Industrial and critical infrastructure organizations often struggle to gain a global view of their OT assets, vulnerabilities, and threats.

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.

It 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.

**Four Different Views of Global Security Posture**

Central Manager provides four different color-coded dashboards for all networks and zones across geographies. Combined, these dashboards provide a comprehensive graphical view of your risk posture across the following four areas:
1. **Risk Management** – Shows the aggregated risk score from each site’s Vulnerability Assessment allowing security managers to prioritize improvements to their OT security risk posture.

2. **Malicious Activity** – Shows sites that have exhibited signs of known malware such as TRITON.

3. **Incident Response** – Shows sites that have exhibited other types of suspicious or anomalous behavior such as port scanning.

4. **Operational** – Shows potential operational incidents such as disconnected devices, PLC Stop commands, firmware uploads, and program uploads.

**Seamless Integration with Your Security Operations Center (SOC)**

Central Manager streamlines threat detection and prevention by enabling a unified approach to IT and OT security through integrations with existing SOC workflows and security stacks, including SIEMs, ticketing systems, security orchestration and automation systems, and next-generation firewalls. This enables SOC analysts to leverage optimized workflows based on insights gained from global CyberX deployments across all industrial sectors and six continents.

The CyberX ICS Malware Analysis Sandbox, a separate cloud-based service for identifying ICS-specific malware, allows analysts to upload suspicious files and immediately receive IoCs without the need to hire skilled reverse-engineering personnel.

**Correlate Events and Alerts Across Multiple Sites**

Central Manager provides a unified timeline view of alerts and events across all global facilities, enabling analysts to cross-correlate suspicious and unauthorized activities that may be occurring in different geographies and sites.

This enables SOC analysts to rapidly identify root-causes in order to accelerate incident response, investigations, and forensics. What’s more, an intuitive data mining interface enables sophisticated threat hunting across geographies and sites.
Continuous Visibility — Even When Disconnected from Central Manager

Unlike other solutions that simply collect and forward network traffic data, CyberX local appliances continue to analyze network traffic data and generate real-time alerts, even when disconnected from the Central Manager. Local plant personnel can thus continue to see alerts during, for example, malware outbreaks that require disconnection of local facilities from the corporate network.

With other solutions that rely on the Central Manager to perform all analysis, local teams are blind to anomalies and unable to investigate incidents when the local appliance is disconnected from the central site.

Define Logical Management Groups Based on Business Requirements

CyberX’s Central Manager enables analysts to view and manage their ICS environments using custom logical groups based on asset properties such as asset type, production line, physical zones within a plant, or business unit. This enables assets and threats to be managed according to your business requirements, unlike other solutions that force assets to be grouped according to the network to which they’re connected or appliances by which they are monitored.

Figure 2: Centrally manage CyberX appliances as well as integrations with SOC workflows, runbooks and security stacks including SIEMs, ticketing and orchestration systems, and next-generation firewalls.

Configure & Update All Appliances from a Single Console

Central Manager provides the ability to manage all CyberX appliances from a single pane of glass. For instance, from the Central Manager, security managers can easily deploy threat intelligence and software updates to their CyberX appliances worldwide. They can also centrally manage appliance settings such as alert forwarding rules and how CyberX’s five analytics engines are configured.

Additional Enterprise Capabilities

- High-availability and redundancy
- Granular administration of Role-Based Access Control (RBAC)
- Multitenancy support for MSSPs
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.