Threat Hunter Playbook

Playbook Title: "Windows Event Logs Cleared (via Event Viewer GUI)"
Date Created: 2022-07-10

Hypothesis: Attackers will try to cover their tracks using the Event Viewer GUI

Mitre Tactic: T1070 "Indicator Removal on Host"

Mitre Sub Technique: T1070.001 "Indicator Removal on Host: Clear Windows Event Logs" (via Event Viewer GUI)

Simulation Details (if any): None

Proposed Search Query: `index=wineventlogs event.code=1102`

Hunter Limitations/Observation Notes: The Proposed Search Query did find evidence of Windows Event logs getting cleared, but the results were broad. The search query was improved to display the relevant data in a readable format (see Proposed Detection Query). It's important to note that the search results did not specifically show if the Windows Event Logs were cleared via the Event Viewer GUI, and so it would be prudent to test this in a simulation to verify that Windows Security Event ID 1102 would still be triggered (no matter what method an attacker used: GUI, Command, or PowerShell).

Hunt Findings: Windows Event 1102 is wonderful for detecting when Windows Event logs are cleared, and the query developed below should be made into a detection.

Proposed Detection Title: "ALERT: Windows Event 1102 - The audit log was cleared"

Proposed Detection Query:

```
index=wineventlogs event.code=1102 | rename winlog.user_data.SubjectUserName as user | table _time host.name event.code winlog.task user | sort _time
```