THREATSVIEW
Make it Simple

Tier-1 Gulf Bank Consolidates Vulnerability Chaos Across 18,000 Assets

Client profile

A leading retail and corporate bank headquartered in Doha, with branches across the GCC and an asset estate of roughly 18,000 endpoints, servers, and web applications.

The challenge

The InfoSec team was running Tenable.sc for infrastructure scanning, Fortify for SAST, and quarterly third-party penetration tests. Findings lived in separate dashboards, PDF reports, and Excel trackers. Asset owners weren't notified automatically, SLA breaches went unnoticed, and producing a single board-level risk view took the CISO's team three full days each quarter.

Why ThreatsView

The bank needed one platform where every finding scanner-generated or human-discovered could be deduplicated, mapped to an asset owner, prioritized by business criticality, and tracked to closure against Qatar Central Bank security circulars.

Implementation highlights

Tenable.sc and Fortify were connected via native integrations within two weeks.

Assets were imported from the CMDB and tagged by criticality (Crown Jewel, High, Medium, Low).

SLAs were configured by severity (**Critical: 7** days, **High: 30** days).

Jira was wired in so remediation tickets auto-created and synced status.

Results & impact

- Mean time to remediate (MTTR) for critical vulnerabilities dropped from 47 days to 11 days within one quarter.
- Duplicate findings across tools fell by an estimated 38% after deduplication rules were tuned.
- Quarterly board risk report generation went from 3 days to under 2 hours.
- Auditor evidence requests for the QCB inspection were served from ThreatsView's audit log directly.

> *"For the first time we have one number we trust for residual risk and we can show the auditor exactly how we got there."*
>
> **— Head of Information Security**