

ANGRIFFE UNTERBRECHEN MIT

A large, abstract graphic representing network data. It consists of numerous thin, white, wavy lines that flow horizontally across the frame, interspersed with small, bright white dots, creating a sense of dynamic movement and digital connectivity. The text 'NETWORK EVIDENCE' is superimposed in the center of this graphic.

NETWORK EVIDENCE

NETWORK DETECTION UND RESPONSE ON PREMISE UND IN DER CLOUD

Open NDR

Für mehr Transparenz in Ihren Netzwerkdaten !

About Corelight

- Open Network
- Ergänzt durch
- Firmengründer
- Einsatz bei me
- 35 Regierungen
- Investoren sind
- Headquartered



Our origins:

1995 – Unser Co-Founder Vern Paxson entwickelt Open Source Zeek (Bro).

2013 - Vern & führende Zeek Projekt Entwickler gründen Broala um kommerzielle Projekte zu unterstützen

2017 - Aus Broala wird Corelight, sammeln VC Fundings ein & bringt ersten kommerziellen Sensor auf den Markt

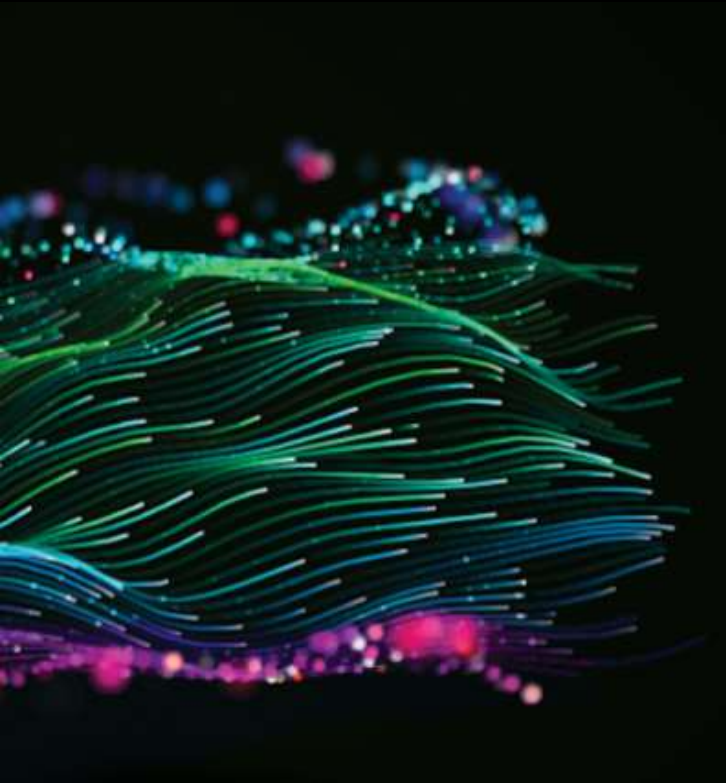
Open-Source-Communities

Projekts Zeek

0 F500-Unternehmen und mehr als

up, General Catalyst, HIG, und Insight

Die Macht der Netzwerkevidenz



- Angreifer können das Netzwerk nicht umgehen
- Das Netz kann nicht lügen
- Beweise schaffen Wissen
- Wissen ist die Grundlage für disruptive Verteidigung (Umgebung verstehen)

NETWERK EVIDENCE IN AKTION

Initiale Detektion **jeder Hersteller scheiterte**



Applikations Level vuln anfänglich übersehen von EDR, IPS/IDS, etc.



Malware verbarg sich vor EDR, IPS/IDS, etc.

