CASE STUDY

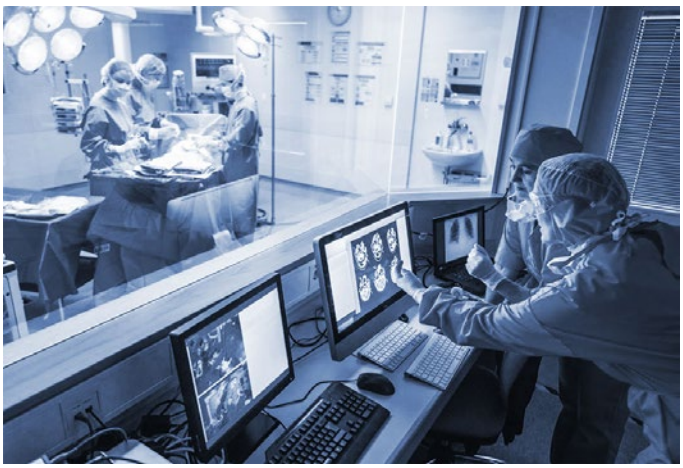
Securing a Large Hospital Campus

OVERVIEW

You'd be hard-pressed to think of a more complex environment to cyber-secure than a hospital campus, as was in the case of a major hospital campus in the EMEA region.

Beyond typical Building Management System functions, hospitals operate a myriad of interdependent critical systems, and are required to operate in preparedness mode, in case of a mega-event or epidemic, so OT-network uptime is crucial.

To make things worse, many hospital systems were not designed with cyber-security in mind.



Hospitals are among the most complex industrial environments, operating a myriad of interdependent critical systems

OBJECTIVES AND CHALLENGES

The highest priority items (typical to hospital security projects) were:

- 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

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

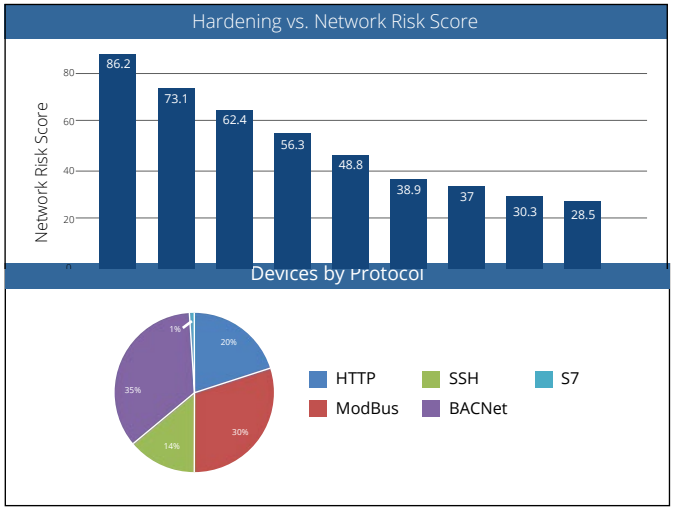
Most of the above challenges are due to the way hospital campuses and their data networks evolved over the years, as a patchwork of disparate systems and no segmentation between critical systems:

- OT and IT systems that share the same LAN, with only nominal firewall protection
- Lack of segmentation between buildings ,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 and logging maintenance operations

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.

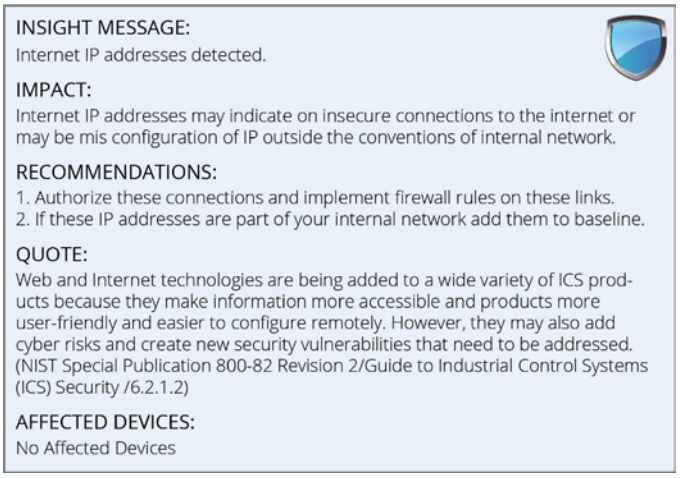


Two of the many items included in the network analysis report

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.



Insights produced by the Radiflow system provide simple, plain-language mitigation recommendations

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 greenlighted for installation throughout the entire hospital chain. The project will ultimately include an OT-SOC (Security Operations Center) outsourced to an MSSP, that will monitor all iSID systems installed at multiple hospitals.

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cyber-security vendors. Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 3,000 critical facilities worldwide. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com