Cross-Platform Detection of Data Transfer to Cloud Account, Detection Strategy DET0573

Archived: 2026-04-05 16:26:50 UTC

AN1580

Detects snapshot sharing, backup exports, or data object transfers from victim-owned cloud accounts to other cloud identities within the same provider (e.g., AWS, Azure) using snapshot sharing, S3 bucket policy updates, or SAS URI generation.

Log Sources

Mutable Elements

Field	Description
CrossAccountIDList	List of external cloud accounts authorized for snapshot or bucket sharing
Region	Geographic region in which the sharing occurs (may impact logging availability)
VolumeSizeThresholdGB	Threshold to alert on snapshot size or object volume
TimeWindow	Temporal window between snapshot creation and external sharing

AN1581

Detects user activity that shares or syncs files with external domains via link generation, OneDrive external sharing, or file transfer actions involving non-whitelisted partner tenants.

Log Sources

Mutable Elements

Field	Description
ExternalDomainList	Known partner or adversarial cloud identities/domains
TimeWindow	Duration between file access and external sharing
SharingMethod	Type of link (anonymous, internal, organization-wide) to alert on

AN1582

Detects use of built-in SaaS sharing mechanisms to transfer ownership or share access of critical data to external tenants or untrusted users through API calls or link generation features.

Log Sources

Mutable Elements

Field	Description
UserContext	Whether the user is in a high-privileged or VIP group
DomainReputationList	Allowlist or blocklist of external SaaS domains
PayloadVolumeThreshold	Size or number of shared files triggering alert

---