DISCOVERY

Alibaba / Apache Foundation findet Sicherheitslücke und nennt Netzwerk als wichtigste Empfehlung für die Entdeckung

"Die Angreifer hatten es schwer, sich vor den Untersuchungen der Mitarbeiter von @corelight_inc zu verstecken."- Scott Runnels, Mandiant



DETECTION

Detections verfügbar innerhalb von 48 Stunden

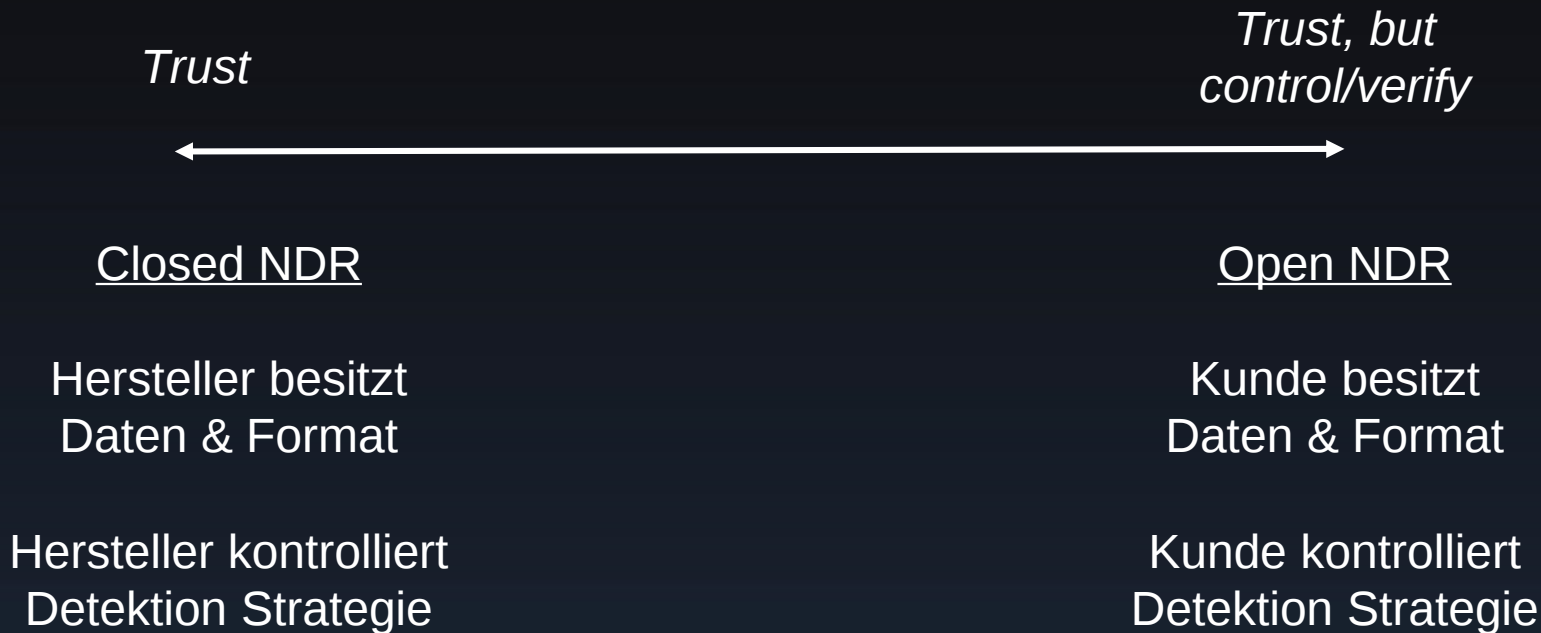
Detections verfügbar innerhalb von 48 Stunden

INVESTIGATION

"Was geworden, wo es doch so viele Exploits Pfade gibt?"

Wann war ich zum ersten Mal betroffen und was ist dann passiert?

CLOSED NDR versus OPEN NDR



Warum OPEN NDR?



