Detection Strategy for Overwritten Process Arguments Masquerading, Detection Strategy DET0164

Archived: 2026-04-05 13:51:33 UTC

AN0466

Detects adversary behavior where the command-line arguments of a running process are overwritten in memory to spoof the process name, typically replacing it with a benign or misleading string. The detection correlates unexpected null byte sequences, discrepancies between `/proc/<pid>/cmdline` and process ancestry, and suspicious memory writes shortly after process start.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time threshold after process creation during which argv memory manipulation is expected to be rare; anomalies occurring outside this window may be more suspicious.
AllowedArgvMismatchPatterns	List of known legitimate processes where argv[0] mismatch is expected due to application logic or packaging quirks.
ParentExecutableTrustList	Trusted parent binaries allowed to spawn processes with altered command-line names.
