corelight

The world's best network evidence

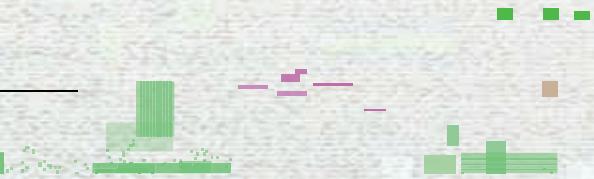
HOW DO YOU KNOW?

Are adversaries hiding in your encrypted traffic?

How did that **attack start** a year ago?

Do you have the **evidence to validate your alerts?**

HOW DO YOU **KNOW?**



EVIDENCE FOR SECURITY'S TOUGHEST QUESTIONS

Defenders at critical government, financial, and infrastructure organizations capture everything on their networks in extraordinary detail. This evidence is highly structured, interlinked, and spans years so they can understand their networks and spot anomalies—not just specific attacks. Corelight gives you the exact same network evidence, except it's simple enough for anyone to use, and it's deeply integrated with detections.

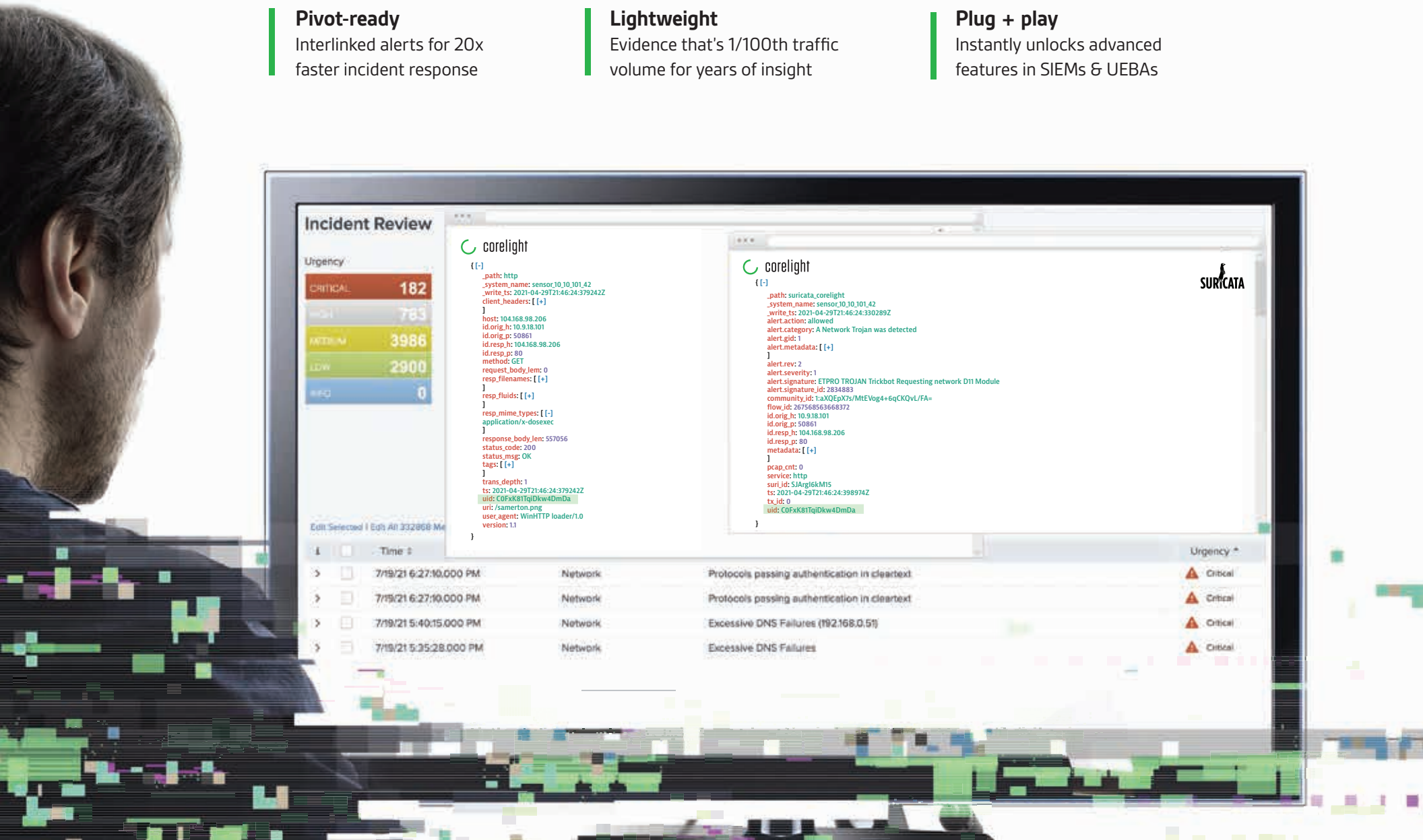
CORELIGHT GIVES YOUR TEAM THE ANSWERS

The world's best network evidence and insights are comprehensive and security-specific.

