corelight

INVESTIGATOR

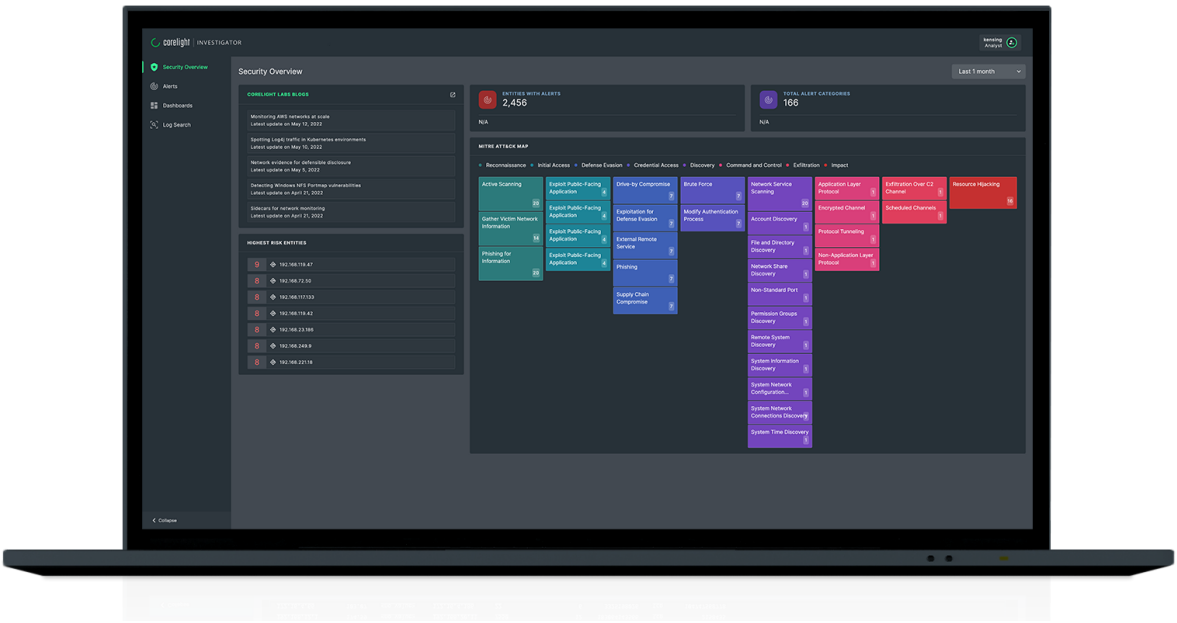
Open NDR with Next-Level Analytics

Accelerate incident response with intelligent alerts and correlated evidence fueled by machine learning and open source communities.

Solution overview

Investigator is a SaaS-based network detection and response (NDR) solution that combines comprehensive network evidence with machine learning (ML) and advanced analytics. It features a fast, intuitive search platform that improves SOC performance metrics and consolidates legacy toolsets.

Investigator is easy to implement, highly scalable, globally accessible 24/7, and is continuously updated with new ML-based threat detections created by Corelight Labs – providing users with immediate access to the latest analytical content.



The Investigator home screen highlights risky entities with alerts alongside security guidance from Corelight Labs, and threat detections mapped to MITRE ATT&CK®.

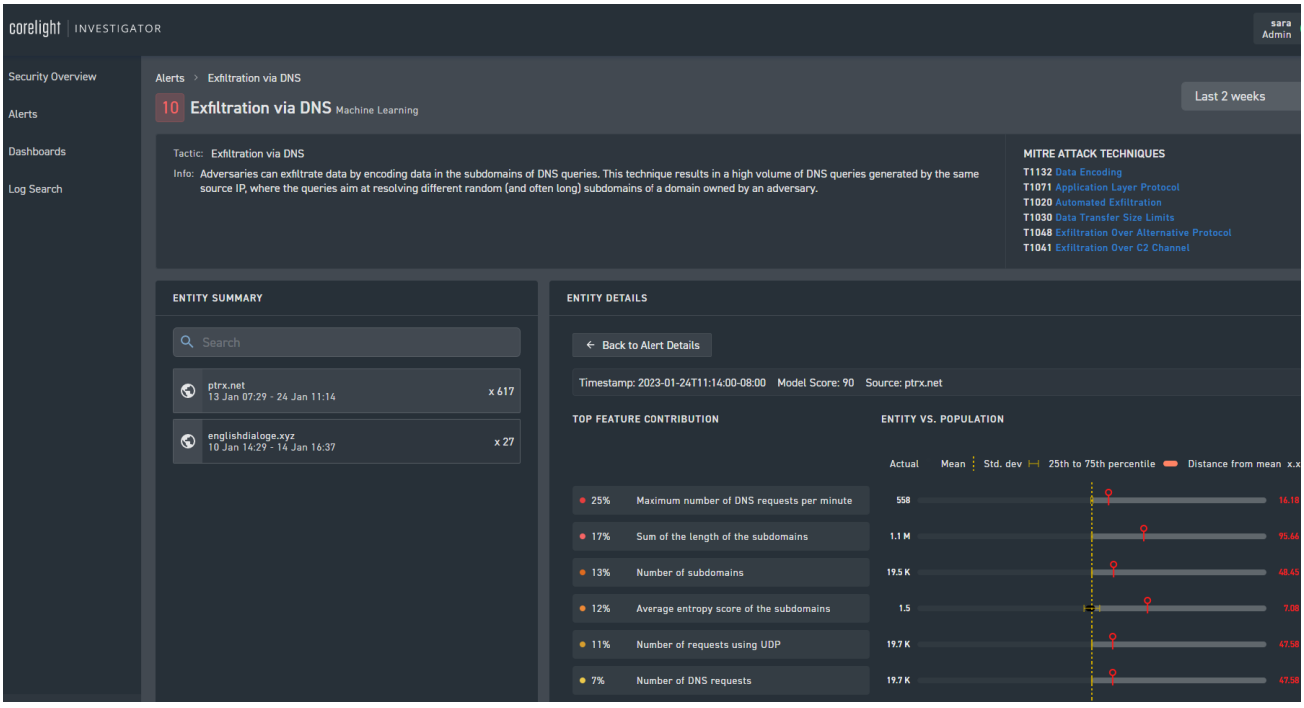
Solution benefits

Complete visibility: Investigator reveals a complete view of your network through evidence consisting of Zeek® logs, file metadata, and packets. Your team can pivot quickly through all traffic via unique connection IDs

