Detection Strategy for File Creation or Modification of Boot Files, Detection Strategy DET0150

Archived: 2026-04-02 12:39:00 UTC

AN0428

Detection of raw access to physical drives, modification of boot records (MBR/VBR), and suspicious file creation or alteration within the EFI System Partition (ESP). Correlates privileged process execution with low-level disk modification and unexpected driver or firmware interactions.

Log Sources

Mutable Elements

Field	Description
KnownGoodMBRHashes	Baseline hashes of clean MBR/VBR sectors for comparison
ESPFileWhitelist	Approved EFI executables within ESP directories
TimeWindow	Correlation window between privileged access, raw disk modification, and EFI file creation

AN0429

Detection of suspicious write operations to block devices, modifications of bootloader files (GRUB, initrd, vmlinuz), and unexpected changes within the EFI System Partition. Monitors privileged execution of utilities like dd, grub-install, or efibootmgr that modify boot sectors or loader entries.

Log Sources

Mutable Elements

Field	Description
BootloaderHashBaseline	Baseline checksums of GRUB, kernel, and initramfs images
EFIFileAllowlist	Trusted EFI executables for Linux environments
AlertThresholds	Tunable thresholds for triggering alerts on repeated EFI/bootloader writes

Source: https://attack.mitre.org/detectionstrategies/DET0150#AN0429