JOINT SOLUTION

Modernize SecOps with Corelight & Elastic Security

IMPROVE DETECTION, INVESTIGATION, AND RESPONSE

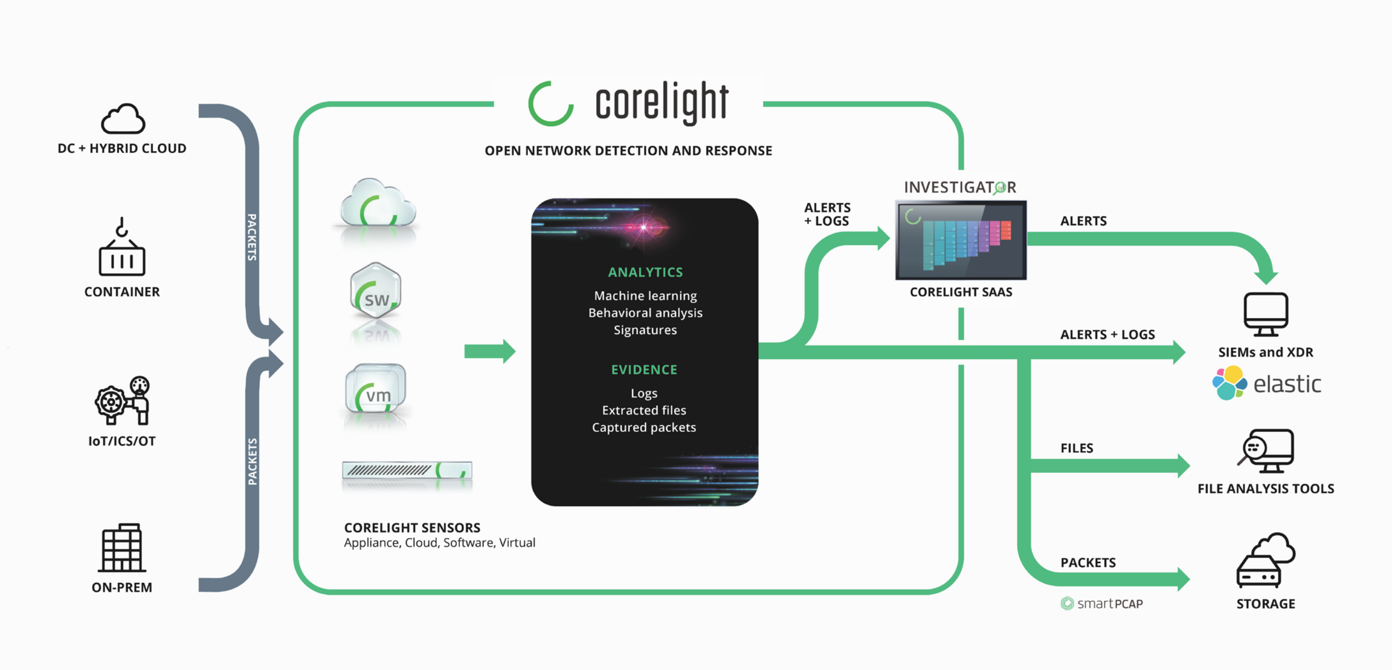
Elastic's open and modern SIEM and XDR solutions help organizations outpace adversaries, operate at scale, and act decisively. However, without rich network telemetry, SecOps teams often struggle to obtain crucial insights into operational and adversarial activities occurring within the network. Without it, analysts have limited visibility into what is happening across the environment, limiting their threat detection and response capabilities.

Corelight's Open NDR Platform addresses these challenges with rich network evidence that can greatly improve detection coverage and accuracy and accelerate incident response while amplifying Elastic investments. With native Elastic Common Schema (ECS) support, Corelight data integrates seamlessly into Elastic Security environments with normalized network data for fast analysis, visualization, and correlation.

