Raise Your SIEMs IQ While Improving Their ROI

Gigamon®

SIEM Overview and Limitations

A Security Information and Event Management (SIEM) solution enables organizations to capture and analyze a wide variety of security event data to support early detection of attacks and breaches. SIEM systems collect, store, investigate and report on security data for threat mitigation, incident response, forensics and regulatory compliance. This technology aggregates event data produced by security devices, network infrastructure, host and endpoint systems, applications and cloud services. The primary data source is log data, but SIEM technology can also process other forms of data, such as JSON structured data and trace data as well as network telemetry (i.e. flows) and metadata.

With hundreds of thousands of dollars or more spent every year on purchases, maintenance and upgrades, IT views their SIEM tools as both an essential and expensive component of their security infrastructure. SIEM solutions are priced based on data volume ingestion, with add-on reporting functionality options. They can ingest raw packets as an add-on front-end function, but this is prohibitively expensive and virtually never done. Traditionally, they take in large amounts of NetFlow and log data, which can easily drive up licensing costs and overwhelm their storage.

Another concern with SIEMs is they often depend on unreliable sources of data. NetFlow is frequently limited to '5-tuple' details that lacks thorough insights and is typically sampled. Generated logs suffer from information gaps. Such gaps can be a consequence of how logs are created:

+ They are generally the end-product of coding by developers. The information in logs in many cases is intended to help developers, and not the operational teams that need to analyze them.
+ Generating logs consumes CPU resources, so log levels may be turned down ad hoc to reduce processing impact without considering the information needs of the InfoSec team.

For SIEMs to provide effective threat hunting and detect lateral movement attacks such as those involving command and control malware, utilizing real-time network traffic to obtain meaningful insights is imperative.

SIEMs offer a wide range of reports, but producing actionable information is challenging. That's because traditional data sources, such as log file data, don't include the contextual data behind an event that only network, and application metadata can provide. To work optimally, SIEMs need a critical mass of thousands of specific L3-7 metadata attributes across a broad swath of applications and protocols.

Gigamon is Key to Application Visibility and Optimizing SIEMs

The network is the ultimate source of telemetry data as it sees all traffic. The Gigamon® Visibility and Analytics Fabric™ (VAF) collects network data from across physical, virtual and cloud environments, transforms it and distributes optimized flows to the appropriate monitoring and security tools. With Gigamon, organizations can rely less on agents and endpoints, and instead obtain granular control over what gets sent to the SIEM. This also indirectly lowers TCO by allowing log levels to be reduced, therefore minimizing impact on server CPU processing and storage.

By specifying the type and granularity of information that is sent to SIEMs, InfoSec groups can be very precise about what data they receive. They gain full control of the data needed for analysis without having to rely on developers, IT support, and other teams. IT can tag this data, write simpler queries, ensure faster triage of incidents and events, address compliance issues and accelerate forensics.

Gigamon is able to provide all tools, including SIEMs, with telemetry data all the way up the OSI stack including the applications themselves. Gigamon leverages TAPs deployed throughout the data center infrastructure, including those involving agents running within virtual workloads, as VMs installed on each hypervisor or as containers within a pod for comprehensive visibility. IT can customize the data required and how it's processed, and then send that information to SIEMs such as those from Splunk and IBM QRadar. Adapters and templates have been developed for these tools to ease the ingestion and parsing of incoming CEF or IPFIX-formatted metadata, writing of queries, generating detailed and customizable reports, obtaining real-time alerts and more.

Providing application-aware metadata to the SIEM for more contextual insights and the framework behind the network data yields faster detection, triage and response times. Gigamon Application Metadata Intelligence (AMI), which is deployed with the Gigamon VAF™, generates over 5,000 L3-7 metadata elements across more than 3,200 applications. InfoSec teams can granularly select those attributes that are needed. This extensive list of attributes can be utilized by the SIEMs to solve a host of use cases thereby making them more effective and indirectly reducing TCO by reducing or eliminating other security tool needs.

