corelight

Solution brief

Corelight Threat Intelligence for the AI-centric SOC

Accelerate detections and minimize false positives with high-quality threat intelligence and ground-truth network evidence

Threat intelligence is the beating heart of modern cybersecurity, yet many organizations struggle to operationalize it effectively. Security teams are inundated with a high volume of Indicators of Compromise (IOCs) from disparate feeds, leading to chronic alert fatigue and difficulty prioritizing real threats. Without a meaningful approach to automatically validate and contextualize this intelligence, security teams spend valuable time second-guessing or, worse, ignoring alerts while sophisticated adversaries slip through the cracks.

THE CHALLENGE

The sheer volume of threat data generated daily presents a massive challenge for security teams. Without effective curation and integration, threat intelligence can create more problems than it solves.

- **Alert fatigue and false positives**
  Low-fidelity and open-source IOC feeds generate an overwhelming number of alerts, forcing analysts to sift through noise to find credible threats
- **Rapidly evolving and sophisticated attacks**
  Cyber threats are constantly becoming more advanced and complex, requiring timely and relevant intelligence to counter effectively
- **Lack of necessary context**
  Raw IOCs—like a suspicious IP address or domain—lack the "who, what, and when" context needed for rapid investigation, slowing down response times
- **Delayed detection**
  Organizations struggle to identify vulnerable hosts and devices across their environments when new IOCs are published

Making matters worse, maintaining multiple threat intelligence feeds and manually deploying rule sets across today's dynamic environments can be slow, cumbersome, and prone to human error, creating gaps in an organization's defense.

THE SOLUTION

Corelight Threat Intelligence, powered by CrowdStrike Falcon Adversary Intelligence, provides a curated, high-fidelity feed of IOCs as an integrated part of the Corelight Open NDR Platform. This enables security teams to operationalize threat intelligence more effectively by automatically correlating a premium feed trusted by more than 30,000 organizations worldwide against Corelight's rich network evidence. Combining this with Corelight's AI-powered multi-layer detections gives overburdened analysts the edge by greatly reducing false positives and accelerating investigations to stay one step ahead of even the most sophisticated adversaries.

Improve threat detection

- Identify known and unknown threats with a multi-layered detection strategy
- Apply the most current, high-fidelity IOCs to both real-time and historical network data
- Uncover advanced threats, including evasive techniques clever adversaries use to bypass traditional defenses

Reduce false positives and improve accuracy

- Validate IOCs with rich network evidence to identify real threats
- Eliminate the noise from low-fidelity and open-source intelligence feeds
- Prioritize alerts based on validated, contextualized intelligence

Accelerate SOC efficiency

- Streamline operations with a unique combination of high-fidelity network evidence and high-quality threat intelligence
- Simplify security operations by reducing the complexity of managing multiple 3rd-party threat feeds
- Seamlessly integrate contextual alerts into existing SIEM, SOAR, and XDR solutions

THE SOLUTION IN ACTION

During its regular update with the sensor, Corelight Threat Intelligence adds a new malicious domain to its list of IOCs. Corelight Investigator (or the customer's SIEM) identifies an employee's laptop connected to this domain, based on Corelight's DNS logs.

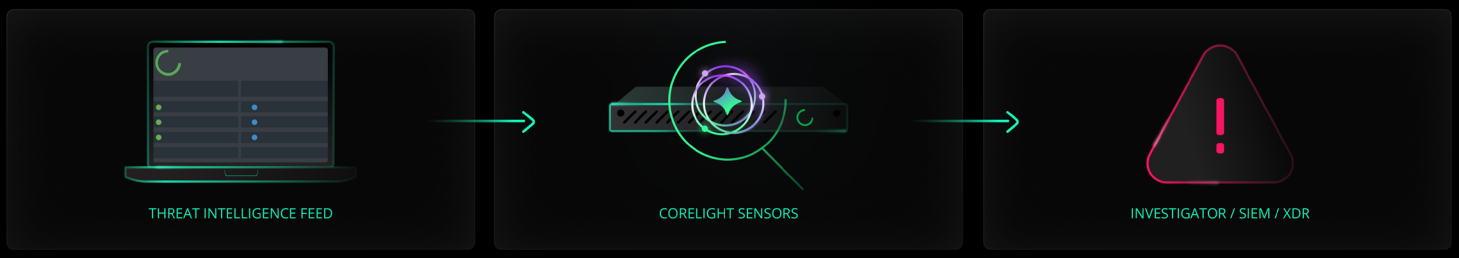
The analyst can then pivot quickly to other correlated Corelight logs to see additional endpoint details in Corelight Investigator or their SIEM to investigate further. Further inspection with the EDR system shows no corresponding malware alert—possibly because the user may have just clicked a link without downloading anything.

Nevertheless, Corelight's endpoint-enriched network data triggers an alert based on a rule associated with the newly published domain IOC that suggests they are using benign-looking links for initial reconnaissance on the target. The analyst can now hunt for other devices that have visited this domain and proactively block any connections, preventing a future attack. Evasive malware detected. Case closed.

HOW IT WORKS

1. **High-quality IOCs** trusted by over 30,000 organizations and enriched with detailed context, such as adversary attribution, related malware, targeting, and associated vulnerabilities are automatically updated in the Corelight platform every hour.
2. The **Corelight Sensor** searches for matches by correlating these IOCs against rich, real-time network evidence.
3. When a match is found, Corelight uses new tailored alerting logic to generate a **high-confidence, contextualized alert** that can be forwarded to Corelight Investigator, SIEMs, or EDR/XDR platforms for immediate investigation and response.

Prioritize alerts with validated, contextualized intelligence



1. Curated IOCs updated hourly

2. Match IOCs with real-time network evidence
3. Generate high-confidence contextual alerts

4. Accelerate investigations with high-fidelity prioritized alerts