CASE STUDY

Optiv Helps Multi-National Food and Beverage Client Implement OT SOC

OVERVIEW
One of the world’s largest consumer packaged goods companies wanted to better understand their cyber vulnerabilities, including on their production floor. There had been a growth in attacks on supervisory control and data acquisition (SCADA) networks and they wanted to ensure production could not be interrupted by a bad actor.

Prior to Optiv’s engagement, IT assets and data were stored locally and cyber threats were handled by an overworked (and under-tuned) firewall. The lack of global visibility left the organization blind to threats and vulnerabilities. Additionally, the brewery could not modernize their most important assets due to legacy architecture and technology in the production environment. Each facility also managed their own assets, further contributing to a lack of global visibility.

HOW OPTIV HELPED
The client’s existing security operations centers (SOCs) were not set up to handle operational technology (OT) alerts, so they decided to create a brand new SOC to optimize capabilities. It was decided that Optiv would initially host the SOC and would transfer operations to the client once it was up and running. We worked with Claroty to onboard OT alerts into the newly-created SOC and trained 15 operators on the new integration. The team of 15 went on to build runbooks for alerts and orchestrated automation through their SIEM to reduce false alarms. Alongside these new SOC capabilities, Optiv also implemented IT service management capabilities tools for services management. This combination opened up global visibility and control of the client’s assets. After three months of successful operation and training, Optiv transferred management of the new SOC to the client.

INDUSTRY
Consumer Packaged Goods

CHALLENGES
- SCADA networks increasingly being targeted by attackers
- Legacy architecture and technology prohibiting modernization
- Organization was blind to vulnerabilities due to localized asset management
- Security relied on overworked firewalls

SOLUTION
- Integrated operational technology (OT) alerts through Claroty platform into newly-created SOC
- Programmed security orchestration, automation and response (SOAR) system
- Introduced IT Service Management to manage services
- Transferred control of the SOC to the client for future operations

RESULTS
- Reduced alerts from 5,000 per month to five per month
- Modernized client environment in both defense and visibility to cyber threats

NEXT STEPS
- Assessment, deployment, tuning and management of OT tools

Secure your security.™
Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.