Detection Strategy for Disk Structure Wipe via Boot/Partition Overwrite, Detection Strategy DET0297

Archived: 2026-04-05 16:03:56 UTC

AN0827

Processes attempting raw disk access to overwrite sensitive structures such as the MBR or partition table using \.\PhysicalDrive notation. Detection relies on correlating process creation, privilege escalation, and raw sector writes in Sysmon and Security logs.

Log Sources

Mutable Elements

Field	Description
SectorRange	Specify which sectors are considered critical (MBR, partition table) to reduce noise.
ProcessWhitelist	Exclude legitimate low-level disk management or imaging tools used by administrators.

AN0828

Execution of utilities (dd, hdparm, sgdisk) or custom binaries attempting to overwrite disk boot structures (/dev/sda MBR sector or partition tables). Detection correlates shell execution with syscalls writing to sector 0 or disk metadata blocks.

Log Sources

Mutable Elements

Field	Description
TargetDevices	Define specific device paths to monitor (e.g., /dev/sda, /dev/nvme0n1).
OffsetThreshold	Focus on suspicious writes at disk offsets corresponding to MBR/partition structures.

AN0829

Abnormal invocation of diskutil or asr that modifies partition tables or initializes raw devices. Monitor for IOKit system calls targeting disk headers or EFI boot sectors, correlated with elevated privileges.

Log Sources

Mutable Elements

Field	Description
AdminToolWhitelist	System provisioning workflows may legitimately re-partition disks; whitelist by context.

AN0830

Execution of destructive CLI commands such as format flash:, format disk, or equivalent vendor-specific commands that erase filesystem structures. Detection correlates AAA logs showing privileged access with immediate format/erase commands.

Log Sources

Mutable Elements

Field	Description
CommandPatterns	Expand detection to cover vendor-specific destructive commands.
PrivilegedUsers	Whitelist authorized maintenance sessions to reduce false positives.
