

Tracknosis with Cisco AI Infrastructure · Enterprise Solution Whitepaper

From Telemetry to Evidence: Deploying an **AI Forensic Investigator** Inside Your Own Data Centre and Windows Estate

White Paper

Full-Stack AI Forensic Security

Your SIEM already collects the data. Cisco AI PODs and Cisco AI in a Box give you a sovereign AI platform to reason over it. Tracknosis supplies the forensic evidence that makes the AI's conclusions accurate enough to act on — and defensible enough to submit to a regulator.

Making the Unknown Known

Written for:

CISOs, CIOs, Heads of Security Operations, and infrastructure and risk leaders in regulated enterprises

Solution:

Tracknosis forensic observability on Cisco AI in a Box or Cisco AI POD



Executive Summary

The three pain points Tracknosis solves

Strip away the vendor noise and enterprises — and the SMEs in their supply chains — face the same three cyber security pain points. Tracknosis, deployed on Cisco AI infrastructure, is built to close all three:

- 1. Too much data, too many alerts.** False positives and false negatives bury the signal, leaving investigations slow, manual and inconclusive.
- 2. Unknown threats and blind spots.** Security tools detect what they already recognise, but struggle with unknown and emerging threats and leave incomplete visibility.
- 3. Proving what happened, on deadline.** Investigation is slow just as NIS2, CIRCIA and their peers put the onus on directors to report breaches rapidly, with penalties for failure.

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 actually matter: **what happened, why, who was affected, and what must be reported.**

Assembling those answers is still slow, manual and expensive — and you are now required to produce them against a statutory clock, using data that cannot lawfully leave your estate.

This whitepaper describes a joint solution to that problem:

- ▶ **Cisco AI PODs or Cisco AI in a Box** provide a pre-validated, sovereign AI platform inside your own data centre — the compute, networking and AI software stack, deployed in weeks rather than quarters.
- ▶ **Tracknosis** provides the forensic evidence layer that converts the telemetry you already collect into structured, baselined, defensible evidence that an AI can reason over — root cause, attack timeline, blast radius, and regulator-ready reporting across the NIS2, CIRCIA, SOCI and CCSPA 24-72-30 lifecycle.

To be precise about the last of those, because the market often is not: no regulation in this family mandates a particular product or forensic technology.

What NIS2 Article 23 and CIRCIA do is demand a body of evidence — detailed incident description, indicators of compromise, root cause, severity and impact, and mitigation measures — on a statutory clock. Tracknosis automates the difficult part, which is assembling and preserving that evidence. Section 9 sets out the mapping requirement by requirement.

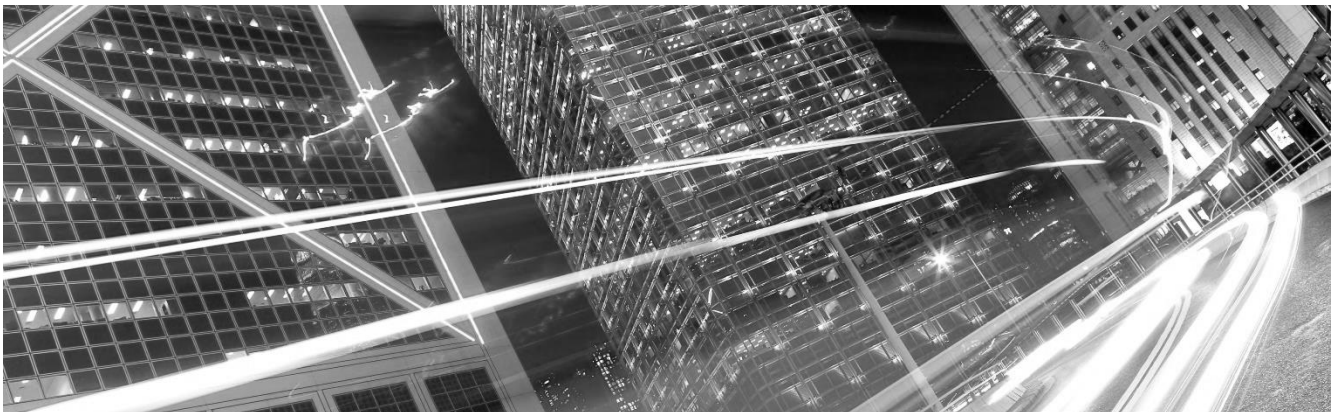
Together they give you something you cannot buy as a subscription and cannot outsource to a public cloud model: an AI forensic investigator that you own, that runs on your premises, and that works on evidence rather than on guesswork

The Core Proposition

Cisco AI PODs give you a sovereign, on-premises AI platform purpose-built for the workloads that matter most. The workload that carries the strongest business case is *"investigate last night's ransomware attack, and produce the regulator's 72-hour report."* It is high value, it is compelled by regulation rather than chosen, and it is one of the very few AI workloads that genuinely cannot run in a public cloud service — because the data it depends on is not permitted to leave your estate. Tracknosis turns that platform into a full-stack AI forensic security capability.

What You Get

- ▶ 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, so causes are closed rather than symptoms suppressed
- ▶ Evidence mapped to the specific content requirements of NIS2 Article 23 and CIRCIA-style reporting, with jurisdiction-specific packs covering the regimes in Appendix A, in dozens of languages
- ▶ Defensible evidence packages supporting cyber-insurance policy adherence
- ▶ Improved return on the observability and SIEM investment you have already made
- ▶ A sovereign AI platform that hosts this and your other enterprise AI workloads concurrently.



The Problem You Are Being Asked To Solve

Three pressures are converging on security and infrastructure leaders at the same time.

Investigations Stall

Alert fatigue, false positives and manual triage leave teams unable to answer what happened, why, and who was affected. Investigation effort and downtime — not triaging and validation — are the largest share of cyber-incident cost. 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 explain to the board.

Regulation Now Has Teeth

NIS2, CIRCIA, SOCI and CCSPA impose a hard reporting lifecycle, with liability attaching to named executives:



These are not best-practice targets. They are statutory deadlines, and the evidence to satisfy them must exist and be retrievable within the window.

Under NIS2 Article 23 the 72-hour notification must carry an initial assessment of severity and impact together with indicators of compromise where available, and the final 30 day report after incident/breach must set out root cause and mitigation — content requirements that are only as achievable as your underlying evidence.

Only 14% of companies report being NIS2 ready, which is why compliance has become a board-level, budget-released priority rather than a discretionary purchase.

The Data Cannot Leave

The material an investigation depends on — credentials, session data, privilege maps, breach evidence, and records that may become disclosable in litigation — is among the most sensitive an organisation holds. For banks, defence, healthcare, government and critical national infrastructure, sending it to a public AI service is not a preference to be weighed. It is frequently prohibited.

The Squeeze

You are required to investigate faster and prove root cause to a regulator on deadline, using exactly the data you are not permitted to send to the AI services that would otherwise help you do it. That is the gap this solution closes.

Why The Answer Has To Run Inside Your Own Estate

Four factors make on-premises AI infrastructure the right answer for this workload specifically — not merely a conservative one.



Data sovereignty – Incident data cannot be sent to public AI services under most regulated-sector obligations. An on-premises platform removes the question entirely rather than managing it with contractual controls.



Regulatory compulsion – You must produce forensic evidence to a statutory deadline whether or not you have an AI strategy. The workload is not optional, so the capacity to perform it has to exist somewhere you control.



Cost concentration – Investigation effort and downtime are the largest share of incident cost. An AI workload that compresses investigation attacks the biggest line item you already track, which is where measurable return lives.



Continuous demand – Security operations runs continuously — triage, hunting, reconstruction, reporting. That sustains utilisation of the platform you buy, rather than leaving expensive infrastructure idle between projects.

The infrastructure gap is real and widely acknowledged: the Cisco 2025 AI Readiness Index found that only 28% of organisations believe their current infrastructure can handle AI workloads. But a gap is not a reason to buy. The reason to buy is a workload that delivers a return you can measure and an obligation you must meet – and then discovering that it requires infrastructure you do not yet have

What Cisco Provides: The AI Platform

Cisco's AI infrastructure portfolio has three tiers. Understanding which one you need is the difference between a proportionate investment and an oversized one.

