corelight

SecOps transformation with network **evidence-driven preemptive threat detection**

The reality of EDR, SIEM and NGFW based SOC

Traditional SOC architectures struggle to keep pace with emerging threats. Those with EDR, SIEM and NGFW at core rely on automation to drive response.

Visibility and data collection

94%

of CISOs reported experiencing at least one disruptive attack in the past year, driven by insufficient visibility from inadequate log practices and non-standardized data sources that create blind spots in threat detection.

(Source: 2025 Splunk CISO report)

Detection alignment with threat profiles and attack surfaces

Breaches at firewalls/VPN gateways surged from

3% ⟶ 22%

exposing the difficulty in aligning detection rules with specific organizational threat profiles. This leads to a scattered approach that misses relevant threats and exposes weaknesses in EDR and SIEM-based SOC architectures.

(Source: 2025 Verizon DBIR)

Balancing automation with human expertise

By 2030,

75%

of SOC teams are expected to experience erosion in foundational security analysis skills due to overdependence on automation and AI. Automation cannot replace human expertise; SOCs must integrate AI with human insights to ensure accurate detection and streamlined workflows.

(Source: 2025 Splunk CISO report)

Over-reliance on a singular threat detection method

Companies spend an estimated

$1.27 million

annually and 395 hours per week chasing false positives. Traditional methods relying on historical patterns and known threats—like signatures, malicious IPs, and harmful files—as well as modern machine learning struggle against dynamic, adaptable GenAI-driven threats, leading to high false positive rates.

(Source: Gartner)

Network evidence as the foundation for SecOps transformation

Network data is essential for transforming SecOps

Unmatched visibility

You can't defend what you can't see

Network data offers comprehensive visibility across all network traffic, especially in areas where EDR coverage doesn't exist, enabling SOCs to **see the unseen** and detect evasive threats.

Tailored threat detection

Detection strategies and engines can be tuned to **adapt to the organizational threat** profile and attack surfaces.

Deep context and AI integration

The right network data strategy can **enrich the data with context from threat feeds** and other tools like EDR and turn it into evidence that detection engines can leverage.

Preemptive threat detection for SecOps transformation

The shift from reactive detection and response to preemptive threat detection is critical for SecOps transformation

Attack anticipation

With assumed breach mentality, SecOps needs to monitor and fine-tune threat detection continuously, to **stay ahead of threats** by identifying, disrupting, and neutralizing them early.

Threat hunting as a standard practice

Fuel proactive threat hunting, enabling detection of novel and unknown attacks by **leveraging network evidence.**

Build SecOps knowledge base

Leverage the explainability of detections and AI assistance to **accelerate triage and expand** the SecOps teams' knowledge base.

Corelight's Open NDR-fueled preemptive threat detection

Corelight's **network evidence enables a proactive approach** that helps organizations defend against AI-enabled threat actors, advanced malware, zero-days, ransomware, evasive attacks, and other threats often missed by traditional "detect-and-respond" methods.

CORELIGHT DELIVERS:

A multi-layered detection strategy

fuses machine learning, behavioral analytics, curated signatures, and threat intelligence to **deliver prioritized aggregated alerts** based on risk and expert-tuned detections without relying on any single methodology, reducing alert fatigue.

Broad network visibility

complements EDR by detecting threats that evade endpoint defenses, such as lateral movement and anomalous activity. Its high-fidelity security data fuels proactive threat hunting, enabling the detection of novel and previously unknown attacks.

Network evidence-enriched detections

with deep context and AI-driven automations—providing **evidence-backed** summaries, explainability, guided triage, and analyst-ready workflows to **accelerate investigations and expand the SOC knowledge base.**