VECTRA
SECURITY THAT THINKS.®

CMMC BRIEF

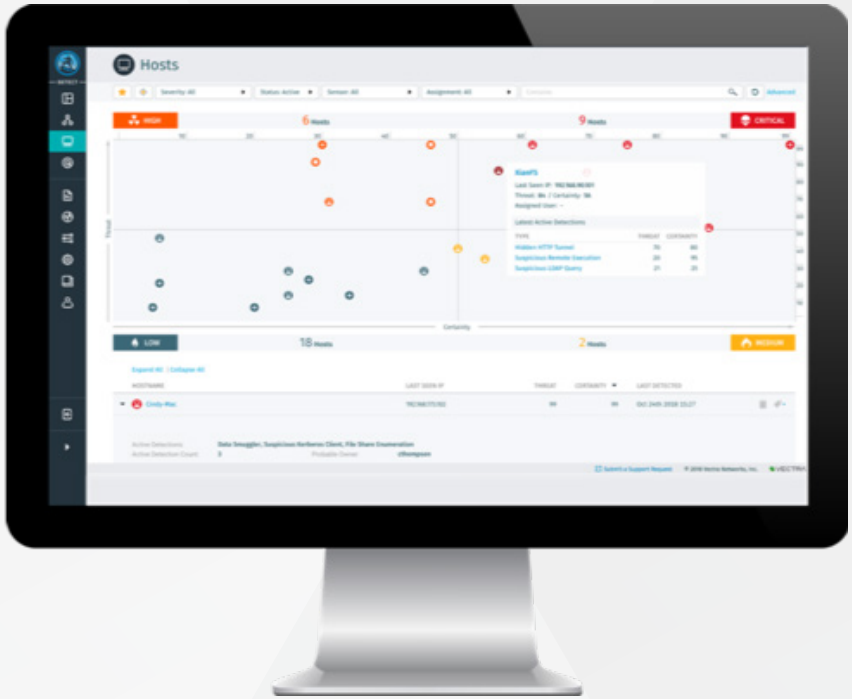
Meeting the Challenges of the Cybersecurity Maturity Model Certification (CMMC) with Vectra®

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

The CMMC, effective since November 2020, is a combination of various best practices and cybersecurity standards that represents a continued evolution of the current DFARS 252.204-2012. CMMC added verification as a requirement with various levels available for qualification; however, most organizations are required to self-certify at Level-3 and obtain additional certification for Level 4 or Level 5, 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 Cognito NDR platform support all workloads – from the cloud to the data center, as well as traditional IT assets to IoT/OT industrial controls and sensors – the applicability and value benefits of continuous monitoring and real time alerting assist in many certification challenges while also reducing 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 Cognito NDR platform from Vectra fulfills the category. Weeks or months of workloads and analysis are automated in minutes through Cognito's patented machine learning (ML) and artificial intelligence (AI). For more information, contact the 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 Cognito® network detection and response (NDR) platform from Vectra. This allows mapping of the CMMC to the DFARS (NIST 800-171) and traditional NIST 800-53 controls.

Domain: Access Control (AC)

C002: AC.2.007 Control internal system access (CMMC 2 – 5): Employ the principle of least privilege, including for specific security functions and privileged accounts. (800-53: AC-6, AC-6(1), AC-6(5))

Cognito Detect™, which runs on the Cognito NDR platform from Vectra, 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 Office 365 environments.

C002: AC.2.008 Control internal system access (CMMC 2 – 5): Use non-privileged accounts or roles when accessing non-security functions. (800-53: AC-6(2))

Cognito Detect from Vectra 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.

C002: AC.3.018 Control internal system access (CMMC 3 – 5): 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))

Cognito Detect from Vectra provides monitors privileged access for anomalies, which in turn can disclose which users are conducting privileged activities. These detections occur within on-premise deployments, Azure, AWS, and Microsoft Office 365 environments.

C002: AC.4.023 Control internal system access (CMMC 4 – 5): Control information flows between security domains on connected systems. (800-53: AC-4)

Cognito Stream™, which runs on the Cognito NDR platform from Vectra, provides network connection details that identify information flows between security domains. This information can be ingested into high-level SIEMs and data lakes such as Splunk, ArcSight, Elastic, Elk, Sentinel, and others.

C003: AC.2.013 Control remote system access (CMMC 2 – 5): Monitor and control remote access sessions. (800-53: AC-17(1))

Cognito Detect and Cognito Stream from Vectra monitors 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 Cognito Detect. This enables analysts and engineers to focus on higher-risk users without the noise usually associated with tracking remote access sessions.

C003: AC.3.021 Control remote system access (CMMC 3 – 5): Authorize remote execution of privileged commands and remote access to security-relevant information. (800-53: AC-17(4))

Cognito Detect from Vectra monitors the remote execution of privileged commands. This capability exists natively for networks, in the cloud, and in Microsoft Office 365 environments. Observed remote execution of privileged commands automatically assigns a high or critical score to an asset based on other observed behavioral activities.

