EndaceProbe and Splunk® SOAR

Together, Endace and Splunk SOAR bring clarity to every incident, alert or issue with an open packet capture platform that integrates to supercharge your security operations. Work smarter, respond faster, and strengthen your defenses with Endace and Splunk SOAR.

EndaceProbes record 100% accurate Network History to solve Cybersecurity, Network and Application issues rapidly and with confidence by providing an unparalleled level of detail and accuracy.

Splunk SOAR combines security infrastructure orchestration, playbook automation, case management capabilities and integrated threat intelligence to streamline your team, processes and tools. With Splunk SOAR, improve threat response, eliminate manual, monotonous tasks, overcome alert fatigue, and respond to threats in seconds - not minutes or hours.

Integrating Splunk's automation, orchestration, detection, with EndaceProbe's accurate network recording gives analysts deep context around cybersecurity events and provides the definitive evidence they need to conclusively investigate indicators of compromise 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, the Endace Connector for Splunk and the Endace App/Playbook for Splunk SOAR enable rapid investigation and automated preservation of relevant packet data in any investigation. Security Operations (SecOps) or Network Operations (NetOps) analysts can select an event in their Splunk dashboard or execute a Splunk SOAR Playbook to search, download and quickly pivot to the related packet-level history recorded by EndaceProbes on the network, dramatically reducing the time needed to investigate and resolve issues.

PRODUCTS

- **Splunk SOAR (Formerly Phantom)**
- **Splunk Enterprise & Splunk Enterprise Security**
- **EndaceProbe Analytics Platform**
- **Endace Fusion Splunk Connector**

BENEFITS

- Respond to cybersecurity threats faster, with greater confidence, and reduced dwell times when critical network evidence is always at your fingertips.
- Automate the search and download of recorded network traffic to save your teams precious time and ensure critical evidence is always preserved and available to your team.
- Strengthen your defenses, with an accurate and complete record of the network activity that accurately exposes the nature, seriousness, and extent of cybersecurity threats.
- Focus your efforts on understanding and neutralizing threats rather than learning new tools when Splunk SOAR, Enterprise and Enterprise Security can search and retrieve network captures from any EndaceProbe.
- Integrate your existing security infrastructure together so that each part is actively participating in your defense strategy.
- Customize workflows to best suite your team, processes, and environment.
- Unlike logs that can be manipulated or wiped by a skilled hacker, recorded network history provides a reliable, irrefutable evidence trail that is difficult to tamper with.

FURTHER INFORMATION

- endace.com/splunk.html
- splunkbase.splunk.com/apps/#/search/Endace/

Solution Details

The Endace SOAR App and Endace_Splunk_Search_Dowload_PCAP Playbook for Splunk SOAR are free, easy to use and available through the SOAR App list. These integrations enable analysts to integrate EndaceProbe packet capture devices and packet data search into SOAR playbooks for fast and accurate threat investigation and incident response.

When a threat arises, executing the Endace playbook searches an entire estate of EndaceProbes for traffic relevant to the threat and

then automatically downloads the pertinent PCAP into Splunk SOAR. This PCAP is then available for analysis and/or inspections by other security tools or applications. For example, a data exfiltration event can be investigated by automatically searching and retrieving all relevant network traffic recorded by EndaceProbes and then reassembling to reconstruct the exact files or data that left the network.

EndaceProbe also integrates with Splunk Enterprise Security. From the Enterprise Security Console users can search and download packets or pivot straight to the packets of interest in EndaceVision, the EndaceProbe's built-in, browser-based investigation tool. With the relevant packets isolated in EndaceVision, analysts can zoom out to look at precursor events, or zoom in to look at packet-level detail in Wireshark® hosted on the EndaceProbe.

Conclusion

Integrating EndaceProbe with Splunk SOAR and Splunk Enterprise Security allows your team to work smarter and faster with accurate packet level evidence search and download automated right within your playbooks. Your teams' efforts can focus on neutralizing threats quickly and accurately when all the necessary evidence is always at their fingertips.

This integration offers security teams the fastest, most conclusive way to investigate and respond to cybersecurity threats. It provides a standardized, streamlined investigation workflow that allows analysts to quickly identify the nature and seriousness of threats and respond appropriately to keep your organization safe.

