Detection Strategy for Runtime Data Manipulation., Detection Strategy DET0391

Archived: 2026-04-05 16:13:16 UTC

AN1097

Monitor for runtime data manipulations by detecting suspicious modification of application binaries, API hooking, or unexpected behavior from processes responsible for rendering or displaying data. Correlate registry edits, process creation, and unexpected binary hash mismatches.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Directory paths of business-critical applications where runtime manipulations are most impactful.
HashBaseline	Expected cryptographic hashes of application binaries used for runtime data display.

AN1098

Detect runtime manipulation by monitoring system calls for modifications to shared libraries, ELF binaries, or environment variables that affect how data is displayed. Look for suspicious writes to application directories and mismatch in binary integrity baselines.

Log Sources

Mutable Elements

Field	Description
WatchedBinaries	Specific critical application binaries or libraries to monitor for unauthorized changes.
IntegrityCheckFrequency	Interval for verifying hashes of executables and libraries.

AN1099

Monitor for runtime manipulation by observing changes in application bundles, unexpected signing modifications, and runtime API calls that inject or alter how data is displayed. Detect alterations in CFNetwork or

CoreFoundation frameworks responsible for rendering data.

Log Sources

Data Component	Name	Channel
File Metadata (DC0059)	macos:unifiedlog	Unexpected application binary modifications or altered signing status
File Modification (DC0061)	macos:osquery	CALCULATE: Mismatch in file integrity of critical macOS applications

Mutable Elements

Field	Description
AllowedApps	Whitelisted applications expected to handle sensitive runtime data.
SignatureEnforcement	Policy enforcement for validating application code signing integrity.
