VECTRA

Meeting the DoD Zero Trust Capabilities & Activities Mapping

Mapping Vectra AI to the Individual Activity IDs

Table of Contents

About Vectra AI

As the leader in hybrid attack detection, investigation, and response, Vectra AI arms your SOC team to quickly discover and respond to would-be attackers —before they act.

The Vectra AI Platform rapidly identifies malicious attacker behavior and activity across your hybrid cloud environment. Vectra AI's Attack Signal Intelligence™will find it, flag it, prioritize it and alert security personnel so they can investigate and respond immediately.

Vectra AI finds attacks others can't using artificial intelligence to improve threat detection, investigation, and response (TDIR) over time, and eliminating false positives so your team can focus on real threats.

With major milestones of Zero Trust anticipated to advance in 2025, industry must provide a coordinated effort across vendors to simplify the process for government program offices. Vectra AI Federal has been supporting the DoD CIO ZTA organization since the inception of the program office, and prior, supporting various intelligence community components assisting in early ZTA doctrine. Within the following pages, Vectra AI provides both the existing mappings to the DoD's seven ZTA pillars along with individual mappings of the 152 activities Vectra AI supports.

A key aspect of mapping into the DoD and Intelligence Community frameworks extends past how a specific vendor or partner can meet a specific, point activity. To properly support the government agencies and program offices, the vendor community must also provide guidance in how complete their offering is to each ZTA activity. Understanding where a vendor or product offering fulfills, partly fulfills, or supports an activity via integrations allows a program team to build a composite set of vendors that fulfill as many of the activities while keeping the list small. A unique vendor for every activity would result in an unmanageable domain of tools, licensing, and custom integrations.

On top of where a vendor can fulfill various ZTA activities, providing the government with a list of technology alliances that have native integrations or API based interactions permits for greater planning and reduces complexity. Leaving it up to a modestly overworked and understaffed government team to make their own assessments can yield dangerous results. First, the government cannot be subject matter experts (SMEs) in every product and new release to understand how tools work together or don't. Only industry engineers can validate and provide documentation to ensure proper system operations when fielded. Second, the continued release of new capabilities from a vendor and new code-versions are often unknown variables to the government. This can create preconceived concepts of partnerships that may have worked in the past, or that previously did not but now exist. Finally, there may be vendors who overlap on certain product offerings, yet complement each other in another offering. To provide the best solution to the government, competitive alliances can sometimes be the right joint solution to meet an activity or set of activities faster.

Vectra AI presents the following data points to answer the needs:

- Listing of the DoD ZTA capabilities and activities
- Notation on where Vectra AI fulfills, partly fulfills, or supports with metadata/artifacts each activity
- Technology alliance listing of partners that Vectra AI natively supports to create an integrated ecosystem

Defining Vectra AI's Fulfillment of the ZTA Capabilities and Activities

While easy to claim a vendor completes a specific aspect of the 152 activities, often it is a stretch to fully complete activities. Instead, Vectra AI took the approach of categorizing the completeness of the capability or activity and how the Vectra AI solution stacks up. The following represent the three categories of Vectra AI's alignment with the DoD and IC ZTA activities.

Vectra AI Directly Meets: Under this level of completeness, Vectra AI's offering fulfills the criteria and intent of a specific capability or activity. While Vectra AI offers certain SaaS offerings, those are not included in the Directly Meets label, as the specific options either are not FedRAMP HIGH or do not have proper controls and authorizations in place to be leveraged within the DoD or IC.

Vectra AI Meets with Integration: Meets with integration implies that Vectra AI's offering has a direct impact to a capability or activity, however to 100% meet the outcomes and intent, that partnership with a technology alliance would be in order. Within the document, Vectra AI will highlight those integrations; calling out those with 100% native operations today and those that require some level of API coordination to be successful. For applications without native integrations, the current API can be found at https://support.vectra.ai and searching for REST API to obtain the latest version (2.5 at time of writing).

Vectra AI Supports via Artifacts: The most basic level of completeness from Vectra AI is the support into other tools with enriched artifacts and metadata. The forensics data that Vectra AI provides has a full bearing on host and user inventory, privilege access, orchestration and PDP, and numerous other activities. Vectra AI's ability to influence and support allows for greater correlation and utilization of the system across the entire security and operations stack. Vectra AI's metadata 'types' are extensive and customizable based on the application.

Summary of Vectra AI ZTA Coverage

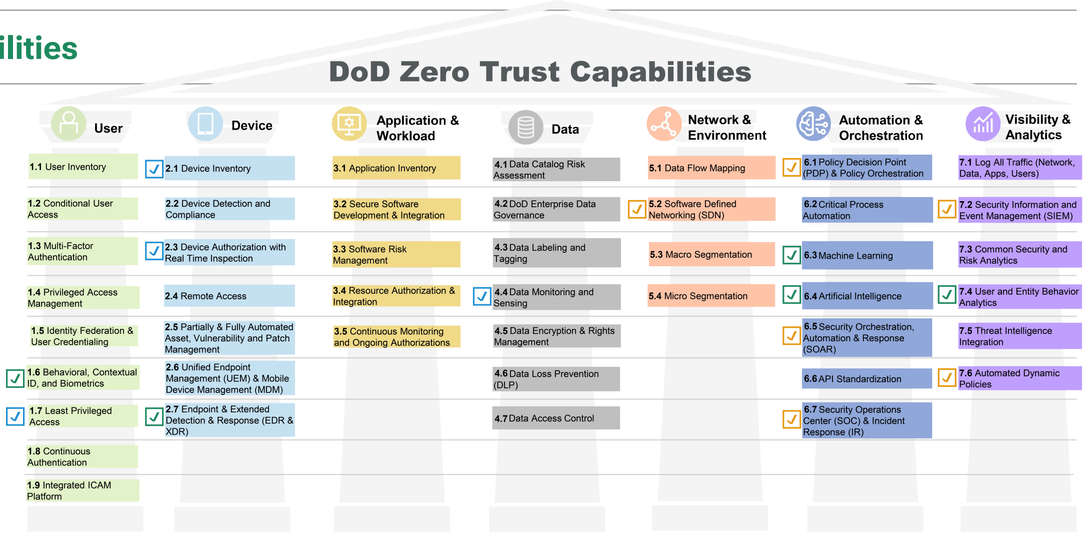
To provide an upfront summation, Table 1 provides a listing of the 74 DoD ZTA activities where Vectra AI provides a level of coverage. The table is broken down into the three categories of completion as described in the "Defining Vectra's Fulfillment of the ZTA Capabilities and Activities" section. As new capabilities are released by Vectra AI, integrations and APIs continue to evolve, and new data types are exposed, the summation values can expect to increase. Vectra AI's interpretation of the 152 specific activities was taken in a conservative and engineering process-based approach. No positive outcome would be served if the list, by any vendor, was inflated without proper justification and analysis.

	Total	Directly Meets Activity	Meets w/Integration	Supports via Artifacts
Target Level ZT	41	9	13	19
Advanced ZT	33	8	4	21
Total	**74**	**17**	**17**	**40**

Supporting the DoD Zero Trust Top Level Pillars & Capabilities

Vectra AI's support into the seven pillars of the DoD Zero Trust starts with a top-level mapping into the capabilities. It is important to note that at no point does Vectra AI "do" Zero Trust. The greater than 150 AI/ML model engine (Vectra Detect), Suricata legacy signatures (Vectra Match), and enriched metadata capability (Vectra Stream) create individual components that enable a Zero-Trust architecture. No single vendor "does" Zero Trust as the approach requires an integrated ecosystem of native integrations, custom API connectors, and thoughtful orchestration and planning.

Within the high-level capabilities, Vectra AI provides the mapping as shown in Figure-1, the well-known DoD Zero Trust Capabilities diagram.



DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	☑ 2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	☑ 6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	☑ 5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	☑ 7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	☑ 2.3 Device Authorization with Real Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	☑ 6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	☑ 4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	☑ 6.4 Artificial Intelligence	☑ 7.4 User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption & Rights Management		☑ 6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
☑ 1.6 Behavioral, Contextual ID, and Biometrics	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	☑ 7.6 Automated Dynamic Policies
☑ 1.7 Least Privileged Access	☑ 2.7 Endpoint & Extended Detection & Response (EDR & XDR)		4.7 Data Access Control		☑ 6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Fig-1. DoD Zero Trust Capabilities

☑ Vectra AI Meets Capability Objective ☑ Vectra AI Partially Meets w/ Integrations ☑ Vectra AI Supports via Artifacts/Metadata

DoD ZTA User: 1.6 Behavioral Contextual ID, and Biometrics

Vectra AI supports full behavioral activity monitoring for both hosts and users within SBU and CLASSIFIED environments. The use of numerous, purpose-built models allow for correlation across systems and presentation to the operator and other tools of less detection numbers with higher efficacy of threat and certainty.

