# Part 1 – Review Malicious Logs

Check the following logs under “events”:

1. Clear event log – shows data when a process is deleting the entire log traces.
   1. What is malicious about this?
   2. Should we alert in all cases where the event log is cleared? Is it always suspicious? Which benign scenarios can be?
2. CredMan – try to recognize the malicious behavior from the traces.
   1. What is the malicious activity taking place?
   2. How can we detect it using this event? How can we distinguish between normal behavior and unusual behavior?
3. Wmi-persistance – find an event that indicates on malicious activity.
   1. How did you identify malicious behavior vs. benign behavior? \*hint in white: check the consumer\*
   2. Do you have a suggestion to a detection logic for this API?

# Part 2 – Explore Malicious Scripts

Go the “scripts” directory:

1. Run the credman script “Credman.ps1 -ShoCred -All
2. Try to find the traces this script is creating. You may use the custom view in the event log, called “CredMan”. Make sure to clean it before running the script, and refreshing it after the execution.
3. Open the wmi-persistance script. Try to understand the different steps in the script.
4. Run it and check the traces in the event log. You may use the Wmi-persistance custom view.

# Part 3 – Explore your own script!

1. Go to <https://jpcertcc.github.io/ToolAnalysisResultSheet/>
2. Choose a script to run.
3. Download the script to your machine.
4. We already configured all the traces for you. Run the script and find all the expected telemetry in the event log.

You rock!

