DEPARTMENT · SECURITY OPERATIONS

The SOC, run as a governed AI team.

Three agents — threat-intel-researcher, security-analyst, soc-lead — running the incident hand-off DAG under deny-by-default policy, a signed audit chain, and behavioral-drift quarantine. Real work, on a live zero-trust stack.

Asphodel + Tiresias-ZT · ACME Corporation

THE STAKES

An autonomous analyst with no enforcement boundary is an incident of its own.

Security Operations is the one department that cannot accept an AI worker on trust. Every read of intel, every hand-off, every escalation has to be authorized, isolated, and provable after the fact — or the tooling becomes the attack surface.

WITHOUT GOVERNANCE

Shared credentials, silent tier-hopping, no per-call attribution, no way to prove an agent stayed inside its mandate when an auditor asks six weeks later.

WITH TIRESIAS-ZT

Deny-by-default policy at the PEP, per-agent capability tokens, an Ed25519-signed audit chain, and SoulWatch drift detection that quarantines a misbehaving agent automatically.

THE WORKFORCE

367 governed agents, mapped to the real org.

Security Operations is not a bolt-on. It is one segment of a fleet that mirrors the Acme directory like-for-like — every department, region, and role-family represented.

367	360	7	28
GOVERNED AGENTS	FLEET AGENTS	SHOWCASE AGENTS	DEPARTMENTS
325,154			
DIRECTORY PRINCIPALS			

Source: ARCHITECTURE-FACTS · CP registry (367 agent tenants) + agent-manifest.json · Samba-AD (120,120 humans + 205,034 NHI, 28 depts / 10 regions / 626 roles)

ARCHITECTURE · THE SLICE THAT MATTERS

Every SecOps call is a governed call.

Nothing an agent does touches data directly. The Enforcement Plane (PEP) validates, evaluates policy deny-by-default, and only then forwards verbatim to the agent's isolated backend.

`runner mints HS256 cap-token` → `PEP :8343 — deny-by-default` → `soul-svc tenant` → `PostgREST /rest/v1` → `acme_soul · RLS forced`

AUTH	**Two-factor per call** X-Tiresias-Api-Key (tenant) + X-Capability-Token (HS256, minted from a 64-hex secret)	`deny-by-default`
ISOLATE	**Per-agent data tenancy** Each agent is a soul-svc tenant; _memories + _soul_api_keys are FORCE RLS on Cloud SQL	`RLS forced`
PROVE	**Signed audit chain** SoulKey Ed25519 chain, durable WAL at /data/audit-wal, shipped to the control plane	`Ed25519`

Source: ARCHITECTURE-FACTS · Plane 3 (PEP, host :8343) + Plane 4 (soul-svc / Cloud SQL acme_soul)

THE DEPARTMENT FLOW

The incident hand-off DAG.

Security Operations owns the front of a 14-edge topological hand-off DAG. Intel is gathered, triaged, and escalated across three named agents before the work leaves the department.

`threat-intel-researcher` → `security-analyst` → `soc-lead` → `research-lead` → `data-analyst` → `content-editor` → `compliance-officer`

THREAT-INTEL-RESEARCHER

Gathers and normalizes raw intel into a domain brief. Entry point of the DAG; feeds the analyst.

SECURITY-ANALYST → SOC-LEAD

Analyst triages and correlates; soc-lead adjudicates severity and decides whether to escalate up-tier or hand off out of the department.

Source: ARCHITECTURE-FACTS · Plane 5 · personas.json (7 showcase agents, 14-edge DAG, runner.py schedule --interval 3600)

LIVE PROOF

Real numbers from the running instance.

These are not projections. They are read off the live GCP deployment — the same figures the ROI board and CP registry serve today.

3 SECOPS DAG AGENTS	14 HAND-OFF DAG EDGES	8343 PEP ENFORCEMENT PORT	1514 SIEM SYSLOG INGEST
$0.19 OPUS-4.8 / CALL, CEILING TIER			

Source: ARCHITECTURE-FACTS · CP registry + Grafana ROI dashboard (uid acme-roi-economics) reading tzt_usage · Promtail :1514

WALKTHROUGH · TIERING & ESCALATION

Severity buys compute. Nothing else does.

Each agent runs a home tier with a ceiling and a floor. Keyword escalation moves a job up only when the incident warrants it — and cost follows severity, not habit.

