Detecting MMC (.msc) Proxy Execution and Malicious COM Activation, Detection Strategy DET0222

Archived: 2026-04-05 17:52:57 UTC

Abuse of mmc.exe to execute non-Microsoft or user-staged .msc files and malicious COM CLSIDs. Behavioral chain: (1) suspicious mmc.exe invocation with /a or -Embedding and non-standard .msc path → (2) COM activation of non-baseline CLSIDs by mmc.exe → (3) mmc.exe loads non-baseline DLLs (user-writable/UNC/unsigned) → (4) optional network/DNS activity from mmc.exe.

Field	Description
TimeWindow	Correlation window (e.g., 5–10 minutes) tying .msc creation → mmc.exe start → module loads → COM/net activity.
AllowedMSCList	Set of Microsoft-supplied .msc names/paths allowed in the environment to suppress noise.
SuspiciousMSCPathRegex	Regex for user-writable and network paths indicating risky .msc staging (Users, AppData, Downloads, Desktop, UNC).
AllowedCLSIDs	Baseline of CLSIDs expected to be activated by mmc.exe; alert on unknown/new.
ParentProcessAllowList	Expected parents for mmc.exe (explorer.exe, services) vs. unusual (powershell, wscript, office apps).
SignedToUnsignedTransition	Flag when signed mmc.exe results in loading unsigned DLLs.
ExternalIPAllowlist	Approved external ranges/domains to exclude when mmc.exe makes network requests.