Google Cloud | corelight

JOINT SOLUTION

Advanced network detection & response for Google Chronicle

IT COMPLEXITY IS DECREASING VISIBILITY

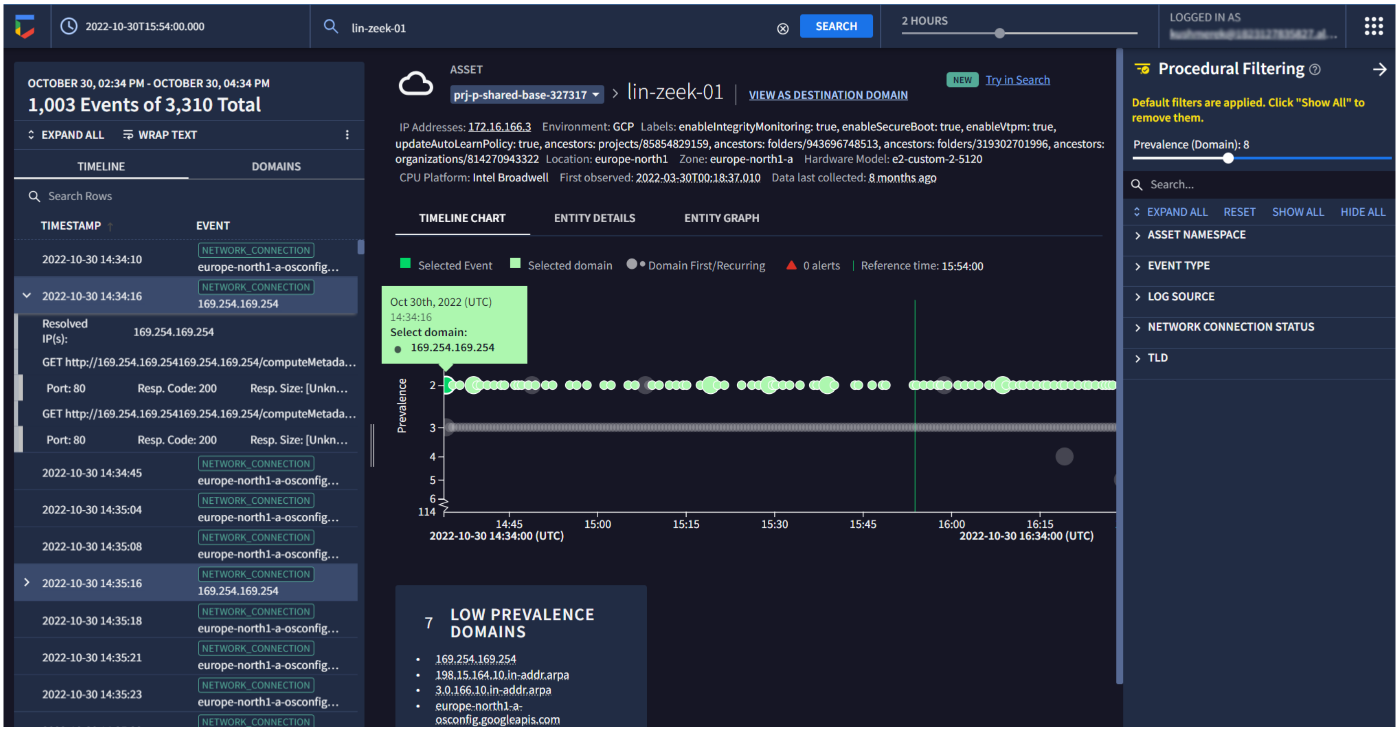
Navigating today's cybersecurity landscape is challenging, particularly without a complete view of what's happening across an organization's increasingly distributed environment. As cloud services become more prevalent, smart device usage surges, and microservices architectures become more common, the 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 Chronicle Security Operations Suite tame the exponential growth of security alerts and incidents to understand the interrelated details of even the most sophisticated attacks.

INTEGRATION HIGHLIGHTS

- Best-in-class NDR and internet-scale SIEM/SOAR platform
- Optimal visibility of all activity across IT, IoT, and OT networks
- Reduce alert fatigue, simplify investigations, and know the origins of attacks
- Trusted by Mandiant Incident Response and Managed Defense teams

TRANSFORMING NETWORK TRAFFIC INTO COMPREHENSIVE, DETAILED EVIDENCE



[redacted]

OCTOBER 30, 02:34 PM - OCTOBER 30, 04:34 PM
1,003 Events of 3,310 Total

TIMESTAMP	EVENT
2022-10-30 14:34:10	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:34:16	NETWORK_CONNECTION 169.254.169.254 Resolved IP(s): 169.254.169.254 GET http://169.254.169.254169.254.169.254/computeMetada... Port: 80 Resp. Code: 200 Resp. Size: [Unkn... GET http://169.254.169.254169.254.169.254/computeMetada... Port: 80 Resp. Code: 200 Resp. Size: [Unkn...
2022-10-30 14:34:45	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:35:04	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:35:08	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:35:16	NETWORK_CONNECTION 169.254.169.254
2022-10-30 14:35:18	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:35:21	NETWORK_CONNECTION europe-north1-a-osconfig...
2022-10-30 14:35:23	NETWORK_CONNECTION europe-north1-a-osconfig...
	NETWORK_CONNECTION

