<)FORESCOUT®

Brewery Invests in Continuous Network Monitoring to Improve Their Cyber Resilience

Project delivered in cooperation with

LOGITEK·>
real time solutions

Device Visibility and Control

The investment was decided as a result of a successful proof of concept in their largest production plant, during which the company enjoyed the benefits of network monitoring in terms of visiblity and situational awareness.

The Objective

Analyze the assets, information flows and operations in its production networks in order to improve its security and efficiency, and comply with national regulation and international standards and guidelines.

The Challenge

- Large, complex and unstructured production networks with more than 2000 endpoints and applications, and limited network segmentation
- Multiple ICS vendors and a combination of proprietary and standard protocols, including: Modbus/TCP, Siemens' and Emerson's protocols
- Traditional IT protocols and applications in both server and OT networks, such as: SSL, TeamViewer, SNMP, HTTP, SMB, DNS, RDP, and DHCP
- New endpoints constantly added to the network (including private laptops), and semi-unregulated connectivity to the Internet

The Solution

SilentDefense was initially deployed for a network assessment and proof of concept. The visibility and control over the network it enabled convinced the customer to deploy it in its four major production facilities. Implementation for three additional sites was completed in 2018.

The Results

SilentDefense provided critical insights and capabilities to enable the company to enhance the underlying infrastructure and cybersecurity posture of its production facilities, including:

- A detailed inventory of all active devices and communications
- An overview of the existing misconfigurations, vulnerabilities and exposure of the network to cyber security threats
- Insights into the timing and sequence of operations for maintenance and backup activity
- Support for definition of better network segmentation
- Ability to define a baseline of desired network communications, including hosts that can or cannot communicate with the Internet
- Real-time alerts if the baseline or company policy is violated

Learn more at Forescout.com

‹›) FORESCOUT.