CYBERX
BATTLE-TESTED 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.

Worse, 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/OT 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 were being connected to their OT network on a regular basis, which caused both operational and security challenges.

His search for an OT security solution revealed there were 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.

HIGHLIGHTS

- A breach originating from a remote connection infected hard drives worldwide
- The malware threatened to interrupt the company's ability to produce medicines that patients around the world depended on to stay alive
- CISO concerned about new devices being connected to the network causing security and operational challenges
- Diverse mix of OT equipment from multiple vendors including Rockwell, Aveva Wonderware, Siemens, and B&R Industrial Automation complicated the search for security solutions
- During evaluation process, CISO concluded that most OT security solutions were just IT security solutions repackaged as OT security
- CyberX now sends OT alerts to ArcSight in the company's SOC
- The metrics and output that CyberX produces are now part of the CISO's regular reports to the Board of Directors

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 three of the top ten 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, historians, engineering workstations, PLCs that they hadn’t had before.

For the CISO, having CyberX in place enables him to track and report meaningful ICS security metrics to the board. 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 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 that there is significantly reduced risk of unauthorized activity in their OT network going undected.

Why CyberX?

Reference calls with 3 of the top 10 global pharmaceutical companies convinced the CISO that CyberX was the best choice.

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 cyberespionage attacks aiming to steal sensitive intellectual property about proprietary medicines developed by the firm.

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/OT risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

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 ICS-aware threat analytics and machine learning technology.

Notable CyberX customers include three of the top ten US energy utilities; three of the top 10 global pharmaceutical companies; Global 2000 companies across other diverse industries including manufacturing, chemicals, oil & gas, mining, transportation, and healthcare; multiple government agencies including the US Department of Energy; and national electric and gas utilities across Europe and Asia-Pacific. Integration partners and MSSPs include industry leaders such as Splunk, IBM Security, Palo Alto Networks, ServiceNow, Fortinet, HPE/Aruba, Cisco, RSA, McAfee, Optiv Security, DXC Technology, Toshiba, Singtel/Trustwave, 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.

CYBERX
BATTLE-TESTED CYBERSECURITY

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