Joint Solution

JASK | corelight

Corelight & JASK: More Network Visibility and Security Insights, Less Noise.

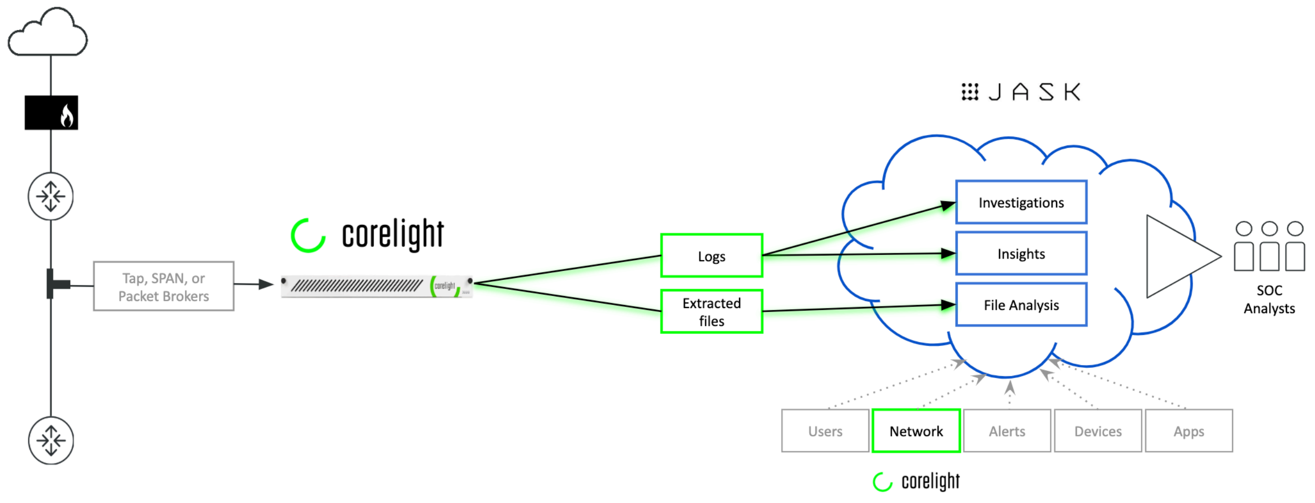
Common network logs like Netflow or DNS records often leave security operators in the dark, lacking critical detail related to events on the wire. Full packet capture, while comprehensive, quickly becomes cost-prohibitive at scale and is ultimately difficult to search quickly. Security analysts can spend hours manually analyzing packets just to arrive at a single conclusion. Corelight provides a better approach to network monitoring by transforming raw traffic into rich, protocol-specific logs that comprehensively summarize network events at less than 1% the size of full traffic capture. JASK, in turn, correlates the log data from Corelight with all other logging and security data sources (endpoints, firewalls, IAM, threat intelligence feeds, and more) to generate meaningful insights that provide a "call for action" for security operators.

This joint solution combines Corelight's network security monitoring capabilities built on open source Zeek (formerly called Bro) with the JASK Autonomous Security Operations Center (ASOC) platform to eliminate the noise traditionally resulting from thousands of alerts. Customers can stream Corelight's network logs and extracted files to JASK ASOC platform for security analysis, producing a finely-tuned group of security Insights generated by JASK. Using the JASK ASOC platform, analysts can query Corelight's underlying logs and obtain fast, actionable intelligence into their network traffic to accelerate incident response and unlock new threat hunting ground.

> Stream network visibility data from Corelight to JASK to unlock new threat detections and dramatically accelerate incident response times.

Working Together: The Corelight & JASK Solution

Corelight's out-of-band network sensors sit behind a packet broker or network TAP, transforming mirrored traffic (up to 25 Gbps per sensor) into rich logs and extracted files. Corelight Sensors stream this data in real-time to the cloud-native JASK ASOC platform, where JASK's UI provides three distinct security capabilities and workflows highlighted in the diagram below and use cases on the following page:



Use Case #1: Reducing Alert Noise, Accelerating Incident Response Workflows

By streaming logs to the JASK ASOC platform, Corelight complements your endpoint and application data with critical visibility into the network attack surface. This gives security analysts a single place to understand, assess, and investigate their environment across users, networks, devices, applications, and security alerts.

