**Code Alpha**

**Task 4 Report**

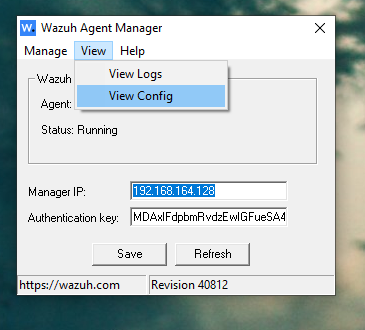
Muhammad Kamran Yousaf

**Task:**

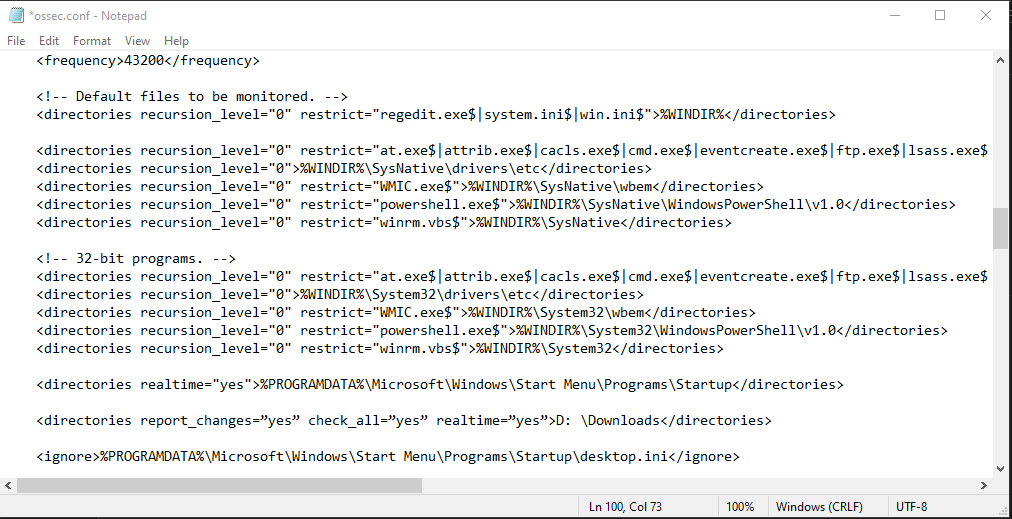
**Setting up an IDS**

**Solution:**

To complete this task we first configure virustotal with Wazuh manager for the detection phase so that we can detect and malicious file being downloaded.



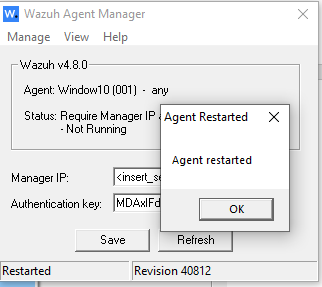
Firstly we restarted the wazuh manager and agent and then edited the configuration file, for file integrity monitoring.

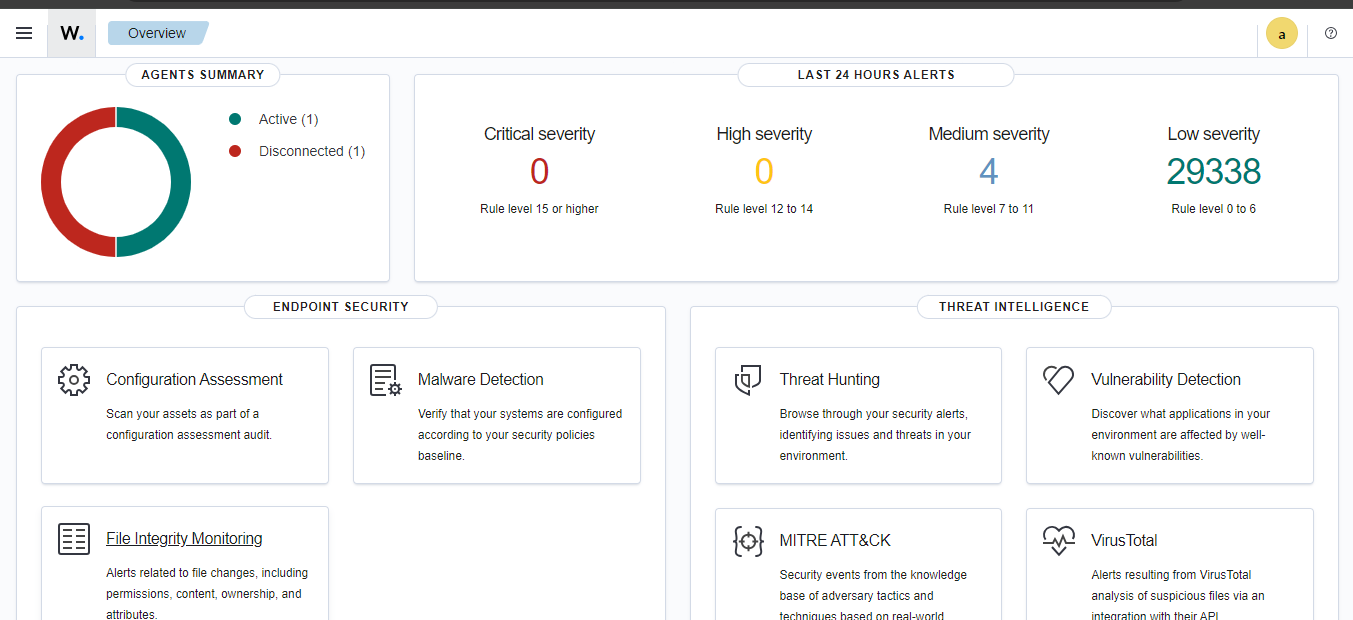


File integrity monitoring is necessary to know about any changes happening in the system so that if any of the files in the specified directories are modified an alert is triggered.

