Detection Strategy for Impair Defenses via Impair Command History Logging across OS platforms., Detection Strategy DET0563

Archived: 2026-04-05 18:43:47 UTC

AN1555

Detection of environment variable tampering (HISTFILE, HISTCONTROL, HISTFILESIZE) and absence of expected bash history writes. Correlation of unset or zeroed history variables with active shell sessions is indicative of adversarial evasion.

Log Sources

Mutable Elements

Field	Description
MonitoredUsers	Specific accounts or groups where history logging must always be enforced.
TimeWindow	Correlation period to detect unset/export of history variables during active shells.

AN1556

Detection of bash/zsh history suppression via HISTFILE/HISTCONTROL manipulation and absence of ~/.bash_history updates. Observing environment variable changes tied to terminal processes is a strong indicator.

Log Sources

Mutable Elements

Field	Description
ShellProfiles	Different shells (bash, zsh, fish) may require customized monitoring for history tampering.

AN1557

Detection of PowerShell history suppression using Set-PSReadLineOption with SaveNothing or altered HistorySavePath. Correlating these options with PowerShell usage highlights adversarial evasion attempts.

Log Sources

Mutable Elements

Field	Description
AllowedPaths	List of acceptable PowerShell history save paths for baseline comparison.

AN1558

Detection of unset HISTFILE or modified history variables in ESXi shell sessions. Correlation of suspicious shell sessions with no recorded commands despite active usage.

Log Sources

Mutable Elements

Field	Description
AdminSessions	Differentiate root/admin shell sessions from adversarial misuse of ESXi shell.

AN1559

Detection of CLI commands that disable history logging such as 'no logging'. Anomalous lack of new commands in session logs while activity persists is a strong signal.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:cli	Commands like 'no logging' or equivalents that disable session history

Mutable Elements

Field	Description
DeviceVendors	Command syntax differs across Cisco, Juniper, Fortinet, etc., requiring vendor-aware tuning.
