Service Metadata, Data Component DC0041

Archived: 2026-04-05 18:37:16 UTC

Name	Channel
auditd:CONFIG_CHANGE	delete: Modification of systemd unit files or config for security agents
esxi:hostd	Stop VM or disable service events via vim-cmd
esxi:hostd	registers services with legitimate-sounding names
esxi:hostd	Service events
kubernetes:audit	seccomp or AppArmor profile changes
kubernetes:audit	kubectl delete or patch of security pods/admission controllers
linux:osquery	scheduled/real-time
linux:syslog	service stopped messages
linux:syslog	auditd service stopped or disabled
linux:syslog	Service restart with modified executable path
macos:osquery	launchd
macos:unifiedlog	launchctl disable or bootout calls
macos:unifiedlog	subsystem=com.apple.launchservices
macos:unifiedlog	Observed loading of new LaunchAgent or LaunchDaemon plist
macos:unifiedlog	Modification of system configuration profiles affecting security tools
networkdevice:config	write: Startup configuration changes disabling security checks
Service	None
WinEventLog:Sysmon	EventCode=4
WinEventLog:System	EventCode=7035
WinEventLog:System	Service stopped or RecoveryDisabled set via REAgentC
WinEventLog:WinRM	EventCode=6

Source: https://attack.mitre.org/datacomponents/DC0041