corelight

Solution brief

# Complete multi-stage intrusion detection with Corelight Open NDR

## THE VISIBILITY GAP ADVERSARIES COUNT ON

Modern attackers rarely trip a single, obvious alarm. They move quietly across multiple stages of an attack chain: (1) gaining initial access, (2) execution, (3) defense evasion, (4) establishing communications (command and control), (5) moving laterally and (6) exfiltrating data, all while blending into normal traffic. Living-off-the-land (LotL) techniques, encrypted channels, and Kerberos abuse let them evade endpoint security controls and log-based detection mechanisms entirely.

For detection engineers, that creates a hard problem. You can only write rules for what you can see. When telemetry is limited to the endpoint or arrives pre-summarized in the Security Information and Event Management (SIEM) platform, whole stages of an attack are missing. Corelight Open NDR closes that gap by turning every packet into forensic-grade evidence, then mapping and correlating detections across an entire multi-stage intrusion attack.

## WHAT CORELIGHT DELIVERS

Corelight Open NDR includes multiple layers of detection engines, including IOC, signature, YARA, behavioral, supervised machine learning (ML), and anomaly detection. These layers are built on a Zeek® foundation in the Corelight Sensor and provide the basis for multi-stage intrusion detection. Corelight tracks and detects an attack as it progresses in an attack, starting with initial access, moving laterally across the network, communicating back to the attack source, and exfiltrating data.

Instead of receiving fragmented security signals across multiple log types with inconsistent field names and incompatible severity scales, agentic triage takes alerts from different detection engines and correlates them to a specific entity and maps them to the MITRE ATT&CK framework, giving analysts a consistent and easy-to-understand view of an attack with the ability to easily pivot to the underlying evidence as proof of the attack.

The result is high-fidelity detections based on deep, inspectable network evidence that you can trust, tune, and version like code.

- **Over 100 MITRE ATT&CK TTPs covered**, with over 90% coverage across network-relevant tactics including Initial Access, Lateral Movement, C2, and Exfiltration
- **Forensic-grade telemetry** from Zeek, extracting 400+ data fields across 35+ protocols in real time
- **Layered detection engines:** IOCs, Suricata signatures, YARA file analysis, behavioral analytics, supervised and unsupervised ML
- **Smart PCAP** to capture the packets that matter, cutting capture volume by up to 95% and cost by roughly 50%
- **Unified evidence model** that links logs, files, and PCAPs by a unique entity identifier into one investigative timeline

## DETECTION ACROSS EVERY STAGE OF THE INTRUSION

Corelight aligns detections to the stages of an attack, so no stage goes dark.

### Initial access

Corelight exposes the earliest stages of an intrusion, surfacing techniques that typically evade endpoint detection:

- **Credential guessing and brute-force:** automated detection across critical authentication protocols (SMB, SSH, LDAPS, RADIUS, MSSQL, WinRM)
- **OS credential harvesting:** evasion-resistant identification of MITRE T1003 techniques, even when adversaries use renamed tools, like anomalies with DCSync
- **Kerberos & NTLM abuse:** behavioral modeling to catch sophisticated attacks using Kerberoasting and NTLM
- **Adversary infrastructure exposure:** proactive identification of risky connections and malicious SSL/TLS certificates associated with disposable or automated domains
- **Insider and foreign threats:** detect use of shadow AI and communication with specific countries that may indicate the beginning of either malicious or unintentional insider activity

### Execution

Corelight surfaces execution-stage attacks by detecting malicious file delivery and unauthorized code execution patterns, ensuring visibility into the transition from initial access to active threats.

- DGA malware detection
- Detections of malicious executable file downloads on subnet

### Defense evasion

Corelight identifies efforts by attackers to mask their presence and bypass security controls by analyzing traffic patterns and certificates that deviate from legitimate network behavior.

- Tor connections
- Malicious SSL certificate
- Anomalous protocol tunneling

### Command and control

Corelight ships 50+ C2 detections spanning known and novel activity. ML catches DGA domains, beaconing, multi-domain HTTP C2 frameworks, and anomalous use of protocol tunneling, VPN, and other tactics for C2 communication. Purpose-built detectors identify Caldera beacons and QuasarRAT's hardcoded TLS certificate. DNS and ICMP tunneling get caught through native protocol parsing, not guesswork.

### Lateral movement

Behavioral models can analyze and baseline normal east-west traffic, then surface the anomalies and tactics that matter:

- **Administrative tool usage**, including admin share and SMB access
- **RDP, SSH** unusual activity and usage
- **Protocol tunneling** and **encrypted traffic** anomalies
- **DCE/RPC** tracking and anomalous use
- **LOTL** usage: Unusual use of native OS tools (e.g. PowerShell)
- Internal **file transfers**: data staging and exe file transfers

### Exfiltration

ML models target exfiltration, including anomalous large outbound files, exfil over DNS, and other tactics, while cloud sensors detect S3 data exfiltration and service enumeration. File extraction across 200+ file types supports scoping, recovery, and containment verification.

