FIM - FILE INTEGRITY MONITORING

FIM allows us to monitor files and folders (directories) for any changes made within them.

Example:

I. if a new file was created
ii. if a file was tampered with or edited
iii. if a file was deleted

Changes like this will be picked up by the Wazuh SIEM so we can monitor and know what happened in that folder/directory.

Preamble:

Open Wazuh SIEM in your Windows browser. Confirm your Wazuh VM IP address. In your Windows browser, type your Wazuh IP address, e.g., 192.168.56.102, as a wazuh ip will be https://192.168.56.102 when typing it into your browser.

Now wazuh's dashboard should be opened in your browser

1. Locate the ossec.conf file. You can find it in the C:\Program Files (x86)\ossec-agent\ folder. Don't forget you can locate your C drive under "This PC."
2. **Edit the C:**\Program Files (x86)\ossec-agent\ossec.conf configuration file, telling it the folders/directories you would like to monitor. For this use case, you'll configure Wazuh to monitor the C:\Users\<Your PC Account>\ Desktop directory
3. Once you have found the ossec.conf file, open Windows PowerShell as administrator and type: notepad "C:\Program Files (x86)\ossec-agent\ossec.conf" to open the ossec.conf file using Notepad on Windows.
4. **Search (Ctrl+F):** Type syscheck to search for the syscheck section. You'll find directories listed that are already being monitored. Now add your own desktop directory to be monitored using the code below just before the closing </syscheck>

```
<directories check_all="yes" report_changes="yes"
realtime="yes">C:\Users\<Your PC Account>\Desktop</directories>
```

5. Once added, save changes to Notepad through the file menu: File - Save. This will save changes made to your ossec.conf file.

THE GENERAL FORMAT FOR MONITORING DIRECTORIES IS ALWAYS:

```
<directories check_all="yes" report_changes="yes"
realtime="yes">MY DIRECTORY PATH</directories>
```

6. Now restart the Wazuh agent service while on PowerShell using the command below: Restart-Service -Name WazuhSvc. Wait for about 10 seconds.
7. On your desktop, let's create a new text document (notepad file). Right-click on an empty space on your desktop and select "New," then select "Text document." You can name the document "American history." By default it will have the extension - .txt.
8. Refresh your Wazuh dashboard page in your browser. Click "Agents," which reveals your Windows machine endpoint, and then click on your Windows machine/PC in the list to reveal security events within this endpoint. You'll notice a new security event displayed. It shows that a new text document had been created in the desktop directory of Windows, indicating that Wazuh SIEM is tracking events on your Windows PC.
9. Go back to your desktop. Open the "American history" text file, add some new content, and save.
10. Refresh the Wazuh dashboard and wait 6 seconds. You'll receive a new notification that the same file has been modified in Wazuh when you check your Windows endpoint on the Wazuh dashboard.