corelight

Corelight Unternehmens Überblick

ANGRIFFE UNTERBRECHEN MIT

NETWORK DETECTION UND RESPONSE ON PREMISE **UND IN DER CLOUD**

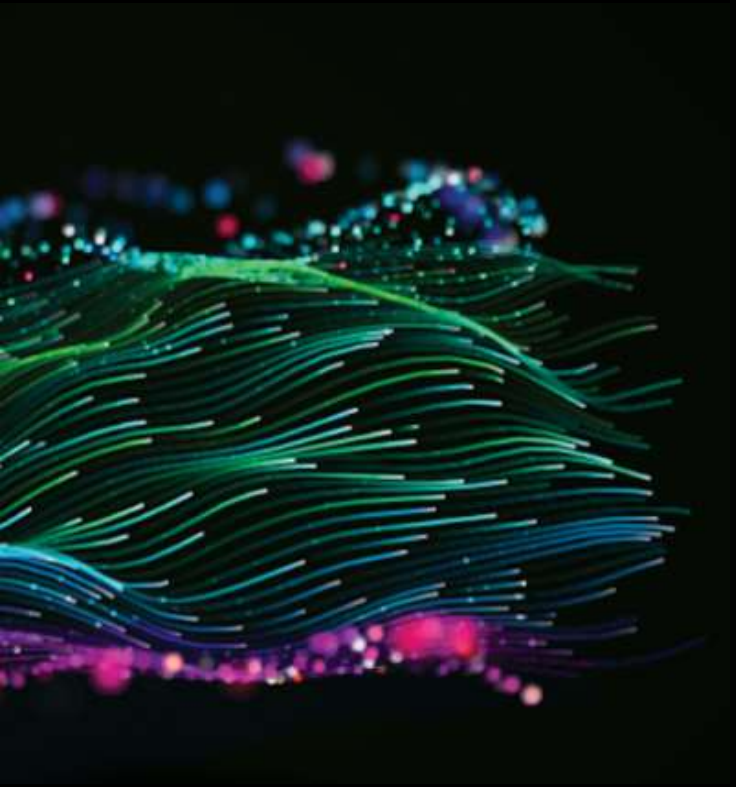
corelight

Open NDR
Für mehr Transparenz in Ihren Netzwerkdaten !

About Corelight

- Open Network
- Ergänzt durch Open-Source-Communities
- Firmengründer Projekts Zeek
- Einsatz bei me 0 F500-Unternehmen und mehr als 35 Regierunge
- Investoren sin up, General Catalyst, HIG, und Insight
- Headquartere

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?

corelight

CLOSED NDR versus OPEN NDR

Trust

Trust, but control/verify

Closed NDR	Open NDR
Hersteller besitzt Daten & Format	Kunde besitzt Daten & Format
Hersteller kontrolliert Detektion Strategie	Kunde kontrolliert Detektion Strategie

corelight

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.
- Properitär: VPN, SSH, RDP, etc.
- ICS/IoT: S7, BACNet, MS-TDS, etc

