corelight | Google Cloud

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.

Integrated across google security operations platform

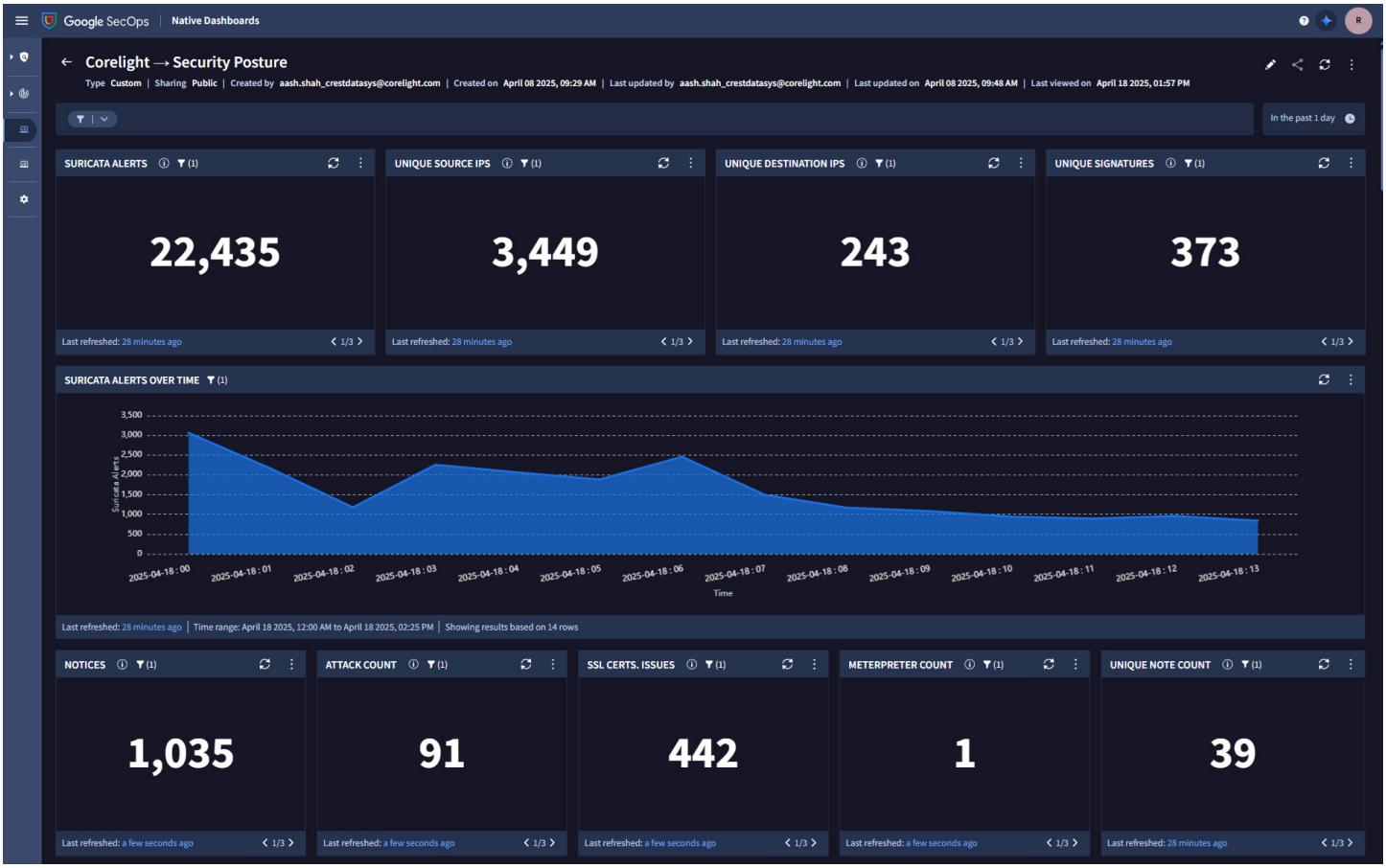
Corelight's Open NDR Platform integrates across the Google Security Operations Platform to deliver a superior level of attack visibility, response, and threat hunting capabilities. Organizations can use Google Threat Intelligence to enrich Corelight's comprehensive, high-fidelity logs and prioritize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

