NTT | CYBERX

Data Sheet

# Securing IoT, Operational Technology (OT) & Industrial Control Systems (ICS) with CyberX

## The IoT/OT Security Challenge

As digital transformation and Industry 4.0 unlock new levels of productivity and efficiency, they are also driving deployment of new IIoT devices and increased connectivity between IT and OT networks.

Because these devices don't support agents — and are often unmanaged, unpatched or misconfigured — they can easily be compromised by adversaries.

As a result, boards and management teams are increasingly concerned about the expanding attack surface and risk of **costly downtime, safety incidents, and theft of sensitive intellectual property.**

**Did you know?**

- **64%** of industrial sites are still using plaintext passwords
- **71%** of sites are running older versions of Windows that no longer receive security patches
- **22%** of sites exhibit indicators of threats such as scan traffic, malicious DNS queries, abnormal HTTP headers, and malware such as LockerGoga and EternalBlue.

*Source: CyberX 2020 Global IoT/ICS Risk Report, based on passive analysis of 1,800+ production networks*

## The CyberX Platform

CyberX's agentless IoT/OT security platform is easy to deploy and provides real-time visibility to all unmanaged devices within minutes of being connected to the network.

Leveraging the industry's only patented, IoT/ICS-aware behavioral analytics — eliminating the need to configure any rules or signatures — the CyberX platform:

- **Discovers and profiles all IoT/OT assets** to provide deep asset visibility and enable robust segmentation and zero-trust policies.
- **Provides a risk score with risk-based mitigation recommendations** for each device, based on vulnerabilities detected as well as threat intelligence provided by Section 52, CyberX's team of security researchers.
- **Continuously monitors network traffic** and generates real-time alerts when devices exhibit suspicious or unauthorized behavior indicating compromise or misconfiguration.
- **Integrates out-of-the-box with IT security stacks via bi-directional APIs** — including with SIEM, SOAR, ticketing, CMDBs, firewalls, and NAC solutions — to rapidly operationalize OT security in your SOC.

## NTT's OT Security Practice

NTT has built a specialised practice to secure industrial networks and Building Management Systems (BMS). Our focus is to keep your OT networks running and keep threat actors out of your enterprise.

NTT has partnered with **CyberX** , a recognized leader in the space, to help you identify and mitigate cybersecurity risks.

## Proven Expertise in Large and Complex Environments

CyberX has been battle-tested across diverse industries and organizations. These include:

- **3 of the top 10 pharma firms**
- **3 of the top 10 US energy utilities**
- **One of the world's largest cloud providers**, where CyberX is securing BMS in data centers.
- **F500 Manufacturer.** Suffered intermittent downtime for 1.5 days. Using CyberX's investigation tools, the OT team immediately identified a misconfigured device that was flooding the network.
- **F500 Manufacturer**: CyberX found malware that caused a plant to ruin a batch. This was removed before it caused further damage.
- **Energy Utility**: Deployment timeframes were dictated by limited maintenance windows Deployed 25+ sites in 1 month.

**Automation & Integration**
Fundamental to ease of deployment is a high level of automation and integration with existing systems.

## IoT/OT Cybersecurity Approach


*NTT approach to IoT/OT Cybersecurity*

We understand that it is not easy to commit to deploying technology into your highly critical systems.

Our methodology is designed to break down milestones into smaller, manageable tasks. Each task is designed to provide assurance that our approach does not cause interruption to production.

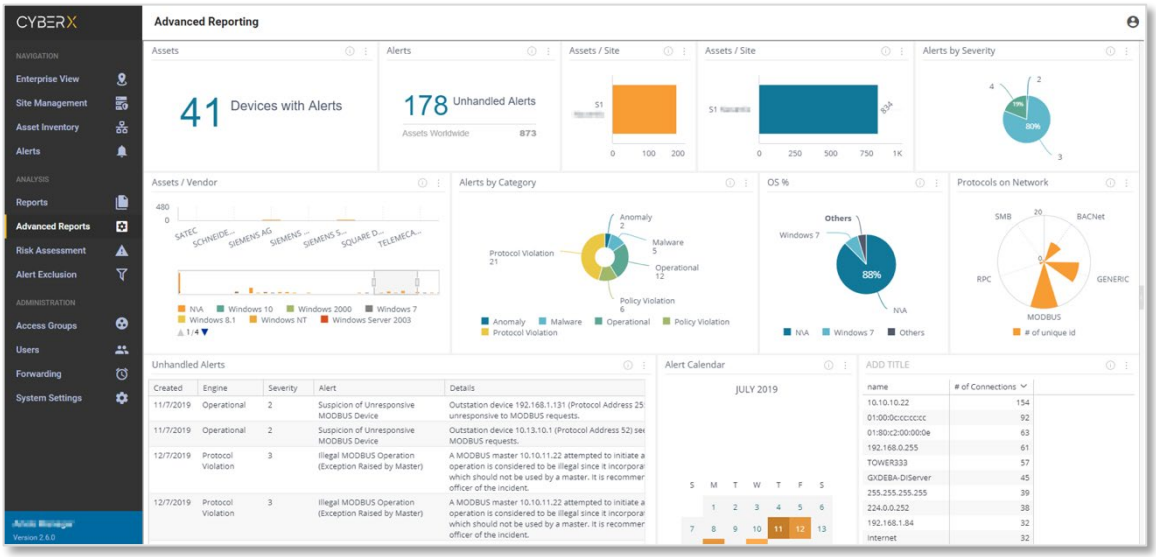
Our process allows you to:

