File Integrity Monitoring System

Team member:

Name	ID
Abdelrahman Khaled Abdallah Hamed	2021170914
Abdelrahman Mohamed Yehia Sohsah	2021170916
Ziad Mahmoud Gomaa	2021170911
Mohamed Waleed Soliman	20201701823

Security solution used:

Wazuh open source platform used for threat prevention, detection, and response.

Project idea:

Securing cardholder data files by monitoring and checking for any modification happen to it.

How it is done:

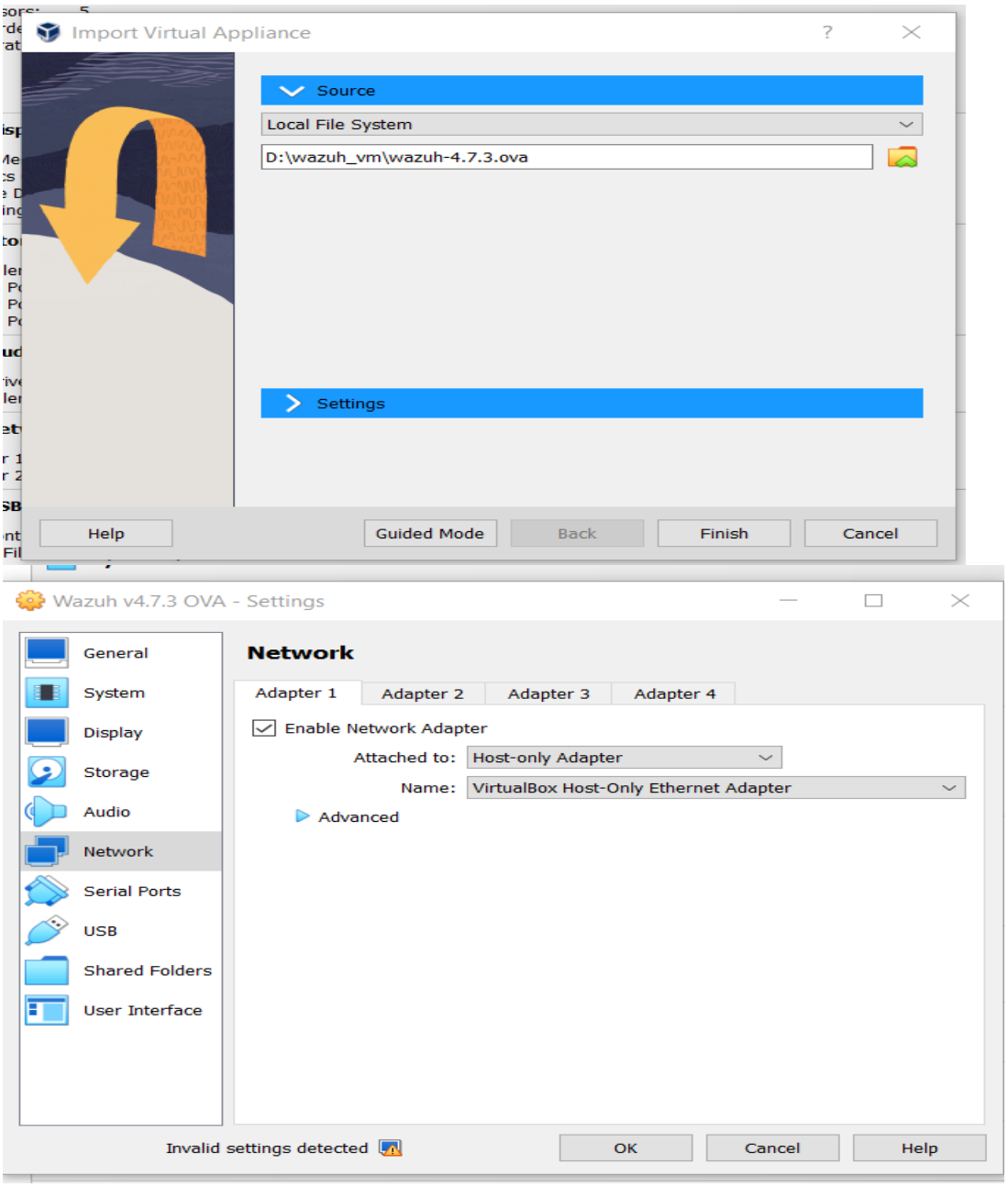
Step 1: installing and configuring wazuh (.ova) machine

Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format
imported to VirtualBox or other OVA compatible virtualization systems. Take into account
runs on 64-bit systems. It does not provide high availability and scalability out of the box
be implemented by using distributed deployment.

