CYBERX
BATTLE-TESTED CYBERSECURITY

CASE STUDY

GLOBAL AUTOMOTIVE MANUFACTURER

With revenues of over 3.3b USD, this specialty automotive parts maker is headquartered in Europe, listed on the NYSE, and runs 15 manufacturing plants worldwide. Each of those sites includes as many as 60 assembly lines and include a heterogeneous mix of equipment from diverse automation suppliers. The innovative designs and parts created by this company have been used by nearly every major global automaker, and today over 100 million vehicles powered by gas, diesel, electric, and fuel cells use their applications.

THE PROBLEM

No visibility into IoT/ICS networks

The conglomerate that owned and controlled this company did not have adequate visibility into the assets, let alone the threats, in their plants. As a result, they didn't know which parts were vulnerable, and they had no way to know whether the traffic in their networks was behaving normally or if their networks were affected by operational inefficiencies due to malfunctioning or misconfigured equipment, or worse, malicious actors.

Within the past few years, the specialty automotive parts maker was spun off by their parent company and was thus given an opportunity to re-think how they secured their operations.

The newly anointed CISO of the newly formed entity took advantage of the opportunity and worked with partners to find an IoT/ICS security provider that would give him and his team greater visibility into the assets in his plants -- and the ability to rapidly detect and respond to suspicious or unauthorized behavior in their plant networks. Together with his team, the CISO created a list of problems they wanted their IoT/ICS security vendor to solve. Highlights from that list include:

1. Prevent costly downtime associated with destructive ransomware that has hit other automotive plants worldwide.
2. Detect threats in networks governed by IoT/ICS-specific protocols.
3. Alert us when internal employees or contractors create unexpected (either intentionally or unintentionally) changes to assets (including HMIs, PLCs, and other SCADA devices) on our networks.
4. Report on known vulnerabilities in our IoT/ICS networks.
5. Bring IT and OT alerts under a single management platform (Splunk).
6. Support a diverse mix of automation vendors including ABB, Schneider Electric, Siemens, Rockwell, and Codesys.

HIGHLIGHTS

- CyberX deployed in 1 week across sites on multiple continents
- Found and eradicated WannaCry in multiple sites
- Integrated with the customer's existing Security Operations Center tools including Splunk
- Implementation sparked collaboration between OT and IT teams
- Hardware-agnostic architecture eased customer's purchasing decision

Though the CISO took the initiative to make the change, news of WannaCry attacks and subsequent downtime at other automotive makers got the interest of the board. Timing became an even greater challenge because of this top-down pressure.

THE SOLUTION

Asset Discovery, Continuous Network Security Monitoring, Vulnerability Management, and Integration with Existing SOC

Through the recommendation of a trusted 3rd party, the company chose to run a proof of concept with CyberX in several sites. CyberX was charged with discovering the assets in their network, providing continuous network security monitoring, managing vulnerabilities, and integrating into their existing SoC systems.

According to the CISO, "ease of deployment," along with an unprecedented level of support from CyberX staff during the rollout, was one of the main reasons CyberX was chosen. The CyberX platform delivered insights about assets, vulnerabilities, and threats in less than an hour after being connected to the network switch. The platform was deployed in 1 week across plants in multiple continents. CyberX had no problem identifying assets and continuously monitoring network traffic. Most importantly, at multiple sites, CyberX found and eradicated WannaCry -- ransomware that has previously caused hundreds of millions of USD in damage at other F2000 companies.

THE BENEFITS

Eradication of WannaCry malware

With the help of the CyberX support team, the customer was able to eradicate the destructive ransomware from their sites and networks in Brazil, Slovakia, and India.

CyberX was successfully integrated with Splunk so that IT and OT alerts could be correlated via a single system in the SoC. The CyberX platform sends alerts whenever internal employees or contractors create any changes to assets. CyberX also detects and sends alerts to Splunk whenever malicious actors attempt to conduct reconnaissance or deploy malware in the customer's IoT/ICS networks. The process of integration of CyberX with Splunk sparked cooperation and communication between the IT and OT teams.

CyberX has a deep understanding of more than 80 IoT/ICS-specific protocols and incorporates patented M2M-specific analytics with machine learning to identify anomalous behavior. This means it can quickly identify suspicious or unauthorized activities with minimal false positives and a faster learning period. The customer also liked the fact that they could deploy the software on any hardware server of their choice.

Last but not least, the CISO and his team were also given accolades from the executive team when all their milestones were achieved ahead of the board-prescribed schedule.

Why CyberX?

"Ease of deployment," along with an unprecedented level of support, were cited as the main reasons the CISO of this automotive manufacturer chose CyberX.

ABOUT CYBERX

We know what it takes.

CyberX delivers the only 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/ICS risk and preventing costly production outages, safety and 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 M2M-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; 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, ServiceNow, Palo Alto Networks, CyberArk, Fortinet, McAfee, Cisco, HPE/Aruba, 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/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.

CYBERX
BATTLE-TESTED CYBERSECURITY