# LAB5

## Scenario

*PurpleHawkS SOC Manager came across compromised system logs, and he wanted Threat Analyst to review the device logs and run detection tool to identify alerts.*

## Compromised System

Log file is added to GitHub - PurpleHawkS-Zircolite_Detection_Windows_Logs.evtx

## Exercise

As a Threat analyst, review logs and run Zircolite detection tool to identify which incidents are matching with current detection.

Requirements:

1. Run Zircolite tool against the log file.
2. Run the Zircolite report template.
3. Write the summary of the incident detected.