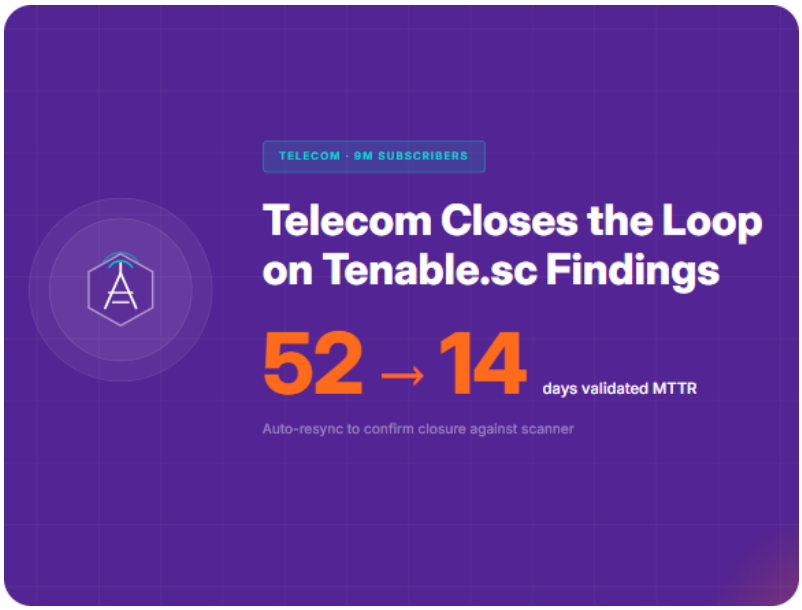
THREATSVIEW
Make it Simple

Regional Telecom Operator Closes the Loop on Tenable.sc Findings Across 40,000 Assets



Client profile

A telecommunications operator serving over 9 million subscribers across two countries, with a hybrid estate of 40,000+ assets spanning core network infrastructure, BSS/OSS systems, retail branch IT, and customer-facing portals. Tenable.sc was the standardized enterprise vulnerability scanner.

The challenge

Tenable.sc was generating between 80,000 and 120,000 raw findings per scan cycle. The vulnerability management team triaged in the Tenable console, emailed CSV exports to seven different remediation teams, and chased status over Teams and email. When teams reported "patched," nobody re-scanned to confirm. Auditors repeatedly flagged the gap between reported remediation and validated remediation.

Why ThreatsView

The team needed Tenable.sc to remain the source of truth for scanning, but wanted ThreatsView to own the lifecycle — ingestion, deduplication, ownership routing, SLA enforcement, and most importantly, automated revalidation by resyncing with Tenable to confirm a vulnerability genuinely disappeared from the next scan.

Implementation highlights

- Tenable.sc connected via native integration; scan results pulled automatically on each completed scan cycle.
- Findings deduplicated and grouped by asset, CVE, and plugin ID.
- Assets mapped to remediation queues via CMDB tags, with auto-assigned findings.
- SLA policies configured with automated breach escalations at 75% of SLA elapsed.
- Auto-closes resolved findings and reopens tickets with audit trail intact if findings reappear.

Results & impact

- Validated (not just reported) MTTR for critical findings dropped from 52 days to 14 days within two quarters.
- Approximately 12% of findings previously marked "remediated" by teams were caught by the resync as still present and automatically reopened — closing a long-standing audit gap.
- Eliminated manual CSV exports entirely; vulnerability analysts reclaimed an estimated 30+ hours per week.
- First clean external audit on vulnerability management closure evidence in three years.

> *"Tenable tells us what's broken. ThreatsView makes sure it actually gets fixed — and proves it."*
>
> **— Vulnerability Management Lead**

sales@threatsview.com | www.threatsview.com