VECTRA
SECURITY THAT THINKS.®

CMMC BRIEF

# Meeting the challenges of the Cybersecurity Maturity Model Certification (CMMC v2) with Vectra®

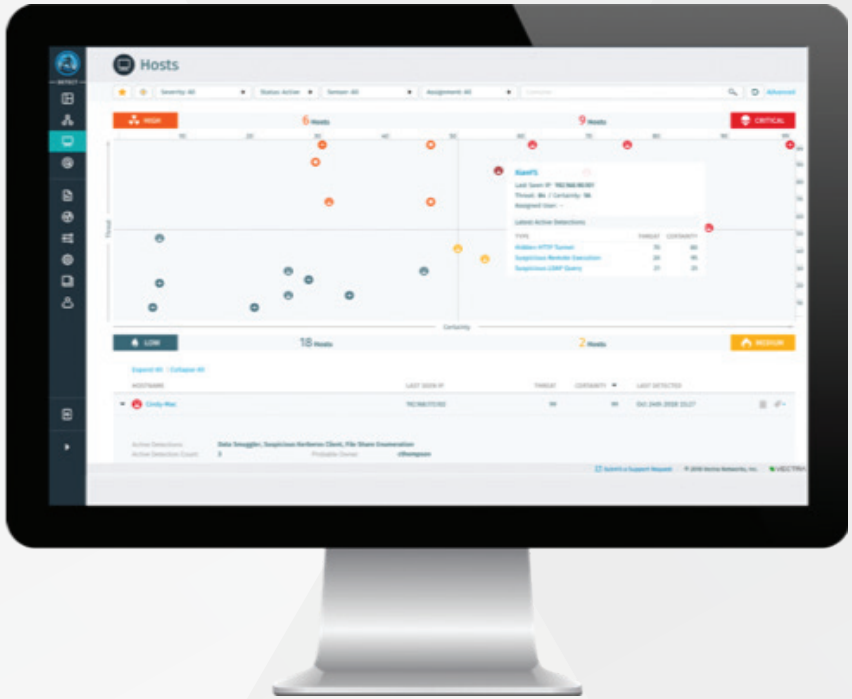
To meet the protections of Controlled Unclassified Information (CUI) and Covered Defense Information (CDI), federal contractors of all categories are now required to meet CMMC in order to participate in new contract pursuits, extensions, or modifications.

The CMMC 2.0, set to take effect in December 2021, is a combination of various best practices and cybersecurity standards and represents a continued evolution of the current DFARS 252.204-2012. CMMC adds in verification as a requirement with various levels available.

However, most organizations will be required to self-certify at Level 1 and obtain additional certification for Level 2 or Level 3, depending on the contract requirements.

As policies, standards and best practices continue to evolve, this mapping should be used only as a guide on how to automate NDR across enterprise networks at any classification level. Because the Vectra Threat Detection and Response platform supports all workloads – from the cloud to the data center, and traditional IT assets to IoT/OT industrial controls and sensors – the applicability and value benefits of continuous monitoring and real-time alerting can assist in many certification challenges while reducing the overall security operations center (SOC) and security analyst workloads.

The following section highlights the key requirements of the CMMC with details that explain how the Vectra Threat Detection and Response platform fulfills the category. Using patented machine learning (ML) and artificial intelligence (AI) allows weeks or months of workloads and analysis to be automated into minutes. For more information, contact your Vectra federal team today and request a solution brief.




To support the federal community, Vectra has provided this high-level guide that maps the various requirements to the Vectra Threat Detection and Response platform. This allows mapping of the CMMC to the DFARS (NIST 800-171 and NIST 800-172) and traditional NIST 800-53 controls.