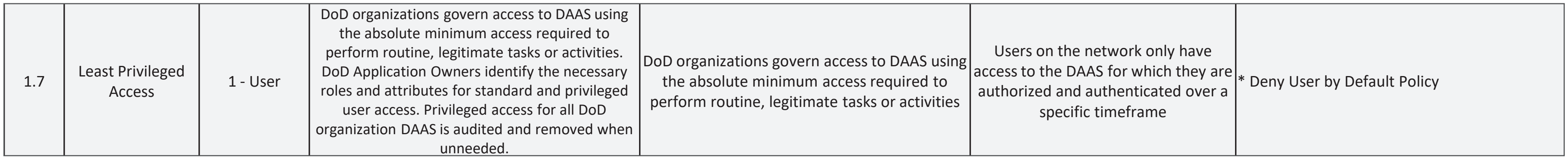
1.6	Behavioral, Contextual ID, and Biometrics	1 - User	Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	DoD organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls	Behavioral, contextual, and biometric telemetry enhances MFA with	* Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling * User Activity Monitoring Pt1 * User Activity Monitoring Pt2

- Looking for stitched together activities to detect successive indicators worth escalating to the SOC and operators for further investigation associated with:
  - Privilege escalation of users and hosts outside of the unsupervised AI/ML learned norms
  - Anomalous activity for a UID/GID to be performing
  - Peer learning of groups
  - "Observed Privilege" models that observe how much privilege is granted to a user/host
- Greater results than chatty UEBA tools that flag false positives; instead, stitch together successive indicators into a user/host container that shows progression prior to damage being inflicted or continued campaign activities.

Vectra AI provides full support and coverage within AzureAD, LDAP, A/D, and other identity sources for enrichment with host based EDR artifacts to observe service execution. When models are correlated across identity, cloud access, network traffic, and enrichment with Kerberos, EDR, and other telemetry, the resulting outcomes allow for rapid evaluation and action to be take in a ZTA orchestrated system.

DoD ZTA User 1.7: Least Privileged Access

Vectra AI supports determination of "Observed Privilege" via unsupervised AI/ML within the platform. These sets of AI algorithms are primarily unsupervised, self-learning within the environment. The models require anywhere from 4-hours to 10-days, depending on the model, to fully learn the environment.



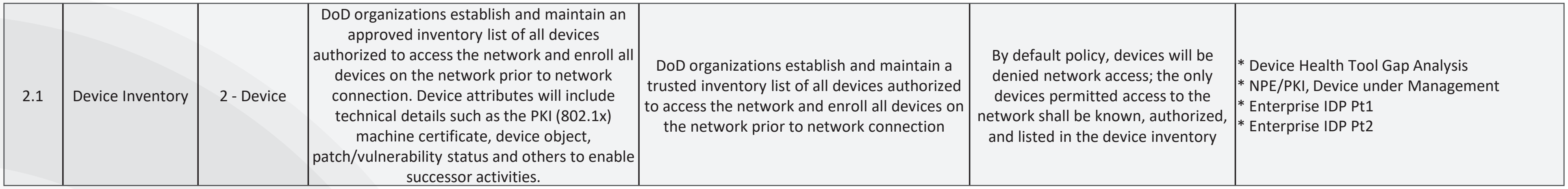
1.7	Least Privileged Access	1 - User	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities	Users on the network only have access to the DAAS for which they are authorized and authenticated over a specific timeframe	* Deny User by Default Policy

- Allows for audit and evaluation of UID, GID and other artifacts that will provide a context to the amount of privilege a user or host has been granted.
- Supports correlation with LPA methods to observe over-granted permissions and privilege.

Observed privilege scores for accounts derive from the number or services an account connects to, either exclusively or in partnership with a samll number of other accounts. An account that connects to 200 services, each of which is used by only a small number of other accounts, will score high. An account which connects to 5 services, each of which is used by a large number of other accounts, will score low.

DoD ZTA Device 2.1: Device Inventory

Vectra AI provides support for device inventory within a ZTA environment via multiple areas. The data provided by Vectra AI can be correlated and leveraged across numerous tools and workflows. Many analysts leverage Vectra AI's detections associated with "New Host" as a first line of correlation into malicious events.



2.1	Device Inventory	2 - Device	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection	By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory	* Device Health Tool Gap Analysis * NPE/PKI, Device under Management * Enterprise IDP Pt1 * Enterprise IDP Pt2

Every time a host connects to the network, Vectra AI triggers a "New Host" detection. While a host in itself is not usually note-worth, understanding how a host operates, changes over time, and moves in an environment provides significant operational data.

- Hosts containers are built for every host that tracks the historical of a host as it changes IPs, networks, hostnames, etc.
- Further enrichment of hosts are performed by native integrations with LDAP, Kerberos, A/D, Windows Security and Event Logs, Endpoint Detection & Response (EDR) artifacts, etc.
- Various government operators have called the Host Container the single most valuable resource in their arsenal as it performs the correlation via AI for the operators.

DoD ZTA Device 2.3: Device Authorization w/ Real Time Inspection

Vectra AI's AI/ML and Signature engine perform anomalous activity detection of hosts by looking for more than a single anomaly. Correlation of detections results in trustable, real-time data that can be leveraged in NAC, C2C, SOAR and other tools to created automated workflows. By correlation of multiple detections into single events with higher efficacy, the resulting 50% reduction in SIEM alerts will permit greater automation vs. human operator inspection.

2.3	Device Authorization w/ Real Time Inspection	2 - Device	DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time	Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Security threats identified are remediated faster through continuous activity inspection enables faster remediation of security threats	* Entity Activity Monitoring Pt1 * Entity Activity Monitoring Pt2 * Implement Application Control & File Integrity Monitoring (FIM) Tools * Integrate NextGen AV Tools with C2C * Fully Integrate Device Security stack with C2C as appropriate * Enterprise PKI Pt1 * Enterprise PKI Pt2

- Single anomaly events create alert fatigue for operators/analysts; correlation of detections allows for trust of the AI/ML models.
- Vectra AI's 150+ AI/ML models allow for stitching together of successive attacker behaviors that are indicators of an attack ongoing or in early stages.
- Integrations w/ EDR, Windows Security and Event Logs, Kerberos, and other artifacts and identity sources permit for real time detection of host events and behaviors prior to compromise.

DoD ZTA User 2.7: Endpoint & Extended Detection & Response (EDR & XDR)

Providing complete capability for XDR based requirements is a necessary initial step into the User side of ZTA. Vectra AI fulfills the aspects of the many key XDR requirements both natively and with integrations into the ecosystem of DoD & IC deployed EDR tools with authorizations.

2.7	Endpoint & Extended Detection & Response (EDR & XDR)	2 - Device	DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints.	Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint)	* Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1 * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2

- XDR, NDR, and EDR have all become somewhat interchangeable (or used in the same conversation) with XDR encompassing both endpoint and network.
- EDR continues to play an important role, however, has become compromised by truly sophisticated nation states/adversaries, where the network itself maintains ground truth.
- Vectra AI provides coverage for Public/Gov Clouds (incl TS), SaaS, federated identity, network, SASE, and EDR extensions.
- Vectra AI supports C2C integration and orchestration, providing the high confidence, correlated events via AI to ensure C2C actions are properly trained and executed.
- Vectra AI's alliance and native orchestration with primary EDR vendors permits for correlated detection data and learnings.

DoD ZTA Data 4.4: Data Monitoring and Sensing

Moving into the data monitoring fabric allows Vectra AI to leverage specific models surrounding inspect of the data itself in correlation with users, observed privilege, and other AI/ML aspects. Vectra AI's enriched metadata and forensic artifacts allow for alerting in real-time to potential missuses of data that owners may not validate with traditional DLP capabilities.

