Major European Defense Company Bolsters IT/OT Security Convergence in Manufacturing

Customer deploys eyeInspect to improve building automation and industrial control threat detection capabilities for the critical production of defense components.

CUSTOMER PROFILE

Defense & Aerospace

A multinational Fortune 500 company with global customers and a diversified product set with services with manufacturing plants that traverse multiple countries. The company has an advanced cybersecurity strategy centered on monitoring and response capabilities through a corporate Security Operations Center.

THE CHALLENGE Securing IT and OT Convergence

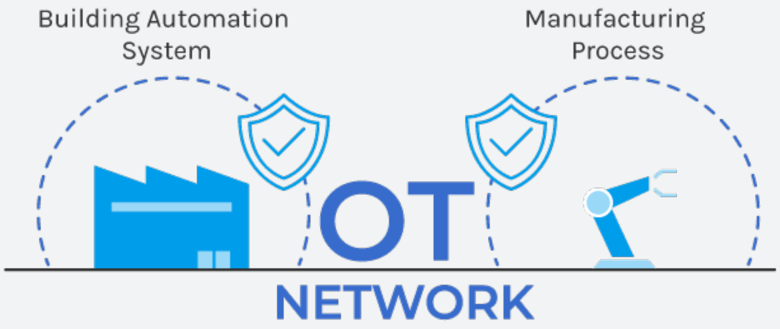
The drive to increase productivity and reduce costs in manufacturing environments has led to an exponential increase in the adoption of automation, IoT and mobile device assets on plant floors. Commercial-off-the-shelf (COTS) computers with control systems interact with field sensors and actuators to drive the production process. On top of these core technologies, intelligent devices are often employed to collect, exchange and analyze data and produce valuable business analytics

The customer identified the need to evolve from IT-centric SOCs to create converged IT-OT SOCs capable of monitoring and managing events occurring in their OT systems. They need to detect attacks and malicious behaviors that could affect their industrial facilities and factories across the world.

THE PROJECT BAS + ICS + Mobile Devices

The scope includes the OT network to be managed, including building automation systems *and* hand held devices supporting the manufacturing process. The building automation system is implanted with Siemens Desigo SW and Siemens PLCs. The hand held devices are tablets ruggedized for military use.

The project required a complete redesign of the security architecture to implement a defense in-depth strategy, as well as evolve an existing SIEM to integrate the new systems and devices on the industrial networks.



THE SOLUTION Asset Intelligence and Control

1

First, a thorough analysis of the assets on the industrial network was conducted to classify any alert and the eventual routing toward the SOC's SIEM.

2

eyeInspect sensors were deployed together with other event-collection probes to capture all the relevant cyber and operational threats.

3

Then, an automated workflow was implemented to ensure that important security alarms were forwarded to the SIEM while OT-related alarms were kept in the eyeInspect Command Center.

THE RESULTS Complete IT/OT Security Integration

Workload reduction and full OT security integration into company processes

Delivery of a converged IT/OT solution covering the industrial network *and* the SOC

Development of procedures for cyber incidents environment and operational use-cases affecting the industry

Reference model for deploying IT/OT converged security throughout the entire organization

Full documentation of the network and lessons learned

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com