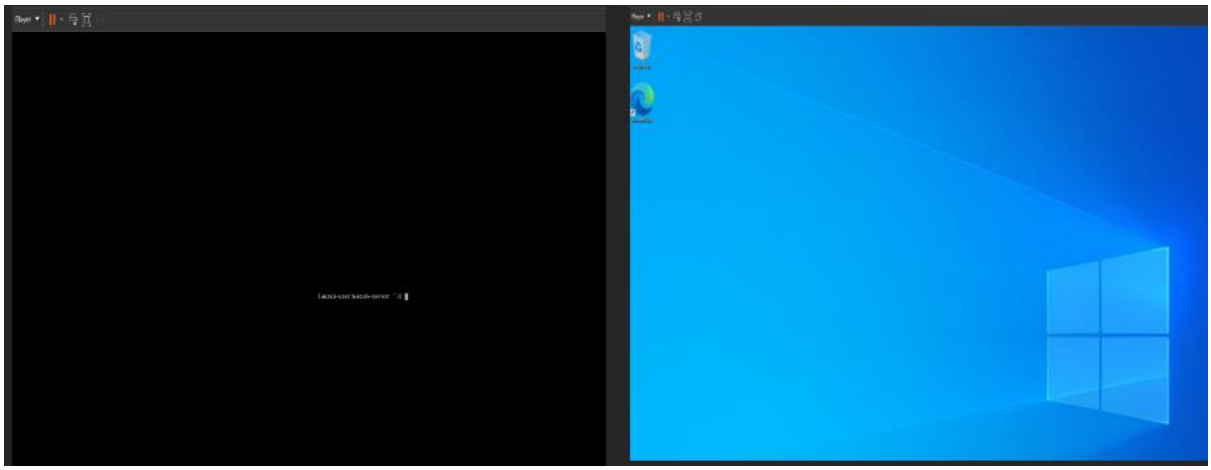
File integrity monitoring

File Integrity Monitoring (FIM) helps in auditing sensitive files and meeting regulatory compliance requirements. Wazuh has an inbuilt FIM module that monitors file system changes to detect the creation, modification, and deletion of files.

This use case uses the Wazuh FIM module to detect changes in monitored directories on Ubuntu and Windows endpoints. The Wazuh FIM module enriches alert data by fetching information about the user and process that made the changes using who-data audit.

In this lab, I am going to test the file integrity in windows Instance.