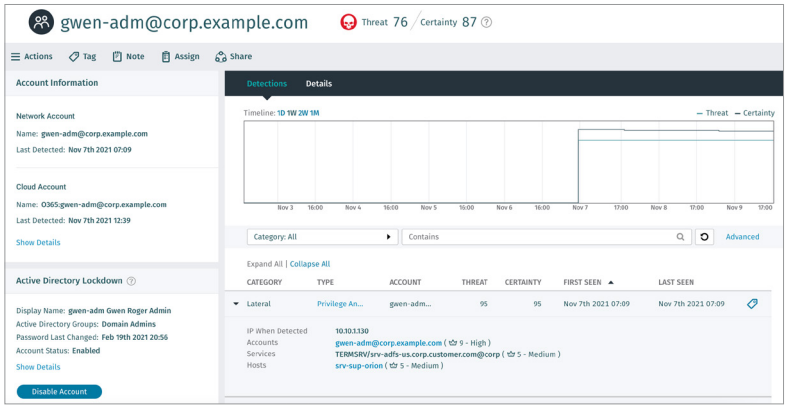
## Domain: Access Control (AC)

**AC.L2-3.1.5** *Least Privilege* (CMMC 2 – 3): Employ the principle of least privilege, including for specific security functions and privileged accounts. (800-53: AC-6, AC-6(1), AC-6(5))

Vectra Detect™, which runs on the Vectra Threat Detection and Response platform, monitors privileged access for anomalies, which in turn can identify users who are conducting privileged activities. These detections occur within on-premise deployments, Azure, AWS and Microsoft 365 environments in both Commercial and Government tenants. Most organizations lack any ability to validate or track changes in a user or hosts access once privilege has been granted and look for anomalous behaviors indicative of attackers executing Command and Control, mass file exfil, ransomware or other activities.

**AC.L2-3.1.6** *Non-Privileged Account Use* (CMMC 2 – 3): Use non-privileged accounts or roles when accessing nonsecurity functions. (800-53: AC-6(2))

Vectra Detect monitors privileged access for anomalies, which in turn can identify which users are conducting privileged activities. These detections occur within on-premise deployments, Azure, AWS and Microsoft Office 365 environments. Both in the Commercial and Government tenants. In using various unsupervised AI models, Vectra Threat Detection and Response platform can raise the threat and certainty score on account use that is outside the norm. When this detection is taken in correlation with other attacker behaviors seen in the environment, it permits high fidelity alerting that an account is involved in an attack; and not just doing 'something different'. Anomaly detection often creates great amounts of noise and are unreliable. The correlation of the anomaly with other behaviors provides greater certainty.




**AC.L2-3.1.7** *Privileged Functions* (CMMC 2 – 3): Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. (800-53: AC-6(9), AC-6(10))

Vectra Threat Detection and Response platform provides automatic and real time alerting of users acting in privileged manners via integrations into AzureAD, Active Directory, LDAP, and other identity sources. By examining the accounts actions and 'observed privilege' in correlation with other behavioral based detections, real time alerting and account lockdown/containment can be put in place to mitigate potential threats.

**AC.L2-3.1.12** *Control Remote Access* (CMMC 2 – 3): Monitor and control remote access sessions. (800-53: AC-17(1))

Vectra Detect and Vectra Stream monitor remote access sessions and pathways. Information can be acted upon based on integrations with NAC, SOAR, EDR and SIEM tools. Remote access sessions are categorized and given a risk and impact score in Vectra Detect. This enables analysts and engineers to focus on higher-risk users without the noise usually associated with tracking remote access sessions. Within the metadata, specific details on remote access sessions and protocols are tracked and correlated with potential attacker behaviors from the AI models. Correlating the results of the various models with the remote access session information observed allows for automatic responses, controls, etc. to be enacted.

**AC.L2-3.1.15** *Privileged Remote Access* (CMMC 2 – 3): Authorize remote execution of privileged commands and remote access to security-relevant information. (800-53: AC-17(4))

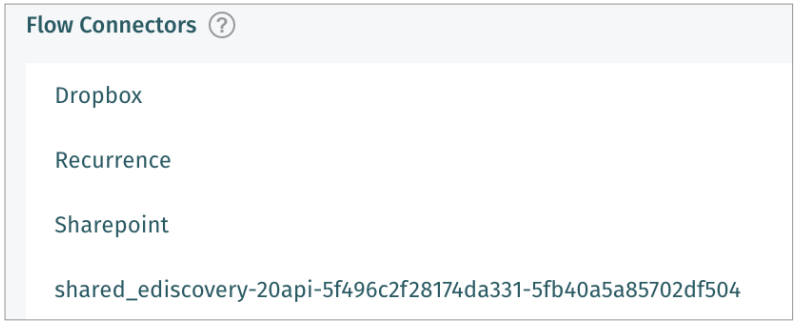
Vectra Detect monitors the remote execution of privileged commands. This capability exists natively, in the commercial and government cloud(s) and in Microsoft 365 environments. Observed remote execution of privileged commands automatically assigns a high or critical score to an asset based on other observed behavioral activities.

