

## **Alert Triage Workflow**

Cloud security tools generate a high volume of alerts across multiple cloud accounts and services. Security engineers need a way to quickly understand which alerts matter most, investigate their impact, and track resolution without being overwhelmed by noise or forced into complex remediation flows.

The challenge is not only detecting issues, but enabling effective triage, investigation, collaboration, and resolution tracking in a way that reflects real-world security workflows.

### [Figma Document](#)

## **User Persona**

**Primary user:** Cloud / Security Engineer

Responsibilities:

- Monitor security alerts across environments
- Assess severity and potential impact
- Investigate alerts and gather context
- Coordinate remediation with service owners or infrastructure teams
- Verify fixes and mark alerts as resolved

Pain points:

- Alert fatigue and poor prioritization
- Lack of context when reviewing alerts
- Difficulty tracking ownership and resolution status
- Unclear audit trail for who handled an alert and when

# Design Overview

The proposed design focuses on a two-screen workflow that mirrors how security teams actually work:  
a triage queue for prioritization, followed by a detailed view for investigation and resolution tracking.

The system is intentionally designed as a visibility and coordination tool, not a remediation console. Technical fixes are assumed to happen outside the system, with this interface serving as the source of truth for alert status and accountability.

## Screen 1: Alert List (Triage View)

The alert list acts as a prioritized work queue.

### Key features:

- Alerts grouped by day to support daily on-call and triage routines
- Severity-based visual indicators for quick scanning
- Clear resolution state using a reversible checkbox
- “Resolved by” attribution to support accountability and handoffs

### Design rationale:

Grouping alerts by day reflects how engineers typically process alerts in time-based batches, while severity indicators ensure that critical issues are not buried. Resolution is treated as a reversible state, allowing alerts to be reopened if remediation is incomplete or incorrect.

## Alert Prioritization Logic:

Alert priority is derived from a combination of severity, resource criticality, and exposure duration, rather than raw alert volume alone. Severity reflects the inherent risk of the issue (e.g., public access, unrestricted network exposure), while resource criticality accounts for whether the affected asset is production-facing, sensitive, or business-critical. Exposure duration acts as a modifier, ensuring that long-standing unresolved risks are surfaced even if their initial severity is lower. This approach ensures

that alerts with the highest potential impact are surfaced first, while still allowing security engineers to quickly scan and batch lower-risk issues.

## Designs:

(Please do not rely on screenshots. Reference the figma design links)

The screenshot shows the AWS Alerts interface. At the top, there's a header with the AWS logo, a bell icon, and a user profile icon. Below the header, the word "Alerts" is prominently displayed in a large, bold font. Underneath "Alerts", a subtitle reads "Prioritized security issues across cloud accounts". A "Sort" button with a dropdown arrow is located on the right side of the header area.

The main content is a table divided into two sections: "Yesterday - Wed, 24 Dec, 2025" and "Today - Thu, 25 Dec, 2025".

**Yesterday - Wed, 24 Dec, 2025:**

Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	Critical	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	Low Priority	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	High Priority	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	Medium Pri...	15:01 IST	-

**Today - Thu, 25 Dec, 2025:**

Status	Alert title	Priority	Reporting time	Resolved By
No issues reported today. That's all we know.				

A large question mark icon is centered below the tables, and a tooltip message "No issues reported today. That's all we know." is visible.

## Zero State

This screenshot is identical to the one above, showing the AWS Alerts interface for December 24, 2025. It displays the same table structure with four rows of alerts and a "No issues reported today" message at the bottom.

## Triage view



## Alerts

Prioritized security issues across cloud accounts

Sort

Yesterday - Wed, 24 Dec, 2025

Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>Critical</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>Medium Priority</span>	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	15:01 IST	-

Today - Thu, 25 Dec, 2025

Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>High Priority</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>Low Priority</span>	14:52 IST	-
<input type="checkbox"/>	Compute service allowing unrestricted network access	<span>Medium Pri...</span>	15:01 IST	-