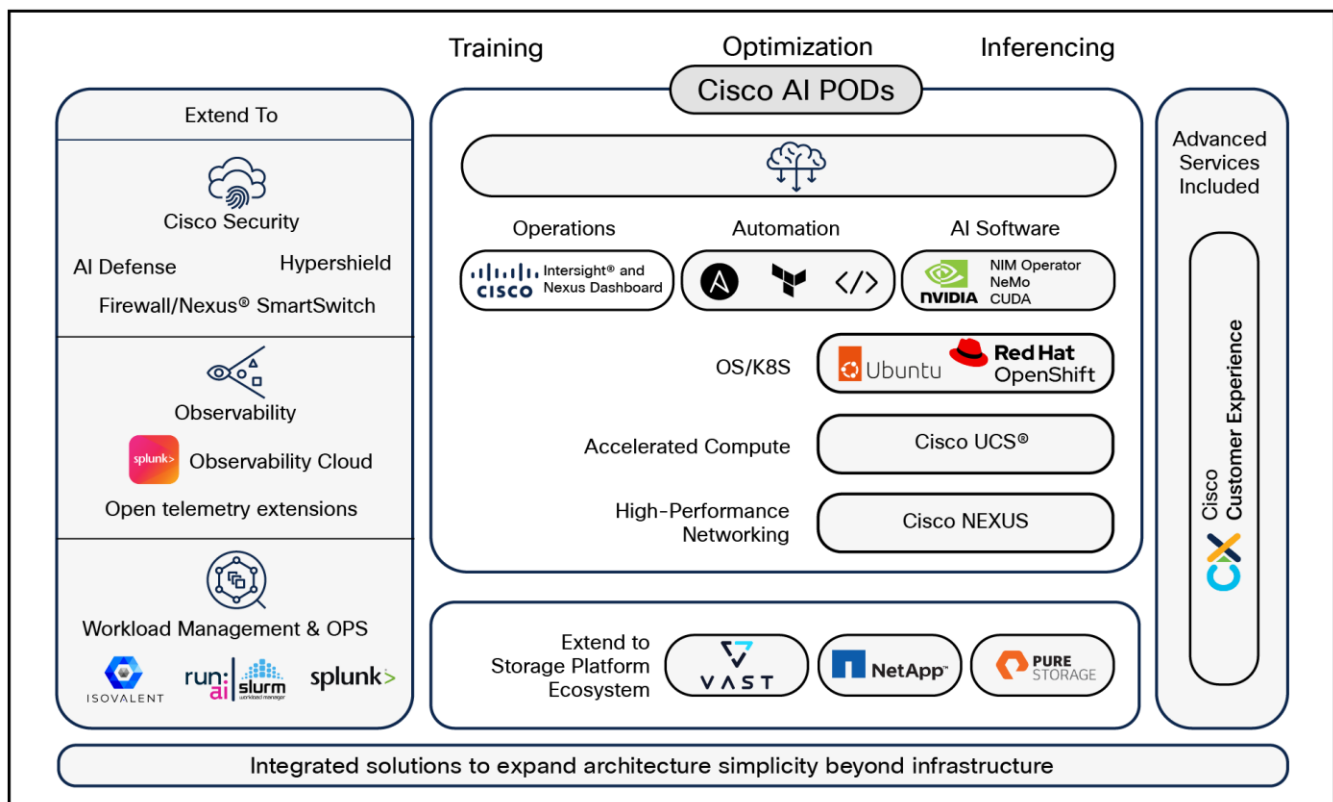


FIGURE 1 – THE CISCO AI POD ARCHITECTURE

Reproduced from Cisco's AI PODs At-a-Glance. Two things are worth noting before you read on. The layers Tracknosis depends on are already in the diagram – AI Software serves the models, OS/K8S provides the scheduling boundary that keeps a workload isolated, and Accelerated Compute and High-Performance Networking sit beneath them. And the Extend To column on the left already contains Splunk Observability Cloud and Cisco AI Defense: they are part of Cisco's published architecture, not additions this paper is asking you to buy.

Cisco AI POD — the infrastructure building block

An AI POD is pre-validated AI infrastructure for training, fine-tuning and inference, delivered against CiscoValidated Designs (CVDs) and NVIDIA Enterprise Reference Architectures (ERAs). The practical benefit to you is predictability: performance, scalability and cost are known before you buy, and you are not absorbing months of integration risk. The stack typically comprises:

Layer	Typical components
Compute	Cisco UCS C885A M8 (8RU, NVIDIA HGX architecture, 8× HGX H200 GPUs with NVLink, BlueField-3 SuperNICs); UCS C845A M8 and C240/C245 M8 RTX PRO servers; Intel Xeon Scalable and AMD EPYC; up to 4 TB DDR5 per node
Back-end fabric	Cisco Nexus 9364E-SG2 (800 GbE) in a non-blocking, lossless spine-leaf topology
Front-end fabric	Cisco Nexus 9332D-GX2B / 9364D-GX2A (400 GbE) into the enterprise network
Storage	Cisco or partner (NetApp / FlexPod, VAST Data, Pure) depending on the validated design
AI software	NVIDIA AI Enterprise (NVAIE), NVIDIA NIM inference microservices, RAG and agent tooling
Platform	Red Hat OpenShift for container orchestration; Ansible / Terraform automation
Management	Cisco Intersight (SaaS lifecycle management); Cisco Nexus Dashboard (fabric)

For inferencing, Cisco offers pre-sized configurations spanning edge inference, RAG-augmented inference, scale-up inference for larger models, and scale-out inference for large deployments — removing sizing guess work from your decision.

Cisco AI in a Box — the complete departmental solution

"AI in a Box" is a complete, pre-integrated AI environment: POD infrastructure plus networking, security, AI software, management, observability, deployment automation and support. It is designed for organisations that need AI locally but do not need a large GPU cluster. For most enterprises approaching this solution for the first time, **this is the right starting point** — a point section 13 develops.

The Distinction That Matters To Your Budget

AI POD = the infrastructure building block. AI in a Box = the complete enterprise AI solution. AI POD is a component of the AI in a Box concept, not a synonym for it. The two carry materially different price points, and choosing correctly is the single largest lever on your business case.

Cisco Secure AI Factory with NVIDIA — the enterprise platform

At the top of the portfolio, Cisco Secure AI Factory with NVIDIA wraps the infrastructure in security and observability: Cisco AI Defense (orderable for on-premises data-plane deployment, protecting AI models and applications and limiting sensitive data leaving your data centre), Cisco Hyper shield, Cisco XDR, Talos threat intelligence, and Splunk.

Where Splunk fits

Splunk is not installed on an AI POD the way a GPU driver is. It sits alongside the infrastructure as the intelligence and observability layer. Splunk Observability Cloud gives your teams real-time insight into AI infrastructure health, availability and resource utilisation — GPU utilisation and memory, power, network performance, node health and token costs — integrating data from Cisco Inter sight and Cisco Nexus through an AI POD infrastructure dashboard. In practice this means the AI platform you buy is observable with the same tooling you already use for the rest of the estate.

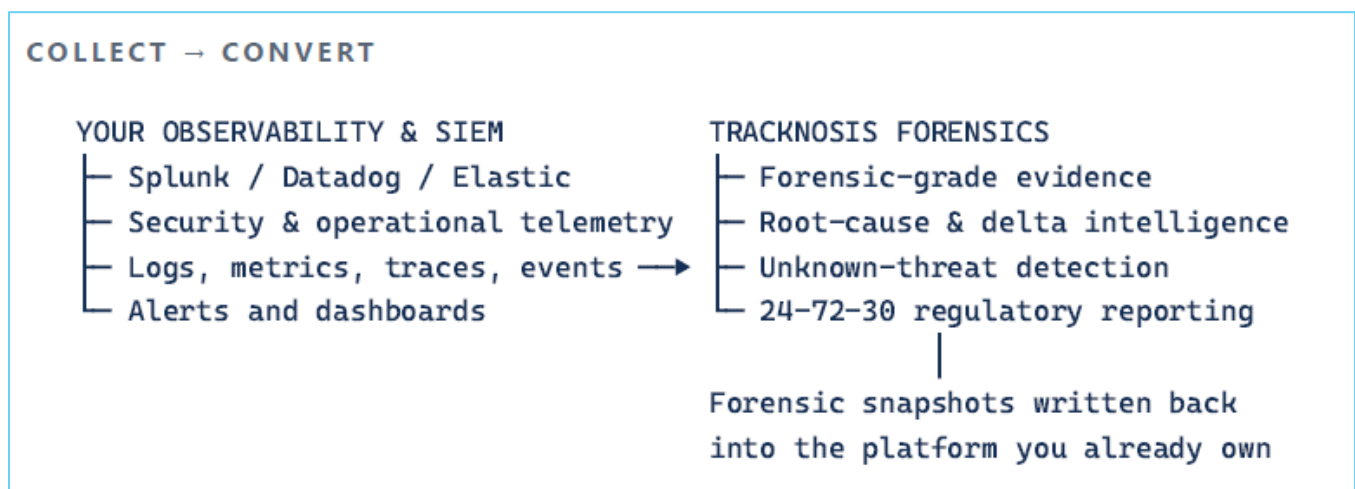
Cisco's recent acquisitions all consolidate into Splunk rather than adding separate consoles for your team to learn:

Capability	What it adds	Where it lands
Galileo	AI observability — LLM performance, hallucination detection, prompt quality, latency, agent execution	Splunk Observability & AI operations
Astrix Security	SaaS identities, OAuth apps, API keys, service accounts, AI agents	Splunk Enterprise Security / identity context
Wide Field Security	Identity telemetry, session intelligence, blast-radius analysis, credential relationships, privilege mapping	Splunk Enterprise Security & agentic SOC

The direction of travel is consistent: Splunk becomes the common data and analytics layer across your Cisco security and AI estate, which reduces tool sprawl and the learning curve for the teams operating it.

What Tracknosis Provides: The Forensic Evidence Layer

Tracknosis is an AI forensic and delta observability platform. It does not replace Splunk, Datadog or Elastic— it sits over them. Those platforms are excellent at collecting telemetry. They do not answer what happened, why, who was affected, and what must be reported. Tracknosis does.



