Detection of Domain or Tenant Policy Modifications via AD and Identity Provider, Detection Strategy DET0270

Archived: 2026-04-02 11:42:20 UTC

AN0755

Adversary modifies Group Policy Objects (GPOs), domain trust, or directory service objects via GUI, CLI, or programmatic APIs. Behavior includes creation/modification of GPOs, delegation permissions, trust objects, or rogue domain controller registration.

Log Sources

Mutable Elements

Field	Description
ObjectDN	Filter to specific AD containers (e.g., CN=Policies,CN=System,DC=domain,DC=com) for GPOs.
AttributeModified	Focus on high-risk attributes such as gPCFileSysPath, ntSecurityDescriptor.
TimeWindow	Correlate changes with suspicious process creation or privileged user logon.
UserContext	Alert on unexpected user or service account modifying domain policy.

AN0756

Adversary modifies tenant policy through changes to federation configuration, trust settings, or identity provider additions in Microsoft 365/AzureAD via Portal, PowerShell, or Graph API. Includes setting authentication to federated or updating federated domains.

Log Sources

Mutable Elements

Field	Description
OperationName	Identify rare modification operations that are not part of standard admin lifecycle.
InitiatedBy	Filter by known administrators or service principals. Flag unknown initiators.
UserAgent	Detect scripted modifications (e.g., PowerShell/Graph API vs Azure Portal).

Field	Description
TimeWindow	Correlate tenant policy changes with new sign-ins or token forgery attempts.

Source: https://attack.mitre.org/detectionstrategies/DET0270#AN0756