VECTRA
SECURITY THAT THINKS®

INTEGRATED SOLUTION

Integrating Vectra with Splunk

Faster investigations into active cyberattackers

Vectra® delivers AI-driven threat detection and response that seamlessly integrates automated threat hunting and incident response with the operational intelligence of Splunk. This allows organizations the ability to quickly stop and respond to cyberattack progression that would otherwise go unnoticed while gaining full context of attacker actions.

The combination of advanced AI-driven threat detection and the ability to capture and correlate attack data, puts security teams back on offense against cyberattackers, significantly raising the resiliency level for organizations.

A New Level of Resiliency Against Cyberattacks

- **Faster Investigations**: Automatically triage and score hosts ranked by risk
- **Threat Visibility**: See all known and unknown threats in the entire attack lifecycle
- **Valuable Insight**: Correlate detections from Vectra with events in Splunk

Vectra empowers security analysts with a rapid approach to bringing malicious activity and breaches into view earlier and instantly. Vectra threat detection capabilities surface hidden malicious actor tactics already in play in the network that impact SaaS and IaaS environments where Firewalls, IDPS, EDRs, and workload protection solutions don't have visibility.

Together, Vectra and Splunk increase cybersecurity efficacy and streamline enterprise security operation workflows.

Vectra detections allow Splunk to ingest valid security data filled with context—only information from actual attacks—to produce an easy-to-use dashboard depicting meaningful charts and graphs with context to be readily consumed by stakeholders without further scrubbing.

CHALLENGE: Limited Data Ingestion and Analytics

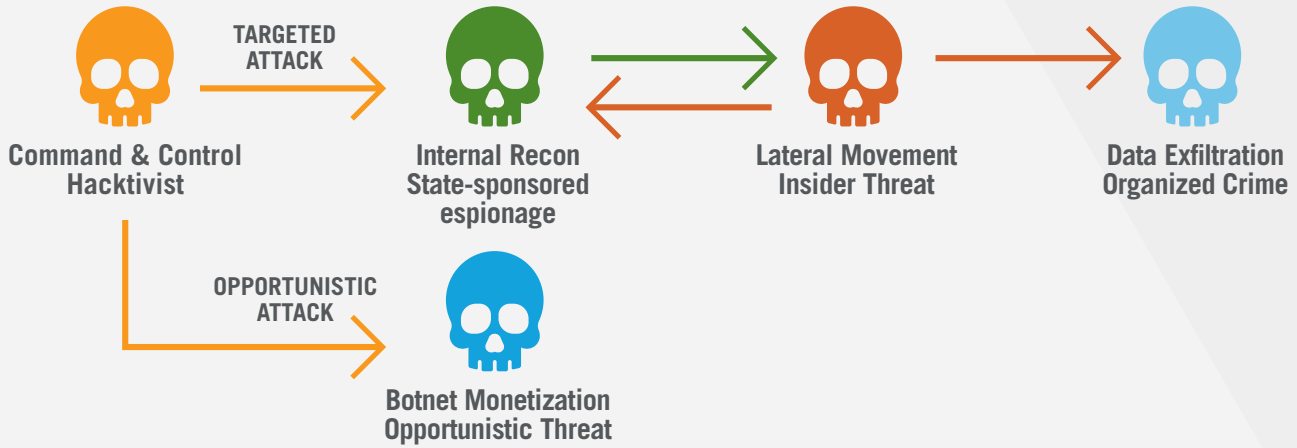
Today's cyberattacks regularly circumvent prevention security tools to move laterally and conduct recon efforts until they can steal and exfiltrate critical data assets from an organization's environment. As a result, security teams are saddled with manual, time-consuming threat investigations and costly forensic analysis after a breach—long after the damage is done.

SOLUTION

Vectra aligns AI-driven threat detection capabilities to the operational intelligence of Splunk. Integrating Vectra'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, Vectra and Splunk enable security teams to quickly mitigate and stop cyberattacks before damage occurs. Vectra 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

Quickly Understand the Attack Impact on Your Organization

Together, Vectra and Splunk go beyond assuring fast responsive action. The combination of these advanced cybersecurity tools enable corporate security teams to easily navigate through data from data center to cloud and easily see vulnerabilities along with the coverage gaps.

A New Threat Detection Model

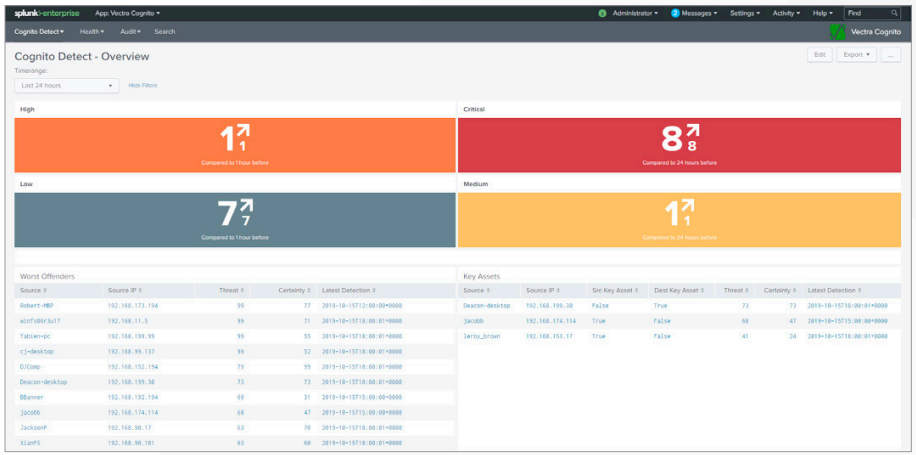
Vectra detects cyberattacks in progress across all phases of the attack lifecycle, ranging from command-and-control traffic, internal reconnaissance, lateral movement, and data exfiltration without depending on signatures or reputation lists.

The underlying behavior of the attack is analyzed from the network perspective. 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.

Vectra threat detections are integrated directly into Splunk dashboards—incorporated into existing workflows with automated correlation and logs from devices in the Splunk database—providing greater context about threats.

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



Key features

- **Hosts ranked by risk** – To enable faster investigations and responses, Vectra 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.

  Vectra includes individual apps and add-ons for Splunk. Vectra 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 Vectra redirect security analysts to the host page and filter on that particular detection's severity to help speed up investigations.

- **Visibility into threats across the attack lifecycle** – Vectra 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. Vectra makes it easy to connect and correlate findings with other solutions, with correlation rules pulling in additional context from other systems that integrate with Splunk.

  Splunk captures, indexes and correlates Vectra 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 Vectra events with other events in Splunk.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai