CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

Case Study:
US Energy Company

The Problem: Lack of OT Visibility

The Principal Control Engineer at one of USA's Top 5 power and energy companies had seen what happened after the company's IT team installed a Security Information and Event Management (SIEM) system in their enterprise IT network, and he liked what he saw. With the SIEM in place, the Security Operations Center (SOC) now had full visibility into all network activity, anomalies, and most importantly, high-risk intrusions such as targeted attacks and malware. Where once they were blind, they now could see.

With that taken care of, they turned their attention to the last network into which they did not have visibility: The critical Operational Technology (OT) network that runs the company's energy plants. Traditional network security monitoring (NSM) tools offered by IT security companies didn't understand the specialized protocols and industrial control system (ICS) devices deployed in OT networks.

As the engineers at the Company put it, "Our SOC analysts needed deep visibility into our OT network — especially around cyberattacks that could bring down our plants or cause safety and environmental incidents."

The Solution: Purpose-Built ICS Security Monitoring

After an examination of several OT security vendors, the Company chose two for final consideration. A positive recommendation for the CyberX platform from another customer pushed CyberX over the top. The timing was fortuitous -- both in terms of installation and getting approvals – since a new LNG terminal was under construction. With the purchase order for the facility's network came a purchase order for the ICS network security monitoring solution from CyberX. CyberX was installed even before the network went live.

The Benefits: Operational Efficiency, Continuous Threat Detection, and Streamlined Compliance

The company now enjoys full visibility into their OT network just as they do for their IT network, enabling them to immediately spot suspicious or unauthorized activities that indicate an adversary may have compromised the network.

This enables the Company to reduce the risk of costly production outages that could disrupt the flow of energy to millions of businesses and consumers. It also reduces the risk of catastrophic safety failures and environmental incidents.

In particular, the Company now enjoys benefits in each of these areas:

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

Risk & Vulnerability Management
They now have 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 company's OT network and generates real-time alerts for anomalies such as new devices being plugged into the network, unauthorized programming changes to Programmable Logic Devices (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 reporting for NERC-CIP. Activities that were previously performed manually, such as collecting and reporting on 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. As an IT Manager put it: “We don’t use CyberX just for security – CyberX has also helped us enhance day-to-day operations.”

Once CyberX provided visibility into the OT network, they quickly saw where operational improvements could also be made. For example, when CyberX alerted on what IT engineers characterized as a network “packet storm,” he used CyberX’s Event Timeline and data mining capabilities to pinpoint the specific devices that were causing bandwidth issues. After asking OT engineers to check the configuration of these devices, the two teams together discovered that their interval settings were misconfigured. After adjusting the settings, the network traffic returned to normal.

Centralized Command-and-Control

Perhaps most importantly, the engineers and 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, they implement firewall rules to block intrusions.

CyberX is now an essential part of this Fortune 500 American power and energy company operations and security posture. CyberX is providing defense-in-depth strategy, OT asset maps, vulnerabilities and risk management, behavioral anomaly alerts, and providing a unified approach to IT and OT security monitoring and governance.