Pivot-ready
Interlinked alerts for 20x faster incident response

Lightweight
Evidence that's 1/100th traffic volume for years of insight

Plug + play
Instantly unlocks advanced features in SIEMs & UEBAs



THE OPEN NDR PLATFORM

Corelight's Open Network Detection and Response platform delivers integrated alerts and evidence—logs, files, and PCAP. Because it's built on open, universal standards, the platform makes integration easier with the data and technology you already use. There are no black boxes here—if you want to see how a detection works, you're welcome to examine the code.

Suricata | Fast, custom alerts tied to evidence

Suricata generates alerts that we embed directly into Zeek logs, putting every detection into context to save time, cut alert backlogs, and improve analytics.

Zeek® | The global standard for network evidence

The Zeek open source network security monitor generates lightweight metadata and detections to enable threat hunting and speed incident response.

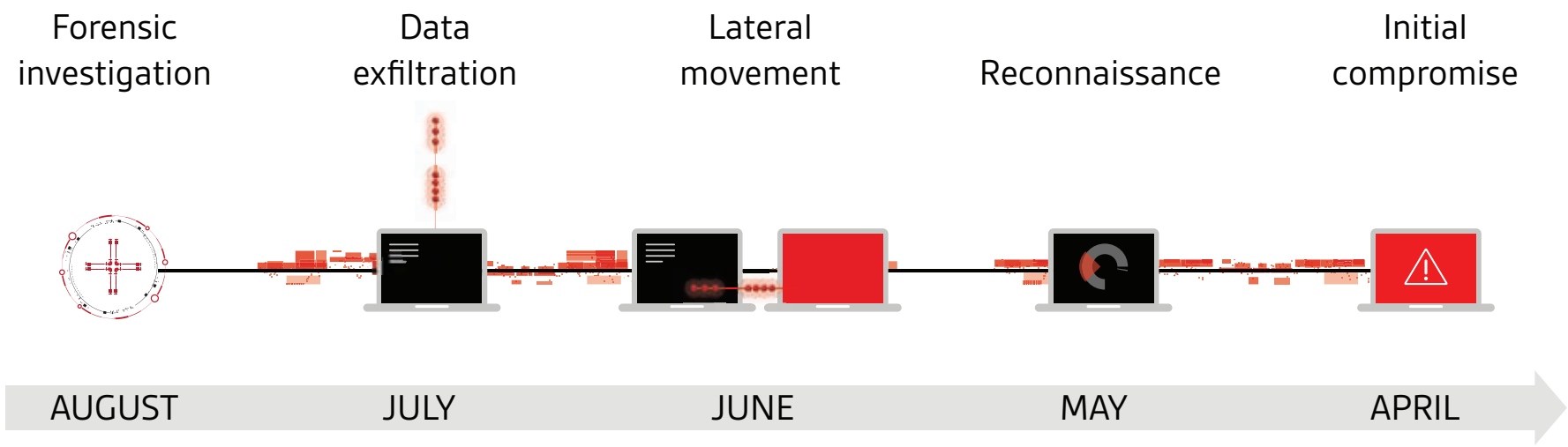
Smart PCAP | Super efficient, highly-flexible packet capture

Smart PCAP links logs, extracted files, and insights with just the packets you need, to reduce storage costs while expanding retention times by a factor of 10.

LONG-TERM BREACHES

HOW DO YOU UNCOVER ATTACKS THAT STARTED MONTHS AGO?

When a vulnerability like PrintNightmare (CVE-2021-34527) drops, your first step after patching it is to analyze last week's traffic for IOCs. If your only data is what's captured via traditional methods, you'll find nothing and move on. With Corelight's lightweight yet comprehensive evidence, you can go back months or even years to find traces of exploitation—and the data that was exfiltrated afterwards—that none of your other systems saw. That same evidence can be stored and used to train your analytics, AI/ML, and other tools to find the next attack.



