SentinelOne

SOLUTION BRIEF

Combine SIEM and EDR for Improved Detection, Investigation and Response

SentinelOne & Splunk Joint Solution Brief

splunk>

Addressing the SOC Visibility Challenge

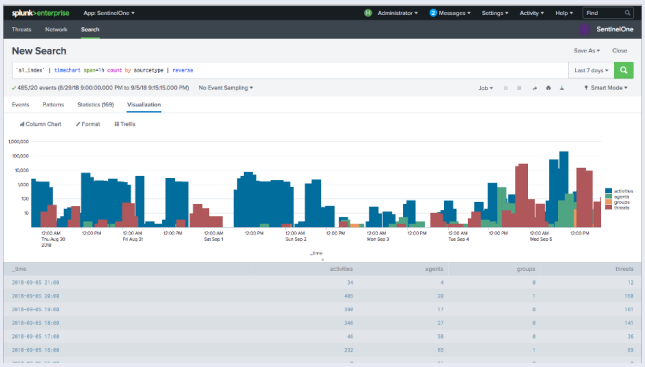
Security teams are overwhelmed with data - from the infrastructure they support to the multitude of tools they use. Visibility across the estate becomes a challenge, hindering the security operations center's (SOC) ability to detect and respond to threats as they occur. Attackers often vary their tactics, latching on to multiple systems to move laterally and establish persistence in the environment. To detect these threats, many organizations turn to security information and event management (SIEM) to centralize, correlate, and apply threat detection analytics. Endpoint telemetry provides SIEM with a valuable stream of telemetry that not only powers SIEM analytics but provides an additional detection and response capability to augment threat management workflows.

Joint Solution

The integration of SentinelOne and Splunk empowers organizations to combine the strengths of their Splunk deployments to collect, monitor, analyze and visualize massive streams of machine data, with the visibility, detection, response, remediation and forensics capabilities of SentinelOne. SentinelOne offers deep bi-directional integration with Splunk, enabling joint customers to maximize the value of their SIEM and EDR investments.

How It Works

With the SentinelOne Technology Add-on (TA) for Splunk, clients can take advantage of a prebuilt ingestion pipeline that includes parsing of SentinelOne events, mapping to Splunk Common Information Models (CIM), and saved searches. Once downloaded from Splunkbase, SentinelOne can be configured to send telemetry and alerts to Splunk using either using forwarded Syslog or over SentinelOne APIs.



JOINT SOLUTION HIGHLIGHTS

+ Consume and correlate endpoint telemetry
+ Triage and investigate endpoints
+ Integrated response workflow

INTEGRATION BENEFITS

Enhance Threat Detection

Accelerate Alert Triage

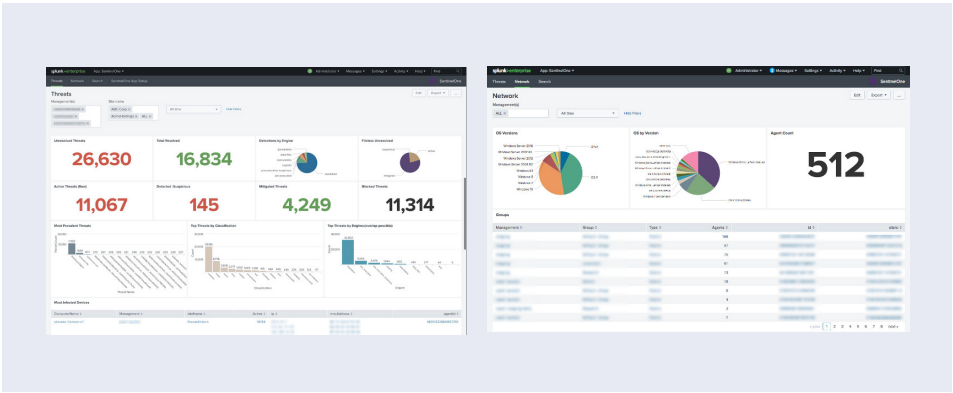
Increase Response Efficiency

"Data is the common currency for enterprises; our bidirectional integrations with SentinelOne for SIEM and SOAR capabilities are used by some of the largest enterprises in the world.

Eric Schou

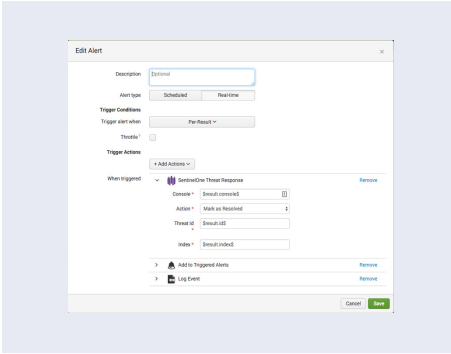
AVP & HEAD OF MARKETING, SPLUNK

Once SentinelOne data is within Splunk, it can be used for searches and queries which can be saved to generate Spunk alerts. Searching SentinelOne data in Splunk is made easier by predefined mapping to Common Information Models (CIM) which makes it easier to build Splunk queries.



Additionally, the data can be visualized in dashboards, and when used in conjunction with Splunk Enterprise Security, automatically updates Enterprise Security Dashboards for **Malware** and **Endpoints**.

With the SentinelOne App for Splunk, clients can easily perform endpoint triage and response from within the Splunk console. The app provides rich capabilities for viewing endpoint and threat information at a glance. Analysts can view all connected SentinelOne endpoints from a consolidated network view and can filter to select a Management, scope, and time frame.



Splunk users can take manual action to manage ongoing threats, or use Adaptive Response Actions that automatically trigger a real-time response in SentinelOne when certain conditions are met.

Conclusion

The combined solution provides SOC teams using SentinelOne and Splunk with unparalleled visibility and an integrated workflow to detect and respond to threats with consistency.

JOINT SOLUTION BENEFITS

Enhance Threat Detection

Consume and correlate high fidelity endpoint logs and alerts

Accelerate Alert Triage

Investigate endpoint information at a glance with prebuilt dashboards

Increase Response Efficiency

Automatically initiate SentinelOne endpoint response capabilities within the Splunk console

Download the SentinelOne TA (Add-on) for Splunk
splunkbase.splunk.com/app/4187/

Download the SentinelOne Application for Splunk
splunkbase.splunk.com/app/3677/

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice

97% Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97% Customer Satisfaction (CSAT)

FedRAMP · ISO 27001 CERTIFIED by schellman · EU GDPR COMPLIANT · TEVORA PCI DSS Attestation HIPAA Attestation · Gartner peerinsights 4.9

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

About Splunk

Splunk Inc. turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, and analyze and act on data at any scale.

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733