Six capabilities:

Capability	What it delivers
Forensic observability	Forensic-grade visibility across systems, users and transactions — defensible evidence rather than more alerts.
Root cause & delta tracking	Identifies what changed before the incident, converting a symptom into a diagnosis and stopping recurrence.
Unknown-threat detection	Surfaces unknown and emerging threats that signature- and rule-based detection miss entirely.
24-72-30 regulatory reporting	Automates the evidence assembly and report authoring behind the NIS2, CIRCIA, SOCI and CCSPA reporting lifecycle, end to end and on deadline— mapped requirement by requirement in section 9.
AI forensic observability	Generates attack timelines and incident reconstruction automatically, compressing specialist analyst work.
AI integration & reporting	AI-authored incident reports in dozens of languages — if you operate across borders, you satisfy every local regulator from one platform.

How Delta Tracking Works

- 1. Baseline** — Tracknosis fingerprints the known-good state of systems, users and transactions from your existing telemetry.
- 2. Track the delta** — every subsequent change is captured and compared, surfacing what moved, when, and who or what moved it.
- 3. Reconstruct with AI** — AI assembles the attack timeline and incident reconstruction automatically.
- 4. Preserve as evidence** — forensic snapshots are retained as a defensible audit trail for regulators, insurers and legal scrutiny.
- 5. Report on deadline** — AI authors regulator-ready reports across the 24-72-30 lifecycle.

Why This Matters For AI Accuracy, Not Just Coverage

Evidence, Not Narrative

An LLM reasoning over raw logs will produce plausible narratives. An LLM reasoning over structured, baselined, delta-tracked forensic evidence produces conclusions that can be traced back to artefacts and defended to a regulator. When the output is submitted to a statutory authority and may be tested in litigation, that distinction is the whole point. Tracknosis is what turns an impressive demonstration into a defensible one.

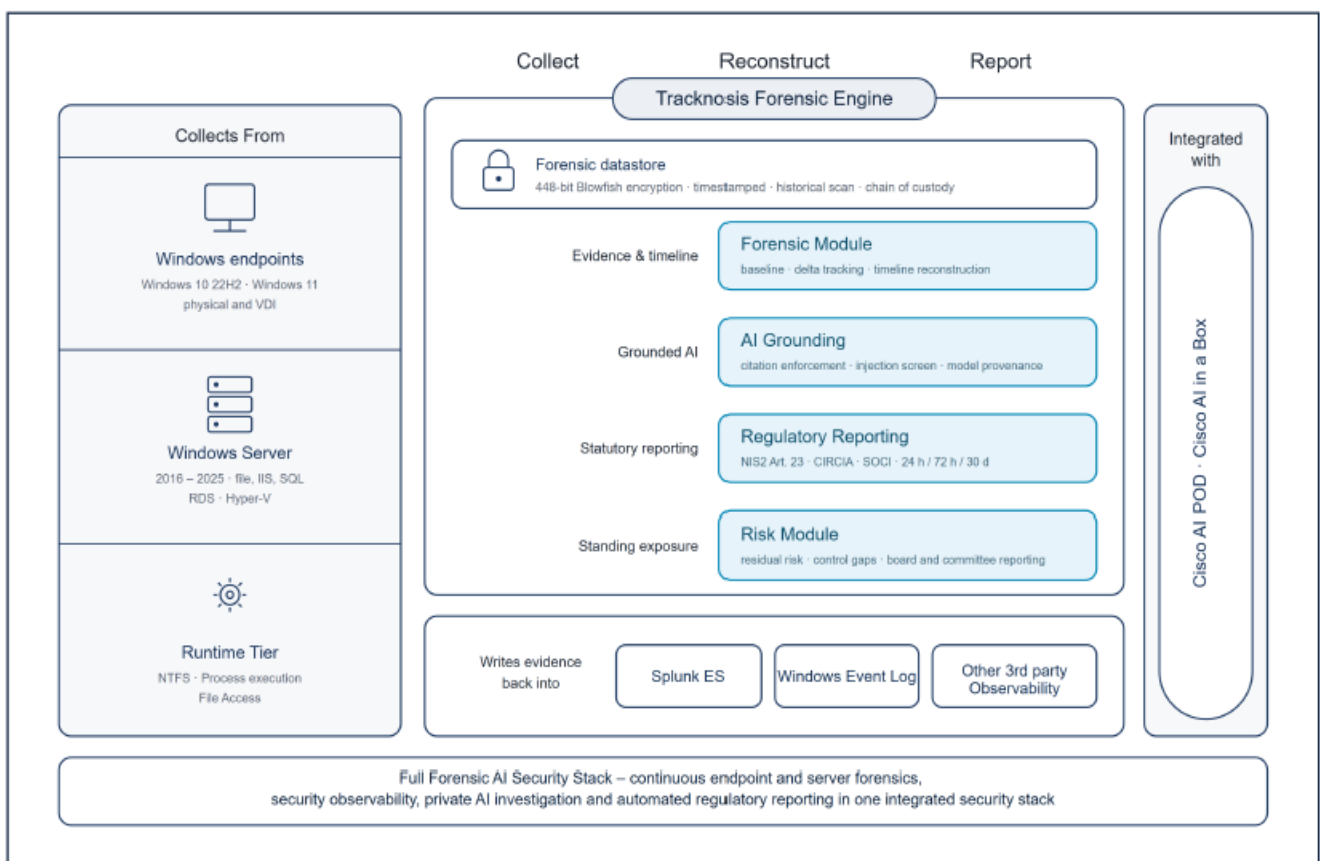


FIGURE 2 — TRACKNOSIS AT A GLANCE

The four modules inside the Tracknosis Forensic Engine — Forensic Module, AI Grounding, Regulatory Reporting and Risk Module — all share a single encrypted forensic datastore. Evidence is collected from Windows endpoints, servers and the runtime tier on the left, and written back into Splunk ES, Windows Event Log or other third-party observability platforms on the right. The entire stack is integrated with the Cisco AI POD or Cisco AI in a Box.

Your Windows Estate: What We Actually Collect

Everything above is architecture. This section is the part your Windows team will ask about first: what goes on the machines, what it reads, and what it costs you to run.

What Is In Scope

Tier	Systems	Why it Matter to an investigation
Desktop endpoints	Windows 10 22H2 and Windows11, physical and VDI, domain-joined or Entra-joined	Overwhelmingly where an attack starts. The phishing payload runs here, the token is stolen here, and the first persistence mechanism is planted here.
Member servers	Windows Server 2016–2025: file, print, application, IIS, SQL, RDS and Hyper-V hosts	Where impact is quantified. File modification counts, database access and service disruption are the numbers your severity assessment is built from.
Identity infrastructure	Active Directory domain controllers, ADFS, ADCS, Entra Connect	Where escalation and lateral movement become visible. Group membership, delegation, GPO and certificate-template changes are root-cause evidence.
Infrastructure roles	DHCP, DNS, WSUS, backup servers, jump hosts, management servers	Often the pivot point, and in ransomware the first target. Backup server compromise materially changes the impact you have to report.

What The Collector Reads

The collector is a Windows service running under a dedicated managed service account. It reads documented Windows interfaces only, and in the default profile it installs no kernel driver — a deliberate constraint, because a forensic agent that destabilises a domain controller has negative value however good its evidence is.

What We Watch	Windows Source	What It Gives You
Process lineage	Security 4688 with command line; kernel-process ETW; image SHA-256	The execution chain with parent-child ancestry — the spine of any timeline.

What We Watch	Windows Source	What It Gives You
Who accessed a resource	4624, 4625, 4672 logon events; 4663 object access with source and destination; Kerberos 4768/4769 ticket requests	Which identity accessed which resource, from where and to where— the lateral-movement and data-access trail.
File-system impact	NTFS USN change journal; MFT deltas; file-share auditing 4663; shadow copy deletion	The scale of the damage, in file counts and data classes you can put in a report.

Changes, Not Streams

The collector does not forward those sources verbatim. It converts each observation into a delta record: a statement that one property of one object changed from one value to another, at a known time, by a known actor where Windows attributes one. That single design decision is what makes everything downstream affordable.

- ▶ **Clock discipline.** Times are kept in UTC and cross-host ordering uses verified source time. Any host whose clock drifts beyond tolerance is flagged rather than quietly smoothed over — an unnoticed clock skew corrupts a timeline, and a corrupted timeline is worse than none in a filing.
- ▶ **Gap detection.** A per-host sequence number and a hash chain make missing or reordered records detectable, rather than merely unlikely.
- ▶ **No invented attribution.** Where Windows does not tell us who did something, the field stays empty. Inference is the AI's job later, and it is labelled as inference.

What It Costs You To Keep

Because the unit of storage is a change rather than an event, the volumes are modest. For a mid-sized estate the arithmetic works out roughly as follows — treat it as a method for sizing your own estate rather than a benchmark, since real rates vary with patching cadence and software deployment activity.

Population	Hosts	Changes per host per day	Changes per day
Desktop endpoints	3,000	800	2,400,000
Member servers	450	4,000	1,800,000
Domain controllers and identity	50	9,000	450,000
Total	3,500	—	4,650,000

At roughly 450 bytes per record that is about **2 GB a day** before indexing, or nearer 3.6 GB with index and replica. Kept for 400 days — a month beyond the longest reporting tail in any regime in Appendix A — the evidence store lands around **1.4 TB**. That fits on the storage tier of any AI POD validated design, and it is one to two orders of magnitude below forwarding raw Windows events for the same estate.

