

TIRESIAS-ZT • SOC OPERATIONS

A monitored agent estate.

367 AI agents are doing real work inside ACME today. The question for the SOC is not whether to allow them — it is whether you can see them, signal on them, and quarantine them the way you already do endpoints.

● Asphodel + Tiresias-ZT • ACME Corporation

THE STAKES

Sprawl, drift, and incident are already in your estate.

Autonomous agents behave like a new workforce with no badge, no shift, and no SOC surface. Three failure modes matter to your desk.

SPRAWL	Agents outnumber your people 205,034 non-human service identities against 120,120 humans — the machine estate is already the larger attack surface.	205,034 NHI
DRIFT	Behavior changes without a deploy An agent that quietly starts acting out of pattern is an insider-threat signal with no HR file behind it.	behavioral
INCIDENT	Autonomous hand-off spreads blast radius Agents pass work to other agents. One compromised step can walk a task across seven roles before a human looks.	7-role DAG

Source: ACME directory sync — 325,154 principals (120,120 humans + 205,034 NHI/service identities).

THE ESTATE

367 governed agents, mapped to the real org.

Not a lab. A live Tiresias-ZT + Asphodel deployment on GCP where every agent is a registered tenant with an identity, a policy, and an audit trail.

367 GOVERNED AGENTS	7 SHOWCASE / INCIDENT AGENTS	360 FLEET AGENTS	28 DEPARTMENTS MAPPED
---	--	--	---

The 360 fleet agents are mapped like-for-like to the real ACME org — department by role-family, by headcount, across all 28 departments, 10 regions and 626 roles. Every one is enrolled to a single enforcement point at `site acme-site`

Source: registry (367 agent tenants) • agent-manifest.json • directory 28 depts / 10 regions / 626 roles.

YOUR SLICE OF THE ARCHITECTURE

One enforcement point. One deny-by-default gate.

Every governed call an agent makes crosses the Policy Enforcement Point (PEP) on :8343 before it reaches any data. There is no side door.

runner mints HS256 cap-token → PEP :8343 — deny-by-default → soul-svc tenant → acme_soul • RLS forced

EVERY CALL MUST PRESENT

X-Tiresias-API-Key tenant key
X-Capability-Token HS256, minted per-agent from a 64-hex capability secret
Policy evaluates deny-by-default. On allow, the request forwards *verbatim*. On deny, it never touches the backend.

EVERY CALL LEAVES A TRACE

Signed audit chain — SoulKey Ed25519 — ships to the control plane, with a durable write-ahead log at `/data/audit-wal`.
Tamper-evident by construction: the chain signs each governed call as it happens.

Source: PEP (TZT_ROLE=proxy) :8343 • deny-by-default policy • Ed25519 audit chain • WAL `/data/audit-wal`.

LIVE PROOF

This is instrumented, not aspirational.

The SOC-facing surface is running now — real ports, real stores, real signal — on the acme-demo host.

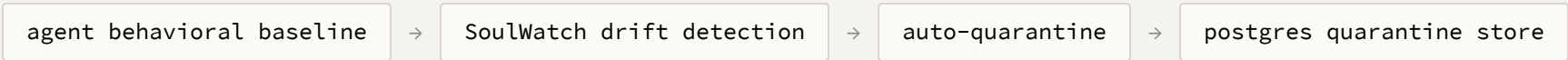
1514 PROMTAIL SYSLOG INGEST (TCP)	3100 LOKI LOG STORE	3000 GRAFANA DASHBOARDS	8343 PEP + /ADMIN CONSOLE
--------------------------------------	------------------------	----------------------------	------------------------------

Every governed store is postgres-backed and reboot-durable — registry, usage, audit, and quarantine survive a restart.

Source: port map (acme-demo) • T2T stores = postgres (registry/usage/enrollment/audit/quarantine).

SoulWatch: behavioral drift to auto-quarantine.

The same primitive you use for user-behavior analytics, applied to agents.
SoulWatch watches each agent's behavioral baseline and acts without waiting for a human.



DETECT	Drift is a first-class signal SoulWatch scores deviation from an agent's established trajectory — not a static rule you have to write and maintain.	behavioral
CONTAIN	Quarantine is automatic A drifting agent is pulled out of the allow path into the shared quarantine store — no allowed calls until an analyst clears it.	auto
REVIEW	Analyst console owns the disposition soulwatch/status, quarantine, and drift analytics live behind the role-token-gated PEP /admin surface.	/admin

Source: PEP SoulWatch → auto-quarantine (shared postgres store) • analyst console pdp.tiresias.watch /admin (soulwatch/status, quarantine, drift).

RFC5424 syslog into the pipeline you already run.

Agent governance events are not a proprietary black box. They emit standard RFC5424 syslog — the format your SIEM already parses.

