Security posture snapshot

Prepared 2026-04-16 04:15 UTC · scope: global · 37 open findings across 1,842 resources

OPEN FINDINGS	CRITICAL	HIGH	EXCEPTIONS
37 -4	3 -1	9 -2	6 +0

Critical findings

public-bucket · AWS · acme-data-bronze-usw2
Evidence: bucket policy grants s3:GetObject to Principal: * on /static/.
Owner: data-eng · Target: 2026-04-20 · Pillar: data exposure.

root-access-key · AWS · acme-legacy-ops
Evidence: long-lived access key AKIA…XWPZ last used 4 days ago. Replacement via IRSA deployed; awaiting cut-over.
Owner: platform · Target: 2026-04-22.

bq-dataset-public · GCP · data-prod.analytics
Evidence: dataset ACL grants READER to allAuthenticatedUsers.
Owner: data-eng · Target: 2026-04-18.

High findings (top three)

FINDING	RESOURCE	PILLAR	TARGET
stage-db-0.0.0.0	acme-stage-aurora	network	04-25
unencrypted-disk × 5	rg-eastus/*	encryption	05-02
wildcard-iam-binding	data-prod/iam	iam	04-24

Closed this week

4 findings closed, including 1 critical (rotated IAM root access key on legacy-ops). Mean time to remediate a critical: 3.8 days. Full closure audit trail in appendix D.

How to read the shields

On the architecture explorer, green shields mark identity / auth controls (IAM, Entra, Workload Identity, KMS, Secrets Manager, Key Vault). Severity pills mark findings. The Security overlay fades all non-security edges so controls and findings read first.