

## Table of Contents

1. Loading and Starting Wazuh Server-----	2
1.1 Loading Wazuh Server OVA File-----	2
1.2 Starting Server-----	2
2. Dashboard Setup and Agent Deployment-----	3
2.1 Getting Dashboard by IP-----	3
2.2 Login to Server -----	3
2.3 Deploying New Agent-----	3
2.4 Dashboard Detections -----	3
3. File Integrity Monitoring Configuration-----	6
3.1 Configurations Edit-----	7
3.2 Activating Services-----	6
3.3 Configurations Changes-----	8
3.4 Dashboard Detections-----	6
4. Integrating Wazuh with VirusTotal -----	9
4.1 Obtaining API Key -----	9
4.2 Editing Configuration for Integration -----	9
4.3 Detections-----	9
4.4 Testing Results-----	9
4.5 Same Hash Detected-----	9
5. File Integrity Monitoring Mitigation Methods-----	14
References -----	15

## Introduction:

This interest is an hands-on practical experience which touches every aspect of installation of security platform Wazuh including through server configuration, agent deployment, record integrity tracking, and VirusTotal integration. Users will find that each element includes instructions used for the right usage of Wazuh by providing a thoroughly detailed risk detection and analysis of the users. Following the guidelines of these directions ensures the protected status of systems and data by an advanced way.

## 1. Loading and Starting Wazuh Server

Description: This section covers the process of loading the Wazuh Server and starting it up.

The next part starts by detailing deployment process i.e., system configuration which entails configuring virtual machines, networks, and storage systems onto cloud infrastructure.

experiment with system parameters, install and configure the required dependencies and shell scripts, and deploy them. It clarifies startup of the server including memory allowance and port allocation, in the course of which we need to check server configuration especially. service and scalability. Moreover, it deals with all these basic things as well, such as getting the database connections running properly and the other auxiliary services—these are key for the smooth operation of the Wazuh platform.

Steps:

### 1.1 Loading Wazuh Server OVA File

Description: Load the Wazuh Server OVA file into your virtualization environment.

Wazuh Server integration can be achieved by importing the provided OVA file into the virtualization platform used by your virtual system. This step starts off by virtualizing your server, specifying parameters such as networking and storage configurations.

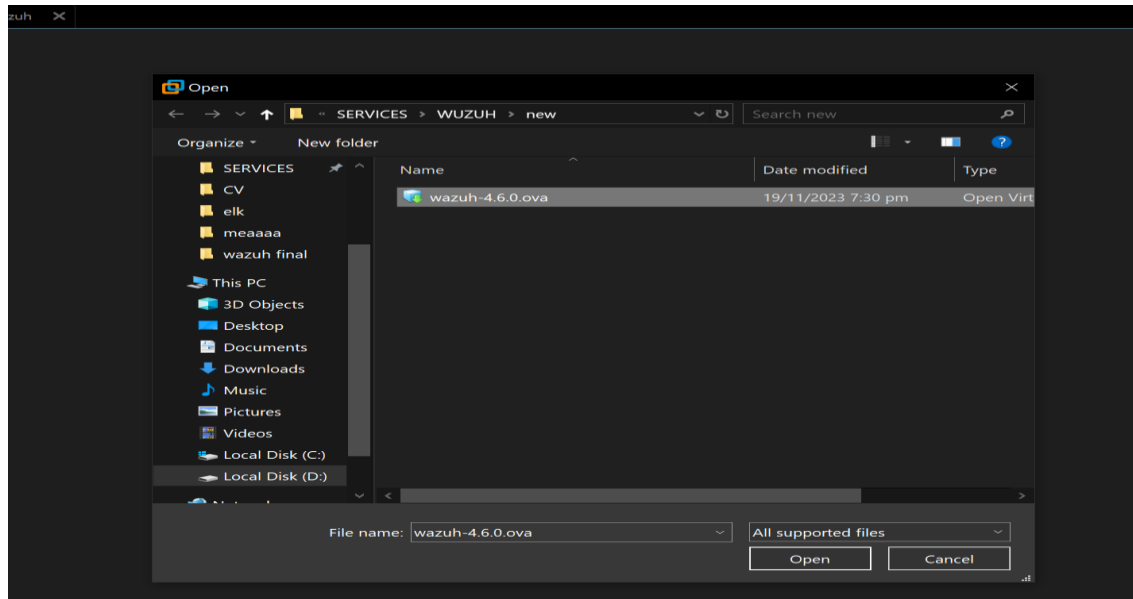


Figure-2 Opening wazuh. OVA file

## 1.2 Starting Server

Description: Start the Wazuh Server to initialize its services.

Commence the Wazuh Server to avail the startup of the basic operations of the server, ranging from log collection to analysis. This step is one of the most critical for imparting a real-time monitoring and threat detection attributes within your cybersecurity environment.

```
Wazuh - VMware Workstation
File Edit View VM Tabs Help
Home X Debian 7.x 64-bit X Wazuh X
[ 768.268768] e1000 0000:02:00:0 eth0: Reset adapter
[ 774.446871] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: N
one

[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.130 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::20c:29ff:feda:18a6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:da:18:a6 txqueuelen 1000 (Ethernet)
    RX packets 584 bytes 43990 (42.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 551 bytes 39454 (38.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5765 bytes 552515 (539.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5765 bytes 552515 (539.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[wazuh-user@wazuh-server ~]$
```

Figure-2 Loading server

## 2. Dashboard Setup and Agent Deployment

Description: This section explains setting up the Wazuh Dashboard and deploying agents for monitoring.

The next section starts with this Wazuh Dashboard configuration that makes it possible centralized monitoring ending. Moreover, it illustrates the particular techniques needed in deploying agents for the whole extended network which guarantees complete cyber security logs.

Steps:

### 2.1 Getting Dashboard by IP

Description: Access the Wazuh Dashboard using the server's IP address.

Wazuh Dash board required to start it using server's IP addresses, which allows the users to detect the security events and manage the system configuration. This approach is especially suitable for the realization of early conflict prevention benefiting the user in terms of streamlined interaction with the dashboard for improved security governance.

