Detection Strategy for Steal or Forge Authentication Certificates, Detection Strategy DET0240

Archived: 2026-04-02 11:37:07 UTC

AN0671

Monitor for abnormal certificate enrollment and usage activity in Active Directory Certificate Services (AD CS), registry access to certificate storage locations, and unusual process executions that attempt to export or access private keys.

Log Sources

Mutable Elements

Field	Description
EKU_Thresholds	Organizations may tune which Extended Key Usage (EKU) values are considered risky.
TimeWindow	Defines how quickly multiple certificate enrollments from the same entity should trigger correlation alerts.
LogonContext	Differentiate between service accounts and interactive user accounts to reduce false positives.

AN0672

Monitor for file access to certificate directories, commands invoking OpenSSL or PKCS#12 utilities to export or modify certificates, and processes accessing sensitive key storage paths.

Log Sources

Mutable Elements

Field	Description
PathExclusions	Exempt trusted automated services regularly accessing PKI stores.
UserContext	Differentiate root/system accounts versus user-level access to key material.

AN0673

Monitor for security commands and API calls interacting with the Keychain, as well as file access attempts to stored certificates and private keys in ~/Library/Keychains or /Library/Keychains.

Log Sources

Mutable Elements

Field	Description
ApplicationAllowList	Whitelist legitimate apps that interact with Keychain to reduce false positives.

AN0674

Monitor for abnormal certificate enrollment events in identity platforms, unexpected use of token-signing certificates, and unusual CA configuration modifications.

Log Sources

Mutable Elements

Field	Description
GeoContext	Detect certificate-related changes occurring from unusual geographic locations.
Thresholds	Adjust enrollment/issuance request volume thresholds per tenant size.

Source: https://attack.mitre.org/detectionstrategies/DET0240