As shown below, I have launched both my Wazuh and windows instances up and alive

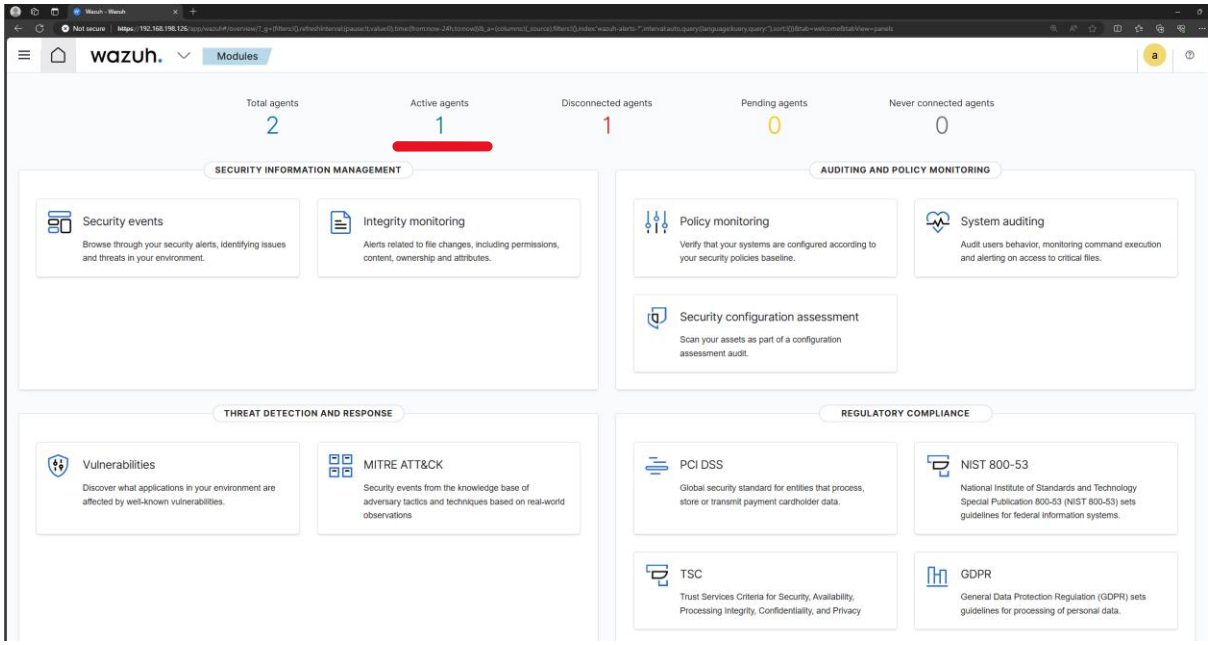


I have logged into the dashboard in windows instance

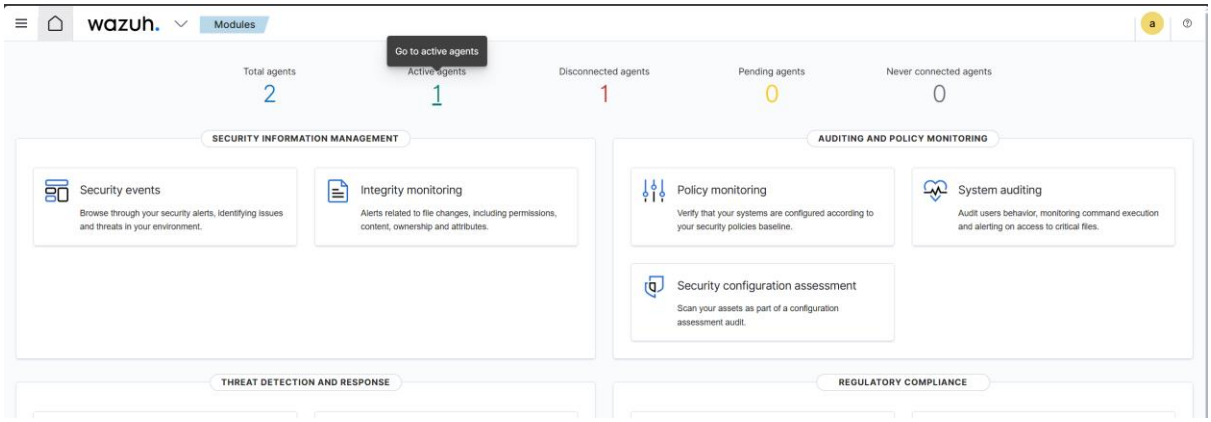
https://your-wazuh-IP

paste this URL in any web browser

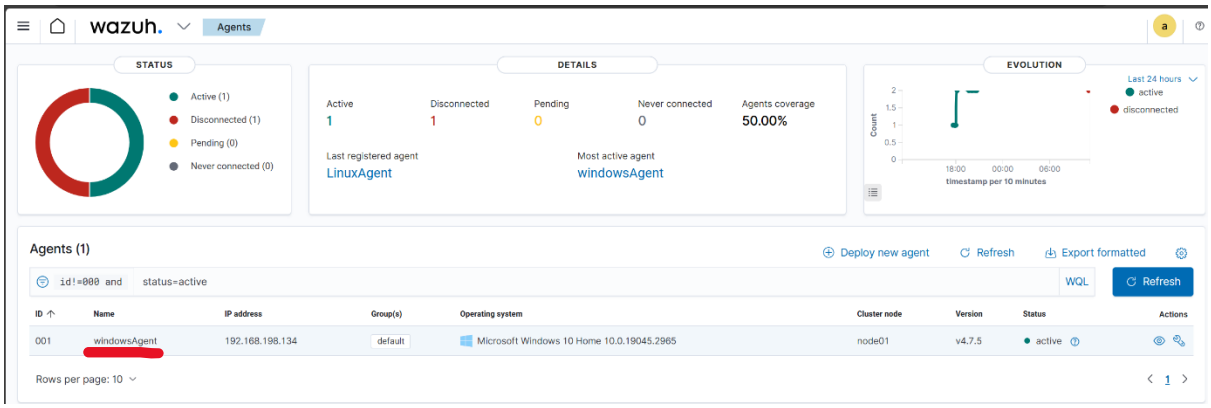
You can see, in my case, I have two Agents already been registered. Since, I have booted only my windows instance, its showing Active agents as “1”.



