

Splunk for Cisco Security Suite

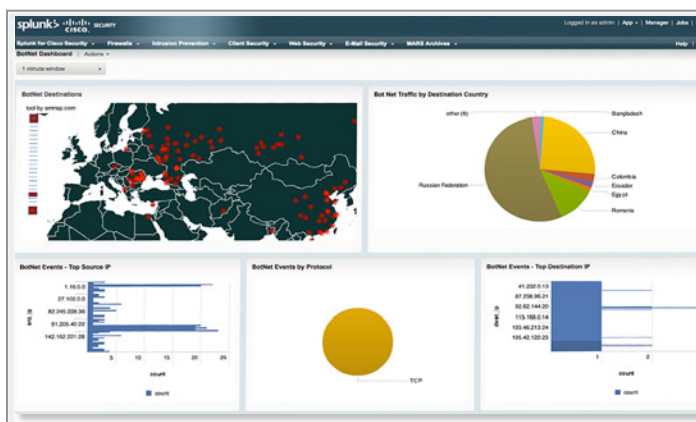
Using Splunk for Real-time Monitoring and Management of Cisco-centric Security Environments

The Challenges

Every Cisco router, switch, firewall, IPS, web proxy or other hardware or software-based solution has a story to tell about the confidentiality, integrity and the availability of your environment. Relevant data from across these systems is critical to investigations and continuous monitoring for situational awareness.

However, the real ROI for security solutions lies in making them work together to provide a comprehensive view of the enterprise security posture. This combined, chronological view of all security-relevant data enables the security team to prioritize events and responses and effectively engage with IT operations and other areas of the business.

It's nearly impossible to make effective business decisions using a product-by-product view of reports. Organizations that attempt this end up with an amalgamation of CSV-to-spreadsheet conversions that only provide a report-based view, delivered quarterly at best. Traditional security information and event management (SIEM) solutions provide an alternative to these highly manual processes but typically require that you eliminate or exclude data sources that don't fit into a schema, or simply can't be collected due to scalability issues. Leaving out specific data sources that don't appear on a list of supported products means forensic investigations are limited before they have begun. Forensic investigations need to be quickly assessed and turned into actionable intelligence to prevent a specific set of activities from happening in the future.



Splunk Enterprise, with its ability to scale to collect, index and report on terabytes of any machine-generated data, is ideally suited to meet these challenges. Expanding on a successful collaboration with Cisco/Ironport, Splunk and Cisco continue to work together to provide content for their other Cisco security offerings. The Splunk Cisco Security Suite provides saved searches, reports and dashboards to help security teams take full advantage of the information collected across their Cisco security devices. When combined with the core Splunk ability to index, search and report on data from any other security vendor technologies, the Splunk Cisco Security Suite enables a single, comprehensive view for complete situational awareness.

Apps and Add-ons for Cisco Security

Splunk for Cisco Security Solution

Our Cisco Security Suite includes multiple apps and add-ons that combine to create one solution running on the Splunk engine. The solution builds on the core Splunk capabilities, giving the security team the ability to search machine-generated data, perform root cause analysis and apply statistical analysis to measure adherence to key performance indicators (KPIs). The apps and add-ons within the Splunk for Cisco Security Suite support specific Cisco point solutions with out-of-the-box content, searches and reports all within a single UI.

Splunk Add-on for Cisco Firewall

The Cisco Adaptive Security Appliance (ASA) represents an evolution that began with the Cisco PIX first released in 1994. As threats have evolved so has the Cisco perimeter firewall, which in addition to firewall capabilities, includes IPS, VPN and content security functionality. In the firewall add-on, firewall and IPS log data are collected and classified using tags, field extractions and saved searches. Connections accepted and denied by port are just a small sample of the information available via the add-on that also supports firewall data from Cisco PIX and FWSM.