VALIDATION

Smart PCAP |

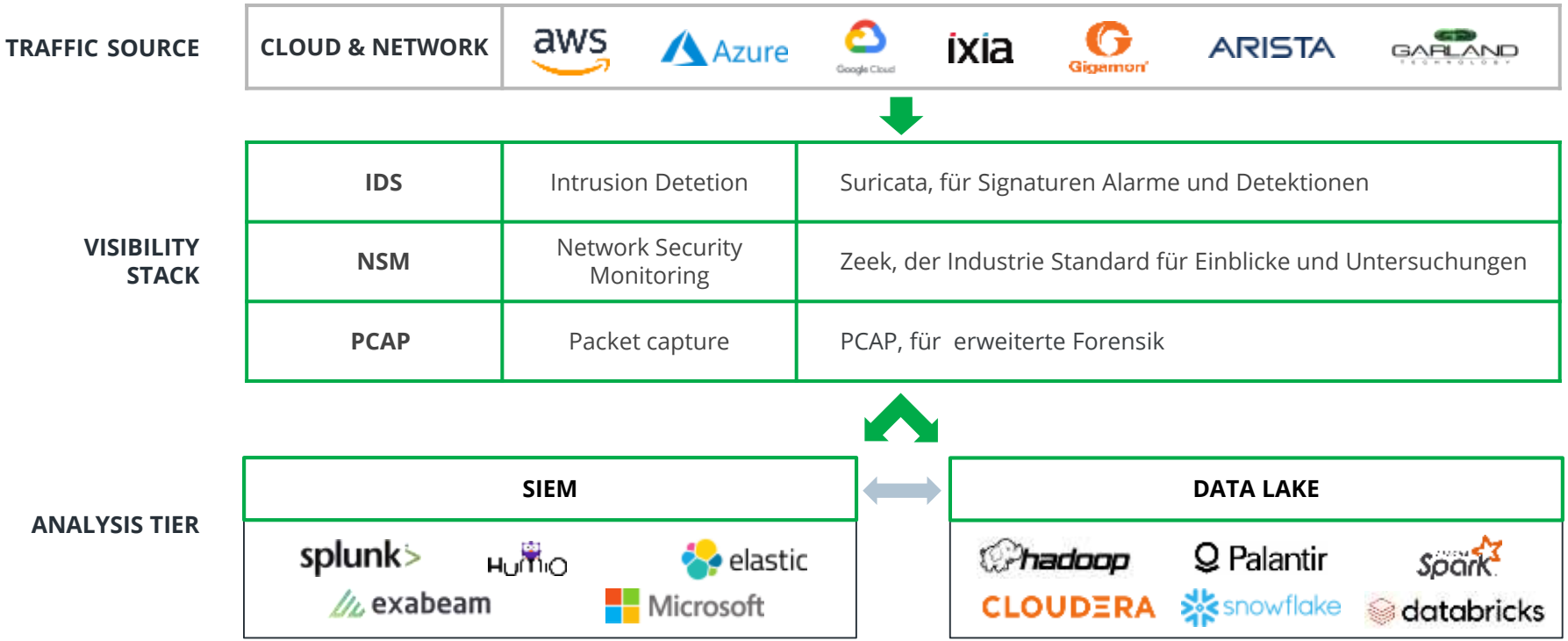
- Selektive Paketerfassung
- Protokoll basierte Trigger
- SIEM 1-Click Abruf

Evidence ist eine *Strategie*

Alarm-First Strategie	Evidence Strategie
	
Erfassen Sie einige Bedrohungen über Alarme	Erfassen Sie alle Bedrohungen durch Beweise
Sammeln Sie nur Beweise für aktuelle Alarme	Sammeln Sie alle Beweise für zukünftige Analysen und IR
Reagieren Sie auf Alarme	Threat Hunting und erstellen eigener Detektionen

