Using Wire Data for Security Forensics

A Next-Generation Approach to Attack Detection and Remediation

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for VIAVI Solutions

March 2019

VIAVI Solutions

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Security threats and attacks are growing in number and becoming increasingly more malicious, posing a severe threat to business survival. To reach the goal of quickly and accurately identifying and effectively responding to incidents, security operations teams have a seemingly insatiable need for more information to provide context for improving accuracy. That ongoing requirement drives the need for more tools.

While NetOps often leverages network packet capture or flow data for troubleshooting, in recent years, companies have seen increased adoption by security teams for incident response and forensic analysis to augment existing defenses and get on top of these threats. Forty-four percent of organizations are using packet capture for network or security troubleshooting, and 32 percent are using flows for the same purpose. Only seven percent of organizations are using both packet and flow datasets. Due to the complexity of effectively stitching the data together, fewer companies can successfully combine data sources to take full advantage of all the data they are collecting to create a unified, high-value dataset.

Only seven percent of organizations are using both packet and flow datasets. Due to the complexity of effectively stitching the data together, fewer companies can successfully combine data sources to take full advantage of all the data they are collecting to create a unified, high-value dataset.

This white paper explains the means and importance of moving to a full wire data collection and enhancement strategy for both NetOps and SecOps operational and forensic capabilities. VIAVI Solutions offers a single platform to integrate wire data with user, log, and other data streams to improve context and increase collaboration while reducing overall tool costs and complexity.

NetOps Needs Enhanced Wire Data for App Performance and End-User Experience Monitoring

In today's digital economy, network performance often determines business performance. For example, a network impedance or failure that causes lagging performance increases website, form, and transaction abandonment. This is a significant issue that plagues businesses and reduces their bottom lines. Across industries, 2018 rates for form abandonment rose as high as 26 percent[1] while 2018 transaction abandonment averaged about 53 percent.[2] While pricing is a factor in transaction abandonment, application and website performance drops cause as much as a 75 percent increase in abandonment and a 50 percent decrease in customer loyalty.[3]

If a performance lag turns into an outage, things get worse. The cost of a network outage on an e-retailer averages about $5,600 USD per minute at most times of the year. However, during various holidays, the losses can reach into the millions of dollars per minute for a large e-retailer.[4] NetOps use packet and/or flow information to monitor numerous aspects of application response and performance to avoid such issues.

However, to track users to the point of being able to distinguish people from bots and separate the benign activities from the malicious, companies also need a much richer dataset. This can include device and user trait information like interface information, DNS, domain and LDAP information, authentication and identity, IP address, and device ID. However, collecting and combining these pieces of information is a time-consuming, manual process. More often than not, pulling them together manually is not feasible, so it never happens.

[1] 5 Tips to Reduce Web-Form Abandonment
[2] The Secret to Reducing Transaction Abandonment
[3] 31 Shopping Cart Abandonment Statistics For 2018
[4] What Does a Network Outage Really Cost?

SecOps Needs Enhanced Wire Data for Hunting and Forensics

While NetOps is focused on identifying performance issues to maintain application function and keep usability at the optimum level, SecOps is monitoring systems to identify both internal and external threats.

For SecOps, the stakes are equally high. IBM's 2018 Cost of Data Breach study found that the global mean cost of a breach is $3.65 million USD.[5] Organizations take 197 days on average to identify a data breach, and 69 days to contain the breach once it is identified.[6] Breaches lead to lost revenue, a tarnished brand image, and customer churn. Breaches can often lead to the loss of valuable intellectual property. Liability for lost customer data is potentially immense, with formidable governmental and organizational regulatory penalties.

When a breach occurs, SecOps must be prepared to deliver quick answers to these critical questions:

- What was compromised and/or exposed?
- Who was responsible for the vulnerability?
- Who was responsible for the attack itself?
- Has the breach been resolved?
- Can the resolution be validated?

SecOps teams have a wide array of tools to address these questions. The tools arsenal includes firewalls, intrusion prevention systems (IPS), security incident and event management (SIEM) systems, data loss prevention (DLP) systems, and many others. While these solutions can detect or prevent many breaches, they don't catch them all. Individually, they can't necessarily help IT understand the full nature of an attack and the extent to which it was successful.

