

Detect Modification of Authentication Process via Reversible Encryption, Detection Strategy DET0589

Archived: 2026-04-05 13:05:19 UTC

AN1621

Detects enabling of reversible password encryption in Active Directory or Group Policy, suspicious PowerShell commands modifying AD user properties, and unusual account configuration changes correlated with policy modifications. Multi-event correlation links Group Policy edits, PowerShell command execution, and user account property changes to identify tampering with authentication encryption settings.

Log Sources

Mutable Elements

Field	Description
MonitoredOUs	Scope of Organizational Units where reversible encryption property monitoring is enabled.
TimeWindow	Time window in which to correlate Group Policy modification and subsequent user property changes.
SuspiciousCmdletList	List of PowerShell cmdlets to monitor for account configuration changes.

Source: <https://attack.mitre.org/detectionstrategies/DET0589#AN1621>