VECTRA®

How Cognito supports adaptive cybersecurity and delivers key elements of the NIST framework

The U.S. government recognizes that the national and economic security of the country depends on the reliable function of critical infrastructure.

Consequently, the federal government has identified 16 critical infrastructure sectors whose assets, systems and networks – both physical and virtual – are vital to the country.

The incapacitation or destruction of the systems and networks of these assets would have a debilitating effect on national security, the economy, and public health or safety. According to the U.S. Department of Homeland Security, these 16 sectors include:

- Chemical and energy industries
- Commercial and government facilities
- Critical manufacturing
- Dams, water and wastewater systems
- Defense industrial base
- Emergency services
- Financial services
- Food and agriculture
- Healthcare and public health
- Information technology and communications
- Nuclear reactors and waste
- Transportation

All of these sectors depend on information technology and industrial control systems to support business decisions and deliver critical services, which makes them vulnerable to cyber attacks.

To address these risks, an Executive Order in 2013 initiated the development of a voluntary risk-based cybersecurity framework. Drafted by the National Institute of Standards and Technology (NIST), the Framework for Improving Critical Infrastructure Cybersecurity provides organizations with a consistent, iterative, technology-neutral approach to identifying, assessing and managing cybersecurity risk.

The following sections highlight key components of the NIST cybersecurity framework and provide detail on how the Cognito® network-detection and response platform from Vectra® provides operators of critical infrastructure with continuous, automated threat surveillance and detection across the entire enterprise.

By automating threat detection and incident response, Cognito condenses weeks or months of work into minutes, enabling security teams to take action to prevent theft or damage.

Framework overview

The NIST cybersecurity framework is technology-neutral to ensure extensibility and enable technical innovation. It relies on standards, guidelines and practices that are developed, managed and updated by industry, with the goal of making cybersecurity tools and methods available that scale across borders and evolve with technological advances and business requirements.

The framework is designed to enable organizations to:

- Describe their current cybersecurity posture and target state.
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- Assess progress toward the target state.
- Communicate among internal and external stakeholders about cybersecurity risk.

Framework practices should be implemented based on their unique vulnerabilities, risk tolerances and security priorities. The framework has three parts:

- The framework core
- The framework profile
- The framework implementation tiers

The framework core

The NIST core is a set of activities to achieve specific cybersecurity outcomes, and includes reference examples for achieving those outcomes that are common across critical infrastructure sectors.

The four elements of the core that work together are functions, categories, subcategories, and informative references. The framework core also defines five functions, subdivided into categories and subcategories of outcomes:

Identify

The activities in the identify function are foundational for effective use of the framework, and help organizations develop an understanding of their business environment, the resources necessary to support critical functions, and how to manage cybersecurity risk to systems, assets, data, and capabilities.

Key categories encompassed by the identify function include asset management, governance, risk assessment, and risk management strategy.

Protect

This function focuses on the development and implementation of appropriate safeguards. Key categories encompassed by the protect function include access control, data security, information protection processes and procedures, and protective technology.

Detect

The detect function involves developing and implementing activities that enable the timely discovery of cybersecurity events. Key categories of the detect function include continuous monitoring, identification of anomalies and events, and detection processes.

Respond

This function entails developing and implementing the appropriate activities to take action in response to a detected cybersecurity event. It supports the ability to contain the impact of a potential cybersecurity event, and encompasses categories such as response planning, communications, analysis, mitigation and improvements.

Recover

This function focuses on plans for resilience, and supports activities for restoring impaired capabilities or services and a timely recovery to normal operations to reduce the impact from a cybersecurity event. Categories encompassed by this function include recovery planning, improvements, and communications.

NIST framework implementation tiers

Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework – that is, risk and threat aware, repeatable, and adaptive.

The tiers provide a way for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. Four tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

The NIST tiers are structured as follows:

Tier 1 – Partial

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. An organization has no processes in place to coordinate or collaborate with external entities, such as partners.