Another way to increase tool efficiency and increase ROI is by reducing unnecessary application traffic going to the SIEMs. Gigamon Application Filtering Intelligence (AFI), offloads SIEMS by reducing the total volume of data they receive without losing any pertinent information. The result is lower licensing expense.

Using Application Metadata to Cost-Effectively Boost the Power of SIEMs

The Gigamon VAF with AMI provides advanced L3 to L7 metadata to assist IT understanding of application and user behavior. AMI sends relevant application metadata to the SIEMs for security analysis, helping IT teams better correlate application behavior and analyze log data from servers and security appliances.

SIEMs leverage metadata attributes to deliver the insight and analytics needed to manage the opportunities and risks associated with digital transformation. SecOps administrators can automate detection of anomalies in the network and stop cyberattacks that overcome perimeter or endpoint protection.

Gigamon not only lowers the cost of SIEMs, but also makes them more powerful in solving numerous security issues. In some cases, other security tools may be reduced or eliminated to further improve the overall ROI.

Here are examples of how organizations can use AMI to identify potential security breaches early:

SPOT DATA EXFILTRATION ATTEMPTS

Organizations can provide their SIEMS with AMI-generated DNS attributes to find malicious attempts by hackers to steal confidential information. IT can evaluate the volume and type of DNS requests, including non-standard ports, at various domain levels including DNS queries involving entropy, statistics, outliers and record types. This data can reveal DNS tunneling in the network and help establish the legitimacy of domains.

DETECT SUSPICIOUS NETWORK ACTIVITY

This involves identifying command and control attacks using machine learning. Admins can determine whether a domain is legitimate or was generated using a botnet-controlled domain generating algorithm (DGA). SecOps can verify authenticity by leveraging external sources such as VirusTotal. AMI dashboards of interest here include the total unique domains seen on the network and those predicted to be legitimate vs DGA generated. Lists of domains predicted to be legitimate versus those from DGAs can be derived. A history of a typical manual adjustments can also predict fraudulent use.

UNCOVER UNAUTHORIZED EXTERNAL REMOTE CONNECTIONS

In this scenario, AMI assists SIEMs in identifying suspicious SSH, RDP and Telnet remote connections. This is done by looking at 'leading indicators' such as bandwidth usage, longevity of these connections, IP reputation and geolocation. A list of suspicious remote sessions can be created to validate malicious intent. Such an investigation can help uncover the detection of unauthorized external remote connections used for data exfiltration. By removing fraudulent remote sessions, the amount of traffic needed to be sent to DLP solutions can be reduced and their volume-based cost minimized.

RECOGNIZE DUBIOUS USER ACTIVITY

Abnormal user login activity can be identified using AMI metadata. Hacker techniques include brute-force attacks on the network involving highly privileged users involving false login IDs; these attacks can be identified by evaluating clients who are logging in from unauthorized systems or have an unusually high level of login activity. User credentials may also have been compromised such that the same user is seen logging in from more than two hosts from different locations. AMI attributes for the SIEM to evaluate include the total number of login sessions observed and multiple logins by the same user.

DEPRECATED PROTOCOLS AND SERVICES: LOCATE WEAK CIPHERS

Working with SIEMs, AMI can help ensure security compliance. Ideally, clients and servers should only employ the strongest cipher suites available and negotiate to one of these during the TLS handshake, but this is not always the case. Metadata can reveal all TLS connections, including those with weak ciphers, along with the applications and systems hosting these apps. IT can be alerted to the use of weak ciphers seen in the live network on TLS connections, including TLS 1.3, and take corrective action.

ANALYZE TARGET TIME WINDOWS

AMI allows IT to derive an end-to-end picture of various security events. This is supported by leveraging metadata with SIEMs to look at Kerberos, SMB, DNS and HTTP use. By isolating prior and post protocol activities that led up to an incident, security breach origins can be found. Administrators can find all activities of each host in a specified time frame.

