corelight

OPEN NDR

CLOSE THE CASE ON NETWORK ATTACKS

Rapidly neutralize and contain network-based threats with Corelight's Open NDR Platform

Detections, artificial intelligence (AI), intrusion detection (IDS), network security monitoring (NSM), and packet capture (PCAP) combine into a powerful single security tool. Disrupt adversaries with IR dashboards and slash SOC response times. Open NDR runs on open-source and proprietary technologies and is available in on-prem and SaaS formats that are built to scale.

IMPROVE NETWORK DETECTION COVERAGE

- **Identify known attacks and tools**
- **Expose novel techniques**
- **Coverage for 80+ TTPs across hybrid-cloud infrastructure**

70,000+ total rules and detections including AI, machine learning (ML), behavioral, and signature-based. Threat intelligence and search-based alerts plus Rapid Threat Response from the Corelight Labs Team.

ACCELERATE RESPONSE

- **Resolve tickets with AI-assisted workflows**
- **Investigate with prioritized alerts + contextual evidence**
- **Minimize impact by identifying true threats and reducing false positives**

Respond with immediacy and accuracy knowing the scope, severity, and spread of adversary activity. Ask about our ***95% faster response time*** case study.

INCREASE OPERATIONAL EFFICIENCY

- **4:1 tool consolidation**
- **Reduce data costs in downstream analytics**
- **Simplify compliance across on-prem and cloud with uniform evidence**

Move faster with connected data in one place. Automate manual data tasks and store more data—10x packet capture retention periods—while saving on costly maintenance.

GET COMPLETE VISIBILITY

- **Monitor N/S, E/W, multi-cloud, and ICS/OT activity**
- **Expand visibility into 50+ protocols, including DNS**
- **Identify 500+ VPNs with our Encrypted Traffic Collection**

Spot early, mid, and late-stage signs of network compromise. Corelight logs capture activity in detail for exceptional insight into network traffic.

TRUSTED BY

CROWDSTRIKE

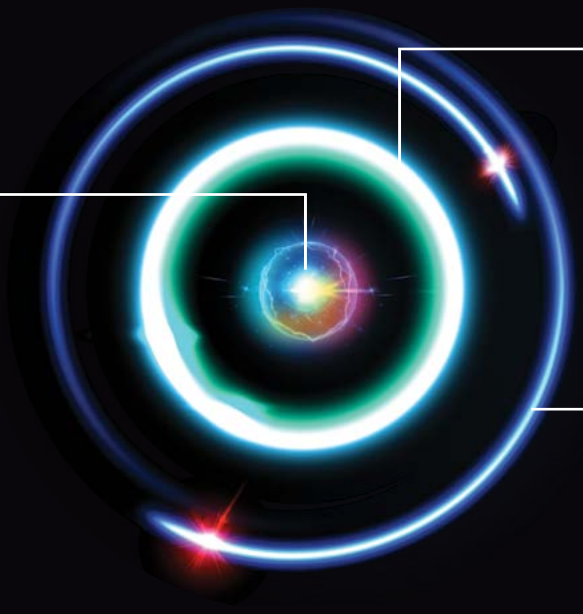
MANDIANT NOW PART OF Google Cloud

Microsoft

black hat

OPEN NETWORK DETECTION & RESPONSE

Corelight’s **open core, data,** and **detections** power rapid action against cybersecurity threats in adverse and shifting conditions.



OPEN CORE

Open NDR is powered by proven open-source technologies Zeek® and Suricata® with over 25 years of insights being continuously improved by a community of elite defenders.

zeek.

NETWORK SECURITY MONITOR

SURICATA

INTRUSION DETECTION SYSTEM

OPEN DATA

Open data formats **easily integrate** with existing SIEM, XDR, or datalake solutions. Avoid vendor lock-in: your data is yours to keep.

OPEN DETECTIONS

Gain broad coverage and detect emerging threats (e.g., SolarWinds with Zeek). Open detections can be customized and extended and are continuously updated.

> *“If your SOC needs better visibility, in particular in a way that will integrate with any of the other tools in your security stack, Corelight is the way to do it.”*

Verified review, G2.com

1-(888)-547-9497

corelight

info@corelight.com

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.

The information provided is intended for general informational purposes only. While we strive to ensure the accuracy and reliability of the content presented, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained herein.