# Detect Subversion of Trust Controls via Certificate, Registry, and Attribute Manipulation, Detection Strategy DET0452

Archived: 2026-04-05 17:12:03 UTC

### AN1246

Detection correlates abnormal installation or modification of root or code-signing certificates, creation/modification of suspicious registry keys for trust providers, and unusual module loads from non-standard locations. Identifies unsigned or improperly signed executables bypassing trust prompts, combined with persistence artifacts.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| TrustedPublisherList | Baseline list of approved certificate authorities that should not change frequently |
| FilePathAllowList | Exclusions for legitimate enterprise-signed binaries stored in unusual directories |
| TimeWindow | Correlation window for registry + file + process activity |

### AN1247

Detection monitors extended attribute manipulation (xattr) to strip quarantine or trust metadata, anomalous installation of root certificates in /etc/ssl or /usr/local/share/ca-certificates, and unauthorized modification of system trust stores. Correlates with unexpected process execution involving package managers or custom certificate utilities.

#### Log Sources

| Data Component | Name | Channel |
|---|---|---|
| File Metadata (DC0059) | auditd:SYSCALL | chmod, chown, setxattr, or file writes to /etc/ssl/* or /usr/local/share/ca-certificates/* |
| Command Execution (DC0064) | auditd:EXECVE | Process execution of update-ca-certificates or openssl with suspicious arguments |

#### Mutable Elements

| Field | Description |
| --- | --- |
| CertificatePathList | Paths to monitor for changes depending on distro-specific trust locations |
| RegexPatterns | Regex patterns for suspicious use of xattr or openssl parameters |

### AN1248

Detection monitors modification of code signing attributes, Gatekeeper/quarantine flags, and insertion of new trust certificates via security add-trusted-cert. Identifies adversary use of xattr to strip quarantine flags from downloaded binaries. Correlates with abnormal module loads bypassing SIP protections.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| QuarantineBypassAllowList | List of enterprise apps where quarantine flag removal is expected |
| CertificateAuthorityList | Baseline trusted root and intermediate CAs for comparison |

---