SOC AUTOMATION OF THREAT INVESTIGATION

White Paper

When a Security Operations Center (SOC) is shown on TV, it has a specific portrayal. There is a large wall full of screens. World maps showing the threat origins and targets are updating in real time. Desks are full of people behind monitors, each working on different tasks from maintenance, to investigation and response. However, when visiting a SOC in most companies, Gigamon included, it looks completely different. There are often only a few people there. The impressive dashboards of activity are instead a few screens, and the role of each screen is to list events. The people aren’t focused on individual systems; instead they all are doing many jobs to keep the SOC running, including monitoring systems, handling events, and deploying long-term projects.

The goal of these ‘real’ SOCs is to optimize the tools they have, reduce the noise from their tools to manageable levels, and automate as much of the process as possible. Their hope is that they can focus on the projects that will continue to enhance the security of the organization. Gigamon recently made a major step towards this goal by integrating the capabilities of its own Gigamon GigaSECURE® Security Delivery Platform with the advanced security detection and analysis provided by BluVector, as well as by automating the collection of all security events through Splunk Enterprise.

This white paper walks through how the Gigamon SOC utilizes the GigaSECURE Security Delivery Platform from Gigamon, BluVector® Cortex™ and Splunk Enterprise together to detect advanced threats, automate full packet capture and empower investigation, response and remediation. Included are the details of each component, how they are configured and integrated, and some example events that were addressed by this automated system. All IP addresses and URLs used in this document have been altered for security.
System Overview

The first step in automating the Gigamon SOC involved implementing a system that, when a malicious or suspicious event is detected, would alert the analyst team and initiate the recording of all traffic related to the host or hosts involved in the event. The SOC team wanted to have access to the network traffic so that they could quickly and effectively investigate incidents. However, recording all network traffic requires a significant investment in storage. Targeted recording tied to AI-based detection, on the other hand, provided the team with the information to investigate an event without the accompanying storage costs.

One of the considerations when building out this system was “why record and investigate when you could just automate blocking?” The Gigamon SOC team recognized that blocking, especially in the case of East-West traffic, isn’t just a security decision, it’s a business decision. Automatically blocking events can have the potential for significant negative impact on the business and its operations. Instead, by alerting on events and accelerating investigation and response, the security team is able to support the business today, while beginning to understand how best to enable a degree of automated blocking in the future.

Solution Components

The five security systems that make up this capability within the Gigamon SOC are: The Gigamon GigaSECURE Security Delivery Platform, BluVector Cortex, Splunk Enterprise, Phantom and Moloch. Below is an overview of these components and their respective configurations.

Component 1: Gigamon GigaSECURE Security Delivery Platform

The GigaSECURE Security Delivery Platform is a next-generation network packet broker that delivers visibility of network traffic to security tools focused on threat prevention, detection, analytics and forensics. The right tools get the right traffic at the right time.

The GigaSECURE Security Delivery Platform also brings to life the Defender Lifecycle Model, a new approach to security that addresses the increasing speed, volume and polymorphic nature of cyber threats. The model enables an organization to integrate security technologies that prevent, detect, predict and contain threats throughout your network. It’s a model that moves the advantage from the attacker back to the defender by integrating machine learning and AI-based technologies and automating security workflows.
The specific Gigamon appliance chosen for this deployment is the GigaVUE-HC2, which provides intelligent traffic visibility in a modular, mid-sized form factor to address complex network visibility requirements for both enterprise and service provider networks. With a broad spectrum of traffic management capabilities and a versatile, high-performance, multi-purpose design, GigaVUE-HC2 helps to future-proof IT.

Key features that drove the selection of the GigaVUE-HC2:

- Mid-sized form factor compressed dozens of ports into a small footprint, saving space, power, and cooling.
- Physical and logical bypass features protected traffic and inline tools, making the overall system more efficient and robust.
- Intelligent Flow Mapping® enabled complex traffic forwarding decisions at wire-speed performance.
- Embedded TAP modules consolidated secure access points in a compressed mode within the node for immediate backplane connectivity.
- GigaSMART® technology which included FlowVUE®, de-duplication and SSL/TLS decryption.

**Component 2: BluVector Cortex**

BluVector Cortex is an AI-driven sense and response network security platform. Designed for mid-sized to very large organizations, the platform makes it possible to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware and ransomware in real time.

At the heart of BluVector Cortex are three components:

1. A pair of AI-based detection engines that process traffic to detect file-based and file-less threats. The first is a patented, supervised machine learning engine trained to accurately identify zero-day and polymorphic malware. The second is a speculative code execution engine that is the cybersecurity industry's first solution specifically designed to find fileless malware traversing the network, in real time.

