Cisco XDR and CMMC Compliance

Introduction

Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to ensure that contractors and subcontractors have adequate cybersecurity measures in place to protect sensitive information. CMMC applies to DoD contractors, who must achieve certification to be eligible for future government contracts. This requirement extends to higher education institutions that perform research under DoD contracts.

With the increasing emphasis on cybersecurity for organizations handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), meeting CMMC requirements has become crucial. Cisco® Extended Detection and Response (Cisco XDR) offers a security solution that enhances threat detection and response capabilities while aligning with the CMMC standards. By leveraging Cisco XDR, organizations can streamline their compliance efforts, ensuring robust protection against cyber threats while adhering to regulatory mandates.

Contents

The solution brief details the specific ways Cisco XDR supports each level of CMMC, mapping its features to the required practices and processes. It demonstrates how Cisco XDR's integration and automation capabilities can simplify the CMMC compliance journey, offering insights into its deployment and utilization in creating a CMMC-compliant secure environment.

> This guide serves as a strategic resource for organizations seeking to bolster their cybersecurity posture and achieve CMMC compliance with confidence.

Overview of CMMC

CMMC 2.0 is a framework designed to enhance the cybersecurity posture of organizations within the defense industrial base. It supersedes its previous version, CMMC 1.0, and further establishes a set of cybersecurity standards and practices that organizations must implement to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC 2.0 streamlines the original model by reducing the number of maturity levels from five to three and aligning more closely with existing cybersecurity standards, such as NIST SP 800-171. The three levels are:

CMMC 2.0 Level 1 (Foundational): Designed for contractors handling Federal Contract Information (FCI). This level focuses on basic cyber hygiene practices and includes 17 practices that align with the Federal Acquisition Regulation (FAR) 52.204-21.

These practices are fundamental and aim to protect FCI from unauthorized access and disclosure.

CMMC 2.0 Level 2 (Advanced): Intended for organizations handling Controlled Unclassified Information (CUI). This level requires compliance with the 110 security requirements outlined in NIST SP 800-171. Level 2 emphasizes safeguarding CUI by implementing a more comprehensive set of cybersecurity practices.

Contents

Organizations must demonstrate a more mature and proactive cybersecurity posture to protect sensitive information effectively.

CMMC 2.0 Level 3 (Expert): Reserved for organizations managing highly-sensitive information and facing advanced persistent threats. Level 3 builds on the practices in Level 2 and incorporates additional requirements from NIST SP 800-172.

This level focuses on advanced cybersecurity practices, such as enhanced monitoring and response strategies, to ensure robust protection against sophisticated cyber threats. Organizations at this level must exhibit the highest degree of cybersecurity maturity and capability.

