Detection of Lifecycle Policy Modifications for Triggered Deletion in IaaS Cloud Storage, Detection Strategy DET0041

Archived: 2026-04-05 17:34:13 UTC

AN0117

Adversary with write access to storage modifies lifecycle policies (e.g., via PutBucketLifecycle) to schedule rapid object deletion across one or more storage buckets. This is often used to trigger impact (destruction), remove logs (defense evasion), or force extortion (ransomware).

Log Sources

Mutable Elements

Field	Description
LifecycleExpirationDays	Policy values setting Expiration in fewer than N days (e.g., 0–1) are highly suspicious.
TargetBucket	Filter by bucket types (e.g., log storage, production DB snapshots) to prioritize detection.
Principal	Correlate rare or anomalous IAM principals making destructive lifecycle changes.
TimeWindow	Link lifecycle policy change with API activity suggesting staged deletion or extortion attempt.