VECTRA®

How Cognito meets CIS Critical Security Controls (CSC) 6.0

The Cognito™ threat detection and response platform from Vectra® continuously monitors and analyzes all network traffic to detect cyber attacks in progress as criminals attempt to steal enterprise data or cause harm to the organization.

By using data science, machine learning and behavioral traffic analysis, Cognito reveals the hidden, fundamental attack behaviors that cyber criminals must perform in order to succeed.

The intelligence in Cognito learns normal network traffic patterns and host behaviors, which makes malicious attack behaviors stand out – even in encrypted traffic.

Always-learning threat detection models pinpoint attackers automatically and in real time over hours, days and weeks, correlates their malicious behaviors with hosts that are under attack, and anticipates their next move.

The Critical Security Controls (CSCs) developed through federal and community efforts, coordinated by the SANS Institute and maintained by the Center for Internet Security (CIS), are designed to mitigate modern attack profiles.

“Realistically, only by adopting basic cyber hygiene will enterprises meaningfully reduce their cyber-risk profile,” said Jane Holl Lute, board member and former CEO at CIS.

“Innovations such as machine learning that incorporate behavioral analytics from Vectra automate a number of the Critical Security Controls and will enable wider-spread adoption of these best practices to really change the game in cybersecurity,” she added.

Cyber attacks are a fact of life. It has become routine to hear about massive data breaches in the news. That’s because organizations have multiple vulnerability points:

- Physical access
- Employees
- Devices
- Network and wireless access routers
- Online presence
- Shared connections with vendors and partners

With Cognito monitoring all network traffic 24x7, organizations can protect their assets, while achieving CIS Critical Security Controls across physical and virtual networks and their individual hosts.

Cognito provides real-time insight into advanced persistent threats (APTs). This insight is fully automated with clear, intuitive reports that enable organizations to create a compliance audit trail as they take immediate, decisive action to stop attacks and mitigate their impact.

Achieving CIS Critical Security Controls with autonomous detection

Cognito continuously monitors all network traffic. Deployed inside the network perimeter, Cognito monitors internal (east-west) and Internet-bound (north-south) traffic to identify malicious attack behaviors that put in-scope assets at risk.

Cognito uses the network to gain high-fidelity visibility into the actions of all devices – from cloud and data center workloads to user and IoT device – leaving attackers with nowhere to hide.

Cognito also detects attack behaviors in all phases of the attack kill chain – command and control (C&C), internal reconnaissance, lateral movement, ransomware activity, data exfiltration, and botnet monetization behaviors – across all applications, operating systems and devices.

For example, Cognito will detect cyber thieves as they patiently make their way to assets in the network, persistently track the hosts involved in an attack, and recognize when a specific host or user account is abnormally accessing servers or data.

In addition, Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when a trusted user's credentials are compromised by an attacker, including the misuse of administrative credentials.

Cognito also provides multiple early-warning opportunities to detect ransomware, other malware variants and malicious activity that precede an attack on any network device, including devices that may not be able to run antivirus software.

This includes the ability to detect malware on mobile and IoT devices and servers that use any operating system. Cognito learns the traffic patterns and behaviors that are typical to a network, while remembering and correlating anomalous behaviors it has previously seen.

Protect enterprise data with Security that thinks®

It's time for security to get smarter. Attackers are already in your network, looking for an opportunity to steal high-value data. Cognito does the hard work by recognizing cyber threats amid the normal chatter in your network and anticipating the next move of attackers in real time so they can be stopped.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 6.0

	Control description	Cognito
Critical Security Control 1: Inventory of authorized and unauthorized devices		
1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	**Host ID** – A host identification engine receives network traffic from a network and uses one or more artifact extractors to extract artifact data items that can identify a host. The artifact data items are stored in a host signature database. Network addresses to which the hosts correspond are stored in a network address database. A mapping table is implemented to match the data in the signature database and network database to generate durable host identification data that can accurately track hosts as they use different identification data and/or move between hosts.
Critical Security Control 4: Continuous vulnerability assessment and remediation		
4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.	**Port scan** – An IT-run vulnerability scanner or asset discovery system is mapping out system services on a host. **Port sweep** – An IT-run vulnerability scanner or asset discovery system is mapping out system services in your network.
Critical Security Control 5: Controlled use of administrative privileges		
5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	**Suspicious admin behavior** – Detects rogue or compromised admins & users; Identifies misuse of low-level management protocols that control system below the OS and BIOS (IPMI, ILO [HPE], iDRAC [DELL]).
Critical Security Control 6: Maintenance, monitoring, and analysis of audit logs		
6.6	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	**Hidden Markov Chain on belief networks (Heuristics + Bayesian networks)** – Automated scoring of hosts to reveal the overall risk to the network; Quickly boil down many events to reveal the key elements of an attack.

