Joint Solution

Corelight App for Splunk simplifies SOC workflows and investigations

Transform Your SOC with Intuitive, Real-Time Insights

Any security analyst will tell you how much they struggle to sort through the deluge of alerts generated from their SIEMs to distinguish real threats from false alarms. The Corelight App for Splunk addresses this by providing actionable, security-centric network insights that can help security teams simplify investigations, accelerate response times, and boost productivity.

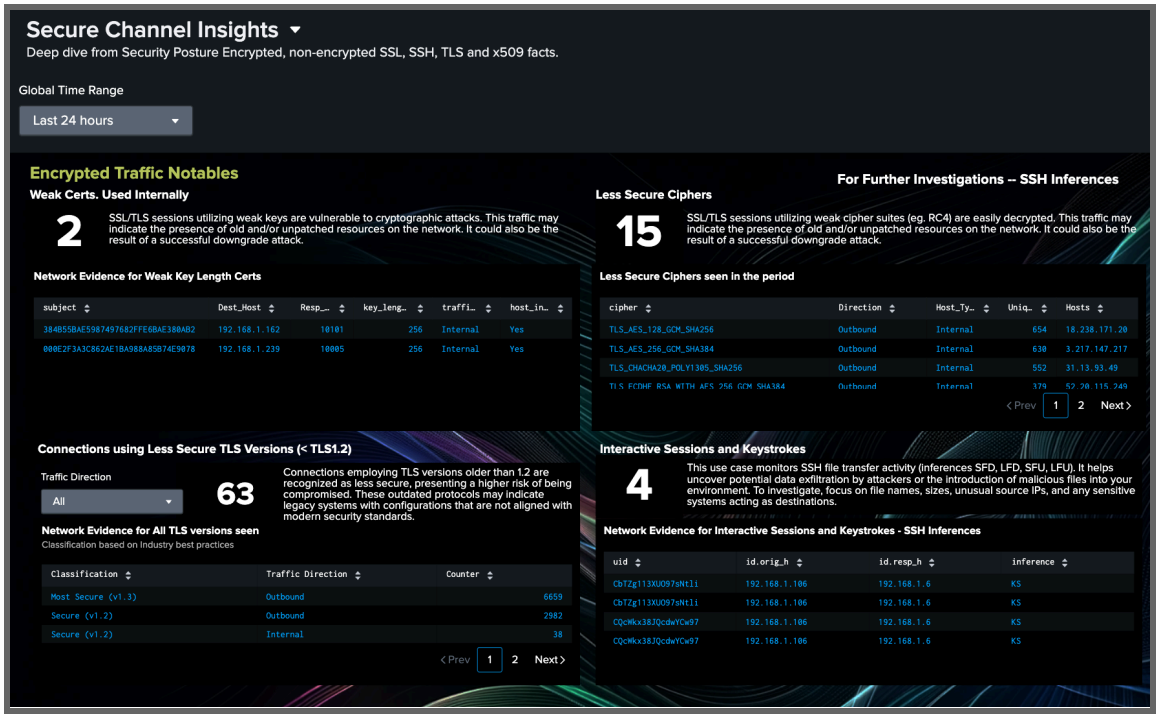
Enhanced visibility into network security hygiene includes comprehensive counters and charts for improved insights with direct links for more details.

Corelight App for Splunk

Intuitive, at-a-glance views of the organization's security posture

As the cornerstone of most security operations centers (SOCs), SIEMS collect and correlate enormous volumes of disparate data from across the environment to detect and alert on potential threats. The steady stream of raw data can be distracting, if not debilitating, for overworked SOC analysts struggling to make sense of it all.

The Corelight App for Splunk brings clarity and guidance on where to focus by providing quick insights from real-time network telemetry that helps analysts determine at a glance the various threats across the environment. Intuitive dashboards with relevant counters, charts, and maps give analysts a quick and concise overview of the organization's security posture. This Security Posture Dashboard gives immediate insight and control back to the analyst with a summary view and direct links to relevant details and clear guidance to help them validate threats and accelerate investigations.



Quick links allow analysts to drill down into relevant details with critical information and recommendations based on time-tested SOC best practices.

Transform your SOC with the Corelight App for Splunk

- **Intuitive, Real-Time Insights** - Direct attention to where it's needed with quick, intuitive views of the organization's security posture, directly from real-time network telemetry.
- **Quick Insights, Powerful Results** - Instant access to summaries, relevant details, and actionable intelligence to quickly validate threats and accelerate response times.
- **Evolving with You** - Frequently updated dashboards with new features and use cases based on feedback from our users and the design patterns of the world's elite defenders.

Solution benefits

Building on our native integration with Splunk, the Corelight App for Splunk can help overworked SOC analysts significantly reduce dwell time, mean time to respond (MTTR), and operational costs compared to typical, minimally integrated solutions. By providing intuitive and insightful dashboards with direct links to related details, the Splunk App allows security teams to quickly understand implications of hybrid, multicloud network activity, as well as streamlining event investigations and upscaling SOC capabilities.

Complete visibility
Gain a commanding view of your organization and all devices that log onto your network—with access to details such as DNS responses, file hashes, SSL certificate details, and user-agent strings—rapidly, without relying on other teams to respond to data requests.

Next level analytics
Machine learning—fueled with network evidence—delivers powerful insights so you can focus on the most critical detections. Corelight's high-fidelity, correlated telemetry powers analytics, machine learning tools, and SOAR playbooks, improving efficiency and unlocking new capabilities so that you can make better decisions—faster.

Faster investigation
Correlate alerts, evidence, and packets so you can establish baseline network activity and integrate that context directly into your existing workflows. Reduce false positives and your alert backlog—with no redesign or retraining necessary. You get a full view of every incident so you can validate containment and remediation.

Expert hunting
Rich, organized, and security-specific evidence enables you to spot vulnerabilities, intruder artifacts, critical misconfigurations, signs of compromise and undetected attacks, further mitigating risk.

Splunk helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks. Delivered by our Open NDR Platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

info@corelight.com | 888-547-9497