corelight

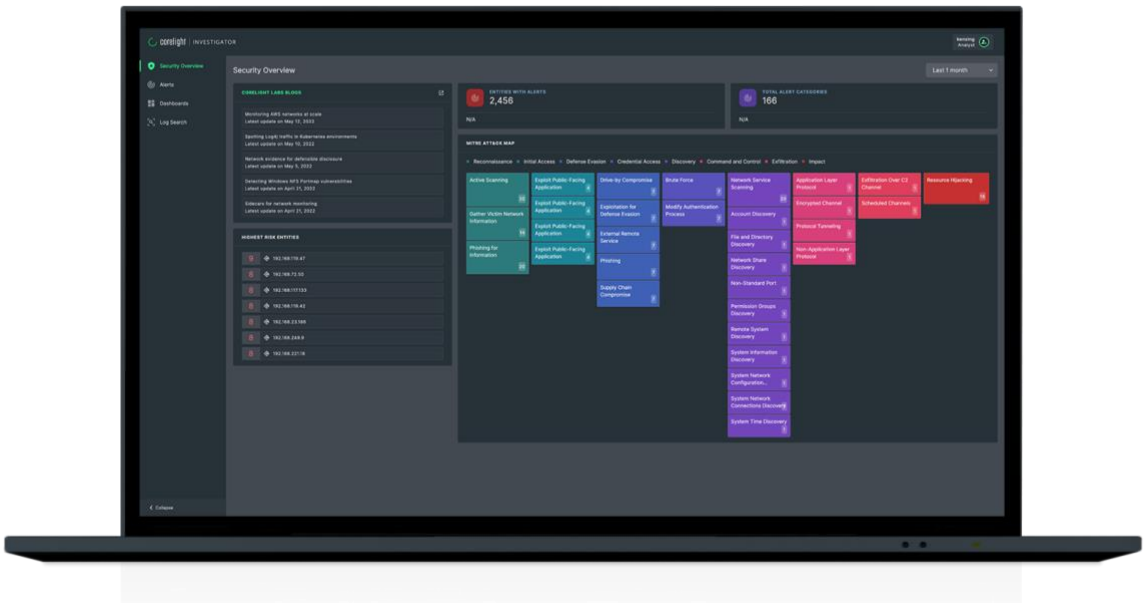
INVESTIGATOR

Open-Source-gestützte Netzwerk-Evidenz, integriert mit maschinellem Lernen und Verhaltensanalyse

Investigator vereinfacht und beschleunigt Untersuchungen von Bedrohungen mit intelligenten Alarmen, integrierten Abfragen und skalierbarer Suche.

Überblick über die Lösung

Investigator ist eine SaaS-basierte Network Detection und Response (NDR)-Lösung, die umfassende Netzwerkevidenz mit maschinellem Lernen (ML) und fortschrittlicher Analytik in einer schnellen, intuitiven Suchplattform kombiniert, die Sicherheitsabläufe beschleunigt und ältere Toolsets konsolidiert.



Der Investigator-Startbildschirm hebt risikobehaftete Entitäten mit Warnungen, Sicherheitsanweisungen von Corelight Labs und Bedrohungserkennungen hervor, die MITRE ATT&CK® zugeordnet sind.

Investigator ist einfach zu implementieren, hochgradig skalierbar und weltweit rund um die Uhr für Ihr Security Operations Center (SOC) verfügbar. Das Team von Corelight Labs entwickelt zudem kontinuierlich neue ML-basierte Bedrohungserkennungen und stellt diese automatisch in Investigator bereit, sodass Benutzer sofortigen Zugriff auf die neuesten Analyseinhalte haben.