ASSET
prj-p-shared-base-327317 > lin-zeek-01 | VIEW AS DESTINATION DOMAIN

IP Addresses: 172.16.166.3 Environment: GCP Labels: enableIntegrityMonitoring: true, enableSecureBoot: true, enableVtpm: true, updateAutoLearnPolicy: true, ancestors: projects/85854829159, ancestors: folders/943696748513, ancestors: folders/319302701996, ancestors: organizations/814270943322 Location: europe-north1 Zone: europe-north1-a Hardware Model: e2-custom-2-5120
CPU Platform: Intel Broadwell First observed: 2022-03-30T00:18:37.010 Data last collected: 8 months ago

7 LOW PREVALENCE DOMAINS
- 169.254.169.254
- 198.15.164.10.in-addr.arpa
- 3.0.166.10.in-addr.arpa
- europe-north1-a-osconfig.googleapis.com

Procedural Filtering

Default filters are applied. Click "Show All" to remove them.

Prevalence (Domain): 8

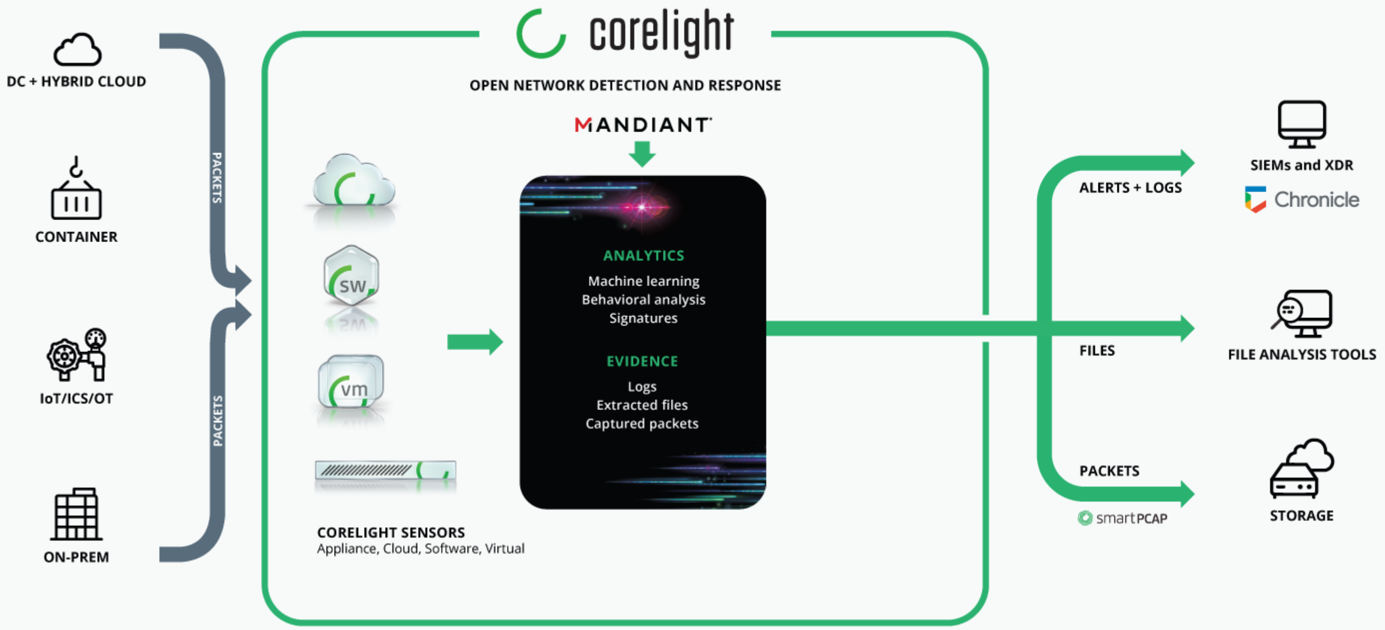
Corelight data integrates directly into Google Chronicle Unified Data Model (UDM).

INTEGRATED ACROSS CHRONICLE SECURITY OPERATIONS SUITE

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

Additionally, with Corelight network evidence powering Chronicle 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 Chronicle users the ease and insight to respond to threats faster and easier than ever.

CORELIGHT OPEN NDR AND GOOGLE CHRONICLE



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 consultants, like those at Mandiant, accelerate investigations like never before.

