White Paper

How Corelight Smart PCAP gives defenders 100% visibility

Introduction

When security investigations require packets, defenders have traditionally turned to full packet capture. This approach, however, often leaves analysts with only a few hours or days worth of traffic to analyze due to prohibitive storage costs. With average attacker dwell times measured in months not minutes, this limited lookback window kneecaps an analyst’s ability to go back in time and understand what happened. Moreover, full packet capture does not integrate well with modern SIEM workflows, forcing analysts to “chair swivel” from their SIEM into another pane of glass to locate and retrieve packets.

Corelight Smart PCAP for the AP 3000 Sensor and AP 5000 Sensor delivers a superior and more cost-effective solution, offering up 50% cost savings and 10x longer retention vs. full packet capture, with 1-click SIEM packet retrieval for streamlined investigations. How? Through Corelight’s Zeek-based protocol analyzers that give defenders comprehensive, yet compact network log evidence and the ability to easily configure precise packet captures. With Corelight logs and captured packets, defenders can achieve 100% visibility and investigate network activity that occurred months, even years, in the past.

Capturing the packets that count

What makes Corelight Smart PCAP so smart? First, it does not waste energy capturing encrypted or file-based traffic since Corelight can already extract files and generate rich, actionable visibility around encrypted traffic without decryption. How? By parsing and logging the observable characteristics of encrypted protocols (e.g. SSH, RDP and SSL) and enriching these logs with powerful encrypted insights that reveals inferred behaviors such as large file transfers over SSH or RDP brute forcing activity.

Thus, with Corelight Smart PCAP analysts can dramatically extend their packet lookback window vs. full PCAP by targeting just the 10-20% of their traffic that contains unencrypted, non file-based packets. This
solution is also smart in that it tracks traffic across port and protocol and allows analysts to quickly build robust packet capture rules using capture levers tied to protocols, anomalous activity, alerts, and more.

*Figure 1: Packet capture levers supported by Corelight Smart PCAP:*

- all
- all-unencrypted
- dce-rpc
- dhcp
- dnp3
- dnp3-tcp
- dnp3-udp
- dns
- dts
- encrypted-rdp
- filetransfer
- ftp
- ftp-data
- gtpv1
- http
- imap
- irc
- modbus
- mqtt
- mysql
- notice
- ntlm
- ntp
- protocol-violation
- radius
- rdp
- rfb
- smb
- smtp
- snmp
- socks
- syslog
- teredo
- sip
- ssl
- unknown-dns-reply
- unknown-tcp
- unknown-udp
- weird

Corelight recommends a baseline capture rule for Smart PCAP (see Figure 2 below) that combines the unknown-tcp, unknown-udp, and all-unencrypted capture levers and configures the capture byte depth for the latter (all-unencrypted traffic) to capture only the first 2,000 bytes of those connections.

*Figure 2: Corelight Smart PCAP UI showing lever configurations for a new capture rule*

This specific Smart PCAP rule depicted above takes just a minute to configure and gives organizations 100% network coverage by capturing packets for all connections not already parsed and logged by
Corelight, along with the first 2,000 bytes of all unencrypted traffic to supplement Corelight logs. This means analysts will have a source of network evidence for every connection that crosses the wire, whether that's in the form of a Corelight log, captured packets, or both!

1-Click SIEM Retrieval Drives Efficient Investigations

To support incident response and threat hunting organizations can stream Corelight's logs to their SIEM of choice. Smart PCAP integrates seamlessly into this workflow by appending a URL for the captured packets to Corelight's conn.log (See URL highlighted in Figure 3 below), giving analysts the ability to 1-click retrieve and load the packets in Wireshark for further analysis.

Figure 3: A Corelight conn.log viewed in Splunk with its 1-click packet retrieval URL highlighted

Corelight's SIEM workflow integration can save analysts considerable time that would otherwise be spent in another UI locating and pulling the packets needed for an investigation. With Smart PCAP, analysts can pivot from an alert, to a connection log, to captured packets right from their SIEM in less than a minute.
Up to 10x Longer Retention with Flexible Storage Options

Corelight Smart PCAP stores packets on external Dell PowerVault storage arrays, with a range of supported configurations (see tables below), giving security teams flexibility and offering considerable cost savings (up to 50%) compared to full PCAP. With Corelight Smart PCAP and max storage, analysts gain weeks to months of packet look back capability and months to years worth of logs in their SIEM.

