SOC Services for OT Security

OT-enable your SOC with customized OT incident response workflows, automated ICS malware analysis, security training, and integration services

Highlights

- **Customized workflows & simulations** for responding to OT security incidents in your existing SOC
- **Automated ICS Malware Analysis via** a cloud-based sandbox service
- **Customized training and workshops** for SOC personnel about the unique characteristics of OT environments
- **Customized integrations** with SOC products (IBM QRadar, Splunk, LogRhythm, ArcSight, Palo Alto Networks, ServiceNow, CyberArk, etc.)
- **Onsite OT incident response**

Benefits

- Smoothly integrate IT & OT security
- Ensure fast & effective OT response
- Address shortage of OT security skills
- Break down IT/OT silos
- Strengthen operational resilience

CyberX Deployment

- Passive monitoring with zero impact on production ICS networks
- Physical or virtual appliances
- No rules, signatures, or agents
- Deep embedded understanding of ICS/SCADA protocols, devices, vulnerabilities & threats
- Continuous ICS asset visibility, vulnerability management & threat monitoring

Reducing ICS & IIoT Risk for Industrial & Critical Infrastructure

Digitalization and IIoT are driving increased connectivity between IT and OT networks. This increases the attack surface and hence the risk to production facilities.

CyberX provides the most widely-deployed and mature platform for continuously reducing OT risk. Benefiting from hundreds of deployments worldwide, the platform provides SOC analysts with continuous, real-time visibility into all OT assets, vulnerabilities, and threats.

Additionally, by integrating with the broadest range of IT security products — from industry leaders such as IBM Security, Splunk, Palo Alto Networks, CyberArk, and others — CyberX enables you to implement a unified IT/OT security governance strategy that leverages scarce security resources across both IT and OT.

Integrating IT and OT Security in Your Existing SOC

As CISOs become accountable for both IT and OT security, they are looking to rapidly add OT responsibilities to existing SOC teams with minimal additional effort.

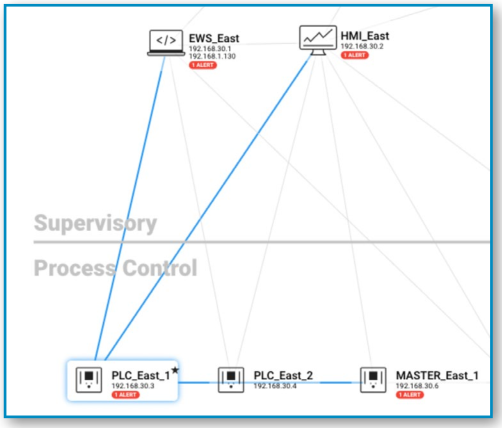
CyberX has developed a suite of services that enable your existing SOC team to integrate OT visibility and alerts into your existing policies and workflows, so they can effectively respond to OT security incidents.

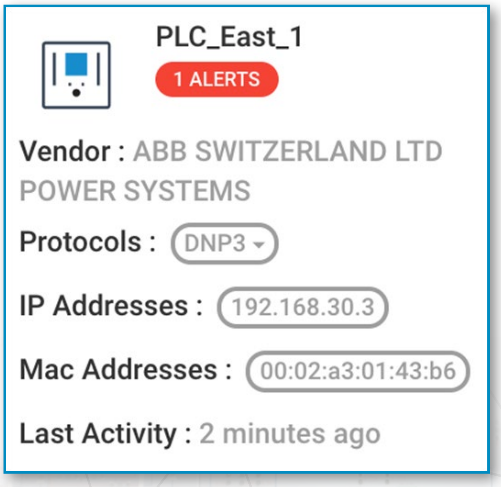
We'll also help your SOC staff and OT control engineers efficiently communicate and collaborate with each other using a common language and objectives — accelerating the removal of IT/OT silos that have traditionally existed in many organizations.

Our goal is to empower your current Tier 1 SOC analysts to handle the majority of OT incidents without escalation, and to minimize alert noise from your OT environment.