Download the virtual appliance (OVA), which contains the following components:

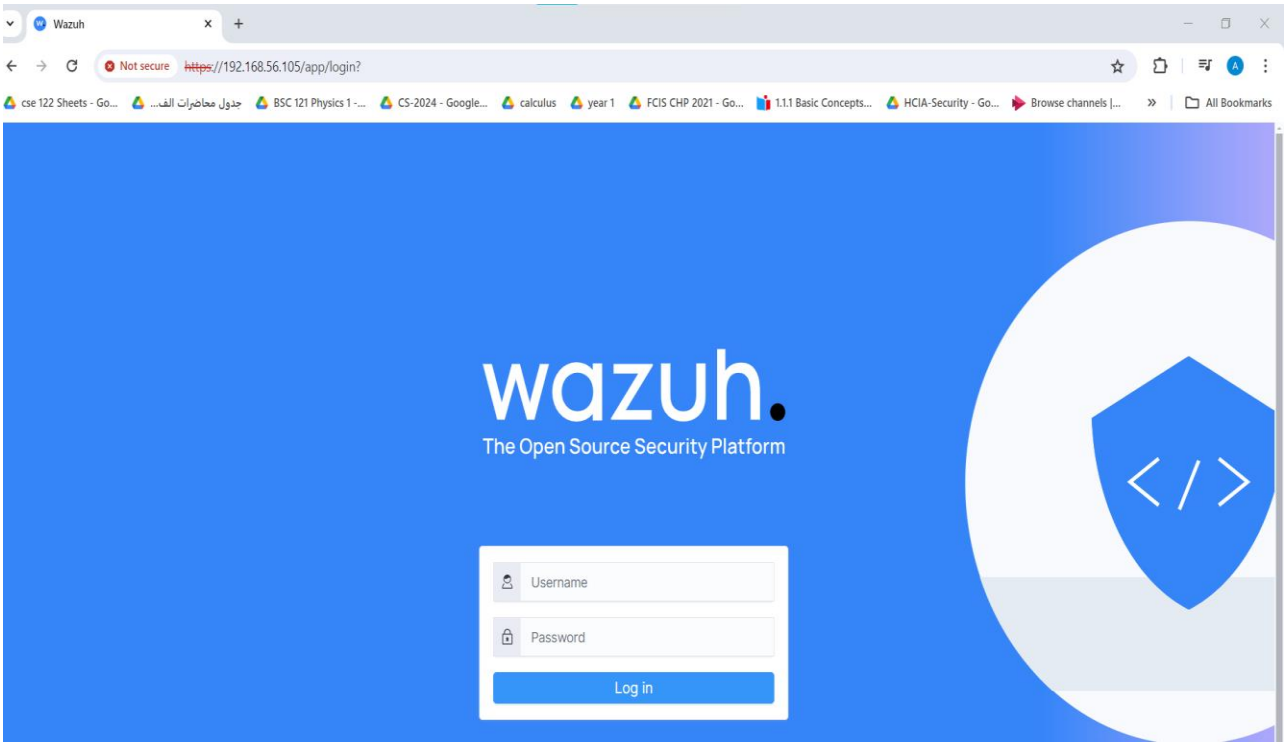
- Amazon Linux 2
- Wazuh manager 4.7.3
- Wazuh indexer 4.7.3
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.7.3

