INVESTIGATE · HITL · VERIFY · TEXT-TO-SQL

AI-Powered SOC & Autonomous Incident Response

Dockerized AIPSOC platform for multi-source security ingest, correlation, AI investigation + RAG/TI, HITL approvals, verified remediation, Scenarios A–D, dashboard, and secured Text-to-SQL — for teams that need production IR automation, not a chatbot on logs.

M0–M10	PASS	1.0.0	ALL_PASS
MILESTONES CLOSED	PHASE 1 / 2 / 3	API VERSION	M10 SMOKE

Built by **Abdul Basit** · AI Automation Engineer

BUSINESS IMPACT

Less noise · safer remediations · audit-ready IR

Ingest→investigate→HITL→verify · unauthorized actions 0 · destructive SQL 0 · Phase gates Met · UAT ALL_PASS

OVERVIEW

IdP, EDR, email, and SIEM events normalize into PostgreSQL. FastAPI owns triage, risk, TI, security RAG, investigation/MCP, HITL, remediation with verify-before-success, analyst chat, Text-to-SQL, and eval. n8n runs modular ingest and notify workflows. Operators get an ops dashboard with API-key RBAC. Live prod cutover is formally waived for sandbox acceptance.

TYPE	AI SOC / IR platform (not a single n8n flow)
ROLE	AI Automation Engineer / AI Security Engineer
DELIVERY	API 1.0.0 · Milestone M10 · Closeout 2026-09-12 · Milestones doc v2.1
STACK	FastAPI · n8n · Postgres · Redis · Qdrant · Caddy · security fixtures · Slack/Email stubs
BUYERS	SOC & IR teams needing gated, grounded automation

THE PROBLEM

- **Alert noise** — SIEM/EDR/IdP floods
- **Weak correlation** — fragmented tickets
- **Invented findings** — ungrounded LLM
- **Ungated actions** — isolate without HITL
- **No verify** — success assumed
- **Free SQL risk** — DROP / UPDATE

THE SOLUTION

- **FastAPI IR** — triage, agents, SQL
- **Thin n8n** — ingest / notify wrappers
- **Correlate** — incidents from events
- **HITL gates** — approve before remediate
- **Verify-before-success** — VER-01
- **SQL RO** — analytics.v_* only

WHO IT SERVES

- Teams needing **gated IR AI**
- Ops needing one incident timeline
- Sandbox demos without live SIEM
- Lead demo: **investigate → HITL → verify**
- Secondary: SQL deny · Scenarios B/C

CAPABILITY SURFACES

SURFACE	FOCUS	SURFACE	FOCUS
Ingest	IdP · EDR · Email · SIEM · P2	Intelligence	Triage · TI · RAG · MCP
HITL / remediate	Approve · revoke · isolate · verify	Ops UI	Dashboard · chat · reports
P1 / P2	RCA · tickets · eval · SQL	Security	Kill switch · SQL deny · audit

Demo lead: ingest → investigate → HITL → remediate/verify → dashboard. **Secondary:** SQL suite executed=0 · Scenario B/C. **Closeout:** `m10_closeout_smoke.py` ALL_PASS.

Architecture rule: FastAPI owns AI / AuthZ / SQL / HITL · n8n stays thin · remediations require approval · verify-before-success · env-only secrets.

ARCHITECTURE & CAPABILITIES

Architecture, journeys, connectors

Principle: FastAPI owns investigation, HITL, SQL guard, and remediation gates; **n8n owns thin side effects** — no god-workflow.

```
Sources (IdP / EDR / Email / SIEM / P2 stubs)
  → n8n ingest + error path → PostgreSQL events/incidents
    → FastAPI: triage · risk · TI · RAG · investigation/MCP · HITL
      → Remediate + verify · Dashboard + notify · Text-to-SQL RO · Qdrant · Redis
```

COMPONENT	ROLE
Caddy + dashboard	Proxy; ops SPA with API-key RBAC
FastAPI	Auth (`X-API-Key` + `X-Role`), IR APIs, agents, SQL, RAG
SQL / analytics	Allowlist `analytics.v_*` ; RO role; destructive = 0
HITL	Approve before revoke / block / isolate
Phase 3	RCA, ticketing, chat, eval, Text-to-SQL, P2

INTELLIGENCE

- Triage + risk + decision
- TI multi-feed stubs
- Qdrant security RAG
- Investigation + MCP ACL
- Eval scorecards + cost stop

INTEGRATIONS

IdP / Email / EDR	P0 fixtures
SIEM / M365 / Azure	Stub P1
Scanner / CF	Stub P2
Jira	Stub path
Live prod	Waived

SAFETY & OPS

- HITL before remediations
- Verify-before-success
- Kill switch + cost stop
- Injection + tool ACL
- Append-only audit

LEAD DEMO PATH

- Scenario A auth storm → one incident
- Investigate with evidence + RAG
- Pending approval blocks side effects
- Approve → revoke → verify success
- Dashboard timeline + SQL ask

SECURITY PROOF POINTS

No API key → **401** · destructive SQL never executes · remediations require HITL · UAT unauthorized actions / SQL executed: **0 / 0**.