Here Winrm is the monitoring of Windows Remote Management which is a very critical thing to be looked at.

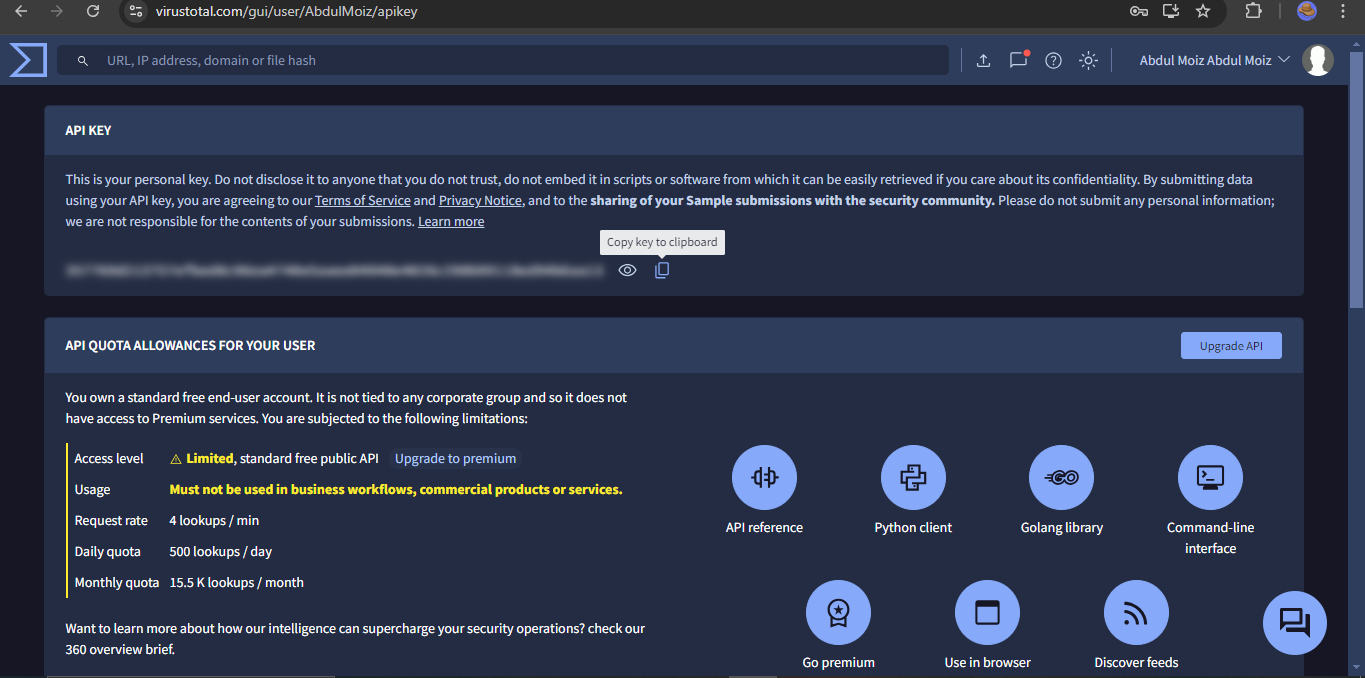
Once it is verified from the Ossec.conf file that file integrity monitoring is on we restart the agent.

