2. Incident Reports

The **Incident Reports** section in Security Core is essential for tracking and managing security-related or general system issues such as bugs, vulnerabilities, and unexpected behavior. It ensures efficient incident resolution, reduces downtime, and strengthens system security by providing structured workflows for issue management.

Use Cases

1. **Create Incident:** A security engineer or developer logs a new issue, ensuring all security concerns are documented.
2. **Assign & Update:** The incident is assigned to the relevant person, severity is set, and progress is tracked for accountability.
3. **Track in Board:** Team members move the incident card across workflow stages (Open → In Progress → Resolved) for clear visibility.
4. **Closure:** Upon closing, the system collects details on the resolution, supporting files, and lessons learned to prevent future occurrences.

Where to Use Incident Reports

1. **Software Development**: To track bugs and unexpected system behavior during development and deployment.
2. **Financial Systems**: For monitoring and resolving vulnerabilities in transaction processes.
3. **Web Applications**: To manage issues affecting user experience, performance, and security.
4. **Enterprise IT**: For handling system outages, security incidents, and compliance issues across departments.

Key Components of Incident Reports

> The Incident Reports Action tracks and manages security-related or general system issues (e.g., bugs, vulnerabilities, unexpected behavior). It provides two main views (Table and Board), plus the ability to filter, change statuses, and add closure details.

1. Table View

Use **Table** view for a detailed, spreadsheet-style list. Columns include:

Column	Description

Severity ⇅	Icon indicating Low (↓), Medium (=), High (↑), or Critical (⇈). Sortable.
Project ⇅	Name of the project this incident belongs to. Sortable.
Name	Clickable incident title; opens the edit drawer.
Assigned to ⇅	Engineer(s) responsible (name + UID). Sortable.
Component	Affected system component or module.
SLA	Target remediation date/time. **If the SLA has passed and the incident is *not* Resolved**, the entire SLA cell is highlighted **red** to draw immediate attention.
Created at ⇅	Timestamp when the incident was first logged. Sortable.
Updated at ⇅	Timestamp of the most recent update. Sortable.
Status ⇅	Current status badge (Open, In Progress, Resolved). Click to change. Sortable.
Actions	✏ Edit opens the side panel; ◫ Delete prompts confirmation.

> **Incident Reports – Clickable Name**
> In the Table view for Incident Reports, the **Name** column entries are clickable: clicking any Name opens the full-width “View Incident Report” drawer, showing all fields, lesson-learned history, attachments, root-cause analysis, and summary.

Status Control: Click the colored status label to choose a new state from a dropdown.

Edit Incident:
Click the ✏ Edit icon in the Actions column to open the side panel.
Update fields like Assigned to, Severity, Status, SLA, or Component.

> **Wider Detail Drawer (Resolved Incidents):** When an incident’s status is Resolved, the side-panel pops out in an **expanded, full-width** layout to neatly display your **Lesson learned** history, attachments, screenshots, or long-form notes without cramped columns or horizontal scrolling.

Post-Resolution Editing

Even after an incident is marked **Resolved**, you can still open the Edit drawer (✏ icon) and change its details:
Editable Status: The **Status** field remains a dropdown—click it to switch from **Resolved** back to **Open** or **In Progress**, or vice versa.

Full Field Access: All other fields (Component, Severity, SLA, Description, Summary, etc.) remain writable. After making adjustments, click **Save** to update the record.

2. Board View:
Kanban-Style Board: Switch to Board view to see incidents arranged by status column (e.g., Open, In Progress, Resolved).
Drag & Drop: Move incident cards between columns to reflect status changes.
Resolving an Incident: When you move an incident to Resolved, a dedicated form may appear, prompting you to describe how the issue was fixed, attach any proof or files, and add a root cause analysis or lessons learned.

3. Filtering & Searching:
Filter Panel: Click **Filter** to open filters for **Status, Severity**, and **Assigned to**. Select your criteria and click **Save** to narrow the list or board.
Search Bar: In either view, type a full or partial incident name (or keyword) into the **Search** field to locate specific reports instantly.

How to Delete an Incident Report

Deleting an Incident Report removes it permanently from the system and records who performed the deletion and which report was removed. Follow the steps below.

Prerequisites:
You must have **Delete** permissions on the **Incident Reports** module.
Ensure you really intend to remove the record, as deletion cannot be undone.

Deletion Steps

1) Open the Incident Reports List:
In the left-hand navigation, select **Incident Reports**.
Locate the row for the report you wish to delete.
2) Trigger Deletion: In the **Actions** column of that row, click the □□ **Delete** icon.
3) Confirm Deletion:
A confirmation pop-up appears:

> **Are you sure?** [Cancel] [Delete]

Click **Delete** to proceed.
4) Completion: The report is removed from the table.
A success toast or message confirms the deletion.

Audit Logging

Every deletion is recorded in the system audit log to maintain a clear trail of administrative actions. The log entry includes:
Report Name – The title or unique identifier of the deleted incident report.
Deleted By – The username of the person who performed the deletion.
Timestamp – When the deletion occurred.

> **Tip:** Regularly review audit logs to ensure all deletions were intentional and comply with your data-retention policies.

Revision #20
Created 27 February 2025 08:45:15
Updated 27 January 2026 11:54:16