THREATSVIEW
Make it Simple

Manufacturing & Logistics Conglomerate Unifies Six Security Tools Into One Remediation Workflow

Client profile

A diversified manufacturing and logistics conglomerate with 22 operating companies, 60+ sites globally, and a security toolset that had grown organically: Tenable.sc for IT infrastructure, Tenable.ot for plant-floor environments, Checkmarx for SAST, Acunetix for DAST, CrowdStrike Falcon for endpoint findings, and an external attack surface management tool for internet-facing exposure.

The challenge

Six tools meant six consoles, six severity scales, six export formats, and six remediation processes. The central security team had visibility into none of it end-to-end. Each operating company self-reported remediation status in monthly slide decks. There was no mechanism to verify whether a reported fix actually held up against the next scan.

Why ThreatsView

The mandate was simple — every finding from every tool should land in one queue, route to the right team, enforce a uniform SLA, and only close when the originating tool confirmed the issue was gone.

Implementation highlights

Integrated all six tools with optimized ingestion frequencies (real-time for CrowdStrike, scan-cycle-based for Tenable and Acunetix, build-triggered for Checkmarx).

Unified risk scoring model applied across all sources — engineers stopped seeing different ‘severities’ depending on which tool detected the issue.

Asset ownership inherited from a master asset registry; each operating company had its own queues but rolled up into a group-level dashboard.

Standardized SLA contract across the group, with operating-company-specific exception workflows requiring CISO sign-off.

Implemented tool-specific resync validation with evidence-backed closure confirmation for every finding.

Results & impact

- Consolidated six remediation processes into one within four months.
- Reduced the group-level vulnerability backlog by 46% in the first year.
- Automated revalidation reopened ~9% of falsely closed findings, exposing hidden process gaps.
- Replaced a 40-slide manual board report with a single live dashboard export.

> *“Before ThreatsView, every operating company had its own version of the truth. Now there’s one — and the scanners themselves prove it.”*

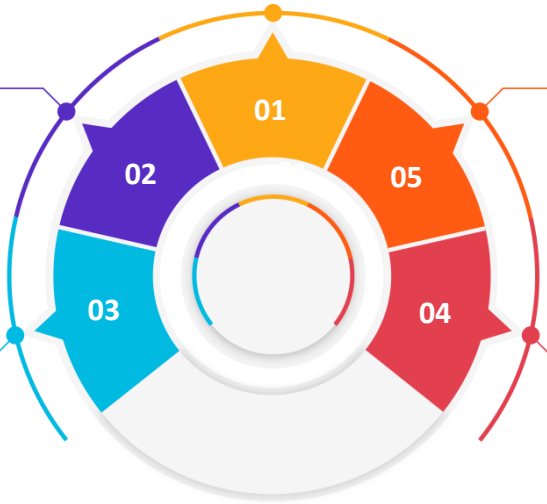
— Group Chief Information Security Officer

Appendix A: The Closed-Loop Vulnerability Lifecycle

Across Case Studies 06, 07, and 08, the same five-step lifecycle is what turns vulnerability management from a reporting exercise into a measurable risk-reduction program:

Ingest

Findings stream in from Tenable.sc, Qualys, Checkmarx, Acunetix, CrowdStrike, penetration testing projects, or any combination, via native integrations.



Normalize & deduplicate

Severity scales unified, duplicate findings across tools merged, business-context risk score applied.

Auto-assign

Asset owner attribute drives ticket routing to the right remediation team without human intervention.

Resync & validate

Closure isn't trusted on the engineer's word; the originating tool is re-queried, and the ticket only closes when the finding is genuinely gone. If it reappears, it reopens automatically.

Enforce SLA

Severity-and-criticality-based timers run with automated escalations to team leads and management on breach.