VECTRA
SECURITY THAT THINKS.®

COMPLIANCE BRIEF

How Cognito from Vectra helps meet FFIEC cybersecurity requirements

FFIEC

To combat the increasing volume and sophistication of cyberthreats, the Federal Financial Institutions Examination Council (FFIEC), in conjunction with the National Institute of Standards and Technology (NIST), developed the Cybersecurity Assessment Tool to help institutions identify risk and determine their cybersecurity preparedness.

The Cybersecurity Assessment Tool provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time. Financial institutions can use the tool's inherent risk profile to categorize risk from areas of most concern to least.

After the inherent risks are scored, the next step determines the financial institution's overall maturity level. As defined by the FFIEC, cybersecurity maturity has five sub-levels: (1) Baseline, (2) Evolving, (3) Intermediate, (4) Advanced, and (5) Innovative.

It includes five domains to determine if the institution's behaviors, practices, and processes support cybersecurity preparedness. The five domains are (1) Cyber Risk Management and Oversight, (2) Threat Intelligence and Collaboration, (3) Cybersecurity Controls, (4) External Dependency Management, and (5) Cyber Incident Management and Resilience.

- **Domain 1** – Cyber Risk Management and Oversight: Oversees the board of director's oversight and management's development and implementation of an effective enterprise. Assessment factors focus on governance, risk management, resources, and training and culture.

Vectra Cognito monitors high-privilege credentials, administrative protocol-realm usage, and how internal users gather/store data from key assets in the network.

- **Domain 2** – Threat Intelligence and Collaboration: The processes to positively discover, analyze and understand threats with the ability to share information internally. Assessment factors include threat intelligence, monitoring and analyzing, and information sharing.

- **Domain 3** – Cybersecurity Controls: Methods used to protect assets, infrastructure and information by reinforcing the institution's defenses through continuous protection and monitoring. Assessment factors target preventive controls, detective controls, and corrective controls.

- **Domain 4** – External Dependency Management: Establishes and maintains a comprehensive program to oversee external connections and external dependencies with access to the financial institution's assets and information. Assessment factors focus on connections and relationship management.

- **Domain 5** – Cyber Incident Management and Resilience: Establishes, identifies and analyzes cyber events. Prioritizes containment and escalates information to stakeholders. Resilience involves planning and testing to maintain and recover ongoing operations. Assessment factors include incident resilience planning and strategy, detection, response, mitigation, and escalation and reporting.

Each domain starts at the Baseline maturity and gradually increases to Innovative:

- **Baseline:** At this level, management reviews and evaluates guidelines.

- **Evolving:** At this level, additional procedures and policies are set with risk-driven objectives. Cybersecurity is increased to include information assets and systems.

- **Intermediate:** At this level, detailed processes occur, controls remain consistent, and risk management is integrated into business strategies.

- **Advanced:** Cybersecurity practices and analytics are included in all businesses. There is also continuous improvement in riskmanagement processes.

- **Innovative:** There is a driving innovation in the people, processes and technology in the institution in managing cyber risks, such as making new tools, new controls or new information-sharing groups.

FFIEC Cybersecurity Assessment categories supported by the Cognito™ threat detection and response platform from Vectra® are detailed in the following tables.

