

SOLUTION BRIEF

Integrating Cognito with Splunk

Faster, context-driven investigations into active cyberattackers

The Cognito[®] network threat detection and response platform from Vectra[®] seamlessly integrates AI-based automated threat hunting and incident response with the operational intelligence of the Splunk platform.

Together, Vectra and Splunk deliver a practical solution to the most persistent problems facing today's enterprise cybersecurity teams – finding and stopping active cyberattacks while getting the most out of limited time and resources.

The need for a new cybersecurity approach

Modern cyberattackers with sophisticated hacking tools at their disposal can easily evade network perimeter security to spy, spread and steal inside the network, largely undetected and hidden from view.

Together, Vectra and Splunk deliver a practical solution to the most persistent problems facing today's enterprise cybersecurity teams.

Unable to rely entirely on perimeter defenses, security teams are left to manually chase-down security alerts and events, unable to determine with any speed or precision which ones are most dangerous and pose the highest risk to an organization.

In practice, this often means that breaches are discovered and reported by an external third-party after theft or damage has occurred. This can result in a debilitating post-breach forensic investigation that can cost upwards of \$1 million.

CHALLENGE

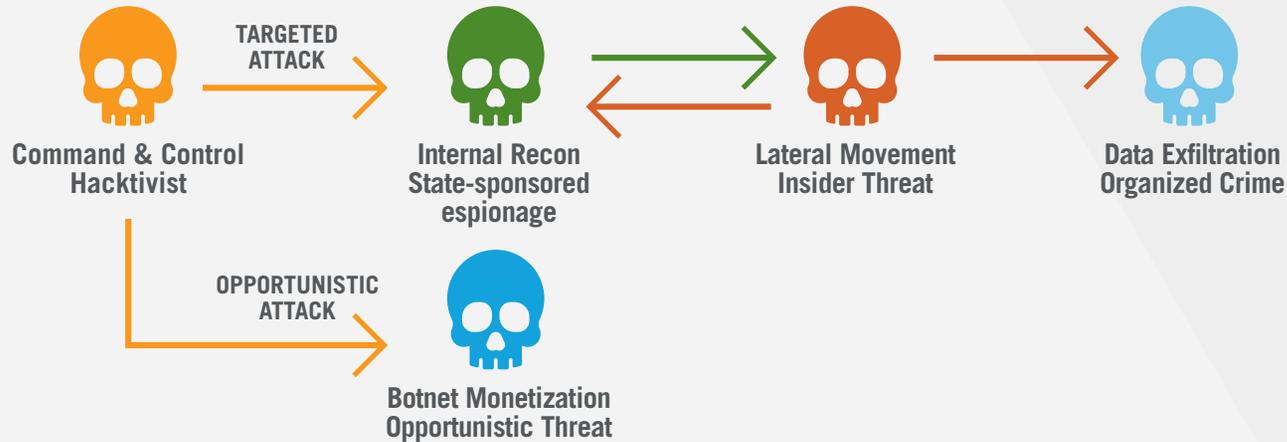
Today's cyberattackers easily circumvent network perimeter security to spy, spread, and steal critical assets inside networks. As a result, cybersecurity teams are saddled with manual, time-consuming threat investigations and costly forensic analysis after a theft has occurred.

SOLUTION

The Vectra App for Splunk brings real-time, precorrelated attack detections to the operational intelligence of the Splunk platform. Integrating the Cognito platform's AI-based detection algorithms with Splunk enriches the context of threat investigations and speeds-up incident response.

BENEFITS

With faster response and improved operational efficiency, the Vectra App for Splunk enables security teams to quickly mitigate and stop cyberattacks before damage is done. Cognito prioritizes infected hosts that pose the highest risk and correlates threats with logs from devices in Splunk to provide greater context for every attack.



