Detection of Cloud Service Dashboard Usage via GUI-Based Cloud Access, Detection Strategy DET0291

Archived: 2026-04-05 14:23:09 UTC

AN0808

Detects web console login events followed by read-only or metadata retrieval activity from GUI sources (e.g., browser session, mobile client) rather than API/CLI sources. Correlates across CloudTrail, IAM identity logs, and user-agent context.

Log Sources

Mutable Elements

Field	Description
UserAgentFilter	Allowlist/denylist of user agents to distinguish browser-based vs. CLI/API sessions
TimeWindow	Maximum time delta between login and suspicious GUI activity
PrivilegedSessionThreshold	Login attempts to dashboard using elevated IAM roles

AN0809

Detects successful login to cloud identity portals (e.g., Okta, Azure AD, Google Identity) from atypical geolocations, devices, or user agents immediately followed by dashboard/portal navigation to sensitive pages such as user or app configuration.

Log Sources

Mutable Elements

Field	Description
GeoIPAnomalyThreshold	Threshold for location anomalies per user profile
UserAgentReputation	Unknown browser/device fingerprint list
PrivilegedPageAccess	List of sensitive dashboard views for alerting

AN0810

Detects login to admin consoles (e.g., Microsoft 365 Admin Center) from unrecognized users, devices, or geolocations followed by non-API data review or configuration read actions that suggest GUI dashboard use.

Log Sources

Mutable Elements

Field	Description
AdminRoleList	Roles allowed to access dashboard views
DashboardNavigationSequence	Pageview paths or clickstreams indicating use of GUI admin console
GeoLocationRisk	List of high-risk regions or unexpected geos

AN0811

Detects SaaS web login followed by dashboard or web GUI page views from unfamiliar locations, devices, or access patterns. Identifies use of sensitive reporting or configuration consoles accessed from high-risk accounts.

Log Sources

Mutable Elements

Field	Description
SaaSDashboardViewList	List of GUI pages or endpoints considered sensitive
IPReputationThreshold	Reputation score or allowlist of source IPs
LoginBehaviorBaseline	Typical user/device login pairings or login frequency

---