Detect Gatekeeper Bypass via Quarantine Flag and Trust Control Manipulation, Detection Strategy DET0288

Archived: 2026-04-05 17:51:56 UTC

AN0800

Correlates suspicious removal or modification of the com.apple.quarantine extended attribute, manipulation of LSFileQuarantineEnabled values in Info.plist, and unexpected process execution of unsigned or non-notarized binaries. Also monitors abnormal trust validation failures in unified logs and unusual activity in QuarantineEvents database entries.

Log Sources

Mutable Elements

Field	Description
QuarantineBypassAllowList	Legitimate enterprise update tools or deployment frameworks that may strip quarantine flags
CertificateAuthorityList	Baseline trusted Apple Developer IDs and enterprise certs used for code signing
TimeWindow	Time correlation window for xattr modification followed by suspicious process execution