4.4	Data Monitoring and Sensing	4 - Data	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets	Data in all states are detectable and observable	* DLP Enforcement Point Logging and Analysis * DRM Enforcement Point Logging and Analysis * File Activity Monitoring Pt1 * File Activity Monitoring Pt2 * Database Activity Monitoring * Comprehensive Data Activity Monitoring

Vectra AI provides AI/ML models associated with file enumeration, data gathering, and data smuggling that fall under the 4.4 Capabilities:

- In correlation with other DLP tools, Vectra AI's "Data Gathering" and "Data Smuggling" detection models provide monitoring for anomalous and malicious activity via AI/ML.
- Vectra AI models supporting M365/AzureAD environments provide additional context for suspicious/anomalous behaviors associated with PowerAutomate and eDiscovery searches that can results in on-premises to cloud attack pivots; a critical aspect of ZTA.
- The Vectra AI model for "File Share Enumeration" provides triggers for excessive file share access (usually indicative of exfiltration or manipulation events) on a network in contrast to how a host or server usually operates on the network.
- Vectra AI's AI model associated with SQL Injection can identify anomalous database injection activities possibly associated with attackers leveraging a compromised system.

DoD ZTA Network and Environment 5.2: Software Defined Networking

Supporting the dynamic access of the network and environment requires the right data and telemetry to create informed decisions. Within Vectra AI and our technology alliances ecosystem, providing the actionable, real-time data is paramount and a key capability that the learnings from Vectra AI provide. Correlating user, host, identity, and access to orchestrate SDN is the resulting outcome from Vectra.

5.2	Software Defined Networking (SDN)	5 - Network and Environment	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane	Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements	* Define SDN APIs* Implement SDN Programable Infrastructure * Segment Flows into Control, Management, and Data Planes * Network Asset Discovery & Optimization * Real-Time Access Decisions

Vectra AI works with the PDP aspects of the ZTA plan and acts as the analytics integration for real time decision making and SDN orchestration:

- Vectra AI's integration into the other ZTA stack via API 2.0 capabilities allow for orchestration (SOAR) and SDN controller level decisions to be executed upon.
- SDN is not a capability of Vectra AI, however supporting SDN micro-segmentation and orchestration based on the AI/ML and signature contextual outcomes of Vectra AI exists.

DoD ZTA Automation & Orchestration 6.1: Policy Orchestration

While Vectra AI is not a primary Policy Decision Point (PDP), the capability outcomes provide the high efficacy data points necessary for a PDP to make informed decisions and coordinate for orchestration.

6.1	Policy Decision Point (PDP) & Policy Orchestration	6 - Automation and Orchestration	DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy	PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources	* Policy Inventory & Development * Organization Access Profile * Enterprise Security Profile Pt1 * Enterprise Security Profile Pt2

Current Intelligence Community and DoD implementations of Vectra AI leverage the massively enriched metadata to create rich workflows. Over the course of multiple years, customers have come to realize that the data from Vectra AI is highly accurate, regardless of the attack surface, and allows for trust in their PDP actions, policy enforcement, and enterprise security profiles.

DoD ZTA Automation & Orchestration 6.3: Machine Learning

Vectra AI is a data science and security research organization. As such, Vectra AI focuses on only one capability: detecting the known and unknown with AI/ML for incident response, correlated anomaly detection, user baseline, etc.

6.3	Machine Learning	6 - Automation and Orchestration	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement Data Tagging & Classification ML Tools

- Alone, anomaly detection is a poor approach to cyber and IR as different is not 'bad'. Many organizations mistakenly implement anomaly detection, only to have analysts/operators being overwhelmed by alerts; or poor SOAR playbooks being executed.
- Vectra AI's combination of 150+ supervised/unsupervised ML algorithms and methods correlated anomaly, privilege, behavioral baselining, and identity into 'host/user containers' vs. presenting individual detections to an operator. The result is a higher confidence and enriched incident response data.

DoD ZTA Automation & Orchestration 6.4: Artificial Intelligence (AI)

The approach to leverage AI is often misunderstood as every vendor and capability now claims to be an AI platform. The difference is in a few keys areas:

1. How is AI and ML defined? Is it recurrent neural networks and deep learning? Or merely simple 'if' lookups based on a condition.
2. How is the AI trained and the efficacy evaluated?
3. How is the AI guarded against poisoning and manipulation?

These are areas where a true data science organization, like Vectra AI, can provide the right results by examining those three questions.

6.4	Artificial Intelligence	6 - Automation and Orchestration	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement AI automation tools * AI Driven by Analytics decides A&O modifications

- With over 150 AI models and the most AI models supporting MITRE ATT&CK and D3FEND, Vectra AI provides the AI aspects for a ZTA approach.
- Vectra AI's data science & security research organizations have been using Generative AI for over 10 years to create net new attack methods to providing increased training data for the supervised and unsupervised AI/ML models. This is the only way to train for the "unknown unknown".
- Allowing the AI to provide the tier-1/tier-2 analyst work and automate the correlation of events/detections increases the efficacy of the detections provided to an operator.
- Vectra AI's ability to correlate detections into a single "host/user container" provides a 40-50% reduction in alerts being sent to the SIEM/SOAR for further correlation, improving analyst workflow and time to response metrics.

DoD ZTA Automation & Orchestration 6.5: Security Operations, Automation & Response (SOAR)

A modern SOAR platform is a key requirement for any ZTA strategy. Without both data that can be trusted to take action upon and a means to automate most workflows, an enterprise level ZTA becomes un-manageable from a process, personnel, and success criteria perspective.

6.5	Security Orchestration, Automation & Response (SOAR)	6 - Automation and Orchestration	DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	DoD organizations achieve IOC of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation	Pre-defined playbooks from collection to incident response and triage enables initial process automation that accelerates a security team's decision and response speed	* Response Automation Analysis * Implement SOAR Tools * Implement Playbooks

Vectra AI is based on an open integration and support for common SOAR platforms and custom capabilities (GOTS WALKOFF) are a key capability that Vectra AI promotes and supports:

- PEP/PDPs can only take action upon trusted and verified data. By providing highly trusted and high efficacy data into the SOAR platform, Zero Trust access and response playbooks can be created and trusted to operate correctly.
- Without a trusted data set to execute playbooks, SOAR capabilities become a hinderance to the mission and may have unintended consequences.
- Vectra AI strongly believes in the human in the loop aspects of a SOAR, providing over-ride capabilities before actions are implemented for certain environments.

DoD ZTA Automation & Orchestration 6.7: Security Operations Center (SOC) & Incident Response (IR)

The ability to provide full operational and response capabilities within the 6.7 associated activities requires full awareness and support for the environment. SIEM and SOAR alone cannot provide the response teams with the forensic data, correlation of events, and historical threat information for the contextual environment. Vectra AI's AI/ML and signature engine permit for full correlation, and then Stream of the metadata into the IR platform for rapid response.

6.7	Security Operations Center (SOC) & Incident Response (IR)	7 - Visibility and Analytics 6 - Automation and Orchestration	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	In the event a CNDSP does not exist, DoD organizations define and stand up SOCs to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility)	Standardized, coordinated, and accelerated incident response and investigative efforts	* Workflow Enrichment Pt1 * Workflow Enrichment Pt2 * Workflow Enrichment Pt3 * Automated Workflow

- Numerous organizations have begun to leverage Vectra AI's AI/ML and signature engine as the basis for their "Modern SOC" in tandem with SIEM/SOAR capabilities.
- To support the 6.7 capability ID, Vectra AI provides a single interface for SOC/IR teams to leverage to hunt, correlate responses, and monitor DoD, IC and CIV network environments.
- Vectra AI's capability supports all COA environments; from on-premises, to GovCloud and hybrid environments where users and federated identity hurdle the boundaries.

DoD ZTA Visibility & Analytics 7.1: Log All Traffic

Vectra AI's extensive ability to provide metadata and forensics information of all traffic, fully encrypted, allows for support within logging requirements. From an operator's perspective, all of the associated PCAP data with an event, correlated detections, and other requirements are visualized in a single interface. As outlined by a confidential intelligence customer, "Vectra AI provides a 7x multiplier to our teams as all of the data from 7 dispersant systems are provided in a single interface view. It eliminates the need to run queries and look into multiple systems; reducing the overall attacker dwell time."

7.1	Log All Traffic (Network, Data, Apps, Users)	7 - Visibility and Analytics	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or SOC	Foundational to the development of automated hunt and incident response playbooks	* Scale Considerations * Log Parsing * Log Analysis

Vectra AI enables a highly-enriched metadata resulting from the AI/ML and signature engine that is often viewed by US Government teams as the single best IR data source.

