Behavioral Detection of Network History and Configuration Tampering, Detection Strategy DET0049

Archived: 2026-04-05 18:01:23 UTC

AN0133

Detects attempts to clear RDP/network history and modify network configuration artifacts through command execution, registry key deletion, firewall rule changes, and suspicious file deletions (e.g., Default.rdp, registry edits to Terminal Server Client keys).

Log Sources

Mutable Elements

Field	Description
TargetPathRegex	Filter file/registry paths like *\Terminal Server Client* or *Default.rdp*
TimeWindow	Correlate command/registry edits within close proximity to suspicious connection activity
UserContext	Detect cleanup behavior from non-interactive or SYSTEM accounts

AN0134

Detects deletion or overwriting of logs/configs that store SSH or proxy activity, such as /var/log/auth.log or custom .bash_history clearing tied to SSH sessions or firewall rule changes.

Log Sources

Mutable Elements

Field	Description
CommandMatchPattern	Commands like `> /var/log/auth.log`, `rm ~/.bash_history`, `iptables -F`
LogPathFilter	Focus on /var/log/auth.log, /etc/ssh/, ~/.bash_history

AN0135

Detects removal of Remote Login or Screen Sharing logs in Unified Logging, deletion of `com.apple.UTun`, or suspicious Terminal use of `rm`, `sudo pfctl -F all` to clear network state/config history.

Log Sources

Mutable Elements

Field	Description
FilenameMatch	e.g., *com.apple.UTun*, *RemoteManagement* log files
TimeDeltaFromLogin	Correlate deletion with recent SSH or GUI remote login session

AN0136

Detects firewall rule modifications or reset of logs/connection tables (e.g., `clear logging`, `erase startup-config`, `write erase`) following remote access activity on routers, switches, or VPN appliances.

Log Sources

Mutable Elements

Field	Description
CommandPattern	e.g., `clear logging`, `no logging buffered`, `no ip domain-lookup`
DeviceTypeFilter	Switches vs VPN vs routers
