

SOC-L2 Lab1

Task 1:

Install [Sysmon](#) on your Windows machine and add [this configuration](#) file to it. After that, perform any action such as executing the **whoami** command or running a process, etc.

Prove your work with **screenshots**.

Task 2

Based on the MITRE ATT&CK® framework, fill these boxes with the correct MITRE technique IDs for the provided attack scenario.

