Module Load, Data Component DC0016

Archived: 2026-04-05 16:00:24 UTC

auditd:file-events open of suspicious .so from non-standard paths auditd:MMAP load: Loading of libzip.so, libz.so, or libbz2.so by processes not normally associated with archiving auditd:SYSCALL openat/read/mmap: Open/mmap .so files from non-standard paths auditd:SYSCALL LD_PRELOAD Logging auditd:SYSCALL mmap auditd:SYSCALL dmesg auditd:SYSCALL module load or memory map path esxi:vmkernel unexpected module load esxi:vmkernel module load ETW:LoadImage provider: ETW LoadImage events for images from user-writable/UNC paths etw:Microsoft-Windows-Kernel-ImageLoad provider: Unsigned/user-writable image loads into msbuild.exe linux:osquery select: Open files path LIKE '/tmp/%.so' OR '/dev/shm/%.so' linux:osquery Dynamic Linking State linux:osquery Process linked with libcrypto.so making external connections linux:osquery Processes linked with libssl/libcrypto performing network activity linux:syslog kmod linux:Sysmon EventCode=7 m365:unified Non-standard Office startup component detected (e.g., unexpected DLL path) macos:endpointsecurity ES_EVENT_TYPE_NOTIFY_KEXTLOAD macos:osquery select: path LIKE '%/Library/%/*.dylib' OR '/tmp/*.dylib' macos:syslog DYLD_INSERT_LIBRARIES anomalies macos:unifiedlog dyld/unified log entries indicating image load from non-system paths macos:unifiedlog dynamic loading of sleep-related functions or sandbox detection libraries macos:unifiedlog DYLD event subsystem macos:unifiedlog process execution events with dylib load activity macos:unifiedlog Process memory maps new dylib (dylib_load event) macos:unifiedlog Dylib loaded from abnormal location macos:unifiedlog Loading of libz.dylib, libarchive.dylib by non-standard applications macos:unifiedlog suspicious dlopen/dlsym usage in non-development processes macos:unifiedlog delay/sleep library usage in user context macos:unifiedlog subsystem=com.apple.kextd macos:unifiedlog loading of unexpected dylibs compared to historical baselines macos:unifiedlog launch and dylib load Module None snmp:status Status change in cryptographic hardware modules (enabled -> disabled) WinEventLog:Application CLR Assembly creation, loading, or modification logs via MSSQL CLR integration WinEventLog:Security EventCode=3033 WinEventLog:Security EventCode=3063 WinEventLog:Sysmon EventCode=7