CONTAINMENT

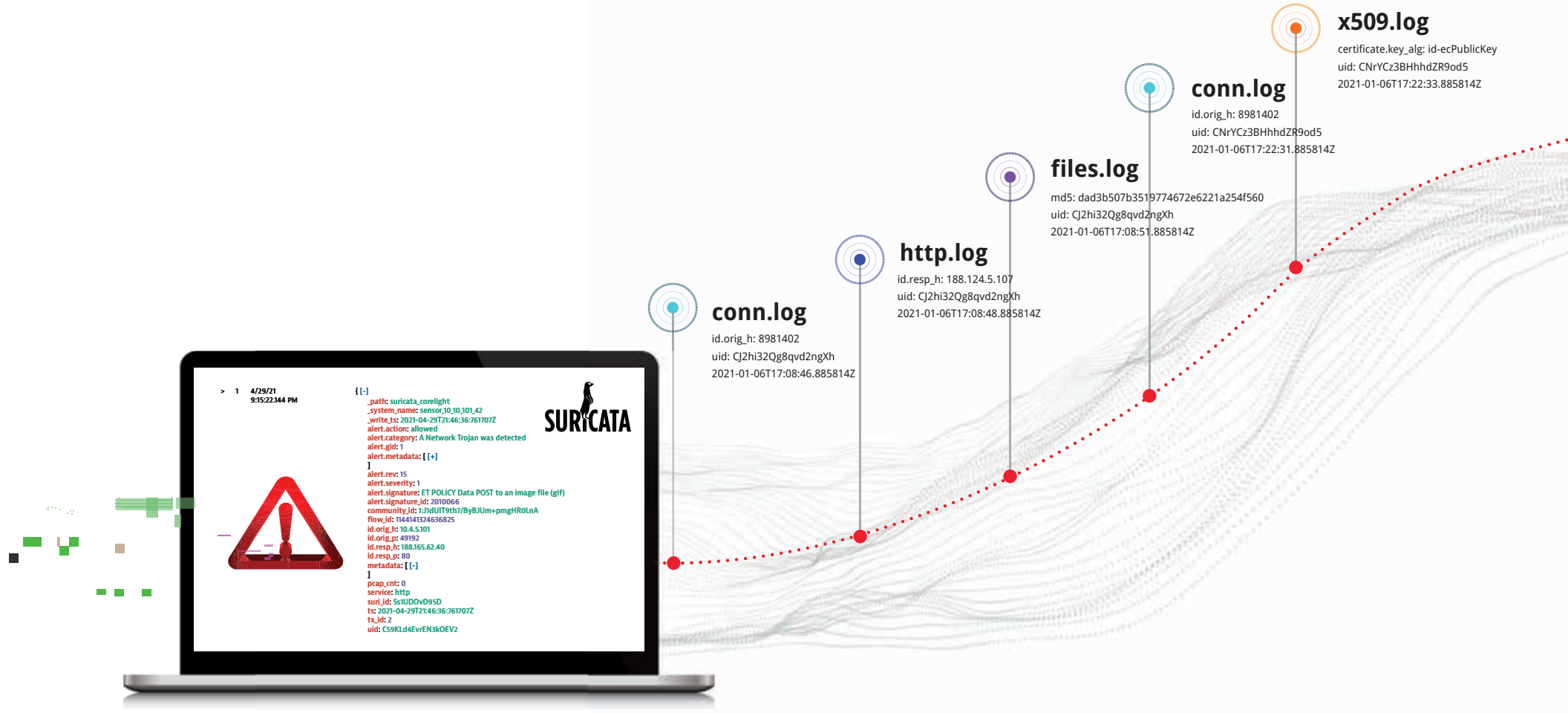
HOW DO YOU PROVE THE BREACH IS OVER, QUICKLY?

You're the CISO at a major retailer when a breach of credit card data lands your company in the news. Fortunately, you're using Corelight, so when consultants fly in, they hit the ground running and find the problem rapidly (hint: it's your POS machines). When it's the lawyers' turn, Corelight offers them a comprehensive view of a breach's scale and evidence that stands up in court, saving your reputation and your valuation.

ALERT FATIGUE

HOW DO YOU KNOW IF IT'S AN ALERT OR *THE* ALERT?

An alert surfaces when someone sends POST data to a GIF file. Tier 1 analysts must quickly determine whether the request was command and control, exfiltration, or something benign, but existing data sources often leave out crucial details that make these alerts impossible to resolve. Suricata alerts linked with Zeek network evidence give analysts direct access to the data they need across 50+ protocols. Plus, Corelight's powerful SOAR playbooks automate data-gathering to save time and eliminate alerts before analysts even see them.