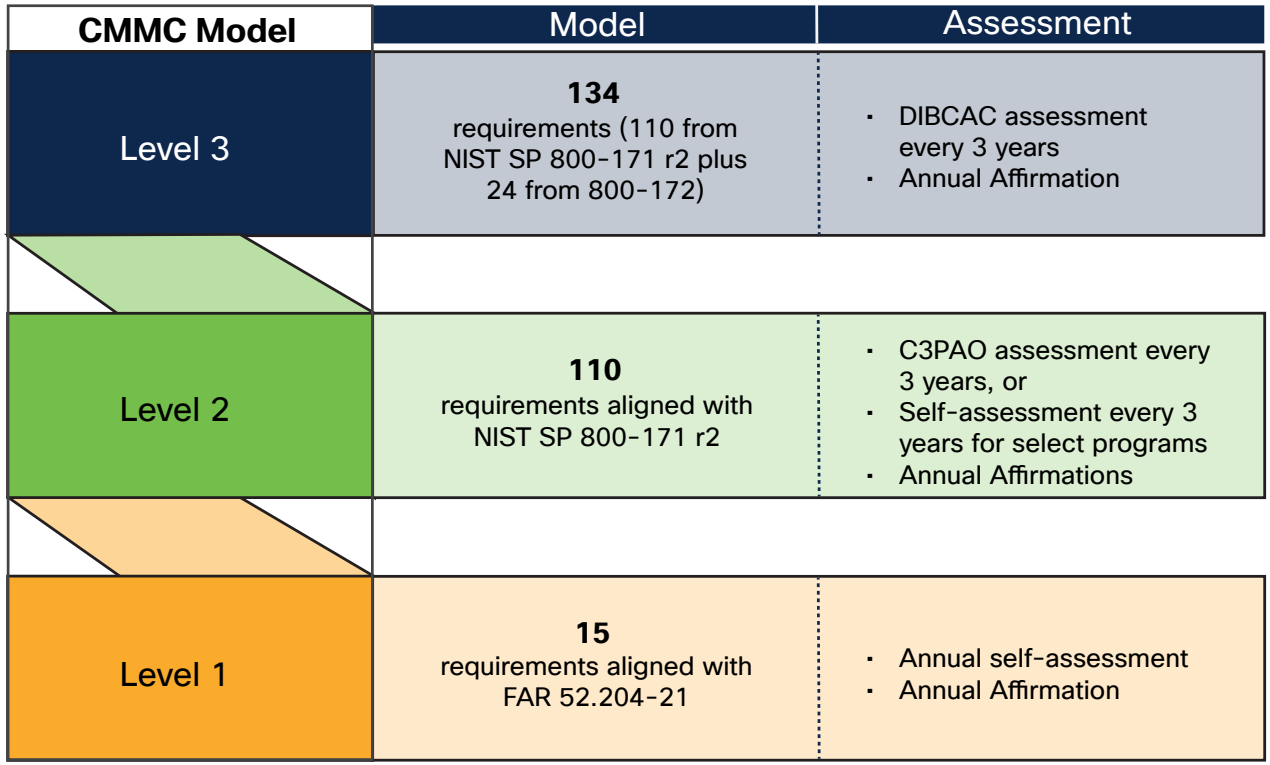

Figure 1. CMMC Model

Contents

The importance of CMMC lies in its role in safeguarding sensitive information that could impact national security if compromised. For organizations handling FCI and CUI, compliance with CMMC is crucial as it is often a prerequisite for obtaining and maintaining contracts with the Department of Defense. By adhering to these standards, organizations not only protect themselves from cyber threats but also contribute to the overall security of the defense supply chain.

Understanding Cisco XDR

What is Cisco XDR?

Cisco XDR is a cloud-native, extensible solution designed to help organizations achieve and maintain CMMC compliance by enhancing their cybersecurity posture, optimizing threat detection, and reducing operational complexity. By integrating advanced analytics and multi-source telemetry, Cisco XDR enables defense contractors and research institutions to protect FCI and CUI more effectively.

Cisco XDR simplifies security operations, accelerates incident response, and empowers Security Operations Center (SOC) teams with AI-driven and proactive threat detection and response. It combines threat intelligence from Cisco Talos with telemetry data from multiple security tools—including endpoint, network, firewall, email, identity, and DNS—and applies machine learning and analytics to provide correlated detections. This unified approach allows for comprehensive threat detection, reducing false positives and prioritizing incidents based on potential risk and impact. The solution's AI Assistant guides response actions, reduces human error, and makes remediation faster and more consistent, enhancing overall SOC efficiency.

Cisco XDR can be delivered on-premises or as a SaaS[1] offering and is typically deployed by organizations with smaller security teams.

Key features and capabilities include:

Threat Detection: Cisco XDR can detect sophisticated threats by connecting the Cisco security portfolio and select third-party tools, enriched with threat intelligence from Talos.

[1] Software as a service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet.

Contents

Prioritization and Response: Cisco XDR prioritizes threats that pose the greatest risk, streamlines investigations with unified context, and provides evidence-backed recommendations for faster action.

Productivity Enhancement: Cisco XDR filters out noise, allowing analysts to focus on critical threats, and also automates tasks and boosts resource efficiency.

Security Resilience: Cisco XDR helps close security gaps, anticipates future threats with actionable intelligence, and ensures continuous improvement.

Integration and Visibility: Cisco XDR offers seamless integration with existing security tools, providing unified visibility and deep context into advanced threats across network, cloud, endpoint, email, identity, and applications.

Automation and AI Assistance: Cisco XDR has built-in automation, orchestration, and customizable playbooks that help to automate repetitive tasks, while the Cisco AI Assistant guides response actions to reduce human error and enhance efficiency.

Flexible Licensing: Cisco XDR offers various licensing options, including Essentials, Advantage, and Premier, to cater to different business needs.

Key Benefits

Cisco XDR can deliver a unified and efficient approach to detecting and responding to threats. It is designed to deliver operational efficiencies with minimal customization.