## BUILT FOR EVASIVE THREATS

Attackers who bypass endpoint security still have to cross the network. Corelight sees the activity. Corelight has custom detections for evasive activity including capabilities around:

- **Encrypted traffic:** JA3 fingerprinting and SNI analysis expose malicious connections without decryption, remaining resilient against TLS 1.3
- **LOTL techniques:** Behavioral analytics catch legitimate OS tools used for illegitimate purposes
- **Protocol tunneling:** Detection of DNS, ICMP, and other protocol abuse used for command and control or data exfiltration via native protocol parsing
- **Kerberos threat detection:** Behavioral modeling tuned for Kerberos and NTLM traffic to identify DCSync, Kerberoasting, and NTLM use in attacks

## OPTIMIZED ACCURACY: REDUCING FALSE POSITIVES

With detection capabilities that include machine learning, there may be a concern about the false positive rate. Corelight reduces false positives at the source by using peer group modeling, comparing an entity against similar users or devices, so an anomaly only alerts when it deviates from both the individual and its peers. In addition, Corelight offers tunable thresholds for machine learning models to let customers adjust these models to their specific environments.

## ONE UNIFIED ATTACK NARRATIVE FOR DETECTION AND RESPONSE

Detection is only half the job. Corelight's Agentic Triage transforms manual, alert-by-alert analysis into automated, entity-centric investigations that group related alerts for complete context. By applying expert-designed playbooks, it delivers structured, evidence-backed verdicts with plain-language explanations, ensuring consistent, high-quality analysis. This approach empowers analysts to achieve up to 10x faster triage by eliminating repetitive manual tasks like data fetching and correlation, while maintaining full transparency through explainable AI workflows—all on a single screen with an interactive visual timeline.

## REAL-TIME INTELLIGENCE, AUTOMATED DEPLOYMENT

Detections stay sharp only when intelligence stays current. In addition to Corelight provided detection subscriptions, other available threat feeds include:

- **CrowdStrike-powered threat intelligence:** an hourly feed of high-fidelity IOCs (IPs, domains, URLs, and file hashes) drawn from Falcon telemetry, filtered centrally by Corelight to minimize noise, and distributed to sensors within two hours via Fleet Manager
- **Analyst1 TIP automation:** automates retrieval, validation, and deployment of Suricata and YARA rules in STIX/TAXII format straight to your sensors, replacing slow, error-prone manual workflows

Pairing rigorously scored IOCs and signatures with the other detection layers and rich network evidence lets you correlate, validate, and prioritize alerts instantly, which is exactly how you turn alert fatigue back into confidence.

## DETECTION-AS-CODE, THE WAY YOU ALREADY WORK

Corelight operationalizes Detection as Code by treating your security detections with the same rigor as application code. Through Fleet Manager, you can manage Zeek, Suricata, and YARA rules across your entire sensor footprint using standardized CI/CD pipelines, providing a version-controlled, repeatable path from commit to production. Because our detection logic is transparent and extensible, rather than a black box, your team can confidently tune models, inject custom logic, and continuously prove coverage against evolving threats.

## OUTCOMES FOR THE DETECTION TEAM

- **Multi-stage intrusion detection:** Corelight tracks and correlates attack activity across the intrusion lifecycle, providing end-to-end visibility from initial access to data exfiltration
- **Broader coverage:** triple your TTP detection across MITRE ATT&CK by replacing standalone IDS
- **Lower false positives:** layered signatures, ML, behavioral analytics, correlated alerts, and peer group modeling feed the SOC high-confidence evidence
- **Faster investigations:** a unified timeline shrinks MTTD and MTTR by ending console-hopping
- **Leaner pipelines:** 50–80% data aggregation lowers SIEM and data lake ingest costs while keeping full fidelity on the sensor

## WHY IT MATTERS

Deploying Corelight Open NDR is more than adding another tool to the stack. It restores visibility to the key stages of an attack that endpoint and log-based tooling miss, and it hands detection engineers the evidence, coverage, and automation to act on it. You see the components of a multi-stage intrusion, create and tune your detection, and ship detection code that holds up against adversaries who keep changing tactics.

To learn more about multi-stage intrusion detection with Corelight Open NDR, request a demo at

**https://corelight.com/contact**

info@corelight.com | 888-547-9497

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.

All rights reserved. © Copyright 2026 Corelight, Inc.