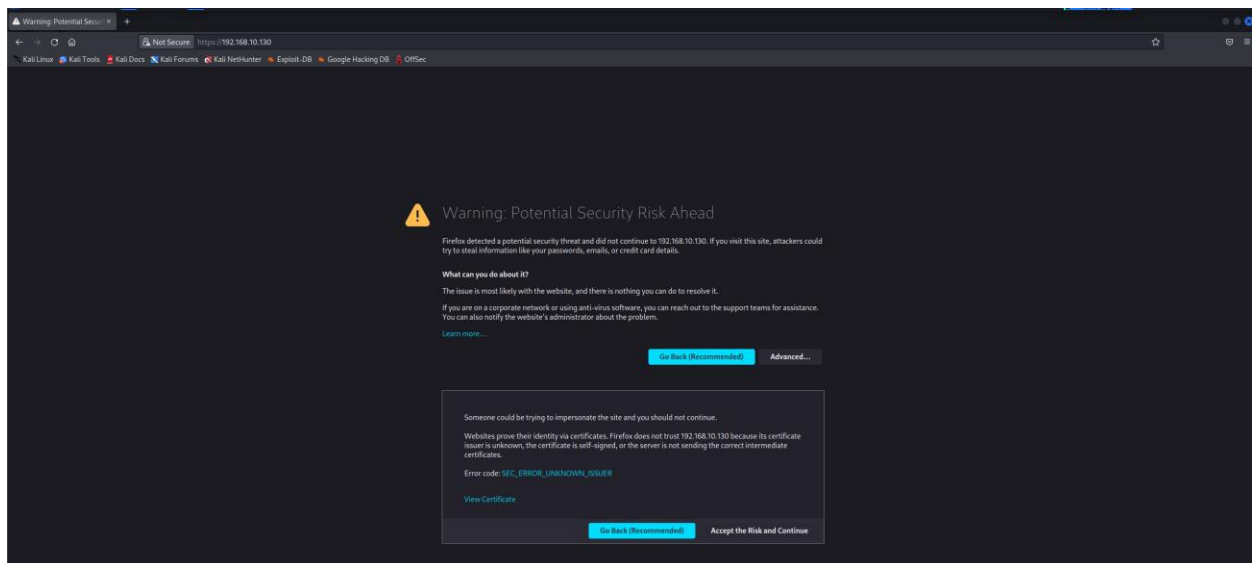


Figure-3 Web Interface

### 2.2 Login to Server

Description: Log in to the Wazuh Server Dashboard.

Access the Wazuh Server Dashboard by entering your credentials, and use a definitely powerful security monitoring and management functions tool.

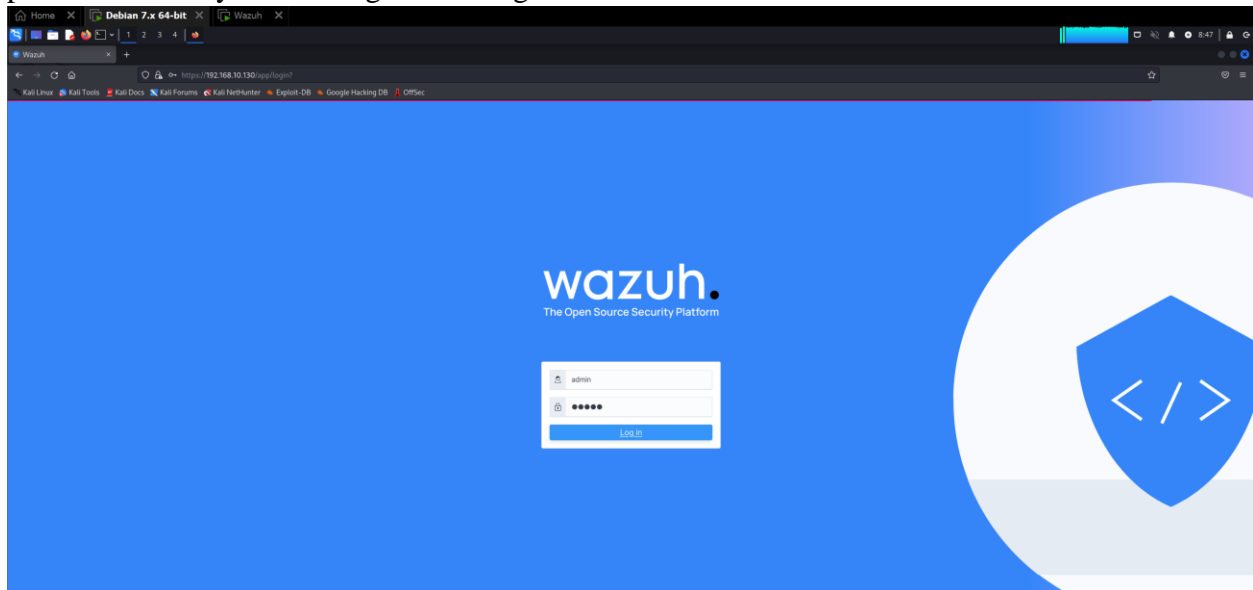


Figure-4 Login

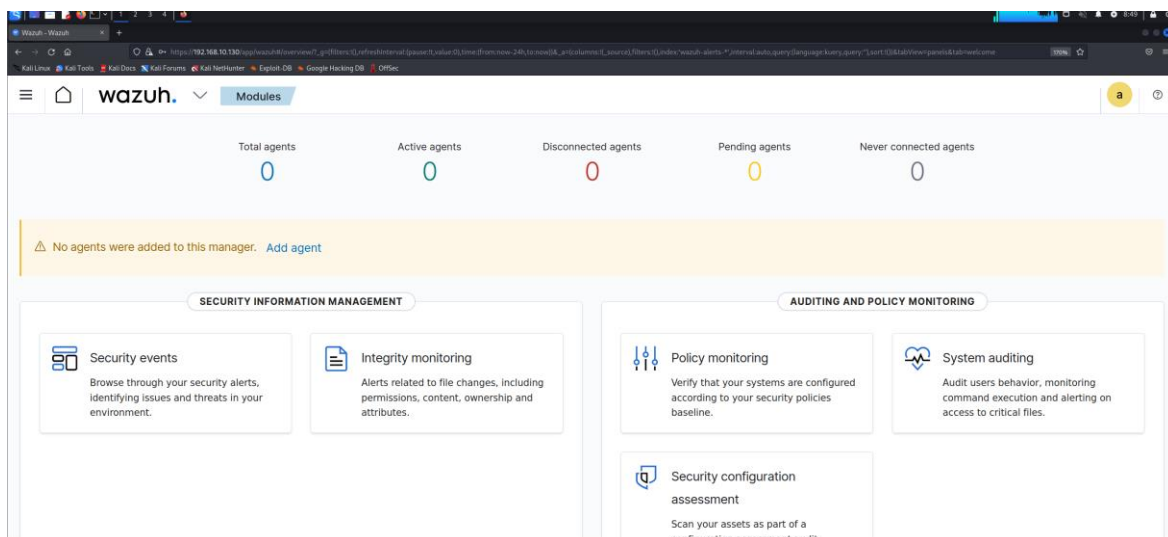


Figure-5 Dashboard

## Dashboard Setup and Agent Deployment

### 2.3 Deploying New Agent

Description: Deploy a new agent for monitoring purposes.

