VECTRA®

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 Cognito network-detection and response platform from Vectra correlates security-enriched metadata with other sources, automatically surfaces hidden attacks in real time, and enables conclusive threat hunting and incident investigations.

Value proposition and name brand justification

The Cognito platform from Vectra enables security operations professionals at Federal agencies to:

- Feed data lakes and SIEMs with Zeek-formatted security-enriched network metadata.
- Leverage our investigative workbench, which is optimized for enriched metadata and enables sub-second searches at scale.
- Detect, prioritize and correlate in-progress attacks to compromised host devices to quickly prevent and mitigate loss.

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.

The Cognito platform includes Cognito Stream™, Cognito Recall™ and Cognito Detect™.

Cognito platform: The right data with the right context

The Cognito platform collects and stores the right network metadata and augments it with machine learning.

- High-fidelity metadata
- Security-enriched metadata
- Real-time and historical metadata
- Scalable architecture
- 360° visibility: user, data center and cloud

Cognito Stream: Network metadata with an opinion

Cognito Stream sends security-enriched metadata in Zeek format to data lakes and/or SIEM.

- Correlate network metadata with other data sources
- Build custom tools and models to detect, investigate and hunt
- Leverage all existing Zeek tooling

Cognito Recall: Built for investigation and hunting

Cognito Recall is a cloud-based application to store and interact with security-enriched metadata.

- Hunt for threats retrospectively
- Accelerate incident investigations
- Focus on security not infrastructure

Cognito Detect: The power of AI to detect and prioritize

Cognito Detect gives you the power of AI to automatically detect, triage, prioritize and score hidden and unknown attacks at speed.

- Stop compromises before they become breaches
- Prioritize investigation and response
- Empower and grow Tier-1 analysts

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.

Cognito from Vectra enables agencies to automate the process of identifying malicious incidents in real-time and triaging threats for the security operations team.

The Cognito 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

Cognito from Vectra 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:
   - Appropriate audit data that can be used to support security assessment and forensic analysis.
   - Audit records that meet regulatory requirements.
   - Audit records that include “Who (asset or entity),” “What (action),” “When,” and “Where (target)” attributes of log messages.
   - Evidence when the audit log data is compromised in transit or at rest.
   - 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).
3. 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
- Splunk Phantom
- Demisto
- Cisco

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai