

# 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:

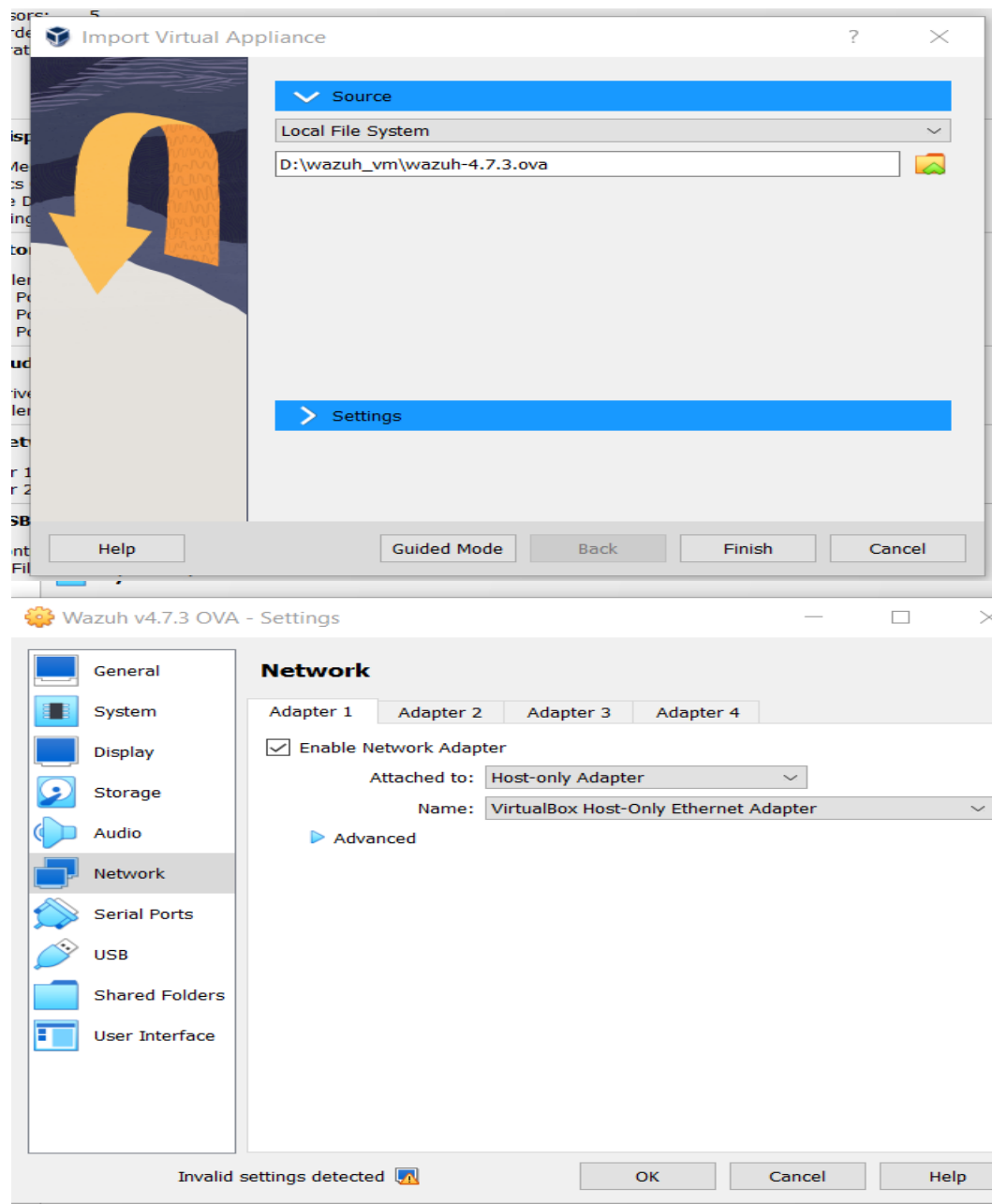
### Step 1: installing and configuring wazuh (.ova) machine

