EventLake

THE PLATFORM LINE

For heads of security operations and detection engineering

Your queue is not too long. It is full of the wrong work.

Most of what an analyst adjudicates tonight is genuinely unusual and genuinely authorised. Deciding between those two is a different problem from detecting the behaviour, and it has an answer sitting in a system nobody connected.

THE ELEVEN MINUTES

Spent once, then spent again tomorrow

An analyst opens a change ticket, a chat thread and a cloud console to establish that a migration was approved. Nothing in the platform learned anything.

THE ALTERNATIVE

A verdict that cites a ticket number

Scoped to this identity, this resource, this window — and expiring with it. Not a suppression rule written in a hurry at 02:20.

THE HONEST PART

What remains is harder work

The queue changes composition, not just length. It is better work per case, and it is not a promise of an easier shift.

The same night, adjudicated

suppression would have covered both lines

02:14 **unusual-geography authentication** · detection fires

02:14 **adjudicated legitimate — recorded, not raised** · cites CHG-4471, window 01:00–05:00

03:41 **write outside the change scope** · the verdict does not extend — raised, and sharper for it

WHAT CHANGES ON THE FLOOR

An alert opens as a path. The subgraph that justified it is stored, not re-queried — so it says the same thing in two years.

Analyst decisions stop evaporating. The corpus is what makes "this identity's authorised-anomaly rate tripled" a question anyone can ask.

A rule can be backtested before it ships. Ninety days of retained events answer how often it would have fired, and on what.

Containment stops waiting on a person. Reversible actions run unattended once the scope is computed; the consequential one waits for a person's approval.

ASK US THESE

When an alert is closed as authorised, do you retain a status or a citation?

Does every adjudication have an expiry, and can I count the live ones?

Can I run a candidate rule over 90 days of my own events first?

What is your measured time-to-withdraw for a rule already on the fleet?

Show me the last three coverage regressions and what caused them.

BRING ONE BAD NIGHT

We will walk your incident, not our demo estate.

Bring an incident you were unhappy with. We will trace what was collected, what was judged, what would have been enforced, and where the answer is still "we cannot say".

Book a working session

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.