By building upon the significant investments CISOs have already made in SOC personnel, processes, and technology, CyberX enables you to confidently assume responsibility for both OT and IT security — thereby supporting a single enterprise-wide risk view across both IT and OT domains.

Examples of OT asset profiles and security alerts generated by the CyberX platform— we'll customize your SOC workflows and enable your SOC analysts so they can quickly respond to OT security incidents using this information.




PLC_East_1

1 ALERTS

Vendor : ABB SWITZERLAND LTD POWER SYSTEMS

Protocols : DNP3

IP Addresses : 192.168.30.3

Mac Addresses : 00:02:a3:01:43:b6

Last Activity : 2 minutes ago

Customized Workflows and IR Simulations

We'll work with your team to adapt your existing SOC workflows to the unique characteristics of OT.

For example, when responding to an alert about an unauthorized change to a Programmable Logic Control (PLC), your SOC analysts will typically need to communicate directly with designated control engineers in the plant, to verify whether the change was malicious or not.

Finally, we'll help you test the entire end-to-end process — by the end of the first day — with simulated malicious network traffic to ensure everything is working correctly.

Automated ICS Malware Analysis

Unique in the industry, CyberX offers a cloud-based sandbox service for automated ICS malware analysis.

With a single click, you can upload suspicious files and immediately determine if the malware targets OT assets — and exactly how they're impacted — along with a list of network- and host-based IOCs associated with the malware.

The automated service is designed specifically for ICS malware and works even for zero-day malware that has never been seen before.

Our team will also suggest clean-up strategies with detailed recommendations about how to protect your OT environment in the future.

This unique approach enables your SOC team to easily embed ICS-specific malware analysis into their existing IR workflows.

How the ICS Malware Sandbox Works

Leveraging CyberX's extensive ICS expertise and deep understanding of ICS protocols, devices and applications, CyberX's cloud-based sandbox creates a virtual ICS environment for executing suspected ICS malware.

The simulated ICS environment in which the malware executes includes all essential run-time components such as ICS-specific libraries, services, connected PLCs, registry keys, DLLs, etc.

The system then instruments the malware during execution to comprehensively analyze its behavior and document its IOCs.

Customized Training & Workshops for SOC Personnel

Leveraging CyberX's extensive ICS expertise and deep understanding of ICS protocols, We'll teach your SOC team about the unique characteristics of OT environments, so they can efficiently communicate with OT personnel when investigating incidents and orchestrating remediation actions.

For example, it's not typically possible to regularly patch and reboot devices in OT environments. Your SOC should understand this key difference, so they can describe alternate ways to protect critical assets (such as via more granular segmentation, continuous monitoring, etc.).

Additionally, although specific TTPs are often different for OT attacks, the attack chain is similar to the one your IT security analysts are already familiar with (e.g., initial compromise, internal reconnaissance, establishing footholds, privilege escalation, lateral movement, etc.).

During our workshops, our OT security experts will describe the similarities and differences so your staff can leverage their existing training and skills.

Customized Integrations with Firewalls

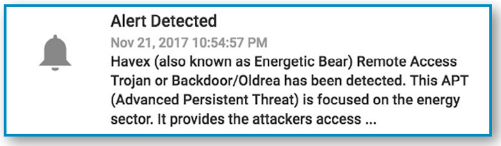
The CyberX platform has also been integrated with standard firewalls (Palo Alto Networks, Checkpoint, Fortinet, etc.) to enable immediate blocking of malicious traffic. We'll work with your team to develop the right prevention mechanisms without risking impact to your production environment.

Additionally, our automated vulnerability assessment technology allows you to upload firewall rules and analyze them to see if they're secure, based on the traffic observed by our platform.

Onsite Incident Response

CyberX experts are also available to back up and supplement your team with onsite OT incident response services. You'll benefit from the proven expertise of military cyber experts who previously performed OT incident response for nation-state threats.

