JOINT SOLUTION

Streamline investigations with native Splunk integration

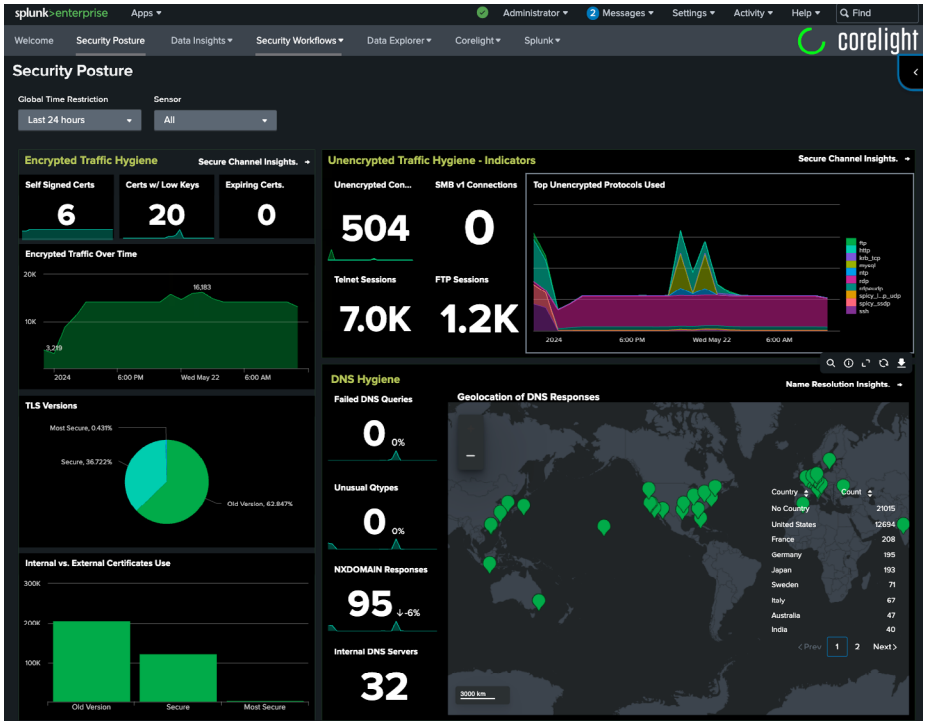
Splunk is a recognized leader in helping security teams make sense of the massive amounts of data collected from across their environment. Unfortunately, however, one data set that is often missing is the rich network telemetry that can provide crucial insights into operational and adversarial activities 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



The Corelight App for Splunk brings clarity and guidance on where to focus by providing quick insights and and relevant details. Better insights means faster and happier analysts.

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

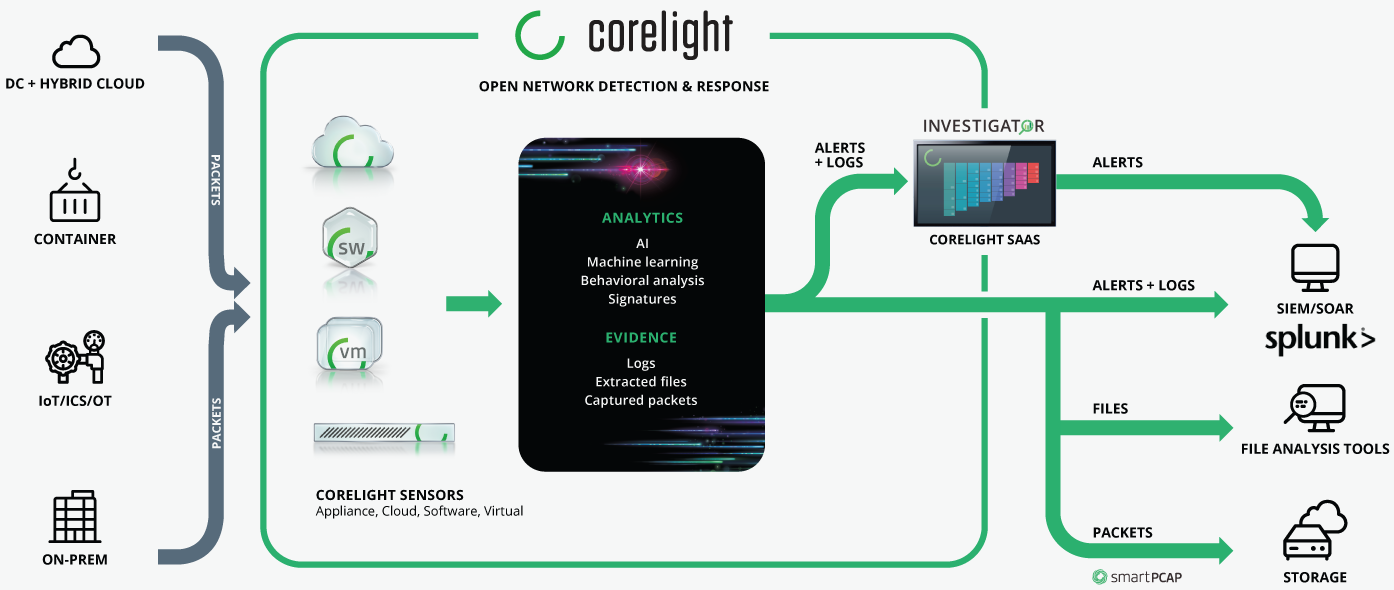
By generating detailed, correlated log data, alerts, and analytics through passive network monitoring, Corelight gives Splunk analysts a complete and contextual view of all the activity across the enterprise. This elevated visibility across on-premise, cloud, and multi-cloud environments greatly accelerates 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

The Corelight App for Splunk accelerates time to value by helping analysts focus on what matters most. By providing insights from correlated, real-time network telemetry, analysts can quickly and easily determine the most interesting threats across the environment. With intuitive dashboards and insights, as well as direct links to relevant details on the most pressing threats, the App enables security teams to streamline investigations, accelerate response times, and boost analyst productivity.

CORELIGHT OPEN NDR AND SPLUNK



SOLUTION BENEFITS

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. Streamline investigations, while reducing false positives and alert backlogs with the Corelight App for Splunk that provides intiuitive summaries and correlated details to quickly validate containment and remediation.

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, a Cisco company, 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 provides security teams with network evidence so they can protect the world's most critical organizations and companies. 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