

WHITE PAPER

How to Augment Security Operations Centers with Artificial Intelligence



ARTIFICIAL INTELLIGENCE

SECURITY CLOUD-NATIVE
OPERATIONS CENTER

ENTERPRISE

TABLE OF CONTENTS

Impediments to building a SOC.....	3
Personnel shortages	3
Manual processes	4
Security technology designed for experts	5
Measuring SOC effectiveness	5
Data science: The brains behind Cognito.....	6
Global learning	7
Local learning	7
Integrated intelligence	7
Benefits of the Cognito Detect approach	9
Augment SOC teams by automating Tier-1 analysis	9
More threat detections, faster time to containment	10
Conclusive incident investigations	11
Cut costs	11
Get an efficiency boost	11
Bring AI to your SOC.....	12

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is *Security that thinks*®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

90% 

By leveraging AI to automate Cognito Detect reduces the time spent on threat investigations by up to 90% so SOC teams can focus on data loss prevention and mitigation.

HIGHLIGHTS

- Time is the most important factor in detecting network breaches. To protect key assets from being stolen or damaged, cyberattackers must be detected in real time.
- Done right, AI-powered security solutions can operate 24/7 and automate much of the work of a Tier-1 analyst, allowing for fewer and lower-cost SOC personnel while significantly cutting the time to detect and remediate threats.
- Automated cyberattack detection is central to Cognito Detect. Our approach is based on a simple principle for finding hidden threats: Apply AI to the most authoritative source of data – network traffic.
- Using behavioral detection algorithms to analyze metadata from captured packets, Cognito Detect reveals hidden and unknown attackers in real time, whether traffic is encrypted or not.
- By providing real-time attack visibility and non-stop automated threat hunting that's powered by always-learning behavioral models, Cognito Detect enables SOCs to cut cybercriminal dwell times and speed-up response times.

More and more enterprises are establishing security operations centers (SOCs) in response to the rising tide of cyberattacks.

Not only are risks, threats and attackers increasing in number, they're also increasing in sophistication and damage potential. Targeted threats are especially dangerous and are the most time-consuming to detect.

The SOC can optimize security as well as improve incident detection and response. It's well understood that people, policies and technology are the foundation of a functioning SOC. However, many organizations are struggling to build one effectively and affordably.

By leveraging AI to automate the manual, time-consuming Tier-1 analysis of security events, Cognito condenses weeks or months of work into minutes, reducing the time spent on threat investigations by up to 90% so SOC teams can focus on data loss prevention and mitigation.

This white paper examines the impediments that enterprises face in combating threats, and how security solutions based on artificial intelligence (AI) are essential for the modern SOC. AI-powered solutions can augment SOC teams to make operations more efficient, as well as detect the early signs of attacks in real time before key assets are stolen or damaged.

Cognito Detect™, a cornerstone of the AI-powered Cognito® cyberattack-detection and threat-hunting platform from Vectra®, combines human proficiency and advanced threat research with a broad set of data science and modern machine learning techniques to provide automated threat detection, triage and correlation 24/7 across the entire enterprise.

Cognito cuts detection times and costs by automating data collection, threat detection, analysis and response functions. This gives SOC teams actionable information to stop attacks fast.

By leveraging AI to automate the manual, time-consuming Tier-1 analysis of security events, Cognito condenses weeks or months of work into minutes, reducing the time spent on threat investigations by up to 90% so SOC teams can focus on data loss prevention and mitigation.

Impediments to building a SOC

Enterprises face several challenges in building a SOC. The following sections elaborate on some of those key challenges.

Personnel shortages

It takes skilled cyberwarriors to staff a SOC. Unfortunately, the demand for seasoned cybersecurity and data science professionals exceeds the pool of qualified applicants, making it difficult to recruit and retain the right talent. In the United States, for example, it's estimated that some 40,000 cybersecurity jobs go unfilled annually.

It's common to have a multilevel personnel structure in a SOC, comprised of three tiers of analysts, each with successively more specialized expertise.





