CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

Case Study: Global Pharmaceutical Manufacturer

The Problem: Ransomware

With a presence in 120 countries worldwide and revenue in excess of $1 billion, this leading pharmaceutical company operates manufacturing facilities across the US, Europe, and Asia. Dedicated to ongoing innovation, the company has built an extensive portfolio of innovative medicines across multiple therapeutic areas.

Just as they rolled out a major distribution and marketing expansion in Europe, the firm was breached via malware that entered their network via a VPN connection originating in Asia. The malware then spread to manufacturing facilities in both the US and UK. Luckily, the malware failed to encrypt the hard drives it infected, and the plants survived unscathed.

Had the malware successfully executed its payload, the firm would have experienced financial losses in the tens of millions of dollars due to lost production and cleanup costs.

More importantly, the malware would have resulted in a failure to produce vital medicines that patients across the world depend upon.

According to the CISO, the cause of the breach was a combination of weak IT security at the Asia facility, where the malware originated, and a lack of any OT anomaly detection capabilities in both the US and UK plants.

Realizing that he had dodged a bullet, the CISO began shoring up the company's IT practices and exploring available IoT/ICS security technologies. He had previously explored endpoint security solutions but found they were not effective for OT environments.

In addition to the malware incident, the CISO was also concerned that new devices are being connecting to their OT network on a regular basis, which causes challenges both operationally and with regards to security risk.

His search for an OT security solution quickly revealed there are only two companies worth exploring – and that most of the other companies claiming to provide OT security were merely IT security solutions "re-packaged" for OT security.

This is particularly important because the firm has a diverse mixture of OT equipment from multiple automation vendors, including Rockwell, Aveva Wonderware, Siemens, and B&R Industrial Automation. Security technologies developed for IT typically have a limited understanding of the specialized protocols, devices, and behaviors found in OT environments, rendering them ineffective in identifying OT assets, vulnerabilities, and threats.

After conducting reference calls with CyberX customers in the pharma industry — including with one of the top 5 pharma companies in the world — and seeing how fast and easy it was to execute the Proof of Concept (PoC) in their production environment, the CISO was convinced that CyberX was the best choice.

The Solution: Rapid Deployment, Continuous OT Threat Visibility

The rollout began shortly after the PoC was conducted. "Rollout is going better than expected, and we're now planning to go live a month earlier than expected," remarked the CISO.

Additionally, alerts generated by the CyberX platform are now integrated with the firm's SIEM solution (ArcSight), providing his Security Operation Center (SOC) analysts with deep visibility into the OT network and its OT devices such as HMIs, engineering workstations, PLCs that they hadn't had before.

For the CISO, having CyberX in place enables him to track and report to the board about on meaningful ICS security metrics. His key metrics are a combination of the likelihood of a threat occurring, the likelihood of the threat being detected, and the likelihood of the threat doing damage.

In the past, these metrics were negatively influenced by the fact that the team had no way to detect suspicious or unauthorized behavior in the firm's (such as unauthorized remote access), known malware such as WannaCry or LockerGoga, or the presence of unauthorized devices in the firm's OT networks.

With CyberX in place, the CISO can now report there's a meaningfully higher likelihood of detecting threats and unauthorized activity in his OT networks.

The Benefits: Reduced Risk of Costly Production Outages, Safety Incidents, and IP Theft

CyberX has helped this pharmaceutical firm reduce the risk of costly production outages that could disrupt the supply of crucial medicines and cost the firm millions of dollars in lost revenue.

Second, they've reduced the likelihood of catastrophic safety and environmental incidents caused by attacks on safety systems monitoring manufacturing processes involving hazardous chemicals.

Finally, they are protected from cyber espionage attacks aiming to steal sensitive intellectual property about proprietary medicines developed by the firm.

Asset Discovery, Vulnerability Management, Threat Monitoring and More

The firm now enjoys benefits in each of these areas:

Asset Discovery
They can now continuously see what devices they have, how they're connected, and how they're communicating with each other.

Risk & Vulnerability Management
The firm now has a complete, up-to-date list of all network and device vulnerabilities and a prioritized to-do list for mitigating those vulnerabilities — based on risk to their most important "crown jewel" assets.

Continuous Threat Detection & Response

CyberX continuously monitors the the firm's OT network and generates real-time alerts for anomalies such as new devices being plugged into the network, unauthorized programming changes to PLCs, destructive malware such as EternalBlue, and cyber reconnaissance activities such as network scanning. CyberX is the only industrial cybersecurity company to have been awarded a patent for its innovative, ICS-aware threat detection analytics and machine learning technology.

Unified IT/OT Security Monitoring and Governance via SOC Integration

Real-time information from CyberX is integrated with the company's SOC via their SIEM, enabling the company to leverage their existing investments in people, training, runbooks, and workflows.

This unified approach to IT/OT security monitoring and governance enables the company to leverage scarce resources across both IT and OT, and more effectively combat advanced threats that often cross IT/OT boundaries.

The company has also held SOC Integration workshops to break down organizational silos between IT and OT, and to help the teams better understand and communicate with each other.

Streamlined Compliance

CyberX has also helped the company streamline its compliance and internal audit reporting for global pharmaceutical and safety regulations. Activities that were previously performed manually, such as collecting and reporting on database changes in historians, or asset inventory information, are now automated and as a result happen more frequently and more quickly.

Operational Benefits

The benefits that the company reaps are not limited to cybersecurity improvements. OT engineers can now quickly identify the root cause of equipment malfunctions and misconfigurations using the built-in data mining and reporting capabilities of the CyberX platform.

Centralized Command-and-Control

Perhaps most importantly, the control engineers and security analysts at the company now have centralized command-and-control over their OT networks. They not only see their current network topology and all activity, they can take action to make their network more efficient. They not only see anomalous traffic but hunt down anomalies and take corrective measures. And they not only spot intrusions and malware, they implement firewall and NAC policies to block or quarantine malicious hosts.

CyberX is now providing defense-in-depth via continuous IoT/ICS asset management, risk and vulnerability management, and continuous threat monitoring — along with a unified approach to IT/OT security monitoring and governance.

In summary, CyberX is now an essential part of ensuring that this global pharmaceutical manufacturer is optimizing its security posture as well as its manufacturing operations.

ABOUT CYBERX

We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IoT and ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IoT/ICS 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 & ICS security company to have been awarded a patent for its ICS-aware threat analytics and machine learning technology.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Splunk, McAfee, Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems.

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 ICS 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.