CyberX mitigates ICS/SCADA risk with patented, ICS-aware self-learning engines that deliver immediate insights about ICS assets, vulnerabilities, and threats — in less than an hour — without relying on rules or signatures, specialized skills, or prior knowledge of the environment.

To address lack of visibility into the security and resiliency of OT networks, CyberX developed the ‘CyberX ICS Threat Monitoring App for IBM QRadar’ – a native integration between CyberX and IBM QRadar that enables a unified approach to IT and OT security. This tight coupling of CyberX’s purpose-built OT security platform with IBM QRadar not only provides improved visibility to address OT security risks, but also serves as an essential building block for removing silos between IT and OT security teams by supporting a “single pane of glass” for monitoring and responding to both IT and OT security alerts.

The app provides SOC analysts with multi-dimensional visibility into the specialized OT protocols and IIoT devices deployed in industrial environments, along with ICS-aware behavioral analytics to rapidly detect suspicious or anomalous behavior.

The app also enables both IT and OT incident response from within one corporate SOC — an important evolution given the ongoing convergence of IT and OT to support new IIoT initiatives such as smart machines and real-time intelligence about production operations.
A STRATEGIC AFFILIATION

CyberX worked closely with IBM to ensure our App utilized the native QRadar API. The resulting application is ‘IBM Validated’ and freely available to the security community through the IBM Security App Exchange.

IBM QRAder Security Intelligence screen shot showing detailed ICS threat information obtained from the CyberX platform, and how it appears to SOC analysts with CyberX’s new ICS Threat Monitoring App for QRadar.

CYBERX PLATFORM

A continuous monitoring platform purpose-built for detecting and addressing OT network security risks. It generates actionable security intelligence that enables enterprises to respond faster to identified risks in their OT networks, thus strengthening the overall resiliency of their ICS environments – the #1 concern of ICS security execs.

IBM QRAder SIEM

Helps security teams accurately detect and prioritize threats across the enterprise and provides intelligent insights that enable teams to respond quickly to reduce the impact of security incidents.

CYBERX ICS THREAT MONITORING APP DEPLOYMENT

- Integration with IBM QRadar using native API
- Available at no cost to the security community through the IBM Security App Exchange

CYBERX DETAILS & DEPLOYMENT

- Agentless technology operates in real time with zero impact on OT networks
- Proprietary ICS self-learning engines inventory and profile assets to detect OT network threats
- Does not rely on rules, signatures, specialized skills, or prior knowledge of the environment
- Broad & deep support for analyzing ICS/SCADA protocols & services to identify vulnerabilities
- Passive monitoring (port mirroring)
- Multiple form factors: physical or virtual appliance
- Delivers insights in less than an hour
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.