HOW CYBERX SUPPORTS CMMC COMPLIANCE

DoD supply chain contractors must meet the standards of the Cybersecurity Maturity Model Certification (CMMC). As the simplest and most robust IoT/OT cybersecurity platform, CyberX provides key benefits in multiple crucial domains of the CMMC model.

CyberX supports multiple CMMC domains, including:

- **Access Control** - Identify unauthorized devices and abnormal connections to IoT/OT devices.
- **Asset Management** - Identify IoT/OT devices & their properties.
- **Audit & Accountability** - Collect audit trails and generate reports.
- **Configuration Management** - Make configuration decisions with full IoT/OT device visibility.
- **Incident Response** - Detect and investigate threats with M2M-aware behavioral analytics & threat intelligence.
- **Security Assessment** - Create automated reports to assess risk & track improvement.
- **Situational Awareness** - Get real-time views of your IoT/OT security posture.
- **System & Communications Protection** - Understand asset communications & accelerate network segmentation and zero-trust initiatives.
- **System & Information Integrity** - Detect IoT/OT threats faster and with fewer false positives, leveraging the industry’s only patented M2M-aware behavioral analytics.

CyberX supports 10 of the CMMC domains.

Overview

The Cybersecurity Maturity Model Classification, or CMMC, is a maturity model certification released by the Department of Defense (DoD) that dictates the handling of Controlled Unclassified Information (CUI).

The overall objective of the CMMC is to ensure commercial companies in the DoD supply chain are adhering to acceptable cybersecurity standards, such as those outlined by NIST 800-53, NIST 800-82, and NIST 800-171. All contractors that operate within the DoD supply chain, no matter the vertical, must have their CMMC maturity level evaluated and assigned by a third-party assessor.
The CMMC establishes five tiered certification levels that reflect an organization’s maturity in cybersecurity processes and practices, evaluated across 17 domains.

CyberX’s agentless IoT/OT security platform is easy to deploy and delivers insights within minutes of being connected to the network — providing immediate value to organizations that need to meet the CMMC standard. Purpose-built for IoT/OT security, the CyberX platform provides broad capabilities for addressing IoT/OT security across multiple CMMC domains, including:

- Asset management.
- Proactive risk and vulnerability management.
- Continuous threat detection and incident response.
- API-level integrations with existing IT security stacks (SIEMs, SOAR, firewalls, NAC, etc.) for unified security monitoring and governance across IT/IoT/OT networks.

This document provides an overview of how CyberX contributes to these CMMC domains, annotated with specific examples of the practices within them.

CyberX and the CMMC Domains, Processes, and Practices

The CMMC defines many practices across seventeen domains. These domains encompass a wide variety of security areas, ranging from physical security to maintenance to incident response. Each of these domains includes a number of practices that correspond to different maturity levels. More detailed information about the CMMC model can be found at [https://acq.osd.mil/cmmc](https://acq.osd.mil/cmmc), or you can download the PDF of the full model, which documents all domains and practices, by clicking here.

CyberX supports practices defined under ten of the CMMC domains. These domains, and how CyberX addresses them, are described below. Included in these descriptions are specific examples of CMMC practices within those domains, which are referenced by practice number. The footnotes include the full text of that particular practice from the CMMC model.

**ACCESS CONTROL (AC)**

CyberX monitors all communications with IoT/OT devices, which allows administrators to identify and verify any abnormal, suspicious, or unexpected connections (as specified in practice AC.1.003). This visibility also allows you to quickly mitigate risk associated with unauthorized devices, unidentified connections, or wireless access points (as specified in AC.5.024). Identifying communication paths and behaviors is also an ideal way to accelerate network segmentation and zero-trust strategies without disrupting operations.

CyberX also helps ensure and enforce secure remote access (as specified in practice AC.2.013). By integrating with leading privileged access management platforms such as CyberArk, CyberX ensures secure remote access by immediately alerting on unauthorized use of remote access credentials. In addition, continuous monitoring and tracking of resource use provide better details about remote worker activity — which is often a particularly difficult-to-mitigate blindspot. Furthermore, CyberX’s auditing and forensic tools allow for rapid and efficient investigations into any unauthorized remote access incidents.

