CASE STUDY

FORTIFYING GLOBAL MANUFACTURING

Global Manufacturing Conglomerate Enhances Operational Technology Security with Claroty CTD

Overview

With its diverse holdings and global footprint, the manufacturer grappled with security challenges due to a lack of centralized visibility into its vast OT environment. Collaboration between IT and OT teams became imperative, driven by the escalating threat of ransomware and the need for cohesive security controls compatible with critical devices.

Challenge

- Limited visibility into Cyber-Physical Systems (CPS) devices, especially in the Operational Technology (OT) environment.
- Inconsistent security governance across IT and OT, particularly in vulnerability management and threat detection.
- Growing concerns about the threat of ransomware.
- A conglomerate with diverse industries, infrastructure, and devices.

About the Company

A privately-held global industrial manufacturing conglomerate operating in over 80 countries, faces the challenge of securing a diverse ecosystem with a wide mix of industries, switches, and devices. As the parent company overseeing industrial manufacturers and related platforms, the challenge lay in securing a conglomerate with a spectrum ranging from standard manufacturing to critical infrastructure such as a chemical catalyst plant.

Solution

The company implemented Claroty's Continuous Threat Detection (CTD) with EMC management implemented in AWS Cloud to address these challenges. The key components of the solution included:

- Real-time visibility into OT devices, irrespective of vendor or industry.
- Seamless integration of CTD into existing security frameworks through integrations.
- Migration of new business units to Claroty xDome for enhanced scalability and immediate threat updates.

Asset Discovery and Management

Utilizing the solution's asset discovery and management capabilities, the manufacturer achieved comprehensive visibility into all CPS devices. This solution provides quick issue identification, network segmentation for improved protection, and establishes a resilient OT environment.

Integration with Existing Tools

Seamless integrations of SEIM and CMDB tools extend the solution's capabilities into a more comprehensive security strategy, ensuring a unified and efficient approach to risk and vulnerability management and enabling the manufacturer to increase the ROI on their existing investments.

Claroty xDome Implementation

As new business units are deployed, the company is migrating to xDome to leverage enhanced scalability, reduced total cost of ownership, reduced support burden, and immediate access to new features and threat definitions.

Benefits

- **Asset Discovery and Enhanced Management** - This enhanced visibility facilitates an improved understanding of asset capabilities, contributing to more effective asset management practices. The newfound insights into the diverse CPS devices within its operational environment allow the global manufacturer to refine its asset management strategies, ensuring a more robust and informed approach to overseeing and optimizing asset capabilities.
- **Real-time Monitoring and Alerts** - This proactive approach to monitoring significantly contributes to the strengthening of their overall security posture, ensuring the prompt detection of suspicious activities within their operational environment. The system's capability for timely identification of vulnerabilities plays a crucial role in fortifying its defenses, allowing the company to address potential security risks promptly and maintain a resilient security stance.
- **Automation and Orchestration** - Integrating CTD with existing tools results in enhanced automation and orchestration of alerts, leading to a more streamlined incident response process. This improved automation and orchestration are pivotal in mitigating potential threats and maintaining a proactive stance against evolving cyber risks.

Conclusion

With Claroty CTD and xDome, the company achieves live monitoring, security, and unprecedented visibility and control over its OT environments. The continuous threat detection capabilities, coupled with seamless integrations and scalability, have strengthened their security posture and equipped them to proactively address evolving cyber threats across their diverse ecosystem.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.