Alarme & Einblicke

Suricata |

- Alarme
- C2, Lateral movement
- Verschlüsselte Traffic Analyse
- Brute Force Authentifizierung



INVESTIGATION

Zeek® |

- Standard für Netzwerk Evidence
- Verbunden über eine UID
- DNS, HTTP, SSL, etc.
- Proprietär: VPN, SSH, RDP, etc.
- ICS/IoT: S7, BACNet, MS-TDS, etc



VALIDATION

Smart PCAP |

- Selektive Paketerfassung
- Protokoll basierte Trigger
- SIEM 1-Click Abruf

Evidence ist eine *Strategie*

Alarm-First Strategie



Evidence Strategie



Erfassen Sie einige Bedrohungen über Alarme

Sammeln Sie nur Beweise für aktuelle Alarme

Reagieren Sie auf Alarme

Erfassen Sie alle Bedrohungen durch Beweise

Sammeln Sie alle Beweise für zukünftige Analysen und IR

Threat Hunting und erstellen eigener Detektionen

OPEN NDR DESIGN PATTERN, PIONEERED BY ELITE DEFENDERS

KOMBINATION VON NETZNACHWEISEN & ANALYSEN ZUR MAXIMIERUNG DER EINBLICKE

TRAFFIC SOURCE

CLOUD & NETWORK



VISIBILITY
STACK

IDS

Intrusion Detetion

Suricata, für Signatures Alarme und Detektionen

NSM

Network Security
Monitoring

Zeek, der Industrie Standard für Einblicke und Untersuchungen

PCAP

Packet capture

PCAP, für erweiterte Forensik



ANALYSIS TIER

SIEM

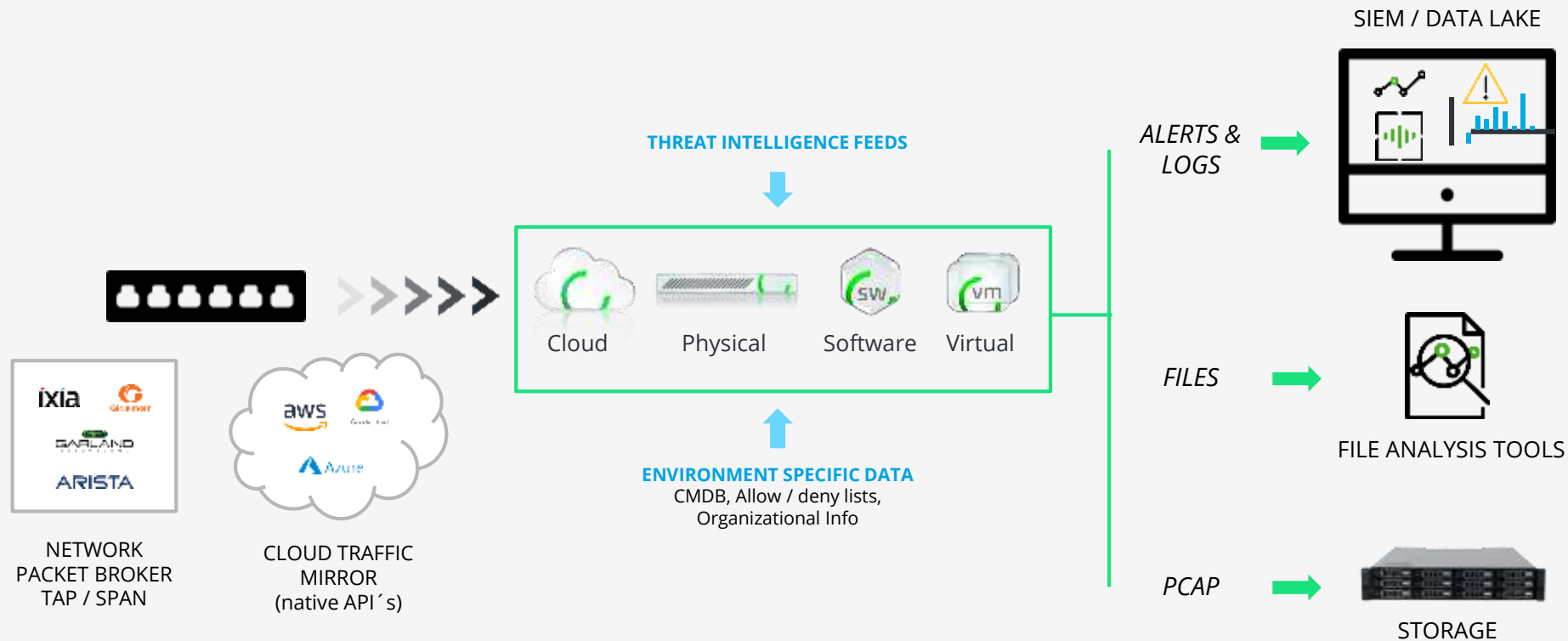


DATA LAKE



Typischer Einsatz nutzt Ihr bestehendes Ökosystem

On-Prem und SaaS Bereitstellung



Produktübersicht der NDR-Plattform von Corelight