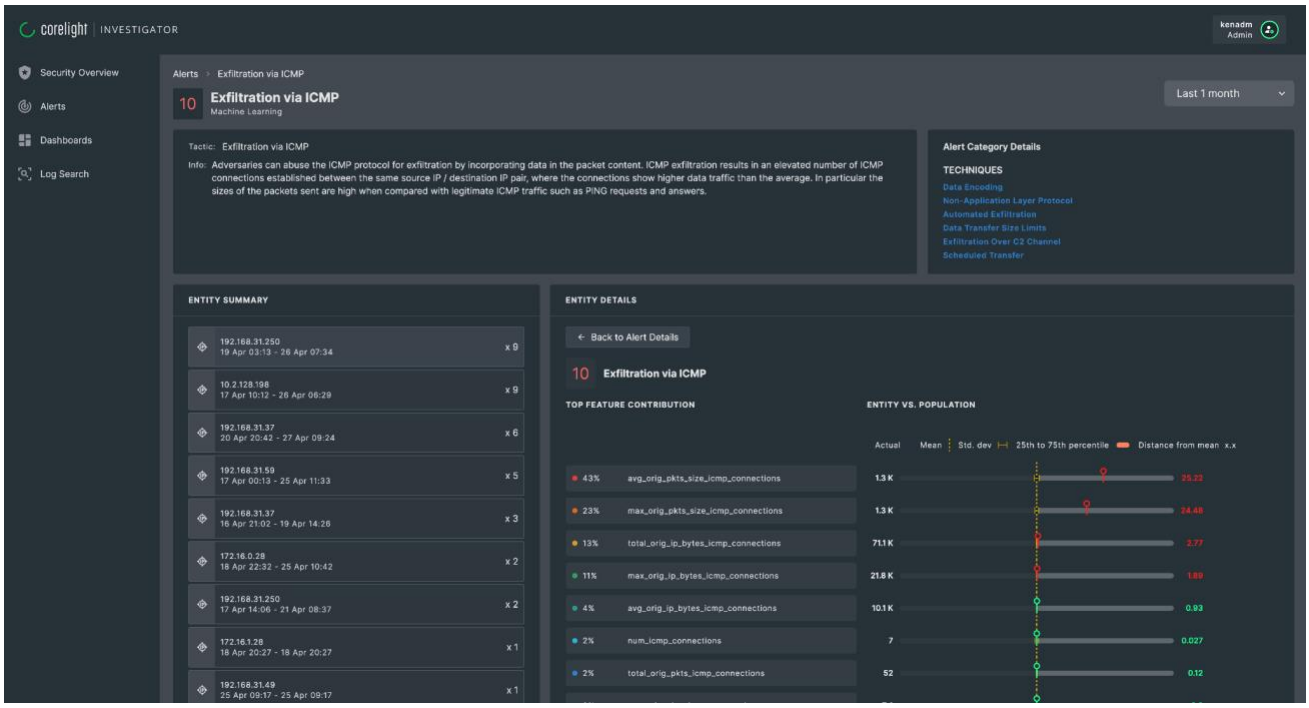
Ihre Vorteile

Vollständige Sichtbarkeit: Mithilfe der Zeek®-Protokolle, Datei-Metadaten und Pakete bietet Investigator vollständige Transparenz über Ihr Netzwerk. Er liefert Beweise für jede Verbindung – indiziert über eine eindeutige Verbindungs-ID – für schnelle Schwenks über einen Datensatz, der kompakt genug ist, um die Netzwerk-Historie für Monate oder sogar Jahre zu bewahren.

Hervorgehobene Funktion:	**Encrypted Traffic Collection:** Investigator liefert unzählige Einblicke in den verschlüsselten Datenverkehr, ohne den Datenverkehr zu entschlüsseln. So erzielen Sie Sichtbarkeit, ohne zu entschlüsseln. Dadurch wird es zum Beispiel möglich die Übertragung von großen Datenmengen oder Tastenanschläge in SSH-Verbindungen zu identifizieren.

Die nächste Ebene von Analytics: Investigator bietet maschinelles Lernen, Verhaltensanalysen, Threat Intelligence und Signaturen, die auf das MITRE ATT&CK-Framework gemapped werden, um eine breite Abdeckung von Bedrohungen zu ermöglichen. Analysten können in Investigator Alarme ansehen und untersuchen oder diese an ein SIEM- oder XDR-System weiterleiten, um diese mit zusätzlichem Kontext anzureichern.