Deploy a new agent to make bigger tracking competencies, enhancing security posture and risk detection throughout the community.

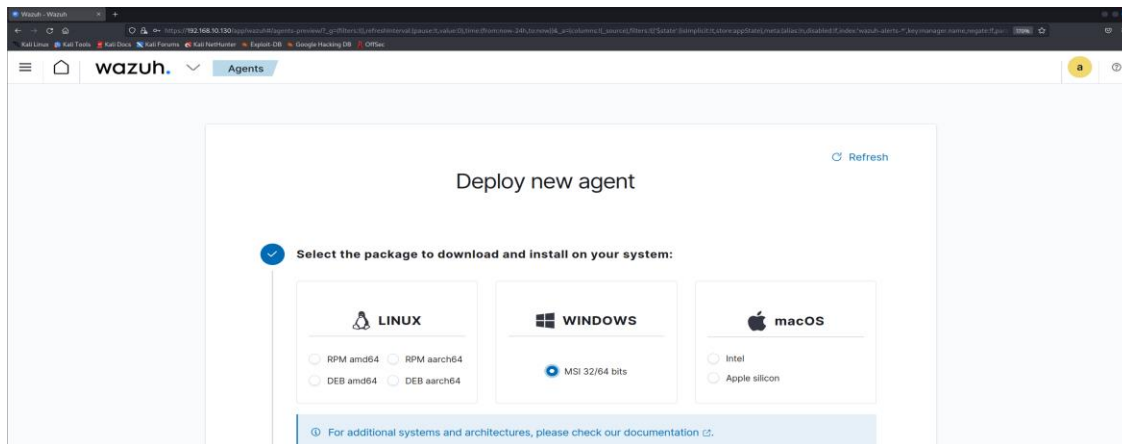


Figure-6 Adding Agent

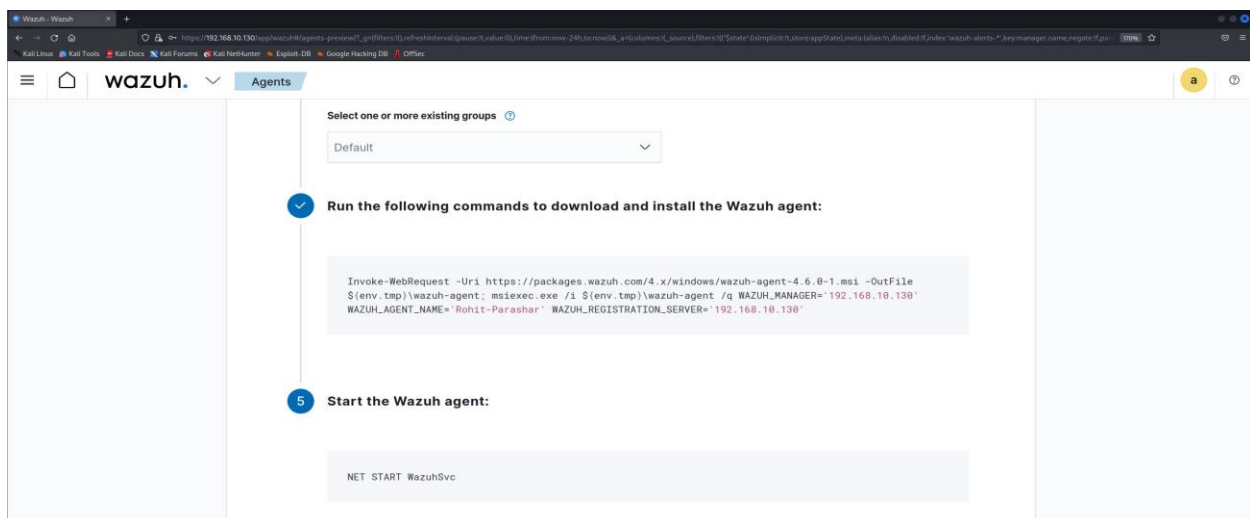


Figure-7 Adding Agent

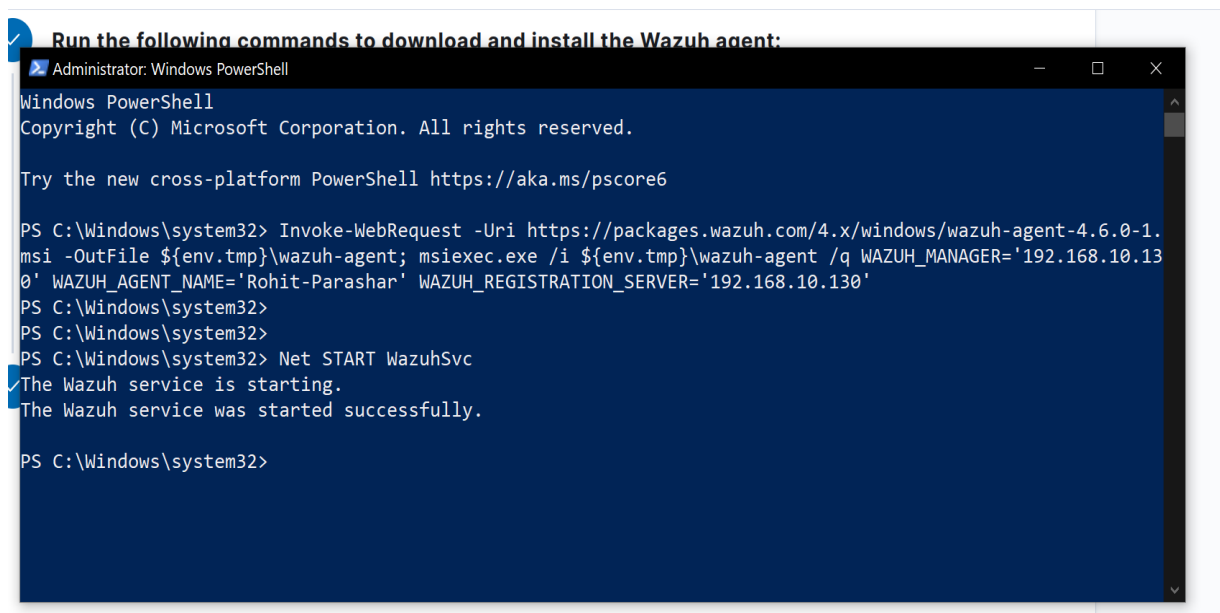


Figure-8 Commands Run

## 2.4 Dashboard Detections

Description: View detections on the Dashboard.

