Integrating Splunk with Endace Always-On Packet Capture

splunk>

Together, Endace and Splunk bolster security and performance by combining real time answers from your connected machine data with streamlined access to network-wide packet capture for rapid, conclusive, issue investigtation and resolution.

Splunk® Enterprise is an industry-leading software platform for collecting and correlating machine data generated by a variety of different IT systems and infrastructure components. Customers use Splunk to provide real-time visibility into network security and performance issues, detect threats and analyze user behavior for evidence of malicious activity.

Combining Splunk's detection and alerting capability with a complete and granular history of network traffic gives analysts deep context around events and provides the definitive evidence they need to conclusively investigate these events and respond appropriately.

EndaceProbe™ Analytics Platforms capture and record 100% of network traffic, regardless of network speeds or loads, providing an unparalleled level of detail and accuracy. Recorded network packets are time-stamped to nanosecond-level accuracy allowing analysts to zoom in to investigate short-lived events, such as microbursts or pre-attack intrusions,that are often invisible to other monitoring solutions. Access to detailed packet-level history lets analysts accurately reconstruct events to identify conclusively what happened, why and how it happened and to then respond appropriately. Critical issues can be prioritized, and false positives quickly identified and flagged so detection can be tuned.

Leveraging the EndaceProbe's open architecture, Endace's Fusion Connector for Splunk integrates with and extends Splunk. Security Operations (SecOps) or Network Operations (NetOps) analysts can select an event in the Splunk dashboard and quickly pivot straight to the related packet-level history recorded on EndaceProbes, dramatically reducing the time needed to investigate and resolve issues.

Solution Details

Endace's Fusion Connector for Splunk is a free, easy to install plugin available from Splunkbase or the Endace Support Portal. It directly connects analysts, via an elegant and seamless workflow, to the precise network packets they need to investigate the root cause of problems and respond.

Analysts can click on a Splunk event to pivot straight to the packets of interest in EndaceVision, the EndaceProbe's built-in, browser-based investigation tool.

PRODUCTS

Splunk Enterprise & Splunk Enterprise Security
EndaceProbe Analytics Platforms
Endace Fusion Splunk Connector

BENEFITS

- Accurate, and complete full packet capture data provides definitive evidence for network security and performance issue investigation and response
- Streamlined investigation workflow improves SecOps and NetOps efficiency and ensures fast investigation and response
- Faster resolution times increase network security, improve uptime and reliability and reduce OPEX costs
- Integrated workflow from all your security and performance management tools through the same investigative UI
- Recorded network history provides a reliable, irrefutable evidence trail

FURTHER INFORMATION

https://www.endace.com/splunk

https://splunkbase.splunk.com/apps/#/search/Endace/

With the relevant packets isolated in EndaceVision, analysts can zoom out to look at precursor events, zoom in to analyze decoded packet data in Wireshark™ (hosted on EndaceProbes) and download PCAP files for additional analysis or for archival as forensic evidence.

Conclusion

Integrating EndaceProbes with Splunk combines total, hybrid-cloud network visibility with comprehensive search and drill down investigative capability directly from your Splunk UI.

This integration offers SecOps, NetOps and DevOps teams the fastest, most conclusive way to investigate and respond to any security and application or network performance issues Splunk records, regardless of which monitoring tool they originated from. It provides a standardized, streamlined investigation workflow that allows analysts to quickly identify the scale and root cause of an issue and respond appropriately to minimize the damage.

