Radiflow

CASE STUDY

Securing a Large Hospital Campus in EMEA

Overview

Following a series of unsuccessful breaches into its IT network, and in the wake of highly-publicized attacks on hospitals, a large hospital campus in the EMEA region decided to consolidate their campus-wide IT-OT network security and install a comprehensive threat detection and alerting system to protect all building management operations and critical medical devices and units.

The new OT security system was to be tasked with mapping all networked assets, providing network visualization for security personnel, detecting device and network vulnerabilities campus-wide and facilitating maintenance operations by a myriad of vendors.

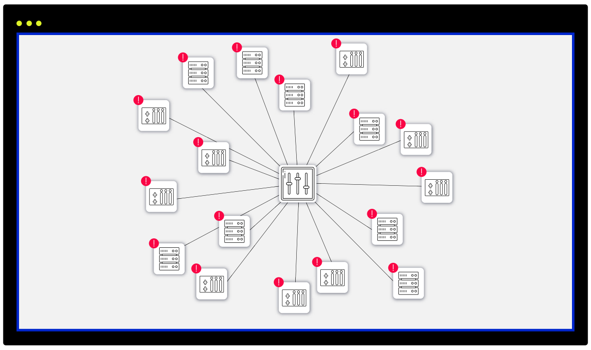
Objectives and Challenges

The highest priority items that required protection in the hospital campus included:

- Protecting the high voltage power supply systems (securing the IEC61850 protocol)
- Securing critical BMS systems (using DPI for ModBus and BACnet protocols): HVAC, electrical, elevators and water/wastewater systems; monitoring the safe usage and storage of medical gases; and monitoring the temperature control systems in cold-storage appliances used for medicine, experiment specimens, organs and corpses.
- Monitoring various HazMat sensors.

Most of the challenges are due to the way the hospital campus and its data networks evolved over the years, as a patchwork of disparate systems and no segmentation between critical systems:

- OT and IT systems that share the same LAN, with only nominal firewall protection
- Lack of segmentation between facilities and systems.
- Separate operational—but not security— monitoring interfaces for different systems
- No procedures in place for patching or hardening devices, leaving the hospital to rely on vendors for initiating per-device maintenance
- No system 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 stage in the project was conducting a thorough OT-security assessment. This involved analyzing a few days' worth of operational data traffic by Radiflow's iSID Industrial Threat Detection system, operating in Learning Mode.
- Once completed, iSID provided a detailed network model, including all assets, ports, open connections and protocols and vulnerabilities/risks associated with different assets.
- As expected, the network model revealed a slew of vulnerabilities, from lack of segmentation between critical systems and networks to mundane configuration issues, such as use of default passwords or unpatched devices.

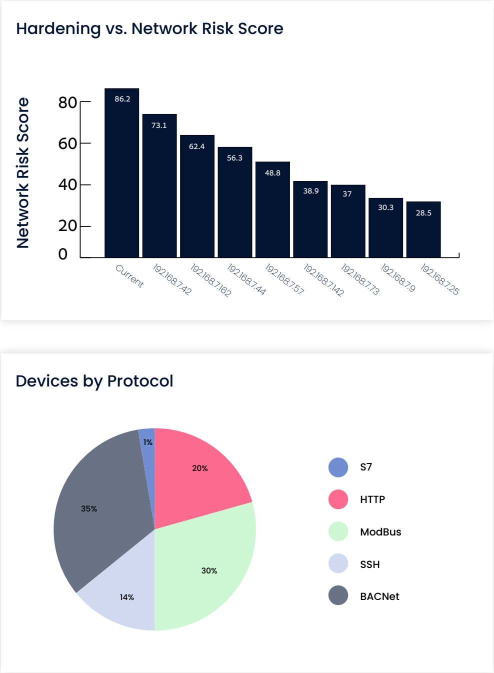
The results of the network analysis were processed by the Radiflow team members that had accompanied the project since inception, resulting in a comprehensive status report and mitigation plan.

