Detection Strategy for Modify Cloud Compute Infrastructure: Revert Cloud Instance, Detection Strategy DET0337

Archived: 2026-04-05 17:52:51 UTC

AN0953

Defenders can detect suspicious reversion of cloud compute instances by monitoring for unusual snapshot restores, rollback actions, or ephemeral storage resets that occur outside expected administrative workflows. From a defender’s perspective, relevant detection chains include: a snapshot restore triggered by a new or rarely used account, a sequence of snapshot creation immediately followed by a restore and instance start, or rollbacks performed from anomalous geographic or network locations. These patterns may indicate attempts to remove forensic evidence or re-establish a clean execution state for persistence.

Log Sources

Mutable Elements

Field	Description
UserContext	Identity of the user or service account performing rollback actions; tuned to exclude automation or approved workflows.
TimeWindow	Threshold for correlating snapshot creation followed by reversion within minutes; tuned to environment activity norms.
GeoLocation	Region or source IP where the revert request originated; tuned to align with enterprise cloud geography.
ChangeTags	Use of administrative tags or headers to distinguish legitimate restores from malicious activity.