View and analyze protection detections without delay inside the Wazuh Dashboard, providing insights into capacity threats and gadget vulnerabilities at a look.

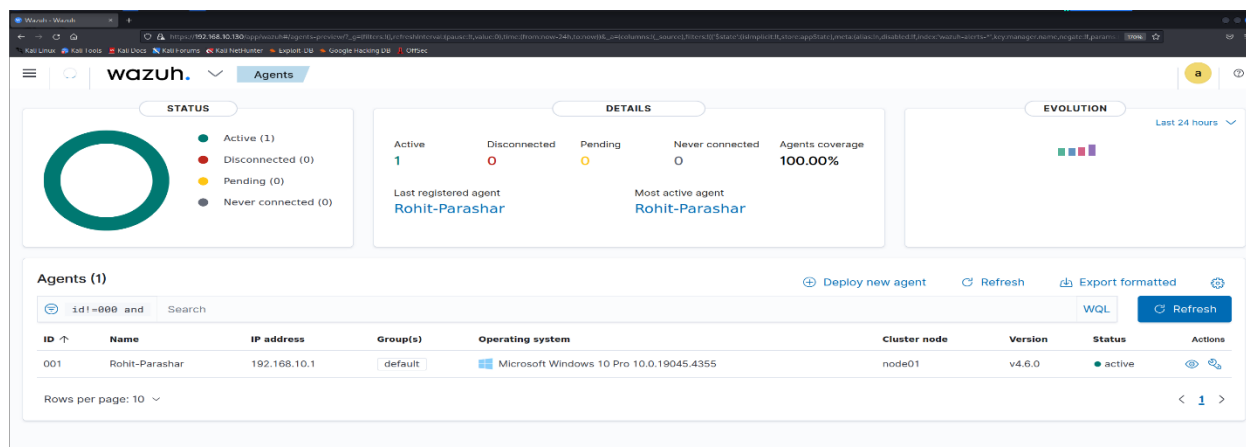


Figure- 9 Agent

## 3. File Integrity Monitoring Configuration

Description: This section covers configuring File Integrity Monitoring (FIM) in Wazuh.

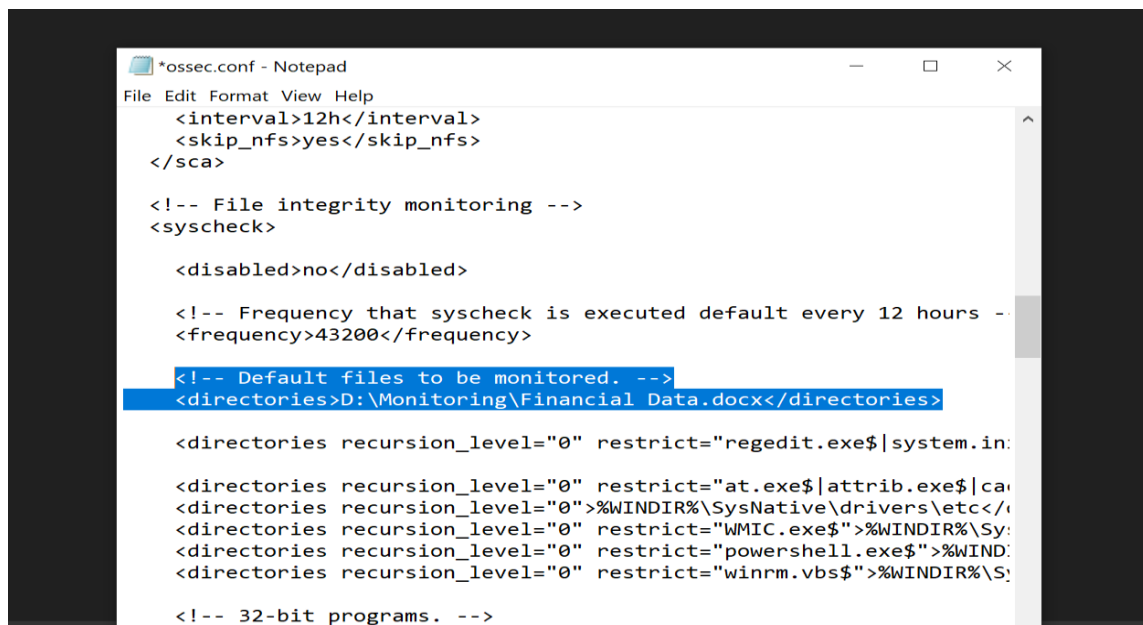
This section guides users thru the setup and configuration of File Integrity Monitoring (FIM) within the Wazuh security platform, ensuring sturdy file integrity tests for enhanced safety posture.

Steps:

### 3.1 Configurations Edit

Description: Edit configuration files to enable FIM.

The files, config. Txt included are responsible for the File Integrity Monitoring (FIM) within the Wazuh setup, which is a proactive tool for detecting unauthorized manipulations in the files and directories used to manage the Wazuh environment..



```
*ossec.conf - Notepad
File Edit Format View Help
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>

<!-- 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>D:\Monitoring\Financial Data.docx</directories>

  <directories recursion_level="0" restrict="regedit.exe$|system.in:
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|ca
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</i
  <directories recursion_level="0" restrict="WMIC.exe$" >%WINDIR%\Sy:
  <directories recursion_level="0" restrict="powershell.exe$" >%WIND:
  <directories recursion_level="0" restrict="winrm.vbs$" >%WINDIR%\S:

  <!-- 32-bit programs. -->
```

Figure-10 Configurations

### 3.2 Activating Services

Description: Activate FIM services.

From the Dashboard we can start the services such as virus total to integrate logs for virus total tool and File Integrity Monitoring.



