Detect Modification of macOS Startup Items, Detection Strategy DET0429

Archived: 2026-04-05 18:28:43 UTC

AN1197

Detects the modification or addition of Launch Agents or Startup Items to establish persistence. Adversaries may write plist or executable files to ~/Library/LaunchAgents/, /Library/StartupItems/, or similar directories and configure them to run at user or system boot. Detection requires correlating file creation or modification events with subsequent user logon or boot-time process execution.

Log Sources

Mutable Elements

Field	Description
directory_path	Specific paths to monitor may differ across macOS versions or enterprise baselines.
user_context	Different users may have unique LaunchAgents folders—tuning may be required.
time_window	The correlation time between file creation and process execution may need to be adjusted for boot persistence.
process_name	Specific startup binaries (e.g., bash, osascript) may vary across implementations.

Source: https://attack.mitre.org/detectionstrategies/DET0429#AN1197