**AC.L2-3.1.8** *Unsuccessful Logon Attempts* **(CMMC 2 – 3):** Limit unsuccessful logon attempts.

Vectra Threat Detection and Response platform provides monitoring and detections indicative of brute force attacks and MFA bypass mechanisms that are commonly associated with unsuccessful logon attempts. Lockouts due to multiple failed attempts are usually benign, however when coupled with other attack behavior detections, Vectra can provide automated remediation, account containment, or other actions.

**AC.L1-3.1.20** *External Connections (CMMC 1 – 3)*: Verify and control/limit connections to and use of external information systems. (800-53: AC-20, AC-20(1))

Vectra Detect and Vectra Stream monitor connections to and from external information systems. Detections based on these capabilities are correlated with other data sources to automate responses based on observed behaviors from Vectra as well as with other security and orchestration tools. As an example, many attackers, malware, or insider threats will leverage PowerAutomate to stand up hidden connections and trust relationships with external data sources (DropBox, SharePoint, etc). Vectra provides an enablement to detect these 'suspicious activities' and federated trusts using escalated privileges.




## Domain: Audit and Accountability (AU)

**AU.L2-3.3.2** *User Accountability* (CMMC 2 – 3): Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. (800-53: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12)

Vectra Detect and Vectra Stream provide contextual details about user actions on the network. Usernames and system names are provided in detection and network metadata to attribute actions to individual users or entities. Integrations via Active Director, AzureAD, LDAP, Kerberos, and enrichment via endpoint detection and response (EDR) tools provide continuity of the users as they traverse hosts and multi-tenancy cloud environments.

## Domain: Identification and Authentication (IA)

**IA.L2-3.5.3** *Multifactor Authentication* (CMMC 2 – 3): Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

While multifactor authentication (MFA) provides enhanced identity verification, many sophisticated adversaries and nation states are able to bypass these controls via compromised credentials, spoofing, and manipulating the underlying configurations within tools such as Azure AD. Vectra's ability to detect logins bypassing MFA, M365/AzureAD administrators making MFA changes that are a-typical, and full scans of the posture of the 7,500+ configurations lines within AzureAD permit for alerts to mechanisms that the root systems themselves cannot.

## Domain: Incident Response (IR)

**IR.L2-3.6.1** *Incident Handling* (CMMC 2 – 3): Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. (800-53: IR-2, IR-4, IR-5, IR-6, IR-7)

Utilizing Vectra capabilities, IR is enhanced with data that supports detection, containment, and other AI-enriched metadata for reporting and forensics. Additionally, Vectra Detect provides upfront behavioral detection capabilities that mitigate the actual IR based on early detection and automated enforcement and alerting. With the ability to detect net new and unknown threats without signatures in real time, Vectra can provide detection and containment within seconds of the first attacker behaviors being seen. To maintain change management, ticketing and SOAR based playbooks can be leveraged to allow for a period of human interaction before creating an automatic containment/lockdown of the host or user.

**IR.L2-3.6.2** *Incident Reporting* (CMMC 2 – 3): Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. (800-53: IR-2, IR-4, IR-5, IR-6, IR-7)

Vectra Detect will detect, triage and alert via the Vectra dashboard incidents as high or critical. These alerts and real-time reporting in Vectra Detect allow immediate actions to be taken. Integration with SIEM and ticketing tools enables additional reporting and response capabilities based on regulations for internal and external sources.

