

USE CASE

Triage multi-cloud findings without losing the unrated ones

Findings from every connected cloud in one list, with severities from the source and a separate band for findings that arrived with none.

THE PROBLEM

Findings come in from AWS, Azure and GCP with different severity scales, and some come with no severity at all. Whoever imported the feed mapped the unknowns upward, so by Monday everything is high. The last time they were mapped to low, something real got ignored.

HOW ARIBOT HANDLES IT

- 1 **Connect accounts**
Read-only access brings each cloud into scope.
- 2 **Collect findings**
The live inventory is checked, and findings land in one view.
- 3 **Keep source severities**
Rated findings keep the severity they arrived with, and unrated ones go to their own band.
- 4 **Triage with a record**
Each assignment records who set the severity and why.

WHAT YOU SEE IN THE DEMO

- Severity bands for Critical, High, Medium & Low, and Unrated
- Search with severity and cloud filters
- An AI Attack Context note on findings that explains the risk to nearby assets
- Findings marked Auto-Fix or Manual, each with resource, rule and category

WHO IT IS FOR

- Cloud Security Engineer
- Head of Cloud Security
- DevSecOps Lead

WHAT YOU GET

- One findings list across clouds, with search and filters
- An Unrated band, so a missing field never lowers a finding's priority
- Severity totals that state they cover rated findings only
- Attack context on findings that explains what an attacker could reach

73%

name false positives as their top detection and response challenge

Source: SANS Detection & Response Survey 2025

See it: ayurak.com/demos/violations-dashboard

€30 per scan · €30 per applied fix (dry runs free)