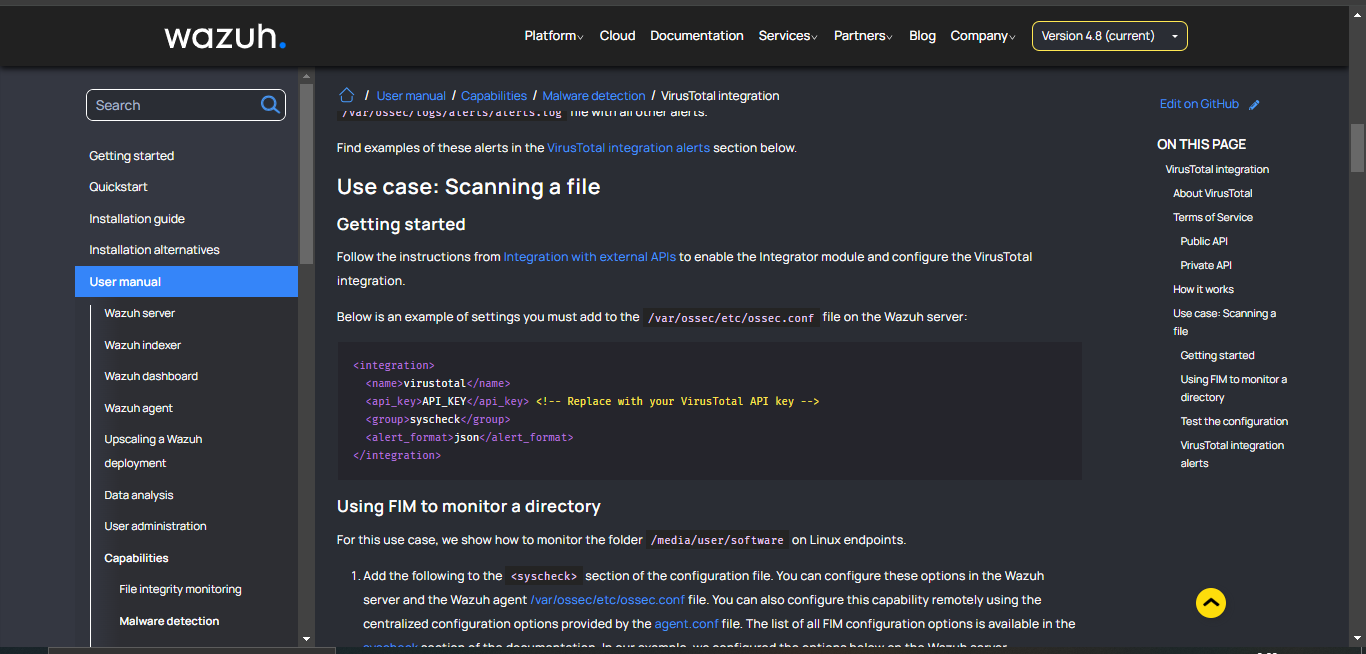


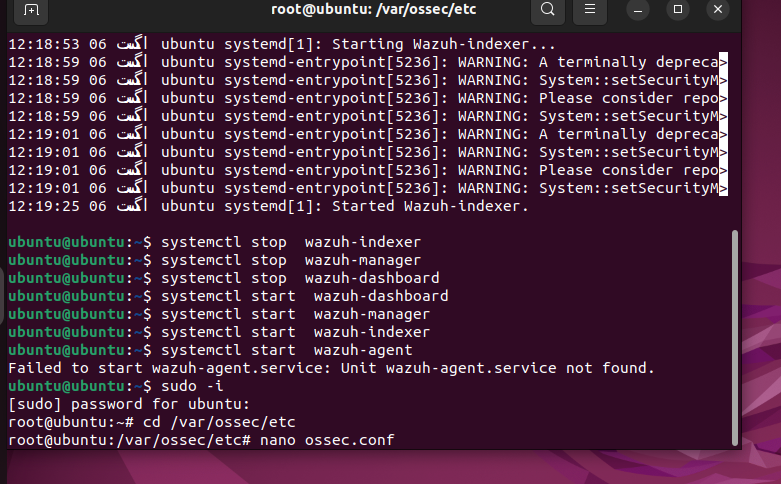
After restarting it we can access the dashboard and check that it is actively running and collecting different logs. Not it is time to integrate Virustotal with it for monitoring files and malwares.

