Detection Strategy for Subvert Trust Controls using SIP and Trust Provider Hijacking., Detection Strategy DET0442

Archived: 2026-04-05 18:40:27 UTC

Analytics

- Windows

AN1222

Detection of anomalous registry modifications to Subject Interface Packages (SIPs) or trust provider DLL mappings, unexpected loading of non-Microsoft cryptographic modules, or attempts to redirect WinVerifyTrust validation logic. Defender view focuses on registry tampering, suspicious DLL loads into trusted processes, and abnormal trust validation failures correlated across event streams.

Log Sources

Mutable Elements

Field	Description
RegistryPathBaselines	Monitor for changes in Registry paths.
TimeWindow	Correlate between changes in Registry values, system files, and modules loaded.