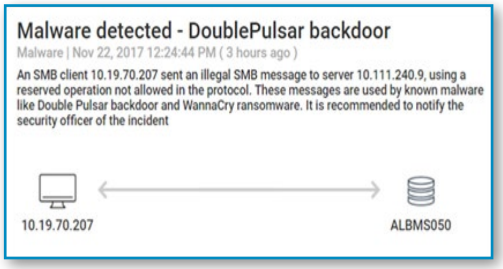
During these onsite engagements, we'll speed incident response by performing critical activities such as: case analysis and scope determination; data acquisition and preservation; network- and host-layer forensics; malware analysis; remediation and clean-Up; and delivering a comprehensive incident response report.



Alert Detected

Nov 21, 2017 10:54:57 PM

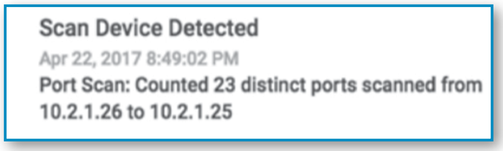
Havex (also known as Energetic Bear) Remote Access Trojan or Backdoor/Oldrea has been detected. This APT (Advanced Persistent Threat) is focused on the energy sector. It provides the attackers access ...



Malware detected - DoublePulsar backdoor

Malware | Nov 22, 2017 12:24:44 PM (3 hours ago)

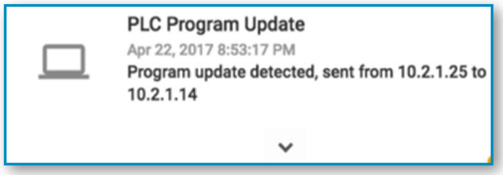
An SMB client 10.19.70.207 sent an illegal SMB message to server 10.111.240.9, using a reserved operation not allowed in the protocol. These messages are used by known malware like Double Pulsar backdoor and WannaCry ransomware. It is recommended to notify the security officer of the incident



