Task.4

I tried to set both version

1- Wazuh-docker-4.5.1, I faced an issue with containers wazuh.manager and wazuh.indexer, which both did not installed, I rested my VM to do the other virsion

2- 2- wazuh-docker-4.9.0, I faced issue with yaml, I attached the file of my work

1. What rule descriptions did you get?

Due to faceing multiple issues in setting up Docker manually, so I followed the below procedure visited the Wazuh Prebuilt Demo Environment documents
- when files are modified or deleted in the monitored folder, wazuh would generate alerts "file integrity monitoring; file added or file deleted"

2. What are the MITRE ATT&CK techniques(include ID) Wazuh reports for these events?

Wazuh maps firm file to MITRE ATT&CK techniques: T1005-Data from Local system when file is added or modifies, it may correspond to data collection, if file deleted is mapped to date.

T1485-Data Destruction: if a file is deleted, this maps to data destruction

3. **What is the reported MITRE technique for deleting files or directories inside monitored directories?** T1485 - Data Destruction: This technique is reported when files or directories are deleted inside monitored directories.

4. **Where, when, and why should these systems be used, and would they be helpful in banking?**
   Wazuh and FIM should be used: in any critical system where sensitive files and data are stored, such as bank servers. Continuously, as part of ongoing security monitoring, because FIM helps detect unauthorized access or tampering with sensitive financial files, which is crucial in protecting banking systems from fraud or breaches.

□