



The CISO's Evidence Problem: Proving **What Happened** Before the Regulator Asks

Your board holds you accountable. Your regulator holds a stopwatch. Yet after an incident, the questions that decide both — what happened, why, who was affected, and what must be reported — are still assembled by hand, slowly, from tools that were built to collect data, not to prove it. This paper is about closing that gap.

Written for

Chief Information Security Officers, and the security, risk and compliance leaders who report to the board

Solution

Tracknosis — proactive forensic data observability, AI investigation and regulatory reporting

Version

1.0 — August 2026

CONTENTS

1. Executive summary
2. The job has changed under you
3. Why your stack can't answer the four questions
4. What Tracknosis is: the forensic evidence layer
5. The 24-72-30 clock and named-executive liability

6. What Tracknosis delivers
7. From alert to evidence to regulatory submission
8. Keeping the AI honest: why the evidence is defensible
9. Building the business case for the board
10. Deployment: alongside the stack you already run
11. A CISO's evaluation checklist
12. Sources and references

01 Executive summary

The modern CISO is measured on two things at once: keeping the organisation secure, and being able to **prove** what happened when it isn't. The second is now the harder problem — and the one with your name on it.

Your security and observability platforms already collect an enormous volume of telemetry. What they do not give you, in the hours after an incident, are the four answers that decide your regulatory position and your board's confidence: **what happened, why, who was affected, and what must be reported**. Assembling those answers remains slow, manual and expensive — and you are now required to produce them against a statutory clock, with liability attaching to named executives.

Tracknosis is a proactive data forensic monitoring solution that sits alongside the SIEM and observability platforms you have already invested in. It converts the telemetry you already collect into structured, baselined, defensible evidence — root cause, attack timeline, blast radius, and regulator-ready reporting across the NIS2, CIRCIA, SOCI and CCSPA 24-72-30 lifecycle. It does not add another detection layer to the noise; it attacks the single largest cost line in an incident — investigation effort and downtime — and the single largest exposure on your desk — the report you owe the regulator.

THE ONE-LINE VERSION

Splunk, Datadog and Elastic **collect the telemetry**. Tracknosis turns it into **forensic evidence, root-cause intelligence, unknown-threat detection and regulator-ready reporting** — the proof a CISO needs to answer the board and the regulator on deadline.

THE THREE PAIN POINTS TRACKNOSIS SOLVES

Strip away the vendor noise and enterprises — and the SMEs in their supply chains — face the same three

PAIN POINT 01

TOO MUCH DATA, TOO MANY ALERTS

Volume overwhelms the SOC. False positives and false negatives bury the signal, and investigations stay slow, manual and inconclusive — consuming the senior-analyst time you cannot recover.

PAIN POINT 02

UNKNOWN THREATS & BLIND SPOTS

Current security products are great at detecting the known, but they struggle with unknown and emerging threats and leave incomplete visibility across systems, users and change.

PAIN POINT 03

PROVING IT, ON DEADLINE

Investigating an incident and proving what actually happened is slow — just as NIS2, CIRCIA and their peers put the onus on directors to report breaches rapidly, with penalties for getting it wrong.

WHAT A CISO GETS

- ▶ Telemetry transformed into forensic evidence, accelerating investigation and response
- ▶ Materially reduced Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTR)
- ▶ Genuine root-cause analysis through pre-incident change tracking — causes closed, not symptoms suppressed
- ▶ Evidence mapped to the content requirements of NIS2 Article 23 and CIRCIA-style reporting, in dozens of languages
- ▶ Defensible evidence packages that support cyber-insurance adherence and lower premiums
- ▶ Improved return on the observability and SIEM investment you have already made

02 The job has changed under you

Three pressures now converge on the security leader at the same time. Individually they are manageable. Together they redefine the role from "prevent the breach" to "prevent the breach — and be ready to prove exactly what happened when one gets through."

2.1 The breach is assumed

Boards and regulators no longer treat a breach as a failure of the CISO alone; they treat it as an inevitability to be managed. That shifts the question you are judged on. It is no longer only "did you stop it?" but "when it happened, how fast and how credibly could you explain it?" Preparedness to investigate has become a control in its own right.

2.2 Accountability is personal

Modern cyber regulation deliberately attaches liability to named senior individuals, not just to the corporate entity. NIS2 makes management bodies responsible for approving and overseeing cyber-risk measures, with the possibility of personal consequences. The practical effect for you is direct: the evidence to satisfy a regulator must exist and be retrievable within the reporting window — and if it does not, the gap is attributed upward.

You cannot delegate accountability you cannot evidence.

2.3 The board wants a number, not a narrative

"We are investigating" is no longer an acceptable board update at hour 24. Directors increasingly expect a defensible position — scope, impact, root cause, and reporting status — expressed in terms they can act on and disclose. That requires an evidence base that is assembled continuously and available on demand, not reconstructed from scratch under pressure while the clock runs.