#### 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:

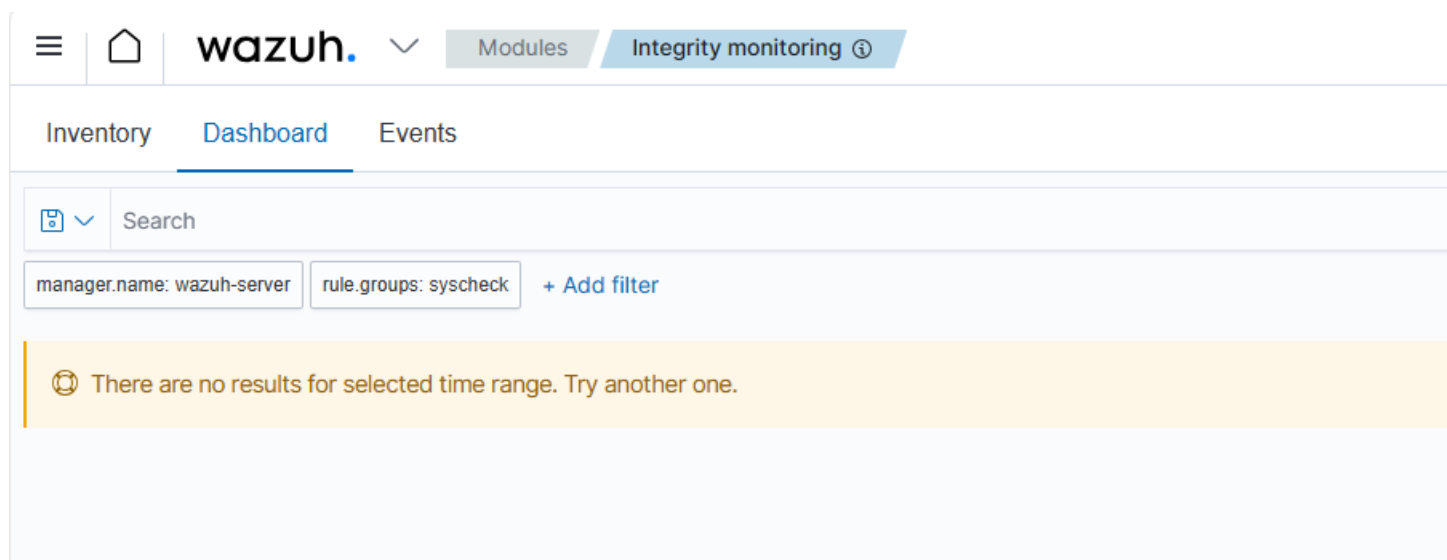
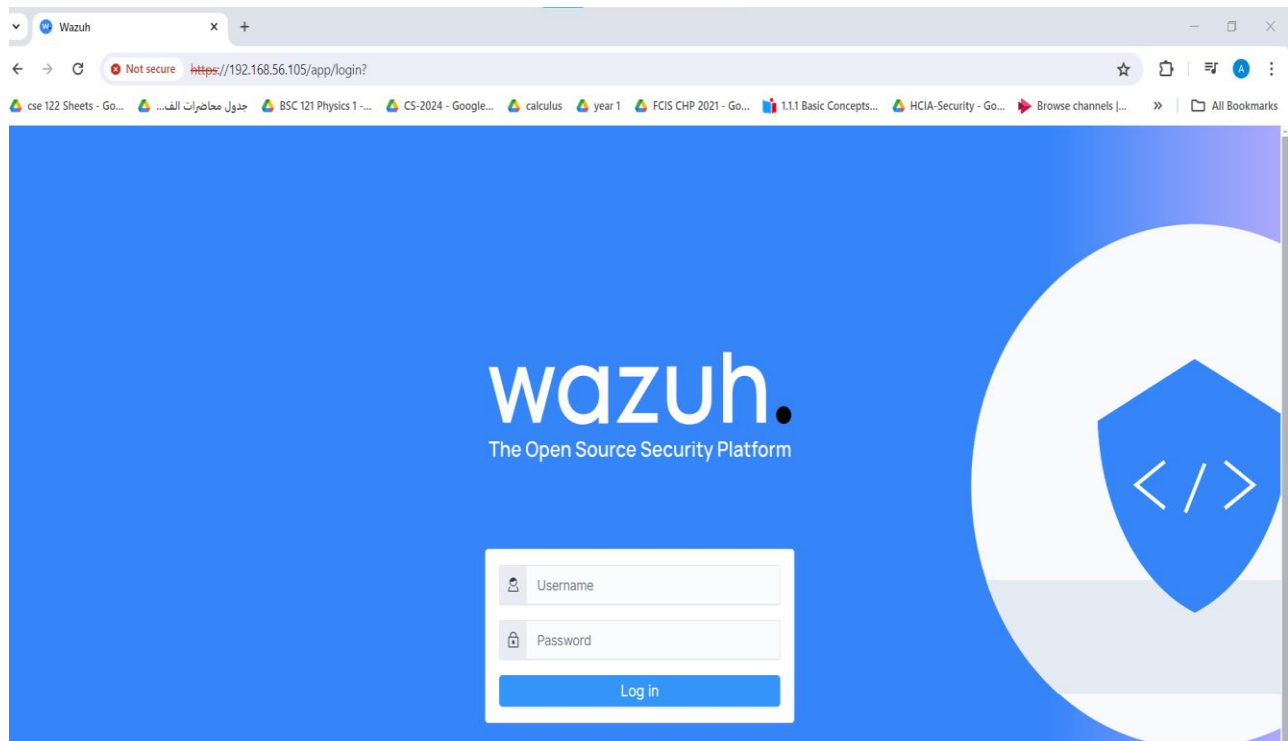
- Amazon Linux 2
- Wazuh manager 4.7.3
- Wazuh indexer 4.7.3
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.7.3



