THREATSVIEW
Make it Simple

Government Digital Services Agency Industrializes Internal Pen Testing for 200+ Citizen-Facing Applications

Client profile

A government digital services agency responsible for delivering and maintaining 200+ citizen-facing and back-office applications — e-services portals, payment gateways, identity verification systems, and ministry-specific tools. The agency mandates penetration testing before every production release and on a recurring basis for live applications.

The challenge

With application releases happening weekly across dozens of squads, the AppSec function couldn't keep up. The previous process relied on a central mailbox where development teams requested pen tests, pen testers (a mix of in-house and external consultants) producing PDF reports, developers emailing testers for retests, and an Excel master log maintained by a single AppSec coordinator who became the bottleneck for the entire program. When the coordinator was on leave, the program effectively paused. External consultants had no consistent format, making cross-application risk reporting impossible.

Why ThreatsView

The agency needed to industrialize the workflow — every application as an inventory item, every developer and tester (internal or external) as a managed user, every finding logged in a structured way with consistent severity, and every retest tracked without human chasing.

Implementation highlights

Application inventory
All 200+ applications onboarded as assets, grouped by ministry and tagged with go-live cadence (one-time pre-release, recurring quarterly, recurring annually).

Developer onboarding
Over 400 developers across squads onboarded with squad-level groupings. Findings auto-route to the squad lead, who reassigns to the right engineer.

Tester onboarding
In-house pen testers given full project access. External consultancies onboarded as restricted-access users — they can only see and log findings against contracted applications, with engagement-scoped permissions and expiry dates.

Structured finding template
A mandatory finding template enforced across both internal and external testers — CVSS, OWASP/CWE mapping, affected URL/endpoint, reproduction steps, screenshot evidence, remediation guidance.

Developer-tester handshake
Findings flow directly tester → developer. Developer comments and "Ready for Retest" status visible to tester in real time. Tester re-validates and either closes or reopens with reasoning.

Recurring test scheduling & reporting
Live applications scheduled for recurring assessments with auto-generated test projects and one-click penetration test reports in the agency's official template.

Government Digital Services Agency Industrializes Internal Pen Testing for 200+ Citizen-Facing Applications

Results & impact

- Pen testing throughput approximately doubled within six months without adding tester headcount.
- The single-coordinator bottleneck eliminated — every squad self-serves on status, history, and retest progress.
- External consultancies now deliver findings in the agency's standardized format on day one, eliminating ~two weeks of post-engagement formatting per project.
- Cross-application risk reporting — previously impossible — now available as a live dashboard segmented by ministry.
- Audit findings related to "inconsistent pen-test evidence" closed permanently.
- Developer-side satisfaction with the AppSec process improved sharply, with squads citing clarity, evidence, and absence of email chasing as top reasons.

> *"We turned a coordinator-dependent inbox into an industrial process. The same team now ships twice the assurance work."*
>
> **— Director of Application Security**