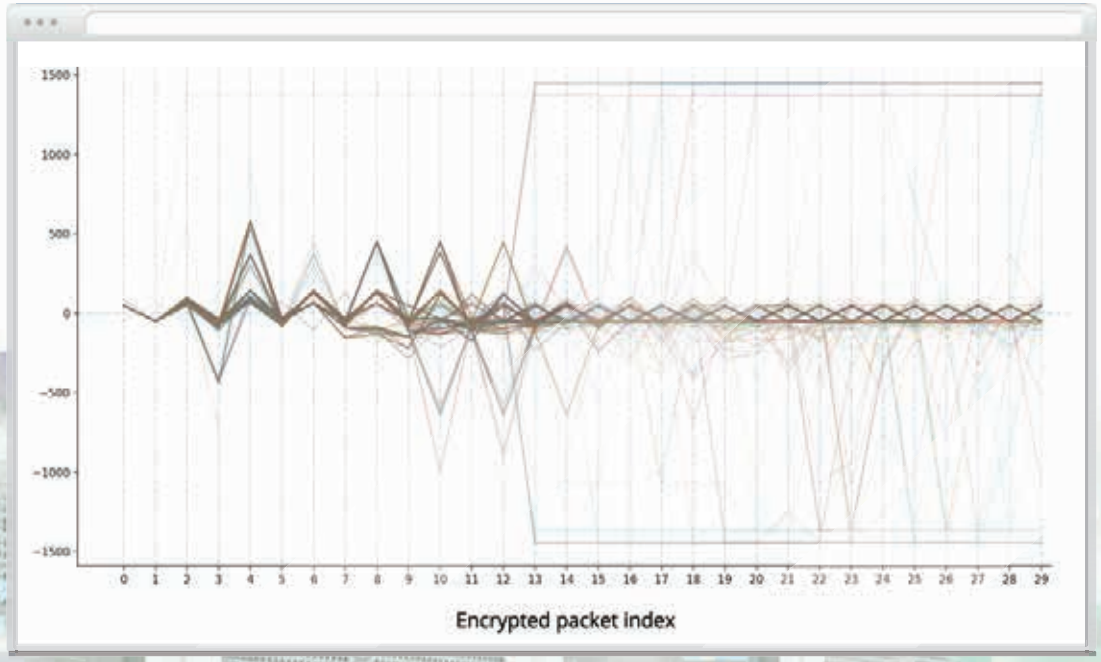


ET Pro rulesets are now available directly from Corelight.

ENCRYPTED TRAFFIC

HOW DO YOU FIND ADVERSARIES YOU CAN'T SEE?

Identifying attackers on your network is tough, and encryption only makes it harder. Without break and inspect, you'll only get the source, destination, and protocols. Corelight renders decryption unnecessary with insight that doesn't rely on direct observation of what's in the traffic—whether keystrokes are human or not, if a login was pasted or typed—and more. That means you can stop attackers before they exfiltrate data or install ransomware without compute-intensive practices that compromise privacy.

