

USE CASE

Kubernetes findings in the same view as your cloud

Cluster findings such as privileged containers or automounted credentials land in the same violations view as the rest of your estate, scoped to cluster resources.

THE PROBLEM

Our workloads change on every deploy, and the cluster security view is a separate tool nobody opens. A developer gets a 'privileged container' alert with no workload named and no sign of how it was rated. At audit, container posture gets answered from memory.

HOW ARIBOT HANDLES IT

- 1 Connect the clusters**
Read-only cluster access brings workloads into scope.
- 2 Read the workloads**
Live pod and policy state is checked, and findings are raised.
- 3 Keep source severities**
Rated findings keep their severity, and unrated ones get their own band.
- 4 Triage with a record**
Each finding names its namespace and workload, and the assignment records who rated it and why.

WHAT YOU SEE IN THE DEMO

- A violations view scoped to cluster resources
- Findings such as a privileged container, automounted API credentials, missing resource limits and an image pulled by a mutable tag
- A cluster topology where pods are scanned and flagged
- Violation types covering network policy, RBAC, pod security and image scanning

WHO IT IS FOR

Kubernetes Platform Owner

SRE / Platform Lead

Cloud Security Engineer

WHAT YOU GET

- One place to look for cluster and cloud findings
- Findings named by namespace and workload
- Unrated findings kept in view
- The same evidence trail as cloud findings

See it: ayurak.com/demos/kubernetes-security

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