Peripheral Device Enumeration via System Utilities and API Calls, Detection Strategy DET0491

Archived: 2026-04-05 17:40:38 UTC

AN1353

Suspicious enumeration of attached peripherals via WMI, PowerShell, or low-level API calls potentially chained with removable device interactions.

Log Sources

Mutable Elements

Field	Description
CommandLineRegex	Regex patterns for device enumeration utilities (e.g., 'Get-PnpDevice', 'wmic path Win32_USBController')
TimeWindow	Time threshold for grouping device discovery with follow-on access or manipulation
UserContext	Filter privileged or service accounts known to legitimately execute enumeration scripts

AN1354

Enumeration of USB and other peripheral hardware via udevadm, lshw, or /sys or /proc interfaces in proximity to collection or mounting behavior.

Log Sources

Mutable Elements

Field	Description
ExecutableList	Set of binaries used for peripheral enumeration (e.g., 'lshw', 'lsusb', 'udevadm')
UserContext	Tuning based on which users/scripts are authorized to query device state

AN1355

Execution of system utilities like 'system_profiler' and 'ioreg' to enumerate hardware components or USB devices, particularly if followed by clipboard, file, or network activity.

Log Sources

Mutable Elements

Field	Description
BinaryList	Commands like 'system_profiler SPUSBDataType', 'ioreg -p IOUSB' that may indicate enumeration
TimeWindow	Temporal grouping of enumeration with follow-on activity (e.g., clipboard capture, exfiltration)
