BITSIGHT Luminate EXCHANGE

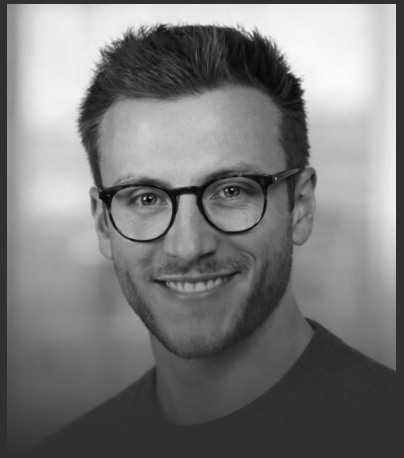
05

Your Breach, My Problem

Third Party Intelligence in the SOC

BITSIGHT

Speaker

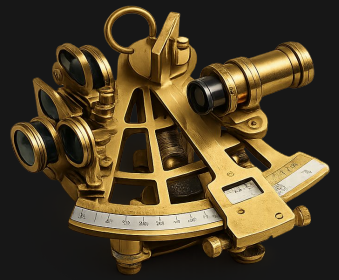


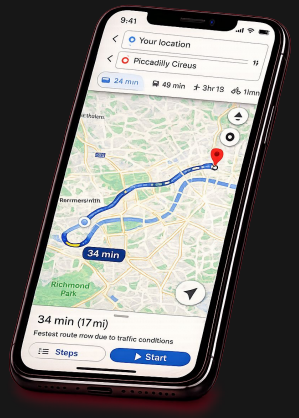
Felix Manig

Manager, Professional Services, Bitsight

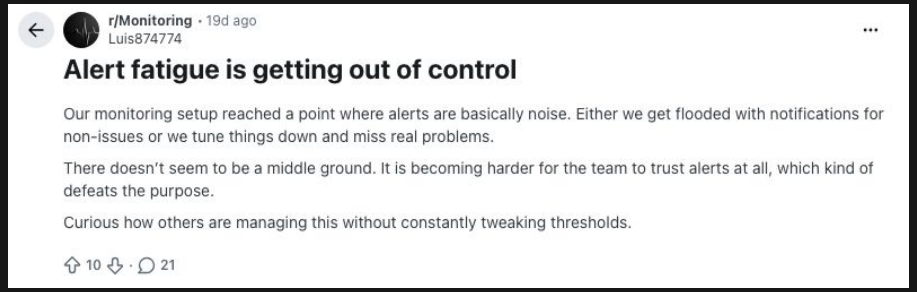
BITSIGHT Luminate EXCHANGE

A transformation story

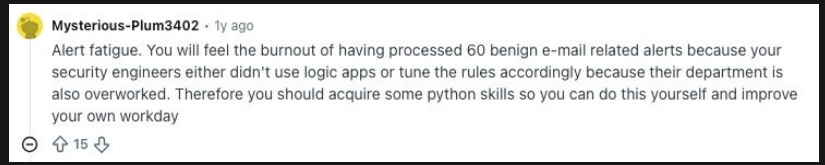




Before we talk about the future, let's listen to the present.



"Our monitoring setup reached a point where alerts are basically noise… It is becoming harder for the team to trust alerts at all."



"Alert fatigue. You will feel the burnout of having processed 60 benign email related alerts… acquire Python skills so you can fix it yourself."

The SOC works.
For a world that longer exists.

BITSIGHT Luminate EXCHANGE

A perimeter you controlled

Alerts from your own estate

Crown jewels inside your walls

BITSIGHT

As the world shifts,
the SOC is being squeezed.

BITSIGHT Luminate EXCHANGE

Attack surface & signal types

- SaaS Integration & 4th Party Supply Chains
- Credential & Token Exposure
- Identity-Layer Vendor Attacks