Tier 2 – Risk informed

Risk management practices are approved by management but may not be established as organization-wide policy. Cybersecurity activities are prioritized based on an organization's risk objectives, the threat environment, or business/mission requirements. There are no formalized capabilities to share cybersecurity information externally.

Tier 3 – Repeatable

There is an organization-wide approach to manage cybersecurity risk, and risk management practices are formally approved and expressed as policy. Dependencies are understood and information is received from partners that enables collaboration and risk-based management decisions in response to events.

Tier 4 – Adaptive

Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on systems and networks.

Through an ongoing process of improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

Organizations manage risk and actively share information with partners to improve cybersecurity before an event occurs.

Framework profile

A profile can be characterized as the alignment of standards, guidelines and practices to the framework core in a particular implementation scenario. To develop a profile, review all of the core categories and subcategories and, based on business drivers and a risk assessment, determine which are most important.

Organizations can use profiles to identify opportunities for improving cybersecurity posture by comparing a current profile with a target profile. In addition, profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

Successful implementation of the cybersecurity framework is based on achieving the outcomes described in an organization's target profile.

Cognito supports automated detection and adaptive cybersecurity

The Cognito network-detection and response platform from Vectra augments cybersecurity teams and enables organizations to achieve a Tier 4 adaptive security implementation.

Cognito correlates security-enriched metadata with other data sources, automatically surfaces hidden attacks in real time, and enables security analysts to perform conclusive threat hunting and incident investigations.

By providing continuous, non-stop network traffic monitoring, threat detection, triage, and incident reporting, Cognito automatically hunts down threats across the enterprise network, from cloud and data center workloads to user and IoT devices.

Cognito employs machine learning and attacker behavior analytics to automatically hunt down threats across the entire enterprise, from cloud and data center workloads to user and IoT devices.

By automating the manual, time-consuming Tier 1 analysis of security events, Cognito dramatically reduces the time spent on threat investigations by 75% to 90%, enabling security teams to focus on data loss prevention and mitigation.

Key capabilities of the Cognito platform include:

- Continuous monitoring and analysis of all network traffic, including internal network traffic, Internet-bound traffic and internal traffic between physical and virtual hosts with an IP address – for example, laptops, servers, printers, BYOD/personal smart-devices, and IoT devices – regardless of the operating system or application.
- Real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.
- Analysis of metadata from captured packets with behavioral detection algorithms that spot hidden and unknown attackers, whether traffic is encrypted or not.
- Send security-enriched metadata in Zeek format to data lakes and/or SIEMs.
- Correlate security-enriched network metadata with other data sources, build custom tools and models to detect, investigate and hunt, and leverage existing Zeek tooling.
- Store and interact with security-enriched metadata to hunt for threats retrospectively and accelerate incident investigations.
- Deterministic identification of attack behaviors, including the use of remote access Trojans, encrypted tunnels, botnet behaviors, and reconnaissance tools. Cognito persistently tracks threats over time and across all phases of an attack, ranging from command and control (C&C), internal reconnaissance, lateral movement, and data exfiltration behaviors.
- Automatic correlation of threats with host devices under attack and threat detection details that include host context, packet captures, the seriousness of the threat, and certainty scores.
- Support for adaptive cybersecurity through an ongoing process of improvement that leverages the work of the Vectra Threat Labs™, a group of highly-skilled security researchers, as well as behavioral detection algorithms that constantly learn from the local environment and from global trends.

Framework core – Detect

Automated threat detection is central to the Cognito platform. Cognito provides continuous monitoring and automated threat surveillance across the entire enterprise, providing a robust foundation for adaptive threat management.

Cognito gives IT security teams real-time visibility into all network traffic, analyzes that traffic using behavioral detection algorithms that spot hidden and unknown attackers, and puts security event details at your fingertips.

The majority of category and subcategory detect functions described by NIST are supported by Cognito and are detailed in the following tables.