 Cloud	 Virtual	 Software	 AP 200	 AP 1100	 AP 3100	 AP 5002
Up to 8 Gbps AWS, Azure, GCP Support Suricata Supports Collections	Up to 8 Gbps / instance VMware or Hyper-V Support Suricata Supports Collections	500 Mbps - 8 Gbps Container / OS Native Support Suricata Supports Collections	Up to 2 Gbps 1U half-depth Support Suricata Supports Collections	Up to 20 Gbps 1U rack-mounted Support Suricata Supports Collections	Up to 35 Gbps 1U rack-mounted Support Suricata Supports Collections Supports Smart PCAP	Up to 100 Gbps 1U rack-mounted Support Suricata Supports Collections Supports Smart PCAP



Fleet Manager | VM, Manage up to 250 Sensors

NETWORK DETECTION AND RESPONSE

INVESTIGATOR

The only evidence-first threat investigation platform



SOC PAIN POINTS



GERINGE SICHTBARKEIT

Blind Spots und das Fehlen vollständiger, detaillierter Informationen über den Netzverkehr



UNVOLLSTÄNDIGE ANALYTIK

Fehlender Kontext und schwer mit anderen Informationen zu korrelieren



ZU VIELE INVESTIGATIONS

Zu viele Warnmeldungen, die sich nur schwer nach Prioritäten ordnen lassen



Kein **THREAT HUNTING**

Mangel an speziellen Ressourcen für die proaktive Suche und Entwicklung disruptiver Strategien

Die perfekte SOC Unterstützung um das Unternehmen zu schützen

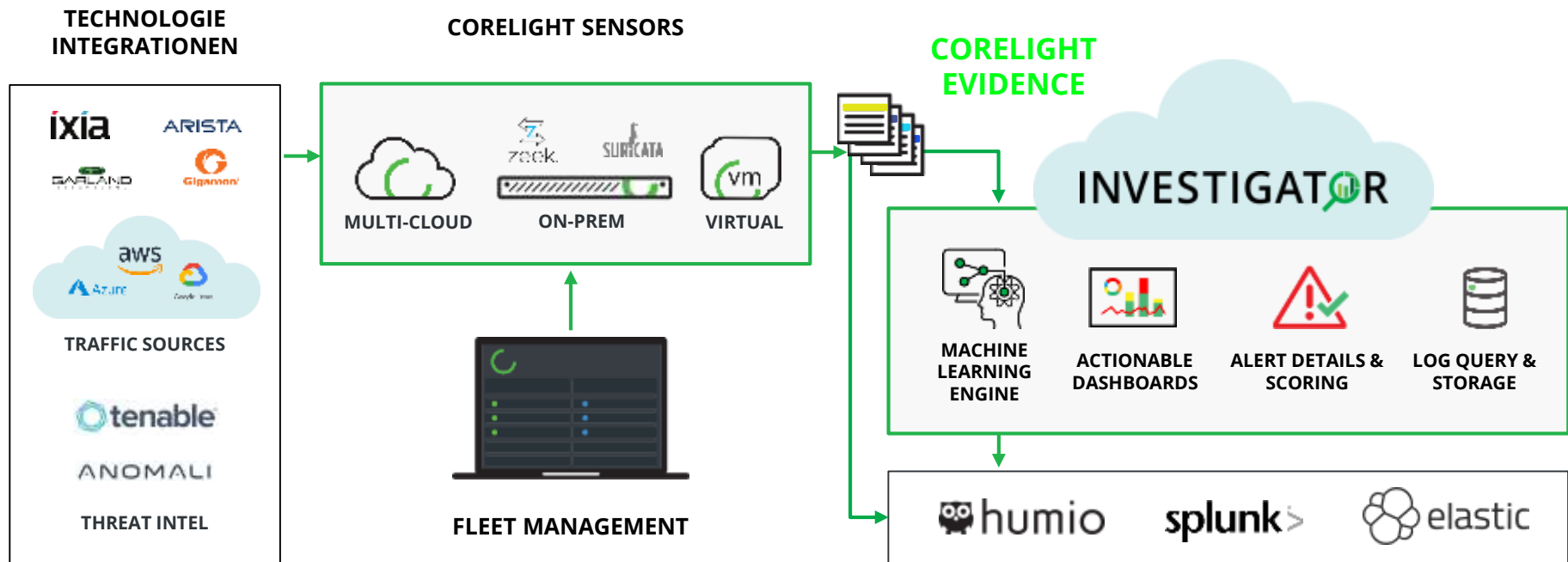
Open-Source-gestützte
Netzwerkevidenz integriert
mit maschinellem Lernen
& Verhaltensanalyse

