Detection of Windows Service Creation or Modification, Detection Strategy DET0552

Archived: 2026-04-05 14:18:39 UTC

AN1527

Detects creation or modification of Windows Services through command-line tools (e.g., `sc.exe`, `powershell.exe`), Registry key changes under `HKLM\System\CurrentControlSet\Services`, and service execution under SYSTEM with unsigned or anomalous binary paths. Detects privilege escalation via driver installation or `CreateServiceW` usage. Correlates parent-child lineage, startup behavior, and rare service names.

Log Sources

Mutable Elements

Field	Description
ServiceNamePattern	Regex for suspicious or uncommon service names (e.g., `svhostx`, `winhelp`, etc.)
ImagePathFilter	Flag services whose image path resides in uncommon directories (e.g., `C:\Users\`, `C:\Temp\`)
DriverExtensionList	Watch for `.sys` files loaded by `sc`, Registry, or `ZwLoadDriver` APIs
StartupTypeChangeWindow	Temporal window to correlate Registry `Start` key changes with service creation
UnsignedBinaryAlert	Raise alerts for unsigned binaries registered as services

---