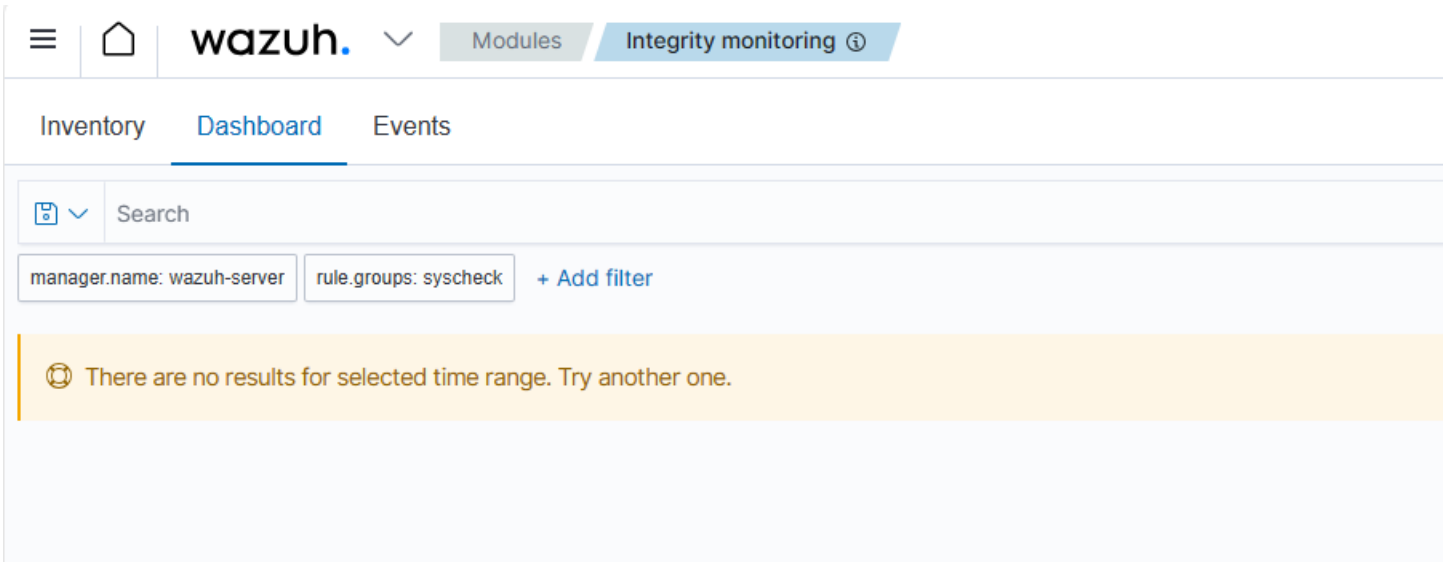


Step 2: connecting to this machine using ssh to be able to run wazuh features easily.

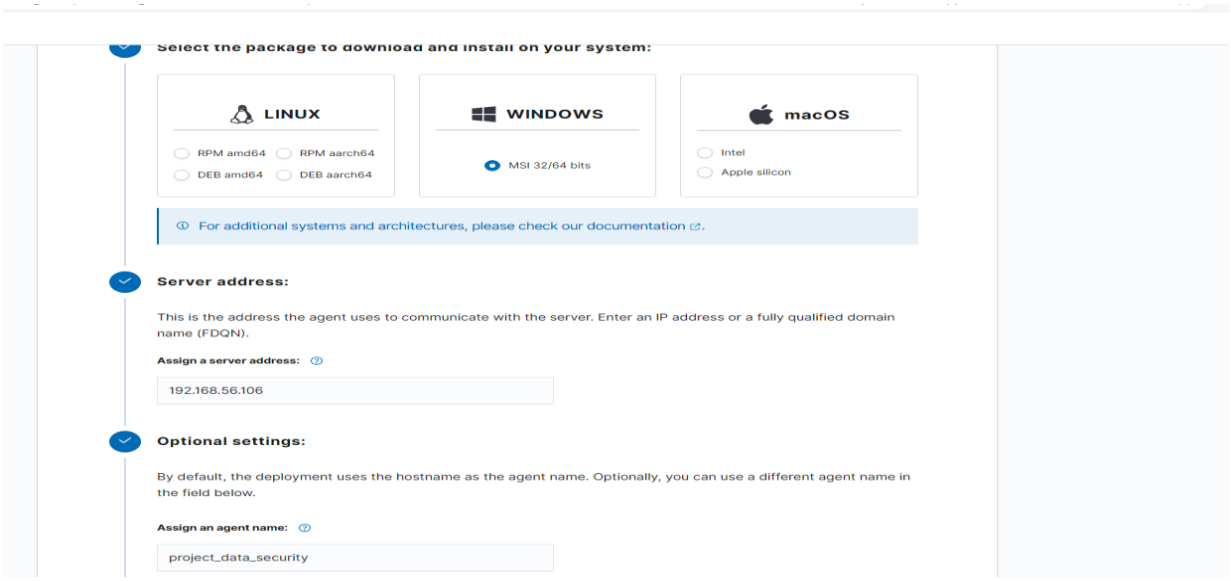
```
C:\Users\Lenovo>ssh wazuh-user@192.168.56.105
The authenticity of host '192.168.56.105 (192.168.56.105)' can't be established.
ECDSA key fingerprint is SHA256:r9eJRrxYuLMuFq1HokQ0msKm028GuaOezl+FA2DJb9U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.105' (ECDSA) to the list of known hosts.
wazuh-user@192.168.56.105's password:
Last login: Wed Apr 24 14:32:29 2024
```

