Cross-Platform Behavioral Detection of Scheduled Task/Job Abuse, Detection Strategy DET0094

Archived: 2026-04-05 13:43:01 UTC

AN0258

Detects creation or modification of scheduled tasks using schtasks.exe, at.exe, or COM objects followed by execution of outlier processes tied to the scheduled job.

Log Sources

Mutable Elements

Field	Description
TaskAuthor	Unexpected user or account context initiating the task.
CommandLineRegex	Suspicious binaries or script usage tied to scheduled tasks.
ExecutionWindow	Lookback window to correlate process execution after task registration.

AN0259

Detects creation or modification of cron jobs via crontab, /etc/cron.* directories, or systemd timer units with execution by unusual users or non-standard intervals.

Log Sources

Mutable Elements

Field	Description
CronSchedulePattern	Look for high-frequency or off-hour scheduling patterns.
ServiceUser	Unusual users scheduling jobs (e.g., www-data, nobody).
BinaryEntropy	Abnormal scripts or binaries tied to the scheduled job.

AN0260

Detects creation or alteration of LaunchAgents or LaunchDaemons with corresponding plist modification followed by execution of associated binaries.

Log Sources

Mutable Elements

Field	Description
PlistLabel	Labels not associated with known applications or vendors.
LaunchPath	Executable path outside of standard directories (/usr/bin, /Applications).
JobRunInterval	Unexpected periodic job intervals (e.g., every minute).

AN0261

Detects unusual use of `cron` or `sleep` loops inside containers executing unfamiliar scripts or binaries repeatedly.

Log Sources

Mutable Elements

Field	Description
ContainerLabel	Labels or tags indicating dev/test containers executing scheduled tasks.
ScriptFrequency	Repetitive invocation pattern within short container lifespan.
ImageSource	Unexpected container image sources creating cron entries.

AN0262

Detects modification of ESXi cron jobs, local.sh scripts, or scheduled API calls to persist custom binaries or shell scripts.

Log Sources

Mutable Elements

Field	Description
StartupScriptName	Filename not matching expected initialization scripts.
ExecutionContext	Commands run from unexpected SSH sessions or elevated shells.
PersistenceInterval	Rare scheduling triggers (e.g., @reboot + hourly repetition).

Source: https://attack.mitre.org/detectionstrategies/DET0094#AN0258