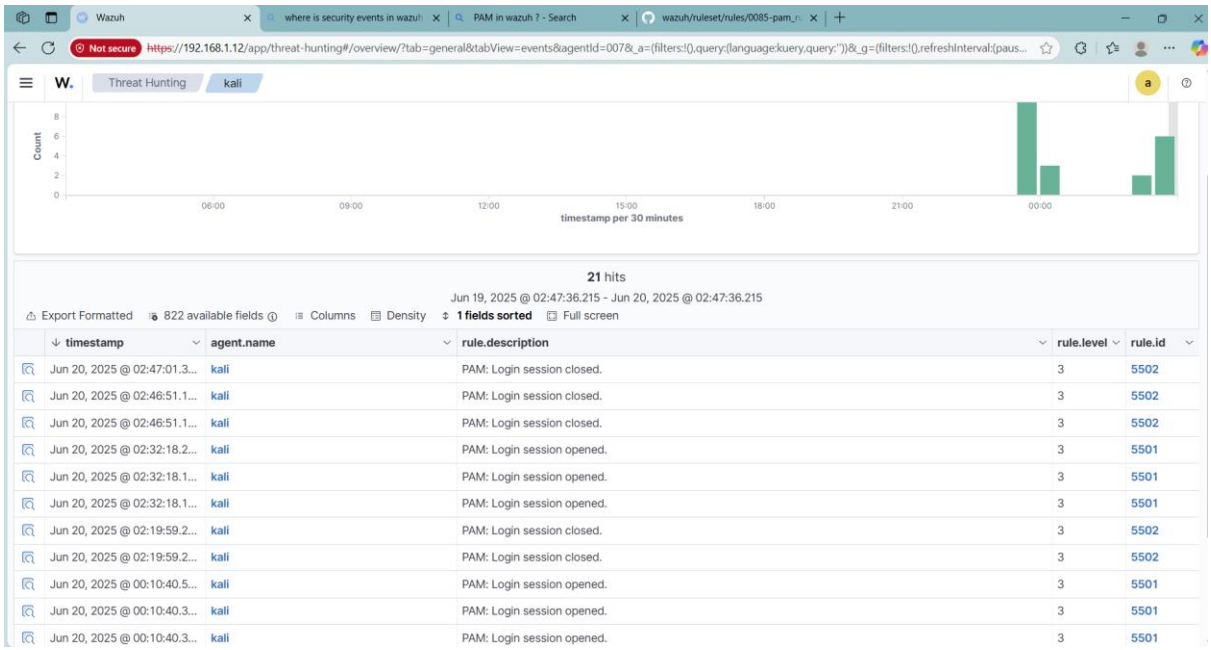
Wazuh Log Analysis and File Integrity Monitoring Guide

-R M NAREN ADITHYA

4. Log Analysis

Step 1: View SSH Logs

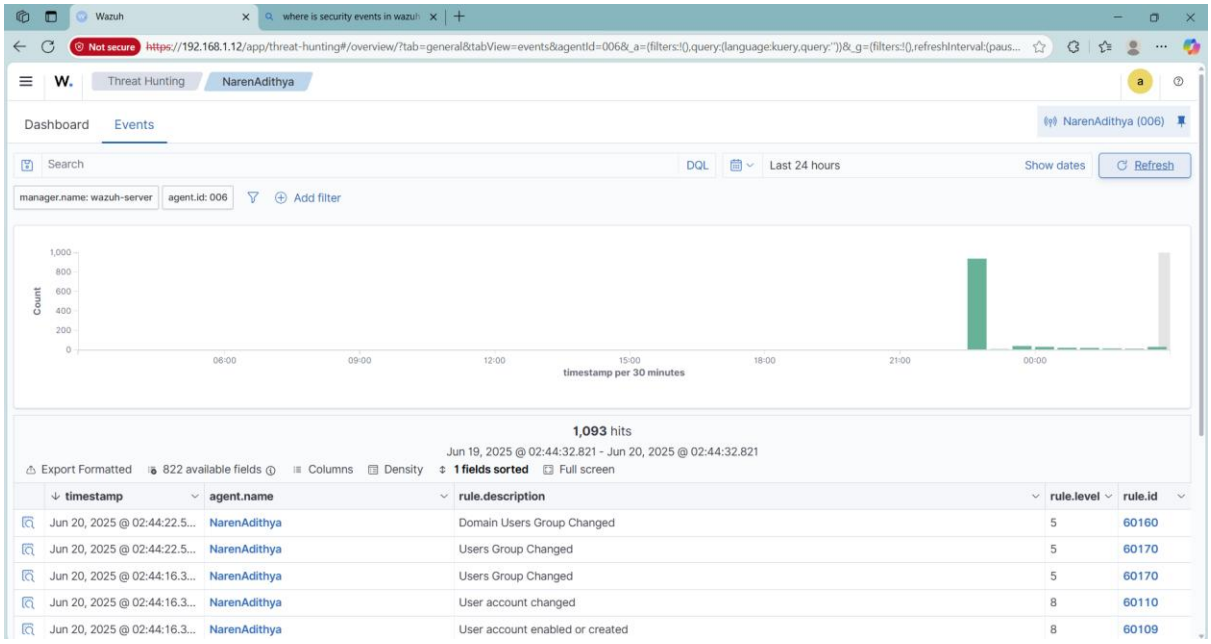
1. **Access Wazuh Dashboard**:
    - Log in to the Wazuh dashboard at https://<your-server-ip>:5601.
2. **Navigate to Security Events**:
    - Go to the "Security Events" module under the Wazuh app.
3. **Filter for SSH Logs**:
    - In the search bar, use a query like rule.groups:authentication AND data.srcip:* to filter SSH-related events.
4. **Review Logs**:
    - Examine details such as source IP, username, and timestamp for each SSH event.