Anomalies and events – DE.AE

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Subcategory	Cognito capability
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	Through a combination of supervised and unsupervised machine learning applied to the local network, Cognito develops the baseline of appropriate and approved behavior.
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Metadata is analyzed with behavioral detection algorithms to identify hidden and unknown attackers. For example, supervised machine learning lets Cognito find the hidden traits that all threats have in common, while unsupervised machine learning reveals attack patterns.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	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.
DE.AE-4: Impact of events is determined.	Automated scoring of hosts reveals the overall risk to the network based on threat and certainty. The Vectra Threat Certainty Index™ scores all threats and prioritizes attacks that pose the biggest risk.
DE.AE-5: Incident alert thresholds are established.	The scoring of compromised hosts by the Vectra Threat Certainty Index allows security teams to define threshold levels based on combined scoring (e.g., critical > 50/50).

Continuous security monitoring – DE.CM

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Subcategory	Cognito capability
DE.CM-1: The network is monitored to detect potential cybersecurity events.	Deployed inside the network, 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.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	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 (e.g., IPMI).
DE.CM-4: Malicious code is detected.	Cognito provides multiple early-warning opportunities to detect ransomware, other malware variants, and malicious activity that precedes an attack on any network device, including devices that do not run antivirus software.
DE.CM-5: Unauthorized mobile code is detected.	Cognito continuously monitors and analyzes all network traffic, including internal traffic between physical and virtual hosts with an IP address, such as laptops, smartphones, BYOD and IoT devices, regardless of the operating system or application.
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Cognito continuously monitors and analyzes internal network traffic, Internet-bound traffic and data center traffic, including traffic between virtual workloads in the data center.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	A combination of supervised and unsupervised machine learning applied to the local network develops the baseline of appropriate and approved behavior from which to identify unapproved behavior of personnel, connections, devices, and software.

Detection Processes – DE.DP

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Subcategory	Cognito capability
DE.DP-4: Event detection information is communicated to appropriate parties.	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.
DE.DP-5: Detection processes are continuously improved.	Analyzing customer-provided metadata and utilizing the latest attack tools and methodologies enables Cognito to continuously improve existing threat-detection models, create new models, 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 continuous feedback loop drives dramatic improvements and allows for the tuning of existing algorithms in the customer's local environment.

Framework Core – Respond

The timely communication of actionable detection information is critical to cybersecurity incident response. By automating the hunt for active threats, Cognito enables security teams to focus on high-priority risks and respond rapidly to cybersecurity incidents.

Cognito provides a variety of communication and automated response mechanisms that improve situational awareness, expedite information sharing, and support response activities. These include:

- Displaying detection information via a simple dashboard that prioritizes compromised hosts that pose the highest risk, changes in a host's threat and certainty scores, and any key assets that show signs of attack.
- Enabling security teams to easily share the same information on demand or on a set schedule using the highly customizable Vectra reporting engine.
- Leveraging the Vectra Threat Certainty Index to trigger real-time notifications so security teams know instantly which network hosts with attack indicators pose the biggest risk with the highest degree of certainty.
- Providing a precorrelated starting point for security investigations within security information and event management (SIEM) systems and forensic tools.
- Driving dynamic response rules or automatically triggering a response from existing security enforcement solutions.

Examples of supported security enforcement solutions:

- Cognito integrates with the Cisco Systems Identity Services Engine (ISE) to immediately isolate or quarantine a host.
- Cognito works with Carbon Black to rapidly isolate or quarantine a host device when a threat is detected and kill a malicious process.
- Cognito integrates with next-generation firewalls from Palo Alto Network, Cisco and Juniper Networks to block a compromised host device.
- Cognito integrates with SIEMs such as Micro Focus ArcSight and IBM QRadar to automate security operations workflows.

*Click here for a complete list of security enforcement solutions supported by Vectra.

Cognito supports key respond and communications functions described by NIST, as detailed in the table below.

