Behavioral Detection of Log File Clearing on Linux and macOS, Detection Strategy DET0520

Archived: 2026-04-05 14:20:42 UTC

AN1438

Detects log-clearing behavior by correlating suspicious command execution targeting log files under /var/log/, anomalous deletions or truncations of system logs, and unusual child processes (e.g., shell pipelines or redirections).

Log Sources

Mutable Elements

Field	Description
TimeWindow	The time window used to correlate log file interaction and suspicious command execution.
LogFilePathPattern	Regex pattern used to match monitored log file paths (e.g., /var/log/auth.log).
UserContext	User or group (e.g., root) that should trigger higher severity detection.

AN1439

Detects adversary clearing log files on macOS by correlating calls to shell utilities (e.g., echo >, rm, truncate) targeting files in /var/log/ with unusual context (non-administrative users or abnormal process lineage).

Log Sources

Mutable Elements

Field	Description
TimeWindow	Duration in which process activity and file I/O should be temporally linked.
LogFilePathPattern	Tunable path filter for macOS logs such as /var/log/system.log or /var/log/asl.log.
UserContext	Detects higher risk when log deletion is performed by unusual users (e.g., interactive vs. system users).

Source: https://attack.mitre.org/detectionstrategies/DET0520#AN1438