FFIEC Cybersecurity Assessment		How Cognito Helps
D2.MA.MA.E	Monitoring systems operate continuously with adequate support for efficient incident handling.	The highest-risk threats are instantly triaged, correlated to hosts and prioritized so security teams can respond faster to stop in-progress attacks and avert data loss. By automating the manual, time-consuming analysis of security events, Vectra Cognito condenses weeks or months of work into minutes and reduces the security analyst workload on threat investigations by 32X.
D3.DC.TVD.B	Antivirus and anti-malware tools are used to detect attacks.	Vectra Cognito provides multiple early-warning opportunities to detect ransomware, other malware variants, and malicious activity that precedes an attack on any network device, including any device that does not run antivirus software.
D3.DC.TVD.E	Processes are in place to monitor potential insider activity that could lead to data theft or destruction.	Vectra Cognito monitors high-privilege credentials, administrative protocol-realm usage, and how internal users gather/store data from key assets in the network. It automatically detects users whose actions lead to data exfiltration or destruction. Cognito threat detections include suspicious admin and Kerberos account activity.
D3.DC.AAD.B	Customer transactions generating anomalous activity alerts are monitored and reviewed.	Deployed inside the cloud, data center and enterprise environment, Vectra Cognito provides nonstop monitoring of all network traffic, including internal (east-west) and internet-bound (north-south) traffic, to identify malicious attack behaviors that put in-scope assets at risk.
D3.DC.AAD.B	Logs of physical and/or logical access are reviewed following events.	Deployed inside the cloud, data center and enterprise environment, Vectra Cognito provides metadata collection of all network traffic, including internal (east-west) and internet-bound (north-south) traffic for further investigation in the event of an incident.
D3.DC.AAD.E	Thresholds have been established to determine activity within logs that would warrant management response.	The scoring of compromised hosts by the Vectra Threat Certainty Index allows security teams to define threshold levels based on combined scoring, such as critical > 50/50.
D3.DC.AAD.E	Systems are in place to detect anomalous behavior automatically during customer, employee and third-party authentication.	Vectra Cognito learns credential usage (such as Kerberos), administrative protocol usage (such as SSH, RDP, IPMI and iDRAC), enumeration of shares, and external connectivity for data transfers used inside the organization. It creates a baseline and triggers an anomalous event for significant deviation from the established baseline. Cognito threat detections include shell knocker, Kerberos account activity and suspicious admin.

FFIEC Cybersecurity Assessment		How Cognito Helps
D3.DC.AAD.I	Tools to detect unauthorized data mining are used.	Vectra Cognito detects the misuse of administrative protocols inside the network. Administrative protocols are used by cyberattackers to move laterally inside a network in which they have already established a foothold. When administrative connections are used with administrative credentials, cyberattackers can have full access to systems, data and, consequently, key assets. Unexpected and unexplained administrative connections represent a significant risk in the lifecycle of a major breach. Cognito threat detections include suspicious admin and data smuggler.
D3.DC.AAD.I	Thresholds for security logging are evaluated periodically.	Vectra Cognito tracks individual hosts over long periods of time and attributes detections to any host that behaves suspiciously. Detection scores and when they occurred are key inputs for the host scores in the Vectra Threat Certainty Index. Since detections are dynamic objects, changes in their scores result in changes to attributed host's scores.
D3.DC.AAD.I	Tools actively monitor security logs for anomalous behavior and alert within established parameters.	The scoring of compromised hosts by the Vectra Threat Certainty Index allows security teams to define threshold levels based on combined scoring, such as critical > 50/50.
D3.DC.AAD.I	Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDOS attack).	The Cognito Attack Campaigns feature further automates security detections by connecting the dots of related attacker behaviors and exposing the relationship between hosts across internal detections, external advanced command-and- control detections, and connectivity to common command-and- control infrastructures.
D3.DC.AAD.A	A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.	Vectra Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when trusted user credentials are compromised by an attacker, including the misuse of administrative credentials and abuse of administrative protocols, such as IPMI.
D3.DC.ED.B	Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks.	Vectra Cognito automated detection, triage and threat prioritization triggers real-time notifications to security teams. Notifications are delivered as one-page explanations of each attack detection, including underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.

FFIEC Cybersecurity Assessment		How Cognito Helps
D3.DC.ED.B	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	Vectra Cognito applies supervised and unsupervised machine learning to the local network to create the baseline of appropriate and approved behavior from which to identify unapproved behaviors of users, connections, devices, and software.
D3.DC.ED.B	A normal network activity baseline is established.	Vectra Cognito applies supervised and unsupervised machine learning to the local network to provide a baseline of appropriate and approved behavior.
D3.DC.ED.E	A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	Vectra Cognito condenses thousands of events and network traits to a single detection using machine learning techniques that automate threat detection based on the characteristics of network traffic.
D3.PC.Im.B.3	Port monitoring to identify unauthorized network connections.	Vectra Cognito's alerts and metadata allow for the detection of unauthorized network connections. The platform supports rapidly identification and validation of hosts, accounts, IPs, domains and ports that are involved with an attacker's progression. The identified information allows users to take action by limiting the use of accounts or hosts, and the blocking or limiting outbound traffic that was identified as being unauthorized.
D4.Co.Co.I	Monitoring controls cover all internal network-to-network connections.	Vectra Cognito eliminates blind-spots by analyzing all network traffic and relevant logs from other security systems, authentication systems and SaaS applications. This provides high-fidelity visibility from network and IoT devices to data centers and the cloud, leaving attackers with nowhere to hide.
D4.RM.OM.I	Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.	Vectra Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when trusted user credentials are compromised by an attacker, including the misuse of administrative credentials and abuse of administrative protocols, such as IPMI.
D5.IRPS.PI.B	Communication channels exist to provide employees a means for reporting information security events in a timely manner.	Vectra Cognito provides consistent reporting of threat data to customers. Security teams receive one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.

