THREATSVIEW
Make it Simple

Government Ministry Aligns to QCSF and NIA Policy Through Centralized Compliance Automation

Client profile

A Qatar-based government ministry with citizen-facing digital services, internal administrative systems, and obligations under the Qatar Cyber Security Framework (QCSF) and the National Information Assurance (NIA) Policy.

The Challenge

The ministry was required to demonstrate continuous compliance against NIA and QCSF control catalogues, conduct regular penetration testing on public-facing services, and provide quarterly assurance reports to the national cybersecurity authority. The existing approach was manual, fragmented across teams, and consumed significant analyst time.

Why ThreatsView

Built-in support for NIA and QCSF control libraries — combined with penetration testing project management — meant the ministry could replace multiple tools and spreadsheets with one platform that already understood the local regulatory landscape.

Implementation highlights

- NIA Policy v2.0 and QCSF control catalogues loaded as compliance frameworks.
- Public-facing applications onboarded as crown-jewel assets.
- Scheduled internal and external penetration testing with separate workspaces.
- Findings routed to system owners via automated email and Jira tickets.

Results & impact

- Reduced manual effort on quarterly NIA/QCSF reporting by approximately 75%.
- Demonstrated traceable evidence for over 90% of applicable controls within nine months.
- Closed 41 high-severity penetration testing findings within agreed SLAs in the first reporting period.
- Stood up a reusable penetration testing playbook used across four downstream entities.

> *"Compliance stopped being a fire drill and became part of how we operate."*
>
> **— Director of Information Security**