Industrial and critical infrastructure organizations know that threats from adversaries continue to become more sophisticated. However, they even struggle to keep accurate inventory of the assets that they need to protect, let alone actually implement strategies to keep those assets protected.

The CyberX platform combines passive monitoring and optional selective probing (or “active scanning”) techniques to provide the most accurate and detailed inventory of assets in industrial and critical infrastructure organizations.

**ASSET DISCOVERY**

Passive monitoring with optional active technology—“Hybrid” approach provides comprehensive asset discovery & ongoing management

Industrial and critical infrastructure organizations know that threats from adversaries continue to become more sophisticated. However, they even struggle to keep accurate inventory of the assets that they need to protect, let alone actually implement strategies to keep those assets protected.

The CyberX platform combines passive monitoring and optional selective probing (or “active scanning”) techniques to provide the most accurate and detailed inventory of assets in industrial and critical infrastructure organizations.

**HIGHLIGHTS**

The CyberX Asset Inventory Advantage:

- Continuous passive monitoring to establish baseline inventory
- Optional selective probing for comprehensive “point in time” view using safe, vendor-approved device queries
- Hybrid “best of both worlds” approach
- Proven expertise: Asset inventory performed on over 1,200 production ICS networks worldwide

**Figure 1:** Topology map showing communication behavior between ICS devices, as provided by passive monitoring.

**Figure 2:** Device profile obtained by clicking on one of the devices in the network topology map.
Passive Monitoring

Historically, industrial and critical infrastructure organizations have been reluctant to allow security devices to connect to their production networks. 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.

Passive monitoring captures detailed information about ICS assets such as the IP and MAC address, serial number, product name, product code, manufacturer, device type, and OS or firmware version.

![Proprietary Deep Packet Inspection and Network Traffic Analysis (NTA)](image)

**Figure 3:** Passive monitoring uses SPAN ports or network taps to analyze traffic with zero impact on production networks

Passive monitoring also provides tabular details of devices, as shown below:

![Asset Inventory](image)

**Figure 4:** Rich device details provided by passive monitoring
Selective Probing ("Active Scanning")

In organizations with highly-segmented environments, it can be resource intensive to connect appliances to each segment of the network for passive monitoring. For more mature organizations, where their policy allows active querying of ICS devices, CyberX offers an optional selective probing approach.

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.

Selective probing (active scanning) provides the same textual information about devices that passive scans provide.

Figure 5: Selective probing queries ICS devices using safe, vendor-approved commands

Hybrid Approach: Best of Both Worlds

Because there are advantages to each approach, CyberX is finding more and more organizations are interested in a "hybrid" approach to asset discovery and inventory. A hybrid approach offers the advantage of providing a baseline view of assets using continuous passive monitoring, while providing a comprehensive "point in time" inventory of assets using selective probing, especially for isolated assets on highly segmented networks.
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.