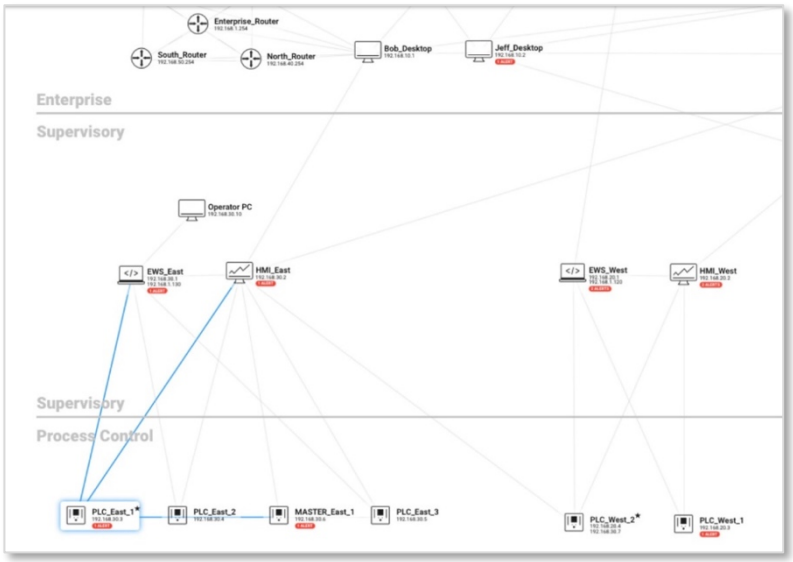
1. **Gain Visibility.** An initial workshop to identify the cyber risks and define a suitable pilot facility. We will use CyberX to perform Deep Packet Inspection (DPI) on live IoT/OT network traffic or via PCAPs.
2. **Understand Risks.** NTT and CyberX will nominate IoT/OT security experts to work with you to validate and discuss the risks found.

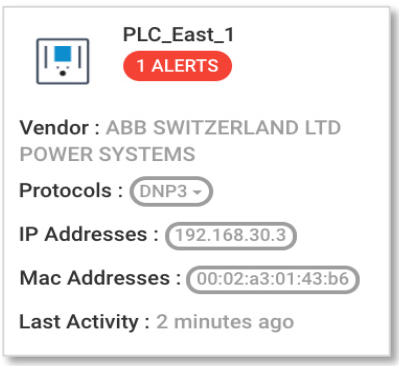
   This task typically takes at least 1 week. As a result, you will have a comprehensive view of your current IoT/OT risk posture and improvements required. These improvements are mapped to industry standards (e.g., IEC-62443, NIST, etc.) and our experience with your industry peers, and is customized to your organization's business plans.
3. **Deploy Architecture.** We will be deploying CyberX to continuously and passively monitor your IoT/OT network. This includes integrating with your existing SOC tools and workflows, and integrating with protective controls like NGFWs or Data Diodes. This phase will require minimal involvement from your personnel as deployment at each site is highly automated.

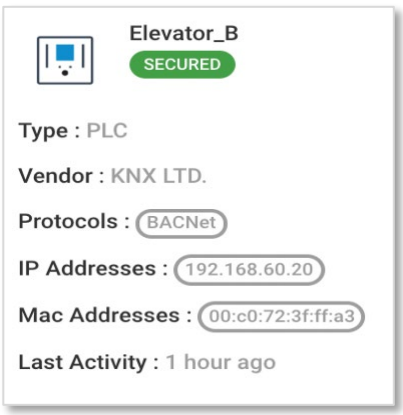
To minimize disruption, we will deploy CyberX to other facilities in stages.

