PROCUREMENT SELF-SERVICE

Security Questionnaire

CSA CAIQ-Lite v4 + SIG-Lite

Pre-answered for SOC/MSSP procurement. Where a control is not yet met, we say so plainly.

~70	30	1.0	2026-05-29
CAIQ-Lite v4 questions	SIG-Lite questions	Document version	Last updated

Threat Engram LLC
EIN: 99-1234567 · Privacy policy: app.threatrecall.ai/privacy
app.threatrecall.ai/security/questionnaire

Contents

In-progress items (amber border) indicate controls not yet fully implemented. Target dates are honest estimates, subject to post-Seed funding.

Honesty statement

No green checkmarks that don't earn them. Where a control is not yet met, we say so plainly with target date. First-client trust is built on candor, not marketing.

01 — APPLICATION & INTERFACE SECURITY

5 questions

AIS-01.1 Do you have documented application security requirements and design specifications?

Yes. Application security requirements are captured in the ThreatRecall SDLC Policy (internal doc). The codebase implements security design specs in middleware/, services/, and routes/ with audit-on-write enforcement at the DB layer. Design specs for new features are reviewed against NIST 800-53 AC, IA, SC families before implementation.

`NIST: SA-3, SA-4, SA-8`

AIS-02.1 Are OWASP Top 10 risks mitigated in your application?

Yes — in progress (Phase 4 of FedRAMP). SQL injection is prevented via parameterized queries (pg parameterized in all db/ functions — no raw SQL injection surface). XSS mitigated by EJS output escaping by default. CSRF prevention via token-based state. Rate limiting on all auth endpoints (4-fail lockout). CI gates run SAST (semgrep) on every push. Full OWASP Top 10 review is part of Phase 4 SAR scope, expected Q3 2026.

`NIST: SI-10, SI-15, SC-8`

`&  In progress — FedRAMP Phase 4, target Q3 2026`

AIS-03.1 Is data in transit encrypted (TLS 1.2+)?

Yes. All external traffic terminates on Azure App Service with TLS 1.2 minimum enforced. TLS 1.3 is preferred (Azure App Service defaults to modern cipher suites). Internal service-to-service calls use Azure App Service internal encryption. HSTS is active on the public domain.

`NIST: SC-8, SC-13`

AIS-04.1 Do you enforce role-based access controls for application users?

Yes. FedRAMP RBAC implemented with four roles: admin, analyst, readonly, audit. Permissions stored as JSONB in roles table. JWT-validated middleware enforces role checks on every API route. TOTP enforcement per-tenant. Per-session revoke and revoke-all supported. 4-fail login lockout per email+workspace.

`NIST: AC-2, AC-3, IA-2`

AIS-05.1 Are API endpoints protected against abuse (rate limiting, input validation)?

Yes. All auth endpoints have per-IP sliding-window rate limiting (5 req/min on POST /api/pilot, 5 req/min on POST /api/auth/login). JWT sessions expire. Per-session revoke supported. Input validation on all public endpoints. Slow queries exceeding SDLC thresholds are logged to slow_queries table with parameterized query text.

`NIST: AC-12, SI-3, SI-10`

02 — AUDIT ASSURANCE & COMPLIANCE

4 questions

AAC-01.1 Are audit logs immutable? Can they be tampered with or deleted?

Yes — write-once by design. DB triggers block UPDATE and DELETE on audit_logs. Every row has an immutable event_id (UUID v4) serving as an immutable export ID. Write-once enforced at the database layer. Tenant-scoped. CSV + JSON export available to admin users.

NIST: AU-9, AU-10, AU-11

AAC-02.1 Do you conduct regular security assessments or penetration testing?

Yes — SDLC-driven CI gates + Phase 3 SAR. Phase 3 (Security Assessment Report) of FedRAMP Moderate completed 2026-05-29. CI enforces 9 gates on every push. Manual penetration testing has not been conducted by an external firm — scheduled post-Seed funding (target Q4 2026).

NIST: CA-2, CA-8, RA-3

& In progress — External pentest — target Q4 2026

AAC-03.1 Do you maintain compliance certifications (SOC 2, ISO 27001, FedRAMP)?

FedRAMP Moderate assessment in progress. SOC 2 Type II not yet complete. FedRAMP Phases 0-3 complete. Phase 4 (Authorization to Operate) in progress. Not authorized — do not represent us as authorized to your CISO. SOC 2: no Type I or Type II report issued. On the post-Seed roadmap (target 2027).

NIST: CA-1, CA-6

& In progress — SOC 2 — target 2027 (post-Seed)

AAC-04.1 Is your infrastructure sub-processor list available and updated?

Yes — updated 2026-06-05. Five sub-processors: Azure App Service (application hosting, East US 2), Azure Database for PostgreSQL (database, East US 2), Postmark (transactional email, US), OpenAI (query strings only), Stripe (billing). ThreatRecall cloud is not FedRAMP Authorized today; self-hosted deployment remains the path for CUI/federal workloads until authorization is complete. Full table at /security §5.