2. An intelligent decision support system that delivers context and visibility to threat security teams and their investigations by pre-correlating and highlighting log entries associated with events prioritized for analysis.

3. An extensible Connectors Framework that automates the hunt process, orchestrates response to threats and enables easy integration of additional security solutions.
Component 3: Splunk Enterprise

Splunk Enterprise monitors and analyzes machine data from any source to deliver Operational Intelligence to optimize NetOps, SecOps and business performance. It is a flexible platform that scales from focused use cases to an enterprise-wide analytics backbone.

The key features of Splunk Enterprise utilized within this solution are the collection and index of log and machine data. The extensive ecosystem of integration partners with Splunk empowered the creation of this solution.

Component 4: Phantom

The Phantom Platform integrates existing security technologies, providing a layer of connective tissue between them. Phantom can automate tasks, orchestrate workflows and support a broad range of SOC functions including event and case management, collaboration and reporting.

Component 5: Moloch

Moloch is a large scale, open source, full packet capturing, indexing and database system. Moloch is designed to be deployed across multiple clustered systems providing the ability to scale to handle multiple gigabits/sec of traffic. PCAP retention is based on available sensor disk space while metadata retention is based on the scale of the Elastic cluster. Both retention sizes can be increased at any time as they are under the analyst’s complete control.
Detection & Automated Response Process Flow

**Step 1: Gigamon Traffic Aggregation**

The GigaVUE-HC2 is configured to aggregate and de-duplicate all traffic from the Gigamon network through the SOC suite of security tools. This includes all North-South and East-West traffic. The SSL Decryption feature decrypts encrypted traffic to be passed for analysis.

To the right is the configuration screen for the GigaVUE® device in the Gigamon SOC.

**Step 2: BluVector Cortex Threat Detection**

As traffic is passed from the GigaVUE node, BluVector Cortex utilizes Bro to perform full content extraction, generation of basic network events (before enrichment by content processing) and correlation of intelligence indicators.

To the right is the BluVector Cortex Dashboard after it has identified an event. In this case, the event was a test file that was hosted on an internal webpage and then accessed by a second internal host.

The system detected the file using its AI-based detection and intelligence analytics engines:

1. **BluVector MLE** – a patented supervised Machine Learning Engine (MLE) developed to accurately detect zero-day and polymorphic malware in real time. BluVector MLE algorithms are pre-trained to immediately identify malicious content embedded within common file formats including Office documents, archives, executables, .pdf and system updates.

2. **BluVector SCE** – the security market’s first analytic engine specifically designed to detect fileless malware as it traverses the network. By emulating how the malware will behave when it is executed, the Speculative Code Execution (SCE) Engine determines, at line speed, what an input can do if executed and to what extent these behaviors might initiate a security breach. By covering all potential execution chains and focusing on malicious capacity rather than malicious behavior, the analytic technology vastly reduces the number of execution environments and the quantity of analytic results that must be investigated.

3. **Suricata** – BluVector Cortex also includes a Suricata engine for detection of known malicious network activity. BluVector Cortex comes configured at installation with multiple threat intelligence feeds. Gigamon also uses additional threat feeds that BluVector Cortex ingests via the STIX/TAXII standard.
**Step 3: BluVector Cortex Decision Support**

When an event occurs, the BluVector Cortex appliance calculates a hunt score based on the correlated results from the engines, including the integrated intelligence. Each engine has a weighting, and the weight of any imported intel, whether from a feed or custom intel generated by the analyst, can be adjusted to represent the confidence of the analyst in the intel.

The fully calculated hunt score ranges from 0-10, with a score of zero meaning that no threats were found. When BluVector Cortex does detect a threat, the platform provides the specific rules or intelligence that triggered during the detection process. This allows the analyst to quickly understand the drivers behind the detection, as well as helps reduce false positives.

The hunt scores are enriched with the network and file metadata surrounding the event. This comprehensive context allows an analyst to better understand the event and quickly investigate or respond to it.

This is the weighted hunt score of the event.

The name of a threat type, if it has already been seen in the wild.

The specific analysis engines that triggered a detection on the event are shown here, with a graphical representation of the scoring.

