

Integrating Splunk SOAR with Endace Always-on Packet Capture for Faster, More Accurate Threat Response.



The Problem

With the growing volume and sophistication of security threats, SOC teams are increasingly under pressure to respond more quickly. Attackers are leveraging AI to increase the speed of their attacks and camouflage attack activity, making it even more challenging for SOC, NOT and IT teams to detect threats and respond quickly.

Without the right systems, managing the investigation and response process can be slow and cumbersome, often requiring repetitive manual tasks such as collecting and collating evidence and switching from one tool to another (“swivel-chair” integration). This results in duplicated effort, missed tasks, and inefficiencies that further delay incident response.

Facing an ever-increasing volume of alerts, teams find themselves constantly fire-fighting, stressed, and unable to free up time for proactive activities – such as threat hunting - that could reduce the organization’s overall threat risk.

Organizations need a solution that:

- Leverages smart AI-supported workflow automation and proven, well-structured processes to accelerate investigations and reduce response times.
- Enables SOC, NOC and IT teams to manage incident cases efficiently and collaboratively with full visibility into every part of the investigation and response process.
- Provides automated, API-driven, evidence retrieval to support more efficient, evidence-backed investigations.
- Delivers complete visibility into real-time and historical threat activity to enable SOC teams, and the tools they use, to investigate and respond to threats quickly and accurately.
- Provides always-on packet capture (not triggered capture) to reliably record every incident and provide a trusted source of forensic network evidence.
- Can flex and scale to meet evolving needs and integrates easily with other security and performance monitoring tools and platforms.
- Is easy to deploy and use.

Benefits

- Powerful workflow automation enables automated response and streamlined workflows that reduce analyst workload and accelerate response.
- A unified solution that combines threat detection, alert triage, threat intelligence, evidence collection, investigation, response, and case management in a single, intuitive platform.
- AI-enhanced incident prioritization that lets analysts investigate and respond to high-priority incidents quickly to prevent escalation.
- Access to a complete packet-level record of network activity related to every incident puts definitive evidence at analysts’ fingertips for faster, more accurate investigation and response.
- Full threat visibility across the entire network with on-prem, private and public cloud deployment options.
- Defense-grade security with FIPS 140-3 and Common Criteria / NIAP NDCPP v2.2e certification.

The Solution

Splunk SOAR streamlines response and automation processes by consolidating and correlating alerts and data from security and other monitoring tools to enable timely and prioritized responses.

With a slew of prebuilt playbooks (which leverage the MITRE ATT&CK and D3FEND frameworks) and the ability to easily create, customize and automate workflows, SOC teams can manage incident response more efficiently and work more collaboratively.

Automated evidence retrieval enables analysts to make faster, better-informed decisions and automate workflows and responses to reduce repetitive manual tasks and reduce mean-time-to-resolution.

The EndaceProbe™ Analytics Platform provides a perfect complement to Splunk SOAR by capturing, indexing and recording every packet of traffic traversing the network. It provides 100% accurate, always-on packet recording, giving SOC, NOC and IT teams access to a complete and accurate record of all network activity across on-prem, cloud and IT/OT networks.

Multiple EndaceProbes (including on-prem appliances and virtual private or public cloud instances) can be connected to form a unified, hybrid cloud recording fabric able to record weeks or months of traffic.

This fabric provides rapid, centralized search, data mining, and analysis of recorded traffic, including file extraction and

rich metadata generation using Zeek. It also supports API-based data retrieval, enabling automated SOAR playbooks to access and archive full packet evidence relating to security incidents or potential threats, putting definitive evidence at analysts' fingertips.

Conclusion

Combining Splunk SOAR with EndaceProbes provides a powerful foundation for protecting the network. It unifies the security and other network monitoring tools in the environment, providing teams with a comprehensive view of network activity and providing an intuitive platform for efficient, collaborative investigation and response.

With a reliable source of definitive network forensic evidence integrated into all their tools, teams can accurately reconstruct any network threat or issue, allowing them to respond with confidence.

How it works

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

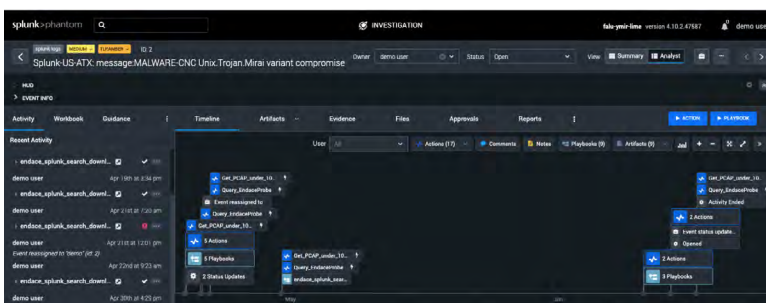
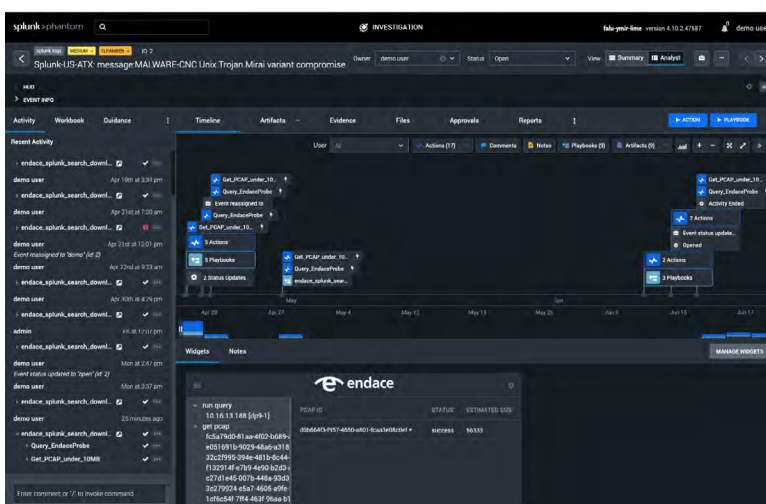


Figure 2. The Endace Search and Download PCAP Playbook searches for and downloads relevant packet data recorded by EndaceProbes on the network.



Solution Components

- » Splunk SIEM
- » EndaceProbe Analytics Platform

© 2025 Endace Technology Limited. All rights reserved. Information in this data sheet may be subject to change.

Endace™, the Endace logo, Provenance™ and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).