As organizations connect massive numbers of unmanaged IoT/OT devices to their networks to optimize operations, boards and management teams are increasingly concerned about the expanding attack surface and corporate liability they represent.

Purpose-built for IoT/OT environments, CyberX’s agentless security platform delivers continuous visibility into all your IoT/OT assets, risks and vulnerabilities, and any anomalous or unauthorized behavior. To rapidly operationalize alerts from the CyberX platform in the SOC and support unified security monitoring and governance across IT, IoT, and OT, the platform integrates out-of-the-box with existing IT security stacks (SIEMs, SOAR, CMDBs, firewalls, NAC, etc.)

In these large and complex environments, it becomes increasingly challenging for security teams to gain a meaningful understanding of their overall IoT/OT risk posture. As an add-on module for the CyberX platform, the CyberX Advanced Reporting Dashboard offers a central reporting and workflow hub for your IoT/OT networks. Flexible, easy to understand, and completely customizable, it integrates with a broad range of enterprise data sources — such as Splunk, Rapid7, and ServiceNow, as well as standard databases, data warehouses, and via REST APIs — to give you the answers that are most important to your organization.

The CyberX Advanced Reporting Dashboard provides a visual overview of IoT/OT networks. Here, see alerts by category & location, asset analytics, & integration with warranty information to track upcoming expirations.

EXAMPLE USE CASES INCLUDE:
• See locations and asset owners for all assets with a particular CVE.
• See all of your facilities on a world map, with a specific malware alert.
• Find all alerts for a particular manufacturer or device type.
• Automatically generate recurring reports for management or stakeholders.
• Track risk mitigation progress over time.

Answer the questions that are most important to your organization and make data-driven decisions faster with a customizable view into your IoT/OT security and compliance landscape.
Flexible, Visual Dashboards and Analytics

UNDERSTAND YOUR IOT/OT SECURITY AND COMPLIANCE LANDSCAPE IN SECONDS.

You can’t improve what you can’t measure. The Advanced Reporting Dashboard is tailored for displaying rich information, discovering underlying trends, and answering specific questions at a glance. The dashboard consists of flexible, customizable modules that you can use to track your Key Performance Indicators, Key Risk Indicators, organizational metrics, or other important data points. Not only are you able to aggregate this data to suit your needs, you can also easily track it over time. What’s more, the Advanced Reporting Dashboard makes it easy to drill down into any of these data panels with just a click.

Dashboard view depicting KRIs such as alerts by device, severity, and protocol, as well as how those data points trend over time to measure improvement.

This dashboard has also integrated CVE and admin directory information for easy CVE management. Search for CVEs by device, ID, description, or admin name. Quickly drill down to generate a report of CVEs that a specific administrator is responsible for (below).

The above dashboard is just one example of the many ways that organizations use the Advanced Reporting Dashboard. The Dashboard is completely customizable, and can be built to support every organization’s individual needs, KPIs, and ongoing governance requirements. Below are two more examples of how organizations can use these visualizations to get a full view across their environments.

Dashboard view depicting unhandled alerts by device, category, and severity, as well as assets by vendor, OS, and number of connections.

Dashboard view depicting KPIs for an OT environment, including alert severity, alerts per OT protocol, alerts by OT vendor, devices per OT protocol, and devices by OT vendor/sensor correlation.
Custom Alerting, Reporting, & Workflows

KEEP YOUR FINGER ON THE PULSE.

The Advanced Reporting Dashboard also offers advanced reporting and alerting capabilities to go hand-in-hand with its visualization tools. Dashboard widgets can be easily converted to an alerting threshold, so your team can be instantly notified of certain risk indicators -- for example, as shown to the right, if your environment exceeds a certain number of high-severity alerts.

In addition, all of these dashboards can be easily exported into PDF format, or scheduled to be sent as recurring emails. This is ideal for regular reporting to management.

Integration with Enterprise Data Sources

INTEGRATE WITH THE DATA SOURCES THAT MATTER MOST TO YOU.

