Detection of Domain Trust Discovery via API, Script, and CLI Enumeration, Detection Strategy DET0007

Archived: 2026-04-05 15:44:21 UTC

Analytics

- Windows

AN0016

Adversary uses nltest, PowerShell, or Win32/.NET API to enumerate domain trust relationships (via DSEnumerateDomainTrusts, GetAllTrustRelationships, or LDAP queries), followed by discovery or authentication staging.

Log Sources

Mutable Elements

Field	Description
ParentImage	Tune based on expected script hosts or authorized administrators invoking trust enumeration.
TimeWindow	Correlate enumeration + subsequent Kerberos activity or DC interaction within a bounded window.
UserContext	Prioritize detection for non-admin or unexpected user accounts performing enumeration.
API_Name	Flag uncommon or low-prevalence API calls like DSEnumerateDomainTrusts for inspection.