Detection Strategy for Modify System Image on Network Devices, Detection Strategy DET0170

Archived: 2026-04-05 16:18:32 UTC

AN0482

Defenders may observe adversary attempts to alter or replace a network device’s operating system image through anomalous CLI commands, unexpected firmware updates, integrity check failures, or mismatches in version and checksum validation. Suspicious behavior includes modification of image files on storage, OS version output inconsistent with baselines, unexpected reloads or reboots after image replacement, and changes to boot configuration that load non-standard system images.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:cli	Execution of commands to load, copy, or replace system images (e.g., 'copy tftp flash', 'boot system')
File Modification (DC0061)	networkdevice:config	Configuration changes to boot variables, startup image paths, or checksum verification failures

Mutable Elements

Field	Description
AuthorizedAdminAccounts	Defines trusted administrator accounts allowed to modify system images; deviations indicate possible malicious modification.
ApprovedFirmwareVersions	Whitelist of validated vendor OS images; unexpected versions may suggest adversarial tampering.
TimeWindow	Correlation window for detecting config changes followed by firmware updates or reboots.
ChecksumBaseline	Baseline cryptographic hashes of approved system images; deviations may indicate compromise.