BluVector and Splunk

Solution Guide

Sense and Respond to Advanced Threats with Confidence and Speed

BluVector® Cortex™ is an AI-driven sense and response network security platform designed to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware, and ransomware in real time. Together with Splunk, the solution seamlessly combines automated threat detection and response with complete Operational Intelligence, solving the problem of advanced threats while freeing up valuable analyst resources.

AN INTEGRATED SOLUTION TO KEEPING AHEAD OF ADVANCED THREATS

Challenge

Cybersecurity analysts are overwhelmed with alerts and notifications coming from all the tools within their security stack. A single event can result in notifications from multiple products, or worse, detection of an advanced threat can be lost in the noise of the other less critical issues. Analysts spend too much time trying to make sense of and prioritize the noise and not enough time investigating and responding to real threats.

Solution

BluVector Cortex is the advanced threat detection and response solution for Splunk, uncovering sophisticated attacks and enabling efficient investigation and response. Utilizing its high-fidelity detection and automated investigation capabilities, BluVector eliminates the need for additional event source integration, correlations or complex queries to support threat investigations. By sending only relevant, prioritized and pre-triaged alerts to Splunk, BluVector enables Security Operations Centers to radically improve the efficacy and efficiency of their threat detection and response efforts.

Benefits

- **Integrated Detection & Correlation**
  Displays prioritized results in Splunk, enabling easy correlation of BluVector's high-fidelity and actionable alerts with the output from other security tools (e.g., endpoint)
- **Accelerated Investigation**
  Accelerates analyst workflow by automating the traditionally time-consuming tasks of alert contextualization and investigation, providing targeted network logs and results from integrated post-analyzers
- **Automated Response**
  Provides the ability for automated response to high-confidence or analyst-confirmed alerts, allowing responders to pivot from Splunk into BluVector Cortex for containment via the solution's rich integration ecosystem
- **Reporting and Visualization**
  Allows for easy reporting and visualization of events and incident response resolution results
- **Infrastructure Monitoring**
  Offers a centralized method for monitoring system health and status for all deployed sensors

400%
IMPROVEMENT IN
ANALYST EFFICIENCY (5:1 FTE)

BluVector App

The BluVector App works hand-in-hand with Splunk to eliminate the need for additional dashboards, and more importantly, it makes the whole experience of advanced threat detection and triage through Splunk radically more efficient and cost-effective. Through the BluVector App, analysts using Splunk receive prioritized alerts and have the opportunity to access all the data and functionality required to triage events without switching tools, writing complex queries or copying and pasting data.

By bringing BluVector's events into a single pane of glass with the alerts from other tools in the security stack, enterprises can also better take advantage of their entire ecosystem, allowing them to take a holistic view of their environment and maximize the performance of individual solutions.

The Event view of the BluVector App displays all of the details of a specific event, enabling rapid threat detection and triage directly in Splunk.

Features

1. Detailed BluVector Cortex events are listed in the Splunk interface, allowing an analyst to monitor the solution without ever having to leave Splunk. The Splunk interface can also display these events alongside alerts from other sources, thereby enabling further correlation of activity from all the security technologies in a user's security infrastructure (e.g., network, endpoint, DDoS protection, DLP, etc.).

2. A 'Pivot to BluVector Cortex' button allows users to seamlessly move from the Splunk interface into the BluVector Cortex event report. By pivoting to BluVector Cortex from the event detail in Splunk, analysts can quickly and easily further investigate and adjudicate events.

BluVector Reports App

The BluVector Reports App provides Splunk with key sensor health and status information and creates easy-to-use views of the aggregated data directly in Splunk, thereby driving increased Security Operations Center efficiency and valuable board-level reporting.

The Reports App enables easy consumption of the device information by Splunk, seamlessly collecting from and reporting on all sensors deployed in a user's environment.

The Current Health view of the BluVector Reports App shows the health and status of each BluVector Cortex sensor in a deployment.

Features

1. View health and event metrics of multiple sensors without the need to monitor each sensor individually.
2. Drill down and see details from a specific reporting interval.
3. Compare operational performance to a historical baseline for the selected reporting interval.
4. View deviations from normal operation (such as appliances that are offline or a sudden increase in events associated with a particular file type when compared to previous periods).
5. Access and export raw performance data to feed into existing reporting tools.
6. Measure and track key compliance metrics, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).