Splunk App for Ironport Email Security Appliance (ESA)

Approximately 90% of email activity is invalid (spam, viruses, etc.). To reduce invalid mail and protect against viruses and other malware, the security team must provide appropriate protection against email-borne threats. The Splunk App for ESA makes email transaction tracing simple with a form-search dashboard that allows you to enter information about the transaction, the sender, recipient and attachments and mine for any email transaction nested in the ESA logs. Splunk provides scalable, out-of-the-box reporting and saved searches that represent the most requested searches and analytics.

Splunk App for Ironport Web Security Appliance (WSA)

The number of web-born security threats has reached record proportions. It's easy for employees to click on a link that might result in the installation of a key-logger, root-kit or some other form of malware. Surfing to certain destinations can violate "appropriate use" policies. According to a recent survey, a rapid escalation in employee web surfing can be an indication of an employee looking to leave and perhaps take proprietary information with them. Splunk helps track and report on web surfing as logged by the WSA appliance. The Splunk App for WSA provides reports that support the HR professional's perspective when analyzing data from WSA and supports security teams that need to fulfill requests for evidence in HR actions.

Splunk Add-on for Cisco IPS - SDEE

Cisco IPS devices and modules use the Security Device Event Exchange (SDEE) message format and protocol to communicate events. Cisco routers, the ASA appliance, or the stand-alone

Cisco 4200 series can include an IPS module that produces SDEE log data. SDEE provides a rich level of reporting wherever the module is implemented or installed. The SDEE support extends to include Cisco global threat correlation, if IPS 7.0 is installed.

Splunk Add-on for Cisco Security Agent (CSA)

Cisco Security Agent (CSA) was the first endpoint security solution that combined zero-update attack defense, policy-driven data loss prevention and signature-based antivirus detection in a single agent. Through the Splunk Add-on for Cisco CSA, users gain additional insight and enhanced support for the CSA data that allows for historical and real-time views of host events as registered by CSA.

Sample scenarios and use cases:

- Correlation of Infected Host with Data Loss — Correlate an identified infected host (via IPS, ASA or WSA) with the loss of data via email or the web
- Threat Mapping with Reputation — Geo-locate the call home IP address of botnet traffic from Cisco ASA and Cisco WSA
- Botnet Events — Provide botnet activity based upon severity, category, website, source IP, geo-location and event type
- Security Change Audit — See real-time and historical changes by user, applied to security rules on all security appliances
- Personnel Access — Determine where a person was when any device using that person's credentials was involved in a security issue (e.g., an email containing spam, a botnet hosted by the person's computer) in real time
- Reputation with Global Correlation — Ratio of events for a period of time that were actionable using traditional IPS inspection vs. ones that incorporate reputation information (reputation filtering and reputation inspection)
- Ability to Import CS-MARS Archive Files into Splunk — Puts you in control over what log data from the security architecture you wish to have remain in MARS and what you want to view long-term in Splunk. Automatically pulls MARS data into Splunk for long-term historic trending

Visibility into Custom Application Logs

For comprehensive investigations and effective root-cause analysis, a review of data from traditional security sources typically isn't enough. Security events and their effect on mission critical applications need to be reviewed as part of the attack timeline.

Splunk's ability to accept multi-line application logs, its freeform search language and interactive interface let you see the complex characteristics of an incident. For example, Splunk can let you know that an attacker gained access to the network but was blocked at the application-level (avoiding further exploit).

The security picture is not complete without visibility into virtually "all the data," including applications. If a successful attack occurs, the security team should know the full extent, if any, of the data loss.

Cisco Data and Beyond

The Splunk for Cisco Security Suite leverages the native capabilities of the core Splunk engine. Splunk's core software provides the ability to search report, monitor and analyze real-time streaming and historical machine-generated data - physical or virtual. Splunk works across vendor environments, all from a single interface, and combines the view of security logs with application data on the same timeline.

To download the Cisco Security Suite, or the individual Cisco apps and add-ons please visit www.splunkbase.com where you can also find dozens of other apps and add-ons that run on top of Splunk.

Free Download

[Download Splunk](#) for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.