THE CYBERX PLATFORM

Protect Your PEOPLE, PRODUCTION, and PROFITS

The Industrial Internet of Things (IIoT) is unlocking new levels of productivity, helping organizations improve safety, increase output, and maximize revenue. At the same time, digitalization is driving deployment of billions of IIoT devices and increased connectivity between IT and Operational Technology (OT) networks, increasing the attack surface and risk of cyberattacks on industrial control systems.

The CyberX platform is the simplest, most mature, and most interoperable solution for auto-discovering assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring ICS networks for malware and targeted attacks. What’s more, CyberX provides seamless integration with existing SOC workflows for unified IT/OT security governance.

Example of a real-time alert including detailed contextual information to enable incident response.

Unauthorized PLC Programming
Policy Violation | Nov 21, 2017 10:54:57 PM (yesterday)

PLC 10.2.1.14 was programmed from device 10.2.1.3 using protocol DNP3, which is not defined as an Engineering Station. This is not allowed by policy. It is recommended to notify the security officer of the incident.

Control Area 1

Mitigation
• Consult a relevant Control Systems Engineer to validate this infraction.

Example of a real-time alert including detailed contextual information to enable incident response.

HIGHLIGHTS

• Address all 4 points of Gartner’s Adaptive Security Architecture: Detect, Respond, Predict, Prevent
• Rapid, non-intrusive deployment
• “Passive monitoring” to establish asset inventory
• Optional “selective probing” or “active” asset discovery
• Expert ICS threat intelligence
• Streamlined incident response, threat hunting & forensics
• Network topology mapping
• Non-invasive ICS risk & vulnerability assessments
• Centralized management
• Automated threat modeling for ICS
• ICS Malware Sandbox
• High Availability (HA)
“The risk to OT networks is real – and it’s dangerous and perhaps even negligent for business leaders to ignore it.”

Michael Assante, SANS Director of Critical Infrastructure & ICS/SCADA Security

How are you addressing risk from modern ICS and IIoT threats like WannaCry, NotPetya, and TRITON?

Recent campaigns clearly demonstrate that perimeter firewalls and conventional ICS/SCADA defenses — including outdated notions like “air-gapping” and “security by obscurity” — are no longer sufficient to protect OT networks from today’s targeted attacks, sophisticated malware, and insider threats.

Business leaders are justifiably concerned about modern ICS threats, which can result in costly production outages, catastrophic safety and environmental failures, and theft of corporate trade secrets.

A NEW APPROACH IS REQUIRED

The new approach must be:

- **Continuous and real-time** — to immediately alert on unusual activity with minimal false positives.

- **Passive and non-intrusive** — with zero impact on OT networks and devices.

- **Heterogeneous and vendor-agnostic** — with broad support for specialized ICS protocols and control system equipment from all ICS vendors (Rockwell Automation, Schneider Electric, Siemens, Yokogawa, etc.).

- **Integrated with existing SOC workflows and security tools** — including centralized SIEMs, firewalls, IDS/IPS, and security analytics technologies.

WHY CYBERX

CyberX provides the most widely-deployed industrial cybersecurity platform for continuously reducing IIoT and ICS risk. To date, the company has deployed its platform in more than 1,200 production ICS networks worldwide, across all industrial sectors.

The CyberX platform delivers continuous ICS threat monitoring and asset discovery, combining a deep embedded understanding of industrial protocols, devices, and applications with ICS-specific behavioral anomaly detection, threat intelligence, risk analytics, and automated threat modeling.

