corelight | CROWDSTRIKE

Joint solution brief

# Corelight Investigator integration with CrowdStrike Next-Gen Identity Security

**Accelerate threat triage and prioritize response with unified network, host, and identity context**

Security teams often struggle to maintain a robust security posture because the variety of traditional tools they've deployed in their threat detection program fails to correlate host and user data with real-time network activity. The resulting visibility gap forces SOC analysts to routinely pivot across disparate tools and multiple screens to manually correlate host, user, and network data. This fragmented approach not only makes it difficult to spot adversaries skilled in avoiding detection but it also elongates response times and amplifies alert fatigue.

Corelight integration with CrowdStrike Falcon Next-Gen Identity Security was designed to address this critical "network-identity blindness" by ingesting real-time host and identity data from CrowdStrike Falcon directly into your Corelight Investigator detections dashboard. In addition to helping analysts focus on systems and users that pose the greatest risks, the solution provides the essential context needed to make quick, high-confidence decisions on alerts, close tickets faster, and maintain a stronger security posture.

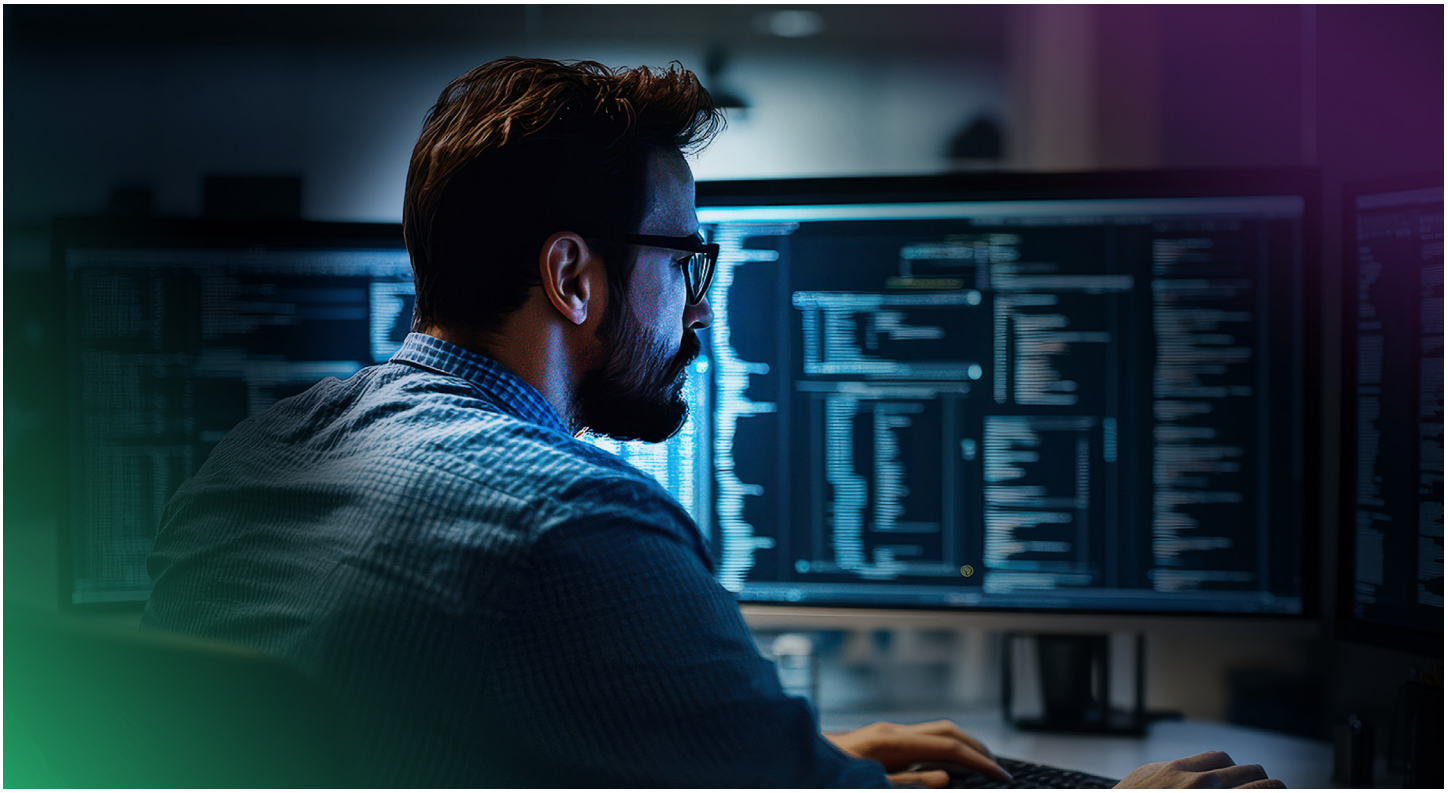
**INTEGRATION HIGHLIGHTS**

**Unified visibility**—Rich Corelight multi-layered detections enriched with contextual real-time host and identity data

**Risk prioritization**—Accelerate investigations by correlating network evidence with CrowdStrike Next-Gen Identity Security risk scores

**Faster remediation**—Improve mean time to detect and respond to threats without leaving Corelight Investigator detections interface

For example, rather than seeing an anonymous IP address attempting a Kerberoasting attack to impersonate an authenticated user, a Corelight Investigator analyst triaging the source IP can immediately see the specific user details, such as login ID, display name, login history, related alerts, and the user's overall risk score as defined by Falcon Next-Gen Identity Security. Directly integrating this real-time identity context into the Investigator detection workflow is crucial for efficient alert prioritization and quick remediation, as it unmasks the user, minimizes context switching between different products, and eliminates the manual effort of stitching data together across various dashboards.



**Ground-truth network evidence for CrowdStrike Falcon**

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 Falcon platform helps resource-constrained SOC teams streamline threat detections in their favorite SIEM or directly from Corelight Investigator.

By ingesting real-time endpoint and identity data from CrowdStrike Falcon Insight XDR and Falcon Next-Gen Identity Security directly into your Corelight Investigator detections, analysts can focus on the systems and users that pose the greatest risks to the environment. No more pivoting and no more copying and pasting incomplete data between different host, identity, and network tools.

Integrating Corelight with Falcon Next-Gen Identity Security provides analysts and threat hunters with the critical context required to swiftly triage, prioritize, and neutralize identity-based attacks before they escalate into expensive breaches.

corelight

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

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

info@corelight.com | 888-547-9497