The list of metadata that is provided about the event and file or files relating to the event include all of the following elements:

<table>
<thead>
<tr>
<th>Network Metadata Elements</th>
<th>File Metadata Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>File Name</td>
</tr>
<tr>
<td>Time</td>
<td>File Type</td>
</tr>
<tr>
<td>Source IPv4 / IPv6</td>
<td>Magic String</td>
</tr>
<tr>
<td>Destination IPv4 / IPv6</td>
<td>File Size</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Sha256</td>
</tr>
<tr>
<td>Hostname</td>
<td>Most Recently Seen</td>
</tr>
<tr>
<td>Protocol</td>
<td>First Seen</td>
</tr>
<tr>
<td>Transport</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>Session ID</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>File Bytes</td>
<td></td>
</tr>
<tr>
<td>Partial File</td>
<td></td>
</tr>
<tr>
<td>Partial File Gap Length</td>
<td></td>
</tr>
<tr>
<td>Partial Gap Offset</td>
<td></td>
</tr>
<tr>
<td>BluVector Cortex Engines that triggered</td>
<td></td>
</tr>
<tr>
<td>HTTP Header</td>
<td></td>
</tr>
<tr>
<td>DNS Log</td>
<td></td>
</tr>
</tbody>
</table>
Step 4: Splunk Correlation

Once BluVector Cortex is integrated with Splunk Enterprise through BluVector’s Connectors Framework, all of the event data is available and correlated within Splunk Enterprise. The dashboard to the right is from Splunk Enterprise and shows all of the metadata from the captured event.

Looking at the metadata, it is clear that a file was transferred from IP 78.90.230.182 to IP 78.165.17.130. This file was the object that BluVector Cortex triggered on. Both of these IPs were inside of the network. If this were a true event, then it would indicate evidence of lateral movement. As many SOCs are not staffed 24/7, this phase would also generate an alert that is passed through the OpsGenie paging solution, which allows the SOC staff to be notified of critical events off-hours, resulting in reduced headcount requirements without loss of response capability.

Step 5: Phantom Triggers

The SOC team used Phantom to create an orchestration playbook. The playbook watches activity in Splunk Enterprise for malicious events reported by BluVector Cortex. When it sees an event, it triggers Moloch to start the PCAP capture process.
**Step 7: Investigation**

Before Gigamon put this system in place, the analyst would leverage the event data as a starting place, but taking any other step would require significant investigation and guesswork. A standard Gigamon investigation included:

- Scouring event logs related to that host to see if there is any traffic which might suggest compromise.
- Pulling the potentially compromised machine from production for analysis.
- Examining the system memory and storage for artifacts on the host.
- Re-imaging the potentially compromised machine.

Even after taking those steps, it still might not be clear if there was a compromise and if there was one, what, if anything, was exfiltrated. With this new, automated system, the analyst can instead look at actual traffic from that host and know for certain what happened and what steps need to be taken.
Conclusion

Today’s Security Operations Centers might lack the impressive visuals and facilities depicted on TV, but the reality is that they are still tasked with managing corporate networks in order to deliver protection from near-constant malware attacks.

Solutions, such as the BluVector and Gigamon ones described here, are critical for real world SOCs to be successful. All too often, a SOC requires that analysts try to find and address the alerts on each system, with no certainty if they are chasing down a real threat or a false positive. That chase alone is a daunting task when the SOC isn’t armed with the necessary context and network activity surrounding the event.

There are three major considerations to keep in mind when building solutions into the SOC:

1. **Visibility** – If the right network traffic isn’t delivered to security tools to analyze, then the quality of those tools doesn’t matter. Building out an infrastructure where all the network traffic can be analyzed is the critical first step.

2. **Detection** – The modern security landscape sees new threats every day, as well as a reemergence of old threats that have been changed to be unrecognizable to traditional security tools. The use of detection solutions that don’t rely on signatures, heuristics or forensic detection is one of the best methods to get ahead of these threats.

3. **Confidence** – Even with solutions to ensure that all the traffic is seen and analyzed, an analyst can be overcome with alert fatigue. This is the result of security solutions that have a low efficacy and therefore provide too many suspicious alerts. In these cases, SOC analysts spend their time confirming that nothing happened or trying to piece together what happened without evidence. With high confidence solutions, analysts are able focus on resolving actual malicious threats and events.

Solutions that address one or all of these considerations, like the Gigamon SOC solution described in this paper, reduce the time spent reacting to security events. This allows the SOC the time to handle the proactive tasks of improving the overall security profile of the organization. When a SOC can take proactive action and handle its tactical responsibilities simultaneously, it can operate as effectively as those giant installations seen on TV, even if it doesn’t have an army of people behind the screens.

For more information about the GigaSECURE Security Delivery Platform please visit: www.gigamon.com

Authors

Jack Hamm, Gigamon Senior Manager of Security Operations

Adrian Liu, Gigamon Director, Alliances and Business Development

Brian Ohlhausen, BluVector Director Strategy and Development

Josh Rosenthal, BluVector Alliances and Integrations Manager