CASE STUDY

Optiv Helps Global Pharmaceutical Manufacturing Client Implement OT SOC

OVERVIEW

One of the world's largest research-based pharmaceutical 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 factory 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

Optiv's team deployed Microsoft Azure Defender for IOT into more than 30 factories and tuned the sensors and alerts. Working jointly with the client, we created SOC runbooks to enable efficient handoffs between the SOC, Network and Production teams. This also split alerts into security and operational categories, allowing for faster resolution.

INDUSTRY

Pharmaceutical Company

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 Microsoft Azure Defender for IOT plaform into newly-created SOC
- Connected SIEM and CMBD (Configuration Management Database) environments in the OT environment
- Transferred control of the SOC to the client for future operations

RESULTS

- Provided internal SOC visibility into OT shop floor
- 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 costefficient 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.

OPTIV

Optiv Global Headquarters
1144 15th Street, Suite 2900,
Denver, CO 80202
800.574.0896 | optiv.com