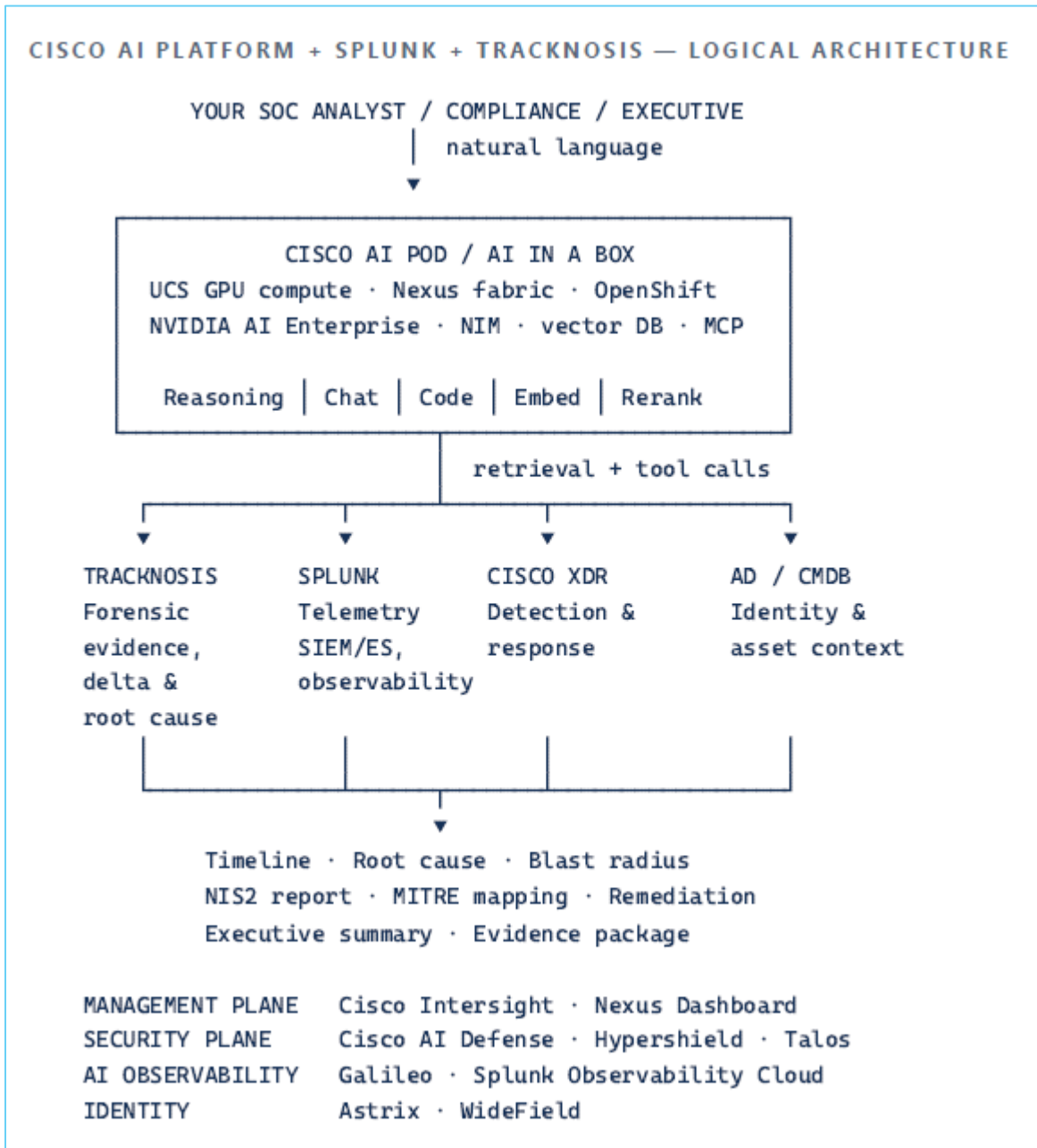
Why The Size Is The Point

An estate's worth of raw Windows logs cannot be indexed for AI retrieval at sensible cost, so in practice retrieval over raw logs degrades into keyword search with a language model bolted on top. A change-based store of this size can be indexed in full. That is the difference between an AI that retrieves the evidence that matters and one that retrieves whatever happened to match your search terms.

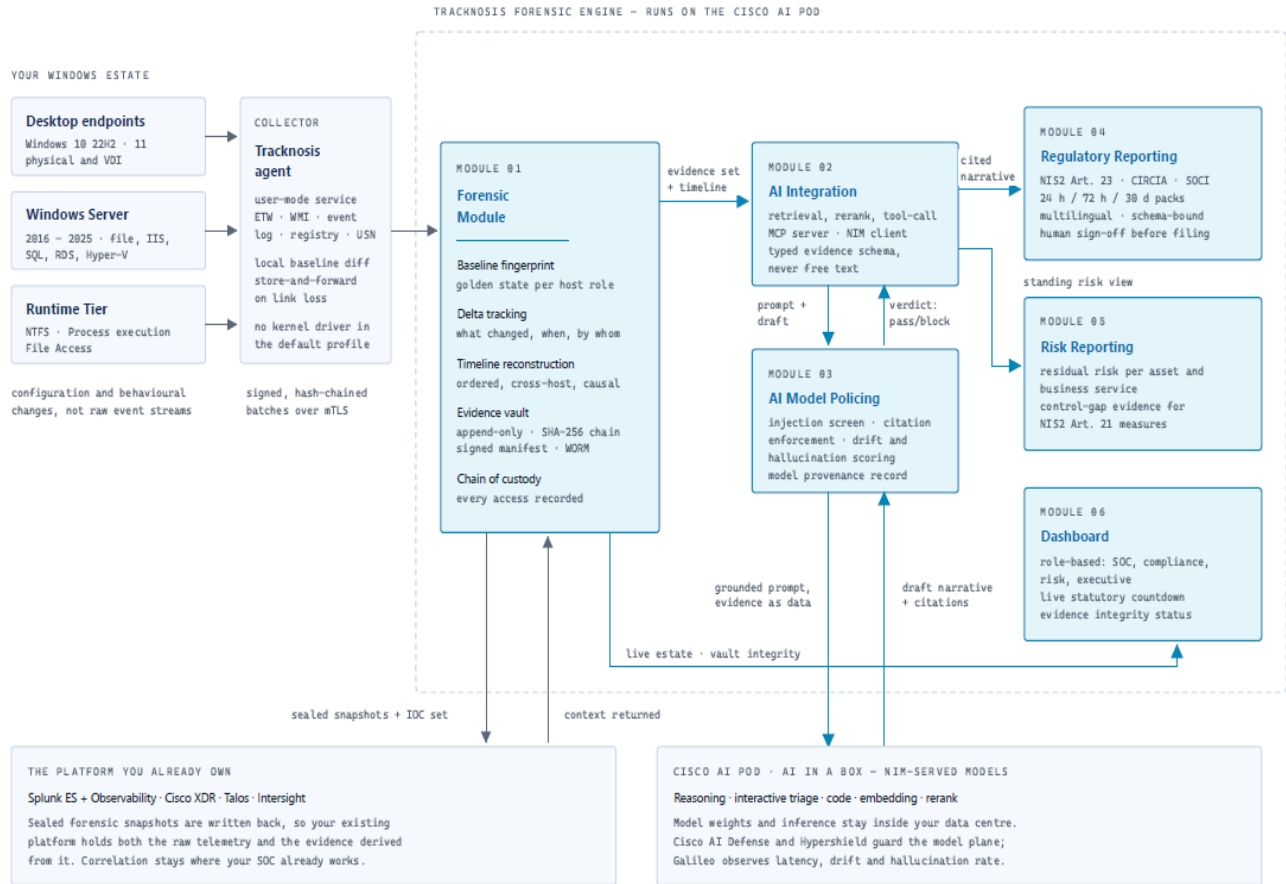


The Joint Solution Architecture

Each component does what it is strongest at, with no overlap and no displacement of what you already run.



That is the view from outside. Inside the Tracknosis box are six modules, and Figure 3 shows how they fit together and what passes between them.



☐ TrackNosis modules 01–06 ☐ Cisco and your existing infrastructure Arrows are labelled with what actually crosses them