INTEGRATION HIGHLIGHTS

- Comprehensive network visibility across endpoints, cloud, OT, and distributed environments
- Advanced analytics to identify 75+ MITRE ATT&CK® TTPs
- Prebuilt Elastic dashboards, detection rules, and queries speed ROI
- Correlated endpoint and network activity accelerates investigations

CORELIGHT'S NATIVE INTEGRATION WITH ELASTIC SECURITY



FEATURES

Comprehensive network evidence for Elastic
Network evidence from Corelight Sensors streams into the Elastic Stack, giving you a seamless blend of rich Zeek® logs, proprietary Corelight detections, and Suricata alerts. This unique integration empowers your SecOps teams with detailed network insights, facilitating faster, more informed responses to threats. Furthermore, Corelight enhances the value of these security signals through its Smart PCAP and file extraction capabilites, allowing analysts to easily pivot from an alert to packet captures or transferred executables.

Unified data analysis with Corelight ECS support
Corelight's Elastic Common Schema (ECS) support means your network evidence is automatically formatted and enriched to work seamlessly with Elastic. Our integration enables easy onboarding, correlation, and analysis of data, giving your teams the ability to act fast and decisively. Learn more at https://github.com/corelight/ecs-logstash-mappings

Enhanced threat detection with Corelight search rules for Elastic
Corelight enriches your Elastic environment with a suite of search rules, informed by Zeek® logs for effective threat hunting. These rules are designed to uncover a range of suspicious activities — from unauthorized task scheduling via SMB to unexpected webshell executions and irregular HTTP requests. Learn more at https://github.com/corelight/Elasticsearch_rules

Out-of-the-box visualizations with Corelight dashboards for Elastic
Corelight's set of Kibana dashboards is designed to enhance visibility and demonstrate how to use network evidence for more effective detection and response. The dashboards, which include views for known entities, MAC addresses, connections, TLS/x509 certificates, files, Suricata IDS alerts, DNS queries, RDP sessions, VPN, SSH, HTTP traffic, and more, offer a granular and accessible overview of network activities. Learn more at https://github.com/corelight/ecs-dashboards

Fast pivoting with Community ID
This open-source standard for network flow hashing links events from Corelight Sensors with Elastic's endpoint logs and other sources for a holistic view of network activity. With Community ID, you have a common identifier to correlate and pivot across network activity across datasets. Learn more at https://github.com/corelight/community-id-spec

SOLUTION BENEFITS

COMPLETE VISIBILITY

Corelight delivers visibility into every connection to give you complete understanding of your network. Our out-of-band sensors parse all North-South and East-West traffic, turning it into rich, correlated, ECS-compliant evidence that goes back months, not days. Gain a commanding view of your organization and all devices that log onto your network—with access to details such as SSH inferences, DNS query/response, file hashes, TLS connection details, and HTTP content.

NEXT-LEVEL ANALYTICS

Corelight delivers a comprehensive suite of network security analytics that help you identify more than 75 adversarial TTPs across the MITRE ATT&CK® spectrum, including 77 detection rules prebuilt for Elastic. Corelight detections reveal known and unknown threats via hundreds of unique insights and alerts across machine learning, behavioral analysis, and signature-based approaches. You can expose behaviors in encrypted traffic, identify command and control activity, summarize entity activity, gain ICS/OT visibility, and more.

FASTER INVESTIGATION

Corelight's rich, pivotable telemetry covers everything that crosses your network, so analysts can make connections and find out what really happened, quickly and confidently. Our comprehensive evidence, pre-built Elastic dashboards, and queries allow your team to cut through the queue and focus on high-priority work. Your SOC will benefit from lower MTTR, higher case closure rates, and validated containment.

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 efficiently stored for years. With structured, high-value, and correlated evidence, everyone on your SOC can have the right insight to elevate their threat investigation skills.

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

Elastic builds real-time, scalable enterprise search, observability, and security solutions on a single free and open technology stack that can be deployed anywhere. Thousands of organizations worldwide use Elastic to instantly find actionable insights from any type of data and power mission-critical systems. Learn more at elastic.co.

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

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.