INVESTIGATE HTTP CLIENT ERRORS

AMI in conjunction with SIEMs can identify additional suspicious activity by analyzing HTTP client errors including the number of HTTP response code errors relative to the total number of codes. Also, the distribution of these errors and the clients seeing these codes can give insight into malicious activity. This also provides details about client IP and the number of errors it has encountered and can indicate a hacker is trying a brute force attack and getting 401 errors.

DETECT ROGUE DNS AND DHCP SERVERS

Attackers can potentially host shadow IT operations with unauthorized servers within the network for diverting traffic and launching man-in-the-middle attacks. In this use case, leveraging AMI attributes with SIEMs allows evaluation of the following details about DNS and DHCP servers in your network. This includes the total number of DNS servers and list of rogue DNS servers; the total number of DHCP servers and list of rogue DHCP Servers; and the list of trusted/publicly known servers. This enables the ability to distinguish unsanctioned from legitimate servers.

IDENTIFICATION OF EXPIRED TLS CERTIFICATES

TLS certificates help facilitate encryption and authentication and are effectively mandatory for web servers. Without them, visitors will quickly move on. With validity dates becoming shorter (some only for a few weeks), it is imperative to find those that are defunct. There are several metadata attributes to spot them.

AMI provides certificate expiry dates as well as any revoked or expired certificates, along with the names of the application servers using these, to tools such as SIEMs for compliance reasons. Also, this allows the detection of the existence and use of untrusted or self-signed TLS certificates, which could indicate nefarious activity. Other relevant AMI attributes include Valid Not Before, Valid Not After, Serial Numbers and Signature Algorithm that help SIEMs validate certificate use. Real-time alerts can be automatically generated to expedite remediation.

MONITOR AND CONTROL FILE ACCESS

Remote workforces routinely download and upload files involving FTP, SMB and CFS protocols for applications from various file sharing service vendors such as Dropbox and Box. It is imperative that IT obtain insights into which clients are obtaining specified files. Otherwise malicious activity, such as disgruntled employees acquiring material without being disclosed or uploading files containing malware, will occur without detection.

Gigamon AFI can not only identify the applications and protocols in play, but AMI attributes can be used by SIEMs to generate lists of files involved, source and destination IP addresses of the end-users and other information and be displayed in a dashboard. Thus, determining who is accessing what files for forensic purposes. DLP and other tools can subsequently be used to prevent future fraudulent activities.

Moving from Reactive to Proactive Security

Organizations using Gigamon VAF with AMI to feed tools like Splunk and QRadar can go from retroactively looking at forensic data, isolating and remediating lapses in security, to proactively identifying threats before they do harm. Each SIEM tool interacts with the GigaVUE®-FM fabric manager and leverages the Gigamon Adaptive Response Application (GARA) , to make changes to traffic flows based on anomaly detections. Administrators can use select attributes and proactively implement corrective action in real-time. For example, administrators can:

+ Take filenames in combination with usernames, and automatically generate and send an alert to a security tool to block or temporarily quarantine specific downloaded files or links based on those attributes.
+ Utilize metadata about an email attachment file to automatically generate alerts that will ensure this file type is sent to a sandboxing tool for analysis prior to opening.

By integrating the SIEM's adaptive response framework with GigaVUE-FM and GARA, administrators can receive alerts to take preventative actions. This includes using GigaVUE-FM to redirect certain application or traffic flows to specific security tools such as advanced threat protection or secure email gateways. These actions can be bound to correlation searches on the SIEM for automated response or executed on an ad-hoc basis with notable events.