C004: AC.1.003 Limit data access to authorized users and processes (CMMC 1 – 5): Verify and control/limit connections to and use of external information systems. (800-53: AC-20, AC-20(1))

Cognito Detect and Cognito Stream from Vectra monitors 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.

Domain: Audit and Accountability (AU)

C007: AU.2.041 Define audit requirements (CMMC 2 – 5): 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)

Cognito Detect and Cognito Stream from Vectra 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.

Domain: Incident Response (IR)

C016: IR.2.092 Plan incident response (CMMC 2 – 5): 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 ML-enriched metadata for reporting and forensics. Additionally, Cognito Detect from Vectra provides upfront behavioral detection capabilities that mitigate the actual IR based on early detection and automated enforcement and alerting.

C016: IR.4.100 Plan incident response (CMMC 4 – 5): Use knowledge of attacker tactics, techniques and procedures in incident response planning and execution. (800-53: IR-1, IR-6, PM-15)

Vectra provides patented ML behavioral detection models that learn about new attacks in real time before they are given names by USCERT/CISA/USCYBERCOM or most major threat labs. Coordinated responses based on real time attacks provide a faster time-to-respond and reduce the impact of incidents.

C016: IR.5.106 Plan incident response (CMMC 5): In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data. (800-53: AU-10(3), AU-12)

Cognito Stream from Vectra provides data lake and other integrations for forensic evaluation of any incidents, and contributes heavily to an IR plan. Automated responses are coordinated within the security integration community and SOAR platforms, allowing which enables automatic remediation and removal of high or critical compromised assets based on observed and learned behaviors.

C017: IR2.093 Detect and report events (CMMC 2 – 5): Detect and report events. (800-53: AR-4, AU-13, IA-10, IR-4, IR-5, IR-6, PE-6, RA-6)

Cognito Detect and Cognito Stream from Vectra provide full IDS/IPS capabilities to detect attacker behaviors and complete reporting of events via the Cognito Detect dashboard or Cognito Stream components in existing reporting tools.

C017: IR2.094 Detect and report events (CMMC 2 – 5): Analyze and triage events to support event resolution and incident declaration. (800-53: IR-4(3))

Leveraging mappings to the MITRE ATT&CK framework, Cognito Detect from Vectra provides full triage of detected threat incidents to avert data breaches. Integration with EDR, SIEM, SOAR, and NAC tools can automatically remediate, quarantine and evaluate IR needs, and assess the potential impact of an event based on ML-enhanced metadata used during post-incident forensics. As a result of the AI-derived ML capabilities and detections, most events are alerted and remediated prior to being classified as incidents.

C018: IR.2.095 Develop and implement a response to a declared incident (CMMC 2 – 5): Develop and implement responses to declared incidents according to pre-defined procedures. (800-53: IR-4, IR-9, SE-2)

Leveraging developed playbooks, Cognito Detect from Vectra is able to coordinate activities with SIEM and SOAR platforms to create responses to incidents in real time. Additionally, SOC organizations can access in-dashboard details about the incident, lateral movement activities and all historical data with linkage into the data lake environment for further investigation.

C018: IR.3.098 Develop and implement a response to a declared incident (CMMC 3 – 5): 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)

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

C018: IR.4.101 Develop and implement a response to a declared incident (CMMC4 – 5): Establish and maintain a SOC capability that facilitates a 24/7 response capability. (800-53: SC-38)

Cognito Detect and Cognito Stream from Vectra act as the basis for many modern SOC environments, allowing a singular dashboard to show all local, cloud, and remote assets and Microsoft Office 365 instances through one

interface. Cognito Detect has access to all network segments via SPANs, taps or packet brokers to provide real time behavioral views of all assets and VPN/ remote users. By itself, the Cognito NDR platform provides an initial SOC environment. Enhanced integration with SIEM, SOAR, EDR, and NAC tools allow for greater fidelity of alerts.

C018: IR.5.102 Develop and implement a response to a declared incident (CMMC 5): Use a combination of manual and automated, real time response to anomalous activities that match incident patterns. (800-53: IR-4(1))

Cognito Detect from Vectra detects and responds to anomalous activities in real time and can be coordinated into known STIX threat feeds, custom response alerting, and manual triggers based on known conditions.

C019: IR2.097 Perform post incident reviews (CMMC 2 – 5): Perform root cause analysis on incidents to determine underlying causes. (800-53: AU-2, IR-4)

Cognito Detect and Cognito Stream from Vectra provide forensics data to determine root cause analysis of incidents. Data includes micro-PCAPs of incidents, inferred movement, command-and-control communication, data exfiltration, and other details. This enables security analysts to perform rapid response, understand how an incident began, assess the impact level, and know how to mitigate. In most scenarios, incidents are reduced as real time behavioral learning allows for immediate action and threat isolation.

Domain: Risk Management (RM)

C031: RM.2.142 Identify and evaluate risk (CMMC 2 – 5): Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. (800-53: RA-5, RA-5(5))

Cognito Stream from Vectra collects and stores security-enriched network metadata from all traffic. The metadata is enriched with deep security insights and contain threat context that identify vulnerable systems within SIEM tools. At the same time, Cognito Detect from Vectra identifies in real time new systems that may be vulnerable based on observed user behavior, attacker lateral movement, and other patented -ML-based behavioral models.

