Behavioral Detection of Command History Clearing, Detection Strategy DET0165

Archived: 2026-04-05 14:01:33 UTC

AN0467

Detects adversary behavior clearing command history via `history -c`, deletion or modification of ~/.bash_history, or manipulation of the HISTFILE environment variable post-login.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Detect shell history clearing shortly after login or command execution.
UserContext	Elevated shell sessions (e.g., root or sudo) without command history may be more suspicious.
HistoryFilePath	Bash/Zsh history file paths (e.g., ~/.bash_history, ~/.zsh_history).

AN0468

Detects adversary clearing shell history using `history -c` or deleting/altering ~/.zsh_history or ~/.bash_history. Focus on sessions with missing or wiped history.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Duration after terminal usage where deletion or modification is considered suspicious.
UserContext	Flag unexpected user activity, especially from users who normally don’t use terminal.
HistoryFilePath	Zsh or Bash history files under the user's home directory.

AN0469

Detects PowerShell `Clear-History` invocation or deletion of `ConsoleHost_history.txt` to erase past PowerShell session history.

Log Sources

Mutable Elements

Field	Description
HistoryFilePath	Path to PSReadLine file, typically in APPDATA.
UserContext	User account or role performing deletion (e.g., low-priv user deleting history).
CommandPattern	Support detection of `Clear-History` and variations.

AN0470

Detects modification or truncation of `/var/log/shell.log` used to persist ESXi shell command history. Especially suspicious shortly after login or config changes.

Log Sources

Mutable Elements

Field	Description
LogFilePath	Path to shell command history on ESXi.
TimeWindow	Time range post-login or privileged escalation.

AN0471

Detects use of `clear history` or `clear logging` commands on network device CLI to remove past activity logs.

Log Sources

Mutable Elements

Field	Description
CommandPattern	Support detection of known variants: 'clear history', 'clear logging', etc.
DeviceType	Router, switch, firewall—may have different CLI behaviors.
