File Deletion, Data Component DC0040

Archived: 2026-04-05 15:47:59 UTC

Name	Channel
auditd:CONFIG_CHANGE	/etc/fstab, /etc/systemd/*
auditd:SYSCALL	unlink/unlinkat on service binaries or data targets
auditd:SYSCALL	file deletion
auditd:SYSCALL	PATH
auditd:SYSCALL	unlink, unlinkat, openat, write
auditd:SYSCALL	unlink, unlinkat, rmdir
auditd:SYSCALL	unlink, rename, open
auditd:SYSCALL	unlink/unlinkat
docker:daemon	container file operations
esxi:hostd	delete action
esxi:hostd	rm, clearlogs, logrotate
esxi:hostd	Datastore file operations
esxi:shell	shell history
esxi:shell	/var/log/shell.log
File	None
fs:fsusage	unlink, fs_delete
linux:Sysmon	EventCode=23
macos:osquery	file_events
macos:osquery	CREATE, DELETE, WRITE: Stored data manipulation attempts by unauthorized processes
macos:unifiedlog	exec rm -rf|dd if=/dev|srm|file unlink
WinEventLog:Microsoft-Windows-Backup	Windows Backup Catalog deletion or catalog corruption

Name	Channel
WinEventLog:Sysmon	EventCode=23

Source: https://attack.mitre.org/datacomponents/DC0040