Severity could range from critical – requiring immediate action – to low risk, where a response can take hours or even a day. Since Tier-3 analysts are the most expensive, it is important that they handle only the most difficult and highest-risk threat incidents.

Depending upon an enterprise’s processes and resources, the SOC may have a dedicated response team or use a variety of resources to handle critical incidents. This can include calling upon surge staff or hiring an outside incident investigator or subject matter expert.

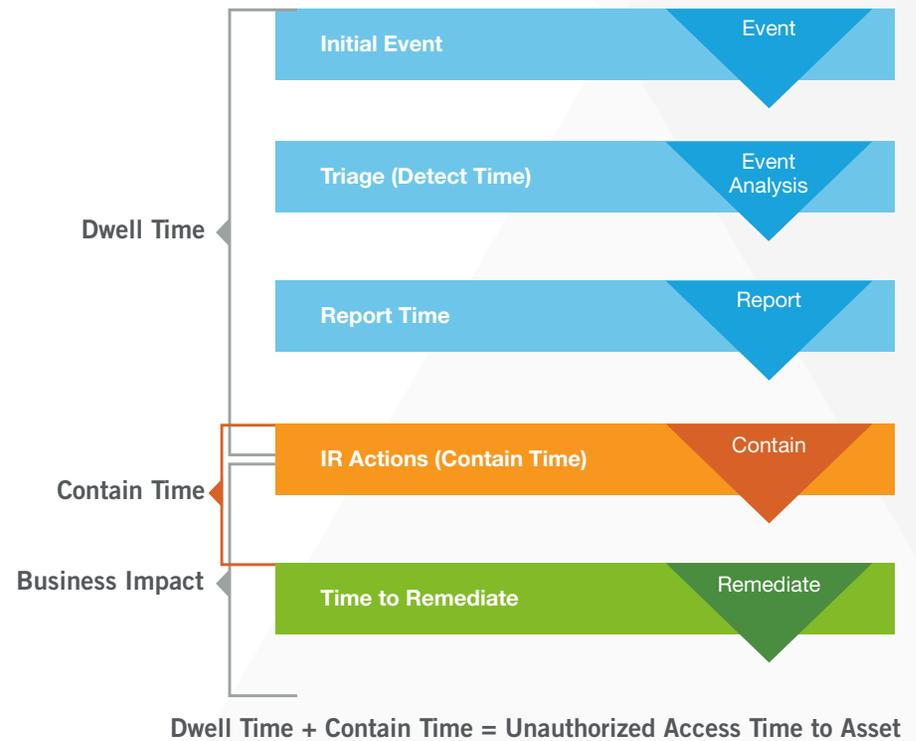
Organizations that hire independent forensics investigators to resolve large-scale data breaches or complex threat incidents often spend \$1 million or more on a single incident.

Manual processes

Advanced threat actors have become quite adept at bypassing signature-based security tools, sandboxes and other security techniques deployed at the perimeter. Once an attacker bypasses perimeter controls, threat detection becomes a very manual and time-consuming process.

Investigations require a broad and specialized set of skills, including malware analysis, forensic packet and log analysis, as well as the correlation of massive amounts of data from a wide range of sources. Security event investigations can last hours, and a full analysis of an advanced threat can take days, weeks or even months.

Time is the most important factor in detecting network breaches. To protect key assets from being stolen or damaged, cyberattackers must be detected in real time.



AI is a key to monitoring and analyzing the huge volumes of traffic on today's networks. Done right, AI-powered security solutions can operate 24/7 and automate much of the work of a Tier-1 analyst, allowing for fewer and lower-cost SOC personnel while significantly cutting the time to detect and remediate threats.

Security technology designed for experts

Historically, security products have required a significant time investment by highly-skilled professionals who are adept at extracting actionable cybersecurity intelligence.

Enterprises need new security approaches and tools that continuously monitor the network, users and applications for suspicious behavior and automatically aggregate key data for security analysts.

Critical data should be aggregated from a wide range of sources, including network flow analysis, system logs, endpoint enforcement points, identity and asset context, threat intelligence, and security events.

