CYBERX
BATTLE-TESTED CYBERSECURITY

CASE STUDY

How CyberX Provided Immediate Value to a Fortune 500 Manufacturing Company

This US manufacturing company has global operations and revenues of over $5b USD, is listed on the New York Stock Exchange, is a component of the S&P 500 and has been a Fortune 500 company for over 10 years, with operating sites in more than 25 different countries. Protecting people, production and profits at this large and growing company was of paramount importance to the CISO and the board of directors and when they began looking for an IoT/OT security solution in 2018.

THE PROBLEM

Lack of Security Controls at Manufacturing Plants

The initial engagement with the company was driven by a multitude of needs: The company lacked visibility into asset inventory and as a result lacked a means of managing the risks and vulnerabilities posed by those “invisible” assets. They also lacked threat monitoring capabilities in their networks. At this particular company, IT security maturity was relatively high -- their SOC included a SIEM from Splunk, firewalls from Palo Alto Networks, Network Access Controllers from Cisco and an IT ticketing system from ServiceNow. They knew that whatever IoT/OT security vendor they chose would have to integrate into their existing IT security stack.

THE SOLUTION

OT Asset Discovery, Risk and Vulnerability Management, and more

After the CyberX proof of concept was set up in the first plant, the first of many asset maps filled up quickly. The evaluators were sufficiently impressed -- even more so when they found that they could generate vulnerability reports at the click of a button, that enabled them to prioritize patching for their most critical "crown jewel" assets.

Continuous IoT/OT Threat Monitoring, Incident Response, & Threat Intelligence

This customer wanted to know if they had any IoT/OT threats in their network, and they wanted to respond quickly to any threats via integration with their existing IT security stack. Of special importance was the need to leverage existing SOC personnel and tools in order to centralize IT and OT security. Finally, they needed to demonstrate to auditors that they had a safety- and security- first environment.

HIGHLIGHTS

- CyberX was deployed in minutes and showed asset maps almost immediately.
- Once assets were mapped, risks and vulnerabilities were reported upon with the click of a button.
- After a baseline of network activity was established, CyberX was able to alert on anomalous network behavior.
- Alerts were integrated seamlessly into the company’s SIEM (Splunk).
- Millions of dollars of losses were avoided when CyberX performed root-cause analysis of an operational issue that caused intermittent downtime.

THE BENEFITS

Operational Insights Provided by CyberX Save Millions of Dollars

Deployments at the first seven plants were finished ahead of schedule. At the first post-deployment meeting, the customer revealed an incident in which CyberX had shown what the customer described as "immediate value."

The site manager recalled: "Our CISO and their team received separate calls to assess an issue at a plant that was causing intermittent down time. The site team had spent the previous 36 hours chasing down what was causing the downtime and had found nothing."

The site team called the CISO to ask if a firewall rule was preventing PLC communication within the plant, which the CISO said was impossible given the architecture. Her first question to the site team was "Did you check the CyberX console?" The site team checked the CyberX console, identified the problem and was able to solve it within 5 minutes.

So what had happened? It turns out that an employee had performed a laptop upgrade, which led to an upgrade of his RSLogix application with default settings. The default settings of RSLogix caused the laptop to start flooding the local network with scans, leading to a disruption in PLC communications.

This particular factory is the customer's single largest production facility and runs 24x7. The failure to check CyberX first likely resulted in over $1m in lost top line revenue. Though a tough lesson to learn, it *was* learned -- the team is now keenly aware that if they encounter equipment malfunctions in the future, the first thing they will do is check CyberX to perform root-cause analysis.

Needless to say, the CISO and the CISO's team --- already impressed with CyberX's ability to deploy quickly, discover assets, manage risk and vulnerabilities, provide threat monitoring, and integrate with their existing IT stack -- are now CyberX uber fans, having seen the millions of dollars CyberX can and will save them when future operational issues arise.

"Did you check the CyberX console?"

This was the first question the CISO asked when intermittent downtime was striking at the heart of this company's most productive facility. The answer was no -- but when the team did check CyberX they discovered the operational issue and fixed it within 5 minutes, potentially saving the company millions of dollars in losses.

ABOUT CYBERX

We know what it takes.

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 risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies.

CyberX delivers the only IoT/OT security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture. CyberX is also the only IoT/OT security company to have been awarded a patent for its M2M-aware threat analytics and machine learning technology.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their IoT and OT networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

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

CYBERX
BATTLE-TESTED CYBERSECURITY