EventLake

THE PLATFORM BOOKLET · 2026

One platform, one event model, one meter.

What security looks like when the system that observes your estate is also the system that acts on it — and both work from the same record of what happened.

01 · THE STARTING POSITION

Nobody chose the estate they are running.

It accumulated — by acquisition, by incident, by the tool that was best in its category the year it was bought. Each part is defensible on its own. The problems live in the seams between them.

Correlation is a mapping exercise

Four record shapes joined onto a common schema, and the fields none of them share are dropped before anyone knows which query will need them.

Detection and response are separate systems

The thing that notices sends a message to the thing that acts. The gap between them is measured in human minutes, every time.

Evidence is reconstructed, not held

An alert stores a query rather than the events that justified it, so the explanation quietly decays as retention windows roll past it.

Six meters, six renewals

Per GB, per endpoint, per seat, per asset, per user, per store. The cost of six products is not six invoices; it is six negotiations and six versions of the truth.

> The predictable consequence: **single-domain detections work well and cross-domain detections do not.** The sequence where a document spawns a process that assumes a cloud role and reads a bucket is three records in three shapes — and joining them was a decision made years earlier by someone optimising for storage.

02 · THE SHAPE OF THE PLATFORM

Two planes, one closed loop.

The edge enforces. The brain learns. The brain compiles what it learns into the rules the edge enforces, and the loop closes without a redeploy. Everything else in this booklet is a consequence of that arrangement.

THE EDGE

Observes and enforces in one process

One agent doing host telemetry, network enforcement, application signals, identity checks and posture — with its rules held locally. A network partition is not an outage of your controls.

evidence →

← rules

THE BRAIN

Correlates across the whole estate

Latency-tiered reasoning — deterministic rules first, then models, then agentic analysis — over one graph of everything observed, so a conclusion can always be walked back to its evidence.

The loop is the product. A detection improved centrally becomes an enforcement decision at the edge; an enforcement decision at the edge becomes evidence centrally. Neither half is useful alone, which is why they are not sold apart.

DECIDED IN LINE

The cheap, certain calls are made where the traffic is, not after a queue.

ESCALATED ON PURPOSE

Ambiguity is what reaches a person — with the case already assembled.

LEARNED ONCE

What one incident teaches is compiled down as a rule, not written up as advice.

03 · THE MODEL UNDERNEATH

Everything is an event.

A process launch, a failed sign-in, a firewall drop, a certificate approaching expiry, a badge swipe, a consent grant, a model promotion — one kind of object, one envelope, whatever domain attributes each needs. Nothing is discarded to fit.

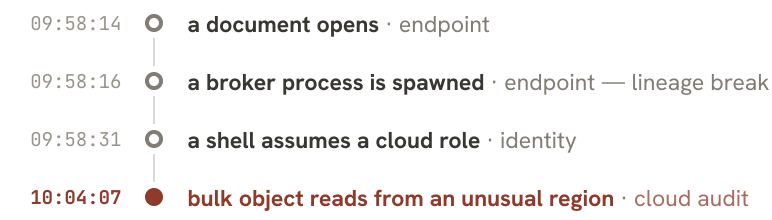
THE ENVELOPE

class	domain · category · type
subject	the entity it is about
time	observed and recorded
severity	judged, or explicitly not

WHY IT MATTERS COMMERCIALLY

Collected is not the same as judged, and both are useful. Keeping un-alarmed observations as first-class records is what lets the platform answer "what runs automatically on this host" and "who may become root here" — questions no alert stream answers, because the honest answer includes everything nobody flagged.

FIGURE · ONE PATH, FOUR DOMAINS, ONE ALERT



Each step alone is defensible; the sequence is not. The alert *is* this subgraph — and it can be assembled at all only because no step had to be mapped onto another step's schema.

04 · THE LINE-UP

One system where a category diagram used to be.

These are not modules bolted onto a console. They are views of the same event graph, which is why a question can cross between them without an integration.