Traditional SIEM platforms are often filled with endless signature-driven alerts that require painful follow up investigations. JASK security Insights provide a focused set of high-value, risk-prioritized alerts that append the relevant environmental context analysts need to quickly assess and respond to incidents. Each JASK Insight appends related Corelight network logs for context. Using the JASK cloud-based console, security analysts can also pivot via the log UIDs into additional logs to see related connections and protocol activity.

Use Case #2: Unlocking New Threat Hunting Grounds

Via JASK's Investigations workflow, threat hunters can dive into Corelight's network traffic logs and easily identify suspicious trends and anomalous network activity such as DNS queries to non-existing domains, the use of self-signed certificates, and top bandwidth consumers by IP address.

Corelight's network logs were purpose-built for security use cases. Threat hunters can use the logs' unique connection IDs to easily track network activity across protocols, identify suspicious activity on non-standard ports, and even look back in time to see network activity--hours, days, and months in the past.

Use Case #3: Analyzing Files for Malware

In addition to generating comprehensive network logs, Corelight Sensors reassemble and extract files at wire speed. Customers can stream these files (such as PDFs and executables) to the JASK platform for file analysis to detect malware. JASK utilizes third-party software from leading products in the industry to detect, investigate and detonate any files containing malware.

Corelight Sensors

Corelight Sensors operate out-of-band in both physical and virtual formats and leverage the power of the open-source Zeek network security monitor to transform traffic into rich logs, extracted files, and security insights via custom scripts. Zeek data is 'rocket fuel' for SOCs, enabling analysts to dramatically accelerate average incident response times and unlock powerful threat hunting capabilities through better, faster network evidence. Corelight's network security monitoring capabilities include:

- Monitoring up to 25+ Gbps of monitored traffic per sensor
- Generating 50+ log types, covering 35+ network protocols
- Fine tuned log data controls: stream, filter, and fork logs to multiple destinations
- A web-based GUI for simple sensor deployment and management
- Detailed sensor performance and health monitoring
- Enterprise support from the creators and builders of Zeek

JASK | corelight

JASK ASOC Platform

The JASK Autonomous Security Operations Center (ASOC) platform is modernizing security operations by giving analysts prioritized and contextualized threat data. This removes the technology limitations that often burden your SOC's speed and effort to stop data breaches and other compromises. Built on a cloud-native platform, JASK delivers auto-scaling capabilities that adapt to peaks in event data and volume to streamline investigations. The JASK ASOC platform's open, flexible architecture was built for big data analytics and easily integrates within your existing SOC environment. By automatically parsing of massive amounts of data and implementing automated analyst workflows, JASK increases investigation efficiencies and enables your SOC to reduce the manual, time-consuming effort involved with alert triage.

Helping Your SOC At the Speed of Corelight

When it comes to cybersecurity, speed matters greatly. Security teams need to catch attacks as early as possible, but can't when they lack the data to make fast sense of their environment and are faced with an ever-growing avalanche of security alerts. Corelight addresses the data gap, providing network data that's both comprehensive and lighting-fast to search and JASK tackles the signal-to-noise challenge by curating a manageable queue of precise, high-value security Insights and integrating all other data sourced in the cybersecurity environment.

Together, Corelight and JASK give security teams full visibility of their network and let them move at the speed of attack.

JASK

JASK is modernizing security operations by delivering an advanced SIEM platform that provides better visibility, better automation, and a better architecture. Built on cloud-native technologies, the JASK ASOC platform streamlines security analyst workflows by automating many of the repetitive tasks that restrict productivity, freeing them for higher-value roles like threat hunting and vulnerability management, while addressing the escalating talent shortage. Learn more at www.jask.com

corelight

Corelight makes powerful network security monitoring (NSM) solutions that transform network traffic into rich logs, extracted files, and security insights for more effective incident response, threat hunting, and forensics. Corelight Sensors run on Zeek (formerly called "Bro"), the open-source NSM tool used by thousands of organizations. Corelight Sensors simplify Zeek deployment and expand its performance and capabilities. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. https://www.corelight.com

For a custom demo of this joint solution, please contact your Corelight and JASK authorized reseller, or reach us directly at:

info@jask.com

info@corelight.com

+1 (888) 547-9497