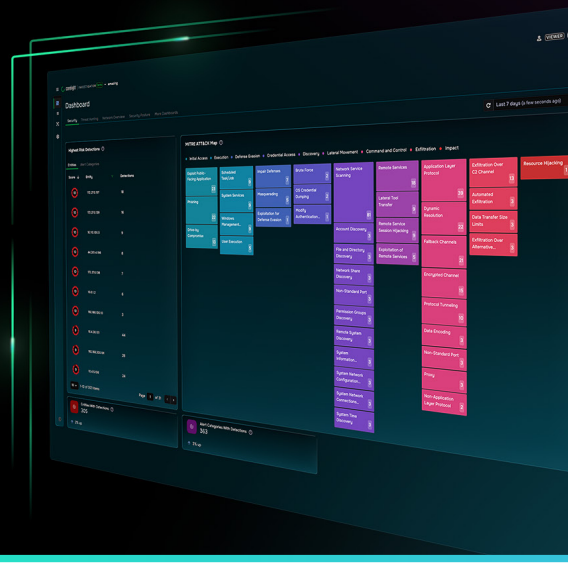
Joint solution brief

Corelight Investigator integration with Cisco XDR



Accelerate incident response with integrated network evidence

Security Operations Centers (SOCs) are constantly striving to reduce complexity and tool sprawl. One way to achieve this is to create a "single-pane of glass" experience that streamlines XDR (Extended Detection and Response) workflows by integrating third-party data, such as Corelight's rich Network Detection and Response (NDR) evidence and alerting. Historically, this required routing Corelight data through Splunk as a middleware step, adding an extra layer of complexity to the security architecture for teams working to centralize their detection and response program on Cisco XDR.

The direct integration of Corelight and Cisco XDR bypasses the need for Splunk to act as middleware. The solution uses a dedicated workflow that ingests Corelight Investigator alerts via webhook, normalizes and parses Corelight's rich network evidence into the appropriate format, and converts them into Custom Security Events within Cisco XDR's Data Analytics Platform (DAP). These events are then promoted to Detection Findings and automatically evaluated for incident generation, enabling the correlation of network threats alongside other security telemetry directly within the Cisco XDR interface.

INTEGRATION HIGHLIGHTS

Automated alert exporting—Delivers high-fidelity network evidence into Cisco XDR without the need for Splunk as a bridge, reducing complexity and overhead

Comprehensive alert coverage—Fully supports and processes Corelight's YARA, Suricata, Anomaly Detection, Machine Learning, and Notice alerts for consistent correlation

Rapid data ingestion—Efficiently ingests up to 25 Corelight alert log bundles per minute directly into the XDR DAP for real-time threat visibility

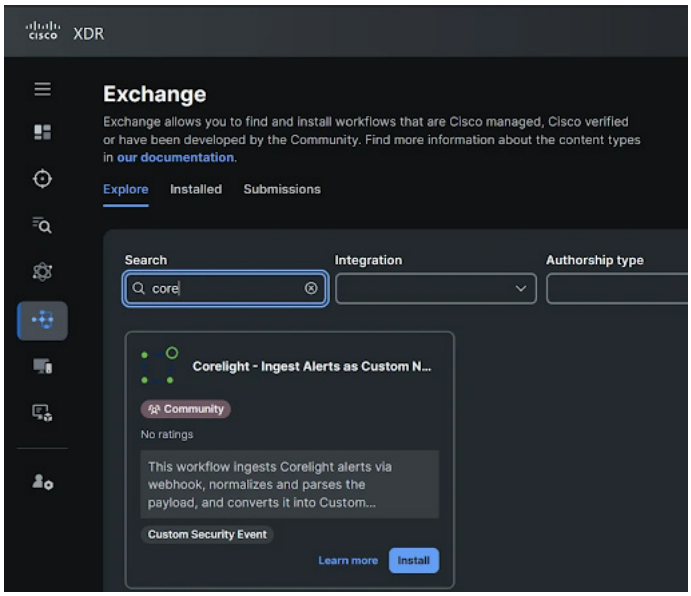
Unified SOC experience—Empowers analysts to view detections, filter sources, and rapidly investigate Indicators of Compromise (IOCs) from the Cisco XDR dashboard

Setting up this solution is straightforward and doesn't require direct sensor integration. First, a customer logs into Cisco XDR to create a new webhook and an associated automation rule, selecting the available "Corelight - Ingest Alerts as Custom Network Security Events" workflow. This generates the webhook URL and API key you'll need to configure the alert exporter in Corelight Investigator. Corelight events will automatically begin flowing into Cisco XDR.

Modernize the SOC experience with integrated network evidence

Corelight acts as the foundational network ground truth for all detection and response programs. By transforming raw network traffic into comprehensive, actionable evidence, Corelight provides the rich network telemetry required to identify and mitigate advanced threats. Furthermore, Corelight's Open NDR architecture gives you complete control over your data, enabling you to customize, create, filter, and integrate it whenever and wherever you want, demonstrating its flexibility and commitment to interoperability.

In addition to its integration with Cisco XDR, Corelight continues to fortify its integration with Splunk and Splunk Enterprise Security to streamline SOC operations for those wishing to unify detection and response on the SIEM platform. For its part, the Corelight App for Splunk provides specialized workflows, intuitive dashboards, and contextual insights that supercharge threat detection, streamline event investigations, and boost overall analyst productivity.



Cisco XDR customers can set up and enable this webhook automation by searching for "Corelight" in XDR Automate—Exchange panel, then setting up alert exports in Corelight Investigator.

corelight

To learn more about Corelight for Cisco XDR, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497