Reduce Unnecessary SIEM Traffic to Minimize Licensing Charges

The Gigamon VAF provides several methods to reduce total data volumes received by SIEMs. Each approach by itself can dramatically reduce flows, log files and events. Taken in totality, they can cut traffic by potentially over 90 percent. These include:

LEVERAGING APPLICATION METADATA RATHER THAN LOGS

The extensive critical mass of rich application-level metadata available can be used in many cases to replace traffic-related logs, such as DNS server logs, that have historically been sent to SIEM tools. This can dramatically reduce traffic flows while boosting SIEM effectiveness. Often, logs can be duplicated and further overload the tools. Furthermore, logs do not provide keen insights that Gigamon AMI can; some examples include:

+ Identification: social media user, file and video names, SQL requests
+ HTTP: URL identification, command response codes
+ DNS parameters: request/response, queries and device identifiers
+ IMAP and SMTP email-based communications with sender and receiver addresses
+ Service identification: audio, video, chat and file transfers for VoIP and messaging
+ Database attributes to correlate SQL queries with query parameter values: error codes, authentication type, user's login/password strings, unique identifiers
+ SSL certificates attributes: Valid Not Before/ After, Serial Number, Signature Algorithm, Server Name Indication, Subject Alt Name, Subject Pub Key Size

AMI also makes available dozens of elements for mainstream apps such as Facebook, YouTube, Gmail and Yahoo. Attributes for protocols such as FTS and SIP are also available.

ELIMINATING PACKET DUPLICATION

One significant cause of superfluous traffic is from duplicate packets. This results when switch mirror or SPAN ports are employed or multiple TAPs are deployed and aggregated throughout the data center to acquire necessary traffic, resulting in redundant copies of packets. Unfortunately, these additional copies can well exceed 80 percent of total traffic volume. SIEMs are forced to spend CPU cycles identifying and eliminating these duplicate packets which are also driving up volume-related expenses.

GigaSMART® De-Duplication identifies and eliminates duplicate packets and sends optimized flows to SIEMs. It offloads the de-duplication task from these tools, allowing IT to centralize the deduplication function and potentially cut traffic volumes and licensing fees in half. This also significantly improves SIEM effectiveness and accuracy.

GigaSMART De-Duplication is robust, accurate and customizable. Duplicate packet detection can be tuned to improve accuracy and effectiveness. For example, specify whether two packets that are identical, except for specific headers or fields (e.g. MAC address, IP TOS or TCP Sequence number), are considered duplicates. In addition, the duplicate detection window is configurable to align with the network traffic acquisition deployment.

FILTERING OUT LOW-RISK APPLICATIONS AND ASSOCIATED FLOWS/METADATA

Threat detection tools such as SIEMs are primarily interested in events based on suspicious traffic. To optimize tool performance and to prevent traffic from hogging limited tool capacity and driving up costs, it's best to not feed them information from high-volume/low- risk applications. Some content can be deemed safe by design, such as high-bandwidth Netflix or Hulu streaming media and Windows updates. This content does not have, for instance, hidden command and control code and it's from a known, secure source. IT needs to distinguish this from other content that is not safe, such as certain YouTube channels and many other

apps where the content could contain hidden malware. As a result, the log files and other data from them can be safely ignored and SIEM traffic ingestion minimized.