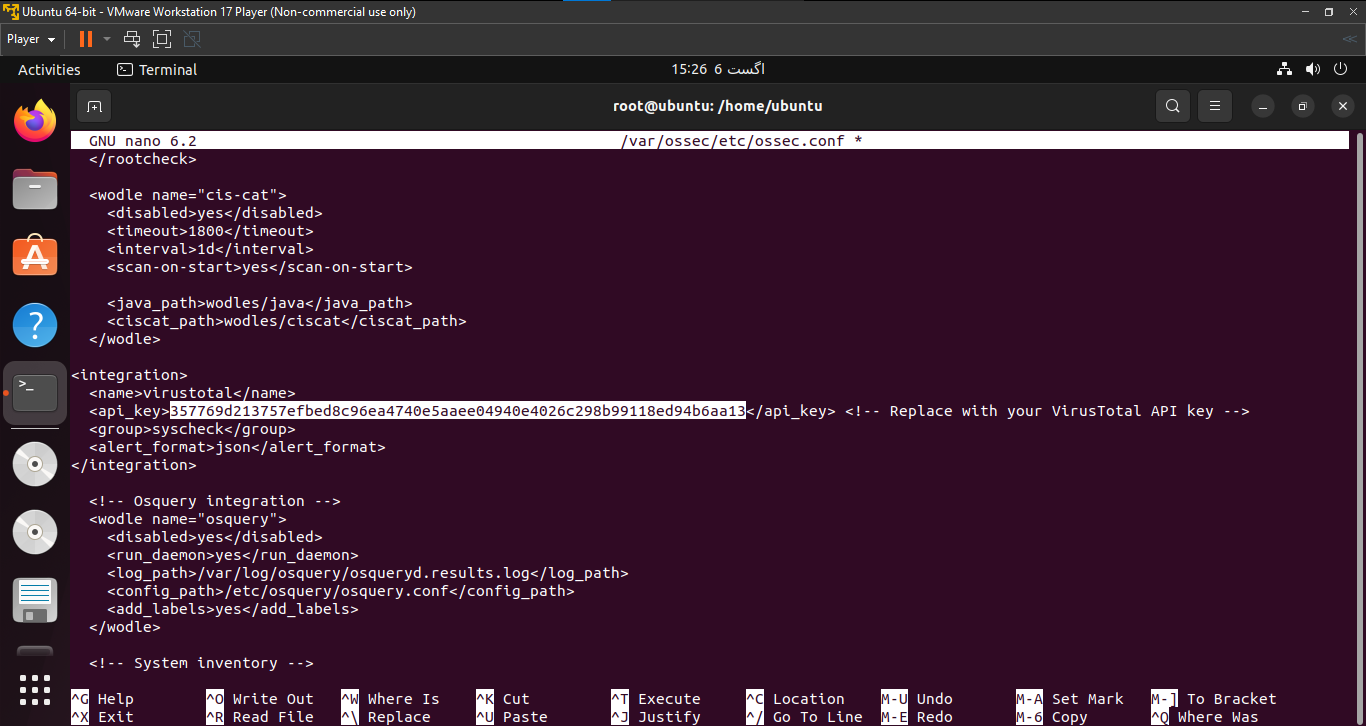
**Integrating with virus total:**



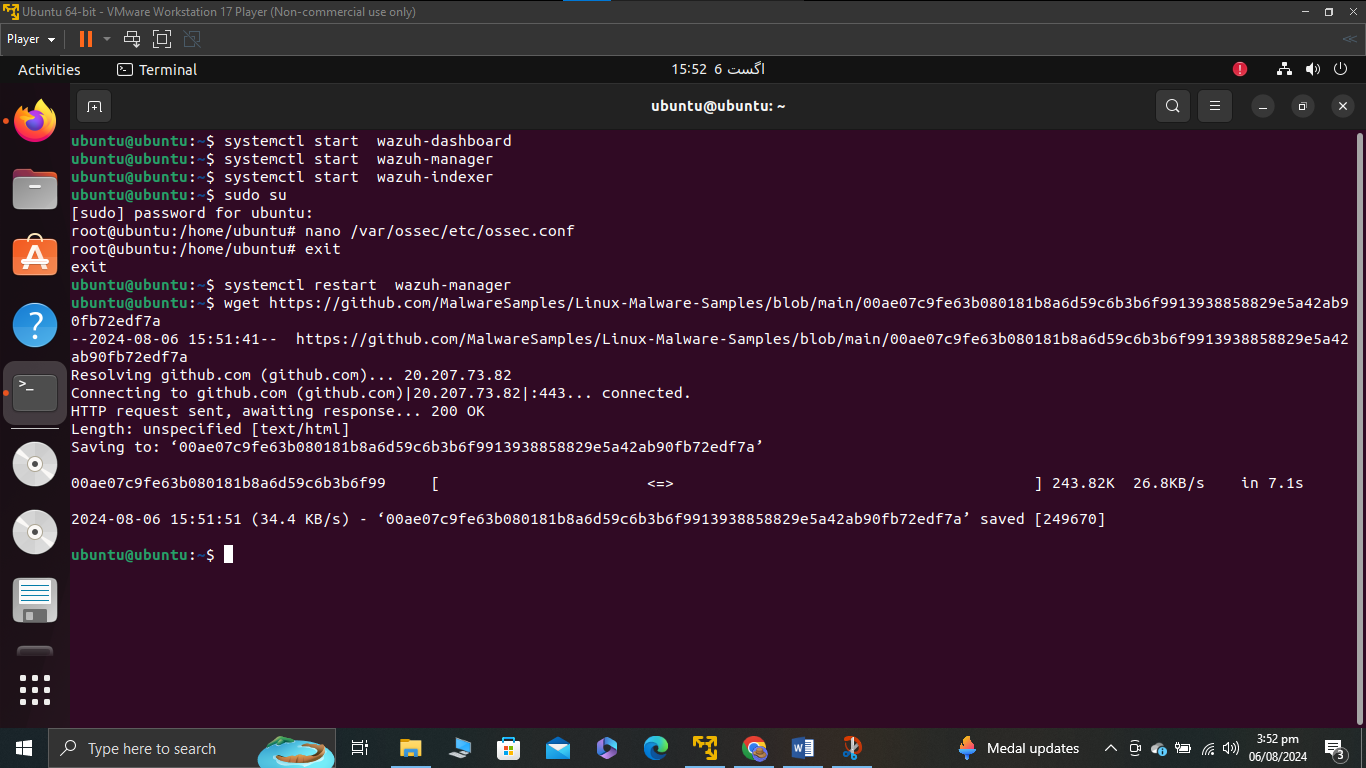




****



Configuring the Config file so that we can add the api key of virustotal and configure it with wazuh