AI is a key to monitoring and analyzing the huge volumes of traffic on today's networks. Done right, AI-powered security solutions can operate 24/7 and automate much of the work of a Tier-1 analyst, allowing for fewer and lower-cost SOC personnel while significantly cutting the time to detect and remediate threats.

Measuring SOC effectiveness

Maturity level and effectiveness are two of the most important measurements of SOC performance.

Maturity reflects an enterprise's development level regarding its approach to managing cybersecurity risk, including risk and threat awareness, repeatability, and adaptiveness.

The National Institute of Standards and Technology (NIST) measures maturity using tiers of implementation. The lowest tier is partial implementation, characterized by informal, reactive responses. The highest tier involves an adaptive implementation, which is characterized as agile and risk-informed.

Effectiveness is best measured using real-world metrics related to security operations and threat hunting, including:

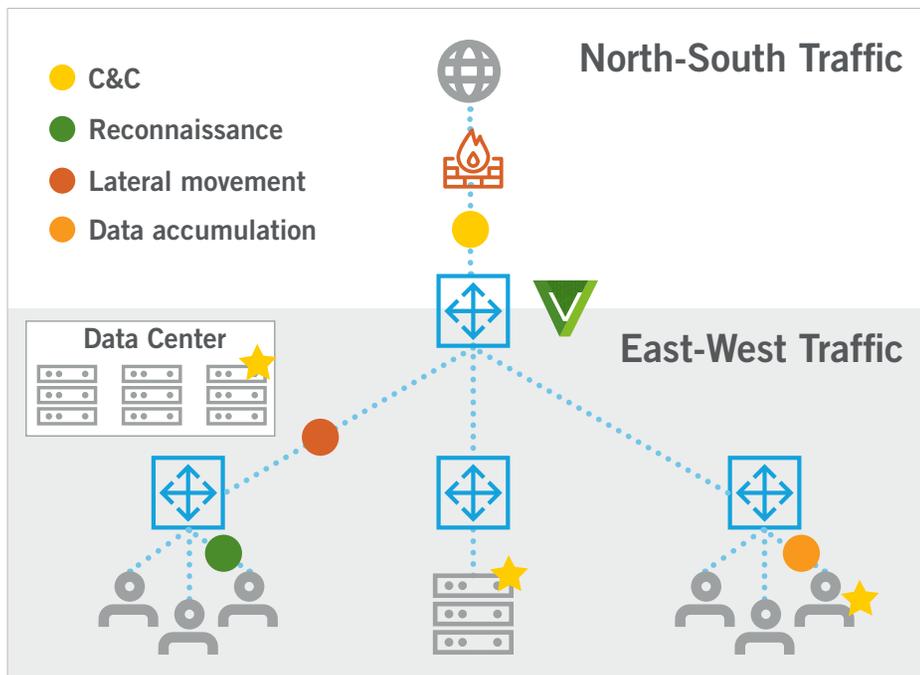
- 1 **Attacker dwell time** – The single most important metric, dwell time measures how long an attacker is in the network, from time of infection to discovery and containment. It provides insight into real-world exposure, how defenses slow down an attacker, threat visibility, and organizational response capabilities.
- 2 **Network visibility** – You can't detect what you can't see. SOC teams must have visibility into all network traffic like Internet-bound and internal traffic, including managed hosts, unmanaged hosts, personal devices, IoT devices, virtual servers, and cloud resources.
- 3 **Lateral movement** – Lateral movement indicates how easily and freely an attacker can move about in the network and how many systems have been compromised.
- 4 **Response time** – How long does it take the SOC to respond to security events? Response time includes all the time spent by defenders to detect, triage, report, and contain a threat or incident.
- 5 **Reinfection rates** – How many times has your organization been targeted and compromised by the same adversary or the same threat?

Data science: The brains behind Cognito

Cybersecurity talent shortages, slow manual processes and complex security tools hamper incident response. Cognito Detect addresses these challenges by blending human expertise with a broad set of data science and machine learning techniques to detect, report and triage threats – augmenting the key functions of a Tier-1 analyst.

Automated cyberattack detection is central to Cognito Detect. Our approach is based on a simple principle for finding hidden threats: Apply AI to the most authoritative source of data – network traffic.