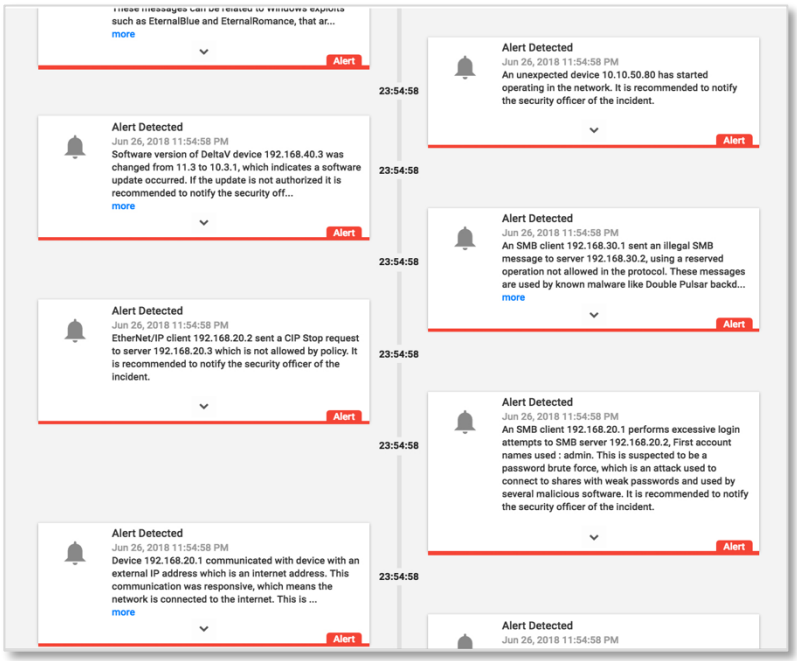
## The CyberX Platform



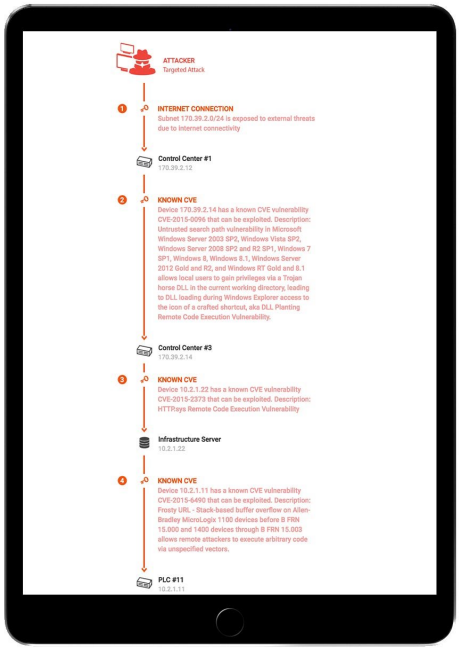

*CyberX Screenshots (clockwise from top): customizable Advanced Reporting Dashboard; device details (protocols, IP, MAC, recent activity); Event Timeline showing all alerts for investigations and threat hunting; network map arranged using Purdue model and showing communication paths between devices.*

## Why NTT and CyberX

- **Ease of Deployment**: CyberX's agentless platform leverages automation to enable rapid deployment without requiring configuration of rules and signatures. Plus it integrates out-of-the-box with your existing security tools and workflows to enable rapid operationalization and time-to-value.
- **Patented IoT/ICS-Aware Behavioral Analytics**: CyberX rapidly spots baseline deviations by modeling IoT/ICS networks as deterministic sequences of states and transitions. Compared to traditional baselining algorithms that were designed for IT networks — where the behavior is primarily non-deterministic — this approach enables faster detection of threats, with fewer false positives and a faster learning period. As a result, defenders can quickly detect attacks in the early stages of the kill chain — before adversaries can disrupt production — by continuously monitoring for suspicious or unauthorized activities rather than static IoCs.
- **Mature & Scalable Platform**: The CyberX platform has continuously evolved based on our experience in large, heterogeneous, and globally-distributed environments. This has contributed to its scalability and manageability. For example, the Central Manager supports hierarchical views at multiple levels including global, by geography, and by business unit. Additionally, the system supports a "Smart Sensor" architecture enabling local real-time analysis and display of security information even when disconnected from the Central Manager (for example, in case of a fast-spreading virus).
- **Deep Expertise**: NTT brings deep experience managing security as a trusted MSSP for enterprise organizations worldwide. NTT has invested in training OT security specialists and provides a converged service enabling enterprises to deliver unified security monitoring and governance across both IT and OT environments.

NTT believes you can benefit more because of the following unique capabilities provided by CyberX:

## Automated IoT/OT Threat Modeling




CyberX's automated IoT/OT threat modeling predicts the most likely paths of targeted IoT/OT attacks on your "crown jewel" assets, based on the network topology and vulnerabilities identified by CyberX.

This is key to a risk-based approach enabling more effective use of limited people resources and narrow maintenance windows.

Security teams can also simulate what-if mitigation actions to continuously adjust their security posture, such as "If I isolate or patch this insecure device, does it eliminate the risk to my most critical assets?"