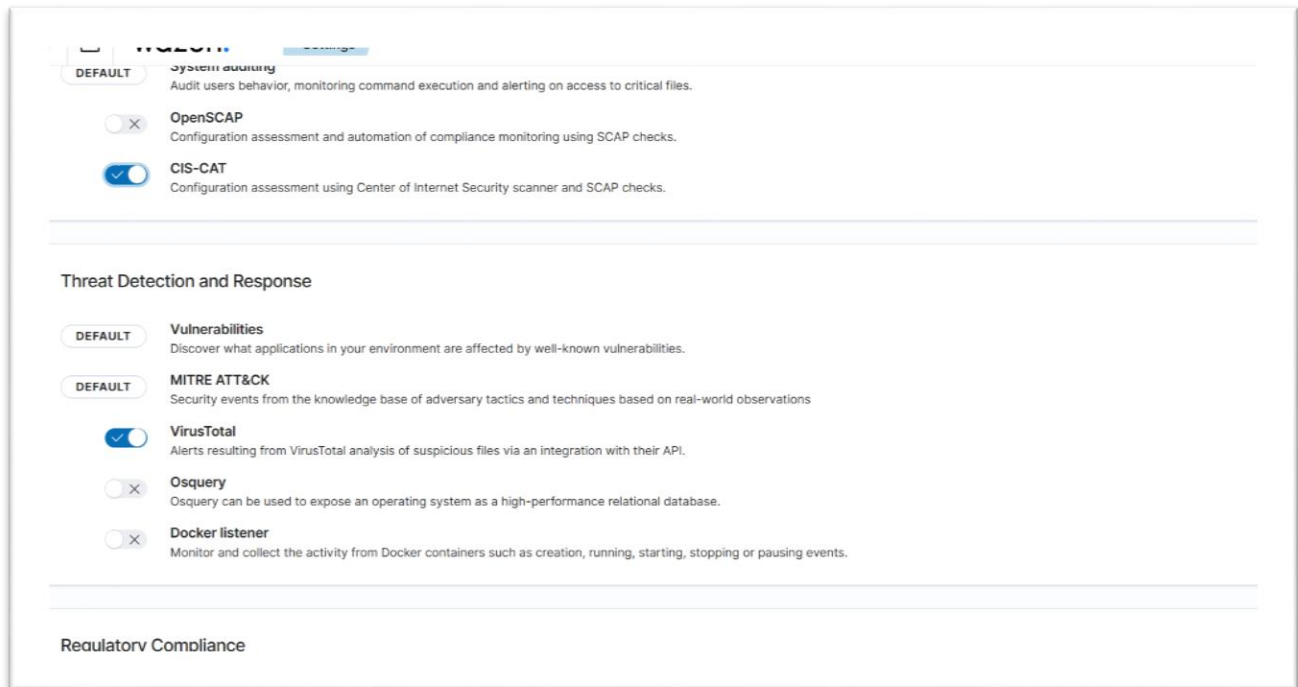


Figure-11 turn on service

### 3.3 Configurations Changes

Description: Make necessary changes to configurations.

Activate FIM offerings from the Dashboard, which means the integration with external offerings as well as the ones provided by VirusTotal will be used for more detailed log analysis and a better understanding of the risks. Then, carry critical configuration modifications in order to fine tune parameters and settings in line with the specific security requirements and organizational preferences. In advance, be sure that FIM options are already activated otherwise they will not be used by FIM and VirusTotal during log analysis as well as threat intelligence aggregation. On top of that, define the vital settings for personal configuration that are going to be adapted to the environment and the business models with different security needs.

```

<synchronization>|
  <max_eps>10</max_eps>
</synchronization>
</wodle>

<!-- CIS policies evaluation -->
<wodle name="cis-cat">
  <disabled>no</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>

  <java_path>\\server\jre\bin\java.exe</java_path>
  <ciscat_path>C:\cis-cat</ciscat_path>
</wodle>

<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <bin_path>C:\Program Files\osquery\osqueryd</bin_path>
  <log_path>C:\Program Files\osquery\log\osqueryd.results.log</log_p
  <config_path>C:\Program Files\osquery\osquery.conf</config_path>

```

Figure-12 Configuration

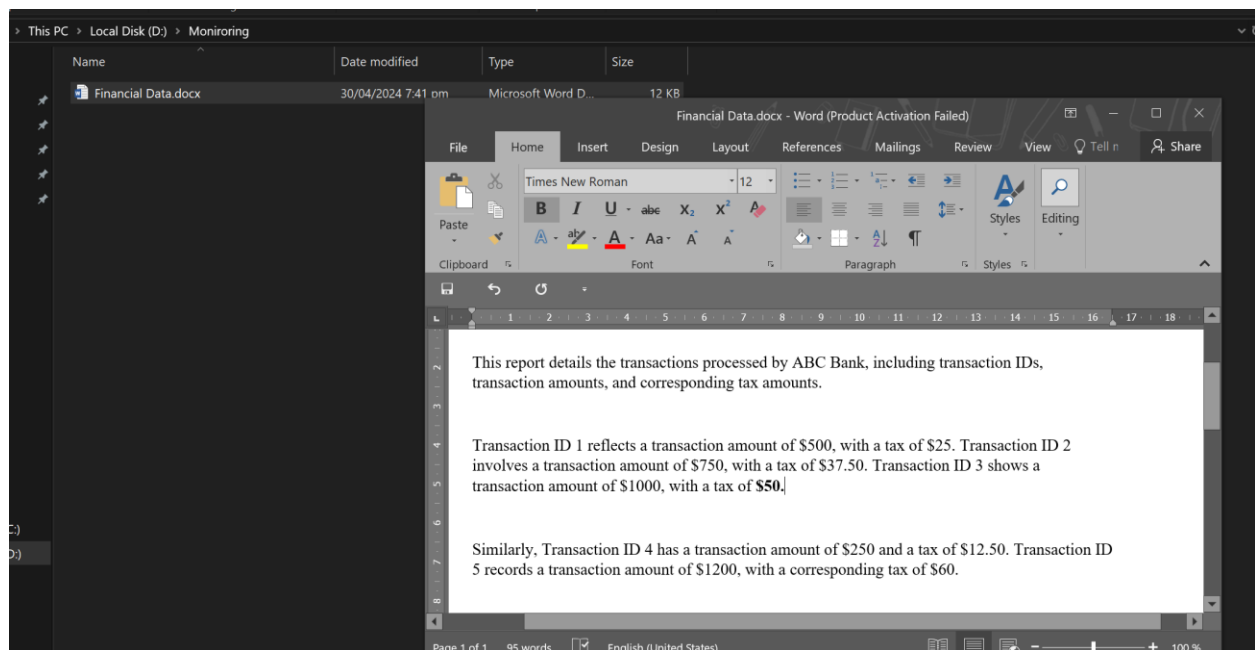


Figure-13 Compromising Integrity

### 3.4 Dashboard Detections

Description: View FIM detections on the Dashboard.