By providing deep, continuous analysis of all network traffic, Cognito Detect exposes the fundamental actions and behaviors that attackers must perform



when they spy and spread across an organization’s networks in search of key assets to steal.

For network coverage and visibility, Cognito Detect provides 24/7 monitoring and analysis of all network traffic. This includes internal (east-west) network traffic, Internet-bound (north-south) traffic, and internal traffic between physical and virtual hosts with an IP address.

This coverage and visibility extends to all devices – laptops, servers, printers, BYOD and IoT devices – as well as all operating systems and applications, including traffic between virtual workloads in the data center and public cloud.

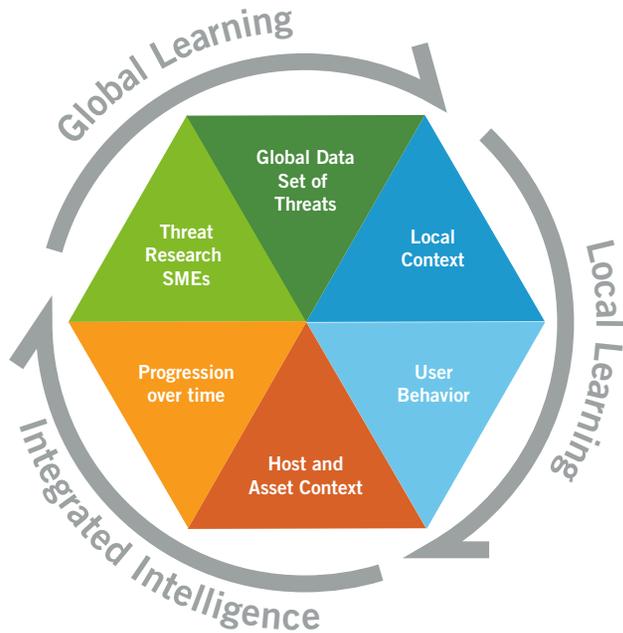
Cognito Detect also monitors and detects suspicious access to critical assets by authorized employees, as well as policy violations related to use of cloud storage, USB storage, and other means of moving data out of the network.

Leveraging a combination of intelligence techniques, Cognito Detect automatically identifies threats in all phases of the attack lifecycle, including:

- Command-and-control and other hidden communications
- Internal reconnaissance
- Lateral movement
- Abuse of account credentials
- Data exfiltration
- Early indicators of ransomware activity
- Botnet monetization
- Attack campaigns, including the mapping of all hosts and their associated attack indicators

Using behavioral detection algorithms to analyze metadata from captured packets, Cognito Detect reveals hidden and unknown attackers in real time, whether traffic is encrypted or not. Only metadata is extracted and analyzed from captured packets to protect user privacy without prying into sensitive payloads.

Let’s look at the technologies behind Cognito Detect to better understand how they address staffing shortages and streamline SOC processes.



Global learning

Global learning is about identifying the fundamental traits that threats share. Global learning begins with the Vectra Threat Labs™, a full-time group of cybersecurity experts and threat researchers who continually analyze malware, attack tools, techniques, and procedures to identify new and shifting trends in the threat landscape.

Their work informs the data science models used by Cognito Detect, including supervised machine learning. It is used to analyze very large volumes of malicious and attack traffic and distill it down to the key characteristics that make malicious traffic unique.

For example, a supervised machine-learning model can be designed to identify the unique behaviors of remote access tools (RATs), learning how traffic from these tools differs from normal traffic. This intelligence enables Cognito Detect to reliably detect new, customized and unknown RATs in real time and without using signatures.

Local learning

Local learning identifies what's normal and abnormal in a local network to reveal attack patterns. The key techniques used are unsupervised machine learning and anomaly detection.

Cognito Detect uses unsupervised machine learning models to learn about a specific customer environment, with no direct oversight by a data scientist. For example, using local learning, Cognito Detect can determine when a user behaves differently than in the past.

Instead of concentrating on finding and reporting anomalies, Cognito Detect looks for indicators of important phases of an attack or attack techniques, including signs that an attacker is exploring the network, evaluating hosts for attack, and using stolen credentials.

