

# Detection Strategy for Disk Content Wipe via Direct Access and Overwrite, Detection Strategy DET0316

Archived: 2026-04-05 16:17:30 UTC

## AN0882

Processes attempting raw disk access via \\PhysicalDrive paths, abnormal file I/O to MBR/boot sectors, or loading of third-party drivers (e.g., RawDisk) that enable disk overwrite. Correlate process creation, privilege usage, and disk modification events within a short time window.

### Log Sources

### Mutable Elements

Field	Description
ProcessWhitelist	Backup, forensics, or imaging tools may perform legitimate raw disk access — requires tuning per environment.
TimeWindow	Correlation threshold for process execution, driver load, and raw disk writes.

## AN0883

Execution of destructive utilities (dd, shred, wipe) targeting block devices, or processes invoking syscalls to directly overwrite /dev/sd or /dev/nvme partitions. Correlate abnormal file write attempts with shell process execution and block device access.

### Log Sources

Data Component	Name	Channel
<a href="#">Drive Access (DC0054)</a>	auditd:SYSCALL	open/write syscalls to block devices (/dev/sd*, /dev/nvme*)
<a href="#">Process Creation (DC0032)</a>	auditd:EXECVE	Execution of dd, shred, or wipe with arguments targeting block devices

### Mutable Elements

Field	Description
TargetDevices	Exclude removable drives or designated partitions that may be overwritten during maintenance.
EntropyThreshold	Tune detection for pseudorandom write patterns to reduce false positives during high-volume I/O.

### AN0884

Abnormal invocation of diskutil or asr with destructive flags (eraseDisk, zeroDisk), or low-level IOKit calls that overwrite raw disk content. Detect correlation between elevated process execution and disk erase operations.

#### Log Sources

#### Mutable Elements

Field	Description
AdminToolWhitelist	Provisioning workflows may legitimately use diskutil/asr — whitelist by user or system context.

### AN0885

Execution of CLI commands erasing file systems or storage (erase flash:, format disk, erase nvram:). Detect authentication events followed by destructive commands within the same privileged session.

#### Log Sources

#### Mutable Elements

Field	Description
PrivilegedUsers	Tune to exclude approved maintenance performed by authorized administrators.
CommandPatterns	Expand or narrow destructive command coverage depending on vendor-specific syntax.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0316#AN0882>