Highlighted feature:	**Encrypted Traffic Collection:** Investigator displays hundreds of Corelight insights around encrypted traffic that give you visibility without decryption. Examples include the ability to identify large file transfers or human keystrokes over SSH connections.

Next-level analytics: Investigator delivers machine learning (supervised and deep learning,) behavioral analysis, threat intelligence, and signatures—mapped to the ATT&CK framework—to enable broad coverage of threats. Analysts are able to view alerts in Investigator and export them to SIEM and XDR solutions.

Highlighted feature:	**Machine learning threat detection:** Investigator applies a number of ML models in the cloud to detect threats (such as data exfiltration over DNS and typosquatting). Then the underlying logic of the ML detection becomes transparent to the analyst to facilitate validation.



An alert view shows machine learning detection of exfiltration via DNS, with a summary of the analytics and detail behind the ML detection.

Faster investigations: Investigator aggregates alerts and applies a score for rapid analyst prioritization. and also displays transparent ML-based alerts linked to the evidence needed to investigate the alerts for rapid validation and triage.

Highlighted feature:	**Intelligent alert scoring:** Investigator aggregates alerts across both entities and threat types with intelligent alert scoring, delivering a high fidelity queue of alerts that analysts can efficiently prioritize and validate with Corelight's network evidence.

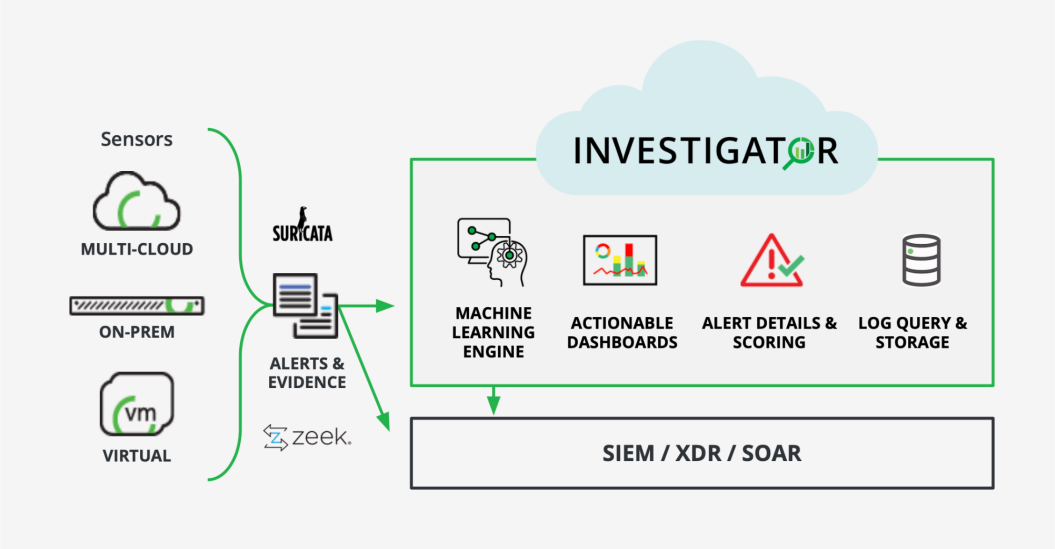
Expert hunting: Investigator supports fast, scalable threat-hunts by giving analysts a powerful query engine and unfettered access to all the evidence. Investigator also includes dashboards with built-in hunting queries and supports custom evidence enrichment (e.g., CMBD) for enriched hunting context.

Highlighted feature:	**Powerful query engine:** Search through all logs quickly, create and save custom searches, and view results in a variety of formats. Perform both live and historic hunting queries with rapid results.

How it works

Investigator extends the power of open-source-driven network evidence to SOC teams everywhere.

Because Investigator is a SaaS solution, customers can access their data from any web browser and ingest evidence from Corelight Sensors. Customers can deploy Corelight Sensors across their hybrid, multi-cloud, and distributed environments. The Sensors connect to traffic mirrors in physical networks via packet brokers, span ports, or optical taps and in cloud environments via native traffic mirroring (e.g., VPC traffic mirroring in AWS).



This implementation diagram shows how Corelight alerts and evidence flexibly stream from deployed sensors to Investigator, a SIEM/XDR/SOAR solution, or both. Investigator is also able to export to these solutions.

Why Corelight?

Organizations that use Investigator benefit from Corelight's open NDR platform, which confers a number of unique and valuable advantages compared to proprietary NDR platforms:

- **Evidence-driven security**—Corelight customers have open, unrestricted access to all the evidence behind every alert and to all evidence across their environment to maximize knowledge and their investigative capabilities and speed.

- **Community-powered analytics**—Corelight customers enjoy a force multiplication advantage by leveraging the power of continuous analytic engineering from open-source Suricata and Zeek communities, who develop everything from rapid zero-day detections to new protocol analyzers.

- **Flexibility & customization**—Corelight customers can easily modify the platform's capabilities, such as building custom detections and also integrate the platform with their favorite security tools thanks to the open, extensible nature of the underlying technologies used.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. Our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497