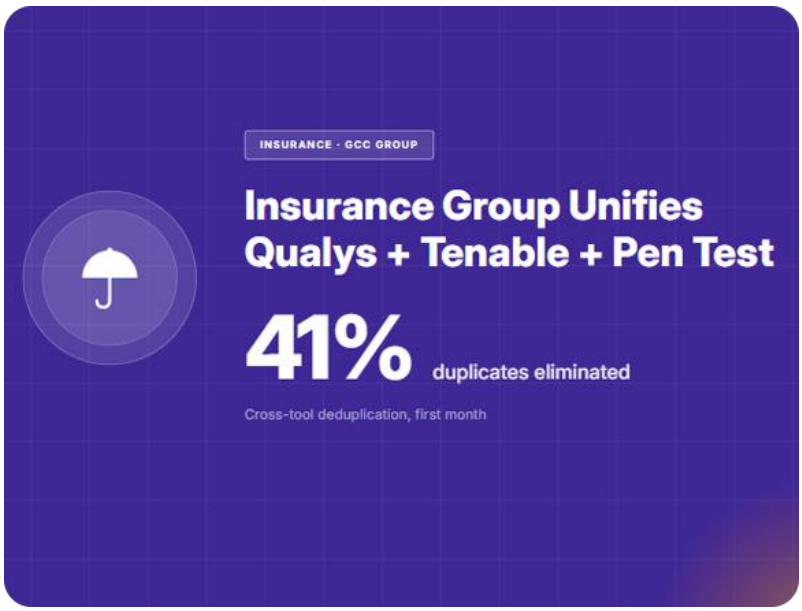
THREATSVIEW
Make it Simple

# Insurance Group Standardizes End-to-End Remediation Across Qualys, Tenable, and Manual




## Client profile

A regional insurance and asset management group with subsidiaries across the GCC, running Qualys VMDR for cloud and external scanning, Tenable.sc for internal infrastructure, and quarterly third-party penetration tests for customer-facing applications.

## The challenge

Each tool had its own console, severity scoring, and reporting cadence. Remediation owners were assigned manually in spreadsheets. The same vulnerability sometimes appeared in both Qualys and Tenable for the same asset, creating duplicate work. Most painfully, when an engineer marked a ticket "fixed" in Jira, nobody re-ran the scanner to confirm — leaving the team blind to silently-failed remediations.

## Why ThreatsView

The group needed a single remediation workflow that worked identically regardless of where a finding originated — automated scanner, pen test, or bug bounty — with consistent SLA enforcement and a closed-loop validation step against the originating tool.

## Implementation highlights

- Qualys VMDR and Tenable.sc both integrated; findings normalized to a single severity model based on CVSS plus business-context risk score.
- Cross-tool deduplication enabled — CVEs detected by both scanners on the same asset were merged into a single finding with both source references retained.
- Pen-test findings imported directly from the testing project workspace into the same remediation queue.
- Auto-assignment driven by asset owner attribute pulled from the CMDB.
- Applied SLA rules based on severity and asset criticality (e.g., Crown Jewel assets: 3-day SLA; low-criticality dev assets: 30-day SLA).
- Implemented auto-resync logic with on-demand rescans via Qualys/ Tenable APIs, confirming closure only when findings were absent.

## Results & impact

- Duplicate findings across scanners reduced by 41% in the first month.
- Average remediation time reduced by 58% across the estate.
- Resync logic caught and reopened ~9% of falsely closed tickets with remediation diffs.
- The Group CISO now reports a single trusted risk score to the audit committee monthly.

> *"We stopped arguing about whose tool was right. The platform just told us what was real."*
>
> **— Group Head of Cybersecurity**

sales@threatsview.com | www.threatsview.com