Wazuh Project beginning 09.28.2023

This project write-up of my work and observations while learning Wazuh. This will continue to be updated.

Wuzah server specs:
Dell Optiplex 3040 i5, 8GB RAM, 256 SSD
OS: Ubuntu 22.04 LTS

Setup the server with default settings. First step was to add another internal user for Wazuh. After that I began to setup agents on 5 systems.

Four systems are running Windows 10 Pro and a fifth was running Windows 11 Pro. I installed Sysmon on one of the four Windows 10 system with default configuration. I did this to see the difference in logs recorded from this one and the others without Sysmon.

Begin going through the interface to see what it can show.

Let it run for a day and then began to look at the basic system benchmarks. The system with Sysmon showed 144 passed, 247 failed. Exported this list as a CSV file. Converted that to an XLSX file to retain column width.

Updated Wireshark and saw new alert messages appear in Wazuh. These were talking about persistence. Reviewed the details of the alerts and showed they were related to my installation of Wireshark.

(updated as of 10-17-2023)