## Open SDK for Proprietary Protocols

Unique in the industry, CyberX's Horizon Open Development Environment and SDK enable customers and partners to develop, test, and deploy custom protocol dissectors for the CyberX platform, without divulging proprietary information about how the protocols are designed or sharing network packet captures (PCAPs) that may contain sensitive information.

## IoT/OT Malware Sandbox

Detect IoT/OT-specific malware by simulating an IoT/OT environment. IT sandboxes typically can't identify IoT/OT-specific malware because they can't simulate IoT/OT assets, specialized protocols, services, and behaviors.

## Optional Cloud-Based Service for IoT Security

Integrates with cloud-based IoT platforms such as Microsoft Azure Security for IoT. Ensures your CyberX investment is future proof when you start managing IoT devices in the cloud. (Note: CyberX's OT platform and sensors are 100% on-premises.)

## Integration with Preventive Security Controls

- **NextGen Firewall (NGFW).** Integration enables NGFWs to automatically block sources of malicious traffic identified by the CyberX platform. Device profiles can also be imported from CyberX to eliminate manual efforts and quickly define segmentation and zero-trust policies without risking impact to business-critical processes.
- **Network Access Control (NAC).** NAC can automatically isolate device that is behaving abnormally.
- **Privileged Access Management (PAM).** CyberX integrates with leading PAM systems to automatically identify unauthorized remote access to your IoT/OT networks.

## IoT/OT-Specific Threat Intelligence

CyberX's Section 52 threat intelligence team is composed of world-class domain experts and data scientists who previously staffed a national CERT defending against daily nation-state cyberattacks.

They bring that expertise to CyberX by tracking IoT/ICS-specific zero-days and CVEs as well as malicious DNS addresses, campaigns, malware, and adversaries.

The team has already submitted more than a dozen zero-day vulnerabilities to the US ICS-CERT, including previously unknown vulnerabilities for devices manufactured by Rockwell Automation, Schneider-Electric, GE, Siemens, CODESYS, AVEVA, and others.

Section 52 has also developed an automated threat extraction platform that uses machine learning to identify malware and APT campaigns targeting industrial and critical infrastructure organizations. Named Ganymede, the platform continuously ingests massive amounts of data from a range of open and closed sources to deliver the most robust, data-driven analysis possible.

## Optional Selecting Probing

Uses safe "active scanning" commands defined by OT manufacturers to provide more granular asset information. Typically executed on a periodic basis, this capability can also be used to identify devices in highly-segmented networks.

## NTT for OT Cybersecurity

We understand that planning, implementing, and managing OT cybersecurity can be difficult. To assist you, we have invested in experts and skills to help you navigate this journey.

Our capabilities include:

- IT/OT Convergence Workshop
- OT Cybersecurity Assessment (business, technical, and based on industry standards like IEC62443 and NIST CSF)
- Solution evaluation, design and implementation
- 24x7 SOC-based proactive management of solution (e.g. managing policies, health monitoring, backup, implementing configuration changes, etc.)
- 24x7 SOC-based threat monitoring & incident response (e.g. to identify threats, and to contain the threat)
- IT/OT Converged Risk Management and Remediation

Benefits to you:

- **Zero-downtime approach** ensuring operations are unaffected while we strengthen your IoT/OT security.
- **Detailed listing of assets and their properties.**
- **Prioritization of risk and vulnerabilities** with an overall risk score that can be tracked over time.
- **Continuous IoT/OT threat monitoring and threat intelligence** to identify known malware as well as targeted attacks using zero-day and fileless malware.
- **Incident response & threat hunting tools** to rapidly identify root cause and how to remediate incidents.
- **Identification of operational issues** that can affect production such as malfunctioning or misconfigured equipment.
- **Integration with your existing workflows and tools** (Splunk, QRadar, ServiceNow, BeyondTrust, Fortinet, etc.).

### About Security and NTT Ltd.

Security is a division of NTT Ltd., a global technology services company bringing together the expertise of leaders in the field, including NTT Communications, Dimension Data, and NTT Security.

The Security's Centre of Excellent has invested in developing solutions to securing OT networks.

Today, we have dedicated OT specialist supporting all continents. We have also invested heavily in understanding challenges and building solutions. Our clients benefit by having a suitable solution, and one that can identify and respond to threats faster than the industry.

Security is also capable of managing & monitoring both IT and OT networks.

As a global ICT organisation, we employ more than 40,000 people in a diverse and dynamic workplace and deliver services in over 200 countries and regions. Together we enable the connected future. Visit us at our new website hello.global.ntt.

### About CyberX

Funded by Norwest Venture Partners, Qualcomm Ventures, and other leading venture firms, CyberX delivers the only cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure.

This difference is the foundation for the most widely deployed platform for continuously reducing IoT/OT risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies.

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 IoT/OT 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