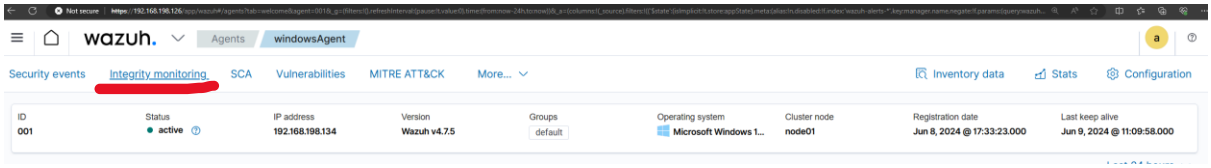
Now, click on “Go to active agents”



Next click on the instance that is show up,in my case“windowsAgent”

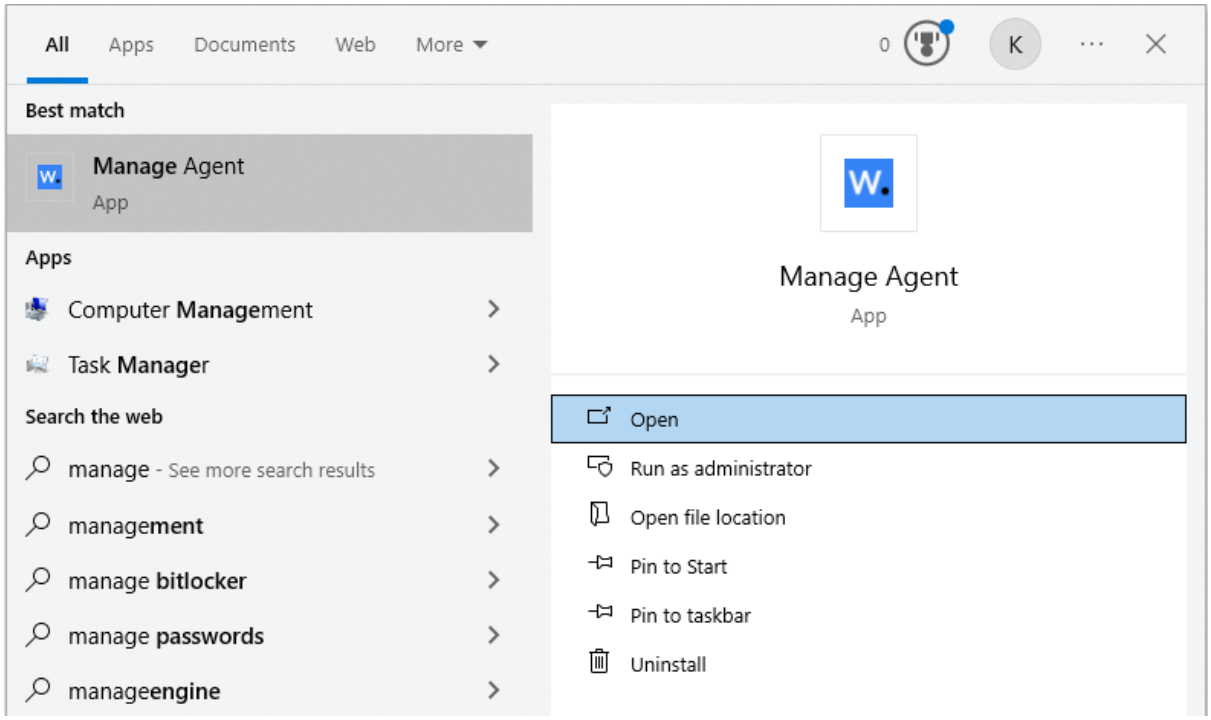


Then, click on “integrity monitoring”