- Vectra AI consumes raw PCAP/network data, EDR artifacts, network enrichment data (Kerberos, LDAP, A/D, etc.), and a myriad of other sources to create a massively powerful metadata.
- Vectra Stream provides the metadata in Zeek format to allow for upstream log and event correlation and storage w/ embedded micro-PCAPs for all incidents and detections. The data can be fed into numerous sources for future archival via Zeek, JSON, syslog, and other formats.

DoD ZTA Visibility & Analytics 7.4: User and Entity Behavioral Analytics (UEBA)

The advanced analytics provided by Vectra AI and correlation of users, hosts, cloud workloads, various identity sources, and operational technology environments allow Vectra AI to provide real time UEBA capabilities. Given the correlation of detections into single events and campaigns, Vectra AI's UEBA operations result in far fewer alerts, but with greater confidence and efficacy. Confidence and efficacy are necessary for any fully orchestrated, ZTA strategy.

7.4	User and Entity Behavior Analytics	7 - Visibility and Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. CNDSPs/SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies	Advanced analytics support detection of anomalous users, devices, and NPE actions and advanced threats	* Baseline & Profiling Pt1 * Baseline & Profiling Pt2 * UEBA Baseline Support Pt1 * UEBA Baseline Support Pt2

Vectra AI provides full UEBA capabilities in addition to the 150+ AI/ML models and signature capabilities within the environment.

- Unlike most UEBA tools that trigger anomaly events to the SOC, Vectra AI correlates numerous behavioral, anomaly, identity, and host-based detection models together to provide high efficacy of the detection data and forensic correlation to reduce false positives.
- Vectra AI integrates across the ecosystem of in-place tooling and new capabilities to further enrich the metadata and provide the operators with the behavioral and peer learning data to take successful actions.

DoD ZTA Visibility & Analytics 7.6: Automated Dynamic Policies

7.6	Automated Dynamic Policies	7 - Visibility and Analytics	DoD Organization ML & AI solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	CNDSPs/SOCs dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management	Users and NPEs are denied access based on automated, real-time security profiles based on external conditions and evolving risk and confidence scores	* AI-enabled Network Access * AI-enabled Dynamic Access Control

While not the dynamic PDP, Vectra AI's enriched metadata and Zeek formatted inputs into the security tool 'stack' of a ZTA allow for real-time updates to security profiles and device configurations.

- Continuous updates of hosts and accounts/identity allow for simple enforcement of new security policies, device containment, account lockdown, honey-potting, etc. Vectra AI's AI engine, coupled with legacy signature matching permits for a continuous posture monitoring and orchestration into various Network Access Control (NAC), Comply-to-Connect (C2C) and other capabilities.

DoD Zero Trust Activities Mapping

As outlined in the earlier part of the document, Vectra AI has aligned the DOD ZTA individual activities against the offerings provided. The following table represents and engineering analysis of all 152 activities and where Vectra AI supports. Note that green cells indicate complete fulfillment, yellow cells indicate fulfillment in coordination with a technology integration, and orange indicate activities that Vectra's metadata and artifacts fulfill via integration into other tool sets.

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
1.1.1	Inventory User	1.1 User Inventory	Target Level ZT	Identified Managed Regular Users; Identified Managed Privileged Users; Identified applications using their own user account management for non-administrative and administrative accounts	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	
1.2.1	Implement App Based Permissions per Enterprise	1.2 Conditional User Access	Target Level ZT	Enterprise roles/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM; DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes; Privileged activities are fully migrated to PAM		
1.2.2	Rule Based Dynamic Access Pt1	1.2 Conditional User Access	Target Level ZT	Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes; All possible applications use JIT/JEA permissions for administrative users	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
1.2.3	Rule Based Dynamic Access Pt2	1.2 Conditional User Access	Advanced ZT	Components and services are fully utilizing rules to enable dynamic access to applications and services; Technology utilized for Rule Based Dynamic Access supports integration with AI/ML tooling	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	
1.2.4	Enterprise Gov't roles and Permissions Pt1	1.2 Conditional User Access	Advanced ZT	Component attribute and role data repository federated with enterprise ICAM; Cloud-based enterprise IdP can be used by cloud and on-premises applications; A standardized set of roles and permissions are created and aligned to attributes	Vectra AI Directly meets with observability / enforcement with native integrations to MSFT AEID / AD / EDR	
1.2.5	Enterprise Gov't roles and Permissions Pt2	1.2 Conditional User Access	Advanced ZT	Majority of components utilize cloud IdP functionality Where possible on-prem IdP is decommissioned; Permissions and roles are mandated for usage when evaluating attributes	Vectra AI Directly meets with observability / enforcement with native integrations to MSFT AEID / AD / EDR	
1.3.1	Organizational MFA/IDP	1.3 Multi-Factor Authentication (MFA)	Target Level ZT	Component is using IdP with MFA for critical applications/services; Components have implemented an Identity Provider (IdP) that enables DoD PKI multifactor authentication; Organizational Standardized PKI for critical services	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.3.2	Alternative Flexible MFA Pt1	1.3 Multi-Factor Authentication (MFA)	Advanced ZT	IdP provides user self-service alternative token; IdP provides alt token MFA for approved applications per policy		
1.3.3	Alternative Flexible MFA Pt2	1.3 Multi-Factor Authentication (MFA)	Advanced ZT	User Activity Patterns Implemented	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
1.4.1	Implement System and Migrate Privileged Users Pt1	1.4 Privileged Access Management (PAM)	Target Level ZT	Privilege Access Management (PAM) tooling is implemented; Identified applications that support and do not support PAM tools; Applications that support PAM, now use PAM for controlling emergency/built-in accounts		
1.4.2	Implement System and Migrate Privileged Users Pt2	1.4 Privileged Access Management (PAM)	Target Level ZT	Privileged activities are migrated to PAM and access is fully managed		
1.4.3	Real time Approvals & JIT/JEA Analytics Pt1	1.4 Privileged Access Management (PAM)	Advanced ZT	Identified accounts, applications, and data of concern (of greatest risk to DoD mission); Using PAM tools, applied JIT/JEA access to high-risk accounts; Privileged access requests are automated as appropriate	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	1.4 Privileged Access Management (PAM)	Advanced ZT	UEBA or similar analytic system integrated with PAM tools for JIT/ JEA account approvals	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	
1.5.1	Organizational Identity Life-Cycle Management	1.5 Identity Federation & User Credentialing	Target Level ZT	Standardized Identity Lifecycle Process	Supports via artifact via PAA detections continuously baselining and observing user behavior interacting with systems and processes	
1.5.2	Enterprise Identity Life-Cycle Management Pt1	1.5 Identity Federation & User Credentialing	Target Level ZT	Automated Identity Lifecycle Processes; Integrated with Enterprise ICAM process and tools		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
1.5.3	Enterprise Identity Life-Cycle Management Pt2	1.5 Identity Federation & User Credentialing	Advanced ZT	Integration w/ Critical IDM/IDP functions; Primary ILM functions are cloud based		
1.5.4	Enterprise Identity Life-Cycle Management Pt3	1.5 Identity Federation & User Credentialing	Advanced ZT	All ILM functions moved to cloud as appropriate; Integration with all IDM/IDP functions		
1.6.1	Implement User & Entity Behavior Activity (UEBA) Tooling	1.6 Behavioral, Contextual ID, and Biometrics	Target Level ZT	UEBA functionality is implemented for Enterprise IDP	Vectra AI directly meets full behavioral activity monitoring for both hosts and users	
1.6.2	User Activity Monitoring Pt1	1.6 Behavioral, Contextual ID, and Biometrics	Advanced ZT	UEBA is integrated with Org IDPs as appropriate; UEBA is integrated with JIT/JEA for critical services	Vectra AI directly meets full behavioral activity monitoring for both hosts and users	
1.6.3	User Activity Monitoring Pt2	1.6 Behavioral, Contextual ID, and Biometrics	Advanced ZT	UEBA/Entity Monitoring is integrated with JIT/JEA for all services	Vectra AI directly meets full behavioral activity monitoring for both hosts and users	
1.7.1	Deny User by Default Policy	1.7 Least Privileged Access	Target Level ZT	Applications updated to deny by default to functions/data requiring specific roles/attributes for access; Reduced default permissions levels are implemented; Applications/services have reviewed/audited all privileged users and removed those users who do not need that level of access; Applications' identify functions and data requiring specific roles/attributes for access	Vectra AI directly meets determination of "Observed Privilege" via unsupervised AI/ML	
1.8.1	Single Authentication	1.8 Continuous Authentication	Target Level ZT	Authentication implemented across applications per session	Supports via artifact(s) in post-processed metadata in SIEM/syslog	Microsoft*, Duo, Ubikey