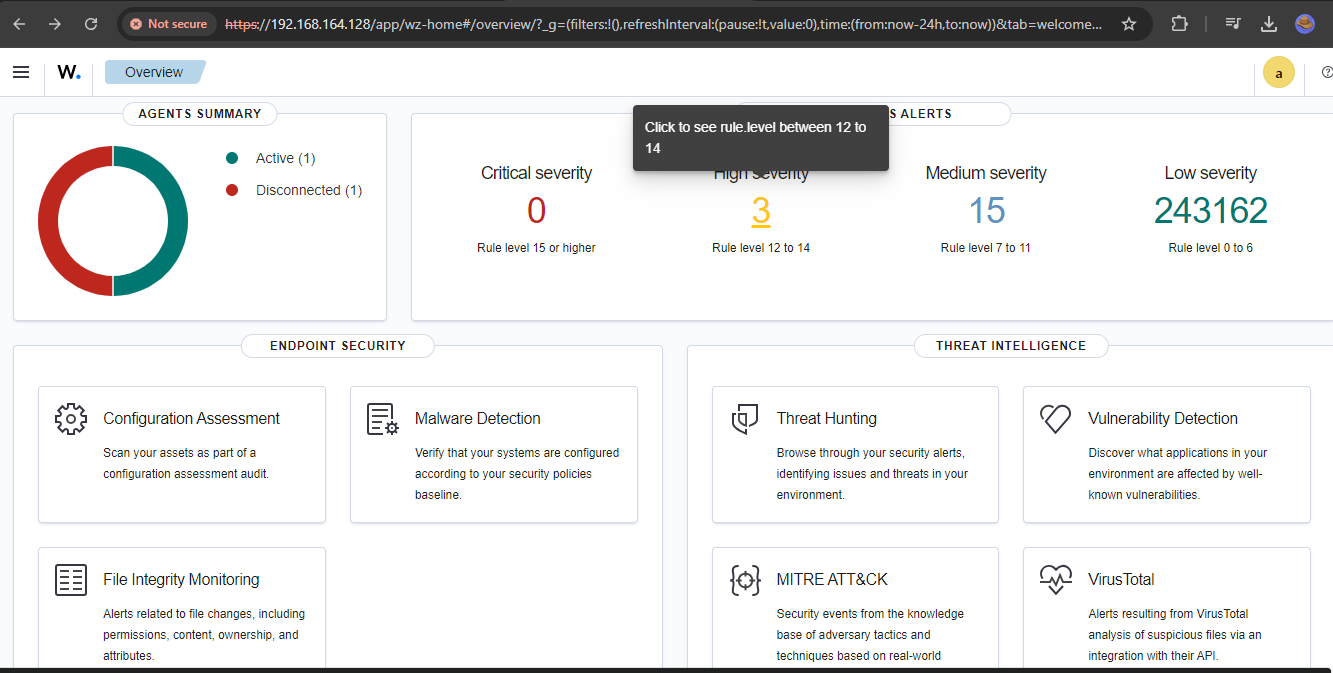


**Malware Download:**

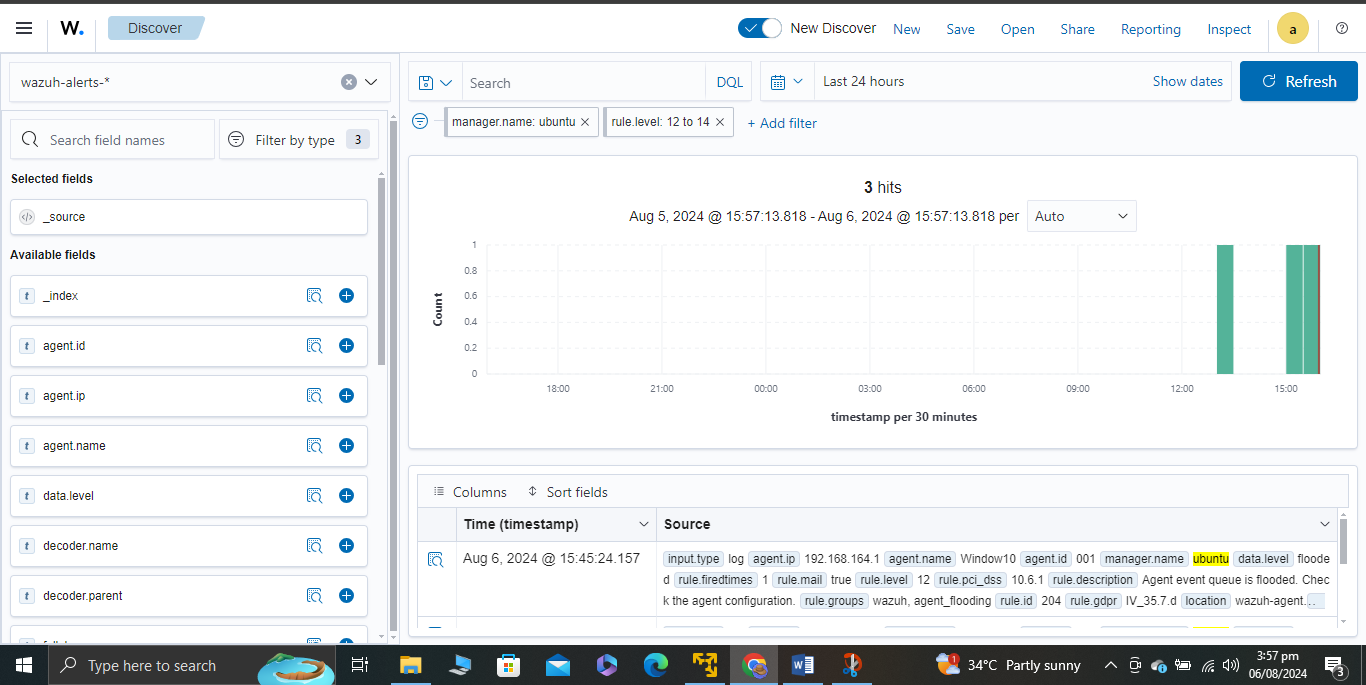
Next step is to download a malware so that it can be detected by wazuh and collect its logs after that. The link to the malware which was downloaded is given below

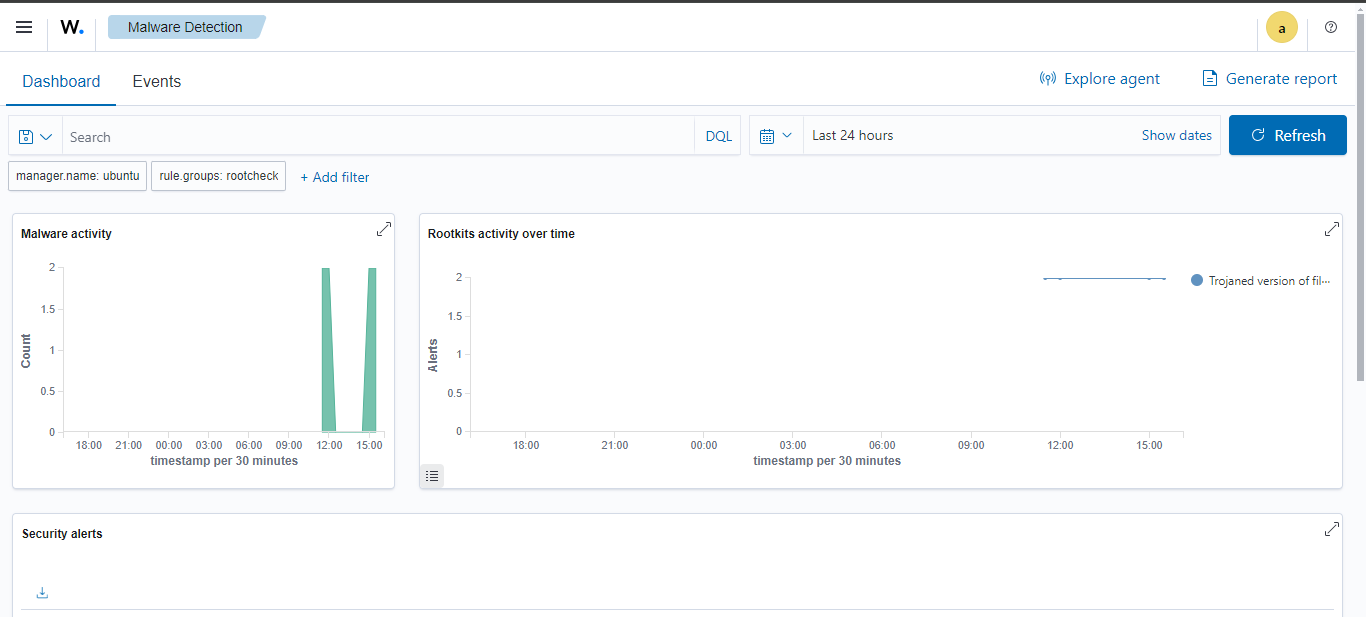
github.com/MalwareSamples/Linux-Malware-Samples/blob/main/00ae07c9fe63b080181b8a6d59c6b3b6f9913938858829e5a42ab90fb72edf7a

Once the malware is donwloaded we can see that it is detected by wazuh and high severity alerts are being generated by it.