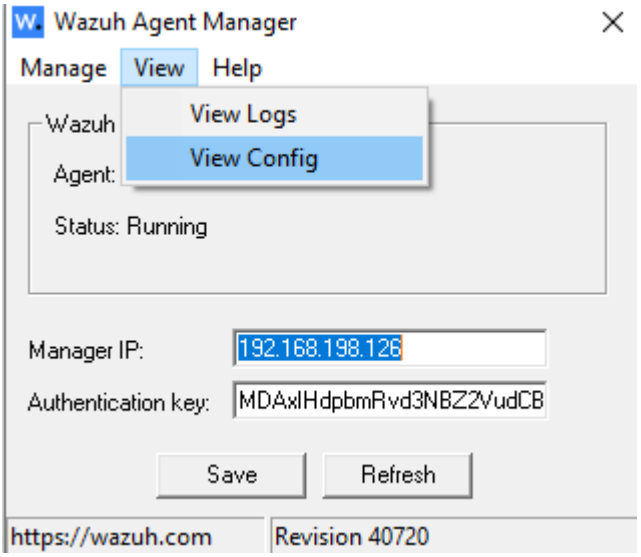


Now, you can see that there were no data found.
in order to configure it.

Click on the start menu and search for “Manage Agent” and run as administrator



Now click on “view” and then “view config”



Now, you can see “ossec.conf” gets open in notepad, there search for “File integrity monitoring” section.

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

   <disabled>no</disabled>

   <!-- Frequency that syscheck is executed default every 12 hours -->
   <frequency>43200</frequency>

   <!-- Default files to be monitored. -->
   <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.exe$|netsh.exe$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.e
   <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
   <directories recursion_level="0" restrict="WMIC.exe$">%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>

   <!-- 32-bit programs. -->
   <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|s
   <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
   <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
   <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
   <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

   <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

   <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

   <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

   <!-- Windows registry entries to monitor. -->
   <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
   <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
   <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
```

Now add these lines at that end of the section

Command:

<directories report_changes="yes" check_all="yes" realtime="yes">Your-stored-directory-section-name </directories>

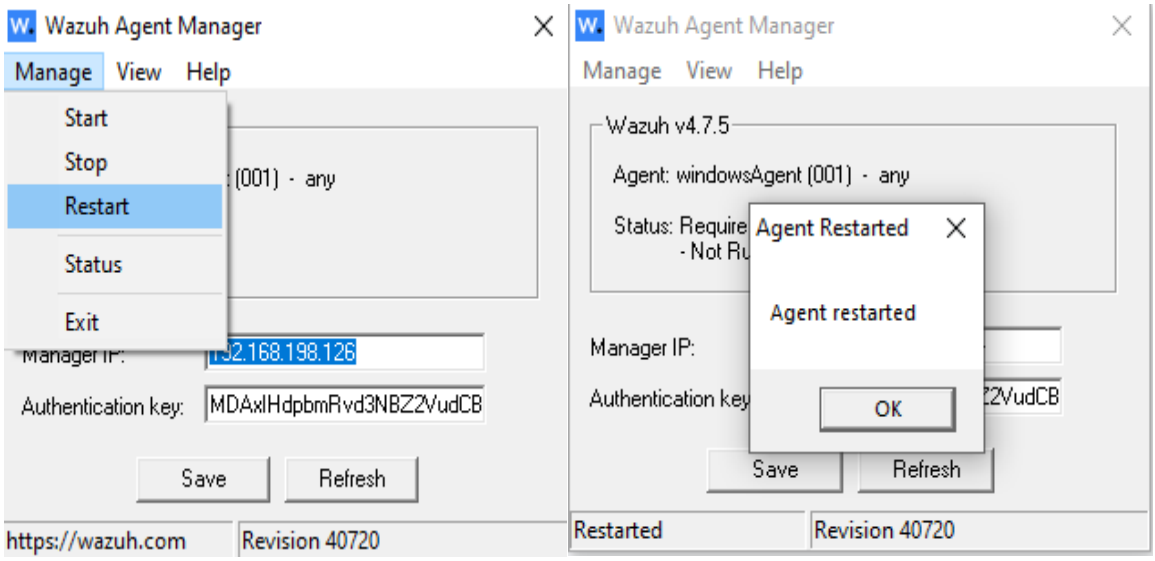
In my case, all the files were saved to downloads section, so, I have given the address as my downloads folder path

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

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <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.exe$|netsh.exe$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%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>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
  <directories report_changes="yes" check_all="yes" realtime="yes">C:\Users\kusha\Downloads</directories>
  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
```