Log in to the Wazuh console to visualize and analyze File Integrity Monitoring (FIM) detections for confirming that purposeful changes and potential compromises in critical assets have been detected in real time. This effectively helps security forces recognize individuals of concern and ensures incidences of threats are responded to appropriately in pursuit of safety all-round.

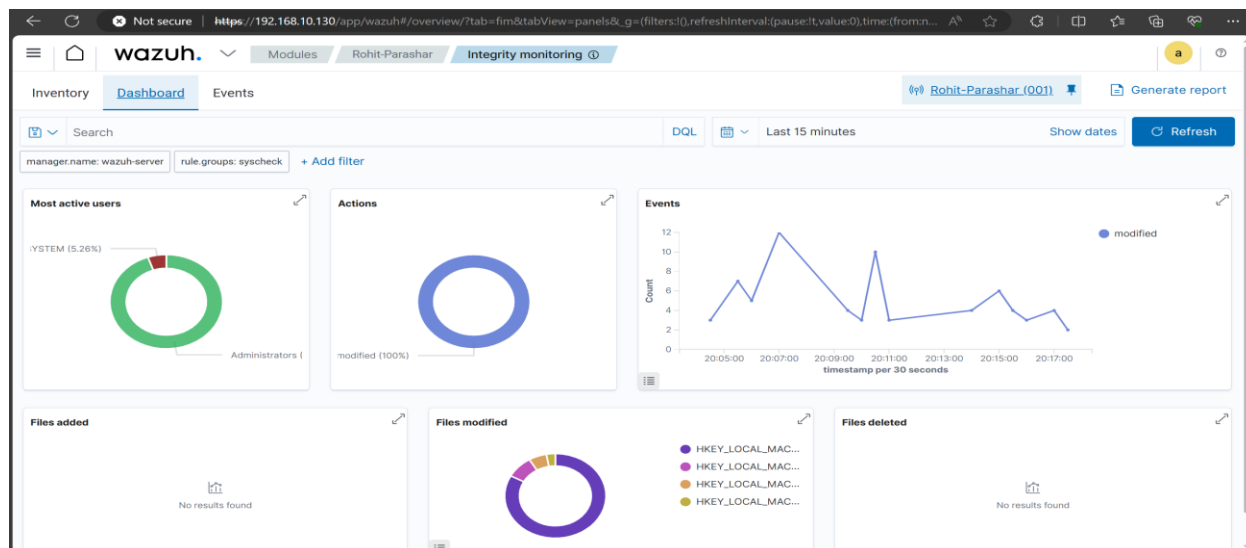


Figure-14 Dashboard

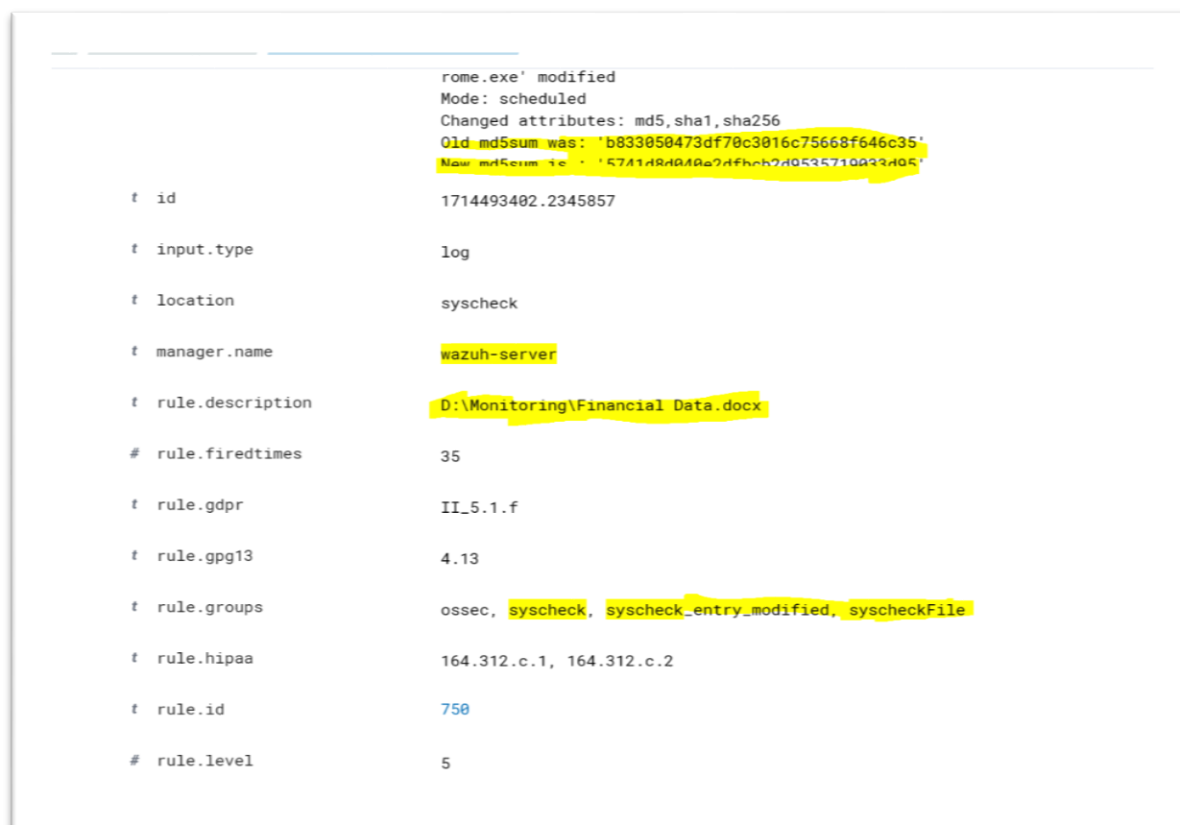


Figure-15 Logs generation

## 4. Integrating Wazuh with Virus Total

Description: This section guides through integrating Wazuh with Virus Total for enhanced threat analysis.