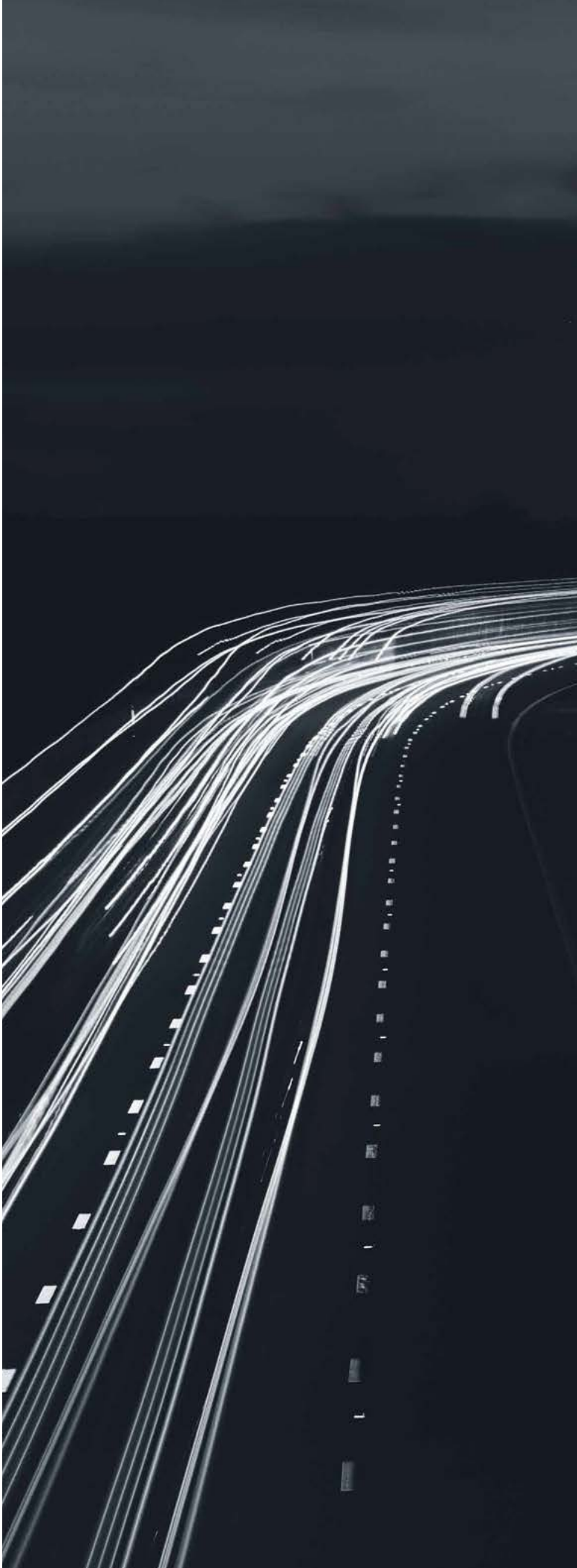
Gigamon Application Filtering Intelligence (AFI) enables IT to identify and screen content from selected applications. In turn, the raw packets, log files and metadata associated with them can be explicitly blocked from being sent to the SIEM. As safe streaming media traffic levels can easily exceed 50 percent of the total, this can greatly reduce SIEM traffic ingestion and cost. AFI uses deep packet inspection (DPI) to identify applications and protocols from network packets and filter them as appropriate.

AFI classifies applications based on various attributes around traffic behavior, and involves flow-based matching, bi-directional flow correlation, heuristics and statistical analysis. This lets SecOps accurately identify and filter traffic from over 3,000 common and well-known applications, as well as from unusual or custom apps. AFI provides this discovery process independent of encapsulation, port number or encryption

FOCUSING ON RELEVANT FLOWS TO OPTIMIZE SECURITY TOOLS

Some network tools focus exclusively on certain applications and protocols, and therefore feeding them anything outside of a narrow protocol suite (HTTP or email, for example) is unnecessary. If SIEMs spend processing power inspecting all network traffic, then most of that tools' resources are expended without yielding any additional threat detection. To optimize tool performance, therefore, it's best to refine traffic with a laser focus upon specific applications or protocols and offload irrelevant traffic from expensive resources.

Gigamon AFI identifies applications, protocols and encapsulated traffic. Selected applications that don't involve particular threats where SIEMs would be of value can be ignored to reduce their traffic and lower SIEM expenses. However, it is imperative that shadow IT or rogue apps be found and properly evaluated.



THROTTLING BANDWIDTH BY APP

AFI provides not only the identification of numerous apps, but also the amount of capacity they are drawing. The main dashboard shows the top ten apps by usage, as well as details on all other apps and traffic levels. With employees misusing corporate resources for Facebook, Instagram or other social networking sites or streaming media, these non-critical, personal-use-only apps can not only cause higher priority traffic to suffer performance loss — particularly as a home-based workforce shifts network traffic from LANs to WANs — but can provide higher loads and costs on SIEMs.

AFI can be used to identify these bandwidth hogs to facilitate enforcement of bandwidth limits by application via rate-limiting and other methods. Excessive non-business-related traffic and their associated logs and metadata can be minimized to further reduce SIEM load.