Regulatory pressure tightening

- DORA
- NIS2
- UK CTP
- FCA OR

SOC in capacity crisis

r/SecurityCareerAdvice · 1y ago
burnedtortillawrap

Overwhelmed after 1 year as a SOC Analyst

BITSIGHT

Your perimeter is now **someone else's network.**

BITSIGHT Luminate EXCHANGE

30%

of breaches involve a 3rd party

2x YoY — DBIR 2025

~3,700

Third-party breach events in 2025

5.28 average downstream victims per event

20%

of initial access via vuln exploitation

Perimeter is the target

45%

Expected to experience a supply chain-attack by 2026

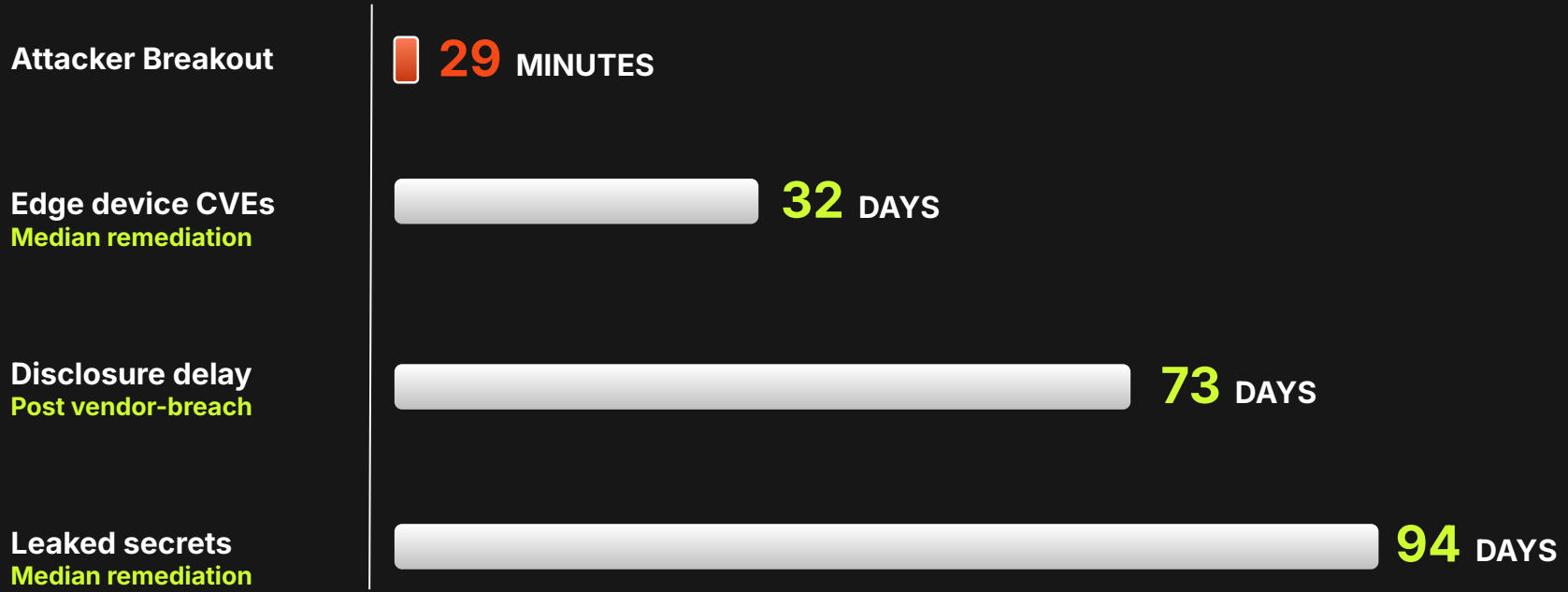
3x incidence rate of 2021

VERIZON DBIR 2025

BITSIGHT

Attackers move in minutes.
Your vendors move in months.

BITSIGHT Luminate EXCHANGE



Verizon DBIR 2025 · CrowdStrike 2026 Global Threat Report

BITSIGHT

Vendor CVE

Friday, 6:00 PM, CISA advisory drops.

ALERT CYBERSECURITY ADVISORY · CISA.GOV PUBLISHED 2026-02-25 18:00 UTC

CVE-2026-20127 — Active Exploitation of VPN Appliance

CISA is aware of active exploitation of CVE-2026-20127 affecting widely deployed VPN appliances. Organisations are urged to apply patches immediately and identify potentially affected third-party providers.

ALERT 6:00 PM	6:15 PM	DAY 3–5	DAY 14+	MEANWHILE
Advisory hits	**Question**	**Outreach**	**Response**	**Attacker is INSIDE**
Active exploitation confirmed	"Do any of our 300 vendors run this?"	TPRM emails vendors	Vendors confirm. No artifacts. No timeline.	Operating in minutes, while you wait weeks.

BITSIGHT Luminate EXCHANGE

Vendor Breach

An infostealer and a trusted integration.

Vercel

FEB 2026

Initial infection

Lumma Stealer infects a Context.ai employee device

FEB 2026

Token theft

OAuth tokens harvested from browser

MAR 2026

Trusted access

Vercel employee grants OAuth to Google Workspace

MAR 2026

Exfiltration

Internal API keys siphoned via integration

APR 2026

Monetisation

Database listed on BreachForums for $2M

EXTERNALLY VISIBLE SIGNALS

- Infostealer feeds
- OAuth grant anomaly
- Credential trade chatter

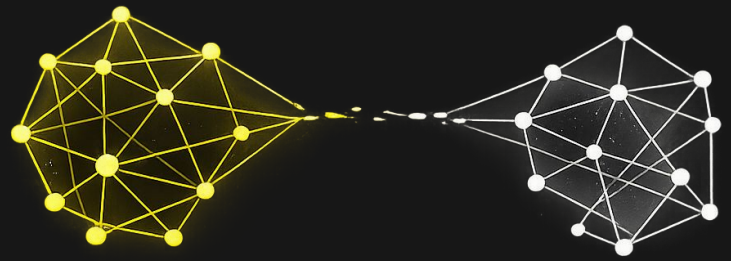
Two teams. Two languages.
One adversary.