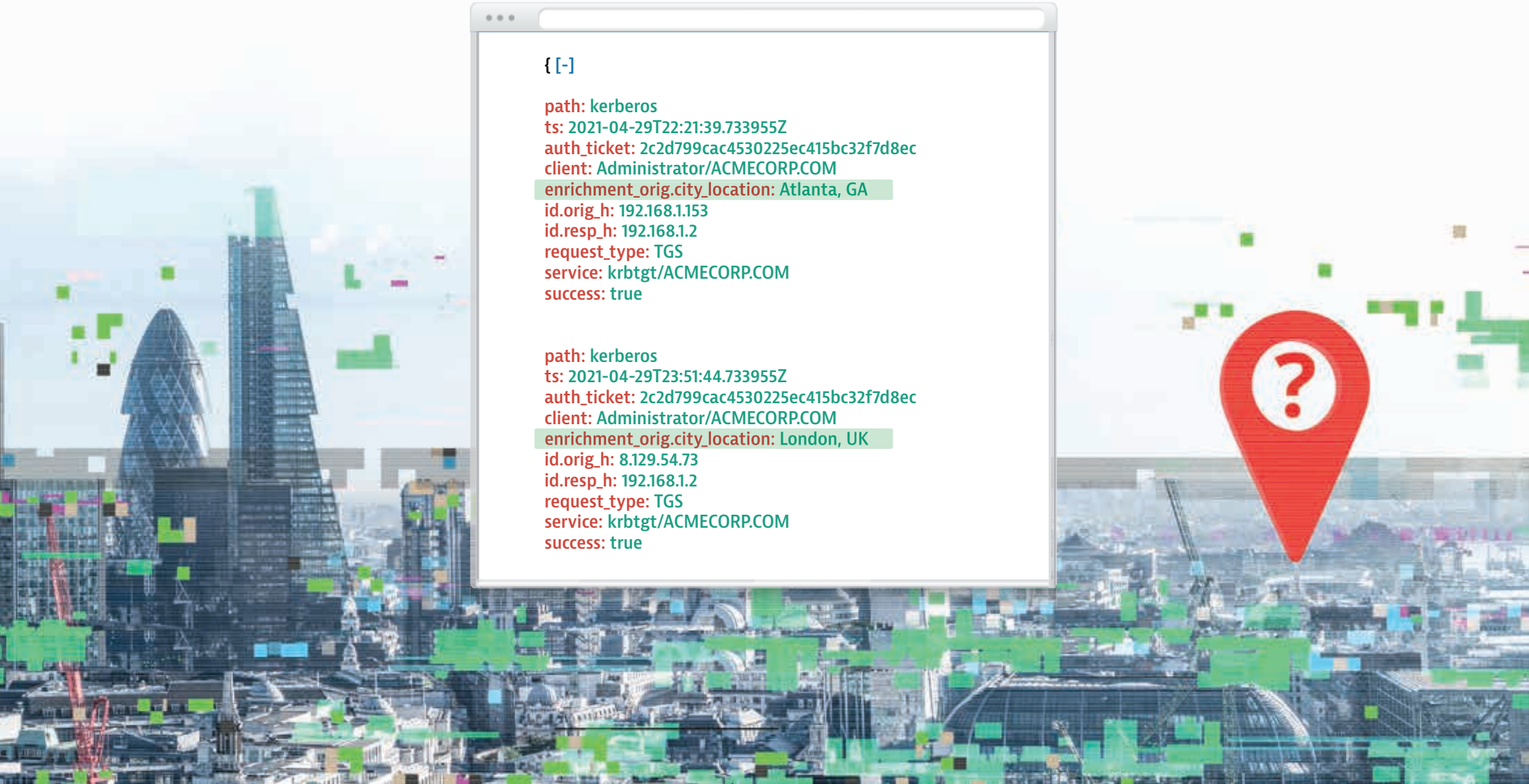


Pattern matching without decryption
Even encrypted packets offer vital clues about underlying applications. In these SSH connections, there are clear patterns in the packet size and timing such as long-lasting spikes that indicate file transfers. Corelight analyzes these patterns to extract valuable insight.

ZERO TRUST

HOW DO YOU TELL WHAT'S WRONG AND WHAT'S RIGHT?

Sam from accounting signs in from the London office—normally they only login from Atlanta—and then starts accessing sensitive servers. Corelight evidence reveals how your network typically behaves, so you notice something's off. When you investigate, you find proof that the *real* Sam from accounting just signed in an hour ago from Georgia, like always. Plot foiled. Corelight gives context, not just alerts, so you know what's normal and what's not so you can enforce Zero Trust.



WORKS WITH YOUR TEAM AND TECHNOLOGY

Corelight's evidence helps you reduce MTTR with the tools you already have because it's built on the open source global standard for network monitoring—so almost every major platform and tool can ingest it. And you won't have to redesign processes or retrain analysts, because our evidence is available in your existing workflows, saving precious time on each task.

splunk>

Azure

CROWDSTRIKE

Chronicle

elastic

humio

DEVO

CORELIGHT PRODUCTS

APPLIANCE SENSORS

Model	IU size	Monitoring interface	Throughput
AP 5000	Full-depth	2 QSFP28 modules. Support for optical modules at 8 x 10G, 2 x 40G or 2 x 100G	100 Gbps
AP 3000	Full-depth	Up to 8 SFP/SFP+ or 2 QSFP interfaces. Support for copper and optical modules at 1G and 10G or 40G	25 Gbps
AP 1001	Full-depth	4 SFP interfaces. Support for copper and optical modules at 100M and 1G	10 Gbps
AP 200	Half-depth	4 SFP interfaces. Support for copper and optical modules at 100M and 1G	2 Gbps

VIRTUAL SENSORS

	vCPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
VMware	4–64	16–256	500–4000	ESXi 6.5 or above	500 Mbps–8 Gbps
Hyper-V	4–64	16–256	500–4000	Windows Server 2016	500 Mbps–8 Gbps