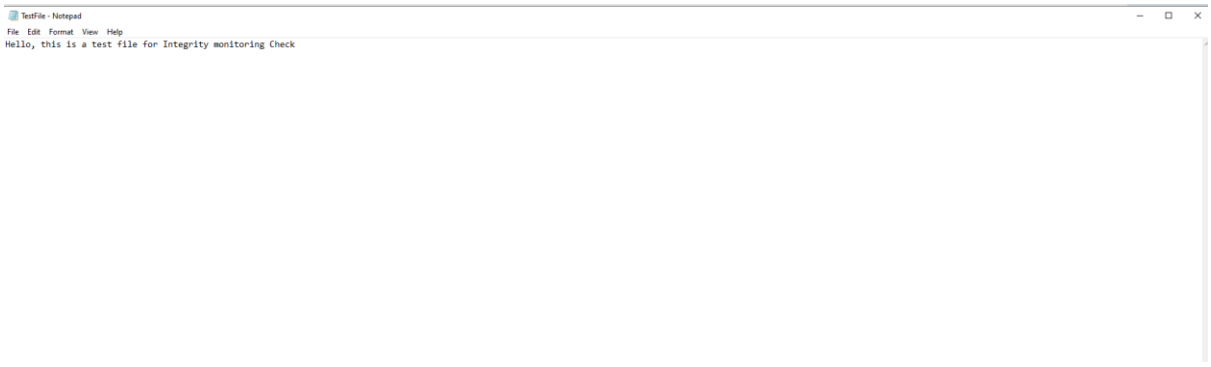
After, that save that file.

Now, try to restart the Wazuh agent, it update the changes that were made.

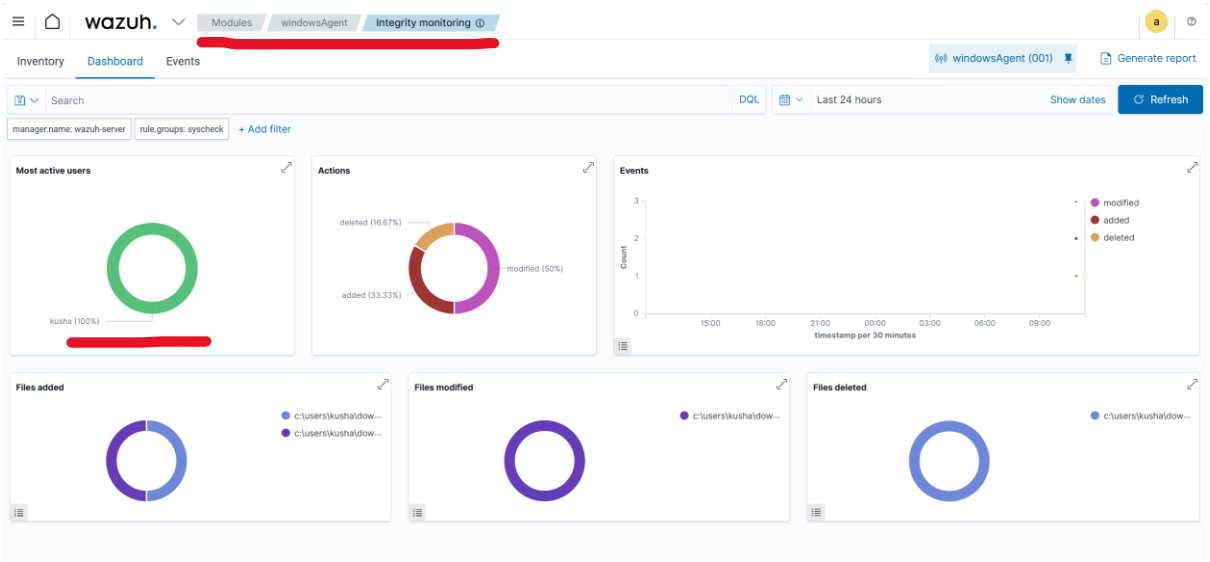
Start menu → Wazuh Agent Manager → Manage → Restart → ok