Vereinfacht und
beschleunigt die Suche
und Untersuchung von
Bedrohungen durch
intelligente
Alarmaggregation,
integrierte Abfragen und
skalierbare Suche

Die SaaS-Bereitstellung ist
einfach zu
implementieren, zu
nutzen und zu skalieren



INVESTIGATOR | SaaS-basierte OPEN NDR Lösung



Corelight transforms raw traffic into *actionable* security stories

The diagram illustrates the relationship between various log files and their contents. The logs are arranged in a grid, with lines connecting related entries across different logs. The logs include:

- httpd.log** (HTTP request details): Contains information about HTTP requests, including the client IP, the requested URL, the status code, and the response size. It also includes information about the user agent and the referrer.
- dns.log** (DNS query/response details): Contains information about DNS queries and responses, including the query type, the query name, and the response data.
- conn.log** (TCP, UDP, ICMP connection details): Contains information about network connections, including the source and destination IP addresses, the source and destination ports, and the protocol used.
- files.log** (File analysis results): Contains information about files that have been analyzed, including the file name, the file size, and the file type.
- smtp.log** (SMTP transactions): Contains information about SMTP transactions, including the sender and recipient email addresses, the subject line, and the message body.

Lines connect related entries across different logs, showing how information is shared and processed. For example, a request in httpd.log might be linked to a DNS query in dns.log, which is then linked to a connection in conn.log, and finally to a file analysis in files.log. Similarly, an SMTP transaction in smtp.log might be linked to a connection in conn.log and a file analysis in files.log.

ts	Timestamps with microsecond accuracy, synchronized across logs
uid	Unique ID for every connection
md5/sha1	File hash of every file
fuid	Unique ID for every instance of every file seen on the network

Detect command & control activity with Corelight

Corelight C2 Collection delivers over 50 unique detection capabilities



HTTP C2 Detection

Detects 15 common families of malware over HTTP



DGA Detections

Detects known Domain generation algorithms use for c2 communications



Meterpreter

Specific detections for Metasploit's command line interface



DNS TUNNELING

Detections cover both specific (known tunneling tools) and broad (tunneling behaviors)



ICMP TUNNELING

Detections cover both specific (known tunneling tools) and broad (tunneling behaviors)

Augmented by cutting-edge encrypted traffic analytics

Corelight Encrypted Traffic Collection



TLS fingerprinting

SSL fingerprinting (JA3)
SSH fingerprinting (HASSH)