This section outlines the approach involved in the process of integrating Wazuh and Virus Total, with the latter's purpose being to enhance threat detection by pooling larger Threat Intelligence data logs with the threats that have been gathered using the former's resource for threat analysis. By setting up this integration, users can advantage deeper insights into ability threats detected by Wazuh, allowing greater informed choice-making and proactive risk mitigation strategies.

Steps:

### 4.1 Obtaining API Key

Description: Obtain an API key from the Virus Total website.

To acquire an API key from the VirusTotal website, users want to navigate to the VirusTotal internet site and create an account in the event that they haven't already. Once logged in, they can access the API segment and generate an API key, on the way to be used to authenticate and allow the integration between Wazuh and VirusTotal.

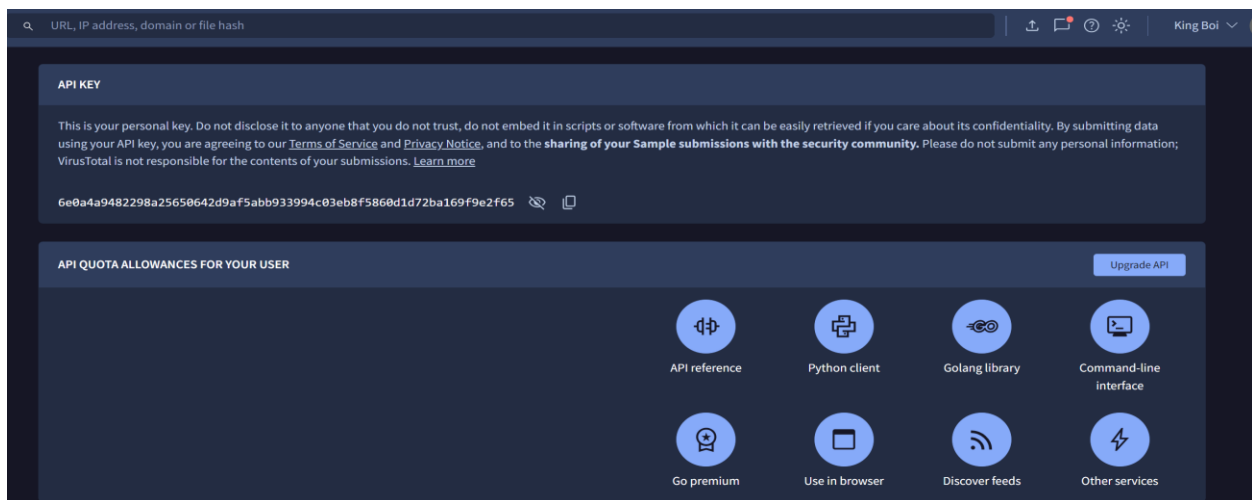


Figure-15 Virus total API

### 4.2 Editing Configuration for Integration

Description: Modify configurations to integrate with Virus Total.

To combine with VirusTotal, customers ought to adjust configuration documents inside Wazuh, usually specifying the acquired API key and associated settings. These changes enable seamless communicate between Wazuh and VirusTotal, empowering better threat analysis and intelligence collecting.

```

<max_eps>>0</max_eps>

<!-- Database synchronization settings -->
<synchronization>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <max_eps>10</max_eps>
</synchronization>
<integration>
  <name>virustotal</name>
  <api_key>6e0a4a9482298a25650642d9af5abb933994c03eb8f5860d1d72ba169f9e2f65</api_key> <!-- Replace with your VirusTotal API key -->
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
</syscheck>

<!-- System inventory -->

```

Figure-16 Edit Configurations

### 4.3 Detections

Description: View detections with Virus Total integration.

The users can see this detection through the VirusTotal feature by login into the Wazuh dashboard and going to the "Detections" section. An interface that will present Wazuh detections with accompanied information from VirusTotal will be crafted. Through the enriched data, they can closely examine the detected threats connected to the relevant metadata and threat detection provided by the VirusTotal system that helps enhance the actions for threat response.

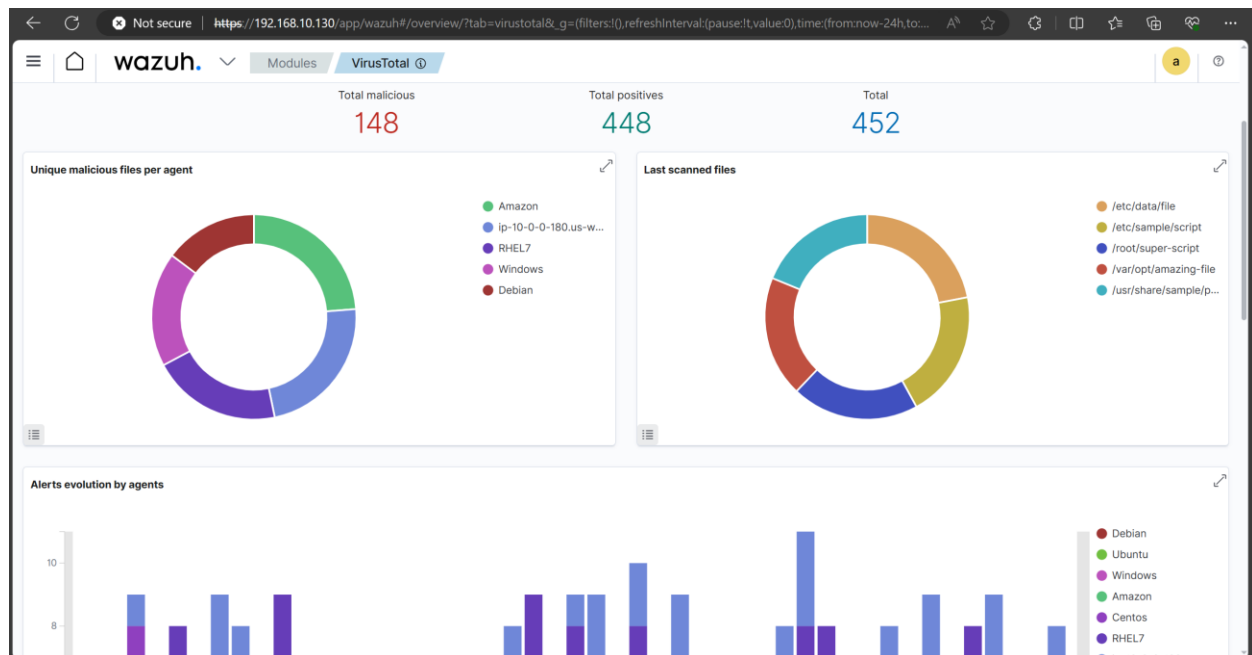


Figure-17 Detection

### 4.4 Testing Results

### Description: Test the integration and review the results.

The scenario will be put to a test by simply simulating a security event or by importing historic data to the Wazuh Dashboard for analysis. Detection needs to be confirmed that they are enhanced with information from VirusTotal, which is possible for a smooth integrations and improve analytics of threat. Besides, if the integration turns out to be a success, evaluation phase should include the examination of how relevant the shared threat intelligence was and if the whole data was available.

