# Threat Hunter Playbook

**Playbook Title:** "Windows Event Logs Cleared via PowerShell (Clear-EventLog)"

**Date Created:** 2022-07-10

**Hypothesis:** Attackers will try to cover their tracks using PowerShell

**Mitre Tactic:** T1070 "Indicator Removal on Host"

**Mitre Sub Technique:** T1070.001 "Indicator Removal on Host: Clear Windows Event Logs" (via PowerShell Clear-EventLog)

**Simulation Details (if any):** None

**Proposed Search Query:** `index=sysmon event.code=1 process.command_line="*Clear-EventLog*"`

**Hunter Limitations/Observation Notes:** The Proposed Search Query produced evidence that the PowerShell cmdlet "Clear-EventLog" was used, but the results were broad. The search query was improved to display the relevant data in a readable format (see Proposed Detection Query).

**Hunt Findings:** Use of the PowerShell cmdlet 'Clear-EventLog' should be monitored for any suspicious behavior, and so the Proposed Detection Query should be made into a detection.

**Proposed Detection Title:** "ALERT: PowerShell 'Clear-EventLog' executed"

**Proposed Detection Query:**

```
index=sysmon event.code=1 process.command_line="*Clear-EventLog*" | rename process.command_line as command | table _time host.name event.code user.name command | sort _time
```