Behavioral Detection of Process Injection Across Platforms, Detection Strategy DET0508

Archived: 2026-04-05 15:26:14 UTC

AN1399

Detects process injection by correlating memory manipulation API calls (e.g., VirtualAllocEx, WriteProcessMemory), suspicious thread creation (e.g., CreateRemoteThread), and unusual DLL loads within another process's context.

Log Sources

Mutable Elements

Field	Description
AccessMask	Specific access rights used during process handle acquisition, e.g., PROCESS_VM_WRITE
TimeWindow	Time correlation window between API calls and thread creation events
InjectedProcessList	Known high-value targets often abused for injection (e.g., lsass.exe, explorer.exe)

AN1400

Detects ptrace- or memfd-based process injection through audit logs capturing system calls (e.g., ptrace, mmap) targeting running processes along with suspicious file descriptors or memory writes.

Log Sources

Mutable Elements

Field	Description
TargetPIDThreshold	Limit to sensitive or unexpected processes being targeted (e.g., sshd, init)
TimeWindow	Correlate mmap or writev usage to process access within a short timeframe

AN1401

Detects memory-based injection by monitoring `task_for_pid`, `mach_vm_write`, and dylib injection patterns through `DYLD_INSERT_LIBRARIES` or manual memory mapping.

Log Sources

Mutable Elements

Field	Description
TargetProcessSignature	Expected signing identity or origin of process being injected
MachSyscallContext	Observed syscall combinations (e.g., task_for_pid followed by vm_write)