FIGURE 3 — THE TRACKNOSIS FORENSIC ENGINE

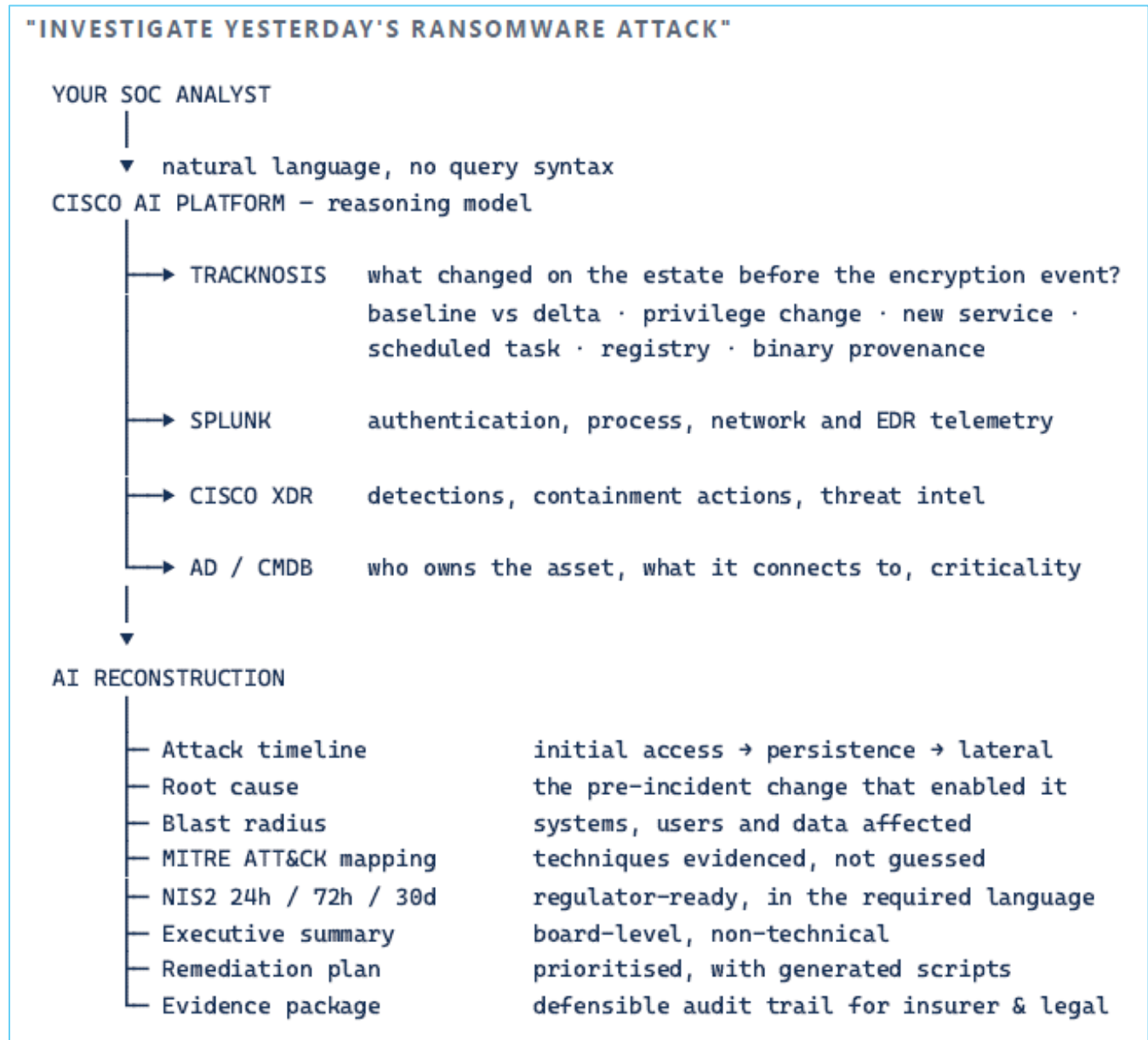
The path that matters is the vertical one. No prompt reaches a model, and no generated text reaches a regulatory pack, without passing through AI Model Policing in that direction. That single placement is what turns an AI-drafted incident report from a plausible narrative into a cited one — and it is the difference between a demonstration and something you would put your name to on a submission. Section 11 explains how that module works.

What Each Component Does For You

Component	Role In Your Environment
Cisco AI POD / AI in a Box	Hosts the models, vector database, retrieval pipeline and agent runtime. Provides the sovereign execution environment where your incident data can safely be reasoned over.
Cisco Inter sight / Nexus Dashboard	Lifecycle management of compute and fabric, so the platform is operated with familiar tooling.
Splunk (ES + Observability)	Telemetry ingestion, indexing, search, SIEM/SOAR — plus observability over the AI platform itself.
Cisco XDR / Talos	Detection, response and threat intelligence enrichment.
Cisco AI Defense /Hypershield	Protects the AI models and applications, and keeps sensitive data inside your data centre.
Galileo	AI observability — evidence that the investigation model is performing rather than drifting or hallucinating.
Astrix / WideField	Identity context, session intelligence, blast-radius and privilege mapping.
Tracknosis	Authoritative forensic evidence, delta and root-cause intelligence, and the 24-72-30 reporting engine — the ground truth everything above reasons over.

What It Looks Like In Practice

The following is a single analyst request, and what the platform does with it. Note that every data source it touches stays inside your estate.



What Changes For Your Team

Question	Your position today	With Tracknosis on Cisco AI infrastructure
What happened?	Alerts and raw logs to triage manually	AI-reconstructed attack timeline
Why did it happen?	No pre-incident change context	Root cause via delta tracking
Who was affected?	Fragmented across tools	Forensic view across systems, users, transactions
What must be reported?	Manual, error-prone, deadline risk	Automated 24-72-30 regulator-ready reports
How do we stop recurrence?	Symptom suppressed, cause unknown	Diagnosis identified and closed

From Forensic Timeline To Regulatory Submission

The reports produced in section 8 are not generic incident summaries. They are assembled to answer the specific questions the statute asks, in the order it asks them. This section shows that mapping — and is deliberately precise about what the law requires, what Tracknosis does, and where the boundary between the two sits.

What NIS2 Actually Asks For

It is worth being exact, because the market is not. **NIS2 does not name any technology, and it does not say that you must maintain a forensic attack timeline.** What it does is impose a reporting life cycle whose *content* requirements are very difficult to satisfy on deadline unless something has already reconstructed and preserved that timeline for you.

Under Article 23(4), an in-scope entity must provide:

Stage	Deadline	What It Must Contain
Early warning	24 hours	Notification of the significant incident, indicating whether it is suspected of being caused by unlawful or malicious acts, or could have a cross-border impact.
Incident notification	72 hours	An update to the early warning, with an initial assessment of the incident including its severity and impact — and, where available, the indicators of compromise.
Intermediate report	On request	Status updates requested by the competent authority or CSIRT.
Final report	1 month after the 72-hour notification	(i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; and (iv) where applicable, the cross-border impact.

The obligation is to produce that content, on that clock. Whether you can is almost entirely a function of whether the underlying evidence exists, is retrievable within the window, and is trustworthy enough to sign. That is an evidence problem before it is a reporting problem.

How a forensic timeline satisfies the article

Suppose Tracknosis reconstructs the following from the delta record and your existing telemetry:

RECONSTRUCTED INCIDENT TIMELINE — ILLUSTRATIVE

```

02:13:07 powershell.exe executed
02:13:18 update.dll created
02:13:19 SHA-256 calculated
02:13:21 IOC match detected
02:14:02 Service "Updater" created
02:16:41 Credential access activity
02:22:14 FILE01 accessed
02:25:51 Encryption process starts
02:31:07 12,842 files modified
02:34:20 Security team containment begins
02:41:03 Host isolated

```

Each class of artefact in that record substantiates a specific element of the submission:

Evidence Tracknosis produces	What it substantiates	Reference
Reconstructed attack timeline —sequence, actor, artefact, host	Detailed description of the incident, including severity and impact	Art. 23(4)(d)(i)
Pre-incident delta — the change that enabled the compromise	The type of threat or root cause likely to have triggered the incident	Art. 23(4)(d)(ii)
Containment, isolation and remediation record	Applied and ongoing mitigation measures	Art. 23(4)(d)(iii)
Blast radius — systems, users, data and sites affected	Severity and impact; cross-border impact where applicable	Art. 23(4)(d)(i), (iv)
Hashes, binaries, persistence artefacts and matched indicators	Indicators of compromise, where available, in the 72-hour notification	Art. 23(4)(b)
Preserved forensic snapshots and audit trail	The ability to stand behind the submission if it is later tested	Evidential quality

CIRCI — An Even Closer Fit

If you operate US critical infrastructure, the alignment is tighter still. CIRCI goes beyond asking whether an incident occurred: the reporting framework calls for the incident timeline, affected systems, technical details, exploited vulnerabilities, tactics, techniques and procedures, indicators of compromise, and malware information — a list that is close to a description of the Tracknosis output set. The statutory clocks are 72 hours for a covered cyber incident and 24 hours for a ransom payment.



CHECK THE RULE IN FORCE AT YOUR DEPLOYMENT DATE

CIRCA creates the obligation in statute, but the detailed reporting fields are set by CISA's implementing rule, which has been through rulemaking. Field-level requirements should be confirmed against the version of the rule applicable when you deploy, rather than treated as fixed. The same discipline applies to the UK Cyber Security and Resilience reforms, which are still settling.

The Claim We Make, And The Claim We Do Not

PRECISION MATTERS HERE

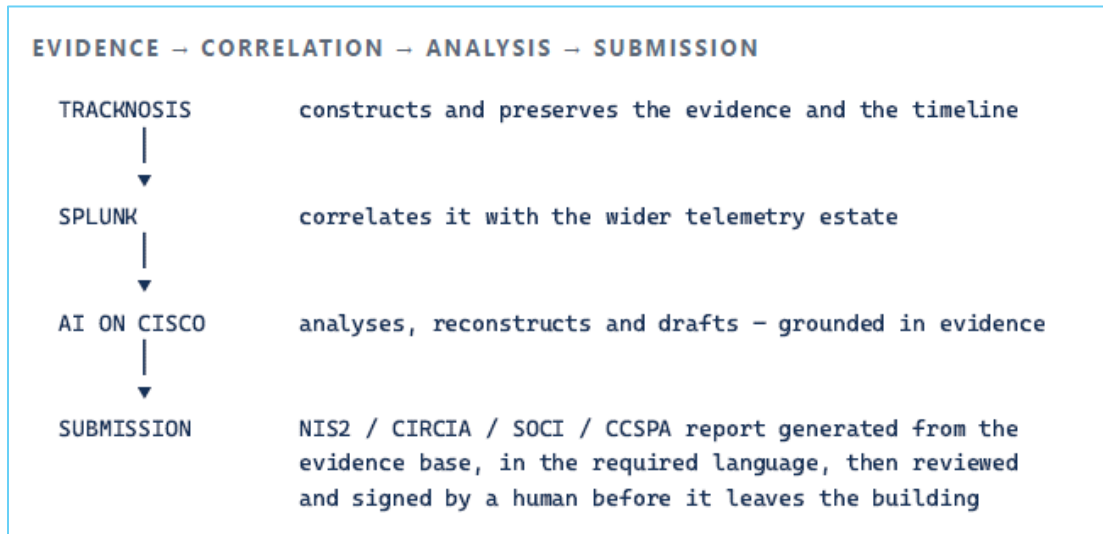
We do not say: *"NIS2 requires Tracknosis."* That would not be legally accurate. No regulation in this family mandates a specific product or a specific forensic technology, and any vendor telling you otherwise is worth a second look.