The lifecycle of a cyberattack

A new threat detection model

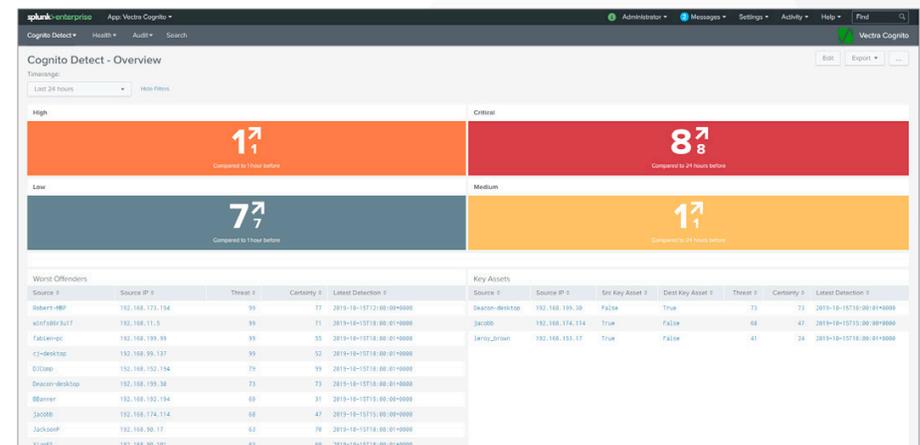
Cognito detects in-progress cyberattacks across all phases of the attack lifecycle, ranging from command-and-control traffic, internal reconnaissance, lateral movement, and data exfiltration without depending on signatures or reputation lists.

Cognito detects these threats by analyzing the underlying behavior of attackers viewed from the objective viewpoint of the network. All threat detections are correlated with the hosts that are under attack while threat and certainty scores prioritize the hosts that pose the highest risk.

This ensures that security teams detect new, customized and unknown threats, as well as attacks that do not rely on malware such as malicious insiders or compromised users.

The Vectra App for Splunk brings all Cognito detections directly into the Splunk ES dashboards, incorporates Cognito high-value detections into existing workflows, and automates their correlation with logs from devices in the Splunk database, providing greater context of a threat.

For example, the Vectra App for Splunk enables security teams to easily correlate the information in Cognito Hosts and Detections with intelligence from other systems, such as URL filtering solutions and firewalls. A link back into the Cognito user interface allows a seamless transition to drive prioritization and workflow.



Key features

- **Hosts ranked by risk** – To enable faster investigations and responses, Cognito automatically associates all malicious behaviors to the physical network host – even if the IP address changes – and scores the host in terms of its overall risk.

Cognito Detect™ and Cognito Stream™ from Vectra both have individual apps and tech add-ons for Splunk. The Vectra App for Splunk provides an interactive dashboard to quickly show the number of hosts classified as critical, high, medium, and low risk.

These scores eliminate the need for security teams to manually investigate events and vastly improve the time to respond.

Drill-downs into each category in the Vectra App for Splunk redirect security analysts to the host page and filter on that particular detection's severity to help speed-up the investigation.

- **Visibility into threats across the attack lifecycle** – The Vectra App for Splunk provides an extraordinary range of threat intelligence to the Splunk machine-data repository, including detections of unknown malware and attack tools, threats that hide in common apps and encrypted traffic, and in-progress threats in every phase of the attack lifecycle.

This visibility enables security teams to instantly distinguish opportunistic botnet behaviors from more serious targeted threats and take quick action before key assets are stolen or damaged.

For example, the Detections view in the dashboard shows individual events and their scores, while the Campaigns view shows individual campaigns that have been identified and the number of events associated with that campaign. The Account view shows observed accounts and their privilege levels in your network giving you a view of credential abuse and other anomalies.

- **Correlation with other solutions** – The Vectra approach to detection enables security teams to detect threats that were missed by other security solutions. The Vectra App for Splunk makes it easy to connect and correlate Cognito platform findings with other solutions, with correlation rules pulling in additional context from other systems that integrate with the Splunk platform.

Splunk captures, indexes and correlates Cognito threat detections in real-time, making it available in a searchable repository from which security teams can generate graphs, reports, alerts, dashboards and visualizations.

For example, the Correlations page provides valuable information about active threats and speeds-up deeper investigations into events by enabling security teams to correlate source and destination IP addresses from Cognito events with other events in Splunk.

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

Email info@vectra.ai | vectra.ai