Detection Strategy for Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations, Detection Strategy DET0492

Archived: 2026-04-05 16:31:50 UTC

AN1356

Defenders should monitor for anomalous or unauthorized changes to cloud compute configurations that alter quotas, tenant-wide policies, subscription associations, or allowed deployment regions. From a defender’s perspective, suspicious behavior chains include a sudden increase in compute quota requests followed by new instance or resource creation, policy modifications that weaken security restrictions, or enabling previously unused/unsupported cloud regions. Correlation across identity, configuration, and subsequent provisioning logs is critical to distinguish legitimate administrative activity from adversarial abuse.

Log Sources

Mutable Elements

Field	Description
UserContext	Identity performing the quota or configuration change; tuned to filter known admins or automation accounts.
TimeWindow	Correlation period for configuration change followed by resource creation; tuned to environment norms.
ChangeType	Type of configuration being modified (quota, policy, region); tuned to organization-specific risk thresholds.
GeoLocation	Region where the configuration change originates; tuned to enterprise’s expected operational geography.