Detecting these behaviors requires a long-term memory of the local network environment, including IP addresses that are used over time. Likewise, the progressive staging of data can be observed but it requires memory and intelligence to build context and recognize that similar amounts of data are being staged and exfiltrated at different times.

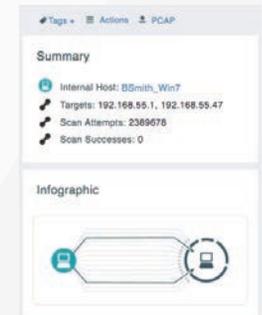
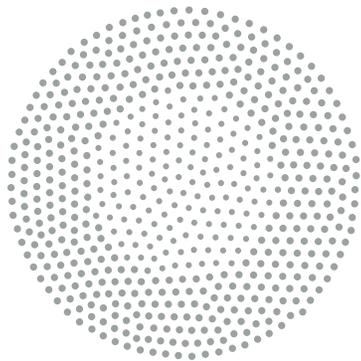
Unsupervised learning and related techniques are powerful security mechanisms that enable Cognito Detect to spot suspicious activity in real time, such as the theft of valid credentials from a compromised host.

Integrated intelligence

Today's cyberattacks are complex, multistage operations that evolve over time and encompass a variety of techniques and strategies that help attackers move deeper into the network.

Consequently, it is critically important for threat detection models to have the intelligence to assimilate all the available information to identify the larger attack, not just the component events, and to track the attack progression over time.

Detect: Hundreds to thousands of events and network traits condensed to a single Cognito detection



Report: Analysts need enough information to make decisions and recommendations for next steps

Triage: Detections automatically correlated to pinpoint physical hosts at the center of an attack

Cognito Detect integrates with enforcement and incident response platforms



- SIEM
- Incident Response



- Firewall
- Endpoint
- NAC

Cognito Detect condenses thousands of events and network traits to a single detection. Using techniques such as event correlation and host scoring, Cognito Detect performs the following:

- Correlates all detection events to specific hosts that show signs of threat behaviors.
- Automatically scores every detection and host in terms of the threat severity and certainty using the Cognito Threat Certainty Index™.
- Tracks each event over time and through every phase of the cyberattack kill chain.

Cognito Detect puts special focus on events that may jeopardize key assets inside the network or are of strategic value to an attacker. Devices that exhibit behaviors that cover multiple phases of the cyberattack kill chain are also prioritized.

As a result, customers get immediate insight into attack behaviors and hosts in the network that pose the greatest risk with the highest degree of certainty. Attacker behavior insights from within CNI organizations

Benefits of the Cognito Detect approach

By combining human expertise with a wide range of AI techniques, Cognito Detect automates the manual, time-consuming Tier-1 analysis of security events, which yields a number of benefits for customers.

Augment SOC teams by automating Tier-1 analysis

Cognito Detect automates security investigations that normally require hours of manual effort from highly trained security analysts and data scientists. Detection, reporting and triage functions typically performed by Tier-1 analysts are fully automated, making all members of your SOC team more efficient and productive.

For example, Cognito Detect displays detection information via a simple dashboard that prioritizes the compromised hosts that pose the highest risk, changes in a host's threat and certainty scores, and any key assets that show signs of an attack. Cognito threat and certainty scores also trigger notifications to SOC personnel.

These brief, single-page notifications explain each attack detection, including the underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.

SOC teams can see the progression of a threat over time and immediately focus on remediation efforts, rather than spending precious time trying to determine the severity and priority of an attack.

Cognito Detect also alerts SOC personnel when data is transferred between parties in a manner

that violates or is not consistent with established practices, and provides insight into the host transmitting the data, where it is transmitting the data, the amount of data, and the technique used to send it.

In addition, SOC teams can easily track reinfection rates by creating a dashboard view that shows if hosts are getting hit by the same malware or repeatedly connecting to a bad site.

With the wealth of information provided, Cognito Detect is an indispensable training tool that can educate SOC team members about what is normal on their network and how attacks unfold and progress.



