Detection Strategy for Modify Cloud Compute Infrastructure, Detection Strategy DET0308

Archived: 2026-04-05 14:05:27 UTC

AN0861

Detection focuses on identifying unauthorized or anomalous changes to compute infrastructure components. Defender perspective: monitor for creation, deletion, or modification of instances, volumes, and snapshots outside of approved change management windows; correlate abnormal activity such as rapid snapshot creation followed by new instance mounts, or repeated infrastructure changes by rarely used accounts. Flagging activity linked to unusual geolocation, API client, or automation script is suspicious.

Log Sources

Mutable Elements

Field	Description
ChangeWindow	Approved maintenance or deployment windows. Helps reduce false positives by distinguishing scheduled activity.
UserContext	IAM user, role, or service account performing the operation. Tunable to allowlist known automation services.
RateThreshold	Number of infrastructure changes (e.g., snapshot creations) in a defined period. Adjusted based on workload scale.
GeoLocation	Region or source IP where changes originate. Useful for tuning alerts to account for multi-region deployments.