FFIEC Cybersecurity Assessment		How Cognito Helps
D5.IRPS.PI.B	Lessons learned from real-life cyber risk incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.	Analyzing opt-in customer metadata and utilizing the latest attack tools and methodologies enables Vectra Cognito to continuously improve threat-detection algorithms, create new algorithms, and develop new machine-learning detection capabilities to find and stop attackers. Behavioral detection algorithms constantly learn from the local environment and from global trends. This ongoing feedback loop drives dramatic improvements and allows for the tuning of existing algorithms in local customer environments.
D5.DRM.De.B	Alert parameters are set for detecting information security incidents that prompt mitigating actions.	The scoring of compromised hosts by the Vectra Threat Certainty Index allows security teams to define threshold levels based on combined scoring, such as critical > 50/50.
D5.DRM.De.E	The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction	Vectra Cognito eliminates manual investigations by automatically prioritizing and correlating threats with compromised hosts and key assets that are the target of an attack. Cognito puts threat detection details – including host context, metadata from captured packets, and threat and certainty scores – within immediate reach.
D5.DRM.De.I	Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.	The highest-risk threats are instantly triaged, correlated to compromised hosts and prioritized by Vectra Cognito so security teams can respond faster to stop in-progress attacks and avert data loss. Each detection is explained in detail, along with the underlying event and historical context that led to the detection. Security analysts can instantly view a connection map of any host to see other hosts the device is communicating with and how. Cognito also provides on-demand access to metadata from captured packets for further forensic analysis. This gives security teams the proof and accuracy they need to take immediate, decisive action.
D5.DRM.De.I	The institution has the ability to discover infiltration, before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems.	By combining advanced machine learning techniques – including deep learning and neural networks – with always-learning behavioral models, Vectra Cognito quickly and efficiently detects hidden and unknown attackers before they do damage. Cognito also eliminates blind spots by analyzing all network traffic and relevant logs from other security systems, authentication systems and SaaS applications. This provides high-fidelity visibility from network and IoT devices to data centers and the cloud, leaving attackers with nowhere to hide. Cognito continuously learns about the environment and automatically detects all phases of the cyberattack kill-chain, including command-and-control, reconnaissance, lateral movement, and data exfiltration.

FFIEC Cybersecurity Assessment		How Cognito Helps
D5.DRM.De.I	Network and system alerts are correlated across business units to better detect and prevent attacks (e.g., simultaneous account takeover and DDOS attack) (transferred from #73); Incident detection processes are capable of correlating events across the enterprise.	The Attack Campaigns capability in Vectra Cognito automates security detections by connecting the chain of events of related attacker behaviors and exposing the relationship between hosts across internal detections, external advanced command-and-control detections, and connectivity to common command-and-control infrastructures. As attackers perform reconnaissance and move laterally from host to host in a network, Cognito correlates their behaviors across all involved hosts and detections and presents a synthesized view of the entire attack campaign.
D5.DRM.RM.B	Incidents are classified, logged and tracked.	Vectra Cognito provides consistent reporting of threat data to customers. Security teams receive one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.
D5.DRM.RM.E	Records are generated to support incident investigation and mitigation.	Vectra Cognito provides consistent reporting of threat data to customers. Security teams receive one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.
D5.ER.ER.B	Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.	Vectra Cognito provides consistent reporting of threat data to customers. Security teams receive one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.
D5.ER.ER.I	Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.	Vectra Cognito automated detection, triage and threat prioritization triggers realtime notifications to security teams, including the ability to create one-time links that can be shared with executive management and the necessary business units. Notifications are delivered as one-page explanations of each attack detection, including underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai