Shomar Security Platform

A CyberCapSec LTD product

Shomar White Paper

Africa’s Security and Compliance Operating System

Audience

Security leaders, compliance teams, fintech operators, bank technology teams, auditors, and platform buyers.

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.

Executive summary

Shomar is a security and compliance operating platform built by CyberCapSec LTD for African organisations that need to run security work and regulatory readiness from one place.

The platform combines application security, VAPT, dependency and container risk, evidence management, regulatory monitoring, workflow assignment, and reporting. Its strongest differentiation is not a single scanner. It is the way security findings become compliance evidence, remediation tasks, executive reports, and audit-ready records.

- Security operations: repository-bound scans, VAPT workflows, findings, tasks, retesting, and reports.
- Compliance operations: assigned framework bundles, gaps, evidence, ownership, reassessment, and exports.
- African context: NDPR/NDPA, CBN controls, NIBSS/NPS readiness, PCI DSS, ISO 27001, and regional regulatory intelligence.

The market problem

African financial institutions, fintechs, public-sector bodies, and high-growth technology teams face a difficult mix of threats, audits, budget pressure, and talent constraints.

Most organisations already have fragments of the answer: a scanner here, a spreadsheet there, a ticket queue, a GRC tracker, and PDF reports from consultants. The result is operational friction. Findings do not naturally become remediation work. Compliance gaps are disconnected from live security posture. Evidence collection becomes a recurring scramble.

- Security tools often stop at detection instead of driving remediation and audit evidence.
- Global compliance products rarely model African regulatory expectations deeply enough.
- Manual evidence gathering creates delay, inconsistent records, and weak board-level visibility.
- Smaller teams need enterprise-grade posture without enterprise-grade complexity.

What Shomar provides

Shomar gives teams one workspace for security scans, compliance gaps, evidence, regulatory alerts, and reports. Platform admins can assign framework bundles to each organisation, while each organisation only sees its subscribed scope.

The product is designed for pragmatic adoption: start with repository-bound scanning and compliance evidence, then extend into VAPT, CI/CD, webhooks, IDE integrations, and customer-owned evidence storage.

- Application security: SAST, secrets, dependency, container, IaC, and mobile security workflows.
- VAPT: public IP, internal IP, firewall, black-box, web, TLS, and wireless assessment support.
- Compliance: gaps, evidence, owner assignment, assessment retakes, and executive reports.
- Operations: audit logs, feature flags, tier limits, webhooks, integrations, API keys, and usage controls.

Reference architecture

Shomar separates the product surface, API, database, cache, and scan-worker runtime. This keeps long-running scans away from the interactive web application and gives the platform a clearer scaling path.

- Source repositories, CI/CD events, VAPT targets, and uploaded artifacts enter through controlled APIs.
- Dedicated workers run scan jobs, normalize results, deduplicate findings, and enrich risk context.
- The risk engine scores severity, confidence, asset context, exploitability signals, and business priority.
- The compliance engine maps findings and evidence to controls across assigned framework bundles.
- Dashboards and reports expose posture, gaps, tasks, and readiness without exposing scanner internals.

Security and data governance

The product model assumes that customers may handle sensitive code, payment data, personal data, and confidential evidence. Shomar therefore supports tenant boundaries, scoped API keys, repository-bound scanning, and customer-owned evidence storage patterns.

Where regulations require local data residency, organisations can attach external storage or evidence links so sensitive documents remain in approved repositories while

Shomar tracks the audit trail.

- Repository scans are bound to imported projects rather than arbitrary external code targets.
- Evidence can be stored in Shomar-managed storage or customer-owned storage, depending on policy.
- API keys and integrations should use least privilege, rotation, audit logging, and revocation.
- Regulated customers can request sovereign, dedicated, or on-prem deployment discussions.

Compliance model

Compliance in Shomar begins with framework bundle assignment. The platform or super admin selects the bundle during onboarding, and the organisation then receives only the frameworks included in that licence scope.

Gaps are generated from assigned controls, evidence state, and scan-derived posture. This means a vulnerability, failed configuration, or missing evidence item can become an actionable compliance gap with an owner and due date.

- Nigeria: CBN cybersecurity, NDPR/NDPA, NITDA, NIBSS/NPS, payment and fintech readiness.
- Global standards: PCI DSS, ISO 27001, CIS Controls, SOC 2, SWIFT CSP, and cloud baseline controls.
- Workflow: assign gap, submit evidence, remediate finding, retake assessment, export report.
- Regulatory intelligence: live-ingested changes can be reviewed before becoming compliance alerts.

Commercial model and trial

Shomar uses annual licences with feature flags and usage limits by tier. New organisations can be offered a trial period of 10 working days or 14 calendar days. After the trial expires, the organisation needs an active paid licence to continue using the platform.

- Starter: core scanning and compliance for smaller teams.
- Growth: broader scan volume, NPS readiness, PCI DSS mapping, and African threat intelligence.
- Business: full compliance suite, higher VAPT volume, SSO, and priority support.
- Enterprise: banks, government, sovereign deployments, dedicated VAPT, SLA, and customer success.

Conclusion

Shomar is designed to become the security and compliance operating system for African organisations that need credible posture, practical workflows, and local regulatory context. It is not just a scanner dashboard. It is a way to connect security activity to remediation, evidence, and executive assurance.