C031: RM.4.150 Identify and evaluate risk (CMMC 4 – 5): Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting and response and recovery activities. (800-53: PM-16)

The Cognito NDR platform from Vectra leverages real time behavioral threat hunting capabilities based on ML and AI. Using STIX intelligence feeds for proactive threat hunting, response and recovery, Cognito Detect is instrumental in coordinating the efforts of security analysts for faster response based on identified risks.

C031: RM.4.151 Identify and evaluate risk (CMMC 4 – 5): Perform scans for unauthorized ports available across perimeter network boundaries, over the organization's Internet boundaries and other organization-defined boundaries. (800-53: RA-5, RA-5(4))

The Cognito NDR platform from Vectra leverages scan data in correlation with behavioral threat detections to identify vulnerability gaps in the perimeter of network boundaries.

C032: RM.2.143 Manage Risk (CMMC 2 – 5): Remediate vulnerabilities in accordance with risk assessments. (800-53: RA-5)

Cognito Detect and Cogito Stream from Vectra are able to take immediate action against vulnerabilities, natively as well as when integrated with an orchestration environment. The Cognito NDR 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.

Domain: Security Assessment (CA)

C035: CA.3.161 Define and manage controls (CMMC 3 – 5): 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 Cognito NDR platform from Vectra 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.

Domain: System and Communications Protection (SC)

C038: SC.3.177 Define security requirements for systems (CMMC 3 – 5): Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (800-53: SC-13)

The Cognito NDR platform from Vectra 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 Cognito NDR 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.

C039: SC.1.175 Control communications at system boundaries (CMMC 1 – 5): Monitor, control and protect organizational communications (e.g., 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)

Cognito Detect and Cognito Stream from Vectra monitor communications at external and key boundaries. ML-based behavioral detections identify and alert security analysts about potential threats in real time at all levels of the communications systems.

C040: SI.1.210 Identify and manage information system flaws (CMMC 1 – 5): Identify, report and correct information and information system flaws in a timely manner. (800-53: SI-2, Si-3, SI-5)

Cognito Stream from Vectra 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 ML-enriched metadata.

C040: SI.4.221 Identify and manage information system flaws (CMMC 4 – 5): Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting. (800-53: SI-5, SI-5(1))

Cognito Detect from Vectra ingests STIX threat indicators to perform targeted detections relevant to high-value assets and systems.

C041: SI.1.211 Identify malicious content (CMMC 1 – 5): 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 Cognito NDR platform from Vectra detects and responds to new threat behaviors, including command-and-control communication, data exfiltration, and lateral movement. As a result, the Cognito NDR platform can automatically quarantine or honeypot a system and use standard NAC solutions to mitigate the additional propagation to other systems and endpoints in cloud, remote and other environments.

C041: SI.1.212 Identify malicious content (CMMC 1 – 5): Update malicious code protection mechanisms when new releases are available. (800-53: SI-3)

Due to the behavioral nature of the Vectra NDR platform, updates are not necessary and the system continuously leverages new ML algorithms to detect emerging threats before traditional definitions have been released by most vendors and security organizations.

C041: SI.5.222 Identify malicious content (CMMC 5): Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions. (800-53: SI-4, SI-4(4))

The ability to distinguish normal behaviors from malicious behavior is cornerstone of the Cognito NDR platform from Vectra. Coupled with cloud-based AWS and Azure instances and Microsoft Office (including Microsoft Office 365) integrations, normal command executions – such as Microsoft PowerShell and Power Automate – can be vetted to detect and mitigate lateral movement as cyberattackers pivot from the cloud to hybrid and on-premises environments. If an abnormal malicious code execution occurs, the Cognito NDR platform enables SOC analysts to respond and remediate faster while stopping the threat from spreading and compromising other assets.

Domain: System and Information Integrity (SI)

C042: SI.2.216 Perform network and system monitoring (CMMC 2 – 5): 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))

Cognito Detect from Vectra provides next-generation IDS/IPS capabilities and ML-driven behavioral detection of attacks without the need for definitions, traffic decryption or other techniques common in most commercial offerings.

C042: SI.2.217 Perform network and system monitoring (CMMC 2 – 5): Identify unauthorized use of organizational systems. (800-53: SI-4)

Cognito Detect from Vectra 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.

C042: SI.5.223 Perform network and system monitoring (CMMC 5): Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior. (800-53: SI-4)

Cognito Detect from Vectra uses behavior-based machine learning models to identify and responds to suspicious events, traffic flows and other activities that indicate an attack is in progress. Vectra automatically detects threats in all remote and on-premises devices, users, and account privileges across native and hybrid clouds, data centers, IoT, and enterprise networks. Additionally, account detections are performed for suspicious behaviors and extend into the Microsoft Office 365 environment for malicious use of compromised credentials or insider threats.

In Summary

Vectra maps the various requirements of the CMMC through the Cognito® network detection and response (NDR) 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 a service representative at federal@vectra.ai.

Email federal@vectra.ai vectra.ai/federal