By combining rich Corelight data with Chronicle's 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.

SOLUTION BENEFITS

COMPLETE VISIBILITY

Corelight gives Google Cloud and Mandiant Services customers a comprehensive view of all an organization’s network traffic and devices, including devices that can’t support an endpoint agent, across hybrid, multi-cloud, and distributed environments.

NEXT-LEVEL ANALYTICS

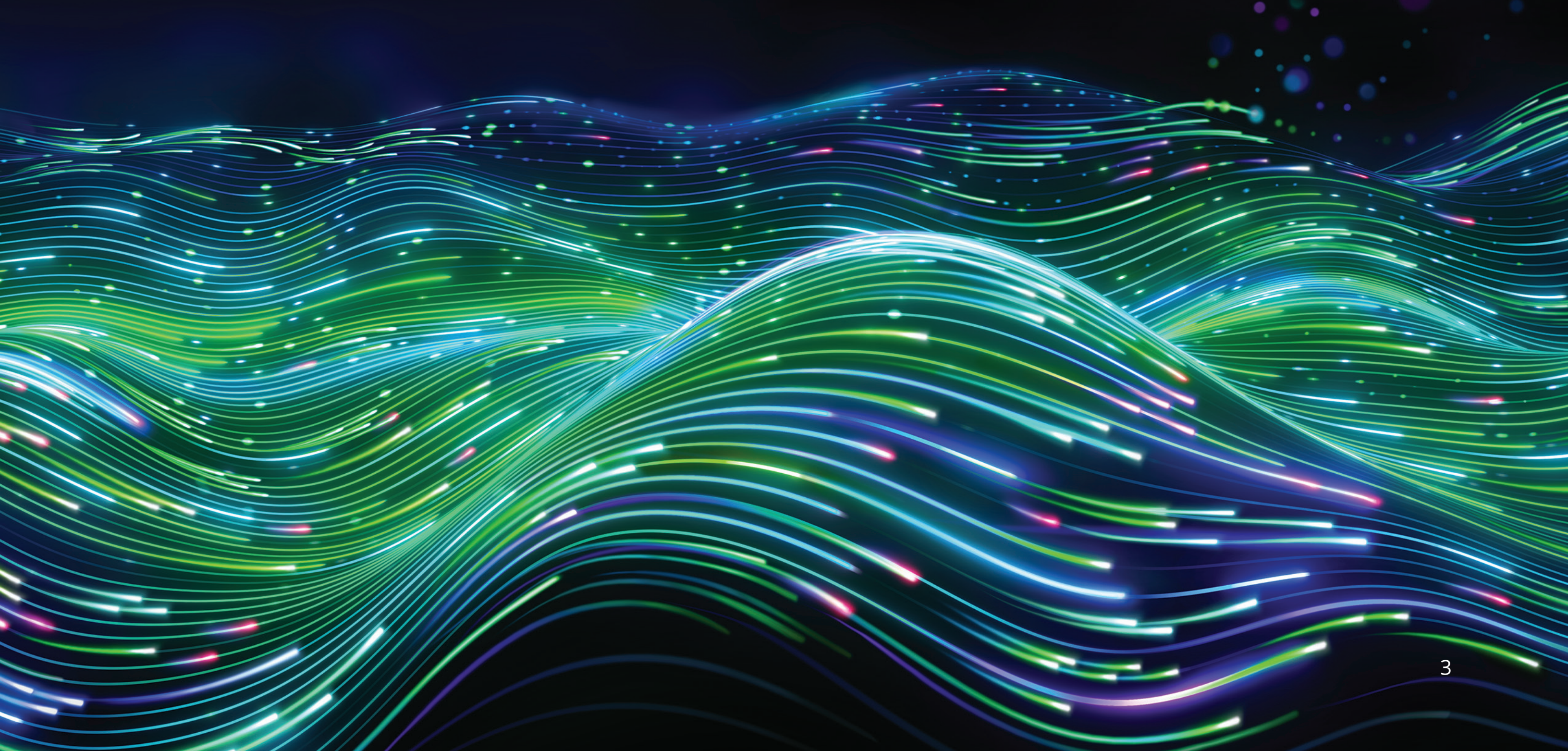
High-fidelity, correlated network telemetry integrated with Google Chronicle and Mandiant Threat Intelligence improves the effectiveness of threat analytics, threat detection, and the passive classification of discovered devices.

FASTER INVESTIGATION

By correlating alerts, evidence, and packet data, Corelight’s rich and contextual evidence powers Google Chronicle and Chronicle SOAR playbooks to greatly simplify and accelerate investigations and enable overtaxed SOC analysts to focus on higher-value activities.

EXPERT HUNTING

Combining Corelight’s rich network telemetry with key elements of the Chronicle Security Operations Suite enables your team to investigate alerts faster and easier than ever so even junior analysts can be expert threat hunters too.



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

corelight

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