PROVIDE COMPLETE CONTROL OVER DATA SOURCES TO REDUCE TRAFFIC

In typical datacenter architectures, NetOps often place numerous physical TAPs throughout the network to mirror all traffic and direct to all security and monitoring tools. NetOps lack the granular capability to only monitor and direct traffic from workloads of interest, such as those prone to result in security events. SIEMs are forced to take in all the resultant log data.

Gigamon provides the needed VM and container visibility for any environment – including public, private or hybrid clouds. Through our GigaVUE G-vTAP™ virtual TAPs for VM and container infrastructures and the GigaVUE V Series virtual visibility nodes, IT can easily and automatically place these solutions only on or near the workloads they want to monitor. These software instances can selectively filter out irrelevant sources of packet data from VMs or container pods and even specified ports. This unnecessary packet data is not sent to the SIEMs, thereby reducing their processing load volumes.

LOAD BALANCE SIEM INGRESS TRAFFIC TO BOOST EFFICIENCY

Network levels are far from static and typically involve transient traffic spikes that vary by server farm type and location. SIEM tools also involve multiple instances of varying ingress capacity levels. To maximize SIEM availability and align inputs to their ability to handle dynamic loads at any given time, incoming traffic should be logically divided among the various SIEM ports or instances. This means adding load balancing support, either through a separate load balancer appliance or basic DNS round robin method at added expense and complexity.

Gigamon provides load balancing that divides and distributes traffic among multiple SIEM instances (and other tools as well) so network and security visibility can scale beyond the capacity a single SIEM instance can support. Using effective load balancing techniques, traffic flows can be distributed based on a variety of options: bandwidth, cumulative traffic, packet rate, connections, round robin and stateless hashing. Incoming traffic and SIEM capacity are matched. The need for overprovisioning SIEMs is reduced while availability increases.

Load balancing allows operators to include any port in the node as a member of the SIEM group, as well as ports operating at different speeds. SecOps can also use load balancing to weight server-traffic delivery on a per-port basis, to accommodate bandwidth differences or processing capabilities of attached SIEMs, or match and load balance based on inner addressing within encapsulated and tunneled packets. With Gigamon IT can:

+ Help scale network infrastructure by dividing traffic between two or more SIEM instances when volume exceeds a single tool or tool port's capacity
+ Improve efficiency by weighting traffic application delivery to match tool processing capabilities or port bandwidth capacity
+ Automatically redistribute traffic to remaining SIEMs in case of failure and subsequently restore SIEM availability for new traffic upon its recovery

Conclusion

The Gigamon VAF, leveraging Application Intelligence (including AMI and AFI), gives InfoSec unparalleled visibility into OSI model Layers 3–7 of the network communications. Powered by deep packet inspection, this solution uniquely provides summarized and context-aware information about raw packets to obtain advanced application-aware insights. These assist threat hunters to identify and resolve security concerns.

Security teams can now control what content is pertinent, and then surgically tune and send only that information without touching endpoints, servers or router SPAN ports. Armed with that knowledge, organizations can efficiently manage, monitor and secure their infrastructure even as more of the workforce logs on remotely; using SIEMs already in place without the need for costly network or tooling upgrades. The value of SIEMs is dramatically raised while simultaneously lowering their licensing costs and overall TCO; combining SIEMs with VAF provides numerous benefits:

+ Proactively identify and remediate potential security infrastructure vulnerabilities
+ Support investigators hunting threats and breaches from shadow IT and file-sharing sites
+ Secure communication links by observing broad Layer 4 to 7 metadata to prevent malicious commands
+ Assist tools to ensure resource security by viewing and blocking actions such as social media users, and requested file and video names
+ Ensure that the new wave of North-south traffic doesn't overwhelm SIEM performance by generating and sending only relevant metadata
+ Reduce the load of log data flooding into SIEM tools from other monitoring and security tools as well as from network elements and applications
+ Simplify SIEM tool deployment

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

Gigamon has been awarded over 75 technology patents and enjoys industryleading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com