SOLUTION BRIEF

endace
Record. Respond.

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

splunk> a CISCO company

The Problem

As cyberthreats increase in volume, speed and complexity, collecting, collating and making sense of telemetry from a widening range of sources to enable organizations to defend against them becomes challenging.

SOC and NOC teams need tools that can correlate and analyze data from threat intelligence feeds, on-prem, cloud and IT/OT network infrastructure, log files, multiple security and performance monitoring tools – including NDR/XDR/EDR solutions, firewalls, IDS/IPS tools - and more.

All this data needs to be collected and analyzed in real-time and turned into actionable, prioritized insights that give teams the ability to investigate and respond to attacks quickly and stop them before they escalate.

As attackers increasingly use AI to accelerate attacks, hide malicious activity and minimize visibility, SOC teams need tools that leverage AI to help them combat this – accelerating and automating threat detection, investigation and response.

Organizations need a solution that:

- Delivers complete visibility into real-time and historical network activity to enable SOC teams to detect, investigate and respond to threats quickly and accurately.
- Can be deployed across on-prem, private and public cloud, as well as IT/OT networks.
- Provides always-on packet capture (not triggered capture) to reliably record every incident and provide a trusted source of forensic network evidence.
- Leverages smart AI for smarter, faster detection, investigation and resolution of network threats, including automating responses where possible.
- Can flex and scale to meet evolving needs and integrates easily with other security and performance monitoring tools and platforms.
- Is easy to use and fast to implement.

Benefits

- Correlating and analyzing data from multiple telemetry sources delivers comprehensive visibility with full context into every threat and issue.
- Streamlined, automated workflows combine threat detection, alert triage, threat intelligence, investigation, response, and case management in a single, intuitive platform.
- AI-enhanced incident prioritization enables analysts to 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 fast, 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® SIEM delivers comprehensive visibility and accurate threat detection (with hundreds of pre-built detections based on MITRE ATT&CK, NIST CSF 2.0 and Cyber Kill Chain), advanced incident prioritization, and enhanced operational efficiency for SOC teams.

Security analysts see the full context of threats, quickly identify root cause, and investigate incidents with easy access to relevant evidence from all telemetry sources.

SOC, NOC (and IT) teams can accelerate incident investigation and response workflows by using AI and automation to increase productivity and efficiency.

The EndaceProbe™ Analytics Platform is a perfect complement to Splunk SIEM, recording every packet of traffic traversing the network. Capable of storing weeks of full packet data, EndaceProbes create a complete and accurate record of all network activity across on-prem, cloud and IT/OT networks

Using EndaceFlow™ - Endace's high-speed NetFlow Generator – and hosted Zeek™, EndaceProbes can stream unsampled network flow data and rich log data to Splunk SIEM, enriching alerts with detailed network context. File transfers can be reassembled and sent to Splunk Attack Analyzer for analysis.

Endace's Fusion Connector for Splunk SIEM lets analysts click from any SIEM alert directly to the related packet data for fast, conclusive, evidence-backed investigation and response.

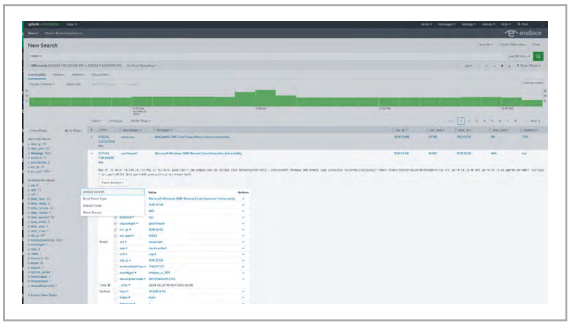
With the relevant packets identified in EndaceVision™ - the EndaceProbe's powerful traffic analysis tool - analysts can zoom in or out to see what happened before, during and after the event and analyze decoded packets directly in hosted Wireshark™ without downloading large pcap files.

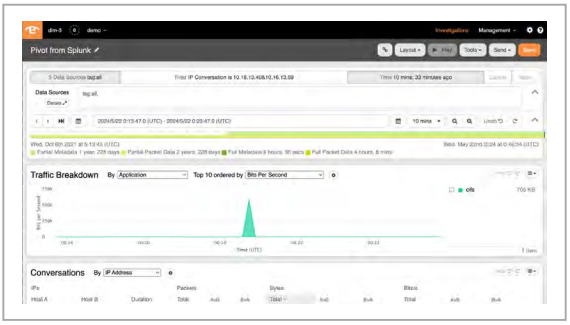
Conclusion

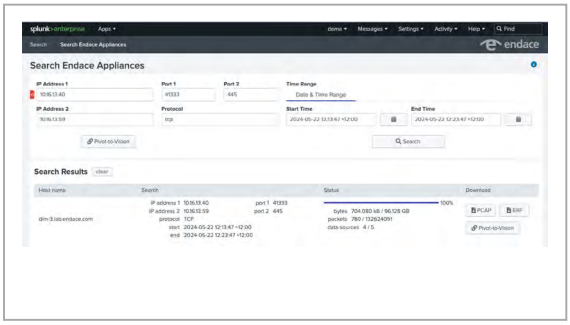
Together, Splunk SIEM and EndaceProbes provide a powerful threat and incident detection and investigation platform for SOC and NOC teams. The combination unifies, and integrates with, a wide range of security and monitoring tools to provide full context surrounding issues and threats in all environments: on-prem, private and public cloud, and IT/OT environments.

With Splunk SIEM's powerful AI-enhanced detection, analytics, and automation, and access to the EndaceProbe's definitive network forensic evidence, SOC, NOC and IT teams can investigate and respond to threats and incidents confidently, effectively, and quickly, without guesswork.

How it works







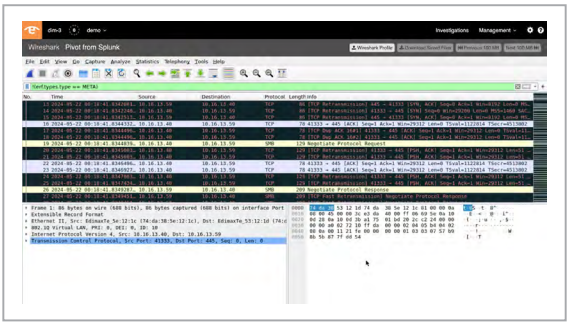


Figure 1. From Splunk events you can initiate a search across multiple EndaceProbes for related packet data and see the results in EndaceVision, a powerful, browser based traffic analysis tool

Figure 2. Analyze traffic in EndaceVision, download a pcap file for offline analysis or archival, or open and analyze the packet data directly using built-in, hosted Wireshark™.

Solution Components

- Splunk SIEM
- EndaceProbe Analytics Platform
- EndaceFlow NetFlow Generator