While CyberX alone provides a wealth of visibility into risk for your IoT/OT networks, we understand that no technology stands in a vacuum. Often, security teams need to step back and combine data from multiple sources to see the big picture. The Advanced Reporting Dashboard provides that ability.

A wide variety of file types and data sources (even cumbersome legacy applications) can be imported with just a few clicks. The Advanced Reporting Dashboard’s built-in connectors support dozens of data sources, including CSV, MySQL, Access, REST APIs, and many more. These data sources can be imported manually, or can be directly integrated via a live connection.

The Power of Visual Analytics in Action

REAL WORLD USE CASES.

Organizations can leverage the Advanced Reporting Dashboard to suit their individual needs in a variety of different ways:

• **CVE Reporting:** The Advanced Reporting Dashboard’s reporting capabilities allow for the immediate identification of devices affected by certain CVEs. Quickly identify which CVEs are associated with particular assets and how many devices are affected by the vulnerability. As upper levels of leadership are now accountable for IoT and OT security, security teams need to be able to quickly produce answers to board-level questions. For example, if a CSO asks how many assets are susceptible to a specific CVE, the Advanced Reporting Dashboard allows you to can answer question in seconds simply by sorting assets by CVE exposure.

• **Cross-Site IoT/OT Dashboards:** Global enterprises with multiple sites require advanced analytics that go beyond rule-based approaches, as well as the ability to analyze large amounts of both current and historical data collected from the CyberX platform across all locations. By integrating with the CyberX Central Manager, the Advanced Reporting Dashboard enables security teams to review actionable information on a global basis -- enabling them to make data-driven decisions based on business impact.
• **Scheduled Monthly KPI Reports:** Developing a proactive approach to cybersecurity means demonstrating the value of security in terms that all levels of leadership can understand. The Advanced Reporting Dashboard can demonstrate this value with tailored monthly reports, including examples like:
  - Metrics and Key Risk Indicators (KRIs) that demonstrate the protection of key areas and crown jewel assets.
  - Prioritized risk reports presented in a consistent format for the C-suite.
  - Remediation reports to prioritize and implement fixes based on risk.

• **Track & Measure Improvement:** Measure the overall improvement and effectiveness of your IoT/OT security posture by tracking vulnerabilities or alerts over time. For example, the Advanced Reporting Dashboard can show you the total number of high-severity alerts in your environment month-over-month, allowing you to measure improvement in overall risk.

• **Network Segmentation Workflows:** The Advanced reporting Dashboard gives you a visual overview of your IoT assets and how they communicate, making it a useful tool in network segmentation projects. For example, an organization may want to segment a network that contains both IoT traffic as well as corporate IT traffic. Using the Dashboard, they can identify all asset types (IT, IoT, OT, etc.), which networks/VLAN these assets are on, and how they’re communicating with each other. This workflow is key to network segmentation projects because it provides valuable insight into how devices would be most easily segmented, and informs which security policies should be put in place prior to segmentation to ensure that no applications break.

• **Track Alert Geolocation:** Displaying alert categories by geolocation allows security analysts to track if a virus is spreading across multiple global sites. Malware such as WannaCry has been known to spread from site to site globally within minutes. Seeing alerts by location enables analysts to react fast and quarantine prior to infection.

---

**Insights for a Stronger IoT/OT Security Approach**

**GET THE DASHBOARDS, ANALYTICS, AND WORKFLOWS YOU NEED FOR A MORE SECURE IOT/OT ENVIRONMENT.**

The complex nature of the IoT/OT environments of global corporations means that it’s impossible to make data-driven decisions without a complete picture of your IoT/OT risk posture. The Advanced Reporting Dashboard gives you the visual insights you need to understand your IoT/OT networks at a glance -- enabling you to more effectively manage your IoT/OT assets, proactively address vulnerabilities, detect and respond to threats, and maintain a unified security approach across IoT/OT environments that is fully integrated into your security stack.
We know what it takes.

CyberX delivers the only cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies.

CyberX delivers the only IoT/OT 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 IoT/OT security company to have been awarded a patent for its M2M-aware threat analytics and machine learning technology.

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 and 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.