Scan Device Detected

Apr 22, 2017 8:49:02 PM

Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25

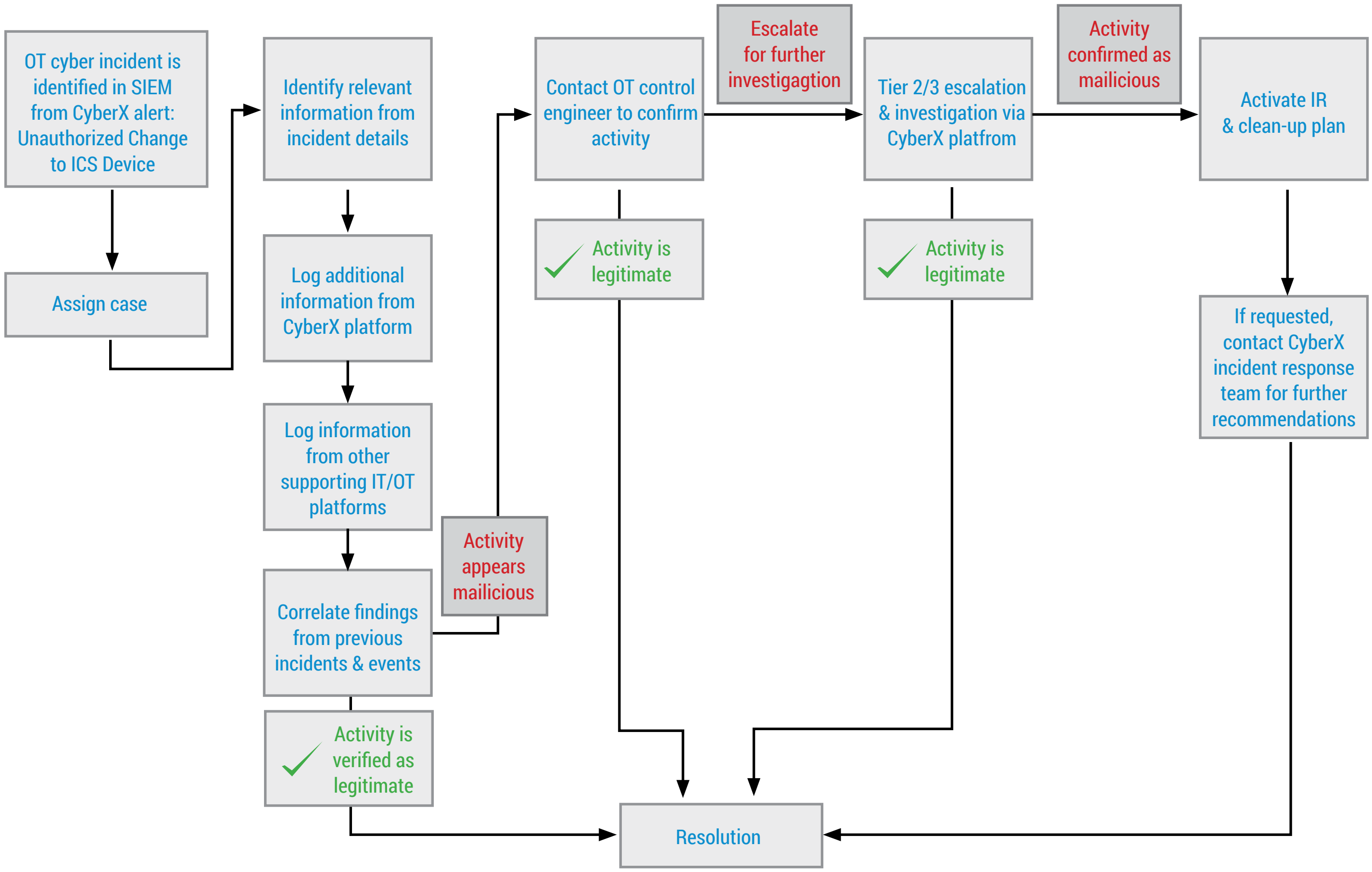


PLC Program Update

Apr 22, 2017 8:53:17 PM

Program update detected, sent from 10.2.1.25 to 10.2.1.14

Example SOC Workflow for Unauthorized Changes to ICS Devices


OT cyber incident is identified in SIEM from CyberX alert: Unauthorized Change to ICS Device
Assign case
Identify relevant information from incident details
Log additional information from CyberX platform
Log information from other supporting IT/OT platforms
Correlate findings from previous incidents & events
✓ Activity is verified as legitimate
Activity appears mailicious
Contact OT control engineer to confirm activity
✓ Activity is legitimate
Escalate for further investigagtion
Tier 2/3 escalation & investigation via CyberX platfrom
✓ Activity is legitimate
Activity confirmed as mailicious
Activate IR & clean-up plan
If requested, contact CyberX incident response team for further recommendations
Resolution

CyberX experts will work with your SOC and OT teams to develop customized workflows and procedures for effectively responding to OT security incidents.

About the CyberX Platform

CyberX combines a deep, embedded understanding of industrial devices, protocols, and applications with continuous monitoring, ICS-aware behavioral analytics, and ICS threat intelligence. CyberX's proprietary self-learning engines deliver contextual insights about ICS assets, targeted attacks, malware, vulnerabilities, and attack vectors — in less than an hour — without relying on rules or signatures, specialized skills, or prior knowledge of the environment.

About CyberX

Founded by military cyber experts with nation-state expertise defending critical infrastructure, CyberX provides the most widely-deployed platform for continuously reducing IIoT and ICS risk. CyberX is backed by elite investors including Norwest Venture Partners (NVP). The company is a member of the IBM Security App Exchange Community and the Palo Alto Networks Application Framework Community, and has integrated with other best-of-breed security suppliers such as CyberArk for secure remote access technology. CyberX's partners also include premier solution providers and MSSPs worldwide including Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems..

Trusted. Industrial. Cybersecurity.