QOSMOS

Use Case Study

Security Information and Event Management (SIEM) Use Case

With 5 Billion IoT devices by the end of this decade*, next generation SIEMs need to tackle latest security breaches and issues with advanced analysis.

** Source: Data Breach Investigation Report (DBIR) 2015, Verizon*

Overview

2015 Security Challenges

- Advanced evasion techniques (AET) and advanced persistence threats (APT) used in sophisticated attacks
- Logs of data captured by the SIEM are growing due to BYOD (mobile) trends
- Organizations need to comply with regulatory standards leveraging multiple types of use cases with different data types
- Full solutions tend to be expensive leveraging in some cases Managed Security Service Provider (MSSP) options
- Automated solutions required to shorten actions as counter attacks

The Solution

- Unify the full packet capture and NetFlow sources of information
- Integrate cost effective DPI probe with advanced classification techniques
- Provide the richest set of data to shift from content to context analysis

Benefits of DPI Probes for SIEM Users

- Faster response to security incidents
- Complete visibility of network-based security risks
- More detailed and actionable information for overall stronger cyber protection

Typical Features of Best-in-class DPI Probes for SIEMs

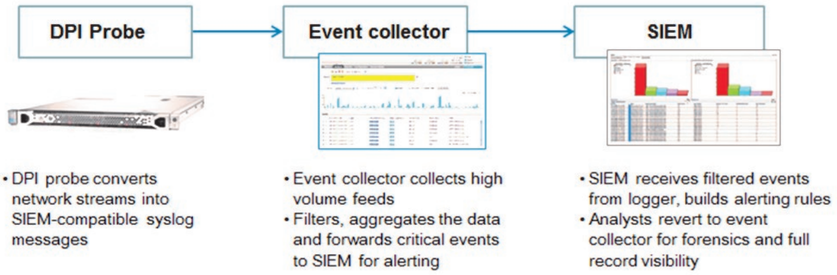
- Classification of flows up to OSI layer 7, exported in a forensic data stream of syslog or syslog in SIEM format
- Transparent upgrade, with no impact on any existing systems
- Rich set of continuously updated protocols and metadata,

Speeding Up Discovery and Containment with DPI Probes Feeding SIEM

Security Information and Event Management systems (SIEMs) are widely used by security analysts to protect sensitive network assets from the most advanced cyber threats. To discover and contain these threats, SIEMs have typically used two sources of traffic information for network forensic analysis:

- Full packet capture: detailed information for better understanding of breaches, but long investigation times and expensive storage of traffic for significant periods
- NetFlow: short investigation times but very limited information and therefore limited ability to discover and contain breaches

A new approach using a DPI probe combines the best of full packet capture and NetFlow: the probe produces forensically relevant traffic information and enables short investigation times. With the addition of traffic records from the DPI probe, security tools like SIEMs can typically reduce time to discovery and containment from weeks to days.



- DPI probe converts network streams into SIEM-compatible syslog messages

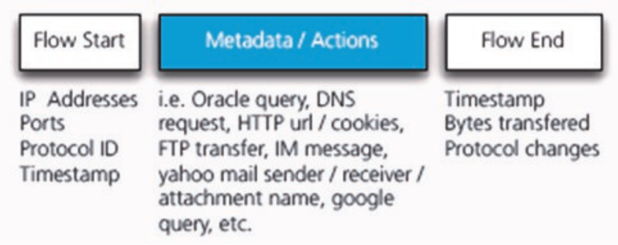
- Event collector collects high volume feeds
- Filters, aggregates the data and forwards critical events to SIEM for alerting

- SIEM receives filtered events from logger, builds alerting rules
- Analysts revert to event collector for forensics and full record visibility

Example of implementation: DPI probe feeding event collector and SIEM

Enriching SIEMs with a Stream of Network Application Behavior

A DPI probe generates a new source of information for SIEMs, in the form of a rich stream of application behavior that security analysts can use to make better and faster decisions. The probe inspects network traffic in real time, and classifies it into organized flows, describing the protocols and associated metadata. This metadata consists of actions or behaviors taken inside the session, as illustrated below:

