CYBERX
BATTLE-TESTED CYBERSECURITY

CASE STUDY

How CyberX Secured Critical Operations at a Fortune 500 Oil & Gas Industry Leader

This international company is one of the world's largest oilfield services companies, providing the oil and gas industry with products and services for oil drilling, formation evaluation, completion, production and reservoir consulting. They are a Fortune 500 company with a strong top-down focus on safety and environmental protection. The oil and gas industry continues to be a high-stakes target for threat actors, and as this company implemented digital transformation to increase operational efficiency, they needed an IoT/OT security solution that would protect their people, production, and profits in the face of increased risk.

THE PROBLEM

Before deploying CyberX, this organization had no visibility into their OT assets, vulnerabilities, or potential IoT/OT threats. OT visibility was also valuable from an operational perspective, to rapidly detect and address misconfigured or malfunctioning equipment and improve operational efficiency.

This company was in the middle of implementing a digital transformation initiative, which only made the need for OT visibility and security more pressing. Digital transformation and Industry 4.0 drive the deployment of many new IoT/OT devices — along with pervasive connectivity between IT and OT networks — and thus also increase the attack surface by a factor of 3x compared to just a few years ago.

These IoT/OT devices don't support agents and are often unpatched, unmanaged, and invisible to IT teams – making them soft targets for adversaries seeking to disrupt production facilities and/or gain access to corporate networks. To make matters worse, most of the legacy OT devices and protocols deployed in ICS environments were developed decades ago and are insecure by design, lacking modern controls such as strong authentication, encryption, and hardened software stacks.

The firm's existing OT environment included a variety of IT security technologies (including Splunk, ServiceNow, and Palo Alto Networks), OT equipment vendors (such as Fujitsu, Honeywell, Mazak, Rockwell Automation, Yokogawa, and more), and OT protocols (such as Ethernet/IP CIP, including Rockwell extensions; and Modbus TCP and RTU, including Schneider Electric extensions). Their chosen solution needed to integrate with their existing IT security stack and SOC workflows, and also needed to be able to provide continuous visibility into this wide variety of protocols and asset types.

HIGHLIGHTS

- In the wake of an internal audit and an incident that resulted in downtime, this Fortune 500 oil & gas leader needed a robust IoT/OT security platform for asset discovery, risk and vulnerability management, and threat detection.
- CyberX automatically discovered assets across a wide variety of manufacturers, device types, and protocols.
- CyberX provides continuous threat monitoring with superior anomaly detection, along with vulnerability management and automated threat modeling to protect their crown jewels.
- Armed with expertise and maturity, CyberX's expert team worked closely with IT & OT to ensure that needs from all key stakeholders were met.
- IT Security Stack: Splunk, ServiceNow, Palo Alto Networks, and more.
- OT Environment: Fujitsu, Honeywell, Mazak, Rockwell Automation, Yokogawa, and more.
- OT Protocols: Ethernet/IP CIP (including Rockwell extensions); Modbus TCP; Modbus RTU (including Schneider Electric extensions), and more.

Furthermore, their networks were mostly flat. This significantly increased their risk level, since flat networks make it easy for threat actors to perform reconnaissance and move laterally unencumbered.

A Call to Action

OT security quickly leapt to the top of the priority list when this company experienced a security incident that resulted in production downtime. Because this company had no visibility into OT assets or vulnerabilities, nor any form of OT threat detection, this incident went on undetected long enough to result in lost production and lost person-hours.

In the wake of this incident, OT security attracted board-level attention. An internal audit was launched to identify weaknesses, and correcting these weaknesses became a top priority.

In addition to concerns about safety and environmental incidents -- and downtime -- the board was also concerned about potential theft of sensitive intellectual property such as information about their proprietary refining processes.

Finally, the management team also wanted to use OT security as a core differentiator when selling to their own clients.

The project was led by the global OT security program manager.

In the wake of an incident that caused production downtime, OT security attracted board-level attention. The company launched an internal audit to identify OT security weaknesses.

THE SOLUTION

This company needed a solution that gave them visibility into all their assets, even across the wide variety of protocols and devices they had in their environment. Their chosen solution also needed to help them detect, manage, and prioritize vulnerabilities (including reporting on CVEs), and detect their top risks to crown jewel assets.