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
1.8.2	Periodic Authentication	1.8 Continuous Authentication	Target Level ZT	Authentication implemented multiple times per session based on security attributes	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.8.3	Continuous Authentication Pt1	1.8 Continuous Authentication	Advanced ZT	Transaction authentication implemented per session based on security attributes	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.8.4	Continuous Authentication Pt2	1.8 Continuous Authentication	Advanced ZT	Transaction authentication implemented per session based on security attributes	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.9.1	Enterprise PKI/IDP Pt1	1.9 Integrated ICAM Platform	Target Level ZT	Components are using IdP with MFA for all applications/services; Organizational MFA/PKI integrated with Enterprise MFA/PKI; Organizational Standardized PKI for all services	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.9.2	Enterprise PKI/IDP Pt2	1.9 Integrated ICAM Platform	Advanced ZT	Critical Organizational Services Integrated w/ Biometrics; Decommission organizational MFA/PKI as appropriate in leu of enterprise MFA/PKI; Enterprise Biometric Functions Implemented	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
1.9.3	Enterprise PKI/IDP Pt3	1.9 Integrated ICAM Platform	Advanced ZT	All Organizational Services Integrate w/ Biometrics		
2.1.1	Device Health Tool Gap Analysis	2.1 Device Inventory	Target Level ZT	Manual inventory of devices is created per organization w/ owners	Vectra AI meets with native integration by creating "HostID container" with observered characteristics and integrated artifacts for all systems connected to networks	
2.1.2	NPE/PKI, Device under Management	2.1 Device Inventory	Target Level ZT	Non-person entities are managed via Org PKI and Org IDP	Supports via artifact(s) in post-processed metadata in SIEM/syslog	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
2.1.3	Enterprise IDP Pt1	2.1 Device Inventory	Target Level ZT	NPEs including devices are integrated with Enterprise IDP	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
2.1.4	Enterprise IDP Pt2	2.1 Device Inventory	Advanced ZT	Conditional device attributes are part of the IdP profile	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
2.2.1	Implement C2C/ Compliance Based Network Authorization Pt1	2.2 Device Detection and Compliance	Target Level ZT	C2C Rollout starts at the enterprise level for low risk and testing environments; Basic devices checks are implemented using C2C	Supports via artifact(s) in post-processed metadata in SIEM/syslog	Forescout*, Cisco ISE, Aruba ClearPass*
2.2.2	Implement C2C/ Compliance Based Network Authorization Pt2	2.2 Device Detection and Compliance	Advanced ZT	C2C is rolled out to all supported environments; Advanced devices checks are completed and integrated with dynamic access (Enterprise IDP / ZTNA)	Supports via artifact(s) in post-processed metadata in SIEM/syslog	
2.3.1	Entity Activity Monitoring Pt1	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	UEBA attributes are integrated for device baselining; UEBA attributes are available for usage with device access	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog	
2.3.2	Entity Activity Monitoring Pt2	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	UEBA attributes are mandated for device access	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog	
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	AppControl and FIM tooling is implemented on all critical services/applications; EDR tooling covers maximum amount of services/applications; AppControl and FIM data is sent to C2C as needed	Vectra AI meets with native integraionts by creating "HostID container"and attributing any potentially adverse activity to this HostID as well as provided post-process enriched metadata to ensure full compliance of posture	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
2.3.4	Integrate NextGen AV Tools with C2C	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	Critical NextGen AV data is being sent to C2C for checks ; NextGen AV tooling is implemented on all critical services/applications	Vectra AI meets with native integrations by creating "HostID container"and attributing any potentially adverse activity to this HostID as well as provided post-process enriched metadata to ensure full compliance of posture	
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	AppControl and FIM deployment is expanded to all necessary services/applications; Remaining data from Device Security tooling is implemented with C2C		
2.3.6	Enterprise PKI Pt1	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	Devices that are unable to have certificates are phased out and/ or moved to minimal access environments; All devices and NPEs have certs installed for authentication in the Enterprise PKI	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog	
2.3.7	Enterprise PKI Pt2	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	Devices are required to authenticate to communicate with other services and devices	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog	
2.4.1	Deny Device by Default Policy	2.4 Remote Access	Target Level ZT	Components can block device access by default to resources (apps/data) and explicitly allow compliant devices per policy; Remote Access is enabled following a "deny device by default policy" approach	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog and further via SOAR integration with native EDR integration	
2.4.2	Managed and Limited BYOD & IOT Support	2.4 Remote Access	Target Level ZT	All applications require dynamic permissions access for devices; BYOD and IOT device permissions are baselined and integrated with Enterprise IDP	Vectra AI meets with native integrations by creating "HostID container"and attributing any potentially adverse activity to this HostID as well as provided post-process enriched metadata to ensure full compliance of posture	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
2.4.3	Managed and Full BYOD & IOT Support Pt1	2.4 Remote Access	Advanced ZT	Only BYOD and IOT devices that meet mandated configuration standards allowed to access resources; Critical Services require dynamic access for devices	Vectra AI meets with native integrations by creating "HostID container"and attributing any potentially adverse activity to this HostID as well as provided post-process enriched metadata to ensure full compliance of posture	
2.4.4	Managed and Full BYOD & IOT Support Pt2	2.4 Remote Access	Advanced ZT	All possible services require dynamic access for devices	Vectra AI meets with native integrations by creating "HostID container"and attributing any potentially adverse activity to this HostID as well as provided post-process enriched metadata to ensure full compliance of posture	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	Target Level ZT	Components can confirm if devices meet minimum compliance standards or not; Components have asset management, vulnerability, and patching systems with APIs that will enable integration across the systems	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog and further via SOAR integration with native EDR integration	
2.6.1	Implement UEDM or equivalent Tools	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Components can confirm if devices meet minimum compliance standards or not; Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoD enterprise; Components asset management systems can programmatically, ie, API, provide device compliance status and if it meets minimum standards	Supports via artifact(s) and enforcement in post-processed metadata in SIEM/syslog and further via SOAR integration with native EDR integration	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
2.6.2	Enterprise Device Management Pt1	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Manual inventory is integrated with an automated management solution for critical services; Enable ZT Device Management (from any location with or without remote access)		
2.6.3	Enterprise Device Management Pt2	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Manual inventory is integrated with an automated management solution for all services		
2.7.1	Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Target Level ZT	Endpoint Detection & Response Tooling is implemented ; Critical EDR data is being sent to C2C for checks; NextGen AV tooling covers maximum amount of services/ applications	Vectra AI meets with native integration and supports C2C integration and orchestration, providing the high confidence, correlated events via AI to ensure C2C actions are properly trained and executed. Vectra's alliance and native orchestration with primary EDR vendors permits for correlated detection data and learnings.	
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Target Level ZT	Integration Points have been identified per Capability; Riskiest integration points have been integrated w/ XDR; Basic alerting is in place with SIEM and/or other mechanisms	Vectra AI meets with native integration via assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Advanced ZT	Remaining integration points have been integrate as appropriate; Extended alerting and response is enabled with other Analytics tools at least using SIEM	Supports via artifact(s) in post-processed metadata in SIEM/syslog and further via SOAR integration with native EDR integration	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
3.1.1	Application/Code Identification	3.1 Application Inventory	Target Level ZT	Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted		
3.4.1	Resource Authorization Pt1	3.4 Resource Authorization & Integration	Target Level ZT	Resource Authorization Gateway is in place for external facing applications; Resource Authorization policy integrated with identity and device; Enterprise-wide Guidance on conversion standards are communicated to stakeholders		
3.4.2	Resource Authorization Pt2	3.4 Resource Authorization & Integration	Target Level ZT	Resource Authorization gateway is utilized for all applications; Resource Authorization is integrated with DevSecOps and CI/CD for automated functions		
3.2.1	Build DevSecOps Software Factory Pt1	3.2 Secure Software Development & Integration	Target Level ZT	Developed Data/Service Standards for DevSecOps; CI/CD Pipeline is fully functional and tested successfully; Vulnerability Management program is officially in place and operating		
3.2.2	Build DevSecOps Software Factory Pt2	3.2 Secure Software Development & Integration	Target Level ZT	Development of applications is migrated to CI/CD pipeline; Continual validation process/technology is implemented and in use; Development of applications is migrated to DevSecOps process and technology		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
3.2.3	Automate Application Security & Code Remediation Pt1	3.2 Secure Software Development & Integration	Advanced ZT	Secure API Gateway is operational and majority of API calls are passing through gateway; Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps		
3.2.4	Automate Application Security & Code Remediation Pt2	3.2 Secure Software Development & Integration	Advanced ZT	Services are provided following a Service Oriented Architecture (SOA); Security Remediation activities (e.g., runtime security, library updates, release approvals) are fully automated		
3.3.1	Approved Binaries/Code	3.3 Software Risk Management	Target Level ZT	Supplier sourcing risk evaluated and identified for approved sources; Repository and update channel established for use by development teams; Bill of Materials is created for applications identify source, supportability and risk posture; Industry standard (DIB) and approved vulnerability databases are pulled in to be used in DevSecOps		
3.3.2	Vulnerability Management Program Pt1	3.3 Software Risk Management	Target Level ZT	Vulnerability Management Team is in place w/ appropriate stakeholder membership; Vulnerability Management policy and process is in place and agreed to w/ stakeholders; Public source of vulnerabilities are being utilized for tracking	Vectra AI meets with native integrations and the Vectra AI Math Suricata engine that allows for known bad vulnerability and methods to be properly detected in real-time and alerted.	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
3.3.3	Vulnerability Management Program Pt2	3.3 Software Risk Management	Target Level ZT	Controlled (e.g., DIB, CERT) sources of vulnerabilities are being utilized for tracking; Vulnerability management program has a process for accepting external/ public disclosures for managed services		
3.3.4	Continual Validation	3.3 Software Risk Management	Target Level ZT	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned; Continual validation tools are implemented and applied to code in the CI/CD pipeline; Code requiring continuous validation is identified and validation criteria are established		
3.4.3	SDC Resource Authorization Pt1	3.4 Resource Authorization & Integration	Target Level ZT	Applications unable to be updated to use approved binaries/code are marked for retirement and transition plans are created; Identified applications without approved binaries and code are updated to use approved binaries/ code; Enterprise-wide Guidance on conversion standards are communicated to stakeholders		
3.4.4	SDC Resource Authorization Pt2	3.4 Resource Authorization & Integration	Target Level ZT	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
3.4.5	Enrich Attributes for Resource Authorization Pt1	3.4 Resource Authorization & Integration	Advanced ZT	Most API calls are passing through the Secure API Gateway; Resource Authorization receives data from Analytics Engine; Authorization policies incorporate identified attributes in making authorization decisions; Attributes to be used for initial enrichment are identified; Identified attributes are assigned to resources and/or entities		
3.4.6	Enrich Attributes for Resource Authorization Pt2	3.4 Resource Authorization & Integration	Advanced ZT	Authorization policies incorporate confidence levels in making authorization decisions; Confidence levels for attributes are defined		
3.4.7	REST API Micro-Segments	3.4 Resource Authorization & Integration	Advanced ZT	Approved Enterprise APIs are Micro-Segmented appropriately		
3.5.1	Continuous Authorization to Operate (cATO) Pt1	3.5 Continuous Monitoring and Ongoing Authorizations	Advanced ZT	Controls derivation is standardized and ready for automation; Controls testing is integrated with DevSecOps processes and technology		
3.5.2	Continuous Authorization to Operate (cATO) Pt2	3.5 Continuous Monitoring and Ongoing Authorizations	Advanced ZT	Controls testing is fully automated; Integration with standard IR and SOC operations is automated; Control derivation and applicability is fully automated; Dashboards are used to track continuing authorization status		
4.1.1	Data Analysis	4.1 Data Catalog Risk Alignment	Target Level ZT	The service catalog is updated with data types for each application and service based on data classification levels		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
4.2.1	Define Data Tagging Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	Enterprise data classification and tagging standards are developed; Organizations align to enterprise standards and begin implementation		
4.2.2	Interoperability Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	Formal standards are in place by the Enterprise for the appropriate data standards		
4.2.3	Develop Software Defined Storage (SDS) Policy	4.2 DoD Enterprise Data Governance	Target Level ZT	Determine need for SDS tool implementation; Policy for SDS is created at the enterprise and org levels		
4.3.1	Implement Data Tagging & Classification Tools	4.3 Data Labeling and Tagging	Target Level ZT	A requirement of Data classification and tagging tools must include integration and/or support of Machine Learning (ML); Data classification and tagging tools are implemented at org and enterprise levels		
4.3.2	Manual Data Tagging Pt1	4.3 Data Labeling and Tagging	Target Level ZT	Manual data tagging begins at the enterprise level with basic attributes		
4.3.3	Manual Data Tagging Pt2	4.3 Data Labeling and Tagging	Advanced ZT	Manual data tagging is expanded to the program/org levels with specific attributes		
4.3.4	Automated Data Tagging & Support Pt1	4.3 Data Labeling and Tagging	Advanced ZT	Basic automation begins by scanning data repositories and applying tags		
4.3.5	Automated Data Tagging & Support Pt2	4.3 Data Labeling and Tagging	Advanced ZT	Full automation of data tagging is completed; Results of data tagging are fed into ML algorithms to develop AI driven data tagging		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
4.4.1	DLP Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Target Level ZT	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels		
4.4.2	DRM Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Target Level ZT	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels		
4.4.3	File Activity Monitoring Pt1	4.4 Data Monitoring and Sensing	Target Level ZT	Data and files of critical classification are actively being monitored; Basic Integration is in place with monitoring system such as the SIEM	Vectra AI meets with native integration and provides AI/ ML models associated with file enumeration, data gathering, and data smuggling. In coordination with a traditional DLP solution, Vectra AI's AI engine alerts of acess allow for greater visibility and AI generated behaviors associated with malicious intent.	
