Script Execution, Data Component DC0029

Archived: 2026-04-05 12:55:55 UTC

Name	Channel
ApplicationLogs:SQL	Stored procedure creation or modification with shell invocation (e.g., system(), exec())
auditd:PROCTITLE	scripting loop invoking sleep/ping
azure:activity	Microsoft.Compute/virtualMachines/runCommand/action: Abnormal initiation of Azure RunCommand jobs or PowerShell/Bash payloads
EDR:AMSI	Malicious inline C#/script blobs embedded in MSBuild projects if intercepted by AMSI-aware loaders (rare but possible via chained LOLBins)
EDR:scriptblock	Process Tree + Script Block Logging
esxi:shell	None
esxi:vmkernel	boot
etw:Microsoft-Antimalware-Scan-Interface	Amsi/Script content + API verdicts during in-memory staging
linux:syslog	/var/log/syslog
linux:syslog	boot logs
m365:defender	ScriptBlockLogging + AMSI
m365:office	VBA auto_open, auto_close, or document_open events
m365:unified	Scripted Activity
macos:osquery	exec: Unexpected execution of osascript or AppleScript targeting sensitive apps
macos:syslog	system.log, asl.log
macos:unifiedlog	log stream --predicate 'eventMessage contains "python"'
macos:unifiedlog	log stream --predicate 'eventMessage contains "wscript" OR "vbs"'
macos:unifiedlog	osascript or AppleScript invocation modifying UI
macos:unifiedlog	log

Name	Channel
macos:unifiedlog	AppleScript creating login item via 'System Events' dictionary
macos:unifiedlog	subsystem=launchservices
macos:unifiedlog	log stream with predicate 'eventMessage CONTAINS "osascript"'
macos:unifiedlog	subsystem=com.apple.Security or com.apple.applescript
macos:unifiedlog	osascript, AppleScript, or Python execution triggered immediately after HID connection
networkdevice:runtime	runtime
Script	None
WinEventLog:Application	Stored procedure creation, modification, or xp_cmdshell invocation via SQL logs or SQL Server auditing
WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106
WinEventLog:PowerShell	Set-ADUser or Set-ADAuthenticationPolicy with MFA attributes disabled
WinEventLog:PowerShell	Scripts with references to XML parsing, AES decryption, or gpprefdecrypt logic
WinEventLog:System	EventCode=1502, 1503
WinEventLog:System	EventCode=4016, 5312
