Detection Strategy for System Services Service Execution, Detection Strategy DET0421

Archived: 2026-04-05 16:28:49 UTC

AN1185

Detection focuses on abnormal service executions initiated via service control manager APIs, sc.exe, net.exe, or PsExec creating temporary services. Defenders observe process creation of services.exe spawning non-standard binaries, registry changes in service keys followed by rapid execution, and network connections originating from processes tied to transient services. Correlation across process lineage, registry activity, and service logs provides strong signals of malicious service execution.

Log Sources

Mutable Elements

Field	Description
ServiceBinaryAllowlist	Known binaries/services expected to be invoked via services.exe
ParentProcessCorrelationWindow	Time window for correlating service creation with execution events
RemoteExecutionHosts	Approved remote hosts that may trigger service execution (e.g., via PsExec)