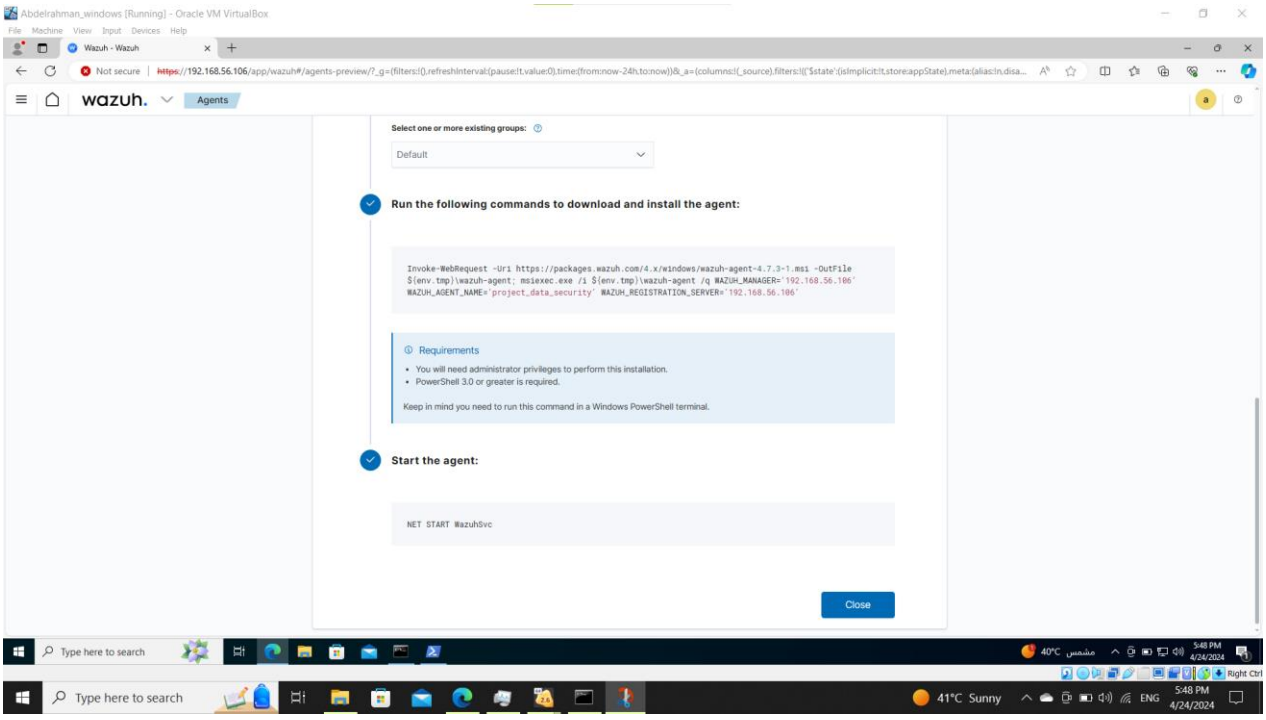
Step 3: Accessing wazuh dashboard and logging into the system