## Hover tooltips



## Alerts

Prioritized security issues across cloud accounts

Sort

Yesterday - Wed, 24 Dec, 2025

Status	Alert title	Priority	Reporting time	Resolved By
<input checked="" type="checkbox"/>	Public S3 Bucket	<span>Critical</span>	14:36 IST	Shalap Pandotra
<input checked="" type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	Shalap Pandotra
<input type="checkbox"/>	Compute service allowing un...	<span>High Priority</span>	14:52 IST	-
<input checked="" type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	15:01 IST	Shalap Pandotra

Today - Thu, 25 Dec, 2025

Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>High Priority</span>	14:36 IST	-
<input checked="" type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	Shalap Pandotra
<input checked="" type="checkbox"/>	Compute service allowing un...	<span>Low Priority</span>	14:52 IST	Shalap Pandotra
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	15:01 IST	Marked resolved by Shalap Pandotra at 16:21 IST

## Resolved State



S

## Alerts

Prioritized security issues across cloud accounts

Sort ↴

Low → High  
High → Low

Yesterday - Wed, 24 Dec, 2025				
Status	Alert title	Priority	Reporting time	
<input type="checkbox"/>	Public S3 Bucket	<span>Critical</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>High Priority</span>	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	15:01 IST	-

  

Today - Thu, 25 Dec, 2025				
Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>High Priority</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>Low Priority</span>	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	15:01 IST	-

## Sorting Options



S

## Alerts

Prioritized security issues across cloud accounts

☰ High → Low ✕

Yesterday - Wed, 24 Dec, 2025				
Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>Critical</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>High Priority</span>	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>Low Priority</span>	15:01 IST	-

  

Today - Thu, 25 Dec, 2025				
Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	<span>High Priority</span>	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Medium Pri...</span>	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	<span>Low Priority</span>	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	<span>Low Priority</span>	15:01 IST	-

## Sorted State

## **Screen 2: Alert Details (Investigation & Resolution)**

The detail view provides all necessary context to investigate and close an alert.

### **Key features:**

- Plain-English explanation of the issue and its potential impact
- Clear display of affected resources and timestamps
- Internal discussion/comments for collaboration and escalation
- Explicit resolution controls and audit trail (who resolved the alert and when)

### **Design rationale:**

This view focuses on understanding and coordination rather than direct remediation. By surfacing risk context and supporting team discussion, the design reflects real-world workflows where fixes are applied externally and verified before an alert is resolved.

## Designs:

The screenshot shows the AWS Alerts interface. At the top, there's a header with the AWS logo, a bell icon, and a user profile. Below the header, it says "Alerts" and "Prioritized security issues across cloud accounts". On the right, there are "Sort" and filter icons. The main area is titled "Alert Details" for a critical alert about a compute service allowing unrestricted network access. The alert status is "Critical" (purple) and "Open". The description box contains a warning about inbound network traffic from any IP address. Below the description are two buttons: "Mark as resolved" (green) and "Reopen Alert" (grey). The "Activity" section shows three status points: "Reported" (green dot), "Investigated" (green dot), and "Resolved" (green dot). The "Resolved by" field is listed as "Manan". The "Comments" section on the right shows a conversation between two users, "a" and "n", with messages like "this is bad.", "no yeah this is really bad actually", and "yeah, escalate this to manan". There's also a "Leave a comment for your team" button.

### Details View - unresolved

This screenshot is identical to the one above, showing the same alert details for a critical issue. The only difference is in the "Activity" section where the final status point is now "Resolved" (green dot) instead of "Investigated". The "Resolved by" field is now "Manan" and the timestamp is "20:02 IST, 24 Dec, 2023". The rest of the interface, including the description, comments, and buttons, remains the same.

### Details View - resolved

## **Success Metrics**

The effectiveness of this design could be measured by:

- Time to first action on newly detected alerts
- Percentage of alerts resolved vs reopened
- Reduction in unresolved critical alerts over time
- Clarity of ownership and resolution accountability

## **Development Action Items**

- Implement an alert state machine (open → resolved → reopened) with reversible actions
- Maintain an immutable audit log for status changes, ownership, and resolution events
- Support priority calculation based on severity, asset criticality, and exposure duration
- Enable alert ownership assignment and reassignment
- Provide a lightweight comment system with timestamps and user attribution
- Expose sorting and filtering APIs to support scalable alert volumes