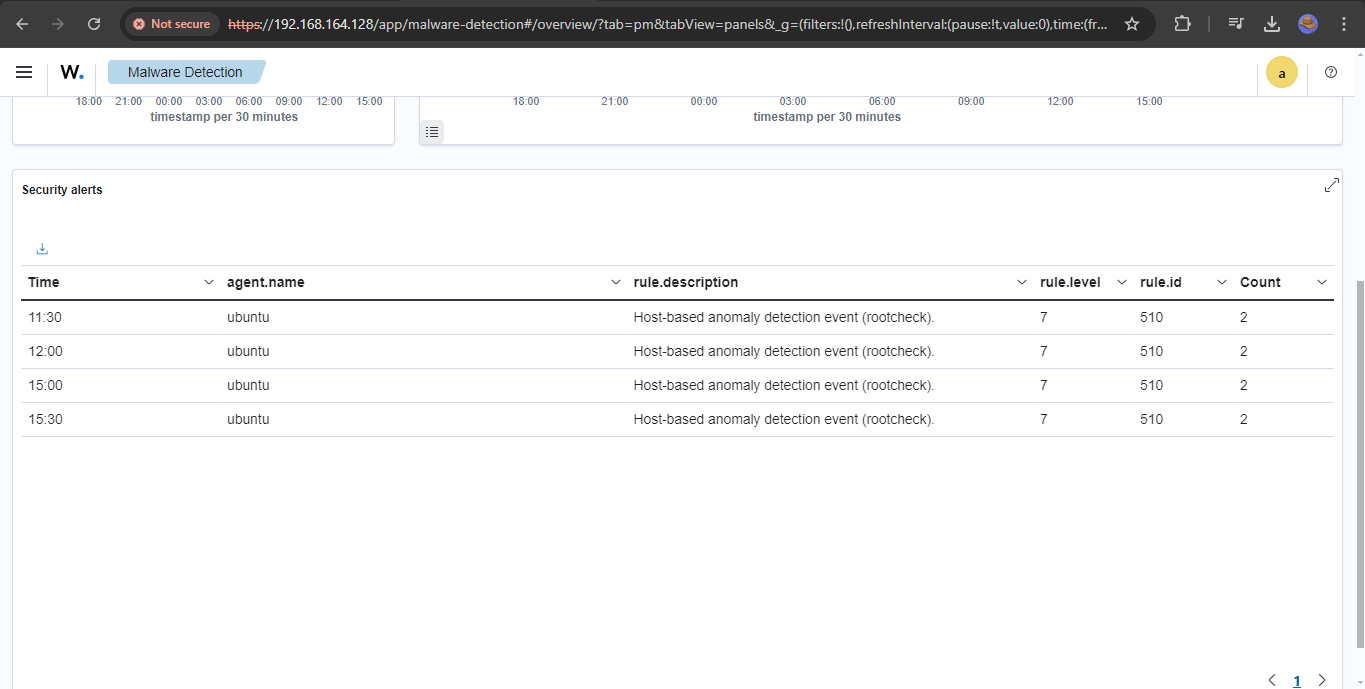


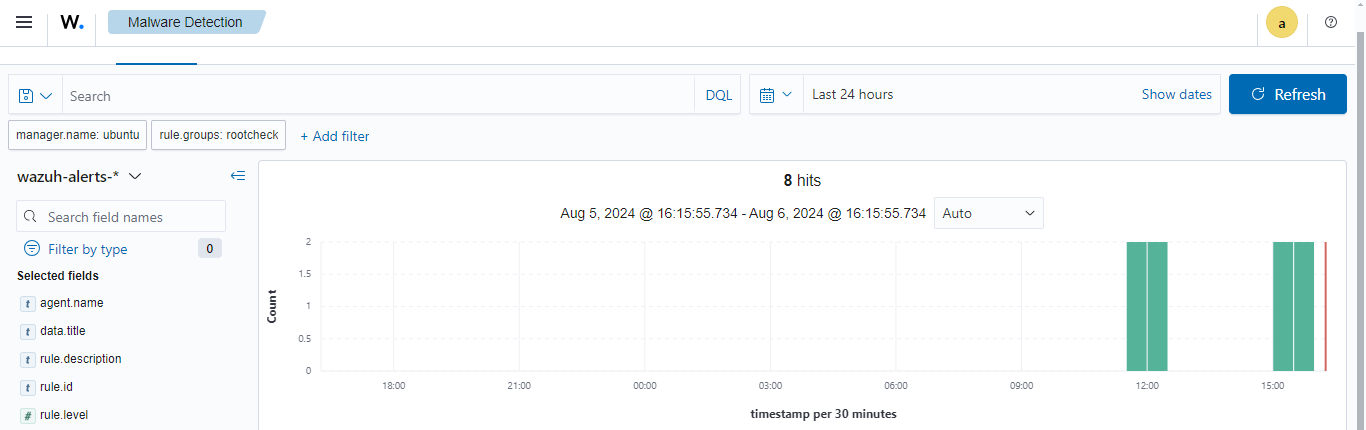
Once we open this to check for further log analysis





Further analysis shows the malware activity.