BITSIGHT Luminate EXCHANGE

SOC

Speaks: Alerts. Playbooks. MTTD/MTTR.

- EDR / SIEM
- Detection rules
- IR playbook
- IOCs & TTPs



TPRM

Speaks: Contracts. Risk scores. Questionnaires.

- Risk governance
- Annual reviews
- Business criticality
- Programme maturity

26% Of orgs incorporate IR into TPRM

<50% Monitor even half of nth-party ecosystem

VERIZON DBIR 2025

BITSIGHT

AI is helping.
But it's not replacing.

BITSIGHT Luminate EXCHANGE

Hype says autonomous AI SOC. Data says human-in-the-loop.

13.9%	Have AI/ML formally defined in SOC operations
39.8%	Use AI/ML (but outside any defined workflow)
11%	Fully trust AI for mission-critical tasks

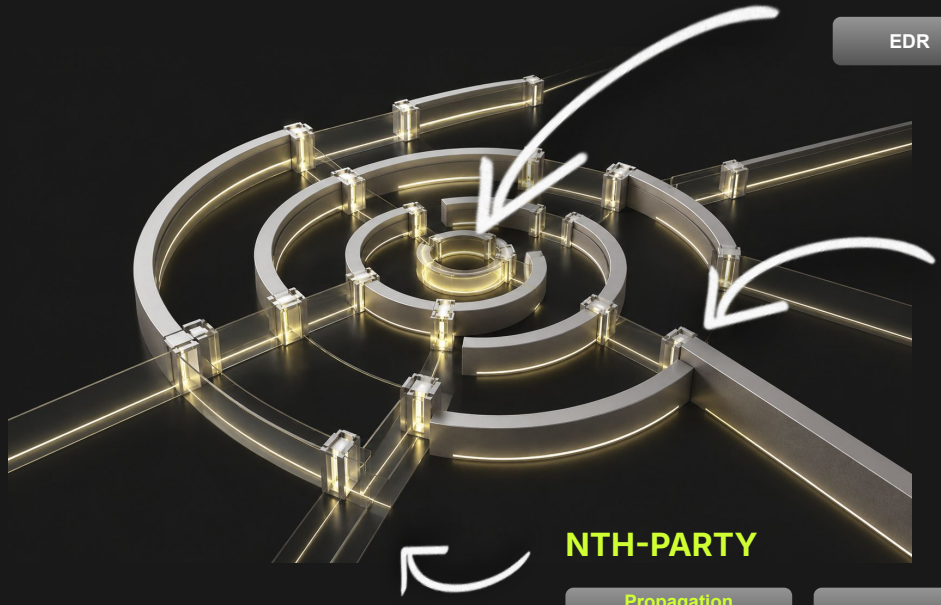
30.1%	MTTR reduction observed with Microsoft Security Copilot
59%	Say AI has improved process efficiency

SANS 2025 SOC SURVEY · SPLUNK STATE OF SECURITY 2025 · MICROSOFT · MANDIANT M-TRENDS 2025

BITSIGHT

Don’t replace the SOC.
Extend it.

BITSIGHT Luminate EXCHANGE



INTERNAL ESTATE

- EDR
- SIEM
- EASM

THIRD-PARTY ESTATE

- Validated Exposure
- Stealer Logs
- Leaked Secrets
- Identity & SaaS
- IdP
- OAuth
- API Tokens

NTH-PARTY

- Propagation Paths
- SBOM/VEX
- Downstream Dependencies

BITSIGHT

Better alerts and close the loop with a shared operating model.

BITSIGHT Luminate EXCHANGE

SOC

OPERATIONS LAYER

High-fidelity signal received	Triage · ATT&CK mapping · evidence	Evidence pack handed over	Remediation verified
INTAKE ▶	VALIDATION ▶	OUTREACH ▶	CLOSURE
Vendor tier applied	Escalation threshold met	Vendor notified · SLA tracked	Risk register · board reporting

GOVERNANCE LAYER

TPRM

BITSIGHT

Bitsight BEACON

BITSIGHT Luminate EXCHANGE

LAUNCHING 19 MAY 2026

Don’t wait for vendors to tell you.

Find out first

BITSIGHT

The SOC was never built for this.
Now you can design what comes next.

BITSIGHT Luminate EXCHANGE

1

Extend the SOC beyond your walls.

2

Trade noise for validated signal.

3

Bridge SOC and TPRM with a shared operating model.

BITSIGHT

Bitsight BEACON

BITSIGHT Luminate EXCHANGE

LAUNCHING 19 MAY 2026

Q&A

BITSIGHT