Detect Access to macOS Keychain for Credential Theft, Detection Strategy DET0396

Archived: 2026-04-05 13:02:10 UTC

AN1112

Detects suspicious access to macOS Keychain files and APIs. Observes processes invoking the 'security' utility or accessing Keychain databases directly, correlates these with abnormal parent process lineage or unexpected user context. Monitors attempts to dump, unlock, or read credential storage beyond normal application workflows.

Log Sources

Mutable Elements

Field	Description
AllowedApplications	Whitelist of applications (e.g., Safari, Mail) normally permitted to access Keychain
AlertThreshold	Number of failed keychain unlock attempts before raising an alert
ParentProcessContext	Legitimate parent-child process relationships for security tool invocations