Gigamon® | splunk>

Using Application Intelligence to Accelerate Threat Detection and Response

THE CHALLENGE

Today's Security Operations Center (SOC) depends heavily on the ability to collect, correlate and analyze relevant network events to quickly identify and respond to security threats. However, getting timely access to the right data from increasingly complex hybrid networks can be a challenge.

THE SOLUTION

Splunk Enterprise Security is a Security Information and Event Management (SIEM) solution that provides insight into machine and operational data generated from a wide variety of sources. The Gigamon Visibility and Analytics Fabric provides access to all data-in-motion across the hybrid network enabling Splunk users to accelerate and automate threat detection and mitigation to build a stronger security posture.

JOINT SOLUTION BENEFITS

+ Tightly integrated solution to feed relevant, context rich data into Splunk Enterprise for faster, more precise threat detection and response
+ Gigamon Application Intelligence and Adaptive Response Applications for Splunk are available for quick and easy download from Splunkbase

Introduction

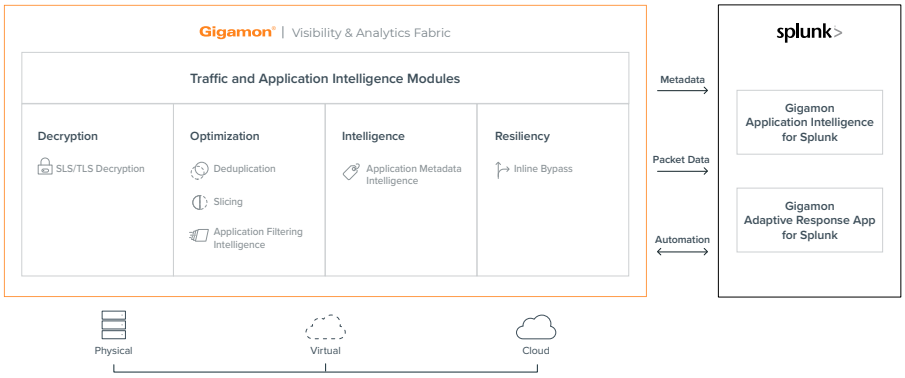
Enterprise networks are essential to modern business. Growing numbers of electronic transactions and increasing network speeds means huge amounts of wire data are being created. The challenge SOC teams face when collecting, manipulating and analyzing this data is how to access it, how to get it into 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 and to automate investigation and mitigation once a potential threat has been positively identified.

The Gigamon + Splunk Joint Solution

Splunk Enterprise is 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 all types of machine data enables InfoSec and SecOps teams to access powerful insights into everything that is happening on their networks.

To fully utilize the power of the Splunk platform, users need visibility and access to all relevant network data – this is where the Gigamon Visibility and Analytics Fabric and the Gigamon Application Intelligence for Splunk application deliver great business and operational benefits to Splunk users.

The Gigamon Application Intelligence for Splunk 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, which provide address a wide range of use-cases such as: identifying rogue DNS services, spotting potential Command and Control attacks, and detecting use of untrusted or self-signed SSL certificates.



Splunk users can now easily select, index and display network metadata generated by Gigamon. The Gigamon Visibility and Analytics Fabric also provides advanced expression-based network traffic filtering to send packet data directly to Splunk through its Application Filtering and patented FlowMapping® technologies. This capability is further enhanced by other Gigamon functions such as de-duplication, packet slicing, masking and SSL/TLS decryption, that reduce the amount of raw traffic and metadata sent to Splunk.

Using the Gigamon Application Intelligence for Splunk, SOC teams can execute automated actions in the Gigamon fabric to respond to threats detected in the Splunk Enterprise platform and other third-party products that integrate with the Adaptive Response Framework.

Gigamon and Splunk Use-Cases

Beyond traffic optimization, the Gigamon Application Intelligence for Splunk and Gigamon Adaptive Response Application for Splunk provides users with full visibility into all the data-in-motion on the network to augment log files and address use-cases including:

+ Avoiding business disruption by tracking expired and expiring SSL certificates and which application servers use these certificates
+ Minimizing shadow or rogue IT risks by identifying, for example, suspicious DNS activity
+ Optimizing customer experience by monitoring applications server performance
+ Mitigating compliance risks using metadata to identify unauthorized websites visited
+ Improving the speed and precision of threat detection by analyzing protocol metadata
+ Identify old or unsupported OS versions on servers that may pose security risks
+ When used with Gigamon TLS/SSL Decryption, Gigamon Application Intelligence for Splunk ensures visibility into TLS 1.3 encrypted traffic

Download Now

The Gigamon Application Intelligence for Splunk and Gigamon Adaptive Response Application for Splunk can be downloaded at www.splunkbase.splunk.com.

© 2017-2020 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.