Despite these tools, in many cases, the information to identify the breach at the time of occurence isn't available or the team does not have the ability to pull the siloed data points together to identify the scope of the breach, so forensic experts have to be called in to figure it out. In high-profile cases like Equifax and Target, the costs for those efforts were tremendous. Equifax has thus far spent a net of about $439 million USD[7] with a final cost estimated to exceed $600 million, while Target spent a net of about $202 million USD.[8] Most of these funds were spent on the hourly cost of professional forensics teams scouring through numerous log repositories to stitch together the required information. These examples help demonstrate the value of having high-quality, real-time forensic data on hand. Having better threat detection and forensics up front would most likely have reduced these costs by a factor of ten or greater.

Some distributed denial of service (DDoS) attacks are actually smokescreens meant to overwhelm or distract network and security monitoring systems so an attack can sneak through. Here, too, wire-based monitoring can help.

In the DDoS/smokescreen scenario, packet-based monitoring can detect the performance problems indicative of a DDoS attack and determine whether existing security tools are able to cope with it. Flow data presents an excellent overview of the protocols and volumes of traffic to help SecOps understand whether a flood of traffic is, in fact, a DDoS attack. Next, analytics provide insights on the other activities going on behind the scenes—or at least at a much smaller footprint—revealing how the attack is related to other activity on the network. If the DDoS attack is a distraction, SecOps can scan the network for the associated attack, while performing enhanced data forensics to define the scope of the attack, incident, or breach.

There are numerous scenarios in which analytics across enhanced wire data bolster SecOps. For example, a packet monitoring tool can often identify the anomalous network behavior associated with a malware attack, such as a situation in which a Russian IP address starts sending a large volume of HTTP requests directly to a database server.

[5] IBM/Ponemon 2018 Cost of a Data Breach study
[6] IBM/Ponemon 2018 Cost of a Data Breach study
[7] https://www.pymnts.com/news/security-and-risk/2018/equifax-cost-275m
[8] Target Pays Millions to Settle State Data Breach Lawsuits

Once this attack is detected, SecOps can use flows enriched with authentication and system process and log information to reveal:

- Where the attack came from
- Which users (if any) were involved
- Which internal assets communicated with the malicious activity
- What data was accessed in the attack
- Whether (and how) the attack spread laterally through the network

A Single Platform Delivering Answers to SecOps and NetOps

EMA asked organizations to identify the top three challenges limiting their ability to succeed in security. Forty-nine percent of respondents identified a lack of vendor-enabled integration as an issue. That was the top response. Forty-six percent identified a lack of analytics capabilities. That was the second-highest answer.[9] EMA also asked NetOps and SecOps teams to rank five items in terms of their influence on decision-making around automation. The final aggregate ranking is as follows: Accuracy, Integration, Price, Ease of Use, and Scalability.[10] This clearly supports the need for better information in single place.

After a team is alerted to an incident of interest by its monitoring systems, engineers can use enhanced wire data to better fuel analytical tools to corroborate and scope the event for faster and more surgical response. While standard wire data tools using packets and flows can recreate much of the relevant context, the ability to augment that foundational data with infrastructure and user data in the same platform would be a boon for operations.

In advanced organizations, both NetOps and SecOps teams have been using much of the same data with different enrichments for years. However, few have been able to connect the dots to understand how each can benefit from the other's expertise and augmentative data. Even SIEMs traditionally had data association and enrichment limitations that hindered advanced analysis and timeliness. They lacked the ability to provide a singular, enriched dataset that had sufficient power to open the door for a new area of tech called security analytics. Using advanced analytics across a broad set of combined source data, such as source and destination IP addresses with packet contents, MAC addresses, interface information, usernames, domain details, system logs, and process information, and further enhancing it with metadata, NetOps and SecOps can more accurately identify incidents and breaches. The inclusion of forensic-quality source data, enriched with a myriad of metadata in a single platform with built-in analytics, creates huge synergies and operational efficiencies.

The inclusion of forensic-quality source data, enriched with a myriad of metadata in a single platform with built-in analytics, creates huge synergies and operational efficiencies.

VIAVI Enhances Wire Data, Further Increasing its Value to SecOps and NetOps

VIAVI Solutions Observer offers an integrated platform with Apex™, GigaStor™, and GigaFlow™. Observer intelligently overlays packet information with multiple additional data sources to create an enriched record of the network conversations and maintains the original information unaltered for future use. This provides in-depth details on network device types, connectivity, traffic control, transactions, and usage patterns, down to individual users and hosts for all communication traversing the environment for extended periods of time. All information is stored in a relational database for fast access to any relevant information.