Triggers

- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal encrypted web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions

For many customers, the automation and ease of use of Cognito Detect means they can employ security generalists, such as student interns, or promote more experienced security analysts to hard-to-fill senior security positions.

As an example, the CISO at a healthcare organization noted that “our interns have done an amazing job with Cognito Detect,” which in turn cut the workload for the rest of the SOC team by 75%.

After deploying Cognito Detect, the Texas A&M University System turned to college interns to help protect its high-value academic and research data. Student interns who are interested in pursuing careers in cybersecurity are trained to use Cognito Detect as Tier-1 analysts in the SOC.

“Cognito Detect is so intuitive and easy to use that interns can decide in a few minutes whether to act on a detected threat or escalate it to a Tier 2 analyst for further investigation,” said Daniel Basile, executive director of the SOC at Texas A&M. “So the highly-skilled employees who used to be Tier-1 analysts are now working as Tier-2 analysts. This is where Cognito really shines.”

More threat detections, faster time to containment

By providing real-time attack visibility and non-stop automated threat hunting that’s powered by always-learning behavioral models, Cognito Detect enables SOC teams to cut cybercriminal dwell times and speed-up response times. This enables SOC teams to align with NIST’s highest level of implementation maturity.

Cognito Detect dramatically reduces the time spent on threat investigations, enabling security teams to focus on data loss prevention and mitigation. Customers have reduced the time spent on investigations by as much as 90%. For example, the SOC team at Texas A&M cut threat investigation times from days to minutes.

In addition, Cognito Detect discovers security events that would otherwise go unnoticed. This leads to a net increase in the number of events, and precise and timely incident response.

After one year of using Cognito Detect, Texas A&M found seven active threats inside its network. Cognito Detect provided the SOC team with all the information it needed to respond quickly to contain each threat and protect critical assets.



Conclusive incident investigations

The other cornerstone of the Cognito platform, Cognito Recall™, enables security analysts to perform AI-assisted threat hunting and conduct deeper, more conclusive incident investigations with remarkable efficiency.

With Cognito Recall, security analysts can easily follow the chain of related events and forensic evidence found by Cognito Detect, third-party security products, and searchable, high-quality threat intelligence in historical network metadata.

When threat notifications are received from Cognito Detect, Cognito Recall ensures that security analysts have a full 360-degree view of all workload and device activity. By pivoting with one click between Cognito Detect and Cognito Recall, security analysts gain deeper, more meaningful context about malicious network communications.

Cognito Detect provides details about specific attack behaviors and compromised host devices involved in an attack while Cognito Recall enables security analysts to search its rich arsenal of historic metadata about network communications that occurred in the same timeframe as the attack.

Cut costs

Expensive incident response and forensic analysis services are often required after an attack. Cognito Detect helps avoid the cost of third-party investigations entirely, while lowering dependence on manual log analysis.

Cognito Detect has produced significant savings for Texas A&M. With Cognito Detect, “our security operations team found the attackers quickly and early so we didn’t need to summon expensive post-breach forensic analysts, who are typically brought in a month after the damage is done,” said Basile.

“You’re looking at about \$1 million every time you call in consultants to perform post-breach forensic analysis,” he noted. “By eliminating this, Vectra saved Texas A&M \$7 million in a year.”

Get an efficiency boost

Cognito Detect provides a variety of communication and automated response mechanisms that improve situational awareness, expedite information sharing, and support incident response activities, helping make SOC processes more efficient. These include:

- Real-time alerts via email, syslog or other tools that have been integrated via REST APIs.
- A precorrelated starting point for security investigations within security information and event management (SIEM) systems and forensic tools.
- Enable SOC teams to easily share the same information on demand or on a set schedule using the highly customizable Cognito Detect reporting engine.
- Drive dynamic response rules and automatically trigger responses from other security enforcement solutions.
 - Cognito Detect integrates with the Cisco Identity Services Engine (ISE) and Forescout to immediately isolate or quarantine a host.
 - Cognito Detect works with Carbon Black to rapidly isolate or quarantine a host device when a threat is detected and kill a malicious process.
 - Cognito Detect integrates with next-generation firewalls from Palo Alto Networks, Cisco and Juniper Networks to block a compromised host device.
 - Cognito Detect integrates with Demisto and Phantom security orchestration platforms to enable faster enforcement.
 - Cognito Detect integrates with SIEMs such as Splunk, Micro Focus ArcSight and IBM QRadar to automate security operations workflows.

