Detection Strategy for Power Settings Abuse, Detection Strategy DET0417

Archived: 2026-04-05 14:30:02 UTC

AN1174

Monitor command execution of powercfg.exe with arguments modifying sleep, hibernate, or display timeouts. Abnormal or repeated modifications to power settings outside administrative baselines may indicate persistence attempts. Correlate process creation with registry and system configuration changes to build behavioral chains.

Log Sources

Mutable Elements

Field	Description
AllowedAdminTools	Whitelist expected administrative scripts that legitimately modify power settings.
TimeWindow	Correlation period between powercfg.exe invocation and registry/policy changes.

AN1175

Detect execution of system utilities (systemctl, systemd-inhibit, systemdsleep) modifying sleep or hibernate behavior. Abnormal edits to system configuration files (e.g., /etc/systemd/sleep.conf) should be correlated with process execution to identify persistence techniques.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of systemctl, loginctl, or systemd-inhibit commands related to sleep/hibernate
File Modification (DC0061)	auditd:PATH	write: File modifications to /etc/systemd/sleep.conf or related power configuration files

Mutable Elements

Field	Description
KnownMaintenanceWindows	Filter benign modifications during patching or system maintenance intervals.

AN1176

Monitor pmset command executions altering sleep/hibernate/standby parameters. Unexpected modifications to /Library/Preferences/SystemConfiguration/com.apple.PowerManagement.plist or similar files should be correlated with process activity.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Process creation events where command line = pmset with arguments affecting sleep, hibernatemode, displaysleep
File Modification (DC0061)	macos:unifiedlog	write: File modification to com.apple.PowerManagement.plist or related system preference files

Mutable Elements

Field	Description
AdminWhitelists	Allowlist expected pmset invocations by IT administrators for power policy enforcement.
