Detection of AppleScript-Based Execution on macOS, Detection Strategy DET0414

Archived: 2026-04-05 16:10:21 UTC

AN1164

Detects AppleScript execution via 'osascript', NSAppleScript/OSAScript APIs, and abnormal application control events across user sessions. Focuses on causal chains such as osascript spawning child processes, script-induced keystrokes, or API-backed dialog spoofing.

Log Sources

Mutable Elements

Field	Description
ScriptInvocationParent	Identify rare or suspicious parent processes launching AppleScript (e.g., Safari, Mail, msedge).
TimeWindow	Flag AppleScript execution during user-inactive hours, especially for automation frameworks.
AppleEventActionType	Filter AppleEvent-based automation involving UI interaction, keystrokes, or remote control.
TargetApplicationSet	Scope AppleScript use toward security-sensitive apps (e.g., Terminal, ssh, Keychain Access).
ExecutionPathRegex	Restrict to unusual paths like /tmp/, ~/Library/, or embedded in Automator workflows.