END_fp_end_splunk_3.2_0524

How it works

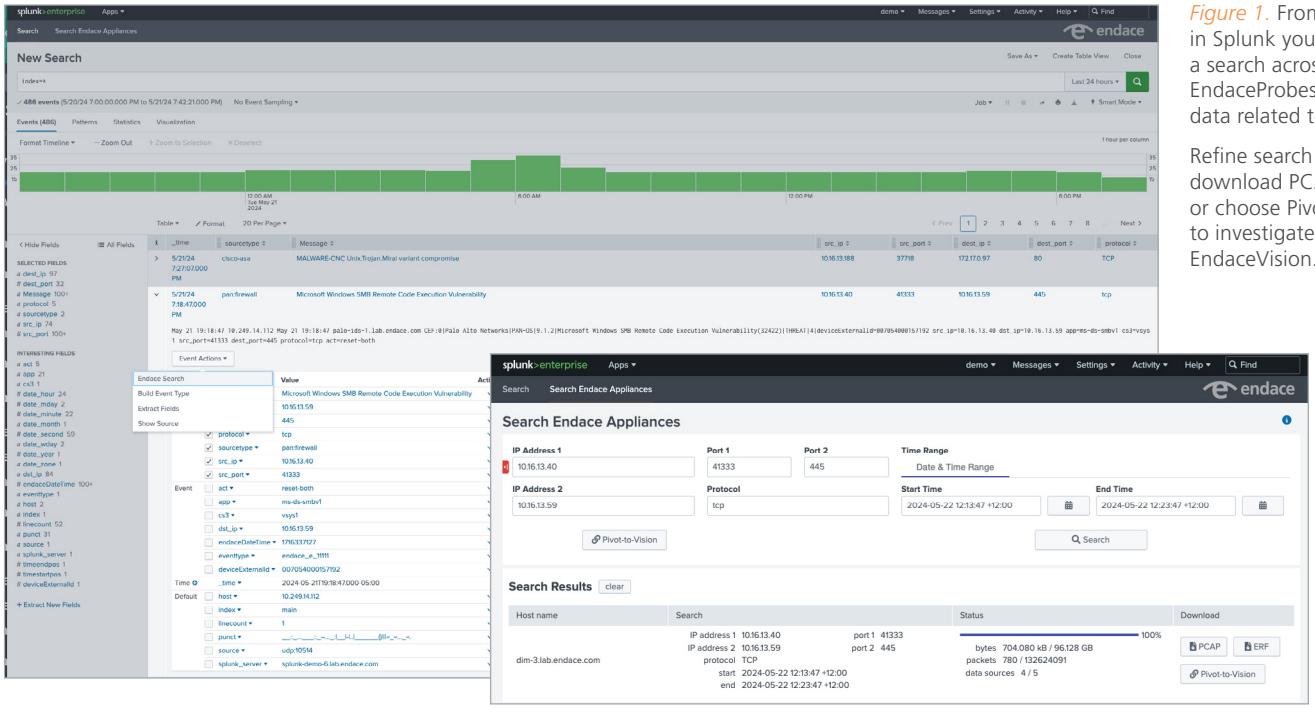

Figure 1. From any event in Splunk you can initiate a search across multiple EndaceProbes for full packet data related to the event.

Refine search parameters, download PCAP or ERF file, or choose Pivot-to-Vision to investigate further using EndaceVision.

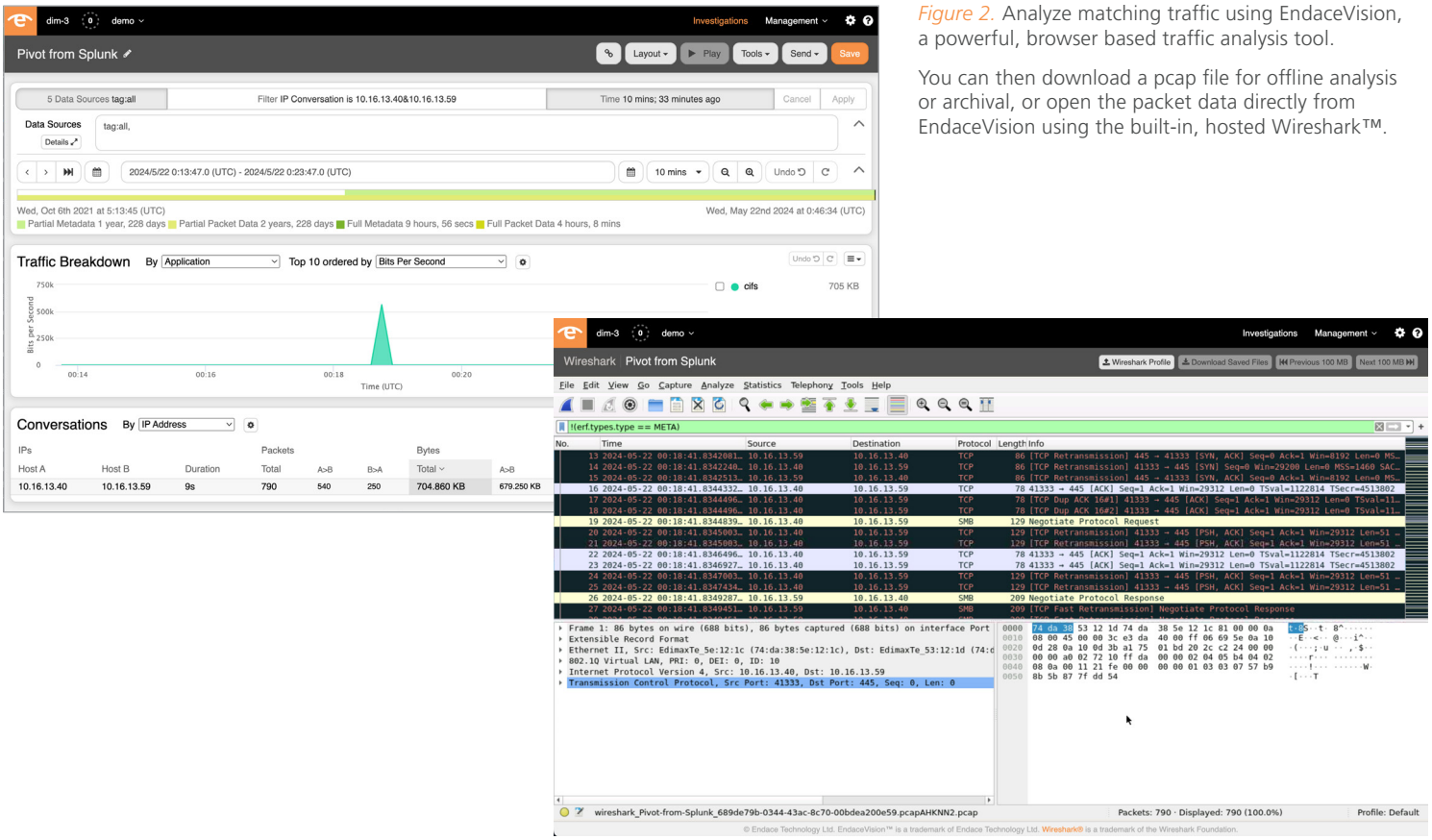

Figure 2. Analyze matching traffic using EndaceVision, a powerful, browser based traffic analysis tool.

You can then download a pcap file for offline analysis or archival, or open the packet data directly from EndaceVision using the built-in, hosted Wireshark™.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com