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 6.0

	Control description	Cognito
Critical Security Control 8: Malware defenses		
8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	**Malware update** – An internal host is downloading and installing software from the Internet. **Abnormal ad activity** – The internal host has been infected and is part of a botnet which is using ad click fraud to make money; A user installed a piece of adware, such as a web browser toolbar, that interferes with the browsing experience by displaying ad impressions. **Abnormal web activity** – The internal host has been infected with malware and is controlled by a botnet.
8.5	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.	**Peer-to-peer** – The internal host is infected with malware which is using peer-to-peer communication for its command and control. **Relay Communication** – An internal infected host is being used as a relay so that all the transactions from the first host appear to originate from the internal host.
8.6	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.	**Suspicious HTTP** – Malware installed on the host may be communicating back to its command and control server. **Suspect domain activity** – An infected host which is part of a botnet is using a domain generation algorithm (DGA) to locate its command and control servers.
Critical Security Control 9: Limitation and control of network ports		
9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.	**Shell knocker** – Detects use of backdoors; Detects subverted network ports.
Critical Security Control 12: Boundary defense		
12.3	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	**Supervised machine-learning, heuristic analysis, random forest** – Find the hidden traits that all threats share in common. **Unsupervised machine-learning, k-means clustering** – Reveals attack patterns that are unique to the network.
12.8	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.	**External remote access** – A host includes malware with remote access capability (e.g. Meterpreter, Poison Ivy) that connects to its C&C server and receives commands from a human operator; A user has intentionally installed and is using remote desktop access software and is accessing the host from the outside (e.g. GotoMyPC, RDP).
12.1	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.	**Hidden DNS, HTTP, or HTTPS tunnel** – A targeted attack may use hidden tunnels to hide communication with command and control servers; A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible; Intentionally installed software is using a hidden tunnel to bypass expected firewall rules.
Critical Security Control 13: Data protection		
13.6	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.	**Data exfiltration** – Detects fast, high-volume data theft; Detects low and slow exfiltration over many connections.
13.7	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.	**Hidden DNS, HTTP, or HTTPS tunnel** – A targeted attack may use hidden tunnels to hide communication with command and control servers; A user is utilizing tunneling software to communicate with Internet services which might not otherwise be accessible; Intentionally installed software is using a hidden tunnel to bypass expected firewall rules.
Critical Security Control 15: Wireless access control		
15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.	**Supervised machine-learning, heuristic analysis, Random forest** – Find the hidden traits that all threats share in common. Unsupervised machine-learning, k-means clustering - Reveals attack patterns

HOW COGNITO ADDRESSES CIS CRITICAL SECURITY CONTROLS 6.0

	Control description	Cognito
Critical Security Control 16: Account monitoring and control		
16.1	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.	**Suspicious admin behavior** – Identifies misuse of low-level management protocols that control system below the OS and BIOS (IPMI, ILO [HPE], iDRAC [DELL]). **Suspicious Kerberos account** – A Kerberos account is being used differently than its learned baseline in one or more ways – connecting to unusual domain controllers, using unusual hosts or accessing unusual services or generating unusual volumes of Kerberos requests using normal domain controllers, usual hosts and usual services
Critical Security Control 17: Security skills assessment and appropriate training to fill gaps		
17.2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.	**Detections explained** – Cognito is able to serve as a training tool for junior security admins. It teaches the type of network behaviors of an attack as well as the what an attack lifecycle would look like using real time network data. Automated detection, triage, and threat prioritization combined with quick and simple one-page explanations of each attack detection including possible triggers, root causes, business impacts, and steps to verify.
Critical Security Control 19: Incident response (IR) and Management		
19.4	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.	**Automated threat prioritization** – IR teams are able to define consistent Tier 1 analyst report times based on continuous monitoring combined with automated scoring of hosts to reveal the overall risk to the network; Quickly boil down many events to reveal the key elements of an attack.

VECTRA®
Security that thinks®

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