03 Why your stack can't answer the four questions

This is not a criticism of your SIEM or your observability platform. They are excellent at what they were built for — collecting, indexing and alerting on high volumes of telemetry. The problem is that the four questions a CISO must answer after an incident are a different class of problem from detection.

WHAT COLLECTION TOOLS DO WELL

- Ingest and index telemetry at scale
- Fire alerts on known signatures and rules
- Dashboard current state and trends
- Retain logs for search

WHAT THEY LEAVE TO YOU

- Reconstructing the attack timeline by hand
- Identifying what **changed** before the incident
- Establishing blast radius — who and what was affected
- Producing evidence in the form a regulator accepts

The result is a gap that opens at exactly the wrong moment. Alert fatigue, false positives and manual triage leave teams unable to answer what happened, why, and who was affected — and every hour spent assembling a timeline by hand is an hour of senior-analyst capacity you cannot recover and an hour of exposure you cannot yet explain to the board. Investigation effort and downtime, not detection, are the largest share of cyber-incident cost.

THE TRAP

More detection produces more alerts, which lengthens investigation, which widens the very gap the deadline is measuring. Adding another detection layer makes the CISO's evidence problem worse, not better.

04 What Tracknosis is: the forensic evidence layer

Tracknosis is the layer your security stack does not have. It does not replace collection; it sits on top of it and converts what you already gather into defensible proof.

Where observability tells you the system is unhealthy, and detection tells you a rule matched, **forensics tells you — and lets you prove — what actually happened.** Anything worthy of the word "forensic" has to clear a higher bar than analysis: integrity (the evidence is provably unaltered), chain of custody (who and what

defensibility (the finding survives scrutiny from a regulator, an insurer and, if it comes to it, a court). Tracknosis is engineered to preserve all four.

PROACTIVE, NOT POST-MORTEM

Tracknosis baselines normal behaviour and tracks change **continuously** — before an incident, not only after one is declared. When an incident does occur, the evidence base already exists; you are retrieving and packaging it, not reconstructing it against the clock.

05 The 24·72·30 clock and named-executive liability

To be precise about a point the market often blurs: no regulation in this family mandates a particular product or forensic technology. What NIS2 Article 23, CIRCIA and their equivalents demand is a **body of evidence** — a detailed incident description, indicators of compromise, root cause, severity and impact, and mitigation measures — delivered on a statutory clock. Tracknosis automates the difficult part: assembling and preserving that evidence.

24h

Initial regulatory warning

72h

Substantiating report with severity, impact and IOCs

30d

Full root-cause and mitigation report

14%

Of firms report being NIS2 ready

These are not best-practice targets; they are statutory deadlines, and the evidence to satisfy them must exist and be retrievable within the window. The scope is broad and widening: roughly **160,000 entities** fall within NIS2 and **300,000+ covered entities** under CIRCIA, before SOCI (Australia) and CCSPA (Canada) are counted. Only around 14% of organisations report being ready — which is precisely why compliance has moved from a discretionary purchase to a board-level, budget-released priority.

Regime	Jurisdiction	What it demands of the CISO
NIS2 (Art. 23)	European Union	Early warning (24h), incident notification with initial severity/impact and IOCs (72h), final report with root cause and mitigation (~30d); management-body accountability.
CIRCA	United States	Covered-entity reporting of significant incidents and ransomware payments to CISA on defined timelines, with supporting detail.
SOCI	Australia	Mandatory incident reporting for critical-infrastructure assets within short statutory windows.
CCSPA	Canada	Reporting obligations for designated critical cyber systems and their operators.

5.1 The consequences of getting it wrong

The penalties in this family are triggered less often by the breach itself than by the failure to report it accurately and on time — or by filing an account you cannot stand behind. The obligation to report is only as strong as its enforcement, and that enforcement is deliberately pointed at the organisation and, increasingly, at named individuals.

Regime	Failure to report / inaccurate report
NIS2 (EU)	Administrative fines up to €10m or 2% of global annual turnover (essential entities) and €7m or 1.4% (important entities), whichever is higher. Authorities may also issue binding remediation orders, suspend certifications, and temporarily ban named individuals from management functions . Management bodies can be held personally liable.
CIRCA (US)	Enforcement by compulsion: CISA can issue a request for information and then a subpoena ; non-compliance is referred to the Department of Justice for civil action or contempt. Knowingly false statements to a federal agency carry separate criminal exposure.
SEC disclosure (US public co.)	A materially late or inaccurate incident disclosure is a separate enforcement track , with monetary penalties and individual liability — accuracy matters independently of the security regulator.
Downstream exposure	An unsupported or inaccurate account can jeopardise a cyber-insurance claim , become disclosable evidence in litigation, and expose directors to shareholder and duty-of-care scrutiny.