The fact is, CyberX is the only company that addresses all four requirements of Gartner’s Adaptive Security Architecture — with a practical, appliance-based system that can be deployed in less than an hour.
Addressing All 4 Requirements of Gartner Adaptive Security Model
Firewalls & Signature-Based Mechanisms Are No Longer Sufficient to Protect Against Advanced Attacks

**DETECT**
- Continuous monitoring
- Behavioral analytics with self-learning
- Patented ICS-aware algorithms

**RESPOND**
- Deep incident forensics, investigation & threat hunting capabilities
- Full-fidelity PCAPs for drill-down analysis
- Native app-level integration with IBM QRadar, Splunk, and ServiceNow

**PREDICT**
- Automated threat modeling to predict most likely paths of attack vector chains
- Baselining behaviors & configurations
- Proprietary ICS-specific threat intelligence (zero-days, malware, adversaries, etc.)

**PREVENT**
- Proprietary ICS-specific risk & vulnerability assessments including asset discovery
- Proactive, risk-based prioritization of mitigation actions for hardening critical "crown jewel" assets
- Integration with leading prevention technologies including next-generation firewalls, unidirectional gateways, and secure remote access (privileged account security) solutions

CyberX Platform Architecture

**RAPID NON-INTRUSIVE DEPLOYMENT**

The CyberX appliance connects to a SPAN port or network TAP and immediately begins collecting ICS network traffic via passive (agentless) monitoring. It has zero impact on OT networks since it isn’t placed in the data path and doesn’t actively scan OT devices.

**CENTRAL MANAGEMENT**

CyberX’s Central Manager provides a consolidated view of all your assets, so you can quickly identify where assets are located based on customizable filters such as type (PLC, RTU, DCS, etc.), manufacturer, model, and firmware revision level.

Central Manager also delivers a real-time view of key OT risk indicators and alerts across all your facilities — tightly integrated with your SOC workflows and runbooks — to enable easy prioritization of mitigation activities and cross-site correlation of threats.

Finally, Central Manager provides centralized deployment of software, threat intelligence, and configuration updates across all CyberX appliances in your organization.

CyberX delivers an agentless platform with “single pane of glass visibility” into all of your assets, vulnerabilities, and threats — achieved via patented, ICS-aware analytics, deep embedded knowledge of ICS protocols and devices, and proprietary ICS & IIoT threat intelligence.
SOLUTION BRIEF: The CyberX Platform

REAL-TIME ANOMALY DETECTION OF ICS THREATS

The CyberX platform identifies anomalies via continuous monitoring and five different analytics engines that incorporate self-learning to eliminate the need for updating signatures or defining rules. The engines leverage ICS-specific behavioral analytics and data science to continuously analyze OT network traffic for anomalies including: the use of packet structures and field values that violate ICS protocol specifications; behaviors indicating the presence of known malware such as WannaCry/NotPetya; policy violations; operational issues such as early signs of equipment failure; and unusual machine-to-machine (M2M) communications and behaviors.

By modeling ICS networks as deterministic sequences of states and transitions — using a patented technique called Industrial Finite State Modeling (IFSM) — as well as embedding deep knowledge about ICS protocols and applications, the CyberX platform requires a shorter learning period than generic mathematical approaches or analytics originally developed for IT rather than OT. It also detects anomalies faster, with minimal false positives.

EXPERT ICS THREAT INTELLIGENCE

CyberX's in-house team of threat analysts are world-class domain experts that track ICS-specific zero-days, campaigns, and adversaries as well as reverse-engineer malware. This intelligence enriches our platform analytics and also supports our managed services for incident response and breach investigation.
The platform provides an intuitive data mining interface for granular searching of historical traffic across all relevant dimensions (e.g., time period, IP or MAC address, ports, plus protocol-specific queries based on function codes, protocol services, modules, etc.). Full-fidelity PCAPs are also provided for further drill-down analysis.

The platform integrates out-of-the-box with all SIEMs and offers native apps for IBM QRadar and Splunk. The platform also integrates with leading firewall providers such as Palo Alto Networks and orchestration platforms such as ServiceNow. These integrations enable more efficient communication and collaboration between IT and OT teams.

CyberX provides a timeline that makes correlation of events and alerts easier.
Gaining visibility into all installed ICS assets and how they’re connected is often the first step in strengthening ICS security. CyberX displays the network based on the Purdue Model, and provides detailed information about devices including name and type (Historian, PLC, DCS, etc.), IP/MAC, manufacturer, protocols used, serial number, firmware revision level, etc.

