



# How a Global Manufacturing Company Protects its OT Assets from Cyber Attacks

According to a Morphisec's "Manufacturing Cybersecurity Threat Index" report, [one in five manufacturing firms](#) had been compromised by a cyberattack in the 12 months preceding the report. This dramatic increase has raised awareness among manufacturers of all sizes to install adequate OT security solutions against ransomware and other OT attack tactics, preferably those that provide added values such as improved asset/technical management and compliance enablement.

This was the case with a multi-billion-turnover manufacturer whose operations had been shut down multiple times due to attacks originating from its mail servers. After a thorough evaluation process, the customer turned to Fujitsu (as Global Systems Integrator) and Radiflow (solution developer & vendor) to take on the project.



## Objectives of the project

The customer's main objectives were:

- Upgrading the OT security system to match the current threat environment, and namely detecting and eliminating the vulnerabilities that enabled malware from the customer's mail servers to impact operations
- Gaining full visibility into the OT network and networked assets – "you can't protect what you can't see"
- Achieve IEC 62443 compliance across all production sites



## Reasons for selecting Fujitsu/Radiflow

Both companies were stated to demonstrate maturity of thinking in securing OT operations. In Radiflow's case, this was apparent in its leading the current industry-wide shift to risk-based OT security and efficiency tools such as bandwidth-friendly smart collectors

- Fujitsu is one of the few GSI's who is also a manufacturer
- Higher value/price ratio than any other competitor's solution
- The Fujitsu/Radiflow solution includes a tried-and-true integration with the ServiceNow, a technical management SaaS provider, which allows OT asset information to be fed into a CMDB.



## Solution and process

At the onset of the project, Radiflow and Fujitsu worked jointly to perform a series of site assessments for approximately 15 plants across Europe and the US. This involved both on-site data capturing and assessments using Radiflow products (iSID Industrial IDS and iSAP Smart Collector as appropriate) and remote assessments (using a remote instance of iSID) using data captured by site staffs, when on-site work was prohibited due to Covid-19 restrictions. The data collection strategy was tailored to each individual site's network topology, technical capacity, and specific assistance needs. The objective of these assessments was to detect vulnerabilities and anomalies in the OT network, and to provide visibility, in the form of a visual network model, of as much of the Operational Technology (OT) networked assets as possible.

During the site assessments the Fujitsu/Radiflow team notified the customer of critical security issues detected, which were remedied in cooperation with the customer. In addition, Radiflow iSID's ServiceNow integration and Fujitsu's ServiceNow consultancy were leveraged to ingest the detected OT asset information into the customer's existing ServiceNow CMDB, thus enabling the customers OT and IT assets to be viewed in parallel.



## Deliverable and outcomes

The deliverable of the assessment process, which was performed to the customer's full satisfaction, was a comprehensive OT risk assessment report based on the real time collected OT data. The report is currently used by the customer to budget and plan IEC 62443 compliance in its key production sites.



## What our Partner say

**Jamie Wilkie, Senior Director Enterprise and Cyber Security Fujitsu Europe:** Radiflow's onsite IDS technology combined with Radiflow's CIARA analysis software provides Fujitsu's consultants with an excellent toolkit to conduct IEC 62443 based OT cybersecurity assessments. This technical capability complements the people and process aspects of the assessments. Radiflow's technology also enables asset discovery, creating double customer value as this data can be fed into a CMDB to drive digitization initiatives beyond cybersecurity. Our assessments are conducted in collaboration with our clients. The working style of the Radiflow team blends perfectly with this approach. Together we can deliver outstanding value to our customers. For customers who wish to take the journey further into continuous security operations, Fujitsu's OT Managed Monitoring Service permanently deploys Radiflow technology to provide round-the-clock cyber visibility, with the further option of ServiceNow integration.

