Gigamon® Lumeta®

Joint Solution Brief

Combating APTs: Correlating NetFlow with Threat Intelligence to Detect Threat Conversations

The Challenge

Advanced persistent threats (APTs) can inflict serious harm to a business. These sophisticated, covert attacks are bent on surreptitiously stealing valuable data from targeted and unsuspecting companies.

Integrated Solution

The Gigamon and Lumeta joint solution enables the use of NetFlow metadata for advanced cyber breach analytics—to detect real-time interactions (threat conversations) between internal origination points and adversaries. Gigamon's GigaSECURE® Security Delivery Platform can generate metadata information from any traffic flow in the network. Lumeta uses that data to provide behavioral analytics and cybersecurity breach detection for real-time monitoring.

Key Benefits

- Tap traffic from any point of interest in the network—from both physical and virtual network links—with the GigaSECURE Security Delivery Platform
- Generate NetFlow/IPFIX metadata from any traffic flow visible to the GigaSECURE platform and forward to Lumeta
- Correlate NetFlow against threat intelligence and compare with an authoritative network index in real time. The data is then filtered to produce contextual, useable information
- Help organization stay current on threats to its IT infrastructure
- Allow security professionals to proactively block security holes and prevent data loss

The Challenge

Advanced persistent threats (APTs) can inflict serious harm to a business. These sophisticated, covert attacks are bent on surreptitiously stealing valuable data—trade secrets, intellectual property, state and military secrets, computer source code, and any other high-value information available—from targeted and unsuspecting companies. These targeted attack techniques are being used on an ever-widening range of industries and sectors—not just governments, manufacturing, financial services organizations, and large energy and utilities companies. No one is immune.

One of the best ways to detect APT activities is to look for large, unexpected information flows of data from internal origination points to other internal computers or to external computers. It could be server to server, server to client, or network to network. To do this, you need a solution that has visibility to traffic across the network and the ability to spot suspicious behavior from normal business.

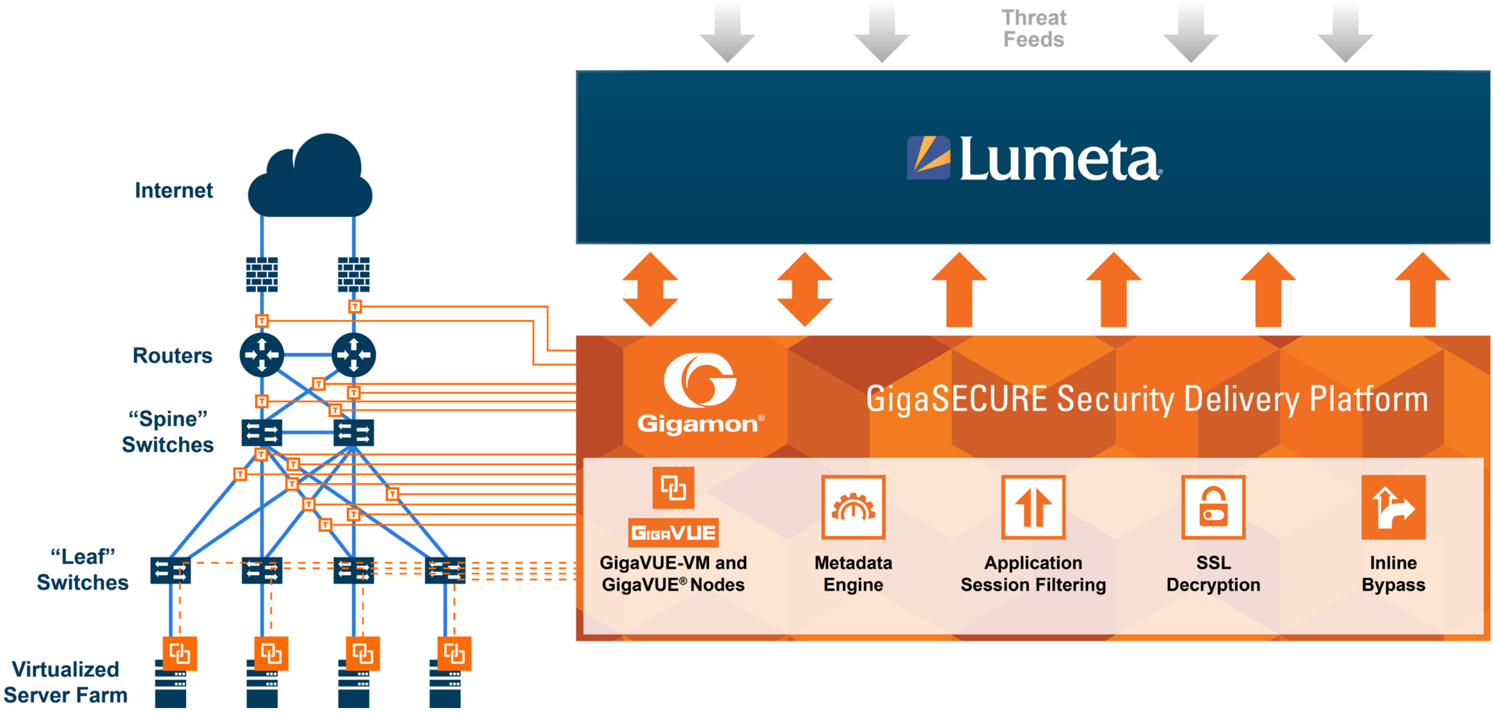
The Gigamon and Lumeta Joint Solution

Together, Gigamon and Lumeta allow you to take proactive and rigorous steps to detect APTs in their early stages and implement asset-protecting remediation.

The Lumeta ESI real-time network situational awareness platform is integrated with the Gigamon GigaSECURE Security Delivery Platform enabling use of NetFlow data for advanced cyber breach analytics—to determine if malware call back, command and control channels, and data exfiltration is happening or if cyber controls are in place and working. The combined solution allows users to detect, investigate and respond to real-time interactions (threat conversations) between internal origination points and adversaries.

How does it work?

- First, GigaSECURE generates NetFlow metadata from any physical and virtual network traffic streams forwarding them to Lumeta ESI. The GigaSECURE platform is extremely valuable for this task given its ability to generate unsampled records and due to its filtering capabilities. Traffic flows can be filtered in or out of the metadata records so that uninteresting traffic doesn't use up processing and analytic cycles.
- Next, Lumeta ESI parses open source and subscription intelligence feeds and repositories to enumerate known bad servers and networks and their associated attributes.



- Lumeta ESI then correlates the NetFlow data against the threat intelligence to identify threat conversations. These filtered results are stored in Lumeta’s HDFS database and are compared with Lumeta ESI’s authoritative index of network IP addresses to identify which device(s) is having the threat conversation.
- Suspect devices are reported (dashed and mapped) by Lumeta ESI. Based on these findings, IT security teams should investigate these machines further (perform incident response, isolate the device immediately, etc.).

Learn More

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

Lumeta
www.lumeta.com

Gigamon®
www.gigamon.com