Cisco XDR offers several key benefits that enhance threat detection, response capabilities, and integration features:

Improving Security Operations

- Improving alert fidelity by combining weak signals from multiple components into stronger signals by correlation into actionable incidents

Contents

- Reducing alert volume to confirmed incidents via automated correlation and confirmation
- Providing centralized configuration with weighted guidance to help prioritize configuration improvements
- Sharing threat intelligence immediately among subcomponents to provide efficient blocking of threats across all sensors and third-party integrations
- Utilizing vendor-provided content to deliver systemic detection content for common threat detection with little to no tuning required

Threat Detection

Cisco XDR provides advanced threat detection through AI-powered analytics, reducing false positives and prioritizing threats based on risk. It integrates data from multiple sources, including network, cloud, endpoint, email, identity, and applications, to offer a comprehensive view of potential threats.

Response Capabilities: The solution includes automated and guided response features, such as customizable orchestration playbooks and AI-driven guidance for identification, containment, eradication, and recovery. This helps reduce the Mean Time to Respond (MTTR) and enables consistent and effective decision-making.

Integration Features: Cisco XDR seamlessly integrates with a wide range of Cisco and third-party security tools, providing visibility across the entire IT infrastructure. It leverages threat intelligence from Cisco Talos and aligns with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework for enhanced threat detection and response strategies.

Improve Security Operations Staff Productivity

- Converting a large stream of alerts into a condensed number of enriched incidents that can be investigated efficiently

Contents

- Reducing training and skills needed to complete operational tasks by providing a common management, policy, and workflow experience across security products
- Providing incident response options that have necessary context from a range of security components to respond to incidents quickly
- Providing response options that go beyond infrastructure control points, including integrations with third-party products
- Providing an orchestration and automation capability for repetitive tasks

Benefiting CMMC

These key benefits assist in CMMC compliance by providing comprehensive threat detection and response capabilities, ensuring that organizations can effectively manage and mitigate cybersecurity risks. The integration of various security tools and the alignment with industry frameworks such as MITRE ATT&CK help organizations maintain a robust security posture, which is essential for meeting CMMC requirements.

Mapping Cisco XDR to CMMC Requirements

The CMMC Framework consists of 14 cybersecurity domains. A domain is a distinct set or group of security practices (controls) which have similar attributes to each other. These domains are core to the success of the protection of both FCI and CUI. The following table details the security domains for safeguarding FCI and CUI within the CMMC Framework. A description of the 14 CMMC cybersecurity domains is detailed below.

Contents

Key:
Green = Yes
Yellow = Partial
* = Additional Note

Table 1. xxxxxxxxx

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Access Control (AC)	The principles of access control are applied to both physical and logical assets. Physical assets include buildings, fences, gates, and doors. Logical access principles are applied to IT assets like servers, laptops, PCs, network communication devices, logic controllers, operating systems, applications, and databases. Core principles of access control are **least privilege** and **zero trust**, allowing access only to assets based upon appropriate, authorized, and regular assessment, using **Role-Based Access Control** (RBAC) principles.	**Level 1** *AC.L1-b.1.i *AC.L1-b.1.ii *AC.L1-b.1.iii **Level 2** *AC.L2-3.1.1 *AC.L2-3.1.2 AC.L2-3.1.3 AC.L2-3.1.6 AC.L2-3.1.8 AC.L2-3.1.10 AC.L2-3.1.13 AC.L2-3.1.14 AC.L2-3.1.15 AC.L2-3.1.16 AC.L2-3.1.17 AC.L2-3.1.19 AC.L2-3.1.20 AC.L2-3.1.22 **Level 3** AC.L3-3.1.3e

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Awareness and Training (AT)	Cyber is a mission, not a technology risk, and everyone in an organization has a part to play in protecting the assets and securing the mission of the enterprise.	**Level 2** **Level 3**
Audit and Accountability (AU)	Audit logging is an important requirement for system governance. It provides the evidence of transaction activity, of what users do, on what system, and when. It logs system transactions including systems access, files transfers, and communication records and retains these over time. Logging is important during digital forensic investigations, including those during and following a cyberattack.	**Level 2** AU.L2-3.3.1 AU.L2-3.3.2 AU.L2-3.3.3 AU.L2-3.3.4 AU.L2-3.3.5 AU.L2-3.3.6 AU.L2-3.3.7 AU.L2-3.3.8 AU.L2-3.3.9
Configuration Management (CM)	It is important to standardize the configuration of technology across the organization. This reduces operating costs, simplifies maintenance, and improves security.	**Level 2** CM.L2-3.4.1 CM.L2-3.4.2 CM.L2-3.4.3 CM.L2-3.4.6 CM.L2-3.4.7 CM.L2-3.4.8 CM.L2-3.4.9 **Level 3**