1. Verify and control/limit connections to and use of external information systems.
2. Identify and mitigate risk associated with unidentified wireless access points connected to the network.
3. Monitor and control remote access sessions.
ASSET MANAGEMENT (AM)

CyberX automatically discovers all IoT/OT assets on your network and displays a continuously up-to-date network topology diagram depicting how those assets are connected. CyberX also auto-discovers detailed asset properties, such as device type, manufacturer, open ports, IP/MAC address, and more (as specified in practice AM.4.2266).

Traditional network scanners and endpoint security agents cannot be used with IoT/OT assets and thus are not able to provide this level of asset property detail. This information is not only key to protecting the IoT/OT attack surface, it also provides a greater capability for detailed audit and compliance reporting, regardless of the vertical.

AUDIT AND ACCOUNTABILITY (AU)

CyberX helps streamline auditing across industry compliance requirements (such as, for example, the NIST Cybersecurity Framework, NERC-CIP, or the EU’s NIS Directive) by addressing key IoT/OT compliance requirements, delivering an objective risk score, and documenting compliance.

CyberX records actionable information to enable rapid incident response, forensics, and threat hunting (as specified in practice AU.2.0426). CyberX documents compliance via customizable reports that can be automatically distributed to stakeholders (supporting practices such as AU.3.0516 and AU.3.0527).

CyberX also provides threat monitoring and detection that alerts on tactics, techniques, and procedures (TTPs), as well as unauthorized or anomalous activities, as identified by our patented M2M-aware behavioral analytics (as specified in AU.4.0536).

CONFIGURATION MANAGEMENT (CM)

CyberX provides full visibility into the devices on your network and how they communicate. This allows you to establish a baseline inventory of your IoT and OT devices and their properties (as specified in practice CM.2.0619). This visibility into your IoT/OT environments also enables you to make informed decisions about how you configure those devices, and which ports and protocols are essential (as specified in practice CM.3.06810).

4 Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.
5 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
6 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
7 Provide audit record reduction and report generation to support on-demand analysis and reporting.
8 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.
9 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
10 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
11 Detect and report events.
12 Establish and maintain a security operations center capability that facilitates a 24/7 response capability.
CyberX also simplifies incident response, forensics, and threat hunting with a full audit trail of activity and GUI-based query tools that make it easy to analyze an event and determine the underlying cause (as specified in IR.2.094\(^{13}\) and IR.2.097\(^{14}\)). CyberX’s contextual alerts give analysts all of the information they need to quickly understand threats, including IP address, device types, granular descriptions of the threat, and mitigation recommendations. Analysts can drill directly down into PCAPs for deeper investigation.

CyberX integrates with leading firewalls, NAC, and SOAR systems to deliver automated responses to incidents (as referenced in IR.5.102\(^{15}\)) — such as immediately blocking or quarantining sources of malicious traffic identified by the CyberX platform.

CyberX also provides IoT/OT-specific incident response as a service, which includes case analysis, data preservation, network and host layer forensics, malware analysis, remediation, and the delivery of a comprehensive incident response report.

**RISK MANAGEMENT (RM)**

CyberX provides everything security teams need to assess vulnerabilities of IoT/OT networks and monitor risk on an ongoing basis. The CyberX Vulnerability Assessment report delivers an objective risk score, identifies device and network-layer vulnerabilities, and provides prioritized mitigation recommendations (as specified in RM.2.141\(^{16}\), RM.2.142\(^{17}\), and RM.3.144\(^{18}\)). These mitigations are prioritized by risk, making it easy to systematically address the vulnerabilities (as specified in RM.2.143\(^{19}\)) and develop data-driven plans for ongoing risk mitigation (as specified in RM.3.145\(^{20}\)).

In addition, CyberX’s automated IoT/OT threat modeling predicts and visualizes the most likely paths of targeted IoT/OT attacks – allowing you to test the effectiveness of your mitigation efforts and address anticipated risks based on current threat intelligence (as referenced in RM.5.155\(^{21}\)).

