Google Cloud | corelight

Joint Solution Brief

Advanced network detection and response for Google Security Operations

IT COMPLEXITY IS REDUCING VISIBILITY

Navigating today's cybersecurity landscape is challenging, particularly without a complete view of what's happening across an organization's increasingly distributed environment. As cloud services become more prevalent, smart device usage surges, and microservices architectures become more common, the complexity of threats intensifies, making it tougher for security operations teams to stay ahead.

Corelight's Open NDR Platform overcomes these persistent challenges by transforming all network data into comprehensive, correlated evidence. This enriched network telemetry helps security operations center (SOC) teams using Google Security Operations Platform tame the exponential growth of security alerts and incidents to understand the interrelated details of even the most sophisticated attacks.

INTEGRATION HIGHLIGHTS

- Streamline workflows with native integration across Google Security Operations platform
- Reduce alert fatigue, simplify investigations, and know the origins of attacks
- Corelight Cloud Sensor for GCP provides complete network visibility in the cloud
- Trusted by Mandiant Incident Response and Managed Defense teams

Transforming network traffic into comprehensive, detailed evidence

Corelight data integrates directly into Google Chronicle Unified Data Model (UDM).

INTEGRATED ACROSS GOOGLE SECURITY OPERATIONS PLATFORM

As a strategic Google Cloud security partner, Corelight's Open NDR Platform integrates across the Google Security Operations Platform to deliver a superior level of attack visibility, response, and threat hunting capabilities. To that end, organizations can use Google Threat Intelligence to enrich Corelight's comprehensive, high-fidelity logs and prioritize Suricata alerts that can be consumed into Security Operations SIEM for unprecedented detection coverage and faster investigations.

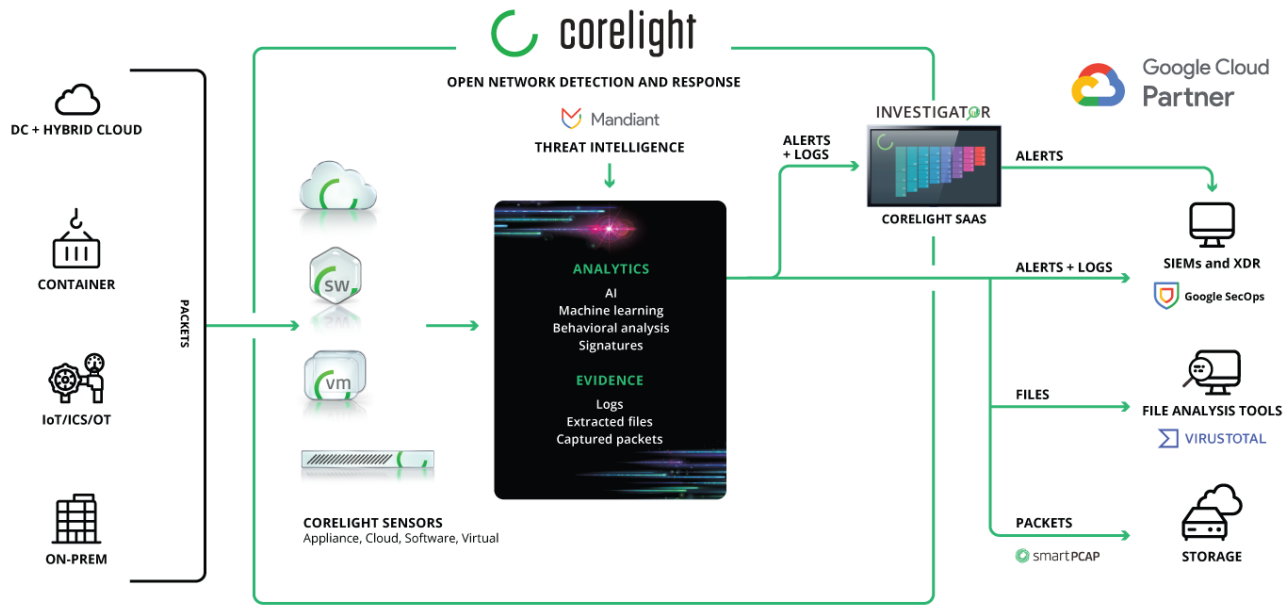
Additionally, with Corelight network evidence powering Security Operations SOAR playbooks, your overextended team can maintain a stronger security posture with more certainty and less effort. And the ability for Corelight to identify suspicious files and trigger malware analysis through Google VirusTotal gives users the ease and insight to respond to threats faster and easier than ever.

HELPING INCIDENT RESPONSE TEAMS OPTIMIZE INVESTIGATIONS

Corelight's advanced network telemetry is trusted by some of the world's most experienced incident responders. By correlating and analyzing over 50 network protocols, Corelight transforms network traffic into comprehensive, protocol-rich evidence that helps incident response and managed defense consultants, like those at Mandiant, accelerate investigations like never before.

By combining rich Corelight data with Google Security Operations massive scalability and "sub-second" search capability, threat analysts can quickly determine the historical genesis of attacks and take steps to reduce the likelihood of future attacks. Whether you're an incident responder or executive responsible for mitigating risk, we encourage you to explore how Corelight has become essential for optimizing investigations, ensuring defensible disclosure to stakeholders, and maintaining a stronger security posture.

Corelight Open NDR and Google Security Operations



SOLUTION BENEFITS

COMPLETE VISIBILITY

Spot early-, mid-, and late-stage signs of network compromise with superior visibility into all network traffic, including across hybrid, multi-cloud, and distributed environments, as well as into devices that can't support endpoint agents. Rich, correlated, security-specific evidence goes back months, not days.

IMPROVE NETWORK DETECTION & COVERAGE

Integrated with Google Security Operations, Corelight's high-fidelity, correlated network telemetry delivers powerful detection insights that enables your team to find and respond to threats quickly and confidently. Organizations can use Google Threat Intelligence to enrich Corelight high-fidelity logs and prioritize Suricata alerts that simplify detections for your over-extended SOC team.

ACCELERATE RESPONSE

Establish a network baseline and spot anomalies with correlated alerts, evidence, and packets so SOC analysts can respond quickly and accurately with the scope and severity of adversary activity. Corelight powers Google Security Operations SOAR playbooks and existing workflows to slash false positives and alert backlogs, so analysts can focus on higher-value activities.

INCREASE OPERATIONAL EFFICIENCY

Boost analyst efficiency and reduce data costs in downstream analytics with 4:1 tool consolidation that provides uniform network telemetry. Simplify compliance requirements across on-prem and cloud environments.

corelight

To learn more about Corelight for Google Cloud Security, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497