3. Violation Reports

Violation Reports generally refer to compliance or policy violations that an automated scanner identifies. For instance, a daily script might check your codebase or server configurations and log any suspicious results:

1. **NPM**: Could be scanning for vulnerable dependencies in a Node.js project.
2. **SERVER_SCAN**: Might check server configurations, open ports, or outdated libraries.
3. **SYNC**: Another custom tool or integration that reports code or config discrepancies.

> Once a violation is “found,” security engineers review it, assign it a State (e.g., “In progress”), and, after investigation, mark it “Resolved” or “Not processed” if it’s a false positive or low priority.

Use Cases

#1. Updating Vulnerable Dependencies
A daily NPM scan detects outdated packages in a Node.js project. Engineers mark the report as "In progress", update the dependencies, and resolve the issue.

#2. Server Configuration Errors
A SERVER_SCAN identifies open ports. The IT team secures the ports and marks the violation as "Resolved".

#3. Sync Discrepancies
A SYNC scan flags code inconsistencies after deployment. Developers review the logs, sync configurations, and close the report.

#4. False Positives Management
An automated scan reports a minor issue. The security team reviews the report and marks it as "Not processed" if deemed harmless.

Typical Workflow

1. Daily/Periodic Scans
A security scanner (via API integration, not by default) runs on a server or code repository on a set schedule, reporting:
"notFound" – No issues detected.
"found" – Issues identified for review.

2. Report Creation
The system automatically creates a Violation Report entry, or a security engineer manually logs it.

Fields include:
Server name: Which server was scanned.
Tool: Name of the scanning tool (e.g., NPM, SERVER_SCAN, SYNC).
Result: Was a violation discovered (found) or not?
State: Whether the issue is “Not processed,” “In progress,” or “Resolved.”
Project: Which project or environment the server is linked to.
Created at/Updated at: Timestamps for when the record was created or last updated.
Description: Any extra details or logs from the scan.

3. Engineer Review
A security engineer checks the new violations.
If the issue needs action, they mark it as “In progress.”

> Once it’s handled or deemed harmless, they set State to “Processed” (or a similar status).

Table View

Use **Table** view for a spreadsheet-style overview, sortable and filterable by any column. By default, you’ll see:

Column	Description
Severity ⇅	Visual severity icon (— for Medium, ↓ for Low, ↑ for High/Critical). Click to sort by severity level.
Created at ⇅	Timestamp when the report was first logged.
Title	Clickable report name; opens the Edit panel.
CVSS v3 Score	The numeric CVSS score (e.g. 7.5).
Assigned to	One or more engineer names/UIDs.
Tool ⇅	Scanning tool (e.g. NPM, SYNC, SERVER_SCAN). Click to sort.
Scan type	Code base or Server scan.
Component	If Code base → module or repo path.
Server name	If Server scan → hostname or IP.
Project	Linked project name.
SLA	Target remediation date / time.
Updated at	Timestamp of the most recent update to the report (status change, reassignment, or edit).
Status	Current workflow state of the report (Open, In Progress, Resolved), editable directly from the table via dropdown.

> **Overdue alert:** If the SLA has expired and the report is not closed, the SLA cell is shaded **red** to draw immediate attention.

> **Violation Reports – Clickable Title**
> In the Table view for Violation Reports, the **Title** column entries are clickable: clicking any Title opens the full-width “View Violation Report” drawer, displaying all of that report’s fields, history, attachments, resolution summary, and close details.

Sorting & Total: Sort reports by any column. The **Total** count shows how many entries match your current view.

Board (Kanban) View

> **Board** view—a Kanban-style layout groups reports into columns by **Status**. Drag & drop cards between **Open**, **In Progress**, **Resolved** to update their status in real time.