Demo arc: investigate→HITL→verify primary · SQL deny / B+C secondary · cite `/health` 1.0.0 · `m10_closeout_smoke.py` ALL_PASS.

RELIABILITY · MILESTONES · GATES

Reliability, M0–M10, Phase gates, closeout

RELIABILITY AND SECURITY

AREA	WHAT SHIPPED
Auth	`X-API-Key` + `X-Role` RBAC
SQL	Allowlist views · deny destructive
HITL	Approve before high-impact remediations
Verify	Success only after verification
Agents	MCP allowlists · kill switch · budgets
Audit	Agent runs · SQL denies · approvals

PHASE GATES + CLOSEOUT

- **Phase 1 (M4)** — ingest→correlate; triage; TI/RAG; investigation; injection → 0
- **Phase 2 (M7)** — Scenarios A+D; HITL; verify 100%; unauthorized → 0
- **Phase 3 (M10)** — B+C; SQL; P2/learning; docs+KT; sandbox Met

m10_closeout_smoke.py	**ALL_PASS**
API version	**1.0.0**
Closeout date	**2026-09-12**
Evidence chain	docs/m4 → m7 → m8 → m9 → m10

MILESTONES M0–M10 (ALL COMPLETE)

ID	THEME	WHAT UNLOCKED
M0	Kickoff & architecture	Architecture baseline, principles, RACI
M1–M2	Skeleton → ingest	Compose, RBAC, normalize/dedupe/correlate
M3–M4	Triage → Phase 1	Risk/TI/RAG, investigation/MCP, Phase 1 Met
M5–M6	HITL → E2E A/D	Remediate+verify, notify, Scenario demos
M7	Dashboard / MVP	Ops SPA, MVP Met (sandbox)
M8–M9	P1 → P2 polish	B/C, chat, eval, Text-to-SQL, learning
M10	Docs / UAT / KT	Closeout pack, Phase 3 Met, API 1.0.0

CORRELATE

Fixtures + P1/P2 stubs → incidents with event links and audit.

INVESTIGATE + SQL

- MCP tool allowlists
- Qdrant cited answers
- Text-to-SQL RO views

OPS + RECOVERY

- Dashboard + HITL queue
- pg_dump backup procedure
- Cutover checklist + KT

Concrete reliability: no-key → 401 · DROP never executes · remediations require HITL · verify-before-success · unauthorized / SQL at UAT: **0 / 0**.

Delivery truth: M0–M10 complete · Phase 1/2/3 Met · m10 smoke ALL_PASS · API 1.0.0 · cite live /health in demos.

OUTCOMES · TECH · DEPTH

Stack, UAT, journeys, n8n, residual risks

TECH STACK + REPRODUCE

FastAPI · n8n · Postgres · Redis · Qdrant · IdP/EDR/email fixtures (+ P1/P2 stubs) · Caddy · Compose AIPSOC

`docker compose up -d --build · python docs/m10/samples/m10_closeout_smoke.py`

Surfaces: /dashboard/ · /health · /docs · n8n :5678 · Auth: `X-API-Key` + `X-Role`

SCOPE HONESTY

- Portfolio case study — no fake logos or reviews
- Sandbox-first connectors without live SIEM OAuth
- Waivers: live prod cutover, live connectors, live LLM, full SSO
- Not a log chatbot — full AIPSOC M0–M10

M10 CLOSEOUT EVIDENCE INDEX

DOC	PURPOSE
UAT.md / ACCEPTANCE.md	A–D Met · PRD Complete/Waived · ALL_PASS
CUTOVER.md / RUNBOOKS.md / KT.md	Deploy checklist · day-2 ops · KT notes
ARCHITECTURE_v1.md	Baseline topology
m10_closeout_smoke.py	Health · SQL · P2 · chat · MVP · eval · 401

DASHBOARD

Incidents	Open / severity
Timeline	Evidence
Chat	Grounded

P1 / P2

RCA / tickets	M8
Eval / cost	Hard stop
Text-to-SQL	RO views
P2 connectors	Stubs

N8N CATALOG

- wf_security_ingest
- wf_* triage / investigate
- wf_human_approval
- wf_e2e_scenario_a–d

N8N (THIN CALLERS)

Ingest · triage · investigation · approval · remediation · exec report · E2E A–D · global error — env API key only

RESIDUAL RISKS (HONEST)

Live vendor sandboxes · prod TLS/secret rotation · LLM quality vs corpus · wet-ink acceptance — tracked as M10 waivers; **none reopen Phase gates**.

SAMPLE JOURNEYS A–D + GATES

A Auth → HITL → revoke	**B** Phish → block	**C** Endpoint → isolate	**D** FP auto-close
SQL Ask + deny suite	**Chat** Grounded ask	**P2** Scanner ingest	**401** No key

PORTFOLIO ONE-LINER

AIPSOC — Dockerized FastAPI + n8n AI SOC: ingest/correlate, investigate with RAG/TI, HITL, verified remediation, Scenarios A–D, Text-to-SQL, dashboard — M0–M10 complete at API 1.0.0.

SYSTEM VISUALS

Architecture & before / after