Behavioral Detection of Command and Scripting Interpreter Abuse, Detection Strategy DET0516

Archived: 2026-04-05 16:02:52 UTC

AN1428

Detects the execution of scripting or command interpreters (e.g., powershell.exe, cmd.exe, wscript.exe) outside expected administrative time windows or from abnormal user contexts, often followed by encoded/obfuscated arguments or secondary execution events.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Tunable to match encoded or uncommon script execution patterns specific to the environment.
ParentProcessName	May vary across managed/unmanaged workstations or user-driven script activity.
TimeWindow	Used to restrict analysis to work hours or known admin maintenance windows.

AN1429

Detects use of shell interpreters (e.g., bash, sh, python, perl) initiated by users or processes not normally executing them, especially when chaining suspicious utilities like netcat, curl, or ssh.

Log Sources

Mutable Elements

Field	Description
InterpreterName	Regex to identify which interpreters (bash, python, ruby) to monitor based on typical usage.
UserContext	Scope to users or service accounts not expected to run interpreters interactively.
ExecutionChainLength	Defines maximum process tree depth to correlate interpreter execution with its effects.

AN1430

Detects launch of command-line interpreters via Terminal, Automator, or hidden `osascript`, especially when parent process lineage deviates from user-initiated applications.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	log stream --info --predicate 'eventMessage CONTAINS "exec"'

Mutable Elements

Field	Description
LaunchAgentName	Monitor for specific plist agents frequently abused for persistence or payload execution.
ScriptName	Path or script name pattern (e.g., hidden files, /tmp locations).
TerminalAppUsage	Adjust based on whether Terminal.app use is common or restricted in user policy.

AN1431

Detects use of 'esxcli system' or direct interpreter commands (e.g., busybox shell) invoked from SSH or host terminal unexpectedly.

Log Sources

Mutable Elements

Field	Description
ShellEnabledFlag	Control alerting based on whether ESXi shell access is typically disabled.
SSHContext	Scope detection to SSH session origins or internal vs. remote access.

AN1432

Identifies CLI interpreter access (e.g., Cisco IOS, Juniper JUNOS) via `enable` mode or scripting-capable sessions used by uncommon accounts or from unknown IPs.

Log Sources

Mutable Elements

Field	Description
UserRole	Which roles or privilege levels should be monitored for interpreter misuse.
DeviceType	Support filtering for routers, switches, firewalls depending on network segmentation.