## Domain: Risk Management (RM)

**RA.L2-3.11.2** *Vulnerability Scan* (CMMC 2 – 3): Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those. (800-53: RA-5, RA-5(5))

Vectra Stream collects and stores security-enriched network metadata from all traffic. The metadata is enriched with deep security insights and threat context that are critical to identifying vulnerable systems within SIEM tools. At the same time, Vectra Detect identifies in real-time new systems that may be vulnerable based on observed user behavior, attacker lateral movement, and overall 70+ patented AI-based behavioral models. Certain portions of the metadata can be used to surface characteristics like weak cyphers (old TLS versions), SMB shares, and beaconing that may be indicative of vulnerable assets. Many organizations find that with Vectra Threat Detection and Response platform, they realize there are many more assets on their environment that are not accounted for; but also are prime targets for attackers.

**RA.L2-3.11.3** *Vulnerability Remediation* (CMMC 2 – 3): Remediate vulnerabilities in accordance with risk assessments. (800-53: RA-5)

Vectra Detect and Vectra Stream are able to take immediate action against vulnerabilities, natively as well as when integrated with an orchestration environment. The detection of accounts with deactivated MFA, hosts with open SMB or weak cyphers, and other metadata traffic analysis permits for remediation before risk assessments have been completed.

The Vectra Threat Detection and Response platform can perform automated account deactivation within LDAP and AD and coordinate change of authorization (COA) within a NAC solution to de-authorize or change ACLs within an environment. Based on various detections, the ability to contain hosts with certain threat and certainty scores from Vectra can be automated within EDR tools such as Microsoft Defender, CrowdStrike, and CarbonBlack.

**RA.L2-3.11.2** *Vulnerability Scan* (CMMC 2 – 3): Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

A major gap in most cloud security assessment and compliance is the posture of the 7,500+ individual configuration lines per user within AzureAD/M365. It has been found in many instances where tokens and authentication have been cloned by adversaries making use of these easy to manipulate spaces. Vectra provides a continual monitoring/scanning capability of the posture within AzureAD in the commercial, GCC, GCC-HIGH and government SECRET and TOP SECRET enclaves. Vectra Protect is the only capability approved by Microsoft to support these initiatives.

## Domain: Security Assessment (CA)

**CA.L2-3.12.3** *Security Control Monitoring* (CMMC 2 – 3): Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (800-53: CA-2, CA-5, CA-7, P-2)

The Vectra AI cyber detection engine provides real-time dashboard views and alerts of potential issues, allowing validation of security controls and the ability to further validate whether security controls are effective and comprehensive. Ideally, an environment is well controlled and locked down, however most enterprises do not provide adequate controls over ancillary systems that allow for lateral movement into more critical environments. Leveraging the Vectra Detect dashboard provides real time awareness of compromised systems, new attacks bypassing the current security controls, and a means to detect Red/Purple teams during assessments.

## Domain: System and Communications Protection (SC)

**SC.L2-3.13.6** *Network Communication by Exception* (CMMC 2 – 3): Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Organizations moving to a Zero Trust Security Architecture are faced with many challenges. As the analytics basis of numerous Intelligence Agency Zero Trust reference architectures, Vectra Threat Detection and Response platform provides all environments with additional context on privilege use anomaly detection of hosts/accounts with elevated privileges using resources outside of their learned norm. While zero trust limits underlying access, it often is not granular enough to track the enabled accounts after they have been granted permissions.

**SC38: SC.L2-3.13.11** *CUI Encryption* (CMMC 2 – 3): Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (800-53: SC-13)

The enriched metadata from Vectra Threat Detection and Response platform is able to differentiate weak cyphers in the environment that are indicative of non-FIPS validated crypto. A major finding in many reports is that, while the environment is FIPS enabled, many legacy tools or OT/IoT/ICS environments use weak or deprecated crypto. The automated surfacing of these within Vectra Threat Detection and Response platform can provide immediate visibility.

The Vectra Threat Detection and Response platform leverages FIPS 140-2-compliant cryptographics for all transmission and federal data-at-rest (DAR) of ML-enhanced metadata and micro-PCAP instances. All interfaces to third-party systems are initiated with compliant cryptographics. The Vectra Threat Detection and Response platform does not require decryption of traffic flows to perform the ML-based behavioral detection capabilities. This means that no break-and-inspect is required for operations.

