Detection Strategy for Cloud Service Discovery, Detection Strategy DET0402

Archived: 2026-04-05 13:58:00 UTC

AN1127

Unusual enumeration of services and resources through cloud APIs such as AWS CLI `describe-*`, Azure Resource Manager queries, or GCP project listings. Defender perspective includes anomalous API calls, unexpected volume of service enumeration, and correlation of discovery with recently compromised sessions.

Log Sources

Data Component	Name	Channel
Cloud Service Enumeration (DC0083)	AWS:CloudTrail	DescribeInstances, DescribeServices, ListFunctions: High frequency enumeration calls or unusual user agents performing discovery
User Account Metadata (DC0013)	AWS:CloudTrail	AssumeRole: Discovery actions tied to assumed identities outside of normal context

Mutable Elements

Field	Description
EnumerationRateThreshold	Rate of API calls used to enumerate services; tuned to reduce noise from automated inventory tools.
UserAgentFilter	Expected user agents for cloud management tools; deviations may indicate adversarial tools.

AN1128

Enumeration of directories, applications, or service principals through APIs such as Microsoft Graph or Okta API. Defender perspective includes unexpected listing of users, roles, applications, and abnormal access to identity management endpoints.

Log Sources

Mutable Elements

Field	Description
QueryVolumeThreshold	Threshold for number of object enumeration calls before triggering detection.
PrivilegedRoleList	High-value identity roles (Global Admin, Application Admin) for targeted discovery monitoring.

AN1129

Discovery of SaaS services connected to productivity platforms (e.g., Microsoft 365, Google Workspace). Defender perspective includes unexpected enumeration of enabled services, API integrations, or OAuth applications tied to user accounts.

Log Sources

Data Component	Name	Channel
Cloud Service Enumeration (DC0083)	m365:unified	Get-MsolServicePrincipal, ListAppRoles: Service discovery operations executed by accounts not normally performing administrative tasks
Logon Session Creation (DC0067)	m365:signinlogs	UserLogin: Discovery operations shortly after account logins from new geolocations

Mutable Elements

Field	Description
MonitoredAppIntegrations	Specific Office Suite applications or plugins that may be enumerated or targeted.
GeoLocationDeviation	Geographic deviation threshold for discovery actions linked to recent logins.

AN1130

Discovery of connected SaaS applications, APIs, or configurations within platforms like Salesforce, Slack, or Zoom. Defender perspective includes enumeration of available integrations, abnormal querying of service metadata, and follow-on attempts to exploit or persist via discovered services.

Log Sources

Mutable Elements

Field	Description
IntegrationDiscoveryThreshold	Number of SaaS integrations enumerated before triggering detection.
ServiceAccountScope	Expected permissions for service accounts to distinguish benign from malicious discovery.