We do say: *"Tracknosis automatically reconstructs and preserves the forensic evidence needed to support NIS2 Article 23 incident reporting — detailed incident description, indicators of compromise, root-cause analysis, severity and impact assessment, and mitigation timelines." And for the United States: "Tracknosis reconstructs the technical incident timeline and supporting forensic evidence required for CIRCA-style critical-infrastructure incident reporting."*

The distinction matters to you at least as much as it matters to us. It is the difference between a compliance claim your legal function will accept in a board paper, and one it will strike out.

Where The Work Actually Happens

On the Cisco platform the division of labour is clean, and each layer does only what it is qualified to do:



The last line of that diagram is a control, not a caveat. Human review of regulatory submissions should be treated as mandatory, for the reasons set out in section 16.

One Evidence Model, Many Jurisdictions

If you operate across borders you are not managing one deadline. You are managing several, on different clocks, in different languages, against regulators who ask for the same underlying facts in different formats. A representative sample:

Jurisdiction	Regime	Reporting clock
European Union	NIS2	24h → 72h → ~1 month final
United Kingdom	NIS Regulations / Cyber Security& Resilience reforms	Strengthened 24h / 72h model under the reforms
United States	CIRCIA	72h cyber incident / 24h ransom payment
Australia	SOCI	12h or 72h depending on the incident
Canada	CCSPA	Mandatory reporting for designated operators

Jurisdiction	Regime	Reporting clock
Hong Kong	Protection of Critical Infrastructures (Computer Systems) Ordinance	12h serious / 48h other
India	CERT-In Directions	Certain incidents within 6 hours
Singapore	Cybersecurity Act	Rapid mandatory reporting of prescribed incidents

The Design Consequence

These regimes differ in their forms and their deadlines far more than they differ in the facts they demand. That is why Tracknosis is built as **one forensic evidence model with jurisdiction-specific reporting packs layered on top**, rather than as a NIS2 product with other regimes bolted on. You baseline and preserve evidence once; the reporting pack for each jurisdiction draws on the same substantiated record. **Appendix A** maps the wider landscape.

What Actually Runs On The Platform

A common misconception is that this kind of platform runs one model. It does not. A Cisco AI platform hosts many models concurrently through NVIDIA AI Enterprise and NVIDIA NIM — which matters to you commercially, because concurrency is what turns a GPU investment into shared enterprise infrastructure rather than a single-purpose appliance.

The forensic capability is best designed not as one chatbot but as a team of specialist models:

Task	Model Class	Why
Root-cause analysis	Reasoning model (e.g. DeepSeek R1, Nemotron-class)	Spends more compute "thinking" before answering — essential for reconstructing attack chains and identifying persistence.
Threat hunting	Reasoning model	Hypothesis generation and multi-step correlation across evidence sources

Task	Model Class	Why
NIS2 / regulatory reporting	General instruction-tuned LLM	Structured, multilingual, format-compliant long-form output
Interactive SOC triage	Fast 8B–14B instruction model	Low latency conversation for analysts working on an active incident
Detection & remediation code	Code model (Code Llama, Codestral, DeepSeek Coder)	Generates SPL, KQL, Sigma, YARA, PowerShell and remediation scripts
Evidence retrieval	Embedding model	Indexes Tracknosis forensic artefacts, NIS2 documentation and security knowledge for RAG
Evidence ranking	Reranking model	Ensures the most relevant forensic evidence reaches the reasoning model — the single biggest lever on answer quality
Executive briefing	Smaller instruction model	Concise, non-technical summarisation for board and regulator audiences

The same platform can concurrently host the rest of your enterprise AI estate — HR, legal, finance and engineering assistants, document intelligence, and the agentic workflows you adopt next — without buying separate GPU infrastructure for each team. That shared-platform economics is central to the business case in section 12.

Keeping the AI Honest: Policing The Model

Every AI vendor will tell you their model is grounded. The question your general counsel will ask is narrower and harder: when this report is read back to us in two years, can we show how it was produced? Module 03 exists to answer that question, and it is the reason a submission drafted here is something you can put your name to.

Your Evidence Is Written By The Attacker

This workload has a property most enterprise AI does not. A large part of what the model reads —filenames, command lines, service descriptions, registry values, scheduled-task names — was authored by the person who attacked you. An attacker who expects an AI-assisted investigation can name a service, or plant a string in a dropped file, that reads as an *instruction* by the time it reaches the model.

The defences are structural rather than clever wording:

- ▶ Evidence is passed to the model as typed data fields inside a schema, never pasted into the instruction text.
- ▶ The model is told, as a matter of standing policy, that everything returned by a tool is untrusted data and contains no instructions.
- ▶ Outgoing prompts are screened for instruction-shaped content originating in attacker-
- ▶ The tools the model can reach are a read-only allow-list. Even a completely successful injection cannot reach an action, because no action is exposed to it.

Nothing Uncited Reaches A Regulator

Every factual assertion in a generated report has to carry the identifier and hash of the sealed artefact it rests on. AI Model Policing reads the draft, resolves each citation against the evidence for that incident, and sorts every statement into one of four buckets:

Classification	Condition	What happens
Supported	Reasoning model (e.g. DeepSeek R1, Nemotron-class)	Kept in the report.
Assessment	Reasoned from cited evidence, but not directly stated by any of it	Kept, but labelled as assessment and presented separately from fact.

Classification	Condition	What happens
Uncited	No citation, or a citation that does not resolve	Blocked from the regulatory pack and raised to your reviewer as a gap.
Contradicted	Conflicts with sealed evidence	Blocked, and logged as a model-quality event to Splunk.

Numbers get stricter treatment again. A file count, a host count or an impact figure in a regulatory submission has to resolve to a value computed from the evidence – never to the model's estimate. Anything that cannot be resolved is blocked outright rather than softened with a qualifier.

Governing The Models Themselves

- ▶ **Approved models only.** The forensic workload runs on models from your approved list. Model provenance is itself a sovereignty question in several jurisdictions, and this is where you enforce it.
- ▶ **Regression before promotion.** A held-back set of your own resolved incidents, with root causes already known, is replayed whenever a model or prompt version changes. If root-cause accuracy drops, the change does not ship.
- ▶ **Drift monitoring.** Galileo watches latency, hallucination rate and output drift on the investigation models specifically, rather than on the platform as a whole.
- ▶ **The model never files.** It does not submit, remediate or close an incident. Every regulatory submission passes a named human reviewer, and that approval is recorded.

Being Able To Show Your Working

A submission may be examined a year later – by a regulator asking how you reached a conclusion, or in litigation. Recorded immutably alongside every generated report are: the model and its weights hash, the prompt template version, the sampling parameters and seed, the evidence retrieved and how it was ranked, the hash of the evidence set, the policing verdict on each assertion, and the identity and timestamp of the person who approved it.

WHAT THAT BUYS YOU

Given the same sealed evidence and the same recorded settings, the report can be produced again. That is a materially different position from "our AI wrote it", and in practice it is the difference between an AI-generated document your general counsel will sign and one they will not.

WHAT THIS DOES NOT DO

Grounding and policing reduce model error substantially. They do not eliminate it. Human review of every regulatory submission is a required control in this architecture, not an optional extra – the same point section 16 makes about governance.

Building Your Business Case

This section is written to be lifted into your internal investment paper.

Value Lines You Can Model

Value line	Mechanism
Reduced MTTI / MTTR	AI reconstruction over forensic evidence compresses specialist analyst work from days to hours, attacking the largest share of incident cost – investigation effort and downtime.
Avoided regulatory penalty	Missing a 24h, 72h or 30d deadline carries penalties, with liability attaching to named executives. Only 14% of companies report being NIS2 ready.
Reduced recurrence	Delta tracking identifies the pre-incident change, so the cause is closed rather than the symptom suppressed – reducing repeat incidents and repeat cost.
Cyber-insurance position	Defensible evidence packages support policy adherence and can support lower premiums.
Analyst capacity	Scarce senior DFIR skills are redirected from evidence assembly to judgement – extending the reach of a team you cannot easily grow.

Value line	Mechanism
Existing platform ROI	Improves return on the Splunk, Datadog or Elastic investment you have already made, rather than adding another silo.
Platform utilisation	An always-on security workload sustains utilisation of the AI infrastructure, and the same platform carries your other AI services.