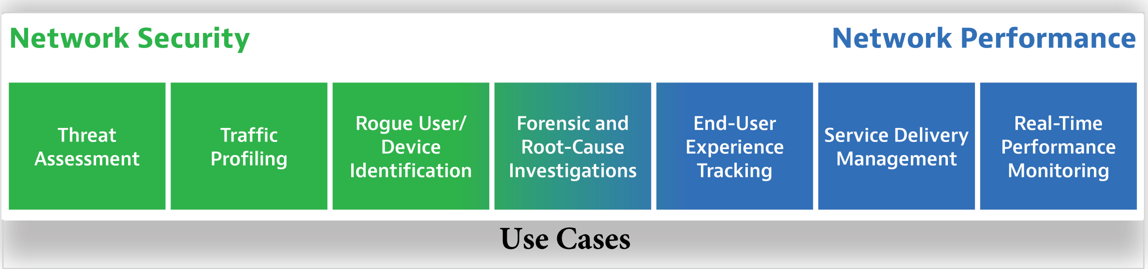
[9] EMA 2019 High-Fidelity Research study
[10] EMA 2019 High-Fidelity Research study

NetOps value this for service troubleshooting and end-user experience monitoring, while SecOps can exploit the same data to enhance existing security solutions. SecOps does this by hunting for previously undetected threats based on suspicious activity that have circumvented other security counter measures or by validating known breaches. It also can greatly accelerate remediation and post-event cleanup, minimizing damage and satisfying the privacy reporting requirements from regulations like GDPR.

Additionally, Observer Apex provides NetOps with centralized management of the end-user experience through active identification of unexpected performance. It does this while giving SecOps strengthened defenses through entity behavior analytics and in-depth, post-event security forensics. Apex leverages multiple data sources to learn expected behavior over time, and can then grade and rank incidents based on a highly accurate, context-driven severity ranking.

Apex has out-of-the-box workflows to begin assessing performance and site-based issues with real-time dashboards to manage and monitor critical resources. Its on-the-fly application dependency mapping offers both SecOps and NetOps fast discovery of app interdependencies with map visualizations to clarify complex relationships. Incidents are sorted by status (critical, warning, and good), so users can quickly assign troubleshooting priority.

Observer, NetOps and SecOps can fluidly address many critical use cases with a single platform.


Network Security
Network Performance
Threat Assessment
Traffic Profiling
Rogue User/ Device Identification
Forensic and Root-Cause Investigations
End-User Experience Tracking
Service Delivery Management
Real-Time Performance Monitoring
Use Cases

EMA Perspective

EMA research found that SecOps teams have recognized the value of network packets for analyzing and responding to security events. This research also found that NetOps and SecOps are collaborating to mitigate security threats, and this is becoming more and more critical to business survival.

In operations, context is king, and data silos only facilitate attackers. To be successful in defense and response, defending teams must be able to collaborate effortlessly and share data fluidly. Tools cannot be the source of any friction.

VIAVI Solutions has created a modular platform for the collection, enhancement, and analysis of data. The company provides a single platform to support NetOps and SecOps. Additional use cases in application and storage delivery are easily included in the foundational NetOps and SecOps use cases identified earlier in this paper.

VIAVI Observer is a highly componentized platform with integrations into other major network infrastructure and security tools, such as Cisco FirePOWER IPS, a leading intrusion prevention solution. From within FirePOWER's management console, users can access Observer GigaStor's long-term wire data and analysis.

From within the context of a snapshot view of a security event in the FirePOWER console, users can even replay network events that were reconstructed from packet captures in Observer GigaStor.

With the currently broad and widening datasets available to both inject and export from Observer, VIAVI is delivering success for IT.

About VIAVI Solutions

VIAVI (NASDAQ: VIAV) is a global provider of network test, monitoring, and assurance solutions to communications service providers, enterprises, and their ecosystems, supported by a worldwide channel community including VIAVI Velocity Solution Partners. We deliver end-to-end visibility across physical, virtual, and hybrid networks, enabling customers to optimize connectivity, quality of experience, and profitability. VIAVI is also a leader in high-performance thin film optical coatings, providing light management solutions to anti-counterfeiting, consumer electronics, automotive, defense, and instrumentation markets. Learn more about VIAVI at www.viavisolutions.com/enterprise. Follow us on VIAVI Perspectives, LinkedIn, Twitter, YouTube, and Facebook.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3700.031819