DESIGN PARTNER PROGRAM

ThreatRecall

app.threatrecall.ai

30 days, no charge, you keep the data.

CTI memory layer for SOC teams. Evidence-backed recall, signed audit logs, TLP-aware storage, and full data export on exit.

THE PROBLEM

- Teams re-derive what they already knew — every shift.
- OpenCTI, MISP, SIEM store. They don't remember.
- Analyst turnover destroys institutional memory.
- Agentic SOC workflows stall without evidence-backed recall.

WHAT YOU CAN DO ON DAY 1

- 01 Natural language recall — ask in plain English
- 02 Knowledge graph — actor!'TTP!'CVE!'IOC chains
- 03 Structured IR — incidents with linked evidence
- 04 Ingest pipeline — STIX-compatible, TLP-classified
- 05 Evidence panel — source, confidence, TLP, timestamp
- 06 Memory correction — reject / merge / correct; 24h rollback
- 07 Signed audit log — write-once, CSV+JSON export
- 08 TLP-scoped access — AMBER/RED never sent to LLM
- 09 MCP server + LangChain adapter
- 10 Full data export on exit — every node, edge, audit log

COMPLIANCE POSTURE

FedRAMP Moderate assessment in progress. Phases 0–3 complete. Not yet authorized — do not represent us that way to your CISO. 9 CI gates

Ph0 ' Ph1 ' Ph2 ' Ph3 ' Ph4 !'

TRUST SURFACE

Evidence Panel
Source URL, confidence bar (0–1), TLP badge, ISO timestamp, linked evidence IDs. Warning on <0.6 confidence or AMBER/RED.

Signed Audit Log
Write-once DB triggers. Immutable event UUIDs. CSV + JSON export. Every action logged with user, IP, TLP.

TLP-Aware Memory
AMBER and RED nodes never sent to LLM — enforced at query layer, not UI.

Memory Correction
Reject with reason/category. Correct with full version history. Merge with per-field winner. 24h rollback.

Tenant Context Bar
Workspace name, color-coded role badge, TLP scope with lock icon, Cmd+K workspace switcher.

RBAC + TOTP
FedRAMP roles: admin/analyst/readonly/audit. TOTP per-tenant. Per-session revoke. 4-fail lockout.

PILOT TERMS

WHAT YOU GET

- 30 days, no charge
- Design-partner pricing locked
- Weekly 30-min founder sync
- Full export on exit

WHAT WE ASK

- 1 named CTI/SOC lead
- Non-sensitive CTI (first 2 wks)
- Written feedback at days 7/14/30

Start a pilot
app.threatrecall.ai/pilot