THE SQUEEZE

You are required to investigate faster and prove root cause to a regulator on deadline — using data that is often too sensitive to send to the public AI services that would otherwise help you move quickly. The capability to do this has to exist somewhere you control.

WHY THIS IS AN EVIDENCE PROBLEM, NOT A PAPERWORK PROBLEM

Almost every consequence above is triggered by the same root failure: an account of the incident that is **late, incomplete, or impossible to substantiate**. A defensible, timestamped evidence trail is what keeps a report accurate, on deadline, and survivable under audit, subpoena, insurance review or litigation.

06 What Tracknosis delivers

Six capabilities the collection-and-detection stack does not provide — each mapped to a question the CISO must answer.

FORENSIC OBSERVABILITY

Forensic-grade visibility across systems, users and transactions — producing defensible evidence rather than more alerts. *Answers: what happened.*

ROOT-CAUSE & DELTA TRACKING

Identifies what changed *before* the incident, converting a symptom into a diagnosis so the cause is closed, not re-fought. *Answers: why it happened.*

UNKNOWN-THREAT DETECTION

Surfaces emerging and unknown threats that signature- and rule-based detection miss entirely. *Answers: what we didn't already know.*

BLAST-RADIUS MAPPING

Establishes which users, systems and data were affected and how the compromise propagated. *Answers: who was affected.*

AI INCIDENT RECONSTRUCTION

AI assembles the attack timeline automatically — with every finding traceable back to immutable, timestamped, verified telemetry. Defensible evidence, not analytics.

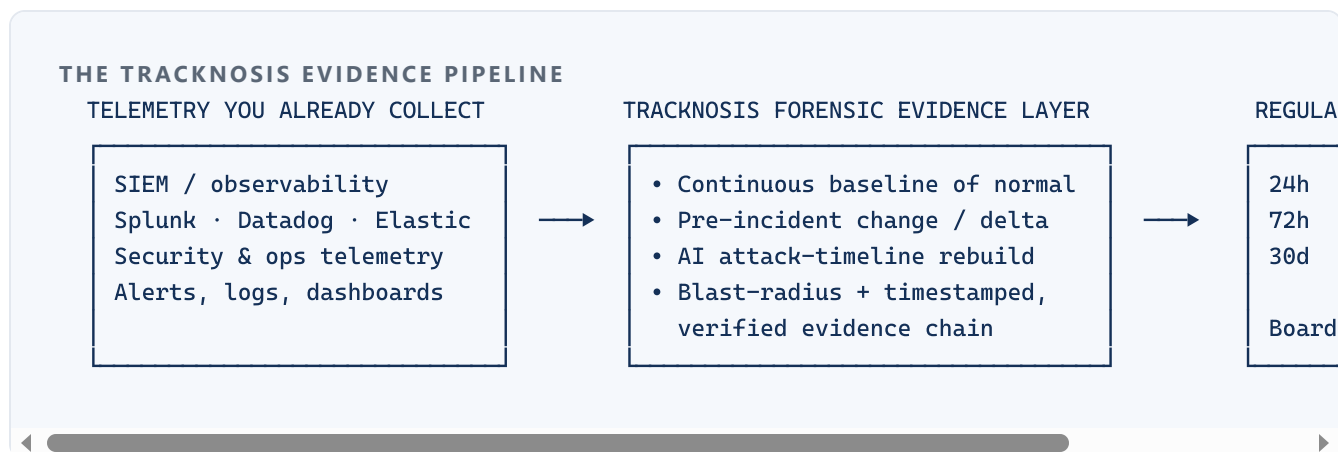
REGULATOR-READY REPORTING

Auto-generated incident reports mapped to NIS2 Article 23 and CIRCIA-style content requirements, in dozens of languages. *Answers: what must be reported.*

07 From alert to evidence to regulatory submission

Tracknosis runs as a continuous pipeline, not a one-off investigation tool. It baselines behaviour in normal

packaged.



WHY "BEFORE" MATTERS

A symptom without a cause recurs. Because Tracknosis tracks what changed **before** the incident, root cause is established rather than inferred — so the same incident is fixed once, not fought repeatedly, and the report you file names a cause a regulator can accept.

08 Keeping the AI honest: why the evidence is defensible

"AI" is doing real work here — timeline reconstruction, anomaly and unknown-threat detection, root-cause and delta analysis, and report authoring. But a CISO cannot submit probabilistic output to a regulator and call it evidence. The distinction that makes Tracknosis defensible is simple and non-negotiable:

The AI does the investigation. The evidence underneath stays deterministic and verifiable.