“Since deploying Cognito, our team can monitor the entire Texas A&M network infrastructure for cyberattackers and run the security operations center with incredible efficiency, despite having an extremely lean staff,” Basile said.

Bring AI to your SOC

Combating cyberthreats will continue to be a major challenge for enterprises large and small, one that requires AI-based solutions to augment the SOC. The data science behind Cognito represents an unprecedented innovation in detection methodologies.

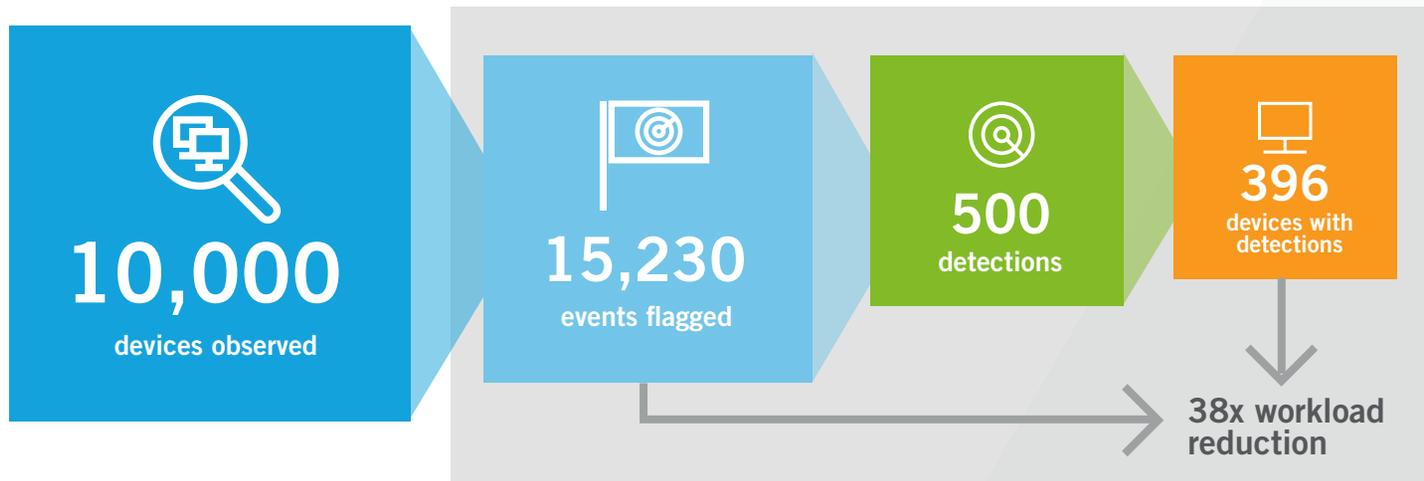
By providing continuous, non-stop network traffic monitoring and leveraging AI for threat detection, triage, and incident reporting, Cognito Detect automatically finds and stops threats across the enterprise network, from remote sites to campuses to data centers and the cloud.

Consequently, customers can manage security incidents faster and without hiring additional cybersecurity professionals. This enables existing Tier-1 security analysts to concentrate on data loss prevention and mitigation.

And Vectra is always working to improve the Cognito platform. Voluntary customer sharing of metadata with the Vectra Threat Labs enables a continuous feedback loop that quickly improves attacker detection algorithms as well as tunes existing algorithms in the customer's local environment.

AI-powered Cognito Detect reduces the SOC workload by 38X, compared to manually hunting for threats.

By automating the detection of hidden attacks and empowering security analysts to respond faster to stop them, Cognito Detect is well-suited to help enterprise organizations build effective and affordable security operations centers.



For more information about Cognito Detect and how to augment SOC's with AI, please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai

© 2020 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.