Detection Strategy for Impair Defenses Indicator Blocking, Detection Strategy DET0239

Archived: 2026-04-05 13:05:53 UTC

AN0667

Correlates registry modifications to EventLog or WMI Autologger keys, suspicious use of Set-EtwTraceProvider, and Sysmon configuration changes. Defender sees interruption or redirection of ETW and log event collection.

Log Sources

Mutable Elements

Field	Description
MonitoredETWProviders	List of ETW providers to baseline and monitor for unexpected removal.
AuthorizedConfigChanges	Whitelist of expected admin actions modifying Sysmon or ETW configurations.

AN0668

Detects disabling or reconfiguration of syslog or rsyslog services. Monitors sudden stops in logging daemons and suspicious execution of kill or service stop commands targeting syslog processes.

Log Sources

Mutable Elements

Field	Description
SyslogServiceName	Service name for syslog daemon, which can differ across distributions.

AN0669

Detection of tampering with Apple's Unified Logging framework or modification of system log forwarding settings. Defender observes execution of logd-related commands or defaults write to logging preferences.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	macos:unifiedlog	defaults write com.apple.system.logging or logd manipulation

Mutable Elements

Field	Description
AllowedLogConfigs	Baseline of approved logging preference modifications to reduce noise.

AN0670

Detection of syslog configuration tampering using esxcli system syslog config set or reload. Defender correlates command execution with absence of syslog forwarding activity.

Log Sources

Mutable Elements

Field	Description
SyslogServerBaseline	Expected syslog destination servers for ESXi hosts.