Use the **Board** view for a high-level, drag-and-drop workflow:

Columns: One column per status—

1. **Open**
2. **In Progress**
3. **Resolved**

Cards: Each report card shows:

1. **Title**
2. **Created at** (with calendar icon)
3. **Snippet of Description**
4. **CVSS score** badge in the top-right

Adding a Violation Report

To log a new compliance or policy violation:

1. Open the Add Form
Click the **+ Add** button in the top-right corner of the **Violation reports** table.

2. Fill in the Report Details
In the “Add violation report” side panel, complete the following fields:

1. **Title:** A short, descriptive name for the issue (e.g. “SQL Injection in Login”).
2. **CVSS v3:** Enter the numeric vulnerability rating (e.g. 7.5) based on the Common Vulnerability Scoring System.
3. **Severity:** Manual classification of the issue (Low, Medium, High, Critical) used for visual prioritization.
4. **Tool:** Select which scanner or pen-test tool generated this report.
5. **Scan Type**
   ▸ **Codebase** → reveals an extra **Component** text field (e.g. the repo path or module name).
   ▸ **Server Scan** → reveals **Server IP** and **Server Hostname** fields.
6. **Component** *(only if Codebase):* Free-text name of the sub-system or code module affected.
7. **Server IP** & **Server Hostname** *(only if Server Scan):* Identify the scanned host (e.g. 192.0.2.15 / api-prod-01.example.com).
8. **Assigned to:** Pick one or more engineers responsible for triage.
9. **Project:** Link this report to the appropriate project or environment.
10. **SLA** *(optional):* Set a target remediation date/time.
11. **Penetration report** *(optional):* Link to a related pen-test entry if available.
12. **Description:** Use the rich-text editor to paste or type detailed logs, error messages, or remediation notes.

3. Save the Report
When all mandatory fields are populated, click **Save** to create the new Violation Report.
The report will now appear in your table (and board) views, ready for review and triage.

Editing a Violation Report

1. Locate the record
In **Table** view, scroll or search to find the row for the violation you want to update.
In **Board** view, find the card in its status column.

2. Open the edit form:
Table: Click the **Edit** (✏) icon in the **Actions** column.
Board: Hover over the card and click the pencil icon or the “⋯” menu, then choose **Edit**.

3. Make your changes
In the side-panel form you can update any field:

1. **Status** (Open, In Progress, Resolved, etc.)
2. **Severity**
3. **Assigned to**
4. **Scan type**, **Tool**, **Component**, **Server name**
5. **SLA**, **Penetration report**
6. **Description** (detailed notes or logs)

4. Save: Click **Save** at the bottom of the panel to apply your edits.

Closure Workflow

When you mark a Violation Report “Processed,” it now—rather than simply updating the status—opens a mandatory “Close Report” dialog so you capture a concise **Resolution Summary**. This guarantees every closed finding has:
Complete Context: How it was fixed or verified
Accountability: Who closed it and when
Audit Trail: Full details bundled into one log entry

What’s New

1. **Close Dialog Auto-Opens:** As soon as you set a report’s status to **Processed**, the **Close Report** modal pops up—pre-filled with all original fields and forcing you to enter a **Resolution Summary** before the change can be saved.
2. **Mandatory Summary:** You cannot finish without entering a brief resolution note.
3. **Data Snapshot:** Read-only view of all original fields (Project, Title, CVSS, Severity, Tool, Scan Type + Component/Server, Description).
4. **Atomic Audit Log:** The system records the summary, closer’s username, and timestamp together.

How It Works

1. **Locate & Process:** In Table or Board view, set State → Processed.
2. **Review Snapshot:** Confirm Project, Title, CVSS v3, Severity, Tool, Scan Type details, and Description.
3. **Add Summary:** Enter your remediation steps, verification, and notes.
4. **Save to Close:** Click **Save**; the summary appears in details and audit logs.

> **Benefit:** Every closed report is now a self-contained record of what was found, who fixed it, how, and when—making compliance and troubleshooting faster and more reliable.

Deleting a Violation Report

1. **Find the violation:** In **Table** view, locate the row you wish to delete.
2. **Click the trash icon:** Click the **Delete** (□□) icon in the **Actions** column for that row.
3. **Confirm deletion:** In the confirmation dialog, click **Delete** again to permanently remove the report

> **Warning:** Deleted violation reports cannot be restored. Be sure you no longer need the record before confirming deletion**.**

Filtering & Searching

1. **Filter Panel:** Click **Filter** to narrow by **Status** or **Tool**.
2. **Search Bar:** Type a partial or full server name in the **Search** field to find specific reports instantly.

Revision #24
Created 27 February 2025 08:57:28
Updated 27 January 2026 12:01:38