Then, in collaboration with the client, the detected vulnerabilities were remedied, resulting in a “clean” baseline topology model which was used thereon for ongoing monitoring, threat detection and alarming also incorporated iSID, this time in Detection Mode.

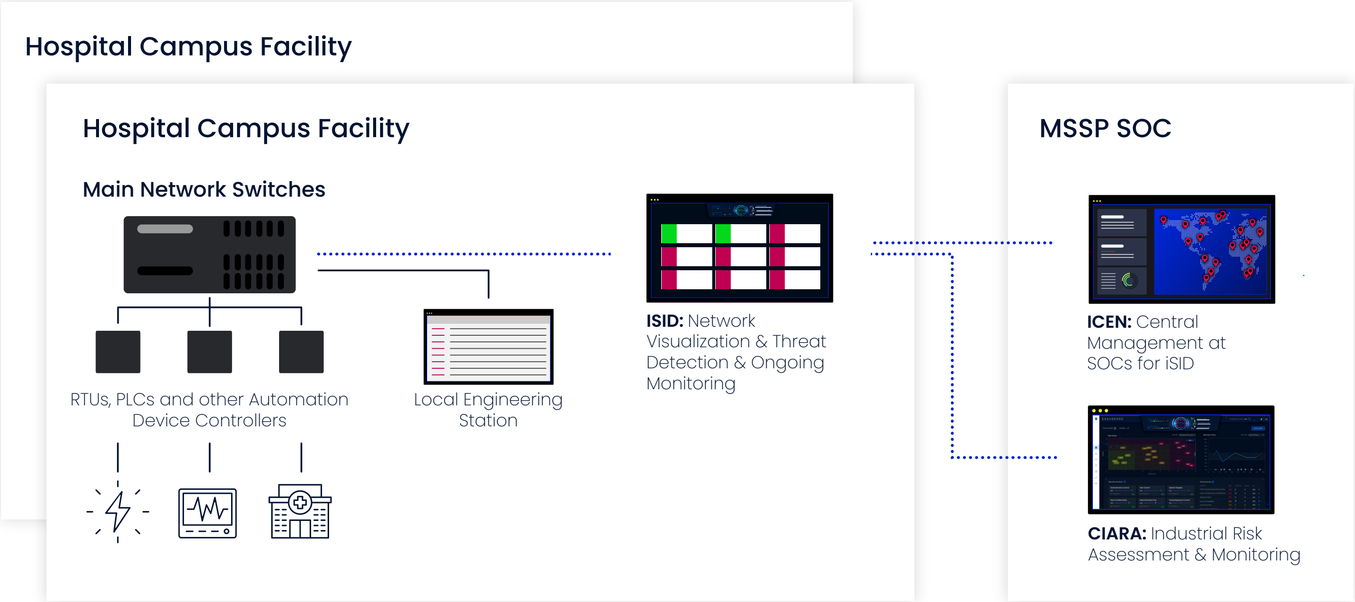
In addition, using rule-based alerts for specific devices, iSID created a central monitoring point for critical systems, with alerts for exceeding different sensor or controller values, as well as changes to controller logic or adding devices to the network.

Current Status

At present, Radiflow’s system is fully operational in one facility and has been green-lighted for installation throughout the entire hospital chain. The project is planned to include an OT-SOC (Security Operations Center) outsourced to an MSSP, that will monitor all iSID systems installed at multiple hospitals and optionally monitor changes to risk using Radiflow's CIARA risk assessment & management platform.



Two of the many items included in the network analysis report


Hospital Campus Facility
Hospital Campus Facility
Main Network Switches
RTUs, PLCs and other Automation Device Controllers
Local Engineering Station
ISID: Network Visualization & Threat Detection & Ongoing Monitoring
MSSP SOC
ICEN: Central Management at SOCs for iSID
CIARA: Industrial Risk Assessment & Monitoring

Schematic diagram of the hospital campus project, including future threat and risk monitoring at an MSSP's SOC

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