Detect Code Signing Policy Modification (Windows & macOS), Detection Strategy DET0523

Archived: 2026-04-02 11:26:59 UTC

Analytics

- Windows
- macOS

AN1446

Monitors execution of administrative utilities (e.g., bcdedit.exe) or registry modifications that disable Driver Signature Enforcement (DSE) or enable Test Signing. Correlates command-line activity, registry changes, and subsequent process executions that bypass signing enforcement.

Log Sources

Mutable Elements

Field	Description
MonitoredExecutables	Expand or restrict monitored utilities (e.g., bcdedit.exe, reg.exe) based on enterprise usage
RegistryPaths	Customize registry paths tied to Driver Signing enforcement depending on OS version
TimeWindow	Correlation window between registry modification and subsequent unsigned binary execution

AN1447

Detects modification of System Integrity Protection (SIP) or code signing enforcement policies through csrutil or kernel variable tampering. Correlates execution of csrutil disable commands with subsequent policy state changes and anomalous unsigned process executions.

Log Sources

Mutable Elements

Field	Description
PolicyPaths	Track configuration files and kernel extensions tied to SIP enforcement
AllowedUsers	Restrict or expand which privileged accounts are monitored for SIP/CSRUTIL changes
TimeWindow	Define correlation between csrutil execution and unsigned process activity

---