NETWORK DETECTION & RESPONSE

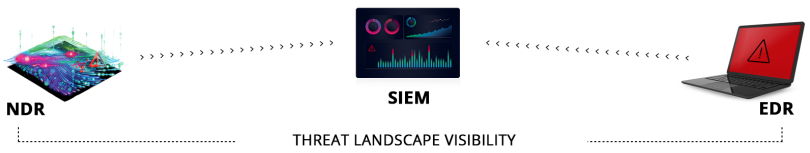
corelight

COMPLETE VISIBILITY WITH OPEN NDR

You can't protect yourself from what you can't see. Visibility over all activity on your network lets you see what adversaries are up to—before they strike.

WHAT IS OPEN NDR?

NDR uses network data to detect and respond to threats. It incorporates traffic analysis and detections (including ML and others) to monitor and log network activity, providing evidence to investigate breaches and perform forensics. NDR platforms analyze network traffic, delivering telemetry into existing SIEM, XDR, or SaaS-based solutions.



Corelight's NDR platform—Open NDR—is a true open platform because it frees you from proprietary formats and UIs. Open NDR is built on established open-source software and enhanced by continuous innovation from Zeek®, Suricata, and other communities.

SEE ALL ACTIVITY & DEVICES

CLOSE VISIBILITY GAPS

SPOT UNKNOWN ASSETS

UNCOVER ATTACKS IN MOTION

ACCELERATE MTTR

VALIDATE COMPLIANCE

EDR + NDR

SOCs discover they need additional visibility on the network after deploying Endpoint Detection and Response (EDR). Paired together, NDR and EDR provide the breadth of coverage needed to paint the complete picture of the threat landscape. NDR telemetry details such as attack vectors and scope of impact are used to investigate and close incidents with decisiveness and certainty.

HOW NDR WORKS

Corelight's Open NDR Platform connects the entire investigation—from detection to Smart PCAP—with network transaction logs that provide a detailed history of every event. Responders can rapidly assess and verify incidents, confidently closing and covering more of them using familiar tools from:

aws CROWDSTRIKE MANDIANT Microsoft splunk>

DETECT AND COVER MORE THREATS

- Speed through alert backlogs with one-click pivots
- Establish a network baseline to spot anomalies
- Add new behavioral, ML, and signature detections
- Cover ATT&CK® tactics such as C2, Discovery, and Exfiltration
- Proactively threat hunt to uncover dwelling adversaries
- Automate to reduce false positives

ANSWER CRITICAL SECURITY QUESTIONS

- How long has the attacker been inside your network?
- Was the attack completely contained?
- What are all the devices connected to your network?
- Are there shadow IT or rogue access points?
- Are compliance controls fully in effect?

DO IT ALL FROM ONE COST-EFFECTIVE PLATFORM

The integrated Open NDR Platform can replace standalone legacy systems such as traditional IDS, Netflow, full PCAP, and DIY open source deployments for a more efficient SOC and lower overall maintenance and operational costs.

Powered by zeek. SURICATA

Corelight supports the Open Information Security Foundation (OISF).

TRAFFIC VISIBILITY

CLOUD

NORTH-SOUTH

EAST-WEST

IOT

ICS

ENCRYPTED

corelight

GET A DEMO

1-(888)-547-9497

info@corelight.com