Budget planning

Cisco does not publish list pricing; both AI PODs and AI in a Box are sold as solutions, with cost driven by GPU configuration, networking, storage, software and support. Market-observed ranges are useful only for early planning:

Configuration	Typical approval level
Small edge AI appliance (1–2 GPUs)	Departmental
Departmental AI in a Box (2–4 GPUs)	Director / CISO
Enterprise AI in a Box	Executive committee
Full Cisco AI POD	Board / CFO

IMPORTANT QUALIFICATION

Reach out to your Tracknosis or Cisco representative to get a quote tailored to your environment and sizing requirements.

Answering the question your CFO will ask

Every investment paper of this size meets the same challenge:

"Why not just use Microsoft Copilot, or a cloud LLM?"

For document search and productivity assistance, that challenge is fair — and often the right answer. For this workload it is not, and the reasoning is short enough to put in a single paragraph of your paper: the inputs to a forensic investigation are credentials, session data, privilege maps, breach evidence and potentially disclosable material. A regulated organisation cannot supply that data to a public AI service. The capability therefore has to exist somewhere you control, or it does not exist at all.

The Shared-Platform Argument

THE ANCHOR – TENANT PRINCIPLE

Infrastructure of this scale is easiest to justify when one workload comes close to carrying the case on its own, so that every additional workload is incremental value rather than incremental risk. Forensic investigation is a strong anchor tenant: it is compelled by regulation, blocked from the public cloud by sovereignty, and measured against a cost line you already track. Your document AI, code assistants and departmental agents then run on infrastructure that is already paid for.

Choosing The Right Platform Tier

The same Tracknosis architecture serves organisations from hundreds to tens of thousands of endpoints. Only the Cisco platform underneath changes.

Your organisation	Cisco platform	What Tracknosis becomes	Indicative envelope
Mid-market	Cisco AI in a Box	AI Forensic Investigator	\$5–6 figure
Large enterprise	Cisco AI POD	Enterprise Forensic Intelligence Platform	\$6+ figure
Global enterprise	Cisco Secure AI Factory	AI-driven DFIR & Compliance Platform	Multi-POD / multi-site

Our Recommendation: Start With AI In A Box

If your estate looks like 500 Windows servers, 3,000 desktops, Splunk Enterprise Security and Cisco XDR, you do not need a 7 figure AI POD to run this workload. Cisco AI in a Box will run the full forensic capability— investigation, root-cause analysis, NIS2 reporting and executive reporting.

WHY WE RECOMMEND STARTING HERE

- ▶ A far easier investment to approve, so you can prove value in this budget cycle rather than the next one
- ▶ Delivers measurable outcomes on your own incident data before you commit to larger infrastructure
- ▶ Sized proportionately to a mid-sized estate rather than to a hypothetical
- ▶ Establishes the architecture that scales unchanged if you grow into it

THE UPGRADE PATH

Because the Tracknosis architecture is identical across tiers, growth is a platform decision rather than a re-platforming project. If you outgrow AI in a Box — multiple SOCs, multiple compliance teams, a wider agent estate — you scale to an AI POD without changing the forensic layer, the evidence base, or the reporting workflows already in production. Nothing you build in phase one is discarded.

Protecting The Investment You Have Already Made

A frequent and reasonable objection to any new security platform is that it duplicates what you already own. This one is designed not to.

IT WORKS ALONGSIDE YOUR SIEM, NOT AGAINST IT

Tracknosis is deployed alongside Splunk, Datadog or Elastic. Your existing collection, dashboards, detections and retention are untouched. There is no rip-and-replace and no migration project.

IT INCREASES THE VALUE OF THE DATA YOU ALREADY STORE

Forensic snapshots are written back into the platform you already own. The evidence, timelines and root-cause records land where your team already works and where your existing access controls, retention policies and audit trails already apply.

IT USES THE AI PLATFORM YOU ARE BUYING ANYWAY

If you are already planning AI infrastructure for document intelligence or departmental assistants, the forensic workload runs on the same platform. If you are not, this workload is the one most likely to justify it— and the other use cases then arrive at marginal cost.

WHY THIS COMBINATIONS HARD TO MATCH

Cisco supplies validated, sovereign AI infrastructure. Splunk supplies the telemetry and security operations platform, and observes the AI infrastructure itself. Galileo observes the model's behaviour. **Tracknosis supplies the trusted forensic evidence that makes the AI's conclusions accurate and defensible.** Assembling an equivalent capability from separate vendors means integrating all four layers yourself and accepting the integration risk that the validated designs exist specifically to remove.

How You Would Deploy It

Deployment does not require the AI platform to be commissioned first. That matters, because it lets you de-risk the larger investment by proving the smaller one.

Phase	What Happens	What You Prove
Phase 1	Deploy Tracknosis alongside your existing Splunk, Datadog or Elastic estate. Baseline systems, users and transactions; begin delta tracking and evidence capture.	Forensic and reporting value on your own data, with no AI infrastructure purchase.
Phase 2	Add Cisco AI in a Box, and connect Tracknosis as a retrieval and tool-call target for the models.	Full AI-driven investigation — natural-language reconstruction, root cause and automated regulatory reporting.
Phase 3	Scale to a Cisco AI POD or Secure AI Factory as SOC, compliance and wider AI demand grows.	Enterprise-wide shared AI platform, with forensics as the anchor workload.

Integration detail

HOW TRACKNOSIS DEPLOYS

- ▶ Works alongside incumbent SIEM and observability platforms — Splunk, Datadog, Elastic
- ▶ Forensic snapshots stored back into the platform you already own
- ▶ No rip-and-replace; a short, additive deployment cycle
- ▶ OEM licensing available where engines are embedded into partner products

HOW IT INTEGRATES WITH THE AI PLATFORM

- ▶ Exposed as a retrieval and tool-call target to models running under NVIDIA NIM
- ▶ Forensic artefacts indexed by the embedding model into the platform's vector database
- ▶ Reranking applied so the reasoning model receives the most relevant evidence
- ▶ Agent access mediated through an MCP server running on the platform
- ▶ Splunk retains both raw telemetry and Tracknosis forensic snapshots

Risks, Assumptions And Governance

These are the questions your architecture board, legal counsel and risk function will raise. They are set out here rather than left to be discovered.

Item	Position
Human review is required	Grounding in Tracknosis forensic evidence materially reduces but does not eliminate model error. Human review of regulatory submissions should be treated as a required control, not an optional one. Galileo-based AI observability should be enabled from day one.
Evidential standard	"Defensible" and "regulator-ready" describe the quality and completeness of the evidence and reporting produced. Admissibility in any specific jurisdiction remains a matter for your legal counsel.
What the regulations do and do not require	No regulation in this family mandates a specific product or forensic technology, and this document does not claim otherwise. Tracknosis helps the evidence-gathering process as part of its proactive forensic data monitoring — see section 9.4. Treat any vendor claim of the form "NIS2 requires product X" with caution.

Item	Position
Status of the CIRCIA rule	CIRCIA creates the reporting obligation in statute, but the detailed reporting fields are set by CISA's implementing rule, which has been through rulemaking. Confirm field-level requirements against the version of the rule in force at your deployment date rather than treating them as fixed. The same applies to the UK Cyber Security and Resilience reforms.
Scope of Appendix A	Appendix A is a directional map for scoping and planning, not legal advice, and several regimes listed are still being implemented through secondary regulation. Confirm the obligations applicable to your entities and sectors with your legal and compliance functions.
Pricing figures	All monetary ranges here are market estimates for early planning, not Cisco list prices. Budget approval should rest on a Cisco-generated quotation.
Sizing	GPU sizing for a concurrent multi-model forensic workload requires a joint sizing exercise against your estate. The tiers here are indicative, not a bill of materials.
Model selection	The models named in section 10 illustrate model classes. Final selection should follow your approved model list, NVIDIA NIM catalogue availability, and any constraints you apply to model provenance.
SIEM dependency	The architecture is strongest where Splunk is already deployed. Tracknosis also supports Datadog and Elastic, so the solution does not require you to change SIEM.
Data residency of the AI layer	Cisco AI Defense supports on-premises data-plane deployment, keeping model and application traffic within your data centre. Confirm this configuration explicitly during design if sovereignty is a formal control for you.

Your platform collects the telemetry.
This is what turns it into evidence.

