JOINT SOLUTION

Accelerating network detection & response with native integration with Splunk

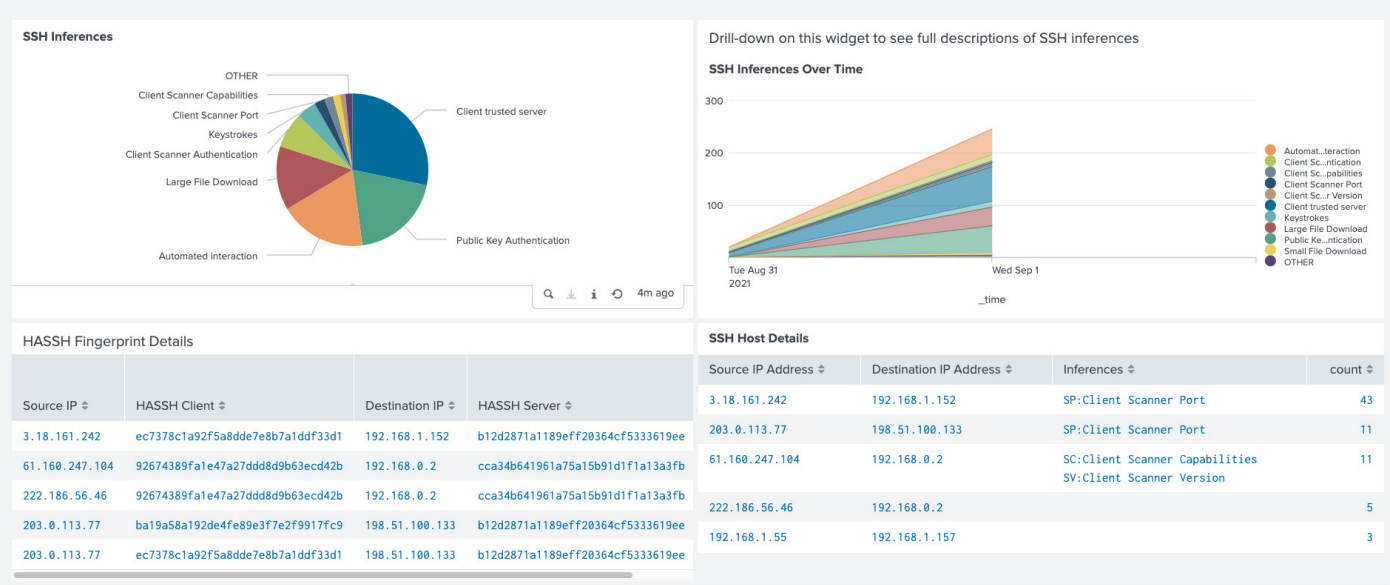
Splunk has been a leader in helping security teams respond more effectively to security incidents by ingesting large disparate data sets and simplifying how they can be analyzed. Unfortunately, however, one data set that is often missing is the rich network telemetry that can provide crucial insights into operational and adversarial activities occurring within the network. Without it, users have limited visibility into what is happening across the environment, which severely handicaps their threat detection and response capabilities.

Corelight overcomes this challenge with rich network evidence that can greatly improve detection coverage and accuracy to accelerate incident response, while amplifying your investment in Splunk automation. With native Common Information Model (CIM) support, Corelight data integrates seamlessly into Splunk Enterprise and Splunk Enterprise Security (ES) environments by

INTEGRATION HIGHLIGHTS

- Seamless ingestion of data with native Common Information Model (CIM) support
- Out-of-the-box support for Splunk ES correlation searches
- Simplified data filtering for faster investigations
- Quick time to value with linked data and Corelight analytics
- The Corelight App for Splunk accelerates deployment for new Splunk users

CORELIGHT HELPS SECURITY TEAMS WORK FASTER AND MORE EFFECTIVELY



Corelight network evidence provides new insights on encrypted traffic that traditional network security tools don't support.

automatically populating fields in common Splunk data models, such as Network Traffic, Network Resolutions (DNS), Network Sessions, Certificates, Web, and Email. The result is much faster and effective detection and response.

How much time can this native integration save? One mutual Splunk and Corelight customer described it as "like Google for your network" and saw a 95% reduction in average incident response time. Read the case study here.