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Identification and Authentication (IA)	Identification is the ability to identify uniquely a user of a system or an application. Authentication is then the ability to prove and verify that the user or application is genuinely who that user or what that application claims to be.	**Level 1** *IA.L1- b.1.v **Level 2** *IA.L2-3.5.1 IA.L2-3.5.5 IA.L2-3.5.7 IA.L2-3.5.8 IA.L2-3.5.9 IA.L2-3.5.10 IA.L2-3.5.11 **Level 3** IA.L3-3.5.1.e
Incident Response (IR)	An Incident Response (IR) plan establishes a clear set of actions to detect, respond to, and recover from an attack. The IR plan can be used to address issues such as cybercrime, data loss, and service outages that threaten operations. The IR plan should be tested frequently to confirm that it is effective and to successfully address the range of possible threats an organization faces.	**Level 2** IR.L2-3.6.1 IR.L2-3.6.2 IR.L2-3.6.3 **Level 3** *IR.L3-6.1.e IR.L3-3.6.2e

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Maintenance (MA)	Regular systems maintenance ensures the smooth running of operations and reduces the risk of breakdown. Maintenance procedures that address system speed and performance can help identify inappropriate processes running on devices, and unpatched software and programs that make devices unstable and more likely to fail, causing disruption to operations. System maintenance identifies vulnerabilities with operating systems, hardware and software which if left unresolved can result in systems being compromised by hackers through recognized vulnerabilities.	**Level 2**
Media Protection (MP)	Without data and information organizations would not be able to operate. Data forms important IP for an organization. If the data is Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), then it must be identified, marked appropriately, and secured throughout the life cycle of its use in whatever form it takes, logical or physical.	**Level 1** **Level 2**

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Personnel Security (PS)	People are an organization's most important assets and pose one of the largest risks to the security of data and information. Sixty percent of data breaches occur from insider threats. Employee screening is an essential activity; it can be used to clarify a person's skills and experience, to confirm the presence of a criminal record, to evaluate reputation, and to confirm legal compliance. It is important therefore that organizations ensure that their staff have been screened appropriately, if they are to encounter sensitive data such as FCI or CUI.	**Level 2** **Level 3**
Physical Protection (PE)	Physical and logical protection are inextricably linked. Without physical protection it is it not possible to protect assets including computers, laptops, and servers that hold the company's IP. If an unauthorized person can damage, destroy, or steal assets, all the firewalls, intrusion detector systems, cryptography, and other security measures will not stop them from getting access to the organization's IP. Therefore it is critical that physical security measures are applied to prevent unauthorized users from gaining access to areas within an organization they are not authorized to access.	**Level 1** **Level 2**

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
Risk Assessment (RA)	Cyberattacks can impact any part of an organization from the board room to the shop floor and extend through the organization's supply chain. Attacks can be targeted or general and can range in impact from minor disruption with no data theft to ransomware attacks that can bankrupt an organization and lead to the theft of its most critical IP. With such a range of possible threats and outcomes, it is important that an organization identifies and manages those risks that it believes are the most significant.	**Level 2** *RA.L2-3.11.1 **Level 3** RA.L3-3.11.1e *RA-L3-3.11.2e RA-L3-3.11.3e *RA-L3-3.11.5e
Security Assessment (SA)	Security assessment is an evaluation of the security posture of the organization based upon its ability to manage its cyber risk profile. The SA identifies an organization's inherent risks, assessing the effectiveness of its controls environment and evaluating its residual risk profile. It is an exercise that continually evolves and improves based upon the changing business environment. An SA can be managed through the creation, adoption, and management of a Systems Security Plan (SSP).	**Level 2** *CA.L2-3.12.1 *CA.L2-3.12.2 *CA.L2-3.12.3 *CA.L2-3.12.4 **Level 3** * CA.L3-3.12.1e

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
System Communications Protection (SC)	Organizations use a wide variety of technology devices to conduct their business operations. These devices are connected to form an ecosystem for the creation, transmission, consumption, and servicing of data, which is unique to an organization's business operations. All these devices, networks, communications, and data need to be secured. An organization must have a clear view of its perimeter, including technology, processes, people, and data. Mature security solutions require having appropriate designs in place to leverage all the security solutions available to provide an adequate level of security. These solutions must include network security, access management, data loss prevention, code security, encryption, and sandboxing among other practices.	**Level 1** **Level 2** SC.L2-3.13.3 SC.L2-3.13.4 SC.L2-3.13.6 SC.L2-3.13.9 SC.L2-3.13.15 **Level 3**

