Radiflow

Use Case

Cyber Security for Manufacturing

In June 2021, global meat-processing giant JBS fell victim to a ransomware attack which resulted in halting its entire US operations network for almost four days. The shutdown led to severe meat distribution disruptions as JBS supplies almost 25% of beef in the U.S.

Unfortunately, the JBS attack is not unique: using widely available tools, criminals, and increasingly nation-state actors have set their sights on critical infrastructures, manufacturing facilities and other industrial operations that utilize ICS systems due to their inherent vulnerabilities and the huge financial impact of prolonged production downtimes.

The Challenge of Securing Manufacturing Facilities

Modern manufacturing has become increasingly reliant on automation since the industrial revolution, helping drive down costs and speed up production. The process culminated with the advent of Industry 4.0 which introduced almost-fully network-based automation control.

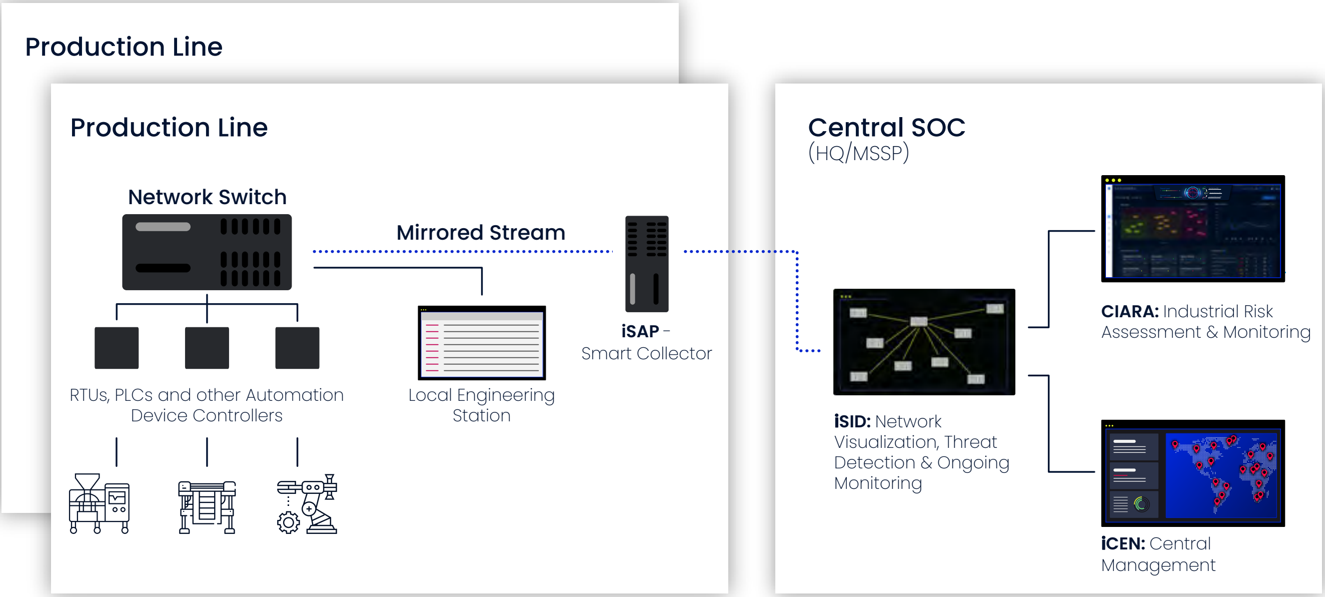
As with other OT systems, the challenge presented by this change is due to the complexity of today's automation systems, which typically host an array of devices from multiple vendors, including both new and legacy assets, as well as IT systems.

The widespread reliance on IIoT-based automation, and the subsequent need to grant network access to in-house as well as 3rd-party (vendors, system integrators) maintenance personnel, greatly increases manufacturers' exposure to cyber-threats, through both malicious and erroneous human activity.

Staying Ahead of the Hackers: Finding Creative Solutions for Securing Manufacturing ICSs

Adequate cyber-protection for networked devices (DCS, PLC and others) requires a multi-prong approach to OT security. Radiflow provides manufacturers with the tools to protect, visualize and safely maintain their systems:

1. Network modeling and visibility: The initial stage in securing industrial operations involves mapping the manufacturing OT network, including network topology, modern and legacy assets, devices, ports and all connections. The result is a virtual model (digital image) of the complete system that is presented to the operator in map form, down-drillable to each and every device's full properties and connections.
2. Risk assessment: the next step includes running numerous breach & attack simulations (OT-BAS) to evaluate the probability of an attack on different business units, and the ability of various mitigation controls (installed and proposed) to protect the network. The resulting Key Indicators (for risk, threat and control levels) and reports provide the ICS operator with a clear picture of the network's exposure to risk.
3. Implementation: based on the simulation results, an ROI-optimized OT security plan is generated, accounting for the user's security preferences and budget constraints. The user is presented with a prioritized list of mitigation measures toward strengthening and optimizing OT security, in accordance with IEC62443.
4. Long-term security management: protecting the OT network and assessing its exposure to risk is an ongoing process. New devices may be added, old ones removed, and systems regularly updated. The threat landscape also shifts rapidly. The key to long-term security is ICS network monitoring, which provides constant identification and mitigation of intrusion attempts as well as changes in the risk posture due to new threats.


Production Line
Production Line
Network Switch
Mirrored Stream
iSAP - Smart Collector
RTUs, PLCs and other Automation Device Controllers
Local Engineering Station
Central SOC
(HQ/MSSP)
iSID: Network Visualization, Threat Detection & Ongoing Monitoring
CIARA: Industrial Risk Assessment & Monitoring
iCEN: Central Management

Radiflow Solutions for Smart Manufacturing

Radiflow offers a complete suite of cyber security solutions especially designed for OT systems, which along with our in-depth understanding of the unique challenges of securing smart manufacturing facilities ensure the best path to mitigating down-time losses:

- MAP (VISUALIZE): Radiflow's iSID industrial threat detection and monitoring system generates a visual model of the entire manufacturing network including all assets, connections, protocols and vulnerabilities.
- KNOW: Radiflow's CIARA industrial risk assessment and management platform uses the iSID-generated digital image of the network, along with MITRE ATT&CK and other threat intelligence resources, to determine the most impactful threat actors and attack tactics and the effectiveness of corresponding mitigation measures, based on each network's unique characteristics. (Using a digital network image eliminates the innate potential harm of running simulations on the live network.) CIARA's risk assessment is fully IEC62443-compliant.
- ACT – Preparation and implementation of a security roadmap based on your long-and short-term security preferences (e.g. strengthening a single business unit vs. reducing overall risk) and budgetary constraints.
- MONITOR – Detection of abnormal behavior indicating breach attempts and changes to various manufacturing components and continuously monitoring the network at the corporate or cloud-based OT security provider's (OT-MSSP) SOC.

Designed especially for OT, Radiflow's solutions support most relevant OT protocols (e.g. BACnet, Profibus) for accurate modeling and anomaly detection (new devices, topology changes, abnormal memory access, and firmware changes).

About

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**