System Discovery via Native and Remote Utilities, Detection Strategy DET0525

Archived: 2026-04-05 17:36:19 UTC

AN1452

Process creation and command-line execution of native system discovery utilities such as `systeminfo`, `hostname`, `wmic`, or use of PowerShell/WMI for system enumeration.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Detect multiple discovery commands executed in short succession.
UserContext	Scope alerts to unusual user accounts or service accounts.

AN1453

Execution of system enumeration commands such as `uname`, `df`, `uptime`, `hostname`, `lscpu`, and `cat /etc/os-release` through local terminal or scripts.

Log Sources

Mutable Elements

Field	Description
CommandList	Customize list of commands of interest (e.g., uname, lscpu, etc.)
TerminalSessionID	Correlate sessions for behavior context.

AN1454

Execution of system info utilities like `systemsetup`, `sw_vers`, `uname`, or `sysctl` by terminal or scripted processes.

Log Sources

Mutable Elements

Field	Description
ParentProcess	Determine if script or terminal executed the command.
FrequencyThreshold	Number of discovery commands in a short window.

AN1455

Execution of `esxcli system hostname get`, `esxcli system version get`, or `esxcli hardware` commands through SSH or local shell.

Log Sources

Mutable Elements

Field	Description
SessionOrigin	Track SSH or console-based entry points.
CommandString	Customize detection for expected CLI queries.

AN1456

Use of cloud API calls (e.g., AWS EC2 DescribeInstances, Azure VM Inventory) to enumerate system configurations across assets.

Log Sources

Mutable Elements

Field	Description
IAMRoleContext	Limit detection to non-standard identities performing these calls.
APIFrequency	Identify enumeration sweeps by volume.

AN1457

Execution of `show version`, `show hardware`, or `show system` commands through CLI via SSH or console.

Log Sources

Mutable Elements

Field	Description
Username	Highlight unexpected users issuing diagnostic commands.
CommandList	Tailor to vendor-specific command syntax.

Source: https://attack.mitre.org/detectionstrategies/DET0525#AN1456