They also required threat monitoring and anomaly detection with full contextual information. While they initially attempted to use logging to address threat monitoring, this approach didn’t provide the level of contextual detail required for rapid detection and response.

They also needed this solution to deploy quickly and scale easily on a global basis, since they have more than 150 plants worldwide.

Finally, it was very important to the OT security program manager to balance the needs of OT with the requirements of plant leadership and IT. By taking a face-to-face approach with the OT team at each individual plant, the program manager ensured that OT priorities and concerns were equally considered. Since OT teams were primarily concerned with safety and efficiency -- and, of course, very focused on avoiding downtime -- this meant that their chosen solution also needed to provide the operational benefits important to OT leadership, as well as avoid using any active scanning techniques or incompatible systems that could result in downtime.

However, fulfilling all these requirements proved to be a challenge. Some OT security platforms lacked the deep device and protocol understanding necessary to understand these complex OT environments, others used risky "active" discovery techniques, and others lacked OT expertise and were slow to respond to unique customer requirements.

A POC with CyberX, however, proved to be the answer to their challenges. CyberX's agentless IoT/OT cybersecurity platform met all requirements for detailed asset visibility, vulnerability management, and threat detection -- all while providing expert, collaborative support to the OT security program manager and his team to ensure that all stakeholder needs were being addressed quickly and pragmatically.

THE BENEFITS

CyberX's agentless platform met and exceeded the core requirements of the project including seamless integration with their SOC tools, enterprise-wide scalability -- and zero impact on the OT network.

CyberX met all requirements for detailed asset visibility, vulnerability management, and threat detection -- all while providing expert, collaborative support to the OT security program manager and his team to ensure that all stakeholder needs were being addressed quickly and pragmatically.

Asset Discovery

CyberX automatically generated an asset inventory of all OT assets, even across their wide variety of vendors and protocols. CyberX has a broad and deep understanding of diverse OT devices and protocols, providing the comprehensive device visibility that they needed. Plus it immediately identifies when unauthorized devices are connected to the OT network, such as by third-party contractors.

Risk and Vulnerability Management

By continuously tracking both network- and device-layer vulnerabilities – regularly updated with CyberX's threat intelligence -- CyberX helps the client track improvements in their overall risk score and prioritize patching activities. What's more, by predicting the most likely paths of targeted IoT/OT attacks on crown jewel assets, CyberX's automated IoT/OT threat modeling enables security and OT personnel to quickly visualize, prioritize, and simulate mitigation actions to protect their most critical processes. This is key to a risk-based approach that enables them to make more effective use of limited people resources and narrow maintenance windows.

Superior Anomaly Detection

CyberX's patented, M2M-aware behavioral analytics gave this company superior anomaly detection, providing deep contextual information for rapid incident response, with minimal false positives and a faster learning period. Deployment is also simplified because there's no need to configure any rules or signatures, nor have any prior knowledge of the IoT/OT environment.

Fast and Easy Deployment That Scales Enterprise-Wide

CyberX was easy to deploy, leveraging extensive automation to minimize time and effort required from plant personnel. What's more, CyberX proved its ability to scale across many sites, while still remaining centrally managed and providing centralized risk views across business units and geographies. CyberX is also integrated with the company's IT security stack in order to leverage existing SOC workflows and quickly spot attacks that frequently cross IT/OT boundaries.

Expertise and Maturity

Ultimately, it was CyberX's unparalleled expertise that was the clinching factor for the OT security program manager. CyberX had the most mature solution of the vendors evaluated -- exhibited both in technology and in the expertise provided by the support team, which ensured that the project was a success for all stakeholders.

Now, CyberX is an integral part of this company's OT security program and a key part of their defense-in-depth strategy. CyberX protects their people, production, and profits by providing continuous IoT/OT asset management, risk and vulnerability management, and continuous threat monitoring -- all while offering a unified approach to IT/OT security monitoring and governance.

CyberX had the most mature solution of the vendors evaluated -- exhibited both in technology and in the expertise provided by the support team, which ensured that the project was a success for all stakeholders.

About CyberX

We know what it takes.

Funded by Norwest Venture Partners, Qualcomm Ventures, and other leading venture firms, CyberX delivers the only cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT/OT risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies.

For more information, visit CyberX.io or follow @CyberX_Labs.