

## 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.

**Secure Channel Insights** ▾  
Deep dive from Security Posture Encrypted, non-encrypted SSL, SSH, TLS and x509 facts.

Global Time Range  
Last 24 hours ▾

### Encrypted Traffic Notables

**Weak Certs. Used Internally**  
**2** SSL/TLS sessions utilizing weak keys are vulnerable to cryptographic attacks. This traffic may indicate the presence of old and/or unpatched resources on the network. It could also be the result of a successful downgrade attack.

**Network Evidence for Weak Key Length Certs**

subject	Dest_Host	Resp...	key_leng...	traffi...	host_in...
3848558AE5987497682FFE68AE388A02	192.168.1.162	18181	256	Internal	Yes
080E2F3A3C862AE1BA988A85874E3878	192.168.1.239	10005	256	Internal	Yes

**Less Secure Ciphers**  
**15** SSL/TLS sessions utilizing weak cipher suites (eg. RC4) are easily decrypted. This traffic may indicate the presence of old and/or unpatched resources on the network. It could also be the result of a successful downgrade attack.

**Less Secure Ciphers seen in the period**

cipher	Direction	Host_Ty...	Uniq...	Hosts
TLS_AES_128_GCM_SHA256	Outbound	Internal	654	18,238,171,20
TLS_AES_256_GCM_SHA384	Outbound	Internal	630	3,217,147,217
TLS_DHACHA20_POLY1305_SHA256	Outbound	Internal	552	31,13,93,49
TLS_PCHBF_RSA_WITH_AES_256_GCM_SHA384	Outbound	Internal	379	62,28,115,249

**Connections using Less Secure TLS Versions (< TLS1.2)**  
**63** Connections employing TLS versions older than 1.2 are recognized as less secure, presenting a higher risk of being compromised. These outdated protocols may indicate legacy systems with configurations that are not aligned with modern security standards.

**Network Evidence for All TLS versions seen**  
Classification based on Industry best practices

Classification	Traffic Direction	Counter
Most_Secure (v1.1)	Outbound	6655
Secure (v1.2)	Outbound	2992
Secure (v1.2)	Internal	38

**Interactive Sessions and Keystrokes**  
**4** This use case monitors SSH file transfer activity (inferences SFD, LFD, SFU, LFU). It helps uncover potential data exfiltration by attackers or the introduction of malicious files into your environment. To investigate, focus on file names, sizes, unusual source IPs, and any sensitive systems acting as destinations.

**Network Evidence for Interactive Sessions and Keystrokes - SSH Inferences**

uid	id.orig_h	id.resp_h	inference
cb72g113XU0978H11	192.168.1.106	192.168.1.6	KS
cb72g113XU0978H11	192.168.1.106	192.168.1.6	KS
cQcMx387QcdwYcW97	192.168.1.106	192.168.1.6	KS
cQcMx387QcdwYcW97	192.168.1.106	192.168.1.6	KS

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](mailto:info@corelight.com) | 888-547-9497**