VECTRA®
Security that thinks.®

CDM Phase 3 DEFEND: Federal Government

OVERVIEW

This overview describes how Cognito™ platform from Vectra®, in combination with existing security technologies, supports the Continuous Diagnostics and Mitigation (CDM) Program and enables agencies to achieve their security objectives.

The Cognito platform from Vectra is now on the DHS CDM approved products list (APL). This means that 66 Federal Civilian Agencies as well as State and Local Government entities can now purchase Vectra cybersecurity products.

The Vectra Cognito automated threat detection and response platform identifies hidden cyberattackers in real time and enables enterprises to quickly stop advancing threats inside networks and across their entire infrastructure.

VALUE PROPOSITION AND NAME BRAND JUSTIFICATION

Vectra is the only American-made FIPS-compliant technology that uses artificial intelligence to automate the hunt for cyberattacks in large-scale infrastructures, including data centers and the cloud, by continuously monitoring internal network traffic, logs and cloud events to detect advanced attacks as they are happening.

Vectra AI software automatically detects attacker behaviors, correlates attack detections with compromised host devices, and prioritizes attacks that pose the greatest risk to key assets. This enables Federal agencies to quickly prevent or mitigate loss.

Vectra technology provides:

- Simplification, automation and augmentation of the SOC operations
- Hunting down malicious actors (external and internal)
- Advanced persistent threat (APT) hunting

HOW VECTRA SUPPORTS THE CDM PROGRAM

Multiple goals of the CDM Program relate to automation at the Agency level: Automated data collection and automated identification of the most critical security issues. Automation is also involved at the Federal enterprise level; it assists with rolling up summary information into an enterprise-level dashboard, enabling near real-time situational awareness and determination of cybersecurity risk posture.

Vectra Cognito enables agencies to automate the process of identifying malicious incidents in real-time and triaging threats to the SOC team. The platform integrates several security technologies, leveraging them as a dashboard, data source or action targets to automate threat detection, triage, investigation, response, and intelligence sharing. Vectra has a large ecosystem of third-party technology partners that integrate with the platform to achieve initiatives from the Program.

MANAGE EVENTS (MNGEVT) REQUIREMENTS

Vectra Cognito uniquely maximizes automation and reduces human interaction by automating the Tier 1 security analyst role. Cognito rapidly detects attacker behavior and feeds the incident response tools, providing real time attacker behavior using our threat and certainty scores, as well as providing context around the attack and forensics. Vectra Cognito is proven to strengthen enterprise customers security postures.

1. The system can be set up to integrate with existing solutions to follow response process and procedures.
2. It can be set up to securely and automatically communicate and share incident response data
3. Important forensic data can be extracted from the system, significantly reducing the amount of time it takes to understand what happened and what has been impacted.
4. Find abnormal, anomalous network behavior and report on it in real time
5. Generate audit data that meet regulatory requirements including:
    a) Appropriate audit data that can be used to support security assessment and forensic analysis.
    b) Audit records that meet regulatory requirements
    c) Audit records that include “Who (asset or entity),” “What (action),” “When,” and “Where (target)” attributes of log messages
    d) evidence when the audit log data is compromised in transit or at rest.
    e) Providing audit and accountability data to report activities related to personally identifiable information and protected critical key assets

INCIDENT RESPONSE MONITORING

1. Vectra Cognito detects events and incidents, in real-time, related to malicious and/or anomalous activities that could impact the security posture of an Agency’s network and infrastructure assets.
2. Automated scoring of hosts reveals the overall risk to the network based on threat and certainty. The Threat Certainty Index™ from Vectra scores all threats and prioritizes attacks that pose the biggest risk. The scoring of compromised hosts by the Threat Certainty Index allows security teams to define threshold levels based on combined scoring (e.g., critical > 50/50).
4. Vectra Cognito provides context around the incident as well as valuable forensic information that would otherwise have to be a manual data collection process.

OPERATE, MONITOR AND IMPROVE (OMI) REQUIREMENTS

Vectra Cognito is designed to detect malicious activity, in real-time using our patented algorithms. Those algorithms are designed to detect anomalous and suspicious network behavior.

"WHAT IS HAPPENING ON THE NETWORK?"

Vectra Cognito acts as a Tier-1 security analyst, watching over all of your software and hardware assets, in real time. Cognito monitors the activity, using its artificial intelligence to track down attacker behavior in real-time. We give unprecedented insight and visibility into what is going on across your infrastructure. Cognito's capabilities include network and perimeter components, host and device components, data at rest and in transit, and some user behavior and activities.

EXAMPLES OF VECTRA ECOSYSTEM PARTNER INTEGRATIONS

- Splunk
- Micro Focus ArcSight
- IBM QRadar
- Carbon Black
- CrowdStrike
- Gigamon
- Ixia
- APCON
- VMware NSX
- VMware
- Palo Alto Networks
- Juniper Networks
- Phantom
- Demisto
- Cisco