Detect Access to Unsecured Credential Files Across Platforms, Detection Strategy DET0307

Archived: 2026-04-05 15:14:39 UTC

AN0856

Correlated file access to insecure credential files (e.g., *.env,* .xml, *.ps1) followed by suspicious process execution or authentication using retrieved credentials. Detected through Sysmon logs and Windows Security Event logs.

Log Sources

Mutable Elements

Field	Description
FileNamePattern	Patterns like *.env, *credential* can be tuned to reduce noise or catch custom implementations
ProcessAccessScope	Defines scope of access (e.g., only untrusted parent processes or high-risk processes)
TimeWindow	Time delta between credential file access and use in logon attempt

AN0857

File reads or process executions involving insecurely stored credential files (e.g., config files with password fields) by non-root or anomalous users followed by ssh authentication attempts.

Log Sources

Mutable Elements

Field	Description
RegexPatterns	Patterns like password, secret, token can be expanded or customized
UserContextScope	Scope of users monitored (e.g., root vs all users)
TimeWindow	Time between suspicious file access and credential use

AN0858

Terminal-based grep or open of plist/config files containing credentials, correlated with Keychain or system login attempts.

Log Sources

Mutable Elements

Field	Description
KeychainToolAccess	Monitor unexpected use of security CLI or Keychain helper binaries
FileTypeList	Add or remove watched file types based on system usage

AN0859

Container processes accessing mounted secrets or configuration paths (e.g., /run/secrets, /mnt/config) followed by network access or credential use.

Log Sources

Mutable Elements

Field	Description
SecretMountPaths	Customize based on deployment structure (e.g., /mnt/, /run/secrets/)
ProcessBaselineDeviation	Tune anomaly scoring for container image deviations

AN0860

Access to local credential/config files (e.g., ~/.aws/credentials) followed by metadata API calls or cloud role assumptions.

Log Sources

Mutable Elements

Field	Description
CredentialFilePattern	Regex to match common credential files (e.g., *.aws/credentials, token.txt)
RoleAssumptionScope	Adjust scope of roles monitored (e.g., admin, service accounts)
TimeWindow	Correlation timing between file access and AssumeRole

---