Detect WMI Event Subscription for Persistence via WmiPrvSE Process and MOF Compilation, Detection Strategy DET0086

Archived: 2026-04-05 16:25:29 UTC

AN0236

Monitor for creation of WMI EventFilter, EventConsumer, and FilterToConsumerBinding objects through WMI or MOF file execution. Detect command-line execution of `mofcomp.exe`, usage of `Register-WmiEvent` via PowerShell, and anomalous child processes of `WmiPrvSE.exe` that indicate triggered execution. Look for lateral anomalies in process lineage and WMI logging channels.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines temporal correlation range between WMI creation and child process execution
UserContext	Tune for specific accounts (e.g., SYSTEM or attacker-controlled users)
ProcessNameAllowlist	Used to exclude known benign consumers triggered via WMI (e.g., backup tools)
ParentProcessAnomalyThreshold	Defines what constitutes anomalous spawning from WmiPrvSE.exe