

Improving enterprise security and resiliency

Providing enhanced cybersecurity solutions through HCLTech's 360° SecureOT Framework



Customer profile

The client is a Sweden based manufacturing organization with more than 20+ globally distributed manufacturing units and generating annual revenue of more than ~ \$350 billion.



Customer business challenges

- Absence of a robust cybersecurity and governance policy for their operational technology (OT) platform that included over 10,000 OT/ICS assets
- Inability to discover OT assets and inadequate visibility on OT devices, processes, and communication
- Insufficient security monitoring and absence of real time risk insights of OT devices
- Lack of integration between security solutions and SIEM

HCLTech solution

Through its 360° SecureOT Framework, the HCLTech Cybersecurity and GRC team provided the customer with an end-to-end cybersecurity and governance program that was bespoke to their requirements. This in-depth ICS program included solutions for governance, risk reporting, service management and triage management. The HCLTech team helped the client to develop a security transformation roadmap to strengthen the cyber resilience of the plant OT network with a risk-based approach based on how people, processes, and technology measures are positioned.

We deployed threat detection sensors, connected to a centralized management console at all sites to achieve an advanced and granular protection against

cybersecurity threats. This included the implementation of an advanced threat detection tool that empowered the client to secure the entire range of their OT devices including SCADA systems, engineering workstations & servers, maintenance servers, PLCs and HMIs. With this threat detection tool, we conducted a thorough security monitoring of the OT devices to provide real-time insights into the threats and risks faced by the organization.

And finally, this tool was integrated with the existing IT SIEM solution to enable an all-encompassing cybersecurity incidents monitoring system that helped the client improve resilience against current and future threats with a secure OT platform for global operations.

Value delivered



Enabled complete systems visibility across more than 20 manufacturing units



Simplified the discovery and profiling of over 20,000 devices and assets in the OT environment



Allowed for the easy discovery of various communication and processes in the OT environment



Centralized the security monitoring of OT devices across all sites with real-time risk insights



Managed 7000+ endpoint assets using Microsoft Defender



Enabled proactive protection against OT/IT security incidents

CI-112A1AI1745412-EN00GL