Detection of System Process Creation or Modification Across Platforms, Detection Strategy DET0571

Archived: 2026-04-05 12:54:48 UTC

AN1575

Detects command-line or API-based creation/modification of Windows Services via `sc.exe`, `powershell.exe`, `services.exe`, or `ChangeServiceConfig`. Looks for creation/modification of autostart services via registry changes, file drops to `System32\services`, and anomalous parent-child process trees.

Log Sources

Mutable Elements

Field	Description
ServiceNamePattern	Regex patterns to flag unusual service names or binaries
ParentProcessFilter	List of non-administrative processes starting service management tools
RegistryPathList	Monitored autorun locations (e.g., `HKLM\System\CurrentControlSet\Services`)

AN1576

Detects creation or modification of `systemd` service units, addition of cron jobs that invoke binaries on boot, or suspicious writes to `/etc/init.d/`. Monitors `chmod +x` and `systemctl` execution paths, especially from non-root parent processes.

Log Sources

Mutable Elements

Field	Description
ServicePathRegex	Path-based filters to identify service unit files or init scripts
UserContextList	List of expected user contexts that normally perform service changes
CommandNameList	Binaries used to register/modify services

AN1577

Detects creation or modification of `LaunchDaemon` or `LaunchAgent` plist files under `/Library/LaunchDaemons/`, `~/Library/LaunchAgents/`, or similar. Monitors execution of `launchctl`, property list edits, and file permission changes.

Log Sources

Mutable Elements

Field	Description
PlistPathList	Watched directories for LaunchDaemons and LaunchAgents
PlistKeyMonitor	Monitored keys such as `RunAtLoad`, `KeepAlive`, or `ProgramArguments`
UnsignedBinaryAlert	Flag execution of unsigned or non-Apple-signed binaries within plist

AN1578

Detects creation of new container system processes via `docker run --restart`, `kubectl exec` to init containers, or modification of container init specs. Flags container images that override entrypoints to embed persistence behaviors.

Log Sources

Mutable Elements

Field	Description
EntrypointOverridePattern	Patterns used to detect modified container start scripts
RestartPolicyMatch	Policy values triggering alert (e.g., always, on-failure)
KubeInitModPath	Path filters for `/etc/init.d/`-like behaviors inside containers

---