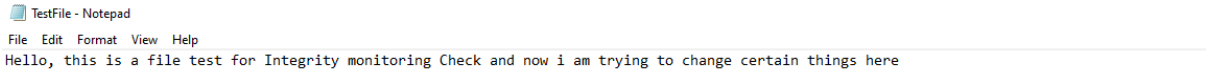
Now, try to create a .text file in your Downloads folder and try to give some input to the file



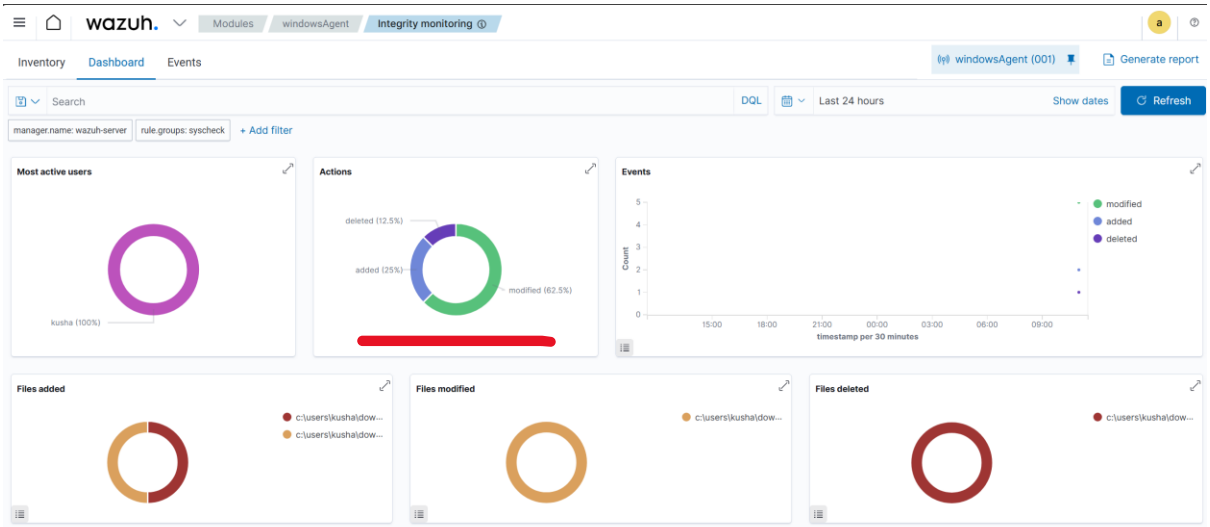
Now, go to your wazuh dashboard and try to refresh it, You can see That the information has been updated



