Detection Strategy for Ignore Process Interrupts, Detection Strategy DET0067

Archived: 2026-04-05 13:26:07 UTC

AN0181

Execution of processes using nohup or shell redirection to ignore SIGHUP and continue running after session termination. Defender perspective: correlation between commands including nohup, disowned jobs, or `&` suffix with continued process execution after parent terminal exit.

Log Sources

Mutable Elements

Field	Description
IgnoredSignals	Specific signals to monitor (e.g., SIGHUP, SIGINT) depending on environment baseline.
ProcessLifetimeThreshold	Duration a process continues running after session logout, adjustable to reduce noise from benign long-lived jobs.

AN0182

PowerShell or script execution with parameters that suppress errors or ignore user interrupts, such as `-ErrorAction SilentlyContinue`. Defender perspective: detecting discrepancies between suppressed error arguments and continued execution behavior.

Log Sources

Mutable Elements

Field	Description
MonitoredCmdlets	List of PowerShell cmdlets where suppressed error handling is suspicious (e.g., Invoke-Expression, Invoke-WebRequest).
ErrorActionThreshold	Frequency of suppressed error actions within time window that should trigger detection.

AN0183

Use of nohup, disown, or AppleScript constructs to suppress process interrupts. Defender perspective: commands containing nohup or hidden background tasks (`osascript` with persistent execution) correlated with processes surviving user logouts.

Log Sources

Mutable Elements

Field	Description
WatchedShells	Shells or interpreters where nohup/disown usage is suspicious, configurable to environment.
PersistenceCorrelationWindow	Time window to correlate process continuation after logout with suspicious commands.
