OS API Execution, Data Component DC0021

Archived: 2026-04-05 18:06:22 UTC

auditd:MMAP memory region with RWX permissions allocated auditd:SYSCALL ptrace, ioctl auditd:SYSCALL Rules capturing clock_gettime, time, gettimeofday syscalls when enabled auditd:SYSCALL openat/read/ioctl: openat/read/ioctl on /dev/video* by uncommon user/process auditd:SYSCALL mmap, ptrace, process_vm_writev or direct memory ops auditd:SYSCALL unshare, mount, keyctl, setns syscalls executed by containerized processes auditd:SYSCALL send, recv, write: Abnormal interception or alteration of transmitted data auditd:SYSCALL sudo or pkexec invocation auditd:SYSCALL mount system call with bind or remap flags auditd:SYSCALL fork/clone/daemon syscall tracing auditd:SYSCALL ptrace, mmap, mprotect, open, dlopen auditd:SYSCALL ptrace, mmap, process_vm_writev auditd:SYSCALL execve of dd or sed targeting /proc/*/mem AWS:CloudTrail GetMetadata, DescribeInstanceIdentity AWS:CloudTrail Describe* or List* API calls AWS:CloudTrail Decrypt EDR:file SetFileTime EDR:memory Behavioral API telemetry (GetProcAddress, LoadLibrary, VirtualAlloc) EDR:memory API usage MFCreateDeviceSource, IAMStreamConfig, ICaptureGraphBuilder2, DirectShow filter graph creation from uncommon callers EDR:memory Objective-C/Swift calls to AVCaptureDevice/AVCaptureSession by non-whitelisted processes EDR:memory VirtualAlloc/VirtualProtect/MapViewOfFile indicators via stack/heap activity and ImageLoad EDR:memory MemoryWriteToExecutable esxi:hostd Remote access API calls and file uploads ETW Calls to GetUserDefaultUILanguage, GetSystemDefaultUILanguage, GetKeyboardLayoutList etw:Microsoft-Windows-Directory-Services-SAM api_call: Calls to DsAddSidHistory or related RPC operations etw:Microsoft-Windows-DotNETRuntime AssemblyLoad/ModuleLoad (Loader keyword) from Microsoft-Windows-DotNETRuntime etw:Microsoft-Windows-Kernel-Base GetLocaleInfoW, GetTimeZoneInformation API calls etw:Microsoft-Windows-Kernel-File ZwSetEaFile or ZwQueryEaFile function calls etw:Microsoft-Windows-Kernel-Process API tracing / stack tracing via ETW or telemetry-based EDR etw:Microsoft-Windows-Kernel-Process APCQueueOperations etw:Microsoft-Windows-Kernel-Process High-frequency or suspicious sequence of QueryPerformanceCounter/GetTickCount API calls from a non-standard process lineage etw:Microsoft-Windows-Kernel-Process API Calls etw:Microsoft-Windows-Kernel-Process NtQueryInformationProcess etw:Microsoft-Windows-Kernel-Process NtUnmapViewOfSection, VirtualAllocEx, WriteProcessMemory, SetThreadContext, ResumeThread etw:Microsoft-Windows-Kernel-Process api_call: UpdateProcThreadAttribute (PROC_THREAD_ATTRIBUTE_PARENT_PROCESS) and CreateProcess* with EXTENDED_STARTUPINFO_PRESENT / StartupInfoEx etw:Microsoft-Windows-Kernel-Process API calls etw:Microsoft-Windows-Kernel-Process CreateTransaction, CreateFileTransacted, RollbackTransaction, NtCreateProcessEx, NtCreateThreadEx etw:Microsoft-Windows-Kernel-Process WriteProcessMemory: WriteProcessMemory targeting regions containing KernelCallbackTable addresses etw:Microsoft-Windows-RPC rpc_call: srvsvc.NetShareEnum / NetShareEnumAll from non-admin or unusual processes etw:Microsoft-Windows-Security-Auditing api_call: LogonUser(A|W), LsaLogonUser, SetThreadToken, ImpersonateLoggedOnUser etw:Microsoft-Windows-Win32k SetWindowLong, SetClassLong, NtUserMessageCall, SendNotifyMessage, PostMessage etw:Microsoft-Windows-Win32k SendMessage, PostMessage, LVM_* ETW:ProcThread api_call: CreateProcessWithTokenW, CreateProcessAsUserW ETW:Token token_analysis: API calls such as DuplicateTokenEx or ImpersonateLoggedOnUser ETW:Token

api_call: DuplicateTokenEx, ImpersonateLoggedOnUser, SetThreadToken fs:fsusage Detached process execution with no associated parent linux:syslog Execution of modified binaries or abnormal library load sequences macos:osquery open, execve: Unexpected processes accessing or modifying critical files macos:osquery CALCULATE: Integrity validation of transmitted data via hash checks macos:unifiedlog None macos:unifiedlog Invocation of SMLoginItemSetEnabled by non-system or recently installed application macos:unifiedlog flock|NSDistributedLock|FileHandle.*lockForWriting macos:unifiedlog application logs referencing NSTimer, sleep, or launchd delays macos:unifiedlog Access decisions to kTCCServiceCamera for unexpected binaries macos:unifiedlog audio APIs macos:unifiedlog com.apple.securityd, com.apple.tccd macos:unifiedlog authorization execute privilege requests macos:unifiedlog ptrace: Processes invoking ptrace with PTRACE_TRACEME flag macos:unifiedlog Calls to AuthorizationExecuteWithPrivileges() observed via Apple System Logger or security_auditing tools macos:unifiedlog access or unlock attempt to keychain database macos:unifiedlog Execution of input detection APIs (e.g., CGEventSourceKeyState) networkdevice:syslog aaa privilege_exec networkdevice:syslog Unexpected reload, crashinfo, or boot message not tied to scheduled maintenance NSM:Flow smb_command: TreeConnectAndX to *\IPC$ / srvsvc or Trans2/NT_CREATE for listing shares Process None snmp:trap management queries WinEventLog:Application API call to AddMonitor invoked by non-installer process WinEventLog:Microsoft-Windows-COM/Operational CLSID activation events where ProcessName=mmc.exe and CLSID not in allowed baseline WinEventLog:Security EventCode=4663, 4670, 4656