**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:r9eJRrxYuLMuFq1HokQ0msKm028Gua0ez1+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 }

The image shows two screenshots related to Wazuh agent configuration and installation.

**Top Screenshot: Wazuh Agent Configuration**

**Select the package to download and install on your system:**

- LINUX**
  - ☐ RPM amd64
  - ☐ RPM aarch64
  - ☐ DEB amd64
  - ☐ DEB aarch64
- WINDOWS**
  - ☒ MSI 32/64 bits
- macOS**
  - ☐ Intel
  - ☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

**Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

**Assign a server address:**

**Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

**Assign an agent name:**

**Bottom Screenshot: Wazuh Agent Installation**

**Select one or more existing groups:**

**Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile $(env:tmp)\wazuh-agent.msi; msexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER="192.168.56.106" WAZUH_AGENT_NAME="project_data_security" WAZUH_REGISTRATION_SERVER="192.168.56.106"
```

**Requirements**

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

**Start the agent:**

```
NET START WazuhSvc
```

[Close](#)

wazuh. Agents

Administrator: Windows PowerShell

Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell <https://aka.ms/pscore6>  
  
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile \$(env:tmp)\wazuh-agent; msixexec.exe /i \$(env:tmp)\wazuh-agent /q WAZUH\_MANAGER='192.168.56.106' WAZUH\_AGENT\_NAME='project\_data\_security' WAZUH\_REGISTRATION\_SERVER='192.168.56.106'  
PS C:\Windows\system32> NET START WazuhSvc  
The Wazuh service is starting.  
The Wazuh service was started successfully.  
  
PS C:\Windows\system32>

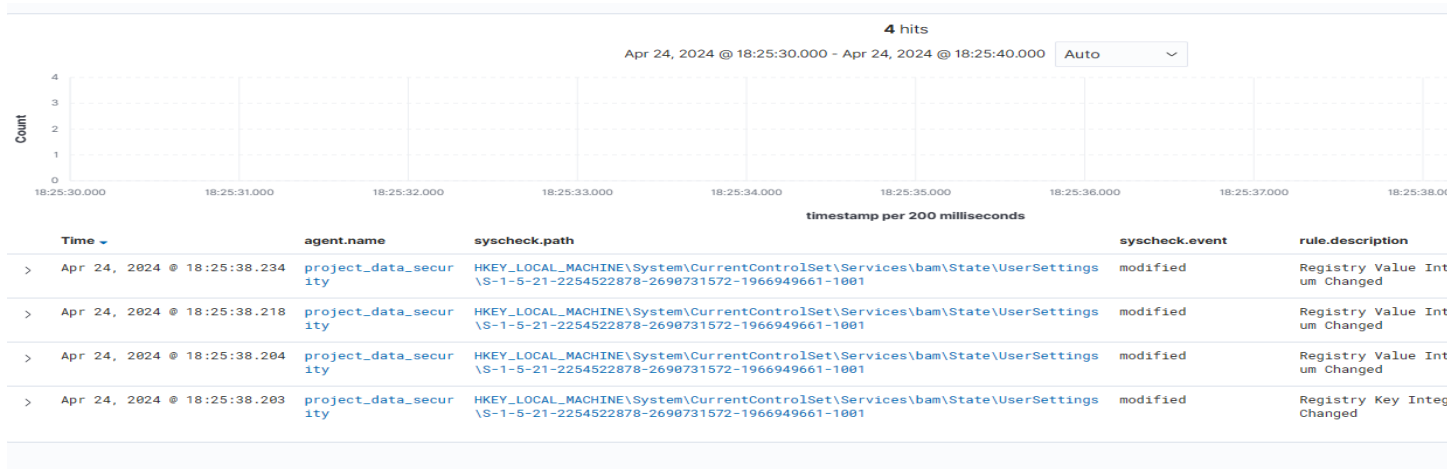
Agents (1)

1d1=898 and Search

WQL Refresh

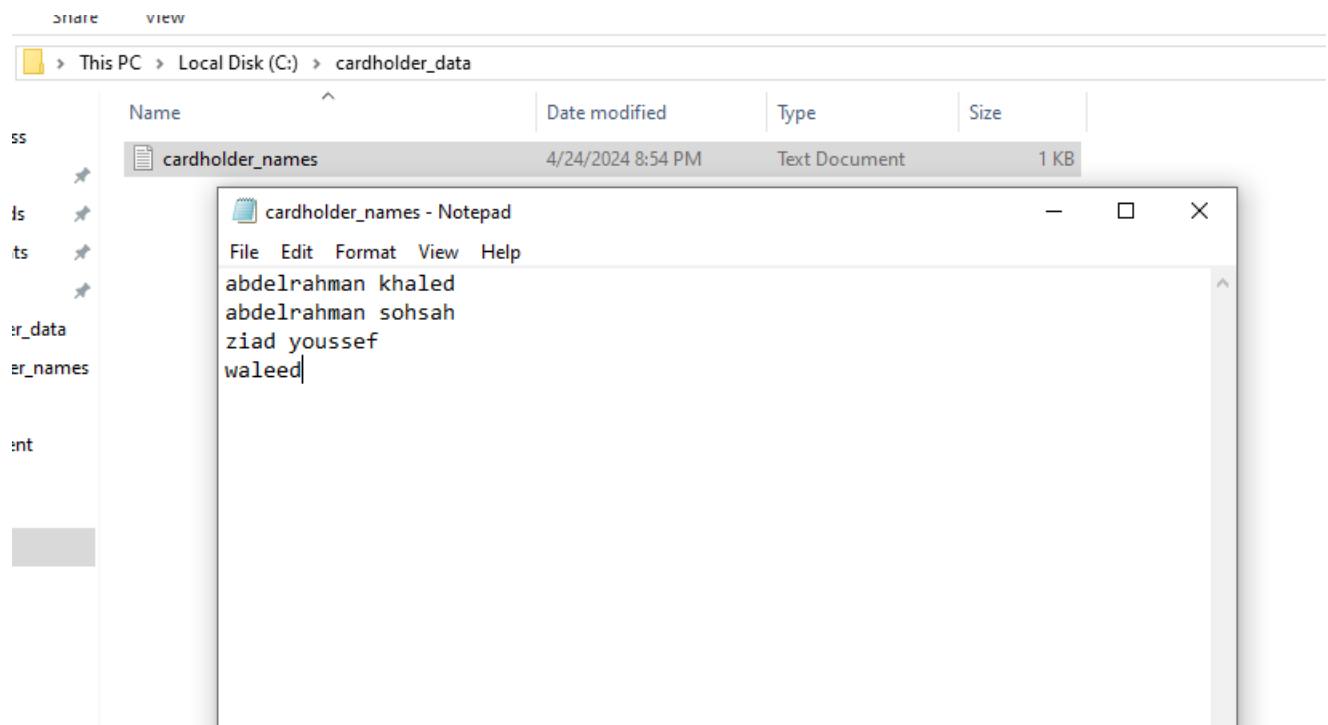
ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	project_data_security	192.168.56.103	default	Microsoft Windows 10 Pro 10.0.19045.4170	node01	v4.7.3	active	

Rows per page: 10 < 1 >

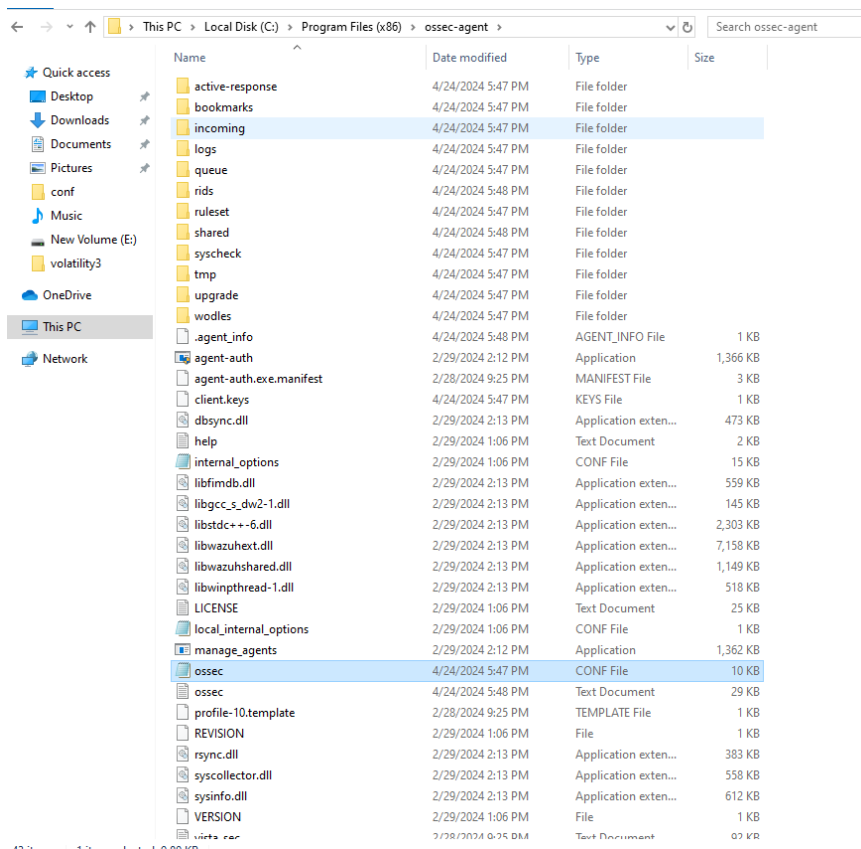


Now we have wazuh server and wazuh agent both running we go to step 5 where we change configurations of agent.

**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>

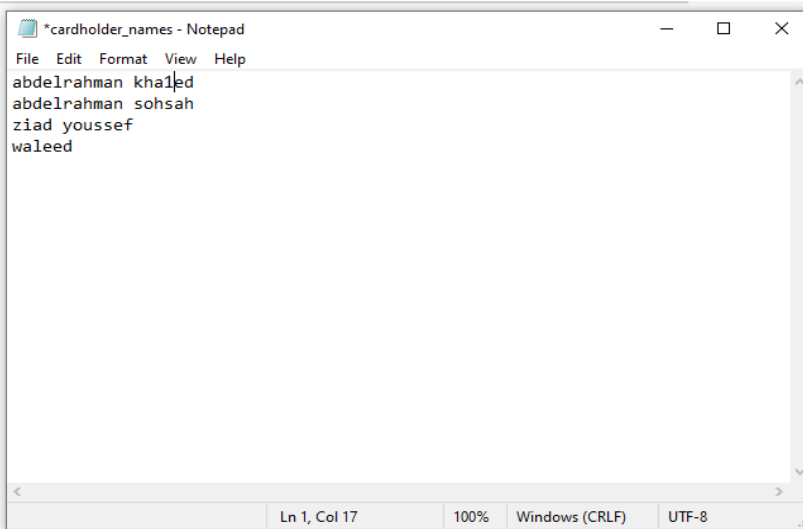
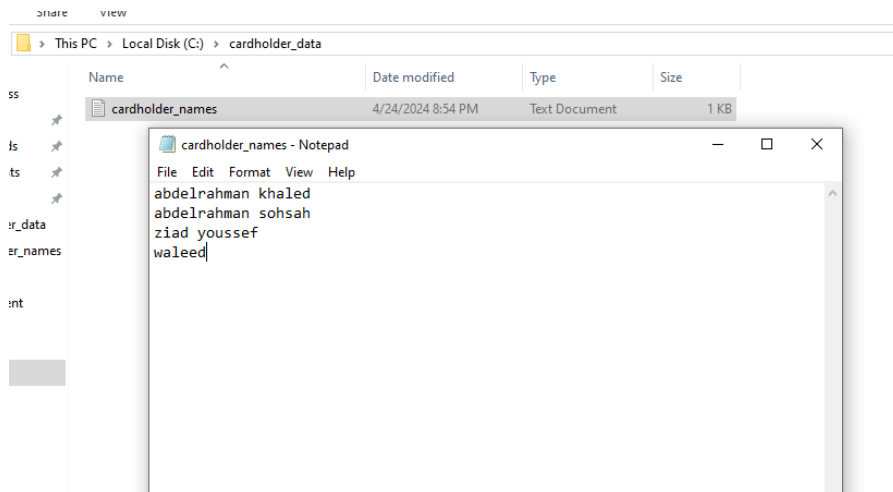
<!-- Default files to be monitored. -->

<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



Apr 24, 2024 @ 20:56:28.869

project\_data\_security

c:\cardholder\_data\cardholder\_names.txt

modified

Integrity checksum changed.

7

558

Expanded document

View surrounding documents

View single document

Table	JSON
	<pre>{  "_index": "wazuh-alerts-4.x-2024.04.24",  "agent.id": "001",  "agent.ip": "192.168.56.103",  "agent.name": "project_data_security",  "decoder.name": "syscheck_integrity_changed",  "full_log": "&gt; File 'c:\\cardholder_data\\cardholder_names.txt' modified\nMode: realtime\nChanged attributes: mtime,md5,sha1,sha256\nOld modification time was: '1713984867', now it is '1713984988'\nOld md5sum was: 'adae24b6300ffdd0472865738771e9e8'\nNew md5sum is: 'd15aa8c1707900cb509104f56734ba4a'\nOld sha1sum was: '1a07806kh00h.faf6r6aahfho1ah1h663775a7003'",  "id": "1713984988.2590946",  "input.type": "log",  "location": "syscheck",  "manager.name": "wazuh-server",  "rule.description": "Integrity checksum changed.",  "# rule.firedtimes": "4",  "rule.gdpr": "II.5.1.f",  "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": "&lt; abdelrahman khaled\n&lt; abdelrahman sohsah\n---\n&gt; abdelrahman khaled\n&gt; 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"}</pre>

Activate Windows

Go to Settings to activate Windows.

Activate Windows  
Go to Settings to activate Windows.

**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>**