Shomar Security Platform

A CyberCapSec LTD product

Shomar Vendor Procurement Pack

Pre-filled VSQ, security-control answers, architecture summary, and data-flow baseline

Audience

Bank, fintech, enterprise, partner, public-sector, risk, security, procurement, and compliance teams reviewing Shomar.

Shomar Security Platform is a CyberCapSec LTD product for security operations, compliance evidence management, and regulated technology teams.

This resource is provided for planning and readiness support. It is not legal, regulatory, or audit attestation advice.

Purpose

This pack gives enterprise procurement and risk teams a ready baseline for Shomar vendor due diligence. It is intended to shorten bank and fintech procurement cycles by answering common security, architecture, integration, and data-handling questions before a custom questionnaire is issued.

Customer-specific items such as deployment model, retention, evidence storage mode, data residency, SLA, and dedicated worker requirements should be confirmed in the final contract or security addendum.

- Pre-filled vendor security questionnaire answers.
- Architecture and data-flow summary.
- Encryption, MFA, RBAC, logging, API security, and tenant-isolation notes.
- Customer-specific confirmation checklist for procurement teams.

Standard VSQ answers

The standardized VSQ source lives in docs/vendor-procurement-pack/vendor-security-questionnaire.md. The answers below summarize the most common bank and fintech risk queries.

- Encryption in transit: production endpoints should use HTTPS with TLS 1.3 as the target baseline for browser, API, webhook, worker, and integration traffic.
- Encryption at rest: database volumes, object storage, backups, and evidence stores should use AES-256 storage encryption where supported by the provider or customer-owned storage.
- Sensitive values: provider tokens and sensitive stored values use application field-level encryption; API keys and refresh tokens are stored as hashes rather than retrievable plaintext.
- MFA: TOTP MFA enrollment, verification, and privileged-role enforcement are supported where configured.
- RBAC: role hierarchy and fine-grained permission checks govern users, scans, projects, compliance, settings, audit, reports, API keys, and workers.
- Audit logging: audit events include actor, organization, resource, result, timestamp, IP, user agent, request ID, and tamper-evident hash-chain fields where available.
- API security: APIs use JWT Bearer authentication and scoped API keys, with organization context, permission checks, security headers, rate limiting, and webhook signing support.

Architecture and data flow

The shareable architecture diagram is available at https://shomar.io/resources/shomar-architecture-data-flow.svg. It shows users, the Shomar web app, API and auth layer, source-control integrations, CI/CD inputs, scan workers, storage, audit logs, reports, and encryption boundaries.

- Users access the Shomar web app over HTTPS and interact with dashboards, evidence workflows, findings, reports, and administrative settings.
- The web app calls the API and auth layer, where JWT, SSO/OIDC, MFA, RBAC, API scopes, rate limiting, and organization context are enforced.
- Source-control and CI/CD integrations submit repository metadata, scan requests, webhook events, SARIF artifacts, and CodeQL-compatible evidence through authenticated APIs.
- Scan work runs through SaaS workers or customer-controlled workers depending on plan and source-code policy.
- Findings, evidence records, reports, audit logs, and compliance mappings are stored in the data layer with tenant scoping and encrypted-storage baselines.
- Evidence can remain Shomar-managed, customer-owned, or externally linked depending on confidentiality and residency requirements.

Integration surfaces

- Browser app: customer users, admins, auditors, engineers, compliance teams, and executives.
- REST API: authenticated product, integration, scan, compliance, reporting, and admin workflows.
- Source control: GitHub, GitLab, Bitbucket, Azure DevOps, and approved repository integrations.
- CI/CD: Jenkins, Azure DevOps, CircleCI, GitLab CI, GitHub Actions, SARIF, and CodeQL-compatible evidence paths.
- Scan workers: standard SaaS execution, customer-controlled workers, dedicated tenant patterns, and sovereign/on-prem options where scoped.
- Evidence storage: Shomar-managed storage, customer-owned storage, external-link evidence, and report artifact storage.
- Webhooks: outbound event delivery and integration workflows with signing and retry support where configured.

Security and privacy posture

- Tenant isolation: organization-scoped auth context, Postgres RLS capability, and tenant-prefixed cache keys.
- Data minimization: customers should avoid uploading secrets, production credentials, or private keys unless a secure evidence-handling workflow has been agreed.
- Source-code handling: standard SaaS scans can use controlled workers; sensitive teams can use customer-controlled workers or artifact-only workflows.
- Secrets redaction: sensitive-token redaction is applied before managed AI analysis paths where those paths are used.
- Rate limiting and security headers: backend middleware supports HTTPS redirects, security headers, CORS configuration, and Redis-backed rate limiting with fallback.
- Auditability: security-relevant events are visible to organization admins and platform teams according to role and scope.

Procurement attachments

- Vendor Procurement Pack PDF.
- Pre-filled Vendor Security Questionnaire markdown source.
- Architecture and Data Flow markdown source.
- Architecture and Data Flow SVG diagram.
- Security and Data Residency Whitepaper.
- Compliance, Evidence, and Data Residency Guide.
- Customer-specific DPA, security addendum, SLA, deployment architecture, penetration test evidence, or compliance certificate where applicable.

Customer-specific confirmation checklist

- Deployment model: SaaS, dedicated tenant, customer-controlled worker, sovereign, or on-prem.
- Evidence storage mode: Shomar-managed, customer-owned, external-link, or mixed.
- Data residency requirements, storage region, backup region, and cross-border transfer expectations.
- Retention and deletion timelines for logs, evidence, reports, artifacts, and account records.
- Required cryptographic configuration, including TLS policy, AES-256 storage encryption confirmation, and key ownership.
- SSO/MFA enforcement, role design, administrator list, and service-account/API-key scope.

- Support SLA, incident escalation contacts, procurement deadline, and regulator or auditor evidence format.

Disclaimer

This pack supports vendor due diligence and procurement readiness. It is not legal, regulatory, audit, or security attestation advice. Final answers should be reviewed against the customer's contract, deployment model, data-processing terms, and evidence requirements.