Local Storage Discovery via Drive Enumeration and Filesystem Probing, Detection Strategy DET0188

Archived: 2026-04-05 18:25:33 UTC

AN0536

Drive enumeration using PowerShell (`Get-PSDrive`), `wmic logicaldisk` , or Win32 API indicative of local volume enumeration by non-admin users or executed outside of baseline system inventory scripts.

Log Sources

Mutable Elements

Field	Description
user_context	Non-system accounts performing drive enumeration may be higher fidelity indicators
parent_process_name	Baseline parent-child process lineage can help distinguish admin tools from malicious scripts

AN0537

Abnormal use of `lsblk` , `fdisk -l` , `lshw -class disk` , or `parted` by non-admin users or within non-interactive shells suggests suspicious disk enumeration activity.

Log Sources

Mutable Elements

Field	Description
TTY_type	Detection can exclude interactive TTY sessions to reduce false positives from admin usage
shell_parent	Differentiate between interactive user shells vs. script-based execution

AN0538

Disk enumeration via `diskutil list` or `system_profiler SPStorageDataType` run outside of user login or not associated with system inventory tools

Log Sources

Mutable Elements

Field	Description
launch_agent_context	Unexpected use of disk enumeration tools from GUI apps or LaunchAgents may indicate abuse
volume_name_filter	Filter known baseline volume names or identifiers used by common device configurations

AN0539

Use of `esxcli storage` or `vim-cmd vmsvc/getallvms` by unusual sessions or through interactive shells unrelated to administrative maintenance tasks.

Log Sources

Mutable Elements

Field	Description
ssh_source_ip	Restrict alerts to unexpected remote sessions accessing host storage commands
esxcli_command_scope	Tailor detection based on subcommands more likely to be abused

---