**SECURITY ASSESSMENT (CA)**

CyberX’s IoT/OT vulnerability reports identify and prioritize vulnerabilities in your IoT/OT network, helping security teams create plans of action to address them (as specified in CA.2.159\(^{22}\)) as well as strategize and track long-term improvement (as directed in CA.4.163\(^{23}\)).

**SITUATIONAL AWARENESS (SA)**

CyberX provides a continuous real-time view of your IoT/OT risk posture, including ongoing updates about new IoCs and TTPs identified by our threat intelligence team, Section 52 (contributing to practices such as SA.3.169\(^{24}\) and SA.4.173\(^{25}\)). Section 52 has developed an automated threat extraction platform, called Ganymede, that uses machine learning to...
identify malware and APT campaigns targeting industrial and critical infrastructure organizations. Ganymede continuously ingests massive amounts of data from a range of open and closed sources to deliver the most robust, data-driven analysis possible. Machine learning and statistical models are used to assign risk scores to specific entities such as files. The risk scores are calculated by machine learning trained on datasets consisting of hundreds of thousands of known good and bad samples. Section 52 threat analysts are used in the final phase to review and correlate the results based on their extensive field experience.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

CyberX contributes to overall system and communications protection by enabling organizations to understand how IoT/OT devices communicate and verify that they’re doing so as intended. CyberX accelerates zero-trust strategies and network segmentation (directed in SC.1.17526) by automatically discovering and profiling all assets, showing how they communicate, integrating with firewall platforms, and providing automated threat modeling to test the effectiveness of your segmentation zones. This degree of understanding of how IoT/OT devices communicate also helps you more effectively isolate high-value critical infrastructure devices and servers (directed in SC.4.22827) and implement more effective policies to permit only necessary communications traffic (SC.3.18328).

This monitoring encompasses all IoT devices, including VoIP technologies (specified in SC.3.18929).

Furthermore, CyberX records packets that are passed between IoT/OT devices and includes those packet capture files (PCAPs) in alerts (as referenced in SC.5.19826). CyberX also detects whether devices are not communicating as intended, such as through disallowed ports or protocols, or by violating protocol specifications as defined by equipment suppliers (as directed in SC.5.20826).

CyberX also offers our exclusive IoT/OT Malware Sandbox to analyze suspicious files that may be malware targeting IoT or OT devices (as referenced in SC.4.20226).

SYSTEM AND INFORMATION INTEGRITY (SI)

CyberX protects system and information integrity with ongoing threat monitoring across IoT/OT devices. With patented M2M-aware behavioral analytics, CyberX alerts on threats faster and with higher accuracy, enabling effective detection of potential threats (directed in SI.2.21623) and quick triaging of these alerts (directed in SI.2.21424).

Furthermore, CyberX’s analytics engines enable the detection of abnormal scripts that indicate malicious actions (specified in SI.5.22225) or anomalous device activity that falls outside of a particular device’s behavioral baseline (such as directed in SI.5.22326).

Conclusion

The benefits that CyberX gives DoD supply chain organizations go far beyond the specific examples mentioned above. The goal of the CMMC, above all, is to secure and strengthen the entire supply chain – and CyberX enables manufacturing organizations to accelerate digitization and Industry 4.0 initiatives without sacrificing security.

CyberX detects threats faster and with more accuracy, streamlines investigations and incident response, and produces detailed audit trails and customized reports to demonstrate compliance. All of these benefits are crucial not only to CMMC compliance, but also to organizational cybersecurity as a whole.

About CyberX

We know what it takes.

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. That 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.

For more information, visit CyberX.io or follow @CyberX_Labs.

---

26 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal this boundaries of the information systems.

27 Isolate administration of organizationally defined high-value critical network infrastructure components and servers.

28 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

29 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

30 Configure monitoring systems to record packets passing through the organization’s Internet network boundaries and other organizationally defined boundaries.

31 Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.

32 Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.

33 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

34 Monitor system security alerts and advisories and take action in response.

35 Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.

36 Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.