Certificate monitoring

SSL certificate monitoring
Custom encryption detection



SSH, RDP, SSL, VPN analytics

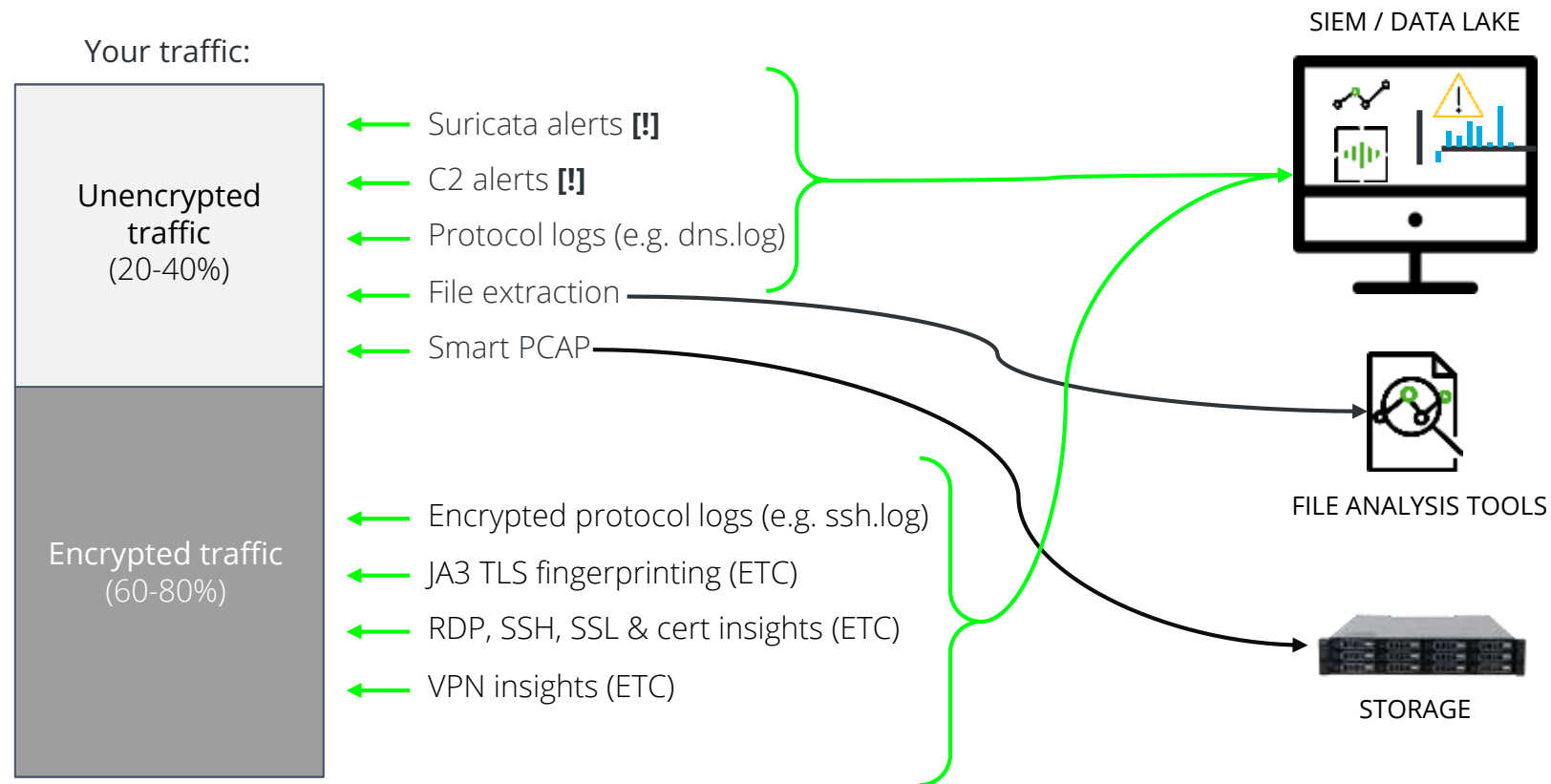
SSH client brute force detection
SSH authentication bypass detection
SSH client keystroke detection
SSH client file activity detection
SSH scan detection
SSH MFA detection
SSH agent forwarding detection
SSH reverse tunnel detection
Non-interactive SSH detection

Expected encryption detection
DNS over HTTPs (DoH) detection

RDP known client detections
RDP authentication insights
RDP password guessing insights
And 10+ additional RDP insights..

Identify 350+ VPN protocols and providers

Corelight comprehensively analyzes your traffic



Fragen?