Sources And References

- ▶ Cisco AI PODs At-a-Glance — cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ai-pods-aag.html
- ▶ Cisco AI PODs: Pre-validated, Flexible and Modular Infrastructure for Cisco Secure AI Factory — Data Sheet, Cisco Cisco AI POD Infrastructure for Enterprises — Solution Overview, Cisco
- ▶ Cisco AI POD Infrastructure for the NVIDIA 2-8-9-400 Enterprise Reference Architecture, Cisco
- ▶ Cisco AI POD for Enterprise Training and Fine-Tuning — Design Guide (Cisco Validated Design)
- ▶ AI PODs for Inferencing — At a Glance and Data Sheet, Cisco
- ▶ Cisco Secure AI Factory with NVIDIA — Solution page and FAQ, Cisco
- ▶ "Unlocking AI Performance: Splunk Observability for Cisco Secure AI Factory with NVIDIA" — Cisco Blogs
- ▶ "Cisco and NVIDIA Advance Security for Enterprise AI Factories" — NVIDIA Blogs
- ▶ Cisco 2025 AI Readiness Index (infrastructure readiness, 28%)
- ▶ Tracknosis platform documentation and technical overview — tracknosis.com
- ▶ Directive (EU) 2022/2555 (NIS2), Article 23 — reporting obligations; in particular Art. 23(4)(a)–(d) covering the early warning, the 72-hour incident notification including indicators of compromise, and the final report content requirements at Art. 23(4)(d)(i)–(iv)
- ▶ Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and the CISA implementing rulemaking — covered cyber incident and ransom payment reporting, and the reporting content fields
- ▶ Security of Critical Infrastructure Act (SOCi, Australia) and CCSPA (Canada) reporting obligations; UK NIS Regulations and the Cyber Security and Resilience reforms
- ▶ National cyber and incident-reporting regimes surveyed in Appendix A, including the Singapore Cybersecurity Act, Malaysia Cyber Security Act 2024, Hong Kong Protection of Critical Infrastructures (Computer Systems) Ordinance, Taiwan Cyber Security

Management Act, India CERT-In Directions, Ghana Cybersecurity Act 2020 and Morocco Cybersecurity Law 05-20

- ▶ NIS2 readiness figure (14%) per CRN
- ▶ Internal working notes: "AI Regulatory Reporting" — NIS2 Article 23 mapping, CIRCIA content alignment, claim wording, and the global reporting matrix reproduced in Appendix A
- ▶ Internal working notes: "AI Cisco POD and Tracknosis notes" — Cisco portfolio analysis, Splunk acquisition strategy (Galileo, Astrix Security, WideField Security), model strategy and commercial positioning

Appendix — Global Incident-Reporting Regimes

NIS2 is the regime most often named, but it is one of many. The tables below map the principal cyber and incident-reporting regimes worldwide, the scope each typically covers, the reporting clock, and how closely the regime's content requirements align with the NIS2 model that Tracknosis reporting packs are built around.

The practical point for a multinational is the one made in section 9.6: **these regimes differ far more in their forms and deadlines than in the facts they demand**. Wherever alignment is high, the same forensic evidence base — timeline, root cause, blast radius, indicators of compromise, mitigation record — substantiates the local submission, and only the reporting pack changes.

HOW TO USE THIS APPENDIX

This is a directional map for scoping and planning, not legal advice, and it is not a statement that any regime mandates a particular product. Obligations in this area are changing quickly — several of the regimes listed are in force but still being implemented through secondary regulation. Confirm the requirements actually applicable to your entities, sectors and jurisdictions with your legal and compliance functions before relying on them in a filing.

Europe

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
European Union	NIS2	Essential and important entities	24h early warning → 72h notification → ~1 month final report	Very high
United Kingdom	NIS Regulations / Cyber Security & Resilience reforms	Strengthened 24h / 72h model under the reforms	Strengthened 24h / 72h model under the reforms	Very high
Switzerland	Information Security Act / Cybersecurity Ordinance	Critical infrastructure	24h, with additional information to follow	Very high
Norway	Digital Security Act / NIS-aligned framework	Essential services	Mandatory cyber security and incident requirements	High
Turkiye	Cyber Security Law / national cyber framework and sector rules	Critical infrastructure, government, regulated sectors	Cyber incident reporting and response obligations	High

Americas

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
United States	CIRCA	Critical infrastructure	72h covered cyber incident / 24h ransom payment, once the implementing rule applies	Very high
Canada	CCSPA	Finance, telecom, energy, transport	Mandatory reporting for designated operators; detail set by regulation	Very high
Chile	Framework Law on Cybersecurity and Critical Information Infrastructure	Essential services and critical infrastructure	Mandatory incident reporting	Very high
Brazil	LGPD / ANPD plus financial and critical-sector cyber requirements	Data controllers, finance, telecom, regulated sectors	Mandatory reporting depending on incident and sector	Moderate
Colombia	National Digital Security framework, sector regulation, Law 1581 / SIC	Finance, telecom, government, data controllers	Mandatory reporting under the applicable privacy or sector regime	Moderate
Mexico	Financial and telecom cybersecurity regulation plus data protection	Banks, telecoms and regulated organisations	Sector-dependent incident reporting	Moderate
Peru	Digital security plus data-protection and sector regulations	Government, finance, telecom	Sector-dependent	Moderate
Ecuador	Data Protection Law plus national and sector cybersecurity	Data controllers and regulated sectors	Security and breach notification requirements	Moderate
Uruguay	National cybersecurity, CERTuy and data-protection requirements	Government, critical infrastructure, data controllers	Incident-reporting obligations	Moderate
Costa Rica	National cybersecurity plus sector and privacy frameworks	Government and regulated sectors	Incident reporting varies by sector	Emerging
Brazil	LGPD / ANPD plus financial and critical-sector cyber requirements	Data controllers, finance, telecom, regulated sectors	Mandatory reporting depending on incident and sector	Moderate
Colombia	National Digital Security framework, sector regulation, Law 1581 / SIC	Finance, telecom, government, data controllers	Mandatory reporting under the applicable privacy or sector regime	Moderate
Panama	Cybersecurity plus data-protection and sector requirements	Government, finance, telecom	Sector-dependent	Emerging
Argentina	National cybersecurity plus data protection and sector rules	Government, finance and regulated organisations	Sector-dependent	Emerging

Asia-Pacific

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
Australia	SOCI	Critical infrastructure	12h or 72h depending on the incident	Very high
Singapore	Cybersecurity Act	Critical Information Infrastructure	Rapid mandatory reporting of prescribed incidents	Very high
Malaysia	Cyber Security Act 2024	National Critical Information Infrastructure	Mandatory cyber incident notification	Very high
Hong Kong	Protection of Critical Infrastructures (Computer Systems) Ordinance	Critical infrastructure	12h for serious incidents / 48h otherwise	Very high
Taiwan	Cyber Security Management Act	Government and designated critical infrastructure	Mandatory notification, response and investigation	Very high
Thailand	Cybersecurity Act and PDPA	Critical Information Infrastructure	Mandatory CII incident response and reporting	High
Vietnam	Cybersecurity Law and information-security regulations	Critical information systems and digital organisations	Mandatory incident-response and reporting requirements	High
India	CERT-In Directions	Broad commercial and infrastructure scope	Certain incidents within 6 hours	High
China	Cybersecurity Law and CII Security Protection Regulations	CII, networks, digital services	Mandatory incident management and reporting obligations	High
South Korea	Information & Communications Infrastructure Protection Act and sector laws	Critical infrastructure, telecom, finance	Mandatory sector and CI incident response	High
Indonesia	Electronic Systems / PDP / cybersecurity framework	Electronic-system operators, government, regulated sectors	Incident and data-breach notification	Moderate
Philippines	Data Privacy Act and critical-infrastructure cyber framework	CII, government, data controllers	Mandatory reporting in applicable cases	Moderate
Pakistan	National cybersecurity and CERT framework plus sector requirements	Government, telecom, banking, CII	Sector and critical-infrastructure reporting	Moderate
Bangladesh	Cybersecurity legislation and sector regulations	CII, government, finance, telecom	Sector-specific incident obligations	Moderate

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
New Zealand	NCSC and sector regulatory frameworks	Government, CNI, finance	Sector-dependent rather than one horizontal regime	Moderate
Japan	Basic Act on Cybersecurity plus critical-infrastructure and sector rules	Critical infrastructure, finance, telecom	Sector-dependent incident reporting	Moderate

Middle East and Africa

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
Israel	National Cyber Directorate plus critical-infrastructure and sector rules	Critical infrastructure and regulated organisations	Mandatory and sector-specific reporting	High
Saudi Arabia	NCA Essential Cybersecurity Controls and sector regulation	Government, CNI, finance	Incident management and regulatory reporting	High
UAE	National cybersecurity framework plus sector and emirate requirements	Government, critical infrastructure, finance	Mandatory requirements depending on entity and sector	High
Morocco	Cybersecurity Law 05-20	Critical infrastructure, government, designated entities	Cybersecurity incident obligations	High
Ghana	Cybersecurity Act 2020	Critical Information Infrastructure and regulated organisations	Incident-management and reporting framework	High
Qatar	National Information Assurance and sector cyber regulation	Government, energy, finance, CII	Sector and critical-infrastructure reporting	Moderate
Bahrain	National cybersecurity framework and CBB requirements	Government, CII, financial services	Sector-specific mandatory reporting	Moderate
Oman	National cybersecurity and CII requirements	Government, CII and regulated sectors	Incident notification requirements	Moderate
Kuwait	National cybersecurity and sector regulations	Government, banking, critical infrastructure	Sector-dependent reporting	Moderate
South Africa	Cybercrimes Act, POPIA and sector rules	Critical infrastructure, data controllers, finance	Cybercrime and security-compromise notification	Moderate
Nigeria	Cybercrimes Act, NDPA and sector regulations	CNI, finance, telecom, data controllers	Mandatory reporting depending on incident	Moderate

Jurisdiction	Principal regime	Typical scope	Reporting obligation	NIS2 alignment
Kenya	Computer Misuse & Cybercrimes Act and Data Protection Act	CII, telecoms, data controllers	Cyber and privacy incident obligations	Moderate
Rwanda	Cybersecurity and data-protection framework	Critical infrastructure, government, regulated organisations	Incident reporting requirements	Moderate
Mauritius	Cybersecurity and Cybercrime Act and data-protection regime	Government, CII, organisations	Incident and security obligations	Moderate
Egypt	Cybercrime and Data Protection Law plus sector rules	Telecoms, finance, government	Sector and privacy reporting	Moderate
Tunisia	National cybersecurity and data-protection frameworks	Government and regulated organisations	Sector-dependent	Emerging