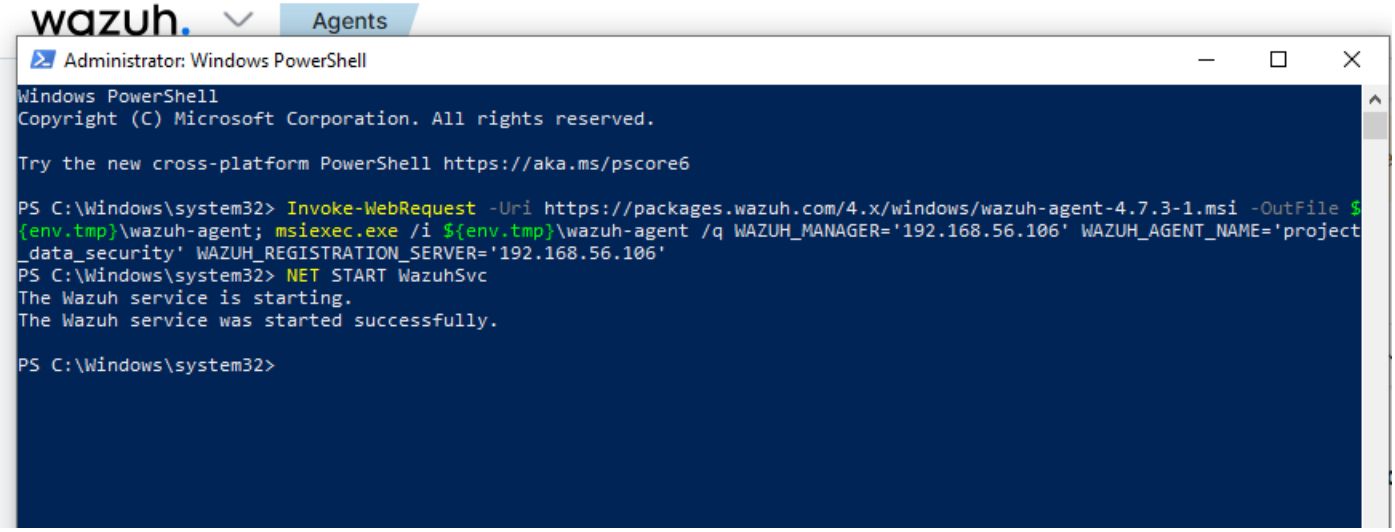


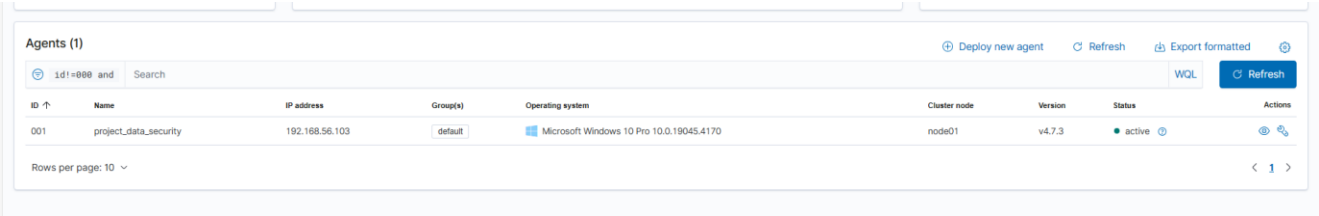


Step 4: Configuring agent for server hosting cardholder data {In this case it is a windows machine }