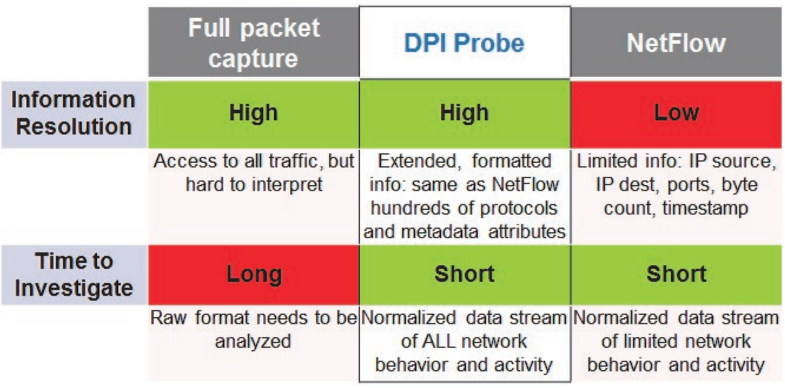


Flow Start	Metadata / Actions	Flow End
IP Addresses Ports Protocol ID Timestamp	i.e. Oracle query, DNS request, HTTP url / cookies, FTP transfer, IM message, yahoo mail sender / receiver / attachment name, google query, etc.	Timestamp Bytes transfered Protocol changes

Combining the Best of Full Packet Capture and NetFlow

The cost and scale of full packet capture systems has limited their practical reach into data centers, with data retention averaging 3-4 weeks. In addition, as more applications become virtualized and are placed in the cloud, access between services has become costly, if not impossible to achieve.

A DPI probe provides traffic information that describes the critical behavior of applications and protocols, formatted in a normalized data stream for easy consumption by SIEM solutions. It brings together the best of the full packet capture and NetFlow environments, as described in the table below:



	Full packet capture	DPI Probe	NetFlow
Information Resolution	High	High	Low
	Access to all traffic, but hard to interpret	Extended, formatted info: same as NetFlow hundreds of protocols and metadata attributes	Limited info: IP source, IP dest, ports, byte count, timestamp
Time to Investigate	Long	Short	Short
	Raw format needs to be analyzed	Normalized data stream of ALL network behavior and activity	Normalized data stream of limited network behavior and activity

By creating a forensically accurate stream in a compact format, a DPI probe can reduce the size of forensic data by 150x compared to full packet capture. The small footprint also means the DPI probe can be run as a virtual appliance, since the bandwidth overhead of a VM chassis is relatively small when exported (critical to bandwidth-limited, shared chassis). This allows a security team to collect much more data. A year's worth of data can be stored when using a DPI probe with a SIEM, compared to the typical 3-4 weeks of data available with full packet capture.

According to the 2015 Data Breach Investigation Report*, in 60% of cases, attackers are able to compromise an organization within minutes, 23% of recipients now open phishing messages and 11% click on attachments with 50% within the first hour and 15% of incidents still take days to discover. This illustrates the vulnerability of relying only on full packet capture, manual interventions and content analysis.

A DPI probe brings application and user behavior to a SIEM at an unprecedented level. Analysts are able to examine usage patterns (common URLs, SQL queries) and build simple but more accurate alerting rules for their environments, with a high degree of confidence.

**Source: Data Breach Investigation Report (DBIR) 2015, Verizon*

Example: Using a DPI Probe to Contain a Spear Phishing Attack

Spear phishing campaigns have generated significant problems for enterprise security teams in the past years. The ease of crafting and executing this type of attack has made them common in all areas, from credit card fraud to industrial espionage. It is especially difficult to assess the extent of an attack and to contain it rapidly enough. If we look at a traditional attack, a strong forensic record is crucial for analysis:
Finding target email addresses and attack vectors, finding who clicked on phishing link and got infected, understanding the extent of the damage…

Conclusion

Security attacks have extended beyond the realm of signature-based detection, and now require behavioral detection; but tools such as SIEMs today lack the right forensic visibility. By using a DPI probe to generate network metadata, behavior is more easily identified for forensic investigations and better alerting rules.

QOSMOS
The Network is Information

Qosmos is the leader in embedded Deep Packet Inspection and L7 Network Intelligence for use in physical, virtualized and SDN architectures. The company's software development kit and components are embedded by vendors and integrators into their products sold to telcos and enterprises. For more information: www.qosmos.com