How it works

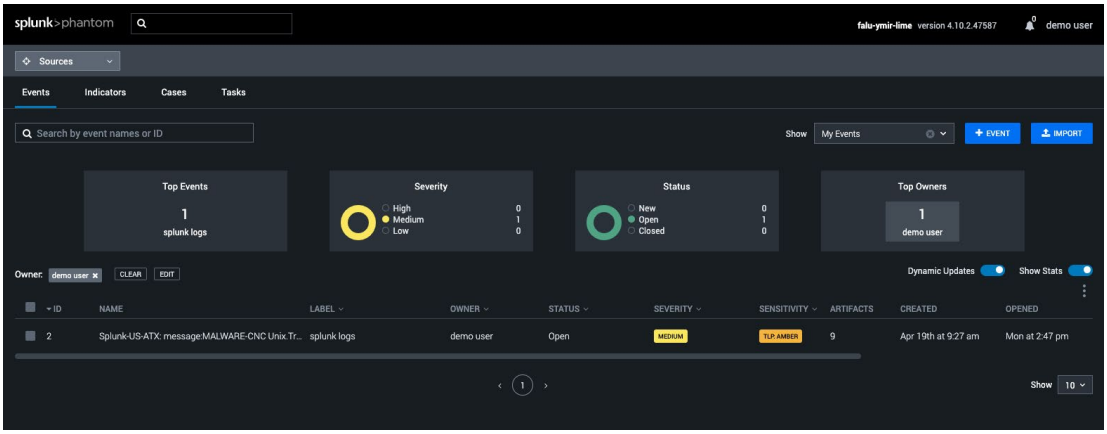

Figure 1. Analysts can select events for investigation in the "My Events" Window to drill down into the event detail.

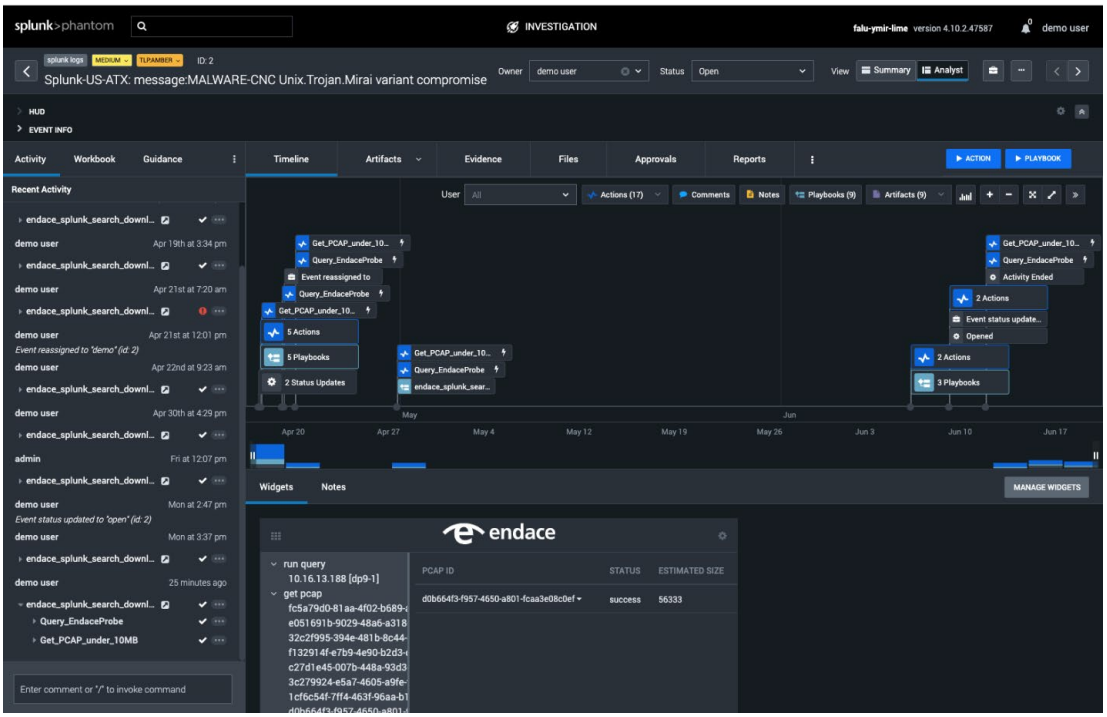

Figure 2. The Endace *Search and Download PCAP Playbook* searches and downloads relevant packet data recorded by EndaceProbes on the network.

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

For further information, email: info@endace.com