Behavior-chain detection for T1134.003 Make and Impersonate Token (Windows), Detection Strategy DET0498

Archived: 2026-04-05 18:29:48 UTC

AN1375

A process creates a brand-new logon session/token (LogonUser/*LsaLogonUser) and then assigns/impersonates it (SetThreadToken/ImpersonateLoggedOnUser) to run actions under that freshly created security context. Chain: (1) suspicious command or script block (e.g., runas /netonly, PowerShell P/Invoke of LogonUser) → (2) ETW/API evidence of LogonUser*/SetThreadToken → (3) Security 4624 New Logon (often LogonType=9 NewCredentials or 2/3 from a non-interactive parent) with no interactive desktop → (4) sysmon 1 process(es) executing with the new LogonId/SID different from the parent process → (5) optional privileged ops/lateral movement.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between LogonUser*/SetThreadToken and the first spawned process (default 5–10 minutes).
SuspiciousLogonTypes	Which 4624 LogonTypes to treat as high risk (e.g., 9 NewCredentials, 3 Network when sourced locally).
AllowedImpersonators	Processes/accounts legitimately creating tokens (e.g., winlogon.exe, lsass.exe, IIS worker, trusted service accounts).
ParentChildUserMismatch	Whether to alert on any SID/LogonId mismatch between parent/child not in allow-list.
IntegrityEscalationDelta	Minimum integrity level jump (e.g., Medium→High/System) to raise severity.