Detection Strategy for Input Injection, Detection Strategy DET0568

Archived: 2026-04-05 17:10:44 UTC

AN1567

Detects suspicious USB HID device enumeration and keystroke injection patterns, such as rapid sequences of input with no user context, scripts executed through simulated keystrokes, or rogue devices presenting themselves as keyboards.

Log Sources

Mutable Elements

Field	Description
AuthorizedUSBDevices	List of known, legitimate USB vendor/product IDs authorized for use in the enterprise.
ExecutionTimeWindow	Restrict detection to times when no user is logged in or activity is outside business hours.
ParentProcessWhitelist	List of legitimate parent processes expected to spawn PowerShell or scripting engines.

AN1568

Detects USB HID device enumeration under `/sys/bus/usb/devices/` and rapid keystroke injection resulting in command execution such as bash or Python scripts launched without interactive user activity.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: parent process is usb/hid device handler, child process bash/python invoked
Drive Creation (DC0042)	linux:syslog	New HID device enumeration with type 'keyboard' followed by immediate input injection

Mutable Elements

Field	Description
USBVendorIDs	Track suspicious or unapproved USB vendor/product IDs.
ScriptExecutionThreshold	Time threshold for script execution after HID injection, e.g., less than 10 seconds.

AN1569

Detects abnormal HID device enumeration via I/O Registry (ioreg -p IOUSB) and keystroke injection targeting AppleScript, osascript, or PowerShell equivalents. Defender correlates new USB device connections with rapid script execution.

Log Sources

Data Component	Name	Channel
Drive Creation (DC0042)	macos:unifiedlog	New IOUSB keyboard/HID device enumerated with suspicious attributes
Script Execution (DC0029)	macos:unifiedlog	osascript, AppleScript, or Python execution triggered immediately after HID connection

Mutable Elements

Field	Description
AllowedAppleScripts	Whitelist of AppleScripts expected in the environment, to minimize false positives.
TimeWindow	Timeframe between HID injection and script execution considered suspicious.