**SC39: SC.L1-3.13.1** *Boundary Protection* (CMMC 1 – 3): Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. (800-53: SC-7, SA-8)

Vectra Detect and Vectra Stream monitor communications at external and key boundaries. Neural Network based behavioral cyber detections identify and alert security analysts about potential threats in real time at all levels of the communications systems. Unlike signature based capabilities, Vectra is not bound to 'known' attack vectors for bypassing the boundaries, but instead is able to detect net new or 'unknown' attacks based on the successive behaviors.

## Domain: System and Information Integrity (SI)

**SI.L1-3.14.1** *Flaw Remediation* (CMMC 1 – 3): Identify, report, and correct information and information system flaws in a timely manner. (800-53: SI-2, Si-3, SI-5)

Vectra Stream provides full data lake integration for reporting and forensic capabilities during and after an incident. This data can be correlated with other platforms to locate flaws in data sets and enable comparative exercises to be completed by SOC teams using AI-enriched metadata. Real-time alerting is completed in the Vectra Threat Detection and Response platform dashboard, the reason many CISO organizations look at Vectra at the start and end of each shift to understand their current situation.

**SI.L1-3.14.2** *Malicious Code Protection* (CMMC 1 – 3): Provide protection from malicious code at appropriate locations within organizational information systems. (800-53: SI-2, SI-3, SI-5)

Instead of preventing malicious code, the Vectra Threat Detection and Response platform detects and responds to net new threat behaviors, including command-and-control communication, data exfiltration and lateral movement. As a result, the Vectra Threat Detection and Response platform can automatically quarantine or honeypot a system and use industry partnership with Network Access Control (NAC), Endpoint Detection and Response (EDR), and Security Orchestration and Response (SOAR) solutions to mitigate the additional propagation to other systems and endpoints in cloud, remote and other environments. The approach to leverage AI for automating a zero trust security response to potential malicious actors and net-new attacks allow Vectra to stop attacks before they have begun.

**SI.L1-3.14.4** *Update Malicious Code Protection* (CMMC 1 – 3): Update malicious code protection mechanisms when new releases are available. (800-53: SI-3)

Due to the behavioral nature of the Vectra Threat Detection and Response platform, updates are not necessary and the system continuously leverages new AL algorithms to detect emerging threats before traditional definitions have been released by most vendors and security organizations. By leveraging AI behavioral detections, the threat from new attackers can be reduced and time to detect and time to respond reduced from hours, days or weeks down to minutes.

**SI.L2-3.14.6** *Monitor Communications for Attacks* (CMMC 2 – 3): Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. (800-53: AU-2, AU-2(3), AU-6, SI-4, SI-4(4))

Vectra Detect provides next-generation IDS/IPS capabilities and AI-driven behavioral detection of attacks without the need for definitions, traffic decryption or other techniques common in most commercial offerings. Supporting most of our national security systems (NSS) consumers, Vectra allows cyber teams to mitigate an attack before it has moved into a state of replication or causing damage.

**SI.L2-3.14.7** *Identify Unauthorized Use* (CMMC 2 – 3): Identify unauthorized use of organizational systems. (800-53: SI-4)

Vectra Detect identifies, responds and mitigates privileged account abuse and compromise when users perform activities that exceed normal behaviors. These malicious behaviors are prime indicators that an attacker has taken over a user's account and privileges or created a fake account to move laterally in search of assets to exfiltrate. The majority of recent attacks have leveraged some level of M365 account compromise and lateral movement across the environments based on escalated privileges. Being able to detect these behaviors before they have time to execute in the GCC-HIGH is a key component to protecting the enterprise.

## In Summary

Vectra maps the various requirements of the CMMC through the Vectra Threat Detection and Response platform. As the number one AI-driven network detection and response platform, Vectra supports workloads across the network at any classification level, including cloud, data center, IoT and enterprise. The platform enables continuous monitoring and real time alerting while reducing overall security operations center (SOC) and security analyst workloads.

**For more information please contact us at federal@vectra.ai.**

Email federal@vectra.ai  vectra.ai/federal

© 2022 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Security that thinks is a registered trademark and the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: **060322**