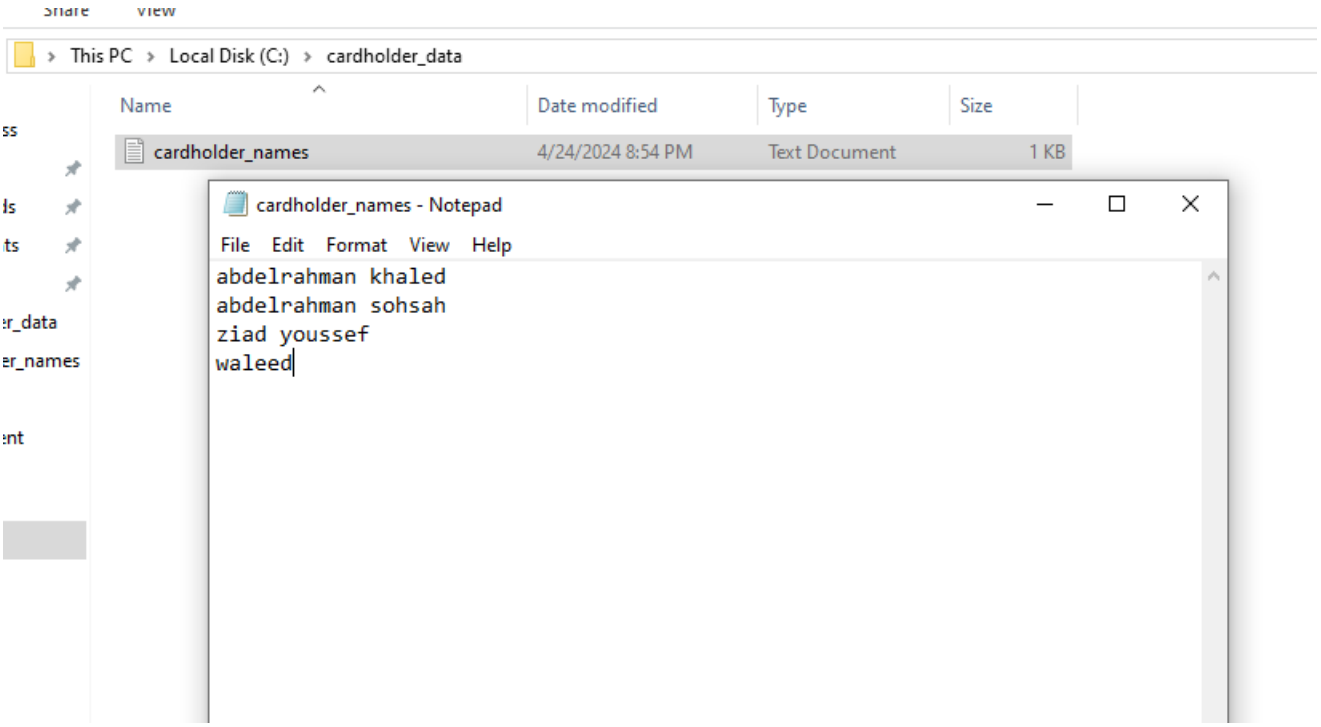




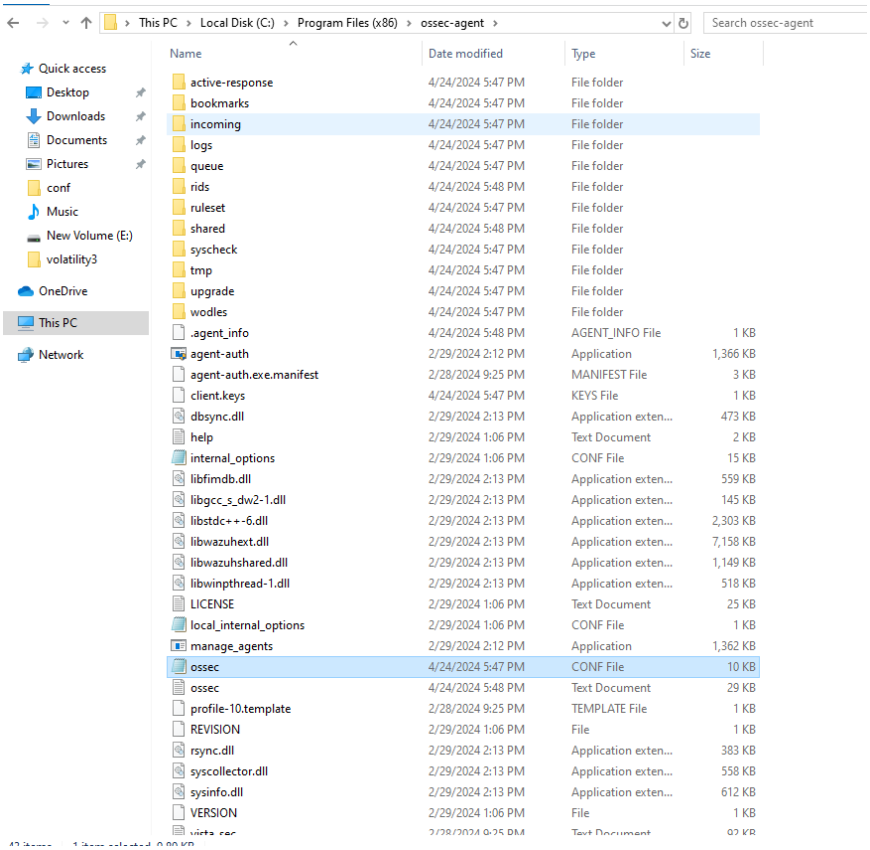


Now we have wazuh server and wazuh agent both running we go to step 5 where we change configurations of agent.

Step 5 : Adding cardholder data file located in c:\Cardholder_data , which