Contents

CMMC V2.13 Domain	Description	XDR CMMC V2.13 Capability
System Information Integrity (SI)	Information integrity is a critical requirement to maintain the confidentiality, integrity, and availability of FCI and CUI, which is the primary goal of information security and cyber risk management. System information integrity requires the adoption of a broad range of security practices including the remediation of known software flaws (security by design, vulnerability scanning, and patch management); the identification and management of malicious software (Anti-Virus); Spam protection (the identification and removal of known sources of Spam at all entry points); systems monitoring (the identification and alert of changes in systems security); the oversight of security alerts, advisories, and directives (the assessment of security threats); and information output handling and retention (information is handled in line with federal laws).	**Level 1** **Level 2** SI.L2-3.14.3 SI.L2-3.14.6 **Level 3** SO.L3-3.14.6e

Contents

Case Studies

Customer Story: Unified Security Platform Improves Network Uptime

While understanding the benefits of Cisco XDR is valuable, nothing speaks louder than real-world results. Let's explore how one higher education institution leveraged Cisco XDR to gain a comprehensive view of incidents to minimize network downtime and data loss through a unified platform.

Safeguarding digital campus learning

Elon University, a nationally recognized leader in hands-on education, serves approximately 7,000 students and 3,000 staff and faculty across 200 buildings. Robert Readling, Enterprise Network Architect, describes the campus as "akin to a small city."

"Our real challenge is securing the digital footprint of our students," says Readling. Students typically connect 5 to 10 unmanaged devices to the wireless network daily, including in dorm rooms. This creates security uncertainties, requiring constant vigilance. Readling emphasizes, "Network uptime is our top Key Performance Indicator (KPI). We regularly evaluate if there has been any downtime or loss of data."

Integrating seamless protection

Elon University employs a comprehensive suite of Cisco security products to protect its campus. Challenged by correlating security data across multiple screens, the transition to Cisco XDR significantly advanced their approach.

Cisco XDR provides Elon's security team with a comprehensive view of attacks along with deeper insights and visibility into the network via integrations across the Cisco security products and third-party tools.

"I love the fact that all of my Cisco security products are integrated into XDR. And the dashboard lets me scroll down and see just about anything I need to see," says Readling.

Contents

Cisco XDR's AI-driven engines correlate telemetry data, improving efficiency. Readling notes, "Before Cisco XDR, we were busy combing logs. XDR gathers all that information in a human-readable format, making the process more efficient."

Improved operational efficiency

Cisco XDR streamlined Elon University's security operations, simplifying secure client package deployment across thousands of endpoints. This process is crucial during the busy start of the school year, enhancing endpoint security with minimal manual intervention.

Cisco XDR playbooks automate threat investigations by establishing rules that reduce detection-to-response times. "Cisco XDR correlates all the data, giving me a comprehensive view of incidents," Readling adds. "I can stop any threat with just a few clicks."

Cisco XDR enhances threat response by allowing security teams to act quickly. Analysts can now enforce policies immediately upon detecting malware, eliminating the need to sift through data during an ongoing threat, which significantly improves overall security efficiency.

Support and Resources

Explore Cisco Security Services

Cisco XDR Premier At-a-Glance (PDF)

Cisco XDR At-a-Glance (PDF)

Cisco XDR Data Sheet (PDF)

Cisco XDR Demo

Contents

Conclusion

Cisco XDR offers a powerful solution for organizations seeking to achieve and maintain CMMC compliance. By providing threat detection, automated response capabilities, and integration with existing security tools, Cisco XDR helps address multiple CMMC requirements. Its ability to enhance visibility, streamline security operations, and provide advanced analytics aligns closely with CMMC's focus on protecting sensitive information and improving the overall cybersecurity posture.

Cisco XDR not only helps organizations meet CMMC standards but also strengthens their overall security infrastructure. With its AI-driven approach and extensive integrations, Cisco XDR positions organizations to confidently navigate the complexities of CMMC compliance while improving the ability to detect, respond, and mitigate cyber threats.

Learn more

Take the first step towards CMMC compliance. Explore Cisco XDR and learn more about CMMC requirements:

Explore Cisco XDR

Learn more about CMMC

C07-4939003-00 02/25