FORESCOUT

Case Study

Major European Defense Company Deploys Building Automation System Security & SOC Integration for Critical Manufacturing

The customer deployed SilentDefense to improve BAS and ICS threat detection capabilities for critical production plants of defense components.

Customer Profile

The Customer is a multinational Fortune 500 company with customers worldwide, many different lines of business and diversified products and services in the DEFENSE & SPACE business. The customer owns manufacturing plants in several countries worldwide and there is in place an advanced Cybersecurity strategy centered on monitoring and response capabilities through a Corporate Security Operation Center.

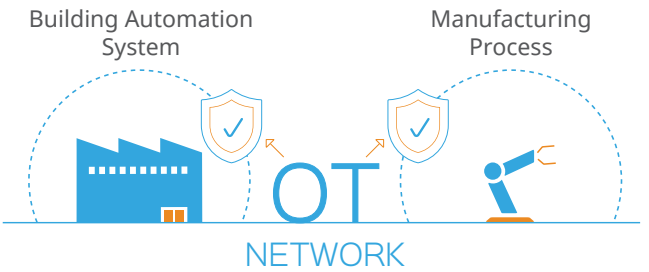
Project delivered in cooperation with S21SEC

S21SEC

The Challenge

The drive to increase productivity and reduce costs in manufacturing environments has led to an exponential increase in the adoption of automation on plant floors. Commercial-off-the-shelf (COTS) computers with control systems, which in turn 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.

In this context, the customer identified the need to evolve group IT SOCs to create converged IT-OT SOCs capable of monitoring and managing events occurring in their OT systems to detect attacks and unwanted behaviors that could affect their industrial facilities and factories across the world.



The Project

The scope of the OT network to be managed included both building automation systems and hand-held devices supporting the manufacturing process. The building automation system was implanted with Siemens Desigo SW and Siemens PLCs, the hand held devices were 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 evolving the existing SIEM to integrate the new systems and devices on the industrial networks.

The Solution

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.

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

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 SilentDefense Command Center.

Main Results

- Workload reduction and full OT security integration in the company processes
- Delivery of an IT/OT converged solution covering both the industrial network and the SOC
- Development of procedures for cyber incidents and operational use-cases affecting the industrial environment
- Reference model for deploying IT/OT converged security throughout the entire organization
- Full documentation of the network and lessons learned

Other Resources That Might Be Interesting for You

Learn more about monitoring your network:

- White paper: Benefits of Network Monitoring for Industrial Automation
- Solution brief: ICS
- Solution brief: BAS

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com