corelight | CROWDSTRIKE

Joint solution brief

Corelight Investigator integration with CrowdStrike Charlotte AI

Accelerate incident response with agentic human-AI collaboration

Security operations teams are constantly battling the "pivot tax", the manual friction of jumping between endpoint and network consoles to validate threats. This fragmented workflow slows down response, increases the risk of human error, and allows threats to dwell longer in the environment.

The Corelight integration with CrowdStrike Charlotte AI eliminates this friction by turning manual data gathering into an automated, collaborative investigation. Built as a native Falcon Foundry application, Corelight plugs directly into Charlotte AI's Agentic Response canvas. This allows Charlotte AI to act as a lead investigator that "interrogates" Corelight's network evidence in real-time. Instead of analysts manually crafting queries, the integrated solution uses Falcon Fusion workflows to ground AI-driven investigations in network reality.

Charlotte AI's Agentic Response canvas accelerates investigations by auto-generating guiding questions to drive investigations - and then answers them. With this integration, Charlotte AI is able to expand the aperture of an AI-led investigation by calling Corelight to contribute critical cross-domain context as the investigation unfolds.

INTEGRATION HIGHLIGHTS

Automated triage—Eliminate manual pivots by allowing Charlotte AI to automatically query Corelight Investigator for network evidence to validate endpoint alerts

Drastically reduced MTTR—Accelerate response times from hours to minutes by automating the evidence retrieval and summarization process directly within the Falcon console

High-fidelity AI grounding—Ensure Charlotte AI's conclusions are backed by Corelight's "gold standard" network data, providing a complete attack narrative for every detection

When Charlotte AI identifies a gap in an investigation, it posts a question to its Response canvas. The Corelight integration automatically recognizes the request, assesses its relevance, retrieves relevant network evidence, and summarizes the findings in plain English. The result is a seamless, automated loop that provides clear evidence to quickly validate and improve detections, so organizations can stay ahead of adversaries with unprecedented speed and technical precision.

Corelight network evidence grounds Charlotte AI in reality

Corelight's Open NDR Platform provides the deep semantic understanding of network traffic required to catch sophisticated threats like lateral movement or data exfiltration. By integrating directly with the Agentic Response canvas, Corelight ensures that Charlotte AI has a "network-aware" perspective on every incident. This means investigations are no longer limited to what happens on the host; they are fueled by the ground truth of what is happening on the wire and can have a complete picture of an attack across domains.

This collaboration transforms how SOC teams operate. Rather than manually correlating data and writing queries, analysts oversee an automated dialogue where Charlotte AI asks the right questions, and Corelight provides the proof. This workflow turns Corelight's network evidence into a native component of the CrowdStrike experience, ensuring investigations are fueled by real-time network data. By combining CrowdStrike's deep endpoint intelligence with Corelight's network ground truth, organizations gain a more holistic and resilient defense while alleviating the toil of manual investigations.

corelight

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

https://corelight.com/contact

info@corelight.com | 888-547-9497