Detection Strategy for Log Enumeration, Detection Strategy DET0255

Archived: 2026-04-05 16:36:09 UTC

AN0705

Monitor for use of native utilities such as wevtutil.exe or PowerShell cmdlets (Get-WinEvent, Get-EventLog) to enumerate or export logs. Unusual access to security or system event channels, especially by non-administrative users or processes, should be correlated with subsequent file export or network transfer activity.

Log Sources

Mutable Elements

Field	Description
WhitelistedAdminTools	Expected log management scripts executed by administrators should be excluded from alerts.
TimeWindow	Correlate enumeration attempts with file export or network transfer within a defined timeframe.

AN0706

Monitor for suspicious use of commands such as cat, less, grep, or journalctl accessing /var/log/ files. Abnormal enumeration of authentication logs (auth.log, secure) or bulk access to multiple logs in short time windows should be flagged.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of cat, less, grep, journalctl targeting log directories (/var/log/)
File Access (DC0055)	auditd:PATH	open: Access to sensitive log files (/var/log/auth.log, /var/log/secure, /var/log/syslog)

Mutable Elements

Field	Description
AdminMaintenanceScripts	Filter routine scripts used for log rotation or troubleshooting.

AN0707

Detect abnormal access to unified logs via log show or fs_usage targeting system log files. Monitor for execution of shell utilities (cat, grep) against /var/log/system.log and for plist modifications enabling verbose logging.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	macos:unifiedlog	Execution of log show, fs_usage, or cat targeting system.log
File Access (DC0055)	macos:unifiedlog	open: Access to /var/log/system.log or related security event logs

Mutable Elements

Field	Description
DebugToolsContext	Allowlist developers or administrators expected to review logs during debugging.

AN0708

Monitor for cloud API calls that export or collect guest or system logs. Abnormal use of Azure VM Agent's CollectGuestLogs.exe or AWS CloudWatch GetLogEvents across multiple instances should be correlated with lateral movement or data staging.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	AWS:CloudTrail	GetLogEvents: High frequency log exports from CloudWatch or equivalent services
File Access (DC0055)	azure:activity	CollectGuestLogs: Unexpected collection of guest logs by Azure VM Agent outside normal maintenance windows

Mutable Elements

Field	Description
LogExportThreshold	Define thresholds for volume/frequency of log export requests considered suspicious.

AN0709

Monitor ESXi shell or API access to host logs under /var/log/. Abnormal enumeration of vmkernel.log, hostd.log, or vpxa.log by unauthorized accounts should be flagged.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	esxi:shell	Execution of cat, tail, grep targeting /var/log/vmkernel.log or /var/log/hostd.log
File Access (DC0055)	esxi:hostd	read: Access to sensitive log files by non-admin users

Mutable Elements

Field	Description
AdminSessions	Correlate with legitimate administrator access sessions to reduce noise.

Source: https://attack.mitre.org/detectionstrategies/DET0255#AN0708