ADVANCED NETWORK EVIDENCE FOR SPLUNK

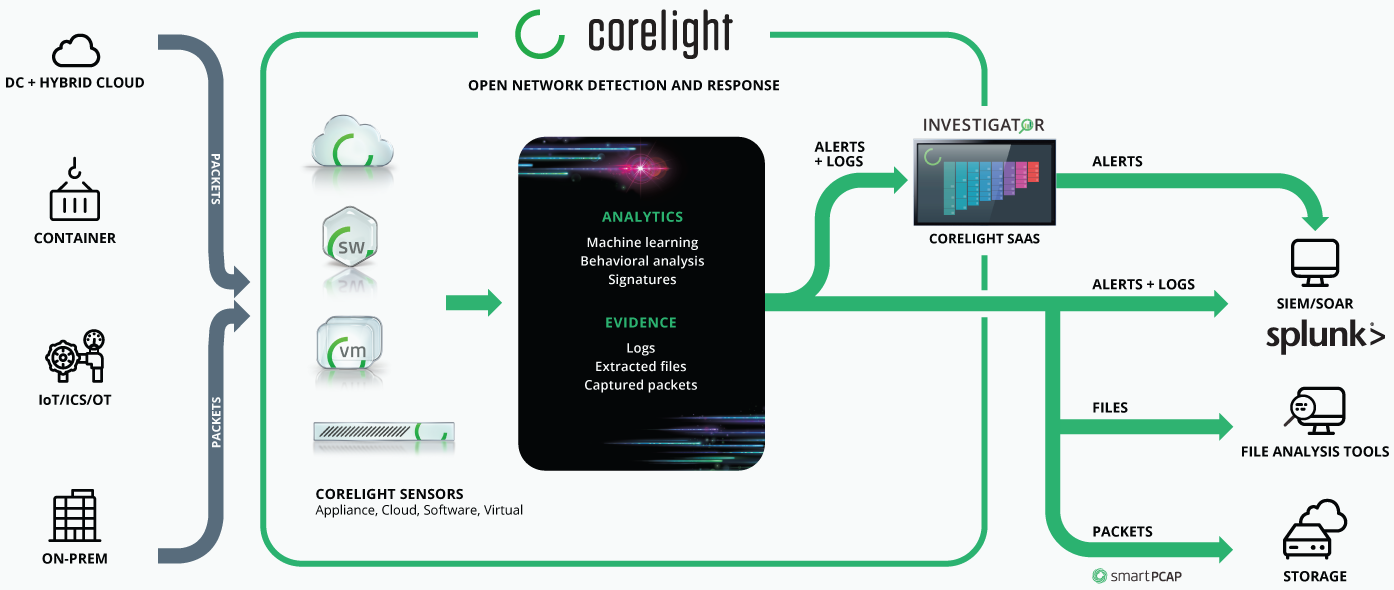
By generating detailed, correlated log data, alerts, and analytics through passive network monitoring, Corelight gives Splunk analysts a complete and contextual view of all the activity across the enterprise. This elevated visibility across on-premise, cloud, and multi-cloud environments greatly accelerates threat investigations and reduces the stress of over-extended Security Operations Center (SOC) teams.

For organizations interested in forwarding only network alerts, the Corelight Investigator SaaS offering can ensure that only critical events are sent to Splunk. So whether forwarding just alerts from Investigator or alerts and rich, correlated evidence, Corelight data is available to help optimize the value of your Splunk environment. Moreover, Corelight data is there to power Splunk SOAR playbooks, allowing SOC teams to automate tasks and keep them focused on high-value activities.

ACCELERATE TIME TO VALUE WITH THE CORELIGHT APP FOR SPLUNK

New Splunk users can take advantage of the Corelight App for Splunk to jumpstart deployments with intuitive dashboards, workflows, and log filters that can help SOC teams come up to speed fast. Existing users can also benefit from Corelight's integration with Splunk by testing their threat hunting and incident response skills with our fun Capture the Flag challenge on Splunk's Boss of the SOC website. Two on-demand modules are available to show how Corelight data in Splunk can accelerate investigations and reduce the time spent fumbling with ineffective queries and pivoting across disparate data sources.

CORELIGHT OPEN NDR AND SPLUNK



SOLUTION BENEFITS

COMPLETE VISIBILITY

Corelight accelerates threat detection and response by parsing all north-south and east-west traffic, turning it into rich security-specific evidence that goes back months, not days. Out-of-band sensors provide correlated evidence and analytics for all devices, including those lacking endpoint agents.

NEXT-LEVEL ANALYTICS

Corelight identifies more than 75 adversarial TTPs across the MITRE ATT&CK® framework to reveal known and unknown threats through hundreds of unique insights and alerts. With advanced machine learning, behavioral analysis, and signature-based approaches, your team can make better decisions faster.

FASTER INVESTIGATION

By correlating alerts, evidence, and packet data, Corelight establishes a network baseline and stores years' worth of activity so analysts can trace the origins of attacks. Contextual evidence integrates directly into Splunk dashboards and workflows to simplify and accelerate investigations.

EXPERT HUNTING

Rich network evidence and analytics provide the context SOC teams need to reduce dwell time and find hidden attacks while being lightweight enough to be stored for years. Superior insight and advanced threat detection turns even junior analysts into expert threat hunters.

To learn more about the Splunk integration, request a demo at **https://corelight.com/contact**

Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future. With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497