NIST: SA-4, SI-12

03 — BUSINESS CONTINUITY & BCDR

4 questions

BC-01.1 Do you have a business continuity plan? When was it last tested?

Partial — formal BC plan not yet documented. Application is stateless at the application layer (PostgreSQL is the only state store). Azure App Service deploys provide basic redundancy. Azure Database for PostgreSQL has point-in-time recovery (PITR). SIGTERM graceful shutdown implemented. Formal BC/DR plan and tabletop exercise scheduled post-Seed (target Q1 2027).

NIST: CP-1, CP-2, CP-4

& In progress — Formal BC plan — target Q1 2027

BC-02.1 Are backups performed and tested regularly?

Yes — Azure Database for PostgreSQL provides automated continuous backup. Azure PostgreSQL runs with 7-day point-in-time recovery (PITR) on all branches. Backups retained by Azure PostgreSQL per their SLA. Manual DB export via /api/admin/demo-data endpoint. Full data export on pilot exit.

NIST: CP-9, SC-13

BC-03.1 What is your RTO and RPO for customer data?

RPO: <1 day (Azure PostgreSQL PITR). RTO: <4 hours (Azure App Service auto-restart + Azure PostgreSQL PITR restore). These are best-effort targets given current infrastructure. Formal RTO/RPO SLA not yet contractually committed — planned for Enterprise tier contracts. Self-hosted customers can define their own RTO/RPO.

NIST: CP-2, CP-10

& In progress — Contractual SLA — Enterprise tier (planned)

BC-04.1 Do you have a failover site or region-level redundancy?

No — single-region deployment (East US 2). Azure App Service services run in a single region. Azure Database for PostgreSQL runs in East US 2. Failover/DR region not yet implemented. This is on the post-Seed roadmap (target 2027). Self-hosted deployment path available for customers requiring multi-region redundancy.

NIST: CP-7

& In progress — Multi-region — target 2027 (post-Seed)

04 — CHANGE CONTROL

3 questions

CC-01.1 Is there a documented change management process?

Yes — SDLC Policy v1.2 governs change management. Changes flow through: branch !' CI gates !' PR review !' merge to main !' auto-deploy (Azure App Service). DDL changes require a migration file in migrations/ and are applied via npm run migrate. No changes made directly to production without PR and CI verification.

`NIST: CM-2, CM-3, CM-4`

CC-02.1 Are production changes tested before deployment?

Yes — CI gates enforce testing on every push. 9 CI gates run pre-merge: secret scan, npm audit, SAST (semgrep), license compliance, infra policy check, signed commit, CodeQL analysis, container image scan, bundle size gate. Regression tests for auth (39 passing) and SIGTERM drain (7 passing). No auto-merge to main without passing gates.

`NIST: CM-3, SI-6`

CC-03.1 Is there segregation of duties between development and production access?

Yes — human-readable RBAC + environment-level separation. Application code runs under a service account. Humans require GitHub PR review to push to main. Azure App Service deploys triggered by GitHub Actions on merge to main — no direct production access for developers. TOTP enforcement per tenant.

`NIST: AC-3, AC-5, CM-5`

05 — DATA SECURITY & LEAKAGE

5 questions

DS-01.1 Is data encrypted at rest in your database?

Yes — Azure PostgreSQL encrypts all data at rest by default with AES-256. Applies to all tables including kg_nodes, audit_logs, users, incidents, and all tenant data. Tenant data is further isolated via Row-Level Security (RLS) — each row has a tenant_id and RLS enforces isolation.

NIST: SC-28, MP-5

DS-02.1 What data do you send to your LLM provider (OpenAI)? Is customer CTI data exposed?

Query strings only. Customer CTI node content, evidence records, incidents, and AMBER/RED nodes never reach the LLM. The recall pipeline sends only the analyst plain-text query string to OpenAI for intent extraction and embedding generation. Node content is returned directly from PostgreSQL and bypasses the LLM. TLP:AMBER and TLP:RED nodes filtered at query layer. Enforced in services/recall.js — not a UI-level setting.

NIST: SC-8, SI-3, PT-2

DS-03.1 How is data isolated between tenants?

Two-layer isolation: application-level JWT + database-level RLS. Every API request validates a JWT containing a tenant_id. PostgreSQL RLS policies block cross-tenant reads and writes at the database layer. No multi-tenant row sharing. No shared secret keys between workspaces.

NIST: AC-4, SC-4

DS-04.1 Can customers export their data in standard formats?

Yes — CSV + JSON export for audit logs. Full data export on pilot exit (every kg_node, kg_edge, evidence_record, incident, audit_log, claim_record). No proprietary lock-in format. Knowledge graph data is structured and portable (STIX-compatible evidence records).

NIST: MP-5, SC-16

DS-05.1 Is CUI (Controlled Unclassified Information) processed by your service?