Table 1: Corelight Smart PCAP storage configurations for PowerVault ME4012 with 12TB drives

<table>
<thead>
<tr>
<th></th>
<th>Config 1</th>
<th>Config 2</th>
<th>Config 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Model</td>
<td>PowerVault ME4012 (iSCSI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td># of drives/unit</td>
<td>12 x 12TB</td>
<td>12 x 12TB</td>
<td>12 x 12TB</td>
</tr>
<tr>
<td>Expansion units (ME412)</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>120TB</td>
<td>240TB</td>
<td>480TB</td>
</tr>
<tr>
<td>Rack Space</td>
<td>2RU</td>
<td>4RU</td>
<td>8RU</td>
</tr>
<tr>
<td>Estimated Retention (10% of 10G)</td>
<td>11 days</td>
<td>22 days</td>
<td>44 days</td>
</tr>
<tr>
<td>Estimated Retention (10% of 15G)</td>
<td>7 days</td>
<td>14 days</td>
<td>29 days</td>
</tr>
</tbody>
</table>

Table 2: Corelight Smart PCAP storage configurations for PowerVault ME4012 with 8TB drives

<table>
<thead>
<tr>
<th></th>
<th>Config 4</th>
<th>Config 5</th>
<th>Config 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Model</td>
<td>PowerVault ME4012 (iSCSI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td># of drives/unit</td>
<td>12 x 8TB</td>
<td>12 x 8TB</td>
<td>12 x 8TB</td>
</tr>
<tr>
<td>Expansion units (ME412)</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>80TB</td>
<td>160TB</td>
<td>320TB</td>
</tr>
<tr>
<td>Rack Space</td>
<td>2RU</td>
<td>4RU</td>
<td>8RU</td>
</tr>
<tr>
<td>Estimated retention (10% of 10G)</td>
<td>7 days</td>
<td>14 days</td>
<td>29 days</td>
</tr>
<tr>
<td>Estimated retention (10% of 15G)</td>
<td>4 days</td>
<td>9 days</td>
<td>19 days</td>
</tr>
</tbody>
</table>
Table 3: Corelight Smart PCAP storage configurations for PowerVault ME4084 with 8TB & 12TB drives

<table>
<thead>
<tr>
<th></th>
<th>Config 7</th>
<th>Config 8</th>
<th>Config 9</th>
<th>Config 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Model</td>
<td>PowerVault ME4084 (iSCSI)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of drives/unit</td>
<td>84 x 8TB</td>
<td>84 x 12TB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expansion units (ME484)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>650TB</td>
<td>1.3PB</td>
<td>1PB</td>
<td>2PB</td>
</tr>
<tr>
<td>Rack Space</td>
<td>5RU</td>
<td>10RU</td>
<td>5RU</td>
<td>10RU</td>
</tr>
<tr>
<td>Retention Rates (10% of 10G)</td>
<td>60 days</td>
<td>120 days</td>
<td>92 days</td>
<td>185 days</td>
</tr>
<tr>
<td>Retention Rates (10% of 65G)</td>
<td>9 days</td>
<td>18 days</td>
<td>14 days</td>
<td>28 days</td>
</tr>
</tbody>
</table>

Conclusion

Elite defenders report that they can resolve the vast majority of their investigations with just Corelight's logs, but some investigations will invariably require packet-level visibility to resolve. The challenge here is that legacy PCAP solutions were designed primarily around the needs of IT teams where network problems are usually identified in real-time (e.g. DNS requests failing) and their short packet lookback windows (hours to days worth of visibility) satisfy most IT use cases.

Security teams are built differently and need to be able to investigate network events in real time as well as events that happened months in the past for deep investigations. With Smart PCAP, Corelight has designed an elegant and purpose-built packet capture solution for security teams that can extend their packet lookback window up to 10x with 50% cost-savings vs. full packet capture solutions. Moreover, Corelight's solution interlinks the captured packets with Corelight's alerts and log evidence to accelerate investigations, with embedded PCAP URLs in Corelight's conn.log that give investigators a 1-click packet retrieval option during an investigation.
Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com  |  888-547-9497