Detect Compromise of Host Software Binaries, Detection Strategy DET0336

Archived: 2026-04-05 16:47:27 UTC

AN0949

Monitors for unexpected modifications of system or application binaries, particularly signed executables. Correlates file write events with subsequent unsigned or anomalously signed process execution, and checks for tampered binaries outside normal patch cycles.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Define critical directories (e.g., C:\Windows\System32, Program Files) for binary integrity checks
SignatureValidation	Adjust enforcement level of digital signature verification based on enterprise risk appetite
TimeWindow	Correlate file modification with subsequent process execution within a defined time window

AN0950

Detects modification of system or application binaries by monitoring /usr/bin, /bin, and other privileged directories. Correlates file integrity monitoring (FIM) events with unexpected process executions or service restarts.

Log Sources

Mutable Elements

Field	Description
WatchedDirectories	Customize monitored directories (e.g., /usr/bin, /usr/sbin, /opt/apps) for binary tampering
BaselineHashes	Maintain golden file hashes for integrity validation

AN0951

Monitors binary modification in /Applications and system library paths. Detects unsigned or improperly signed binaries executed after modification. Tracks Gatekeeper or notarization bypass attempts tied to modified binaries.

Log Sources

Mutable Elements

Field	Description
ApplicationPaths	Tune which application and library directories are monitored for tampering
SignatureVerificationDepth	Define strictness of code-signing validation checks

AN0952

Detects unauthorized modification of host binaries, modules, or services within ESXi. Correlates tampered files with subsequent unexpected service behavior or malicious module load attempts.

Log Sources

Mutable Elements

Field	Description
MonitoredModules	Define critical ESXi binaries and kernel modules requiring integrity validation
CorrelationWindow	Adjust timing correlation between binary modification and module/service anomalies

---