4.4.4	File Activity Monitoring Pt2	4.4 Data Monitoring and Sensing	Target Level ZT	Data and files of all regulated classifications are actively being monitored; Extended integrations are in place as appropriate to further manage risk	Vectra AI meets with native integration and provides AI/ ML models associated with file enumeration, data gathering, and data smuggling. In coordination with a traditional DLP solution, Vectra AI's AI engine alerts of acess allow for greater visibility and AI generated behaviors associated with malicious intent.	
4.4.5	Database Activity Monitoring	4.4 Data Monitoring and Sensing	Advanced ZT	Appropriate Database are being actively monitored; Monitoring technology is integrated with solutions such as SIEM, PDP and Dynamic Access Control mechanisms	Vectra AI meets with native integration via HostID visibility of any potentially malicious / adverse interaction with specific high-value database (or other) systems.	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
4.4.6	Comprehensive Data Activity Monitoring	4.4 Data Monitoring and Sensing	Advanced ZT	Data Activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories; Appropriate integrations exist with solutions such as SIEM and PDP		
4.5.1	Implement DRM and Protection Tools Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	DRM and protection tools are enabled for high risk data repositories with basic protections		
4.5.2	Implement DRM and Protection Tools Pt2	4.5 Data Encryption & Rights Management	Target Level ZT	DRM and protection tools are enabled for possible repositories		
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	Data Tags are integrated with DRM and monitored repositories are expanded; Based on data tags, data is encrypted at rest		
4.5.4	DRM Enforcement via Data Tags and Analytics Pt2	4.5 Data Encryption & Rights Management	Advanced ZT	All applicable data repositories are protected using DRM; Data is encrypted using extended data tags from the org levels		
4.5.5	DRM Enforcement via Data Tags and Analytics Pt3	4.5 Data Encryption & Rights Management	Advanced ZT	Analytics from ML/AI are integrated with DRM to better automate protections; Encryption protection is integrated with AI/ML and updated encryption methods are used as needed		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
4.6.1	Implement Enforcement Points	4.6 Data Loss Prevention (DLP)	Target Level ZT	Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging	Vectra AI meets with native integration and provides AI/ ML models associated with file enumeration, data gathering, and data smuggling. In coordination with a traditional DLP solution, Vectra AI's AI engine alerts of acess allow for greater visibility and AI generated behaviors associated with malicious intent.	
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	4.6 Data Loss Prevention (DLP)	Target Level ZT	Enforcement Points to set to prevent mode integrating the logging schema and manual tags		
4.6.3	DLP Enforcement via Data Tags and Analytics Pt2	4.6 Data Loss Prevention (DLP)	Advanced ZT	Enforcement points have extended data tag attributes applied for additional prevention		
4.6.4	DLP Enforcement via Data Tags and Analytics Pt3	4.6 Data Loss Prevention (DLP)	Advanced ZT	Automated tagging attributes are integrated with DLP and resulting metrics are used for ML		
4.7.1	Integrate DAAS Access w/ SDS Policy Pt1	4.7 Data Access Control	Target Level ZT	DAAS policy is developed w/ enterprise and org level support; SDS Integration plan is developed to support DAAS policy		
4.7.2	Integrate DAAS Access w/ SDS Policy Pt2	4.7 Data Access Control	Advanced ZT	DAAS Policy implemented in an automated fashion		
4.7.3	Integrate DAAS Access w/ SDS Policy Pt3	4.7 Data Access Control	Advanced ZT	SDS is integrated with DAAS policy functionality		
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	4.7 Data Access Control	Target Level ZT	Integration plan with SDS is developed to support existing DAAS access		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
4.7.5	Integrate Solution(s) and Policy with Enterprise IDP Pt2	4.7 Data Access Control	Advanced ZT	If needed implement SDS tooling and integrate with Enterprise IDP to support existing DAAS access		
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	4.7 Data Access Control	Advanced ZT	If tooling is needed ensure there is supported integrations with DLP, DRM and ML tooling		
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	4.7 Data Access Control	Advanced ZT	Integrate SDS infrastructure with existing DLP and DRM infrastructure		
5.1.1	Define Granular Control Access Rules & Policies Pt1	5.1 Data Flow Mapping	Target Level ZT	Provide Technical Standards; Develop Concept of Operations; Identify Communities of Interest		
5.1.2	Define Granular Control Access Rules & Policies Pt2	5.1 Data Flow Mapping	Target Level ZT	Define Data Tagging Filters for API Infrastructure		
5.2.1	Define SDN APIs	5.2 Software Defined Networking (SDN)	Target Level ZT	SDN APIs are standardized and implemented; APIs are functional for AuthN Decision Point, App Delivery Control Proxy and Segmentation Gateways		
5.2.2	Implement SDN Programable Infrastructure	5.2 Software Defined Networking (SDN)	Target Level ZT	Implemented Application Delivery Control Proxy; Established SIEM Logging Activities; Implemented User Activity Monitoring (UAM); Integrated with Authentication Decision Point; Implemented Segmentation Gateways	Vectra AI supports via artifact as the capability works with the PDP aspects of the ZTA plan and acts as the analytics integration for real time decision making and SDN orchestration: Vectra AI's integration into the other ZTA stack via API 2.0 capabilities allow for orchestration (SOAR) and SDN controller level decisions to be executed upon. SDN is not a capability of Vectra AI, however supporting SDN micro-segmentation and orchestration based on the AI/ML and signature contextual outcomes of Vectra AI exists	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
5.2.3	Segment Flows into Control, Management, and Data Planes	5.2 Software Defined Networking (SDN)	Target Level ZT	IPv6 Segmentation; Enable Automated NetOps Information Reporting; Ensure Configuration Control Across Enterprise; Integrated with SOAR		
5.2.4	Network Asset Discovery & Optimization	5.2 Software Defined Networking (SDN)	Advanced ZT	Technical Refreshment/Technology Evolution; Provide Optimization/ Performance Controls		
5.2.5	Real-Time Access Decisions	5.2 Software Defined Networking (SDN)	Advanced ZT	Analyze SIEM Logs with Analytics Engine to Provide Real-Time Policy Access Decisions; Support Sending Captured Packets, Data/ Network Flows, and other Specific Logs for Analytics; Segment End-to-End Transport Network Flows; Audit Security Policies for Consistency across Enterprise; Protect Data-in-Transit During Coalition Information Sharing	Vectra AI supports via artifacts vis providing real-time visibility of potential adverse actions taken across any observed system(s) on a network as well as the full complement of post-proces AI/ML enhanced metadata for all network activity via SIEM	
5.3.1	Datacenter Macrosegmentation	5.3 Macro Segmentation	Target Level ZT	Log Actions to SIEM; Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Analyze Activities with Analytics Engine	Vectra AI supports via artifact by providing real-time visibility of potential adverse actions taken across any observed system(s) on a network as well as the full complement of post-proces AI/ML enhanced metadata for all network activity via SIEM	
5.3.2	B/C/P/S Macrosegmentation	5.3 Macro Segmentation	Target Level ZT	Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Log Actions to SIEM; Analyze Activities with Analytics Engine; Leverage SOAR to Provide RT Policy Access Decisions		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
5.4.1	Implement Microsegmentation	5.4 Micro Segmentation	Target Level ZT	Accept Automated Policy Changes; Implement API Decision Points; Implement NGF/Micro FW/ Endpoint Agent in Virtual Hosting Environment		
5.4.2	Application & Device Microsegmentation	5.4 Micro Segmentation	Target Level ZT	Assign Role, Attribute, & Condition Based Access Control to User & Devices; Provide Privileged Access Management Services; Limit Access on Per Identity Basis for User & Device; Create Logical Network Zones; Support Policy Control via REST API		
5.4.3	Process Microsegmentation	5.4 Micro Segmentation	Advanced ZT	Segment Host-Level Processes for Security Policies; Support Real-Time Access Decisions and Policy Changes; Support Offload of Logs for Analytics and Automation; Support Dynamic Deployment of Segmentation Policy		
5.4.4	Protect Data In Transit	5.4 Micro Segmentation	Target Level ZT	Protect Data In Transit During Coalition Information Sharing; Protect Data in Transit Across System High Boundaries; Integrate Data In Transit Protection Across Architecture Components		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
6.1.1	Policy Inventory & Development	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Policies have been collected in reference to applicable compliance and risk (eg RMF, NIST); Policies have been reviewed for missing Pillars and Capabilities per the ZTRA; Missing areas of policies are updated to meet the capabilities per ZTRA	Vectra AI supports via artifacts as the capability is not a primary Policy Decision Point (PDP), but provides the high efficacy data points necessary for a PDP to make informed decisions and coordinate for orchestration. Current Intelligence Community and DoD implementations of Vectra AI leverage the massively enriched metadata to create rich workflows. Over the course of multiple years, customers have come to realize that the data from Vectra AI is highly accurate, regardless of the attack surface, and allows for trust in their PDP actions, policy enforcement, and enterprise security profiles.	
6.1.2	Organization Access Profile	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device pillars; Initial enterprise profile access standard is developed for access to DAAS ; When possible the organization profile(s) utilizes enterprise available services in the User, Data, Network and Device pillars; Organization Mission/Task critical profile(s) are created		
6.1.3	Enterprise Security Profile Pt1	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Enterprise Profile(s) are created to access DAAS using capabilities from User, Data, Network and Device Pillars; Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
6.1.4	Enterprise Security Profile Pt2	6.1 Policy Decision Point (PDP) & Policy Orchestration	Advanced ZT	Enterprise Profile(s) have been reduced and simplified to support widest array of access to DAAS; Where appropriate Mission/ Task Critical profile(s) have been integrated and supported Organization profiles are considered the exception		
6.2.1	Task Automation Analysis	6.2 Critical Process Automation	Target Level ZT	Automatable tasks are identified; Tasks are enumerated		
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	6.2 Critical Process Automation	Target Level ZT	Implement full enterprise integration; Identify key integrations; Identify recovery and protection requirements		
6.2.3	Enterprise Integration & Workflow Provisioning Pt2	6.2 Critical Process Automation	Advanced ZT	Services identified; Service provisioning is implemented		
6.3.1	Implement Data Tagging & Classification ML Tools	6.3 Machine Learning	Target Level ZT	Implemented data tagging and classification tools are integrated with ML tools	Vectra AI directly meets and is a data science and security research organization. As such, Vectra AI focuses on only one capability: detecting the known and unknown with AI/ML for incident response, correlated anomaly detection, user baseline, etc.	
6.4.1	Implement AI automation tools	6.4 Artificial Intelligence	Advanced ZT	Develop AI Tool Requirements; Procure and Implement AI Tools	Vectra AI directly meets and is a data science and security research organization. As such, Vectra AI focuses on only one capability: detecting the known and unknown with AI/ML for incident response, correlated anomaly detection, user baseline, etc.	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
6.4.2	AI Driven by Analytics decides A&O modifications	6.4 Artificial Intelligence	Advanced ZT	AI is able to make changes to automated workflow activities	Vectra AI supports via artifact producer which can be used to initiate or as part of a SOAR workflow	
6.5.1	Response Automation Analysis	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	Automatable response activities are identified; Response activities are enumerated		
6.5.2	Implement SOAR Tools	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	Develop requirements for SOAR tool; Procure SOAR tools		
6.5.3	Implement Playbooks	6.5 Security Orchestration, Automation & Response (SOAR)	Advanced ZT	When possible automated playbooks based on automated workflows capability; Manual Playbooks are developed and implemented	Vectra AI supports via artifact producer which can be used to initiate or as part of a SOAR workflow	
6.6.1	Tool Compliance Analysis	6.6 API Standardization	Target Level ZT	API status is determined compliance or non-compliance to API standards; Tools to be used are Identified		
6.6.2	Standardized API Calls & Schemas Pt1	6.6 API Standardization	Target Level ZT	Initial calls and schemas are implemented; Non-compliant tools are replaced		
6.6.3	Standardized API Calls & Schemas Pt2	6.6 API Standardization	Target Level ZT	All calls and schemas are implemented		
6.7.1	Workflow Enrichment Pt1	6.7 Security Operations Center (SOC) & Incident Response (IR)	Target Level ZT	Threat events are identified; Workflows for threat events are developed	Vectra AI meets with native integration via assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
6.7.2	Workflow Enrichment Pt2	6.7 Security Operations Center (SOC) & Incident Response (IR)	Target Level ZT	Workflows for Advanced threat events are developed; Advanced Threat events are identified	Vectra AI supports via artifacts and post-process AI/ML enhanced metadata sent to SIEM / syslog and/or Detection information used to initiate or as part of SOAR workflows	
6.7.3	Workflow Enrichment Pt3	6.7 Security Operations Center (SOC) & Incident Response (IR)	Advanced ZT	Enrichment data has been identified; Enrichment data is integrated into workflows	Vectra AI supports via artifacts and post-process AI/ML enhanced metadata sent to SIEM / syslog and/or Detection information used to initiate or as part of SOAR workflows	
6.7.4	Automated Workflow	6.7 Security Operations Center (SOC) & Incident Response (IR)	Advanced ZT	Workflow processes are fully automated; Manual Processes have been identified; Remaining Processes are marked as exceptions and documented	Vectra AI supports via artifacts and post-process AI/ML enhanced metadata sent to SIEM / syslog and/or Detection information used to initiate or as part of SOAR workflows	
7.1.1	Scale Considerations	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Sufficient infrastructure in place; Distributed environment established; Sufficient bandwidth for network traffic		
7.1.2	Log Parsing	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Standardized log formats; Rules developed for each log format	Vectra AI directly meets realted to network and certain user data as the capability enables a highly-enriched metadata resulting from the AI/ML and signature engine that is often viewed by US Government teams as the single best IR data source.	
7.1.3	Log Analysis	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Develop analytics per activity; Identify activities to analyze	Vectra AI directly meets related to network and certain user data as the capability highlights potentially malicious / adverse activities and associates these with systems or users providing supporting information for easier analysis to lower the time to remediate or triage	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
7.2.1	Threat Alerting Pt1	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Rules developed for threat correlation	Vectra AI direcly meets as a network threat detection capability that supports sending all detection infromation as well as post-proccess AI/ML enhanced information to a SIEM	
7.2.2	Threat Alerting Pt2	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Develop analytics to detect deviations	Vectra AI directly meets and is a data science and security research organization. As such, Vectra AI focuses on only one capability: detecting the known and unknown with AI/ML for incident response, correlated anomaly detection, user baseline, etc.	
7.2.3	Threat Alerting Pt3	7.2 Security Information and Event Management (SIEM)	Advanced ZT	Identify Triggering Anomalous Events; Implement Triggering Policy	Vectra AI supports via artifact(s) and assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
7.2.4	Asset ID & Alert Correlation	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Rules developed for asset ID based responses	Vectra AI supports via artifact(s) and assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
7.2.5	User/Device Baselines	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Identify user and device baselines	Vectra AI supports via artifact(s) and assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
7.3.1	Implement Analytics Tools	7.3 Common Security and Risk Analytics	Target Level ZT	Develop requirements for analytic environment; Procure and implement analytic tools		

