Detection Strategy for Modify Cloud Compute Infrastructure: Create Cloud Instance, Detection Strategy DET0449

Archived: 2026-04-05 16:05:35 UTC

AN1242

Detection focuses on abnormal or unauthorized cloud instance creation events. From a defender’s perspective, suspicious behavior includes VM/instance creation by rarely used or newly created accounts, creation events from unusual geolocations, or rapid sequences of snapshot creation followed by instance creation and mounting. Unexpected network or IAM policy changes applied to new instances can indicate adversarial use rather than legitimate provisioning.

Log Sources

Mutable Elements

Field	Description
UserContext	IAM user, service account, or role creating the instance. Tuned to allowlist known automation services.
GeoLocation	Region or source IP where the creation request originates. Helps detect cross-region or unusual location abuse.
RateThreshold	Number of instances created per user or account in a time window. Tuned for environments with elastic scaling.
TaggingPolicy	Expected tags (e.g., owner, purpose, cost center) for new instances. Deviations may indicate adversarial creation.