OPEN NDR DESIGN PATTERN, PIONEERED BY ELITE DEFENDERS

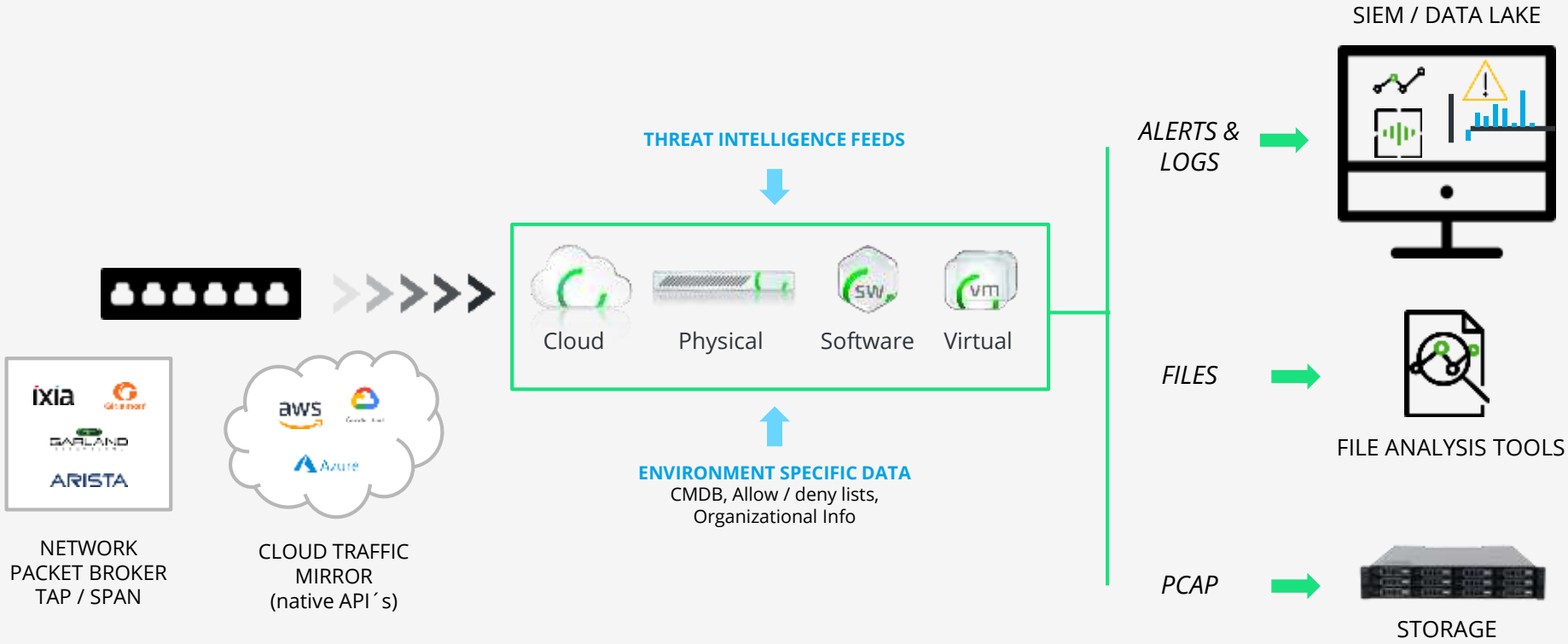
KOMBINATION VON NETZNACHWEISEN & ANALYSEN ZUR MAXIMIERUNG DER EINBLICKE



corelight

Typischer Einsatz nutzt Ihr bestehendes Ökosystem

On-Prem und SaaS Bereitstellung



corelight

Produktübersicht der NDR-Plattform von Corelight

Cloud

Up to 8 Gbps
AWS, Azure, GCP
Support Suricata
Supports Collections

Virtual

Up to 8 Gbps / instance
VMware or Hyper-V
Support Suricata
Supports Collections

Software

500 Mbps - 8 Gbps
Container / OS Native
Support Suricata
Supports Collections

AP 200

Up to 2 Gbps
1U half-depth
Support Suricata
Supports Collections

AP 1100

Up to 20 Gbps
1U rack-mounted
Support Suricata
Supports Collections

AP 3100

Up to 35 Gbps
1U rack-mounted
Support Suricata
Supports Collections
Supports Smart PCAP

AP 5002

Up to 100 Gbps
1U rack-mounted
Support Suricata
Supports Collections
Supports Smart PCAP

