Process Metadata, Data Component DC0034

Archived: 2026-04-05 17:55:08 UTC

auditd:SYSCALL execve call for sudo where euid != uid auditd:SYSCALL Use of fork/exec with DISPLAY unset or redirected auditd:SYSCALL execve, prctl, or ptrace activity affecting process memory or command-line arguments auditd:SYSCALL execve with UID ≠ EUID auditd:SYSCALL execve with escalated privileges AWS:CloudTrail cross-account or unexpected assume role containerd:events Docker or containerd image pulls and process executions EDR:hunting Correlation of signer info, parent-child lineage, rare invocation context (user host role), and API surfaces (CreateProcess*, LoadLibrary*) EDR:Telemetry Process lineage and API usage enrichment (GetSystemTime, GetTimeZoneInformation, NtQuerySystemTime) esxi:auth user session esxi:hostd /var/log/hostd.log API calls reading/altering time/ntp settings etw:Microsoft-Windows-ClickOnce provider: Event Tracing for Windows (ETW) events associated with ClickOnce deployment (dfsvc.exe activity) etw:Microsoft-Windows-Kernel-Process process_start: EventHeader.ProcessId true parent vs reported PPID mismatch linux:osquery Cross-reference argv[0] with actual executable path and parent process metadata linux:osquery select: path LIKE '/dev/video%' linux:osquery state=attached/debugged linux:osquery process metadata mismatch between /proc and runtime attributes linux:osquery process environment variables containing LD_PRELOAD linux:syslog sudo or service accounts invoking loaders with suspicious env vars linux:syslog Kernel or daemon warnings of downgraded TLS or cryptographic settings macos:endpointsecurity ES_EVENT_TYPE_NOTIFY_EXEC, ES_EVENT_TYPE_NOTIFY_MMAP macos:osquery Process Context macos:osquery Process Execution + Hash macos:unifiedlog subsystem=com.apple.process macos:unifiedlog subsystem=com.apple.TCC macos:unifiedlog exec of binary with setuid/setgid and EUID != UID macos:unifiedlog process macos:unifiedlog Code Execution & Entitlement Access macos:unifiedlog Process opening SSH_AUTH_SOCK or /tmp/ssh-* socket not owned by same UID macos:unifiedlog code signature/memory protection macos:unifiedlog log collect from launchd and process start macos:unifiedlog Modifications or writes to EFI system partition for downgraded bootloaders macos:unifiedlog non-shell process tree accessing bash history networkdevice:syslog Admin activity Process None WinEventLog:AppLocker AppLocker audit/blocks showing developer utilities executing scripts/binaries outside policy WinEventLog:Microsoft-Windows-CodeIntegrity/Operational CodeIntegrity/WDAC events indicating unsigned/invalid DLL loads WinEventLog:Microsoft-Windows-CodeIntegrity/Operational Unsigned/invalid signature modules or images loaded by msbuild.exe or its children WinEventLog:Microsoft-Windows-CodeIntegrity/Operational Unsigned or untrusted modules loaded during JamPlus.exe runtime WinEventLog:Microsoft-Windows-DeviceGuard/Operational WDAC policy audit/block affecting msbuild.exe spawned payloads WinEventLog:Microsoft-Windows-Security-Mitigations/KernelMode ETW telemetry indicating ClickOnce deployment (dfsvc.exe) launching payloads WinEventLog:Microsoft-Windows-SmartAppControl/Operational Smart App Control decisions (audit/block) for msbuild.exe-launched executables WinEventLog:Microsoft-Windows-Windows Camera Frame Server/Operational Process session start/stop events for camera pipeline by unexpected executables WinEventLog:PowerShell EventCode=400, 403