Hervorgehobene Funktion:	**Erkennung von Bedrohungen mit Machine Learning:** Investigator wendet eine Reihe von ML-Modellen in der Cloud an, um Bedrohungen zu erkennen (z. B. die Datenexfiltration über DNS). Anschließend wird die zugrunde liegende Logik der ML-Erkennung für den Analysten transparent, um die Validierung zu erleichtern.



Ein Alarm zeigt die Erkennung von Datenexfiltration über ICMP durch maschinelles Lernen mit einer Zusammenfassung der Analyse und der Details hinter der ML-Erkennung.

Schnellere Untersuchungen: Investigator aggregiert und bewertet Alarme für eine schnelle Priorisierung durch den Analysten und zeigt außerdem transparente ML-basierte Alarme an. Diese sind mit den zugrundeliegenden Beweisen verknüpft, welche eine schnelle Validierung und Untersuchung ermöglichen.

Hervorgehobene Funktion:	**Intelligente Auswertung von Alarmen:** Investigator aggregiert Alarme über die beiden Entitäten (IP-Adresse und Domain) und über die Bedrohungstypen, hat ein intelligentes Alarm Scoring und liefert eine Liste von Alarmen, die Analysten effizient priorisieren und mit Corelight's Netzwerkbeweisen validieren können.

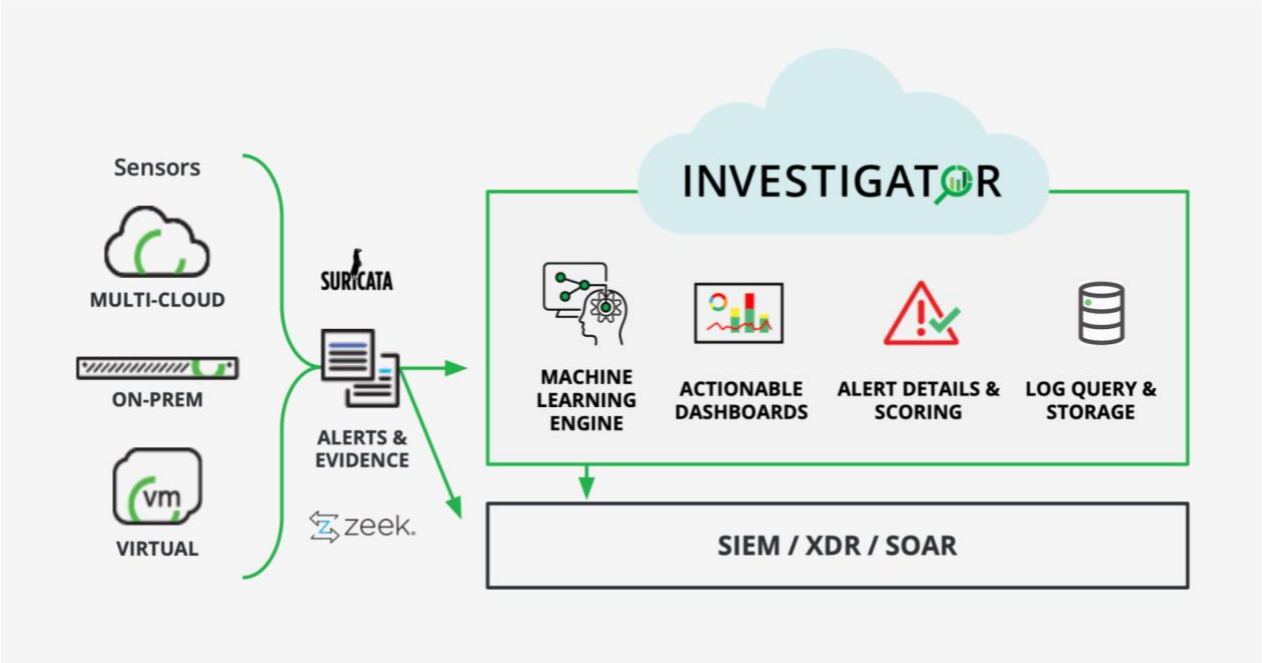
Professionelles Hunting: Investigator unterstützt schnelles, skalierbares Threat Hunting, indem es den Analysten eine leistungsstarke Abfrage Engine und uneingeschränkten Zugriff auf alle Beweise bietet. Investigator enthält außerdem Dashboards mit integrierten Abfragen und unterstützt benutzerdefinierte Anreichung der Beweise (z. B. CMBD) für mehr Kontext bei den Suchen.

