corelight | CROWDSTRIKE

Joint solution brief

Corelight integration with CrowdStrike Falcon® Adversary Intelligence

Automated correlation of high-confidence threat intelligence and network evidence for faster detection and decisive response

Security teams know that combining threat intelligence with real-time network telemetry is essential for defending against AI-enabled adversaries that operate with staggering speed. But simply having access to better intelligence and network telemetry offers only a partial solution for defending against increasingly sophisticated attacks. A complete solution requires operationalizing the two data sources to produce the context needed to respond quickly and confidently to active threats across the environment.

Without high-confidence intelligence and ground-truth network evidence, analysts are left cross-referencing stale or noisy indicators of compromise (IOCs) against historical SIEM data, rather than matching active threats with live network evidence. This disconnect forces defenders to spend critical hours manually connecting the dots across disparate platforms, slowing incident response, increasing alert fatigue, and leaving organizations perpetually one step behind fast-moving adversaries

The Corelight and CrowdStrike integration solves this operational bottleneck by automatically pulling CrowdStrike Falcon® Adversary Intelligence data, including detection rules and current indicators of compromise, directly into Corelight sensors. Instead of forcing analysts to manually piece together stale or siloed data or sift through historical SIEM logs, this joint solution correlates timely high-confidence threat intelligence with real-time, forensic-grade network behavior and historical log data into the detection workflow. By enriching Corelight's network evidence with adversary-focused insights at the sensor, security teams can spot advanced active attacks, uncover "living-off-the-land" threats, and move from tedious investigations to decisive response while reducing operational overhead.

SOLUTION HIGHLIGHTS

- Detect active threats faster with real-time network evidence and high-confidence threat intelligence
- Identify "living-off-the-land" and lateral movement with curated and timely IOCs applied to historical network evidence
- Respond quickly and decisively with industry-leading IOCs and detection rules correlated with world-class network evidence
- Reduce manual workflows by automatically enriching network telemetry with threat intelligence directly at the Corelight sensor

Streamline threat detection and response with confidence

Corelight's Open NDR Platform transforms raw network traffic into comprehensive evidence to help data-first organizations optimize threat investigations and detections. Native integration across the CrowdStrike Falcon® platform helps resource-constrained SOC teams streamline threat detections in their favorite SIEM, XDR platform, or directly from Corelight Investigator.

Operationalizing Falcon Adversary Intelligence with the Corelight platform is easy and done through a standard API credential configuration in Corelight Fleet Manager. Fleet Manager (or the Corelight-update utility) then periodically polls the CrowdStrike Falcon APIs to retrieve curated, high-confidence threat intelligence, including IOCs, Suricata rules, and YARA rules, and pushes it to the organization's Corelight sensors.

The result is a tightly integrated, continuously updated detection pipeline that keeps security teams ahead of threats, not chasing them.

corelight

To learn more about Corelight for CrowdStrike Falcon, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497