includes Cardholder_names text file which include names of cardholders.

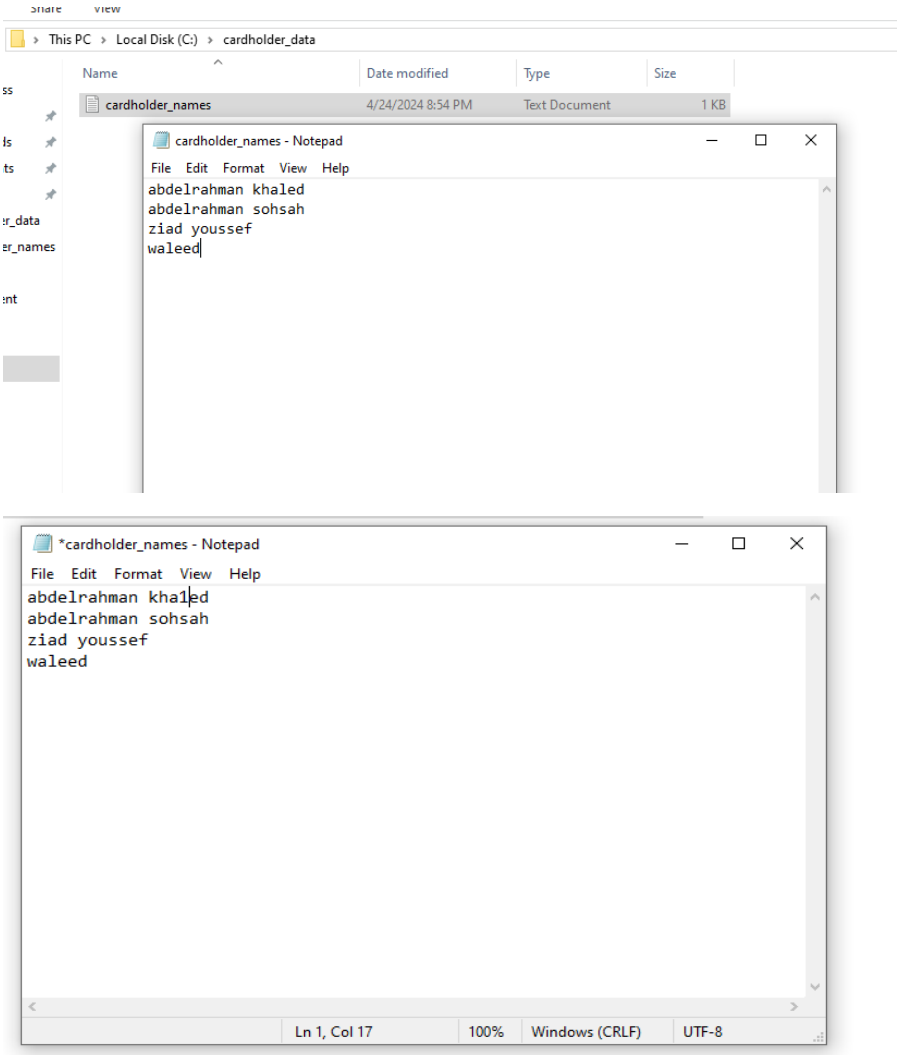


Step 6: Modifying the ossec file {It is the configuration file for wazuh agent } to monitor our file beside registry and binary files every 5 seconds not 12 hours