Hervorgehobene Funktion:	**Leistungsstarke Suchmaschine:** Durchsuchen Sie schnell alle Protokolle, erstellen und speichern Sie benutzerdefinierte Suchen und zeigen Sie die Ergebnisse in verschiedenen Formaten an. Führen Sie sowohl Live- als auch historische Suchabfragen mit schnellen Ergebnissen durch.

So arbeitet Investigator

Investigator erweitert überall die Möglichkeiten der Open-Source-gestützten Netzwerkevidenz für SOC-Teams.

Da Investigator eine SaaS-Lösung ist, können Kunden von jedem beliebigen Webbrowser aus auf ihre Daten zugreifen und Beweise von Corelight-Sensoren einlesen. Kunden können Corelight-Sensoren sowohl in On-Premise- als auch in Cloud-Umgebungen (AWS, GCP, Azure) einsetzen. Die Sensoren erhalten den gespiegelten Traffic in physischen Netzwerken über Packet Broker, Span-Ports oder optische Taps. In Cloud-Umgebungen geschieht dies über natives Traffic-Mirroring (z. B. VPC-Traffic-Spiegelung in AWS).



Dieses Diagramm zeigt, wie Corelight Alarme und Beweise flexibel von den eingesetzten Sensoren zu Investigator oder einem SIEM (oder beidem) gesendet werden können.

Warum Corelight?

Unternehmen, die Investigator nutzen, profitieren von der offenen NDR-Plattform von Corelight, die im Vergleich zu proprietären NDR-Plattformen eine Reihe einzigartiger und wertvoller Vorteile bietet:

- **Evidenzbasierte Sicherheit:** Corelight-Kunden haben offenen, uneingeschränkten Zugang zu allen Beweisen, die hinter jedem Alarm stehen, und zu allen Beweisen in ihrer gesamten Umgebung, um ihr Wissen, ihre Ermittlungsmöglichkeiten und ihre Geschwindigkeit zu maximieren.

- **Community-gestützte Analysen:** Corelight-Kunden haben einen Multiplikationsfaktor, da sie von den kontinuierlichen Entwicklungen der Open-Source Suricata und Zeek Communities profitieren, die alles entwickeln von Zero-Day Erkennungen bis hin zu Protokoll Analyzer.

- **Flexibilität und Anpassung:** Kunden von Corelight können die Funktionen der Plattform leicht ändern, z. B. benutzerdefinierte Erkennungen erstellen und auch dank der offenen, erweiterbaren Architektur andere Security Tools integrieren.

corelight

Corelight versorgt Sicherheitsteams mit Netzwerk-Beweisen zur Sicherheit und Schutz kritischer Unternehmen und sonstiger Organisationen weltweit. Sei es in den Vor-Ort-Infrastrukturen oder in der Cloud: Unsere offene Network Detection und Response-Plattform verbessert die Sichtbarkeit und die Analysen und ermöglicht schnellere Nachforschungen sowie eine erweiterte Bedrohungssuche. Zu den weltweiten Corelight-Kunden zählen Fortune-500-Unternehmen, bedeutende Regierungsstellen und große, in der Forschung tätige Universitäten. Corelight mit Sitz in San Francisco ist ein Open-Core-Sicherheitsunternehmen und wurde von den Gründern der weitverbreiteten Netzwerk-Sicherheitstechnologie Zeek® entwickelt.

info@corelight.com | +1 888 547 9497