Behavior-chain detection for T1134.005 Access Token Manipulation: SID-History Injection (Windows), Detection Strategy DET0136

Archived: 2026-04-05 17:42:07 UTC

AN0383

Detection of unauthorized modification of Active Directory SID-History attributes to escalate privileges. This chain involves: (1) privileged operations or API calls to DsAddSidHistory or related AD modification functions, (2) observed attribute changes in SID-History (Event ID 5136), (3) new logon sessions where the token includes unexpected or privileged SID-History values, and (4) follow-on resource access using elevated privileges derived from SID-History injection.

Log Sources

Mutable Elements

Field	Description
AllowedSIDHistoryChanges	Approved migration windows or known SID-History population events.
TimeWindow	Correlation window between attribute change and suspicious logon activity (default 15–30 minutes).
PrivilegedSIDList	List of sensitive SIDs (e.g., Enterprise Admins, Domain Admins) that should never appear in SID-History.
UserContextFilter	Exclude trusted migration service accounts or pre-approved administrative tasks.
AnomalousSIDCountThreshold	Raise alerts when a token contains more than X SID-History entries (default X=2).