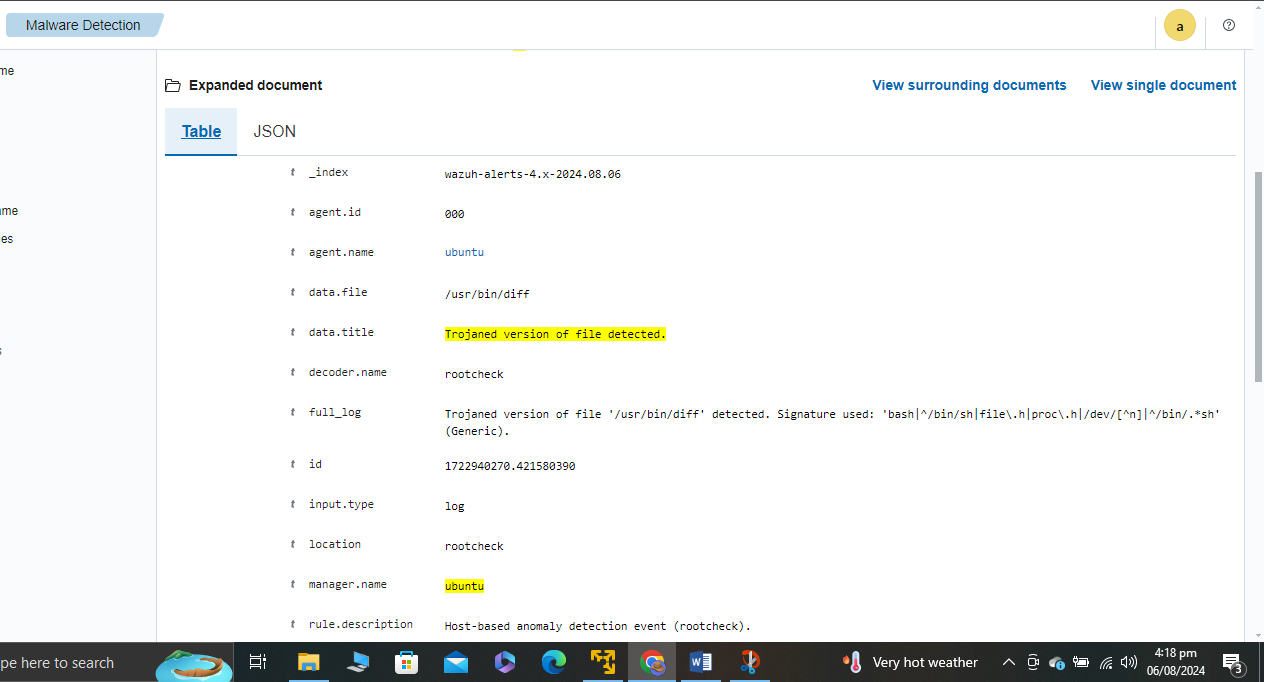




We detected the malware now wee will perform an observable analysis to this by analyzing the logs of the malware which was detected by virustotal.

**Log Analysis:**

We can see in the logs tab that there are severe alerts for trojaned verison of a file.





**Indicators of Compromise (IOCs)**

**File Path and Modification:**

Path: /usr/bin/diff

Alteration: The file has been identified as a "Trojaned version," which typically means unauthorized code or modifications have been embedded within the legitimate file.

**Detected Signature:**

Signature: The alert details mention specific signature patterns associated with the file, possibly indicating the method or nature of the modification. These signatures often match known malware patterns and can be used to identify the specific type of malware or toolkit used.

**Timestamps:**

The logs show timestamps which are critical in understanding when the compromise occurred. This helps in establishing a timeline for the breach.

**Indicators of Attack (IOAs)**

**File Execution Behavior:**

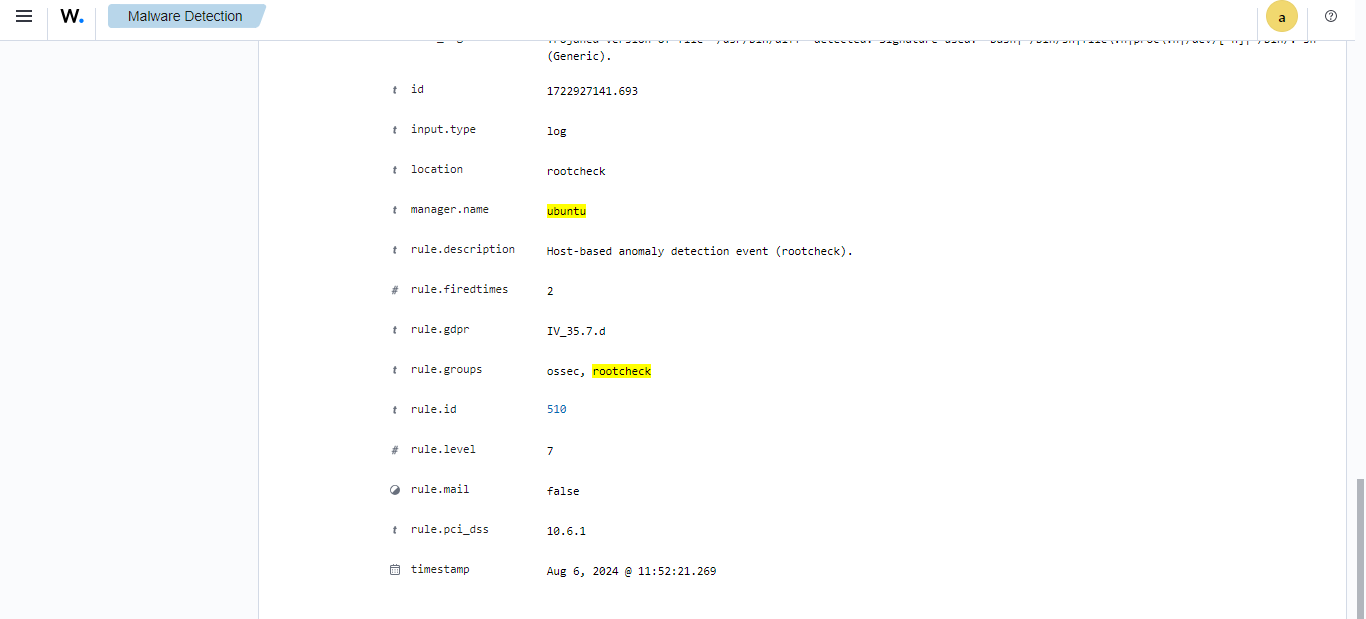
The alteration in /usr/bin/diff suggests that the file could be used to execute malicious actions unbeknownst to the user or other system processes, given that diff is a commonly used system utility.