The CyberX platform combines passive monitoring and optional selective probing (or “active scanning”) techniques to provide this information. CyberX’s passive monitoring technology has been widely deployed because it is non-invasive and has zero impact on production networks. It works by collecting a copy of the traffic from the SPAN port of a network switch or via a network tap, using proprietary Network Traffic Analysis (NTA) to provide valuable and comprehensive information about your asset inventory.

**COMPREHENSIVE ICS ASSET DISCOVERY & NETWORK TOPOLOGY MAPPING**

CyberX auto-discovers all assets and generates a network topology diagram based on the Purdue Model.
Optional selective probing consists of software modules that query Windows and embedded devices like PLCs for specific asset details (such as firmware or Service Pack revision levels) — using safe, vendor-approved commands, scheduled to run as often or as infrequently as desired (typically once per day). The resulting asset information is displayed in our standard console, in the standard asset inventory screens. For example, selective probing provides an immediate snapshot of device details such as OS and firmware revision levels.

**NON-INVASIVE ICS RISK & VULNERABILITY ASSESSMENTS**

Unique in the industry, CyberX uses proprietary Network Traffic Analysis (NTA) algorithms to passively identify all network and endpoint vulnerabilities such as unauthorized remote access connections, rogue or undocumented devices, weak authentication, vulnerable devices (based on unpatched CVEs), unauthorized bridges between subnets, and weak firewall rules. The platform generates a comprehensive report including an objective risk score for the entire ICS network, as well as risk-prioritized mitigation recommendations for strengthening your ICS risk posture.

**AUTOMATED THREAT MODELING FOR ICS**

Exclusive to CyberX, the company’s Automated ICS Threat Modeling technology applies proprietary algorithms to risk and vulnerability data in order to predict the most likely paths of targeted attacks on ICS/SCADA networks. By generating a visual representation of all possible attack vector chains — ranked by risk — targeting your most critical OT assets, it enables you to prioritize essential mitigations and simulate what-if scenarios to reduce your attack surface (e.g., “If I isolate or patch this insecure device, does it eliminate the risk to my ‘crown jewel’ assets?”). This enables more effective use of limited skilled resources during narrow maintenance windows.
CyberX’s comprehensive risk & vulnerability assessment report provides an overall security score with detailed information about network and endpoint vulnerabilities discovered via passive monitoring and Network Traffic Analysis algorithms. It also includes remediation recommendations for improving your score over time, prioritized by risk.

Asset discovery includes detailed information about device type, manufacturer, open ports, and vulnerabilities (CVEs), as well as an overall security score for the device.

Unique in the industry, CyberX’s Automated ICS Threat Modeling incorporates proprietary analytics to continuously predict the most likely paths of targeted attacks on ICS/SCADA networks.
ICS MALWARE SANDBOX

By virtualizing a complete OT environment, CyberX’s ICS Malware Analysis Sandbox can rapidly and automatically identify OT-specific malware, pinpoint its IoCs, and enable threat intelligence sharing across the global ICS community.

Unique in the industry, CyberX’s ICS Malware Analysis sandbox is a cloud-based subscription service that identifies OT-specific malware — including zero-day malware — by executing suspicious files in a virtualized OT environment.

HIGH AVAILABILITY

An optional high-availability (HA) configuration adds a backup centralized management console that periodically receives backups of all configuration files required for recovery. If the master console fails, the local site management appliances will automatically switch to synchronizing with the backup console and continue without interruption.

In addition, each local appliance can be configured to perform periodic backups of its complete system configuration, as well as all event data and the complete system database. Users can configure the backup to be stored on any external device on the network.

The ICS Malware Sandbox analyzes suspicious files by executing them in a virtualized OT environment.
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 IIoT and ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IIoT & 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 IIoT & 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 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.