Detect LSA Authentication Package Persistence via Registry and LSASS DLL Load, Detection Strategy DET0207

Archived: 2026-04-05 17:10:09 UTC

AN0583

Registry modification of the LSA Authentication Packages key followed by LSASS loading a non-standard or unsigned DLL. This includes unusual write access to `HKLM\SYSTEM\CurrentControlSet\Control\Lsa`, especially during non-installation timeframes. Correlated with `lsass.exe` loading DLLs not present in baseline or lacking valid signatures.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time between registry write and DLL load; tune based on reboot cycles or scheduled maintenance
ImageSignatureStatus	Allow listing of known signed LSASS-authenticated DLLs versus unknown/untrusted ones
RegistryPathScope	Allow tuning for subkeys beyond just `Authentication Packages` (e.g., `Security Packages`, `Notification Packages`)
UserContext	Correlate user responsible for registry edit; tune for expected administrative/service accounts
ParentProcess	Validate process lineage for registry modification; expected tools like `reg.exe` or `powershell.exe`