Detect and investigate

Event pipeline, behavioural baselines, the provenance graph, hunting and case management — an alert opens as a path, not a row.

Enforce at the edge

Host protection, identity-aware segmentation, application and API defence, virtual patching — the same agent, one deployment.

Identity and access

Authentication, step-up, privileged sessions, certificate lifecycle and non-human identity — continuous trust rather than a check at the door.

Data and posture

Classification, retention and erasure, exposure management, configuration and compliance evidence held as events like everything else.

Respond and validate

Bounded autonomous response, deception, adversary simulation against a twin of your estate, and the compiler that turns findings into rules.

Report and collaborate

Narrative reporting where every figure links to what produced it, and an encrypted channel for the conversation an incident starts.

LICENSED ON INGESTION

Every app in the line, no SKUs inside it.

One meter, one renewal, one forecast. Turning on a capability is a decision about your security, not a procurement cycle.

~~per capability~~
~~per endpoint~~
~~per seat · per asset~~
~~per user · per store~~

05 · RESPONSE

Automation you can sign off on.

The objection to automated response is not that it is slow. It is that a wrong action at machine speed is an outage you caused yourself. The safety substrate therefore sits underneath the playbook engine rather than inside it, and nothing reaches your estate without passing through it.

BLAST RADIUS	Every automated action declares what it will touch before it runs — hosts, sessions, rules, users. An action whose scope cannot be stated is an action that does not execute.
REVERSIBILITY	Reversible actions run on their own; irreversible ones are held until a person approves them, and the automation that proposed one can never release it. The classification is a property of the action, not a setting someone can quietly relax under pressure.
OUT-OF-BAND	Approval does not depend on the estate being healthy. An incident bad enough to matter is exactly the one that takes your primary channel with it.
SAFETY-AWARE	In operational environments, the response that is correct on a laptop is not correct on a controller. Where the wrong isolation is a safety event, the platform proposes and a person decides.
RECORDED	Every action, approval and refusal is an event in the same graph as the signal that prompted it — so the answer to “why did the platform do that” is retrievable rather than remembered.

> The point of bounding autonomy is not caution for its own sake. It is that a team only delegates to a system it can predict — and the delegation is where the time saving actually comes from.

06 · EVIDENCE AND HONESTY

What we will not put in a datasheet.

A booklet is the format where an unmeasured number gets laundered into a fact, because the visual grammar says specification. Three rules govern everything EventLake publishes outward, and they are worth stating where you can hold us to them.

A figure travels with its date and its source

No coverage percentage without the day it was measured and the runtime that produced it. No throughput number without naming the machine it was measured on in the same breath. Where a figure has gone stale, it comes off the page rather than staying up unqualified.

Gaps are named, not omitted

Some things the platform does not detect, it does not detect by construction — a consequence of a design decision we would make again. Those belong in the coverage sheet next to what we do detect. A vendor who publishes no gaps has not found none.

Nothing here is behind a form

Whitepapers, briefs, datasheets and this booklet are published, not gated. We collect a work email once, when you ask for a conversation, and we tell you what we do with it before you submit.

The same rule runs inside the product. A number in a board report links to the events that produced it; a narrative sentence carries the subgraph that proves it. An uncited sentence does not ship — outward or inward.

NEXT STEP

See it against your own estate.

A working session on your telemetry, not a slide deck. Bring one incident you were unhappy with and we will walk it end to end — what was collected, what was judged, what would have been enforced, and where the answer would still have been “we cannot say”.

READ NEXT

Notes on Active Defense — Paper 01 on the closed loop, Paper 02 on provenance and explainable alerts.

SIZE IT YOURSELF

The public sizing calculator takes your ingestion volume and returns a figure without a conversation.

TALK TO A PERSON

contact@eventlake.com reaches the team that builds it, not a routing queue.

Book a demo

EventLake

contact@eventlake.com

We ask for a work email and a phone number, and we tell you what we will do with them before you submit. We do not sell contact data, and one unsubscribe stops everything.

Nine product lines · every capability in a line included