Connect the Dots for Complex Attacks with Gigamon and Stellar Cyber

THE CHALLENGE

Organizations typically operate using dozens of siloed tools, which means they're working with siloed data. That creates blind spots, slows response times and makes it difficult to correlate common or related events. As a result, security analysts struggle to gather the right data to understand complex attacks.

THE SOLUTION

Integrated with the Gigamon Visibility and Analytics Fabric™ (VAF), Stellar Cyber's Open XDR Security Operations Platform pieces together attacks from across the IT infrastructure, enabling you to pinpoint signs of a large-scale breach.

JOINT SOLUTION BENEFITS

+ See and understand complex attacks so you can mitigate quickly and prevent them in the future
+ Work intuitively as you move from collecting data to detecting, investigating and responding to high-risk events
+ Eliminate tool fatigue and data overload and respond in seconds
+ Boost performance while reducing security operations center (SOC) costs
+ Manage existing security tools on one intuitive dashboard, with a single unified data lake and machine learning engine

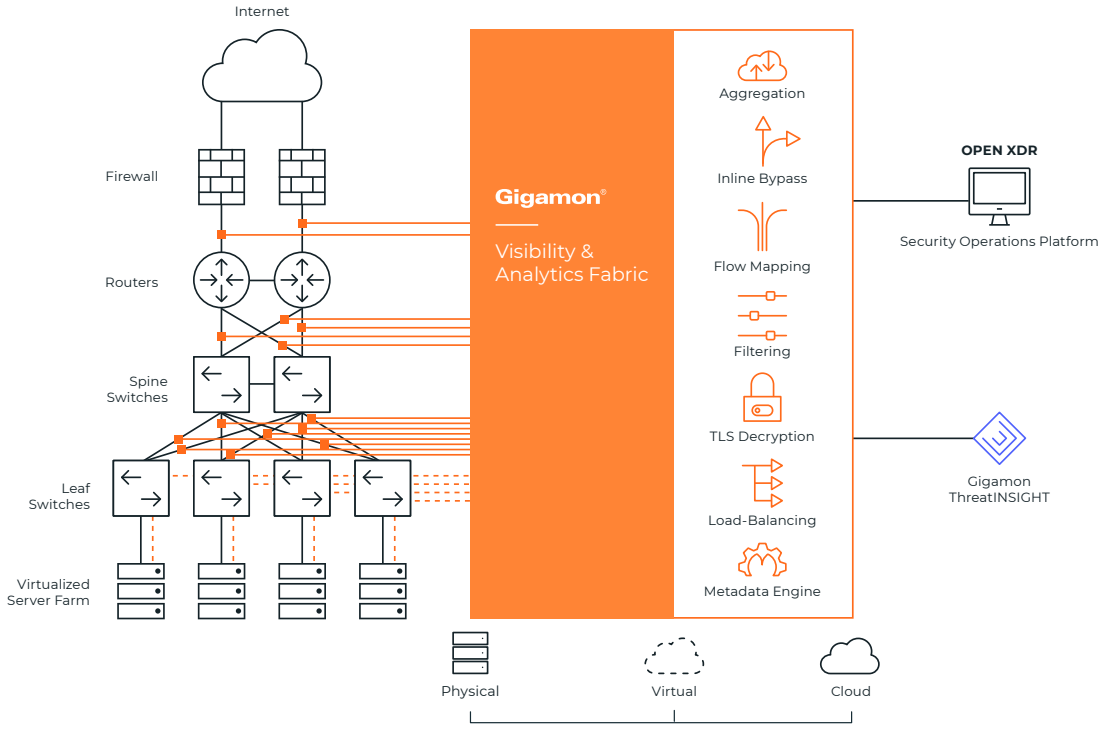
Introduction

Using both unsupervised and supervised machine learning, including deep learning for advanced analytics, Stellar Cyber's Open XDR Security Operations Platform is the only intelligent and cohesive security platform that provides maximum protection by connecting events across your IT infrastructure. That lets you operate more efficiently, dramatically reduce operational costs and detect attacks — fast — wherever they occur.

The Gigamon + Stellar Cyber Joint Solution

Key Gigamon VAF features that enhance Stellar Cyber's Open XDR Security Operations Platform include:

+ **Easy access to traffic from physical and virtual networks:** The VAF manages and delivers all network traffic — including East-West datacenter traffic and private and public cloud workloads — to the Open XDR platform so all traffic can be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior.
+ **Traffic filtering:** The VAF can be configured to send only relevant traffic — or relevant sessions — to the connected Open XDR, so it doesn't become overloaded with irrelevant traffic. This can be filtering on criteria ranging from IP address and TCP port number to over-the-top (OTT) application type.
+ **Load balancing to spread traffic across multiple devices:** When traffic flows are larger than a single Open XDR sensor instance can cope with, the VAF can distribute the flow across multiple Open XDR sensor instances while ensuring sessions are kept together. Additionally, Open XDR sensor numbers can be incrementally grown by adding new devices to those already connected.



+ **Aggregation to minimize tools' port use:** Where links have low traffic volumes, the VAF can aggregate these together before sending them to the Stellar Cyber Open XDR Platform in order to minimize the number of ports that need to be used. By tagging the traffic, the VAF ensures the source of traffic can be identified.
+ **SSL decryption:** The VAF decrypts SSL encrypted traffic for payload inspection by inline and out-of-band security tools, such as Open XDR, and other out of band monitoring tools.
+ **De-duplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid the unnecessary backhaul bandwidth and packet-processing overhead on Stellar Cyber's Open XDR, the VAF removes duplicates before they consume resources.
+ **Flow and Meta-data generation:** Gigamon nodes can generate unsampled NetFlow/IPFIX flow data for any traffic flow. Gigamon also generates extended rich IPFIX/CEF metadata records for things like HTTP response codes, DNS queries and OTT application attributes. This extended metadata can be used to provide far more detailed contextual analysis when looking at network and security events.
+ **Resilience of solution:** Deploy security devices inline and use the Gigamon Inline Bypass functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.
+ **Masking for security/compliance**: The VAF masks sensitive or confidential data within packets before they're sent to other tools, where they may be seen by unauthorized people.
+ **Subscriber-Aware Visibility:** Gigamon Flow Mapping® GTP correlation, Gigamon FlowVUE™ and Gigamon Application Session Filtering capabilities enable intelligent prioritization of subscriber traffic for tool processing targeted at service provider customers.

For more information on Gigamon and Stellar Cyber, visit: www.gigamon.com and stellarcyber.ai.