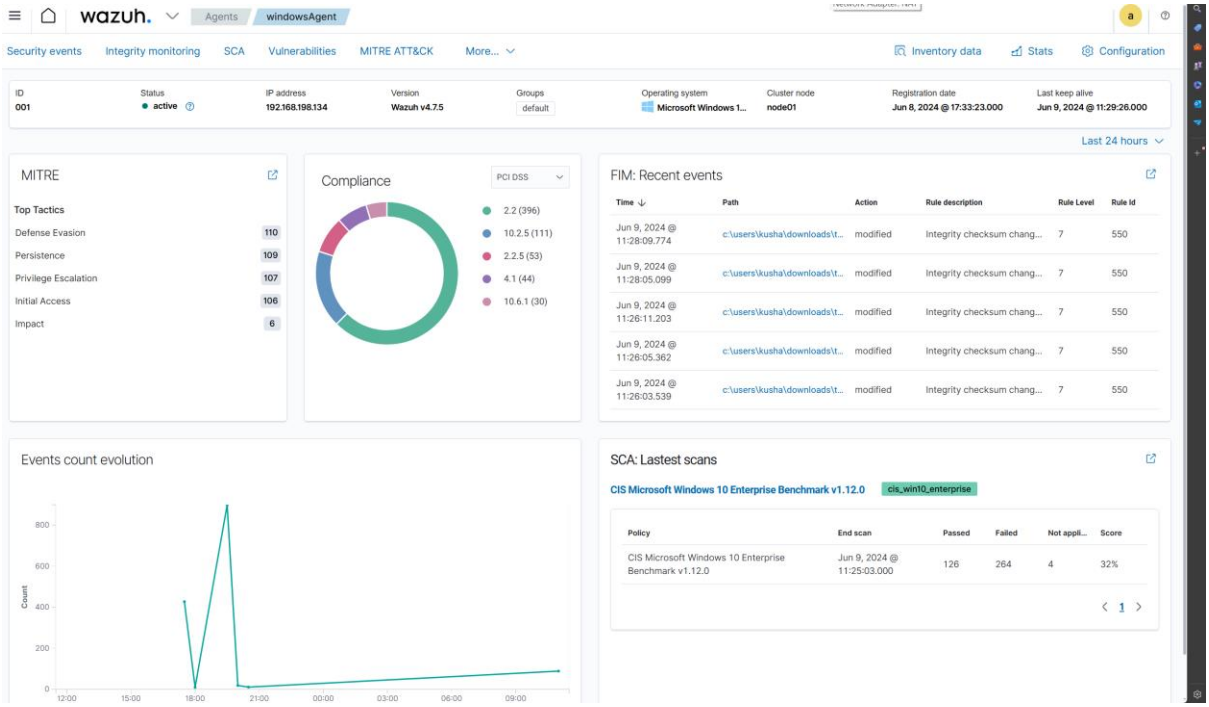
Now, try to modify the information in previous created .txt file



Now try to open your dashboard again and you can see that the file has been modified



You can even have a very detailed view of the modifications, that have been performed



FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Level	Rule Id
Jun 9, 2024 @ 11:28:09.774	c:\users\kusha\downloads\t...	modified	Integrity checksum chang...	7	550
Jun 9, 2024 @ 11:28:05.099	c:\users\kusha\downloads\t...	modified	Integrity checksum chang...	7	550
Jun 9, 2024 @ 11:26:11.203	c:\users\kusha\downloads\t...	modified	Integrity checksum chang...	7	550
Jun 9, 2024 @ 11:26:05.362	c:\users\kusha\downloads\t...	modified	Integrity checksum chang...	7	550
Jun 9, 2024 @ 11:26:03.539	c:\users\kusha\downloads\t...	modified	Integrity checksum chang...	7	550

c:\users\kusha\downloads\testfile.txt

Details

Last analysis
Jun 9, 2024 @ 11:28:08.000

Last modified
Jun 9, 2024 @ 11:28:08.000

User
kusha

User ID
S-1-5-21-3833950814-1893572939-1806992348-1001

Size
111 Bytes

MD5
a823d4a877528904253952 5cab8dc618

SHA1
bbe14a5b18133daee6b8a6fc7a32905714d4b8ac

SHA256
aeabeac102fc55d5fb678e9e28144f19ec84e89ba658bc54dd05f5c0d35289ef

Permissions

Recent events

6 hits

c:\users\kusha\downloads\testfile.txt

@timestamp	2024-06-09T10:28:09.774Z
_id	Q1CK_I8BF57hX5MNIr8D
agent.id	001
agent.ip	192.168.198.134
agent.name	windowsAgent
decoder.name	syscheck_integrity_changed
full_log	File 'c:\users\kusha\downloads\testfile.txt' modified Mode: realtime Changed attributes: mtime Old modification time was: '1717928883', now it is '1717928888'
id	1717928889.421274
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	Integrity checksum changed.
rule.firedtimes	5
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_modified, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2
rule.id	550
rule.level	7
rule.mail	false
rule.mitre.id	T1565.001
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
syscheck.event	modified
syscheck.md5_after	a823d4a8775289042539525cab8dc618
syscheck.mode	realtime