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
7.3.2	Establish User Baseline Behavior	7.3 Common Security and Risk Analytics	Target Level ZT	Identify users for baseline; Establish ML-based baselines	Vectra AI directly meets via assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
7.4.1	Baseline & Profiling Pt1	7.4 User and Entity Behavior Analytics	Target Level ZT	Develop analytics to detect changing threat conditions; Identify user and device threat profiles	Vectra AI directly meets via assigning Threat and Certainty scores for all entities observed on the network and more granular assigns Threat and Certainty score for detections	
7.4.2	Baseline & Profiling Pt2	7.4 User and Entity Behavior Analytics	Advanced ZT	Add threat profiles for IoT and OT devices; Develop and extend analytics; Extend threat profiles to individual users and devices	Vectra AI directly meets and provides full UEBA capabilities in addition to the 150+ AI/ML models and signature capabilities within the environment. Unlike most UEBA tools that trigger anomaly events to the SOC, Vectra AI correlates numerous behavioral, anomaly, identity, and host-based detection models together to provide high efficacy of the detection data and forensic correlation to reduce false positives. Vectra AI integrate across the ecosystem of in-place tooling and new capabilities to further enrich the metadata and provide the operators with the behavioral and peer learning data to take successful actions.	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
7.4.3	UEBA Baseline Support Pt1	7.4 User and Entity Behavior Analytics	Advanced ZT	Implement ML-based Analytics to detect anomalies	Vectra AI directly meets and provides full UEBA capabilities in addition to the 150+ AI/ML models and signature capabilities within the environment. Unlike most UEBA tools that trigger anomaly events to the SOC, Vectra AI correlates numerous behavioral, anomaly, identity, and host-based detection models together to provide high efficacy of the detection data and forensic correlation to reduce false positives. Vectra AI integrate across the ecosystem of in-place tooling and new capabilities to further enrich the metadata and provide the operators with the behavioral and peer learning data to take successful actions.	
7.4.4	UEBA Baseline Support Pt2	7.4 User and Entity Behavior Analytics	Advanced ZT	Implement ML-based Analytics to detect anomalies	Vectra AI directly meets and provides full UEBA capabilities in addition to the 150+ AI/ML models and signature capabilities within the environment. Unlike most UEBA tools that trigger anomaly events to the SOC, Vectra AI correlates numerous behavioral, anomaly, identity, and host-based detection models together to provide high efficacy of the detection data and forensic correlation to reduce false positives. Vectra AI integrate across the ecosystem of in-place tooling and new capabilities to further enrich the metadata and provide the operators with the behavioral and peer learning data to take successful actions.	