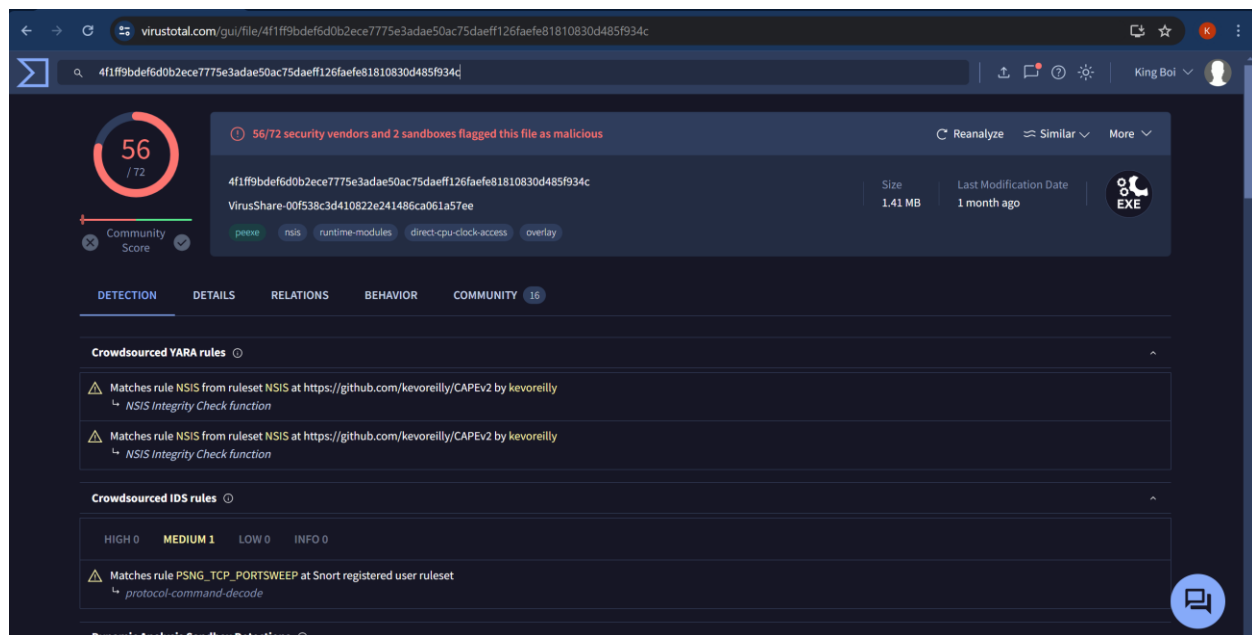


Figure-18 Analyzing

## 4.5 Same Hash Detected

### Description: Identify and handle detections with matching hashes.

To monitor detections with identical hashes within its ecosystem, users can employ a security simulation or import any historical data into Wazuh Dashboard display for evaluation. They should make sure that detections include the information from VirusTotal and as that is the case, Virus Total API will be integrated with threat analytics for data enrichment using threat intelligence. As for evaluation, it is important to check what exactly is more relevance and that it is really no necessary information to measure the quality of the shared intelligence.

Table	JSON
@sampledata	true
_index	wazuh-alerts-4.x-sample-threat-detection
agent.id	006
agent.ip	207.45.34.78
agent.name	Windows
cluster.name	wazuh
data.virustotal.found	1
data.virustotal.malicious	1
data.virustotal.permalink	<a href="https://www.virustotal.com/gui/file/1bbf37332af75ea682fb4523afc8e61adb22f47f2bf3a8362e310f6d33085a6e/de">https://www.virustotal.com/gui/file/1bbf37332af75ea682fb4523afc8e61adb22f47f2bf3a8362e310f6d33085a6e/de</a>
data.virustotal.positives	12
data.virustotal.scan_date	2024-04-30T16:30:44.782Z
data.virustotal.source.alert_id	2476782495.1248979
data.virustotal.source.file	/root/super-script
data.virustotal.source.md5	b66a7367764866c7f2ae2db2e181722a

Figure-19 Detection Logs

## 5. File Integrity Monitoring Mitigation Methods

File integrity monitoring methods of the mitigation in particular are for the prevention of alterations of system data created without authorization. Through regular file integrity checking, setting proper permissions right and enabling continuous monitoring, organizations can build up their security posture and reduce the ability of security compromises to get through their mechanisms. Moreover, these combined efforts with centralized logging, encryption, and user training, build a holistic method to the problem as unauthorized file modifications can be avoided and information can be protected.

### Conclusions

The Task tells a well-structured and useful instruction for setting up and deploying the Wazuh security platform. It provides with workarounds from loading the OVA server file to file integrity monitoring and integration with VirusTotal for better threat analyzation. By following the mentioned simple steps, users are able to conveniently set the Wazuh, manage the agents, monitor the security detection as well as have access to various external intelligence sources. This structured approach helps in enforcing strong cyber security measures and ultimately the organizations to identify and close down the weaknesses before they are exploited by attackers.

## **References:**

- 1- Stanković, S., Gajin, S. and Petrović, R., 2022. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. No Nama Agent Integrity File Added Delete Modified, 1.
- 2- Suryantoro, T., Purnomosidi, B.D. and Andriyani, W., 2022, December. The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods. In 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) (pp. 1-6). IEEE.
- 3- Gómez Vidal, A.S., 2019. Improvements in IDS: adding functionality to Wazuh (Bachelor's thesis).
- 4- Srivastava, P. and Seludkar, K., 2023. Implementation of an Intrusion Detection System and Deception Technologies using Open Source Tools for Small Businesses. In Implementing Enterprise Cyber Security with Open-Source Software and Standard Architecture: Volume II (pp. 151-191). River Publishers.