilities. At the same time, iSID automatically created a logicalmodel for business processes for different functions (e.g. Machineries Rooms, high-voltage grid connections). These business processes, also reflected in the network map, allow applying different communication, asset and protocol rules in iSID, depending on function and process criticality.

Based on ongoing network activity, iSID continually generates insights, or recommendations for mitigation actions. Using rule-based alerts for specific devices, iSID created a central monitoring point for critical systems, with alerts for exceeding different sensor or controller values, as well as changes to controller logic or adding devices to the network.





Two of the many items included in the network analysis report



Schematic diagram of the large financial enterprise

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow | For more info: radiflow.com