Behavioral detection for Supply Chain Compromise (package/update tamper → install → first-run), Detection Strategy DET0537

Archived: 2026-04-05 18:17:34 UTC

AN1480

1) New or updated software is delivered/installed from atypical sources or with signature/hash mismatches; 2) installer/updater writes binaries to unexpected paths or replaces existing signed files; 3) first run causes unsigned/abnormally signed modules to load or child processes to execute, optionally followed by network egress to new destinations.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between install events and first-run activity (default 2h; adjust for staged rollouts).
TrustedPublishers	Publisher/Signer allow-list to suppress expected updates.
TrustedUpdateHosts	Known update CDNs/APIs (e.g., download.microsoft.com) to reduce egress false positives.
RiskScoreThreshold	Score cut-off for alerting when combining path, signer, and reputation features.

AN1481

1) Package manager or curl/wget installs/upgrades from non-approved repos or unsigned packages; 2) new ELF written into PATH directories or replacement of existing binaries/libraries; 3) first run leads to unexpected child processes or outbound connections.

Log Sources

Mutable Elements

Field	Description
ApprovedRepos	Allow-listed APT/YUM repo URLs and GPG key fingerprints.

Field	Description
PathScope	Directories to watch for new ELF writes (e.g., /usr/bin, /usr/local/bin, /lib*/, /opt/*/bin).
MinBinarySize	Ignore tiny helper files; default >16KB.
TimeWindow	Install→first-run correlation window (default 2h).

AN1482

1) pkg/notarization installs from atypical sources or with Gatekeeper/AMFI warnings; 2) new Mach-O written into /Applications or ~/Library paths or substitution of signed components; 3) first run from installer spawns unsigned children or exfil.

Log Sources

Mutable Elements

Field	Description
AllowedTeamIDs	Apple Developer Team IDs permitted in your fleet.
TrustedDMGs	Known DMG/Pkg sources and hashes.
TimeWindow	Install→first-run correlation window (default 2h).
RiskScoreThreshold	Adjust alert sensitivity based on org tolerance.
