Detection Strategy for System Services across OS platforms., Detection Strategy DET0279

Archived: 2026-04-05 16:19:59 UTC

AN0778

Monitor for abnormal creation or modification of Windows services (e.g., via sc.exe, PowerShell, or API calls) that load non-standard executables. Correlate registry changes in service keys with service creation events and process execution to detect service abuse for persistence or execution.

Log Sources

Mutable Elements

Field	Description
ServiceAllowlist	Known good services and installers that regularly modify or create services
TimeWindow	Threshold for correlating service creation with unusual process execution

AN0779

Detect unusual invocations of systemctl, service, or init scripts creating or modifying daemons. Monitor audit logs for execution of binaries from unexpected paths linked to service start/stop activity.

Log Sources

Mutable Elements

Field	Description
ServiceBinaryPaths	Valid directories for service binaries to filter out benign changes
UserContext	Expected accounts performing service management (e.g., root/admin)

AN0780

Monitor launchd service definitions and property list (.plist) modifications for non-standard executables. Detect unauthorized processes registered as launch daemons or agents.

Log Sources

Mutable Elements

Field	Description
PlistAllowlist	Known launch agents/daemons expected to be modified by updates or IT tools
PayloadEntropyThreshold	Entropy level for detecting suspicious binary payloads in launchd services

---