**Anomaly in System Utility Behavior:**

If /usr/bin/diff starts behaving unusually or generating unexpected network traffic, this could be a strong indicator of an attack in progress, particularly since diff is typically used for comparing files and should not be communicating over the network.

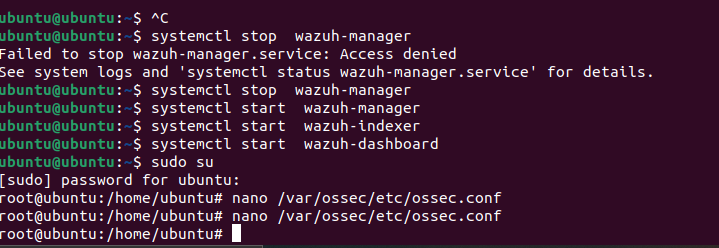
**Repeated Alerts:**

The repeated nature of the alerts, as seen in the screenshots, suggests ongoing or repeated attempts to utilize the trojaned file in operations within the system, which can be considered an active attack indicator.



Now we move to the incident response plan for it. For this purpose we will deploy an active IDS which can detect such incidents timely and generate alerts for it.

**Incident Response Plan:**



**1. Preparation**

Inventory Assets: Catalog all critical system files and software, particularly those vulnerable to tampering (e.g., /usr/bin/diff).

Deploy IDS: Install and configure an IDS like Snort or Suricata on all critical segments of the network to monitor for suspicious activities and known attack signatures.

Update and Patch: Ensure all systems are updated to the latest security patches to minimize vulnerabilities.

**2. Identification**

Monitor Alerts: Configure the IDS to alert the security team about any anomalies that match attack signatures or anomalous behavior patterns.

Integrate with Wazuh: Use Wazuh to aggregate and analyze logs from the IDS, providing a centralized view of potential threats.

**3. Containment**

Short-Term Containment: Immediately isolate affected systems from the network to prevent further spread of the attack.

Long-Term Containment: Assess the scope of the breach to determine if additional segments of the network need isolation.

**4. Eradication**

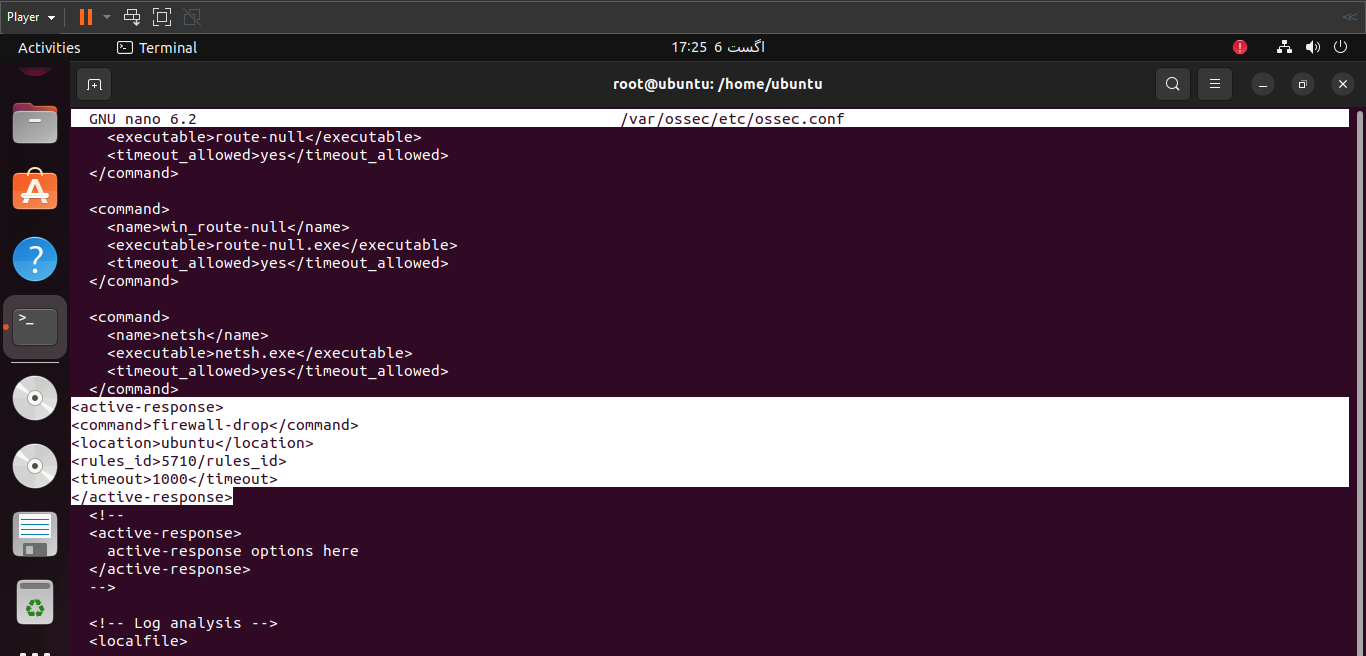
Remove Malware: Use trusted tools to remove any identified malware from systems. Restore affected files from known good backups.

System Hardening: After malware removal, harden affected systems by disabling unnecessary services and applying the least privilege principles.

**5. Recovery**

System Restoration: Gradually restore systems to operation after verifying they are clean.

Verify System Integrity: Run integrity checks to ensure no remnants of the threat remain.



**The End**