Hardware Supply Chain Compromise Detection via Host Status & Boot Integrity Checks, Detection Strategy DET0368

Archived: 2026-04-02 12:11:08 UTC

AN1035

Detects tampered hardware or firmware via anomalous host status telemetry. Behavioral chain: (1) Pre-OS or firmware components exhibit unexpected version changes, signature failures, or modified boot paths; (2) System management/firmware tools log hardware inventory drift; (3) Sensor health telemetry or boot attestation events fail baseline checks; (4) Follow-on process execution from altered firmware or unknown drivers after boot.

Log Sources

Mutable Elements

Field	Description
BaselineFirmwareVersion	Expected firmware/BIOS version for each hardware model.
BaselineDriverList	Approved boot-start drivers.
IntegrityCheckInterval	Frequency of integrity checks (e.g., daily, weekly).

AN1036

Monitors for hardware or firmware tampering by correlating system boot logs, hardware inventory changes, and secure boot/firmware verification failures. Behavioral chain: (1) UEFI/BIOS version drift; (2) secure boot disabled or signature verification errors; (3) unexpected modules or hardware devices enumerated at boot; (4) new device firmware images loaded from non-approved sources.

Log Sources

Mutable Elements

Field	Description
ApprovedFirmwareHashes	List of SHA256/SHA512 firmware hashes allowed.
AllowedDeviceIDs	Known hardware component IDs per host baseline.

AN1037

Detects tampered Mac hardware/firmware by analyzing unified logs, EndpointSecurity events, and Apple Mobile File Integrity (AMFI) checks. Behavioral chain: (1) Boot process reports firmware signature mismatch; (2) Secure Boot policy altered; (3) new EFI drivers or hardware devices appear in inventory; (4) system extension loads from unapproved developer IDs post-boot.

Log Sources

Mutable Elements

Field	Description
AllowedTeamIDs	Developer Team IDs approved for kext/system extension loads.
FirmwareVersionBaseline	Expected EFI/firmware version for Mac model.