Asset Management - ID.AM

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Subcategory	Cognito capability
ID.AM-1: Physical devices and systems within the organization are inventoried	A host identification engine receives network traffic and uses one or more artifact extractors to extract artifact data items that can identify a host. Artifacts, host data, and network addresses are stored in a database. A mapping table is implemented to match the data to generate durable host identifications that can accurately track hosts as they use different identification data and/or move between network.
ID.AM-3: Organizational communication and data flows are mapped	Cognito provides visibility into network communication and applications by extracting metadata from all packets and storing it in the cloud for search and analysis. Captured metadata includes all internal (east-west) traffic, internet-bound (north-south) traffic, virtual infrastructure traffic, and traffic in cloud computing environments. This visibility extends to laptops, servers, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers, cloud infrastrucure and SaaS applications.

Data Security - PR.DS

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Subcategory	Cognito capability
PR.DS-5: Protections against data leaks are implemented.	Cognito covers scenarios where data is being sent to the outside in a way meant to hide the data transfer. While data is constantly being sent out of the network, it usually does not involve the use of techniques meant to hide the transfer. The host transmitting the data, where it is transmitting the data, the amount of data and the technique used to send it all provide indicators of exfiltration.

Analysis - RS.AN

Analysis is conducted to ensure adequate response and support recovery activities.

Subcategory	Cognito capability
RS.AN-1: Notifications from detection systems are investigated	Vectra Cognito extracts metadata from all packets and storing it in the cloud for search and analysis. Every device on the network is identified and tracked and data can be stored for any amount of time. Captured metadata includes all internal (east-west) traffic, internet-bound (north-south) traffic, virtual infrastructure traffic, and traffic in cloud computing environments.
RS.AN-2: The impact of the incident is understood	Cognito enables incident responders to follow the chain of events from an initial threat signal – whether from Cognito Detect, another security event or threat intelligence – using security-enriched network metadata that is searchable by host name.
RS.AN-3: Forensics are performed	With full metadata search capabilities and limitless data storage, Cognito enables security analysts to determine whether indicators of compromise exist in metadata, including user agents, IP addresses and domains. Cognito also delivers in-depth information for more efficient forensics investigation, such as PowerShell commands from a remote machine to a server or a specific type of connection from a remote site.
RS.AN-4: Incidents are categorized consistent with response plans	Cognito aligns detection models with the MITRE ATT&CK model, so that analysts operate in a clear and consistent language to define playbooks and response plans. Cognito Detect covers 57 of 67 (85%) of the network techniques identified by the ATT&CK model.

Communications – RS.CO

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Subcategory	Cognito capability
RS.CO-2: Events are reported consistent with established criteria.	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.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	Voluntary customer sharing of metadata with the Vectra Threat Labs enables a continuous feedback loop to quickly improve detection algorithms as well as tune existing algorithms in the customer's local environment.

Make the most of your security team

Achieving an adaptive cybersecurity implementation entails a process of ongoing improvement and the ability to respond to sophisticated, evolving threats in a timely manner.

For organizations working toward achieving a NIST Tier 4 adaptive cybersecurity implementation, Cognito delivers an ongoing process of improvement that actively adapts to the changing cybersecurity landscape.

Achieving a NIST Tier 4 implementation is difficult, if not impossible, without automation. By providing continuous monitoring and automating threat detection and analysis, the Cognito platform is able to perform weeks or months of work in just minutes.

Instead of requiring additional headcount, Cognito augments an organization's existing security team with the critical information it needs to make smarter, better-informed decisions. And by eliminating manual threat hunting and low-level threat analysis tasks, security teams can focus on rapid response and quick mitigation of cybersecurity incidents.

Cognito also enables organizations to get more value from
their existing security investments by integrating with firewalls, endpoint detection, NAC, SIEMs and other security enforcement points to block unknown and customized cyber attacks.

Finally, Cognito integrates with leading SIEMs and forensic analysis tools to give security teams a head start when launching threat investigations. Cognito enables real-time investigations by showing infected hosts that pose the highest risk and automatically correlating threat detections with logs generated by other devices.

VECTRA®
Security that thinks®

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