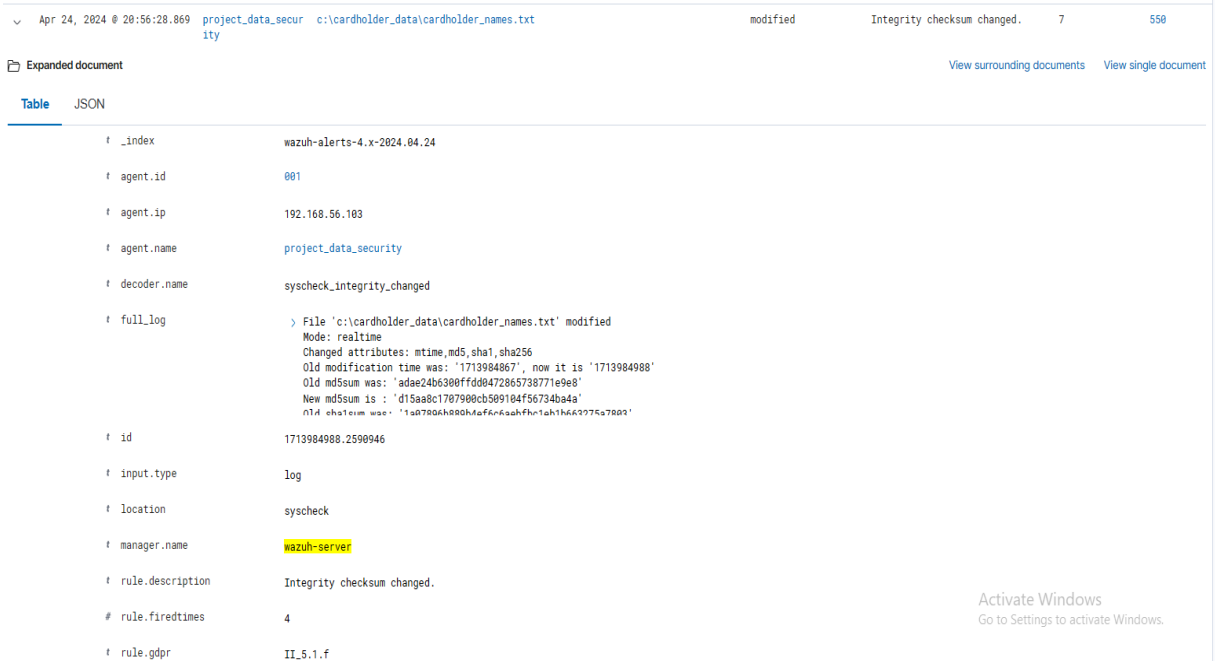



```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>5</frequency>

  <!-- Default files to be monitored. -->

  <directories check_all="yes" report_changes="yes"  realtime="yes">C:\cardholder_data</directories>

  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.ex
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
```

Step 7: Act as a threat actor and modify the file to test detection functionalities {we modify Abdelrahman Khaled to Abdelrahman kha1ed}



Step 8: Opening the dashboard to view any logs



rule.mitre.tactic	Impact
rule.mitre.technique	Stored Data Manipulation
rule.nist_800_53	SI.7
rule.pci_dss	11.5
rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3
syscheck.attrs_after	ARCHIVE
syscheck.changed_attributes	mtime, md5, sha1, sha256
syscheck.diff	< abdelrahman khaled < abdelrahman sohsah --- > abdelrahman kha1ed > abdelrahman sohsah
syscheck.event	modified
syscheck.md5_after	d15aa8c1707900cb509104f56734ba4a
syscheck.md5_before	adae24b6300ffdd0472865738771e9e8
syscheck.mode	realtime
syscheck.mtime_after	Apr 24, 2024 @ 20:56:28.000

Now we are sure our data has been monitored. We apply the same steps in every file carrying sensitive data.

Resources:

1-https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html

2-https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html