Radiflow

CASE STUDY

Securing a Large Data Center in the EMEA Region

Overview

Data centers are among the most complex and difficult facilities to secure, and a prized target for hackers attempting to disrupt a myriad of commercial, industrial and other online activities.

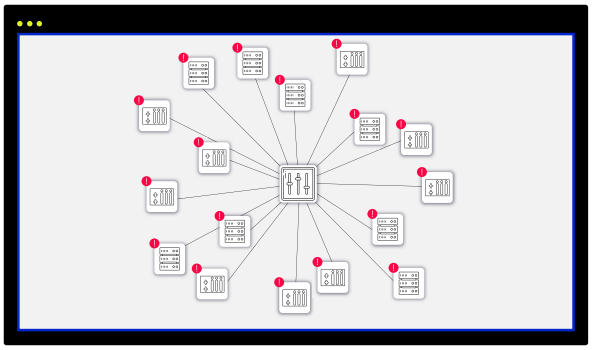
Like any other facility security project, data center security combines physical and software security, that apply to both server operation and supporting systems - cooling, power supply, etc.

The EMEA-based data center operator described herein is one of the largest in the region. Initially, the customer's OT security provided no threat detection or visibility into the industrial network, just passive, firewall-based protection.

Objectives and Challenges

The main objective stated by the customer was hardening the security of the server systems, and creating a framework for in-house operators to monitor the network and receive alerts upon network traffic exceptions:

- Securing the facility's power supply (IEC61850)
- Securing the server cooling system
- Strengthening the segmentation between building and operational systems.
- Creating a visual OT network map
- Setting up a system for presenting supply-chain attacks that may threaten the data center through equipment vendors' maintenance activities



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 project was meeting with the customer to determine their objectives and learning about the nature and the specifics of the IT-OT network at the data center.

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 facilities 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.

Once 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 programatically.

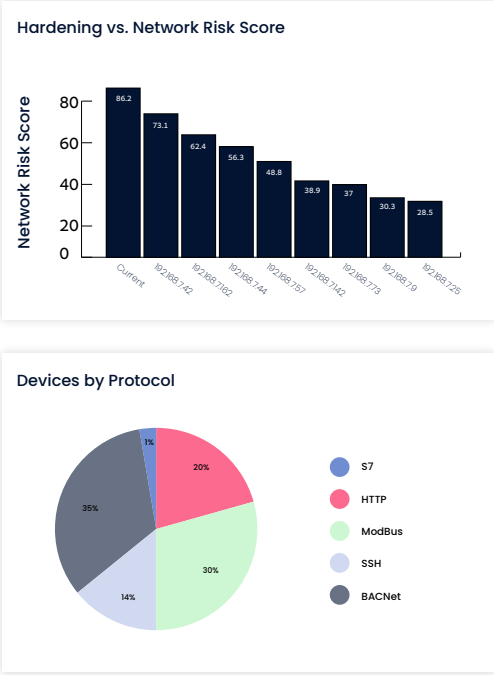
Once all unnecessary open ports and unnecessary protocols were handled, the model was deemed complete and suitable for reflecting the network's baseline activity, as well as for use as a visual network map, down-drillable to each and every device's full properties, links and vulnerabilities.

At the same time, iSID automatically created a logical business unit model, each with different security needs. These business processes, also reflected in the network map, allow applying different communication, asset and protocol rules in iSID, depending on criticality.

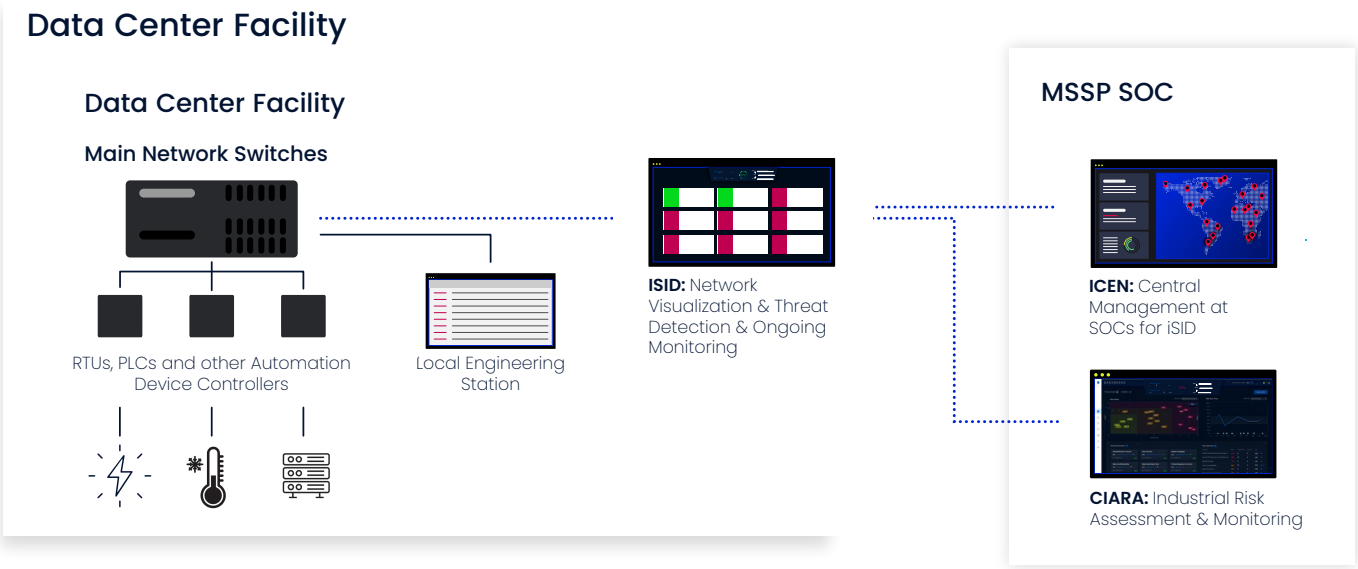
Using rule-based alerts for specific devices, iSID created a central monitoring point for critical systems, with alerts for exceeding different sensor or controller values, as well as changes to controller logic or adding devices to the network.

Current Status

At present, Radiflow's system is fully operational in one data center facility and is being considered for additional data centers operated by the customer.



Two of the many items included in the network analysis report



Schematic diagram of the data center 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

(C) 2021 Radiflow LTD. All Rights Reserved. Radiflow reserves the right to change product specifications without prior notice.