Fleet Manager | VM, Manage up to 250 Sensors

corelight

corelight

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

INVESTIGATOR

Die perfekte SOC Unterstützung um das Unternehmen zu schützen

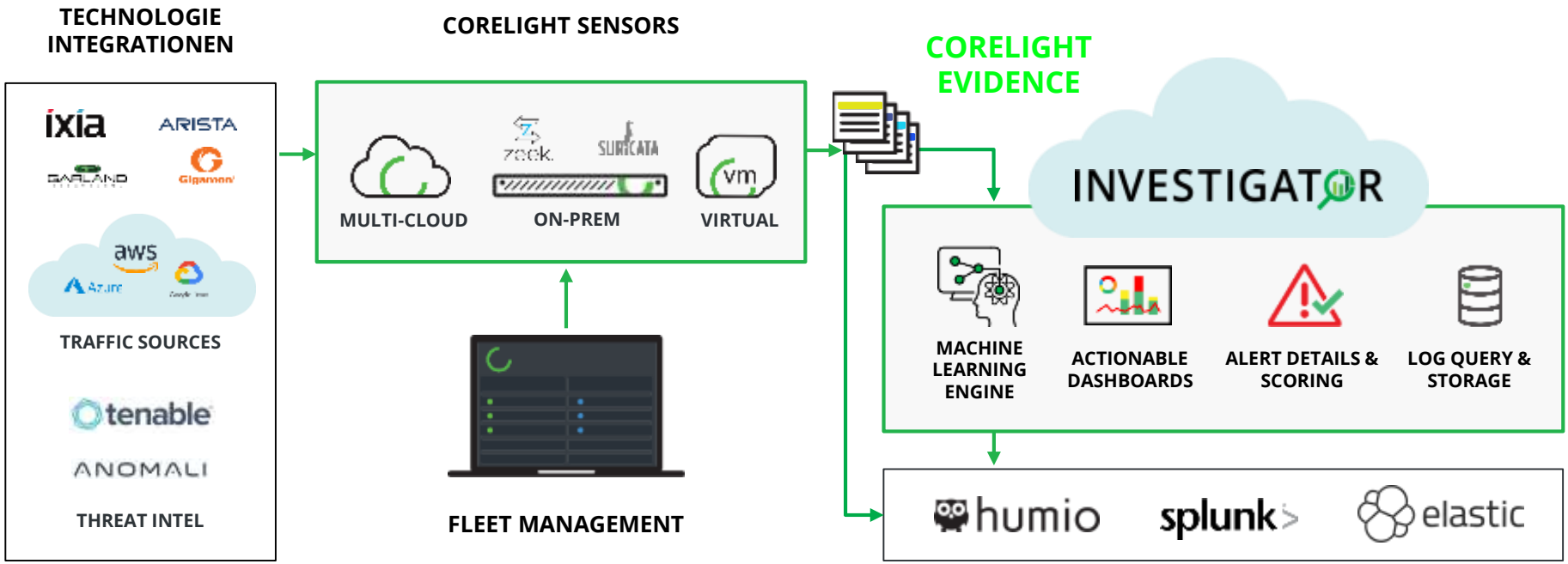
Open-Source-gestützte Netzwerkevidenz integriert mit maschinellem Lernen & Verhaltensanalyse

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

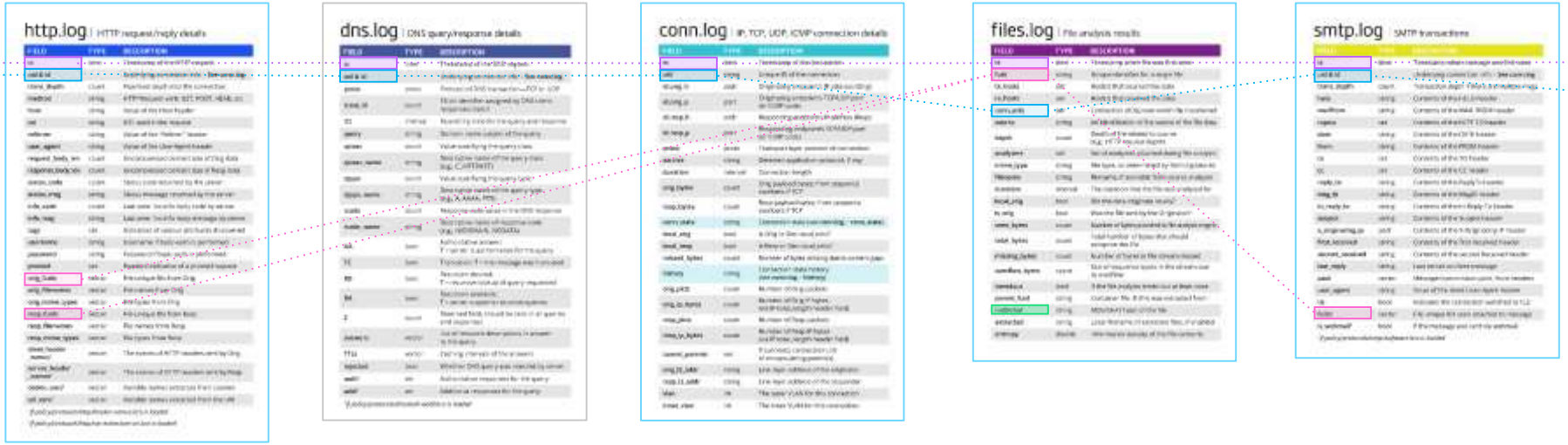
Die SaaS-Bereitstellung ist einfach zu implementieren, zu nutzen und zu skalieren

