Radiflow

CASE STUDY

Securing an International Plastics Manufacturer

The Customer

The customer is an international manufacturer of industrial polymer and plastic products, with operations spanning over a dozen manufacturing facilities in Europe and Asia.

Challenges & Objectives

The customer had already deployed Radiflow's iSID industrial threat detection and management platform (in conjunction with iSAP smart collectors at operational units) at a pilot site in Europe.

The pilot, which followed a thorough selection process, was driven by a cyberattack on the company's facility. Upon review of the outcomes of the pilot installation the customer decided to extend it to four additional factories in Europe.

The objectives of project included:

- Ongoing threat detection and alerting on network anomalies
- Gaining full visibility into the OT network, with central SOC access to each and every site and production line
- Mapping of OT ports and controlling firewall access
- Ensuring regulatory compliance

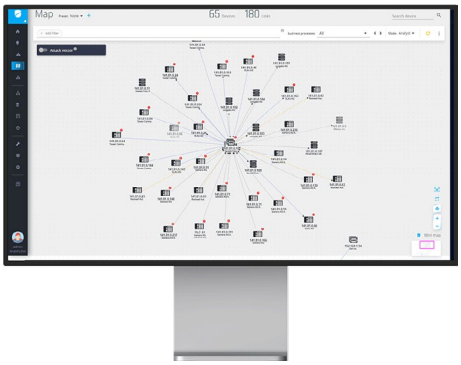
Deployment of the project's various components faced two challenges:

- Lack of remote access to switches, which required physically accessing each network cabinet across the production array at all sites
- Travel and work limitations due to Covid-19, which meant that physical installations were performed by local personnel and remotely configured by the Radiflow team

Proposed Solution

Radiflow's solution consisted of a central, virtual (VM ware) instance of iSID at each site for analysis of all data traffic network-wide.

Upon self-learning each facility's network and assets, iSID would provide full network visibility (in the form of flexible network maps). All instances of iSID would be accessible using a single iCEN management dashboard.



Radiflow iSID's network maps provide drill-down visibility into all devices along with their full properties and connections

For efficient data transfer to iSID, iSAP smart collectors were to be installed at each operational unit at both locations.

iSAP's data filtering and compression algorithm (up to 90% reduction in packet volume with no effect on operational data) prevents LAN overload and would eliminate the need to add bandwidth to accommodate to further expansion.

Deployment

As mentioned, Covid-related travel and labor restrictions necessitated that all physical installations of Radiflow products would be performed by the customer's personnel at each site.

In the end, deployment went extremely smoothly, attesting to the customer's staff's professionalism as well as to Radiflow solutions' ease of installation, both physical and virtual.

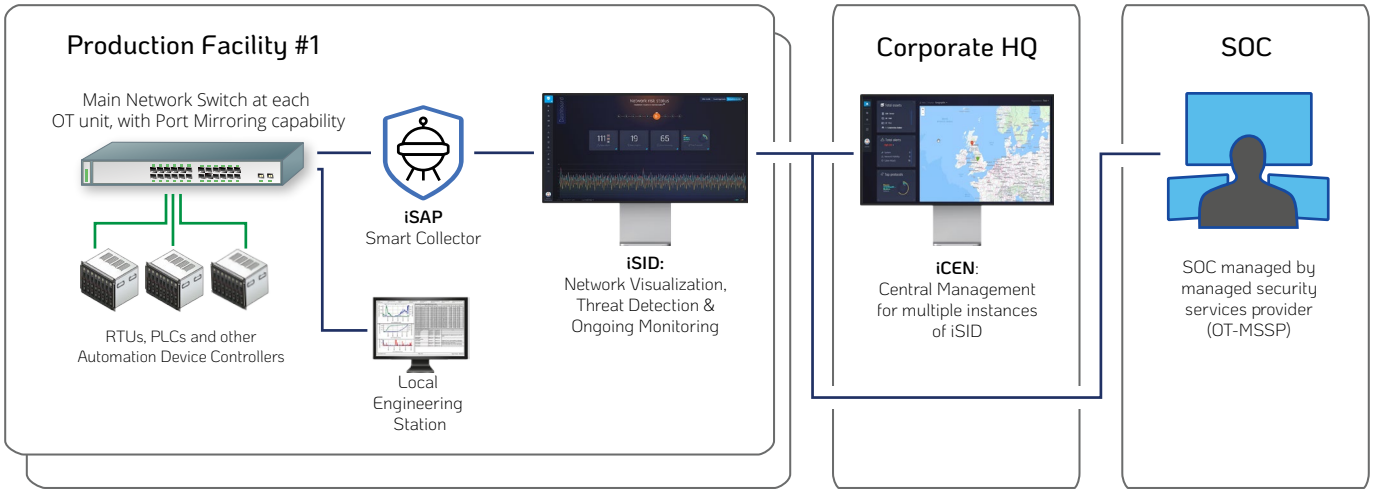
Once installed, and once all iSAP smart collectors were connected to mirrored ports (to ensure non-intrusive monitoring), the first step was self-learning the network and constructing a digital image of the industrial network including all assets properties and vulnerabilities, logical asset groupings, ports and communication protocols.

The digital image is used for network visualization, down-drillable to all asset attributes, as well for anomaly detection, serving as a "clean" baseline-activity model for "beyond-the-horizon" threat detection.

The project also calls for monthly network analyses and issuing of various security reports for different stakeholders in the organization.

Current Status

The deployment of Radiflow's solutions at all of European sites has been concluded to the full satisfaction of the customer, who has announced plans for additional expansion to facilities in Asia.



Schematic diagram of the deployment

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 7000 sites around the globe.

Radiflow