Solution Brief

Gigamon Visibility App for Splunk

Challenges
IT Operators rely on a variety of appliances to analyze wire and traffic data for SIEM, Application and Network Performance monitoring and management. SEIM (Security, Incident and Event Management) vendors like Splunk, the industry’s leading SIEM vendor, are deployed to gain operational intelligence, as well as to analyze and visualize actionable insights from this machine data. Historically, SIEM vendors have focused on correlations across log data and alerts generated from these devices in order to flag events.

But, to really round out this Operational Intelligence, the SecOps and NetOps teams also need to consider the following scenarios:

• Get optimal traffic visibility for network traffic to these security and monitoring tools
• Visualize the health and trend patterns for this traffic visibility

The Gigamon Solution
Gigamon plays a key role in the SIEM ecosystem by facilitating the optimal delivery of traffic data to the passive sensors which generate logs used in alerts. By extracting traffic from various points in the network, using physical and virtual TAPs or SPAN ports, Gigamon provides filtered and customized streams of this traffic to Packet Capture Devices, Intrusion Detection Systems, Network Access Control platforms, and NetFlow Collectors among others.

Gigamon’s GigaSECURE® platform can be deployed to aggregate and isolate key traffic streams to feed packet data to the Splunk App for Stream or provide high-fidelity, un-sampled NetFlow or IPFIX records to the Splunk App for Enterprise Security (see Figure 1). The NetOps and SecOps teams can now gain network and security operational intelligence while visualizing the trends and patterns of the network traffic that signal bottlenecks and anomalies.

The Gigamon Visibility App for Splunk ( downloadable from the Splunk Store) can provide the ops teams with insight into the health and analytics of the Visibility Fabric. This app, which sources the data via open RESTful APIs from the GigaVUE-FM fabric manager, allows for first-level visibility and troubleshooting of infrastructure within Splunk.

In a multi-vendor SIEM deployment with Splunk (see Figure 2), operators could use:

• Third-party vendor appliances to trigger security alerts to Splunk based on KPIs
• Gigamon Visibility App for Splunk to visualize the policies and source of the traffic that caused the alerts

Figure 1: GigaSECURE platform provides traffic visibility to the Splunk apps and the Gigamon Visibility App for Splunk enables operational intelligence

© 2015 Gigamon. All rights reserved.
Gigamon Visibility App dashboards can be used to visualize the following information:

- Health and inventory of the Visibility Fabric (nodes, clusters, ports type and status)
- Port and Traffic Policy/Map properties and statistics (top ports, packet rate, discards, etc.)
- GigaSMART® operation statistics
- System and audit events
- Syslog notifications

**Key Use Cases**

- Customers using Splunk for SEIM analytics that also need wire and packet traffic data in addition to text/log data
- SecOps and NetOps teams that need Operational Intelligence from the Visibility Fabric to augment alerts from security appliances

**Key Benefits**

- OPEX savings: Splunk administrators can now augment their Operational Intelligence with Gigamon visibility health
- Reduces mean time to resolution (MTTR): Provides a first-level visibility, troubleshooting, and root-cause analysis of infrastructure within Splunk, for example, identify source, location, and traffic policy of the application or host that triggered a KPI alert