Detection of Direct Volume Access for File System Evasion, Detection Strategy DET0426

Archived: 2026-04-05 17:25:17 UTC

AN1193

Processes accessing raw logical drives (e.g., .\C:) to bypass file system protections or directly manipulate data structures.

Log Sources

Mutable Elements

Field	Description
TargetObjectPattern	Regex pattern to detect access to raw disk volumes like `\Device\HarddiskVolume` or `\.\PhysicalDrive*`.
ParentProcess	Tune for known tools/scripts (e.g., powershell.exe, cmd.exe) often used in misuse scenarios.
TimeWindow	Correlate file access and creation across a short time window to avoid false positives.

AN1194

CLI or automated utilities accessing raw device volumes or flash storage directly (e.g., via `copy flash:`, `format`, or `partition` commands).

Log Sources

Mutable Elements

Field	Description
CommandScope	Limit detection to volume-level commands (e.g., `format`, `copy`, `mount`, `erase`).
DeviceTypeFilter	Filter by internal vs. removable volume interactions (e.g., flash, SD card).

Source: https://attack.mitre.org/detectionstrategies/DET0426