INTEGRATION HIGHLIGHTS

- Streamline workflows with native integration across Google Security Operations Platform
- Intuitive dashboards provide at-a-glance and detailed insights
- Reduce alert fatigue, simplify investigations, and know the origins of attacks
- Corelight Cloud Sensor for Google Cloud provides complete network visibility in the cloud
- Trusted by Mandiant Incident Response and Managed Defense teams

Intuitive dashboards provide quick views of an organization's security posture with summary charts, maps, and counters to help SOC analysts quickly determine trouble spots that need immediate attention. They can then drill down into relevant details to accelerate investigations while streamlining workflows.

Transforming network traffic into comprehensive, detailed evidence



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

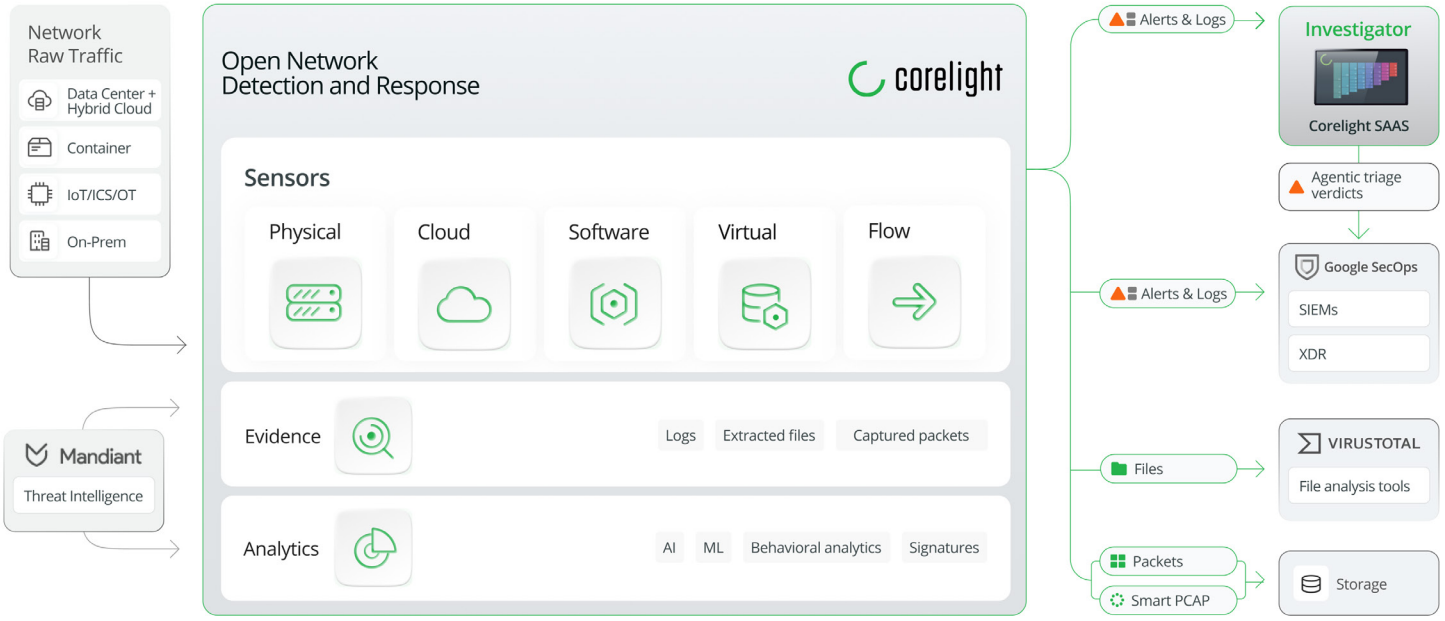
The ability for Corelight to identify suspicious files and trigger malware analysis through Google VirusTotal gives users the ease and insight to respond to threats faster and easier than ever.

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



corelight

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

https://corelight.com/contact

info@corelight.com

All rights reserved. © Copyright 2026 Corelight, Inc.