No — CUI is not processed by the cloud-hosted service. TLP:AMBER and TLP:RED nodes are never sent to OpenAI. ThreatRecall cloud is not FedRAMP Authorized today, so CUI should not be stored in the SaaS service. For CUI workloads, use the self-hosted deployment inside your approved FedRAMP CSP boundary.

NIST: MP-2, MP-5, SC-8

14 — SIG-Lite Excerpt (30 questions)

Data handling, encryption, access control, incident response, subprocessors, BCDR, vuln mgmt

SIG-01 — Where is customer data stored, and in which countries?

East US 2 (Azure Database for PostgreSQL). No data residency options yet. Self-hosted deployment allows deployment in any region.

NIST: SA-9, SC-7

SIG-02 — What encryption is applied to data at rest and in transit?

AES-256 at rest (Azure PostgreSQL default). TLS 1.2 minimum, TLS 1.3 preferred in transit (Azure App Service). HSTS active. Certificate auto-renewal.

NIST: SC-8, SC-13, SC-28

SIG-03 — Is customer data sent to third parties? Which ones?

Yes — five subprocessors: Azure App Service, Azure PostgreSQL, Postmark (email addresses only), OpenAI (query strings only), Stripe. Full table at /security §5.

NIST: SA-4, SI-3

SIG-04 — How do you ensure AMBER/RED TLP nodes never leave your system?

Two-layer enforcement: classification at ingest (stored in kg_nodes.tlp) + filter at query time before any LLM call. Enforced in services/recall.js.

NIST: SC-8, SI-3, PT-2

SIG-05 — Do you have RBAC and least-privilege enforcement?

Yes — FedRAMP RBAC with four roles (admin/analyst/readonly/audit). JWT-validated middleware on every API route. Tenant isolation via RLS. Per-session revoke. 4-fail lockout.

NIST: AC-2, AC-3, AC-5

SIG-06 — Are audit logs tamper-proof? Can they be used for forensic investigations?

Yes — write-once by DB trigger. DB triggers block UPDATE/DELETE on audit_logs. Immutable event UUIDs. Tenant-scoped. CSV + JSON export. System-sentinel rows for AI-agent requests.

NIST: AU-9, AU-10, AU-11

SIG-07 — What is your incident response process and RTO?

IR process: detection !' triage !' containment !' eradication !' recovery. Structured IR records supported. security@threatengram.com — 1 business day response. Formal IR plan post-Seed. RTO best-effort <4 hours.

NIST: IR-1, IR-2, IR-4, IR-6

SIG-08 — What happens to customer data if the service is terminated?

Full data export on pilot exit. No proprietary lock-in format. Structured, portable data. Data retained 30 days after cancellation then deleted per retention policy.

NIST: MP-5,
SC-16

SIG-09 — Is there a BCDR plan? Where are backups stored?

Azure PostgreSQL PITR provides 7-day point-in-time recovery. Formal BCDR plan not yet documented. Failover region not implemented. Formal plan and multi-region scheduled post-Seed.

NIST: CP-2, CP-7, CP-9

SIG-10 — How are vulnerabilities discovered and remediated?

9 CI gates on every push: secret scan, npm audit, SAST, license check, infra policy, signed commit, CodeQL, container scan, bundle size. Critical CVEs remediated within 7 days. External pentest scheduled post-Seed.

NIST: RA-3, RA-5,
SI-2

SIG-11 — Can customers deploy in an air-gapped environment?

Yes — self-hosted deployment with optional air-gapped mode. Set OLLAMA_BASE_URL to local Ollama endpoint. Air-gapped mode disables LLM (keyword search only).

NIST: SC-7, SC-8

SIG-12 — How do you handle API key management for programmatic access?

Per-tenant API keys with SHA-256 hash storage. Raw key shown once at creation, never retrievable. last_used_at tracked. revoked_at for immediate revocation. AI agents use these for MCP server calls.

NIST: IA-5,
SC-12

SIG-13 — Is there a mechanism for memory corrections with rollback?

Yes — memory corrections with 24h rollback window. Three types: reject (reason + category), correct (full version history via memory_versions), merge (per-field decisions). Admin rollback via /api/admin/rollback-correction/:id.

NIST: AU-2,
SI-12

SIG-14 — What compliance frameworks are you aligned with?

FedRAMP Moderate in progress (Phases 0-3 complete). NIST 800-53 Rev 5 Moderate (primary). SOC 2 Type II not yet complete (target 2027). Full posture at /security.

NIST: CA-1,
CA-6

SIG-15 — Do you have a security contact for responsible disclosure?

Yes — security@threatengram.com. Response within 1 business day. No bug bounty program yet — acknowledged and credited when implemented.

NIST: IR-6,
SA-3

Questions not answered here?

Email security@threatengram.com. We respond within 1 business day.

For CUI workloads, federal requirements, or Azure Government deployments:

Use the self-hosted deployment inside your approved FedRAMP CSP boundary, or wait for FedRAMP authorization (Phase 4 completion, post-Seed).

Document version 1.0 · 2026-05-29 · Threat Engram LLC · EIN: 99-1234567