



Case study: Leveraging Splunk for complete and seamless network visibility



Splunk in brief

Splunk is the leading software platform for machine data, enabling customers to gain real-time operational intelligence. Their mission is to address the challenges and opportunities of managing massive streams of machine-generated big data.

Challenge: tackling billions of logs

As one of the most versatile event management tools on the market, Splunk is utilized across industries to collect data from security, network, and server assets throughout the corporate infrastructure. In order to provide the needed insight into network security and performance, any unusual activity registered by Splunk must be analyzed and prioritized.

This task is typically managed by Security and Network Operations Centers (SOCs and NOCs) working to condense billions of log notifications to the highest priority actionable events. But while Splunk collects a substantial amount of event data, it doesn't provide the full recording of what has been sent and received on

the network. SOCs and NOCs therefore need a way to corroborate and resolve any events that look suspicious.

"The average cost of time wasted responding to inaccurate and erroneous intelligence can average \$1.27 million annually."

Ponemon Institute Survey

Solution: Splunk / Pandion integration

This is where Napatech Pandion can help. Pandion provides full continuous packet capture that can be matched to Splunk events or any other anomaly observed. As we shall demonstrate below, everything is stored to disk and the data can then be used by operations staff for further investigation.

Case 1

In our first use case, an SOC security engineer working for a financial services firm is investigating a Splunk event, sent by Suricata, with a suspicious domain name.

Challenge

While Splunk collects a substantial amount of data, it doesn't provide the full recording of what has been sent and received on a network. Security and Network Operations Centers therefore need a tool to investigate any events that look suspicious.

Solution

With the Splunk / Pandion integration, everything is recorded and stored to disk and the data can be accessed directly for further investigation.

Benefits

Thanks to its industry-leading search speed, Pandion provides insights in mere seconds, allowing the Splunk user to determine the full scope of the event and provide remediation. Pandion can be seamlessly integrated with any existing Splunk solution, allowing businesses to leverage earlier investments.



A corresponding event from the firewall indicates that a connection was attempted to the resolved address. To further investigate this activity, the SOC engineer clicks on the event in Splunk, uses the Pandion workflow, and in just a few seconds sees the full packet record corresponding to the name resolution and the subsequent connection.

Without this information, the decision to report or disregard the event would have been based on assumption alone. But by analyzing the packet data, the SOC engineer can determine exactly what was sent/received to the suspicious address, whether or not a harmful document was downloaded, and if any information was actually sent out of the infrastructure. So the Splunk event can be resolved for severity and impact without conjecture or incomplete info.

Case 2

In our second use case, an NOC analyst working at a social media agency sees an application alert in Splunk for slow/no response and needs to identify the exact area of concern; an exercise which could prove time consuming and complex. But with the Pandion / Splunk integration, the NOC analyst can

simply click on the event, search for packets, and quickly determine which infrastructure area is likely at fault: network, server or database. Inevitably, the stakeholders in each of these areas would only have visibility of their own domain, and would tend to claim that there is “no trouble found”. But with this solution, the raw packet data will conclusively show which part of the organization needs to action the event and provide a root cause analysis.

Case 3

In our third use case, an Incident Responder working for a major Defense Contractor notices that a network security device has sent an alert into Splunk indicating suspicious SSL traffic. In this case, the server may be vulnerable to “heartbleed”, where the vulnerability exposes information in memory from recent web transactions, including cleartext usernames and passwords. The Incident Responder clicks on the event in Splunk and by analyzing the packets he can directly determine:

1. whether the bug seems to have been exploited successfully
2. exactly what information was obtained through the vulnerability

“An organization can receive an average of nearly 17,000 malware alerts in a typical week. The time to respond to these alerts is a severe drain on an organization’s financial resources and IT security personnel.”

Ponemon Institute Survey

Benefits

As we have seen, Pandion provides an easy workflow. By clicking on any event in Splunk, the operations user can immediately get the full network packet trace that corresponds to the Splunk event. Thanks to its industry leading search speed, Pandion provides an answer in mere seconds, allowing the Splunk user to determine the full scope of the event and instantly provide the needed remediation.

Pandion can be seamlessly integrated with any existing Splunk solution, allowing businesses to leverage earlier investments and realize substantial savings.

For further information, visit:

www.napatech.com/products/pandion

EUROPE, MIDDLE EAST AND AFRICA

Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

NORTH AMERICA

Napatech inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.

Tel. +1 888 318 8288
info@napatech.com
www.napatech.com

APAC

Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

Napatech Korea
Seoul, South Korea
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com