corelight

INVESTIGATOR | **SaaS-basierte OPEN NDR Lösung**



Corelight transforms raw traffic into *actionable* security stories



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

corelight

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

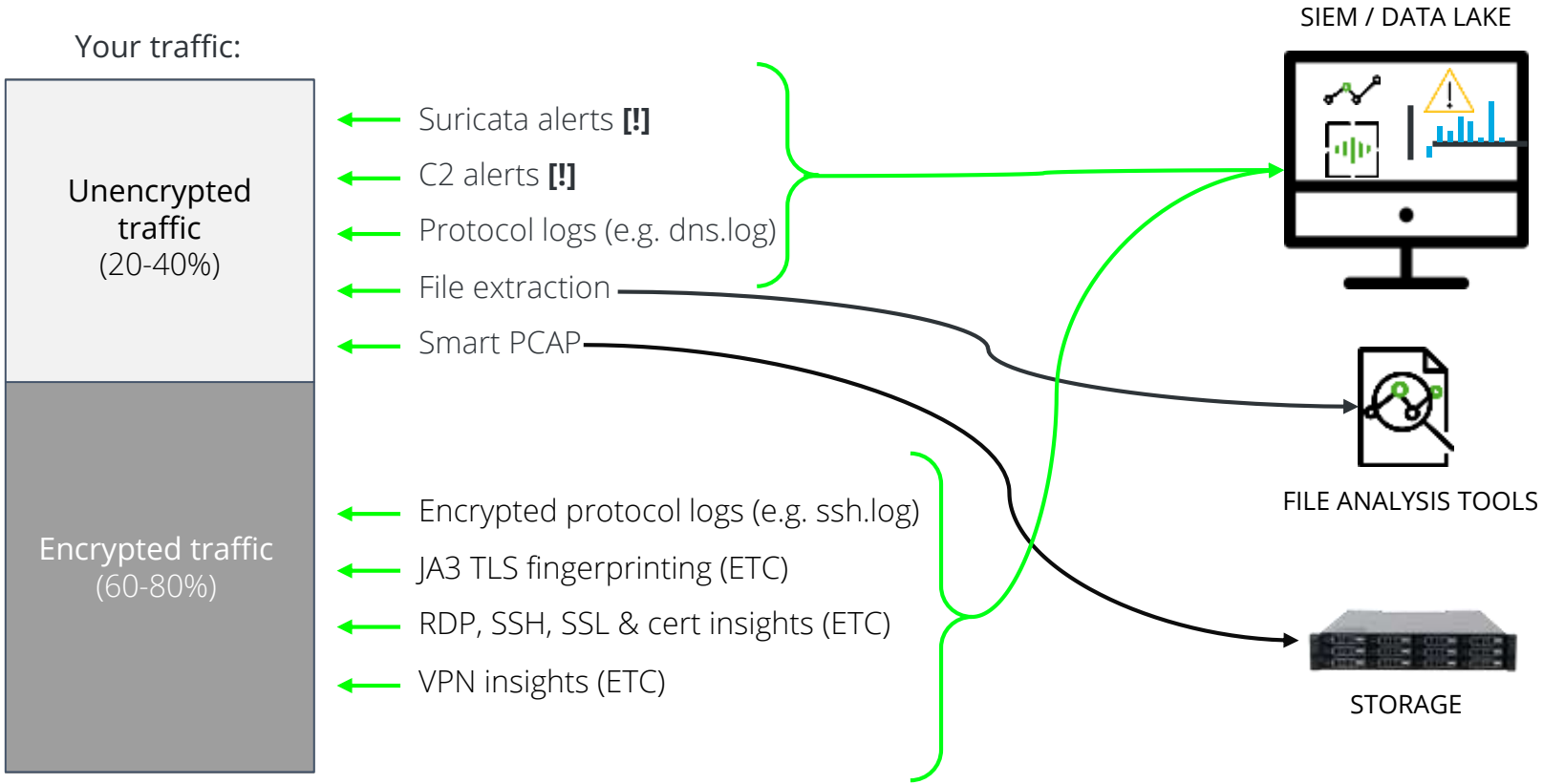
SSH client brute force detection
SSH authentication bypass detection
SSH client keystroke detection
SSH client file activity detection
SSH scan detection
SSH MFA detection
SSH agent forwarding detection
SSH reverse tunnel detection
Non-interactive SSH detection

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



corelight

Fragen?