Detection strategy for Group Policy Discovery on Windows, Detection Strategy DET0055

Archived: 2026-04-05 12:53:02 UTC

AN0152

Detection of adversary attempts to enumerate Group Policy settings through suspicious command execution (gpresult), PowerShell enumeration (Get-DomainGPO, Get-DomainGPOLocalGroup), and abnormal LDAP queries targeting groupPolicyContainer objects. Defenders observe unusual process lineage, script execution, or LDAP filter activity against domain controllers.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the correlation window to link suspicious PowerShell activity, gpresult execution, and LDAP enumeration.
UserContext	Identifies accounts expected to perform GPO enumeration (administrators vs. standard users).
CommandLinePatterns	Patterns for detecting suspicious gpresult or PowerShell cmdlets; tunable to reduce noise in environments where these tools are common.
