

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.

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". To the right of the subtitle is a "Sort" button with a dropdown arrow. The main content area is divided into two sections: "Yesterday - Wed, 24 Dec, 2025" and "Today - Thu, 25 Dec, 2025". Each section contains a table with columns: Status, Alert title, Priority, Reporting time, and Resolved By. The first section has four entries, while the second section has none. A question mark icon is located below the tables, and a message at the bottom states "No issues reported today. That's all we know."

Status	Alert title	Priority	Reporting time	Resolved By
☐	Public S3 Bucket	❗ Critical	14:36 IST	-
☐	Public S3 Bucket	❗ Low Priority	14:47 IST	-
☐	Compute service allowing un...	❗ High Priority	14:52 IST	-
☐	Public S3 Bucket	❗ Medium Pri...	15:01 IST	-

Status	Alert title	Priority	Reporting time	Resolved By
☐				

?

No issues reported today. That's all we know.

Zero State

This screenshot is identical to the one above it, showing the AWS Alerts interface for December 24, 2025. It displays a list of four security issues (three Public S3 Buckets and one Compute service) with their respective details: status (checkbox), alert title, priority (color-coded icon), reporting time, and resolved by (indicated by a dash). The "Today" section is empty.

Status	Alert title	Priority	Reporting time	Resolved By
☐	Public S3 Bucket	❗ Critical	14:36 IST	-
☐	Public S3 Bucket	❗ Low Priority	14:47 IST	-
☐	Compute service allowing un...	❗ High Priority	14:52 IST	-
☐	Public S3 Bucket	❗ Medium Pri...	15:01 IST	-

Status	Alert title	Priority	Reporting time	Resolved By
☐				

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	Critical	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	Low Priority	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	Medium 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
<input type="checkbox"/>	Public S3 Bucket	High Priority	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	Low Priority	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	Low Priority	14:52 IST	-
<input type="checkbox"/>	Compute service allowing unrestricted network access	Medium Pri...	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	Critical	14:36 IST	Shalap Pandotra
<input checked="" type="checkbox"/>	Public S3 Bucket	Low Priority	14:47 IST	Shalap Pandotra
<input type="checkbox"/>	Compute service allowing un...	High Priority	14:52 IST	-
<input checked="" type="checkbox"/>	Public S3 Bucket	Medium Pri...	15:01 IST	Shalap Pandotra

Today - Thu, 25 Dec, 2025

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

Today - Thu, 25 Dec, 2025				
Status	Alert title	Priority	Reporting time	Resolved By
<input type="checkbox"/>	Public S3 Bucket	High Priority	14:36 IST	-
<input type="checkbox"/>	Public S3 Bucket	Medium Pri...	14:47 IST	-
<input type="checkbox"/>	Compute service allowing un...	Low Priority	14:52 IST	-
<input type="checkbox"/>	Public S3 Bucket	Low Priority	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, the word "Alerts" is prominently displayed, followed by the subtitle "Prioritized security issues across cloud accounts". A "Sort" button is located in the top right corner.

The main area is titled "Alert Details" and displays a single alert entry. The alert summary is: "Compute service allowing unrestricted network access" (Priority: Critical, Status: Open). The description box contains a detailed explanation: "This compute instance allows inbound network traffic from any IP address. If exploited, this could allow unauthorized access to the system and increase the risk of data exposure." Below the description are two buttons: "Mark as resolved" (green) and "Reopen Alert" (grey).

The "Activity" section shows a timeline with three circular nodes: "Reported" (2021-12-24), "Investigated" (2021-12-24), and "Resolved" (2021-12-24). Below the timeline are fields for "Resolved by:" (Manan), "Resolved at:" (2021-12-24 10:00:00), and "Notes" (None).

To the right of the alert details is a "Comments" sidebar. It shows a conversation between two users, "a" and "n": "a: this is bad.", "n: no yeah this is really bad actually.", and "a: yeah, escalate this to manan.". There is also a "Leave a comment for your team" button.

Details View - unresolved

This screenshot is identical to the one above, showing the same警报 details for a "Compute service allowing unrestricted network access" issue. The key difference is in the "Activity" section, where the third node is now green, indicating it has been "Resolved" (2021-12-24).

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