Detection Strategy for T1542.002 Pre-OS Boot: Component Firmware, Detection Strategy DET0323

Archived: 2026-04-05 15:11:49 UTC

AN0916

Detection of anomalous driver and firmware interactions, including unsigned or unexpected firmware updates, driver loads linked to hardware components, and suspicious use of privileged APIs to read/write firmware or controller memory.

Log Sources

Mutable Elements

Field	Description
KnownGoodFirmwareHashes	Environment-specific list of baseline firmware images for integrity comparison
DriverAllowList	Drivers approved for loading in production environments
TimeWindow	Correlation period between firmware modification attempt and abnormal driver or process behavior

AN0917

Detection of suspicious use of ioctl/sysfs calls to access device firmware, unexpected flashing tools execution, and anomalous firmware checksums logged by SMART or kernel audit mechanisms.

Log Sources

Mutable Elements

Field	Description
FirmwareImageBaseline	Baseline firmware checksums for comparison
AlertThresholds	Tolerance levels for SMART errors before triggering alerts

AN0918

Detection of EFI/firmware manipulation attempts via abnormal driver loads, unsigned kexts, or tampered NVRAM variables associated with component firmware configuration.

Log Sources

Data Component	Name	Channel
Firmware Modification (DC0004)	macos:unifiedlog	Firmware update events or kernel extension (kext) loads not signed by Apple

Mutable Elements

Field	Description
ApprovedKextList	List of trusted and signed kexts permitted in production systems
EFIHashBaseline	Known-clean EFI image hashes used for verification

---