Behavioral Detection of Cloud Group Enumeration via API and CLI Access, Detection Strategy DET0251

Archived: 2026-04-05 13:47:29 UTC

AN0695

Detects adversarial use of cloud-native APIs (e.g., AWS IAM, Azure RBAC, GCP Identity) to enumerate cloud group memberships or policy mappings via unauthorized sessions or scripts.

Log Sources

Mutable Elements

Field	Description
UserContext	Scope to anomalous IAM principals or assume-role usage.
TimeWindow	Correlate enumeration activity within lateral movement prep windows.

AN0696

Identifies unauthorized access or enumeration of administrative roles, security groups, or distribution groups via Exchange/SharePoint/Teams APIs or role discovery scripts.

Log Sources

Mutable Elements

Field	Description
AccessScope	Adjust based on tenant-level vs. site-level group visibility.
ScriptExecutionContext	Detect script-based role listing (e.g., Graph API call chains).

AN0697

Monitors API calls and service-specific logs for enumeration of organizational roles, permissions, and group structure, particularly outside of normal admin behavior baselines.

Log Sources

Mutable Elements

Field	Description
OrgScope	Scope to cross-team access or unfamiliar org enumeration.
RequestRate	Tuning for excessive group-list API calls.