ID#	Activity Name	Associated Capability	Phase	Outcomes	Vectra AI directly meets / meets with native integration / supports via artifact	Vectra AI Technology Alliance Partners (* indicates native integration)
7.5.1	Cyber Threat Intelligence Program Pt1	7.5 Threat Intelligence Integration	Target Level ZT	Cyber Threat Intelligence team is in place with critical stakeholders; Public and Baseline CTI feeds are being utilized by SIEM for alerting; Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, NG-IPS)	Vectra AI meets with native integrations and is able to integrate with various Threat Intel feeds and / or produce information which can be used for the creation / enrichment of such feeds.	
7.5.2	Cyber Threat Intelligence Program Pt2	7.5 Threat Intelligence Integration	Target Level ZT	Cyber Threat Intelligence team is in place with extended stakeholders as appropriate; Controlled and Private feed are being utilized by SIEM and other appropriate Analytics tools for alerting and monitoring; Integration is in place for extended enforcement points within the Device, User, Network and Data pillars (UEBA, UAM)	Vectra AI meets with native integrations is able to integrate with various Threat Intel feeds and / or produce information which can be used for the creation / enrichment of such feeds.	
7.6.1	AI-enabled Network Access	7.6 Automated Dynamic Policies	Advanced ZT	Network Access is AI driven based on environment analytics	Vectra AI supports via artifacts as the capability's AI/ML engines can produce information / artifacts which can further feed Access Control systems	
7.6.2	AI-enabled Dynamic Access Control	7.6 Automated Dynamic Policies	Advanced ZT	JIT/JEA are integrated with AI; Access is AI driven based on environment analytics	Vectra AI meets with native integrations as the capability is not the full dynamic PDP, Vectra's enriched metadata and Zeek formatted inputs into the security tool 'stack' of a ZTA allow for real-time updates to security profiles and device configurations.	

For more information please contact us: Email: info@vectra.ai | vectra.ai