Every AI-asserted conclusion — "this account was compromised at 14:02," "this change preceded the failure" — points back to the specific, immutable, timestamped, verified telemetry it was derived from. That traceability is what lets a finding survive the only question that ultimately matters in front of a regulator or an insurer: *how do you know?* It is also the difference between "AI forensics" and "AI guesswork," and it is where Tracknosis is deliberately engineered to be conservative.

WHAT THIS GIVES THE CISO

- ▶ Findings that are auditable back to source, not asserted by a black box
- ▶ An evidence chain that holds up to a regulator, an insurer and a court
- ▶ A model kept honest by the evidence, rather than trusted on faith

09 Building the business case for the board

Tracknosis is one of the few security investments that attacks a cost line the board already tracks, rather than adding an insurance-style line item whose value only appears in a crisis. Frame the case on three measurable axes.

COST CONCENTRATION

Investigation effort and downtime — not detection — are the largest share of incident cost. Compressing investigation attacks the biggest number in the incident, which is where measurable return lives.

TIME TO ANSWER

Reduced MTI and MTTR mean faster containment, shorter downtime, and a defensible board position at hour 24 instead of day 10. Speed is now a compliance property, not just an operational one.

INSURANCE & PREMIUMS

Defensible evidence packages support cyber-insurance policy adherence and strengthen your position at renewal — turning forensic readiness into a line the CFO recognises.

SWEATING EXISTING SPEND

Tracknosis improves the return on the SIEM and observability platforms you already own by turning their output into evidence — no rip-and-replace, no re-platforming.

THE BOARD SENTENCE

"We are reducing the largest cost in any incident — the time and effort to investigate it — while guaranteeing we can meet our statutory reporting obligations, using the data we already collect." That is a sentence a board approves.

10 Deployment: alongside the stack you already run

Tracknosis is designed to be adopted without disruption. It is sold and deployed **alongside — not against —** your incumbent SIEM and observability platforms, and high-fidelity forensic snapshots are stored back into the platform you already own.

- ▶ **No rip-and-replace.** It consumes the telemetry you already collect; your existing tooling and workflows stay in place.
- ▶ **Deploys where your data must live.** For regulated sectors where incident data cannot leave the estate, Tracknosis can run inside your own environment, so sovereignty is designed in rather than managed with contractual controls.
- ▶ **Complements your SOC.** It compresses the manual, specialist analyst work — timeline assembly, change correlation, report drafting — rather than replacing the team that owns the response.

GOVERNANCE NOTE

Because Tracknosis handles the most sensitive material an organisation holds — credentials, session data, privilege maps and breach evidence that may become disclosable in litigation — evidence integrity, access control and retention should be governed as first-class controls, and are designed to be.

11 A CISO's evaluation checklist

Whether you evaluate Tracknosis or any forensic-evidence capability, these are the questions that separate a genuine evidence layer from a re-badged analytics dashboard.

Question to ask	What "good" looks like
Can every finding be traced to source?	Each AI conclusion links to specific, immutable, timestamped, verified telemetry — auditable end to end.
Does it track change before the incident?	Continuous baselining and delta tracking, not just post-incident search.
Does output map to the regulations?	Reports map to NIS2 Article 23 / CIRCIA content requirements, not a generic PDF.
Does it work with our stack?	Consumes existing SIEM/observability telemetry; no rip-and-replace.
Can it run where our data must live?	Deployable inside the estate for data that cannot leave.
Does it reduce MTTI / MTTR measurably?	Demonstrable reduction on a real or replayed incident, not a slideware claim.

If you are not fast, you are last — and in the 24-72-30 era, being right slowly is the same as being wrong.

Tracknosis exists to answer the questions that actually matter after an incident — what happened, why, who was affected, and what must be reported — and to answer them in time to meet the regulator, with evidence you can defend. For a walkthrough against your own environment, talk to the team.

12 Sources and references

- Directive (EU) 2022/2555 (NIS2), in particular Article 23 (reporting obligations) and Article 20 (governance / management-body accountability).
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), United States.
- Security of Critical Infrastructure Act 2018 (SOCI), Australia, and subsequent amendments.
- Critical Cyber Systems Protection Act (CCSPA), Canada.
- Industry analyses of cyber-incident cost distribution, indicating investigation effort and downtime as the largest components of total incident cost.
- Reported NIS2-readiness surveys indicating a low proportion of in-scope organisations assess themselves as ready.

Figures cited (entity counts, readiness percentages, the 24·72·30 lifecycle) are drawn from public regulatory texts and industry reporting current at the time of writing and are provided for orientation; organisations should confirm the obligations applicable to their own jurisdiction and sector.

Tracknosis Ltd © 2026 | Making the Unknown Known · CISO Edition Whitepaper, v1.0 — August 2026. This document is provided for information only and does not constitute legal or compliance advice.