PEP — RFC5424 syslog → Promtail :1514 → Loki :3100 → Grafana :3000

STANDARD ON THE WIRE

RFC5424 over TCP to Promtail on :1514. Point your own collector at the same stream, or take the Loki store as-is.

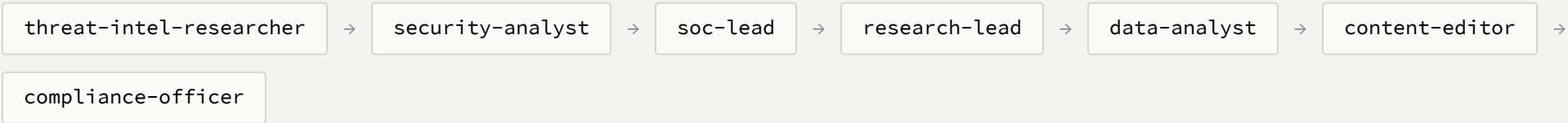
QUERYABLE AT REST

Loki holds the governed event log; Grafana renders it. The usage postgres datasource (`acme-tzt-usage` → `tzt_usage`) carries tenant, agent, model, tokens and cost per bucket.

Source: SIEM path — RFC5424 syslog → Promtail:1514 → Loki:3100 → Grafana:3000 • datasource `acme-tzt-usage` / `tzt_usage`.

The seven-agent hand-off, fully instrumented.

The showcase agents run a 14-edge topological hand-off DAG — a work chain that starts at threat intel and ends at compliance. Every edge crosses the PEP, so the whole chain is auditable end to end.



7	14	1	
AGENTS IN THE CHAIN	TOPOLOGICAL HAND-OFF EDGES	ENFORCEMENT POINT PER EDGE	

Source: `personas.json` — 7 showcase agents, 14-edge topological hand-off DAG (`threat-intel-researcher` → ... → `compliance-officer`).

Incident keywords escalate to the frontier tier.

When work is tagged as a real event, the governed runner does not degrade quietly — it escalates the model tier so the hardest analysis gets the strongest model, under policy.

+incident	Escalate above the agent's home tier The keyword lifts the request toward the ceiling tier for that agent.	escalate
+breach	Same lever, breach-grade work Routing favors free/Ollama by default — these keywords are the deliberate exception.	escalate
+critical	Reach frontier under governance Escalation still crosses the PEP with a capability token — a stronger model, not a bypass.	escalate
LLMError	Fallback-to-floor on failure If a model errors, the agent degrades to its floor tier rather than failing the job — degrade, never drop.	floor

Source: personas.json — per-agent home/ceiling/floor tiers, keyword escalation (+incident/+breach/+critical), fallback-to-floor on LLMError.

The analyst console the SOC actually operates from.

Detection and containment are only useful if a human can review, verify, and clear. The PEP /admin surface is role-token gated and purpose-built for that.

VERIFY

License state, and audit/verify against the Ed25519 chain — confirm the log has not been tampered with.

ANALYZE

Analytics by trajectory, model_baseline, campaign, and drift — the evidence behind a quarantine decision.

soulwatch/status	Live drift posture per agent	/admin
quarantine	Contained agents and their disposition	/admin
pdp.tiresias.watch	Review / analyst console domain	role-gated

Source: PEP /admin (pdp.tiresias.watch) — license, audit/verify, soulwatch/status, quarantine, analytics: trajectory/model_baseline/campaign/drift.

Every governed call is costed — including the tier you escalate to.

The same usage stream that feeds the SOC feeds the ROI board. When an incident escalates to frontier, you see exactly what that decision cost — observed \$/call, per model.

MODEL	TIER	OBSERVED \$/CALL	RELATIVE
opus-4.8	frontier (escalation target)	\$0.19	
sonnet-4.5	paid mid	\$0.03	
deepseek-v4-pro	Ollama Cloud	\$0.002	
gpt-oss:120b	Ollama Cloud	\$0.0015	
Llama-70B (HF)	HuggingFace	\$0.0012	
gemma:free	free-homed floor	\$0.00	

Source: ROI dashboard (uid acme-roi-economics) — observed per-model \$/call, tzt_usage. Free-tier saturation (hermes-405b:free chronic 429) motivates the self-host tiers.

An agent estate your desk can actually run.

You already have the muscles — SIEM, UEBA, quarantine, incident hand-off.
Tiresias-ZT points them at the 367 agents that are already inside ACME.

SEE	RFC5424 syslog → Promtail:1514 → Loki → Grafana	standard SIEM
SIGNAL	SoulWatch behavioral drift, scored per agent	UEBA for agents
CONTAIN	Auto-quarantine into a durable postgres store	no human wait
PROVE	Ed25519 audit chain, verify from /admin	tamper-evident

Deny-by-default at one enforcement point. Drift-to-quarantine without a human in the loop.
A signed chain you can verify. That is a monitored estate.