
USE CASE

One view of findings across AWS, Azure and GCP

A single operations view of alerts, resources and posture across your AWS, Azure and GCP accounts, so triage starts in one place.

THE PROBLEM

**We run on several clouds,
and each has its own console
and its own alert format.**

Triage means switching tabs and rebuilding context every time. Leadership asks for one posture figure and we assemble it by hand.

WHY IT MATTERS NOW

73%

name false positives as their top detection and response challenge

Source: SANS Detection & Response Survey 2025

HOW ARIBOT HANDLES IT

1 **Connect your clouds**

AWS, Azure and GCP accounts are connected with read-only access.

2 **See the estate together**

Resources, violations and compliance appear per cloud in one overview.

3 **Work the alert feed**

Each alert lists its severity, resource, cloud and status.

4 **Investigate a finding**

Open an alert to see the affected resource before deciding on a fix.

WHAT YOU GET

- One place to see findings from every connected cloud
- Alerts tied to a named resource and cloud
- A per-cloud summary of resources, violations and compliance
- A shared starting point for triage and reporting

SEE IT IN THE DEMO

- A Multi-Cloud Overview card for each provider with resources, violations and compliance
- An alert feed with items such as an exposed storage bucket or an over-privileged service account
- Alert statuses of active, investigating and resolved, with an Investigate action
- A security posture gauge

See it for yourself

ayurak.com/demos/command-center

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