CyberX ICS Threat Monitoring App for IBM QRadar

Deliver OT network visibility & security alerts into your corporate SOC

What It Enables

A unified view of all OT alerts

- OT alerts filtered using 5 distinct CyberX analytics engines: cyber anomalies, malware, protocol violations, operational anomalies, policy violations.

Integration of alerts with IBM QRadar

- Accurately detect and prioritize threats across the enterprise
- Choose which alerts appear based on severity level, anomaly type, and industrial protocol.
- Reduce false positives

Correlation of CyberX alerts with IBM QRadar intelligence sources including:

- Log events and network flow data collected from IT and OT systems, devices, endpoints, and applications.

Ability to leverage QRadar integration with other IBM security components

- Watson; User Behavior Analytics; Network Insights; Vulnerability Manager; Incidents Forensics; etc.

Benefits

Enables unification of OT & IT security, strengthens operational resilience, and reduces OT-related security risks:

- Costly OT network downtime
- Damage to critical infrastructure
- Environmental devastation
- Health & safety of human lives
- Regulatory violations

Monitor & Respond from a "Single Pane of Glass"

Industrial and critical infrastructure organizations are increasingly concerned about ICS/SCADA threats.

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.

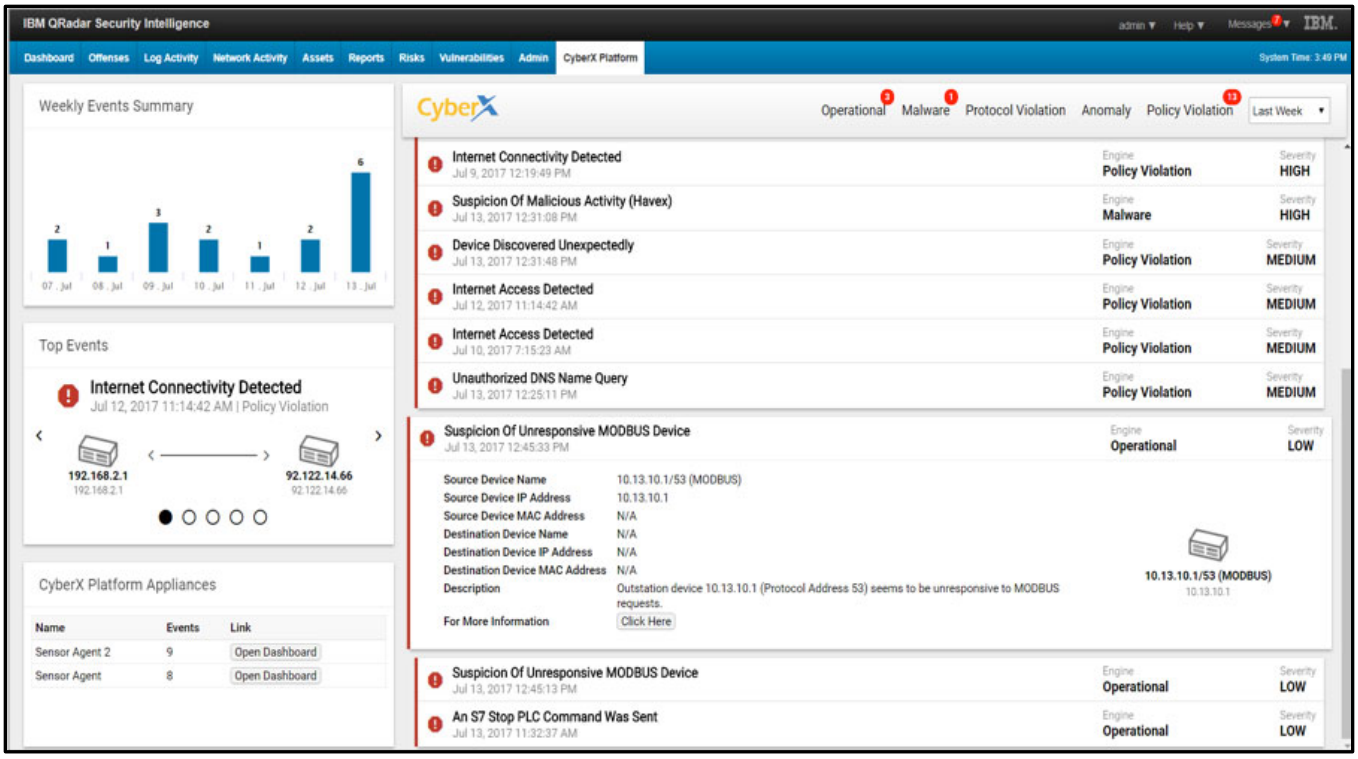
Multi-Dimensional Visibility Across OT Protocols & Devices

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 QRadar 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 QRadar 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 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

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

About CyberX

Founded by military cyber-experts with nation-state expertise defending critical infrastructure, CyberX provides the most widely-deployed platform for continuously reducing ICS and IIoT risk.

CyberX is a member of the Palo Alto Networks Application Framework developer community and the IBM Security App Exchange Community and has partnered with premier MSSPs and solution providers worldwide including Optiv Security, DXC Technologies, and Deutsche-Telekom/T-Systems. For more information, please visit CyberX-Labs.com.