Behavioral Detection of Remote Cloud Logins via Valid Accounts, Detection Strategy DET0008

Archived: 2026-04-05 18:40:21 UTC

AN0017

Cloud login from atypical geolocation or user-agent string, followed by resource enumeration or infrastructure manipulation using cloud CLI/API

Log Sources

Mutable Elements

Field	Description
IPGeoRiskScore	Tunable scoring system for evaluating geo-divergent or TOR-origin logins
UserAgentFingerprint	Flag rare CLI tools or browser-based sessions
SessionDuration	Threshold for how long between login and API access
CloudResourceScope	Limit monitoring to high-value resource groups or sensitive tenants

AN0018

Federated login using SSO or OAuth grant to cloud control plane, followed by directory or permissions enumeration

Log Sources

Mutable Elements

Field	Description
SSOApplicationScope	Tune based on applications federated to high-priv cloud assets
ClientIDScope	Filter based on expected OIDC clients used for login
LoginVelocity	Track multiple geographic logins within short windows

AN0019

Login to M365 or Google Workspace from CLI tools or unexpected source IPs, followed by mailbox or document access

Log Sources

Mutable Elements

Field	Description
DevicePlatformMismatch	Raise alerts on login from CLI when user typically uses web-only
SensitiveDocumentAccessPattern	Track access to documents labeled as internal/confidential
AccessFrequencyThreshold	Tune for high-volume document reads post login

AN0020

Remote access to third-party SaaS with OAuth or API tokens post-initial compromise, followed by sensitive data access or configuration changes

Log Sources

Mutable Elements

Field	Description
OAuthTokenAge	Older tokens issued before password change may indicate compromise
AppScope	Restrict detection to high-value or regulated SaaS apps

---