SOFTWARE SENSOR

CPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
2–64	8–256	100–4000	Any 64-bit Linux distribution	250 Mbps–8 Gbps

CORELIGHT PRODUCTS

CLOUD SENSORS

	Instance	System requirements	Nominal capacity
AWS	M4 or M5 type AWS EC2	Amazon VPC traffic mirroring enabled OR mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps
MS AZURE	Azure Ds v3 series (D8s minimum	Traffic mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps
GOOGLE CLOUD	GCP-E2 or N1 machine type	Google Cloud Packet Mirroring enabled OR mirroring via 3rd party packet-forwarding agents	500 Mbps–8 Gbps

FLEET MANAGER

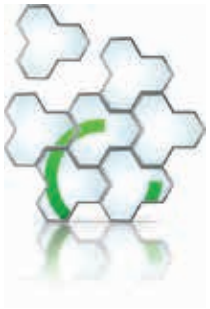
- Manage hundreds of sensors with Fleet Manager
- See overall fleet health in one pane of glass; drill into individual sensor metrics with one click
- Define custom sensor groups, assign individual user roles and access levels
- Create and deploy custom sensor policy templates
- Demonstrate compliance using audit logs

smartPCAP

- Cut your PCAP costs by up to 50%
- Fine tune rules to capture just the packets you need
- Expand retention by 10x while reducing costs
- Access packets directly in your SIEM for faster investigations

CORELIGHT COLLECTIONS

Turnkey packages that deliver proprietary detections plus curated insights from the Zeek community.



C2 COLLECTION

50+ detections and insights into known command and control activity as well as MITRE ATT&CK® C2 techniques to find novel attacks.

- Find Cobalt Strike and known malware families that run C2 over HTTP
- Detect DNS tunneling and other techniques like domain generation algorithms

ENCRYPTED TRAFFIC COLLECTION

Dozens of unique insights into SSL, SSH, and RDP connections along with top encrypted insights from the Zeek community like JA3—all without decryption.

- Track SSL fingerprints, soon-to-expire certificates, and more
- Track user behavior over SSH and RDP with insights that can see if it's a human or a script behind those packets

CORE COLLECTION

Preloaded Corelight packages that help sensors scale in high-throughput environments.

- Detect lateral movement mapped to MITRE ATT&CK
- Find cryptomining traffic over TCP or HTTP

Initial access happened eleven months, six days, and three hours **before discovery.**

That mountain of alerts turned out to be **nothing more than a misconfiguration.**

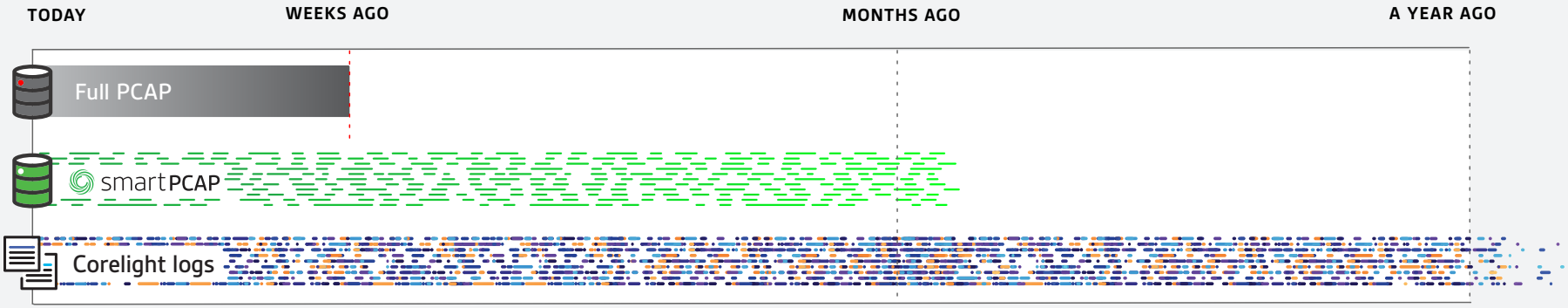
Last month's breach **started with a spearphishing attack** in the CFO's email.

Corelight is

HOW YOU KNOW.

smartPCAP

Save **up to 50%** vs. the cost of full PCAP



A smarter way to get 100% visibility. Capture just the packets you need and expand retention by 10x while simplifying investigations.

corelight

CORELIGHT IS **HOW YOU KNOW**

info@corelight.com | **888-547-9497**