

— CUSTOMER SUCCESS STORY

Every action taken, every action evidenced.

A payments platform needed faster incident response and a complete record of who — or what — changed production. **The SRE Orchestrator** gave it both: autonomous investigation with approval-gated action and a full audit trail.

Audit and speed

Regulated operators cannot trade control for speed. Faster remediation is only acceptable if every action is bounded by policy, attributable to an identity, and reconstructable afterwards — which is precisely where ad-hoc automation and runbook scripts tend to fail review.

— THE SITUATION

Automation the auditors would not accept

The team had built scripts to speed up common fixes. Compliance review found the problem:

- **Scripts ran with standing privilege.** Useful under pressure, impossible to bound, attributable only to whoever triggered them.
- **No consistent record of intervention.** Reconstructing an incident meant assembling chat logs, ticket comments and shell history.
- **Latency incidents demanded rapid judgement** when engineers were least able to exercise it carefully.
- **Change correlation was manual**, so establishing whether a deploy caused a payment failure took longer than reverting it.

— THE DECISION

Autonomy inside guardrails, logged by default

The platform adopted the orchestrator with conservative autonomy settings — investigation and diagnosis fully autonomous, remediation gated by action class — and every run logged, gated and attributed.

Our regulator does not object to automation. They object to automation nobody can bound or reconstruct. Guardrails and an audit trail were what made speed approvable.

— HEAD OF SITE RELIABILITY

DEPLOYMENT SNAPSHOT

SECTOR

Payments platform

ESTATE

Authorisation · Settlement ·
Ledger · APIs

SETUP

Deep integration, private LLM in-
boundary

AUTONOMY

Investigation autonomous;
action gated

GUARDRAILS

Per-service, per-action
boundaries

AUDIT

Runs logged, gated and
attributed

REASONING

In-boundary — never the public
internet

INTEGRATIONS

Prometheus · incident.io · GitLab
· Jira

— HOW IT WAS SET UP

Investigate

Fully autonomous hypothesis testing across logs, metrics, traces and prior incidents — no standing privilege required to **read and reason**.

Guardrails

Execution boundaries per service and action class, so the set of things the orchestrator may do is explicit rather than implied by a script's permissions.

Approvals

Consequential actions — rollback, revert, workflow runs — **gate on a named human**, with the decision recorded alongside the evidence that prompted it.

Audit

Every run **logged, gated and attributed**, producing the reconstruction that previously required assembling chat, tickets and shell history.

— WHAT CHANGED

BEFORE THE SRE ORCHESTRATOR

- Fix scripts running with **standing privilege**
- Intervention records scattered across three systems
- Rapid judgement demanded under maximum pressure
- Deploy-to-incident correlation done manually
- Automation that could not clear compliance review

WITH THE SRE ORCHESTRATOR

- Investigation autonomous; **action explicitly bounded**
- Every run logged, gated and **attributed**
- Evidence-backed root cause before the decision point
- Change intelligence correlating deploys to risk
- Automation the audit function approved

— WHERE THE CHANGE CAME FROM

Bounding beat restricting

Defining what the orchestrator may do per service and action class was more acceptable to risk than either unrestricted scripts or no automation.

The record came free

Attribution and logging as a property of the platform removed the reconstruction work that had made post-incident review expensive.

Judgement moved earlier

Arriving at the decision point with evidence and a confidence score changes what an engineer is being asked to approve at 3am.

— WHY THIS MATTERS IN PAYMENTS

Capabilities doing the work in this deployment:

Execution guardrails

Approval gating by action class

Full audit trail

Private LLM in-boundary

Change intelligence

Evidence-linked RCA

Attributed runs

Post-incident reconstruction

BOTTOM LINE

The SRE Orchestrator gave a payments platform faster resolution without giving up the boundaries and evidence its regulator requires.

Turn up your SRE Orchestrator.

Value-proving POC in about two weeks — deep integration or light discovery.

LUMIOps AI™

LUMIOPS.AI



GET IN TOUCH

lumiops.ai/contact-us

POC

~2 weeks to value



LINKEDIN

linkedin.com/company/lumiops