Joint Solution Brief

Accelerate Threat Detection and Response

The Challenge

Today's Security Operations Center (SOC) depends heavily on the ability to collect, correlate and analyze network events to quickly identify and respond to security threats – but getting access to the right traffic data from across the network, and without overloading the system, can be a challenge.

Integrated Solution

Splunk Enterprise Security is a Security Information and Event Management (SIEM) solution that provides insight into machine data generated from a wide variety of sources. Several components of the Gigamon product portfolio can help Splunk users accelerate and automate threat detection and mitigation in support of a stronger corporate security posture.

Joint Solution Benefits

- Accelerate and automate threat identification and mitigation.
- Utilize key metadata gathered from traffic flows across the network, targeting precise, critical information for analysis within the Splunk platform.
- Extend the capability and value of existing security architectures using these joint solutions, including third-party products utilizing the Adaptive Response Framework.
- Integrated solution to quickly get you up and running feeding highly relevant data into Splunk Enterprise for efficient security and operational control.
- Easily available for download from Splunkbase.

Introduction

Enterprise networks are essential to modern business. Growing numbers of electronic transactions and increasing network speeds means huge amounts of wire data are being created. The challenge SOC teams face when collecting, manipulating and analyzing this data is how to access it, how to get it into the right tool and how to handle the immense volumes of data to find relevant indicators of compromise. They need a way to reduce data volume and extract the relevant security information to quickly zero in on suspicious threats and anomalous behavior. They then need a way to automate further investigation and mitigation once a potential threat has been positively identified.

The Gigamon and Splunk Joint Solution

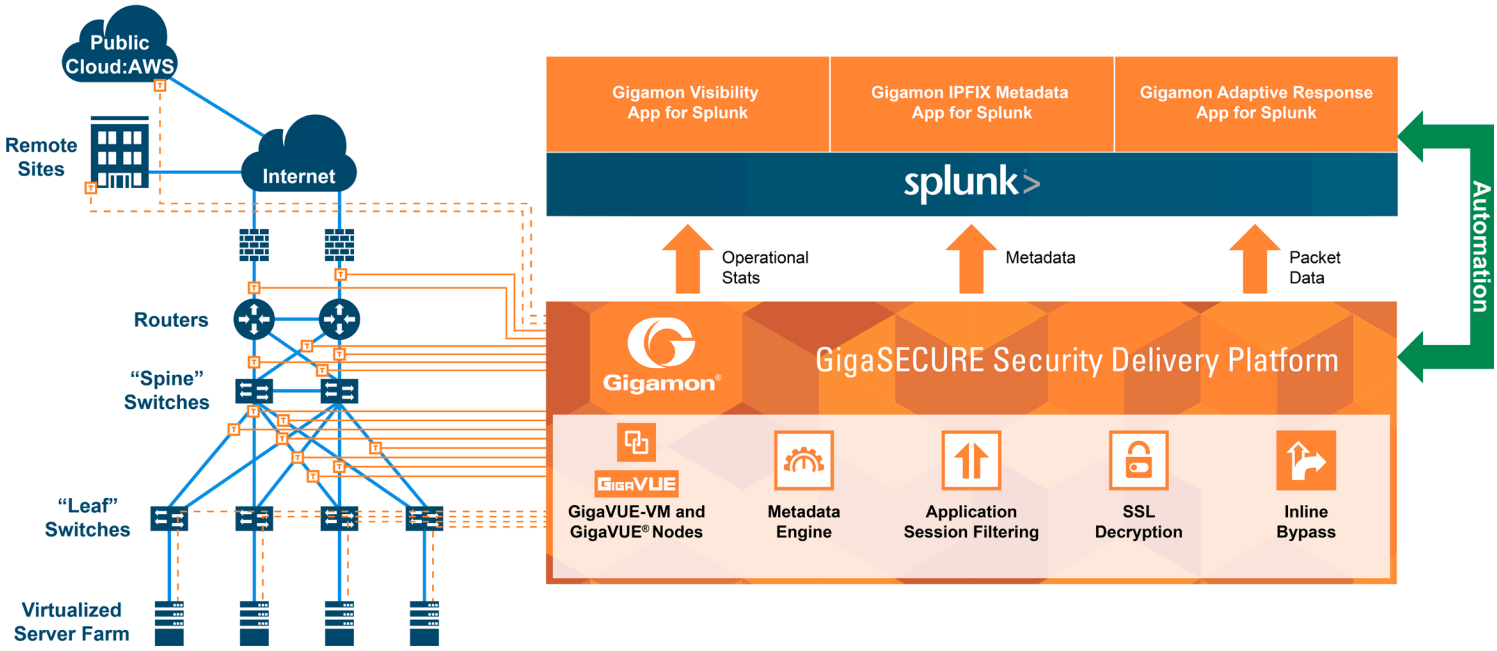
Splunk Enterprise Security has emerged as one of the leading platforms to deliver analytics-based security intelligence to security operations and incident response teams. Its ability to search, index and correlate across all types of machine data enables security administrators and operations teams incredible access to insights as to what is happening on their networks.

Of course, to fully utilize the power of this platform, users need to be able to help ensure that the right data from across their network in available – and can be easily indexed within the Splunk platform. This is where the GigaSECURE® Security Delivery Platform and Gigamon integrated applications for the Splunk solution come in.

The GigaSECURE Security Delivery Platform allows users to extract and consolidate metadata from any monitored network traffic flows, package them into NetFlow v5, v9, and IPFIX records, then send them to Splunk Enterprise for indexing.

Gigamon has enriched the IPFIX records with information including URL information, HTTP/HTTPS return codes, and DNS query/response information, all of which provide the ability to rapidly diagnose security events for use cases such as, identifying rogue DNS services on your network, spotting potential Command and Control server communications using high entropy domains and detecting use of untrusted or self-signed certificates for SSL-decrypted traffic that could indicate nefarious activity.

The Gigamon IPFIX Metadata Application for Splunk allows customers to easily select, index and display network metadata generated by the GigaSECURE Security Delivery Platform.



The GigaSECURE Security Delivery Platform also provides advanced network traffic isolation and filtering capabilities to send select or complete packet data directly to the Splunk software through its Application Session Filtering and patented FlowMapping® technologies. These intelligent traffic applications provide regular expression-based matching and filtering of traffic and application flows. These features can be used in combination with other GigaSECURE Security Delivery Platform capabilities such as de-duplication, packet slicing, masking and SSL/TLS decryption to help ensure that even when full packet data is required for security analysis, only the required packets and payload information are provided and indexed.

The Gigamon® Adaptive Response Application for Splunk enables SOC teams to execute automated actions on the GigaSECURE Security Delivery Platform in response to threats detected in the Splunk Enterprise Security solution as well as other third-party products that integrate with the Adaptive Response Framework.

Beyond traffic optimization, the Gigamon Visibility Application for Splunk also provides the Splunk operator with full visibility into the health of the GigaSECURE Security Delivery Platform, including a complete inventory of the nodes and ports available, the top and bottom port statistics, top conversations and applications and full GigaSMART® traffic intelligence statistics. This allows SOC teams to maintain single-pane monitoring from the Splunk platform and be more effective in securing their networks.

Download Now

The following Gigamon applications for Splunk can be downloaded at **www.splunkbase.splunk.com**.

- The Gigamon IPFIX Metadata App for Splunk
- The Gigamon Adaptive Response App for Splunk
- The Gigamon Visibility App for Splunk

Learn More

For more information on the Splunk and Gigamon solution, contact:

splunk> **www.splunk.com**

Gigamon® **www.gigamon.com**

3247-01 09/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com