HOME	Default working tier Every job starts at the agent's home model; SecOps stays economical until signal changes	per-agent
ESCALATE	Keyword trigger +incident / +breach / +critical in the brief promotes the job toward the ceiling tier	+incident/+breach/+critical
CEILING	Top-tier reasoning on demand opus-4.8 for the hard adjudications the soc-lead cannot get wrong	$0.19 / call
FLOOR	Fallback-to-floor on LLMError An upstream failure degrades to the floor tier rather than dropping the job	reliable degrade

Source: ARCHITECTURE-FACTS · Plane 5 (home/ceiling/floor tiers, keyword escalation, fallback-to-floor) + ROI economics

WALKTHROUGH · SOULWATCH

A drifting agent quarantines itself.

Behavioral drift is not a report you read on Monday. SoulWatch watches every governed call, and an agent that strays from its behavioral baseline is auto-quarantined — no human in the loop required to stop it.

DETECT

SoulWatch scores behavioral drift against baseline across the agent's governed trajectory, model_baseline, campaign, and drift analytics.

CONTAIN

On drift, the agent is written to the shared postgres quarantine store and blocked at the PEP — durable across restart, reviewable from the analyst console at pdp.tiresias.watch /admin.

> The fail-safe for an autonomous SOC is an SOC that can pull its own agent.

Source: ARCHITECTURE-FACTS · Plane 3 (SoulWatch → auto-quarantine, shared postgres store) + PEP /admin soulwatch/status

WALKTHROUGH · SIEM

Governed activity lands in your SIEM, not a silo.

Every enforcement event is RFC5424 syslog. It flows straight into the observability stack SecOps already understands — structured, queryable, correlatable with the rest of the estate.

PEP audit event → RFC5424 syslog → Promtail :1514 → Loki :3100 → Grafana :3000

INGEST	Promtail syslog receiver TCP :1514 on acme-demo — published SIEM ingest for the whole stack	RFC5424
STORE	Loki log store :3100 — SoulWatch SIEM stream and audit events queryable together	:3100
VIEW	Grafana :3000 — dashboards over acme-tzt-usage and the log streams	:3000

Source: ARCHITECTURE-FACTS · Plane 3 (SIEM: RFC5424 → Promtail:1514 → Loki) + Plane 6 (Grafana :3000, Loki :3100)

GOVERNANCE & AUDIT

Provable after the fact, by construction.

The question an auditor asks is not "do you trust the agent" — it is "prove what it did." The signed audit chain and the analyst console answer that without reconstruction.

THE CHAIN

Each governed call is signed into an Ed25519 audit chain with a durable WAL, shipped to the control plane. Tampering breaks the chain; nothing is retro-editable.

THE CONSOLES

Analyst review at PEP /admin (pdp.tiresias.watch): license, audit/verify, soulwatch/status, quarantine, analytics. Management at asphodel-ui :3001 (console.asphodel.ai).

STORES	All durable, postgres-backed registry, enrollment ledger, usage, audit home, quarantine — survive restart	postgres
VERIFY	audit/verify endpoint role-token-gated verification of the signed chain from the analyst console	/admin

Source: ARCHITECTURE-FACTS · Plane 2 (postgres-backed CP stores) + Plane 3 (Ed25519 audit chain, WAL) + UIs (pdp.tiresias.watch, console.asphodel.ai)

ECONOMICS · THE SELF-HOST-VS-API ANSWER

Cost per call, observed on the ROI board.

The ROI dashboard reads tzt_usage directly. SecOps reserves the top tier for genuine incidents and lets everything else run cheap — the spread is three orders of magnitude.

MODEL / TIER	PROVIDER	RELATIVE COST	$ / CALL
opus-4.8 · ceiling	OpenRouter paid		$0.19
sonnet-4.5	OpenRouter paid		$0.03
deepseek-v4-pro	Ollama Cloud		$0.002
gpt-oss:120b	Ollama Cloud		$0.0015
Llama-3.3-70B	HuggingFace		$0.0012
gemma-4-31b:free	OpenRouter free		$0.00

Source: ARCHITECTURE-FACTS · Plane 6 · Grafana ROI dashboard (uid acme-roi-economics) · observed $/1M-token economics per model

SECURITY OPERATIONS · IN ONE LINE

A SOC you can audit like a control, not trust like a black box.

Three named agents on the incident hand-off DAG, every call deny-by-default at the PEP, every action signed into an Ed25519 chain, drift auto-quarantined, and the whole trail in your SIEM. Live today on the ACME instance.

Asphodel + Tiresias-ZT · ACME Corporation · pdp.tiresias.watch