Detection Strategy for Modify Cloud Compute Infrastructure: Create Snapshot, Detection Strategy DET0423

Archived: 2026-04-05 13:55:22 UTC

AN1187

Detection focuses on correlating snapshot creation events with subsequent instance creation and mounting activities. From a defender perspective, suspicious sequences include snapshot creation by unexpected or newly created IAM users, snapshots created from sensitive volumes without preceding change-control activity, or snapshots immediately followed by mounting to unauthorized instances. Cross-referencing with user behavior, IP geolocation, and automation context helps distinguish benign backup operations from adversary-driven snapshot exploitation.

Log Sources

Mutable Elements

Field	Description
UserContext	IAM user, service account, or role performing snapshot creation. Tuned to allowlist known backup automation services.
TimeWindow	Frequency of snapshot creation in a defined period. Adjusted for environments with frequent automated backups.
GeoLocation	Unusual regions or IPs from which snapshot creation API calls originate. Helps identify cross-region snapshot abuse.
VolumeSensitivity	Tagging or classification of volumes being snapshotted. Tuned to prioritize alerts when sensitive volumes are copied.
