Detection Strategy for Modify Cloud Compute Infrastructure: Delete Cloud Instance, Detection Strategy DET0084

Archived: 2026-04-05 18:19:33 UTC

AN0234

Defenders can detect suspicious cloud instance deletions by correlating events across authentication, instance lifecycle, and account activity. From a defender’s perspective, behaviors of interest include instances deleted shortly after creation, deletions initiated by new or rarely used accounts, deletions following snapshot creation, and deletions originating from anomalous geolocations or access keys. These may indicate adversarial attempts to destroy forensic evidence or evade detection.

Log Sources

Mutable Elements

Field	Description
UserContext	Identity of the user/service account performing deletions; tuned to exclude automation or known administrative workflows.
TimeWindow	Threshold for detecting rapid instance lifecycle events (e.g., creation and deletion within minutes).
GeoLocation	Region or source IP where the delete request originated; can be tuned to align with enterprise cloud geography.
RateThreshold	Number of deletions per user/account in a defined window; tuned for organizations with high elasticity.