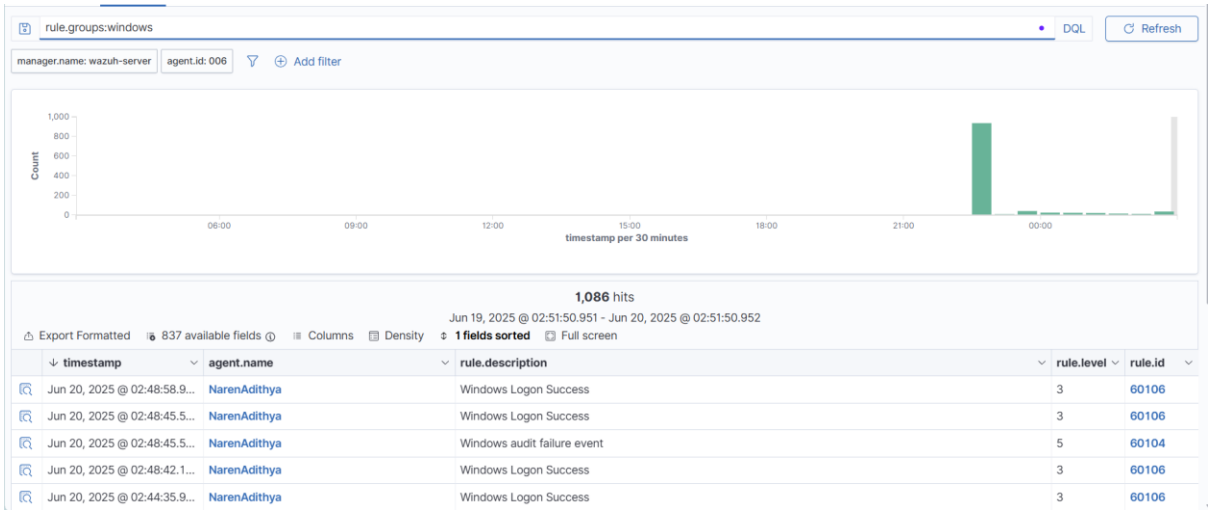


Step 2: View Windows Event Logs

1. **Select Windows Agent**:
    - In the Wazuh dashboard, go to the "Agents" tab and select a Windows agent.
2. **Navigate to Security Events**:
    - Click on the "Security Events" module for the selected agent.

3. **Filter Windows Events**:
    - Use a query like agent.os.platform:windows AND rule.groups:windows to display Windows Event Logs.
4. **Analyze Details**:
    - Review event details, including user, event ID, and description.

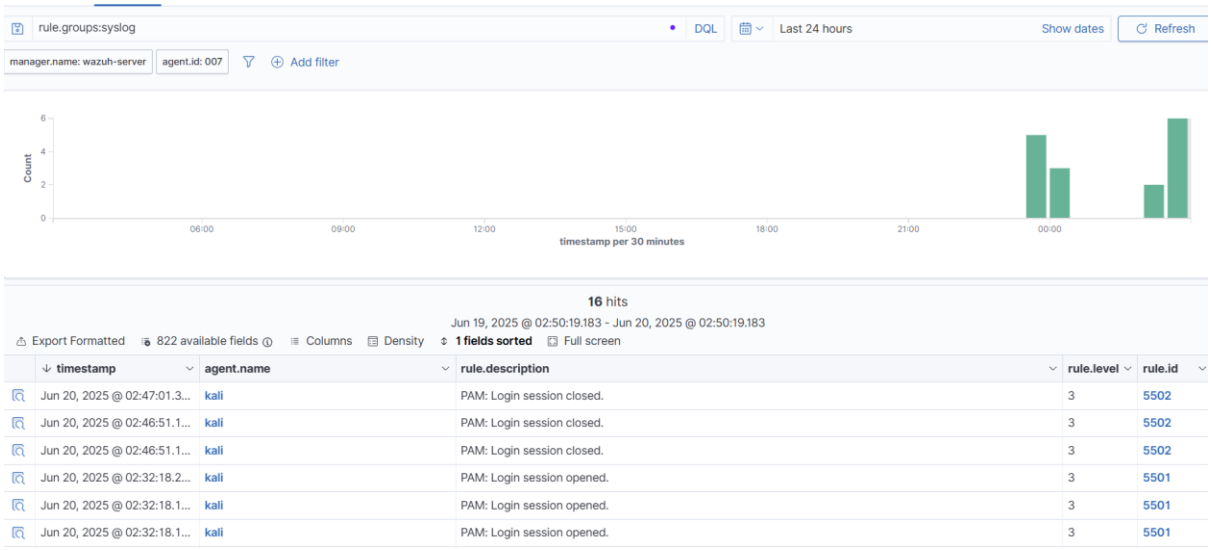




Step 3: View System Logs

1. **Select Linux Agent**:
    - In the dashboard, go to the "Agents" tab and select a Linux agent.
2. **Navigate to Security Events**:
    - Access the "Security Events" module for the agent.

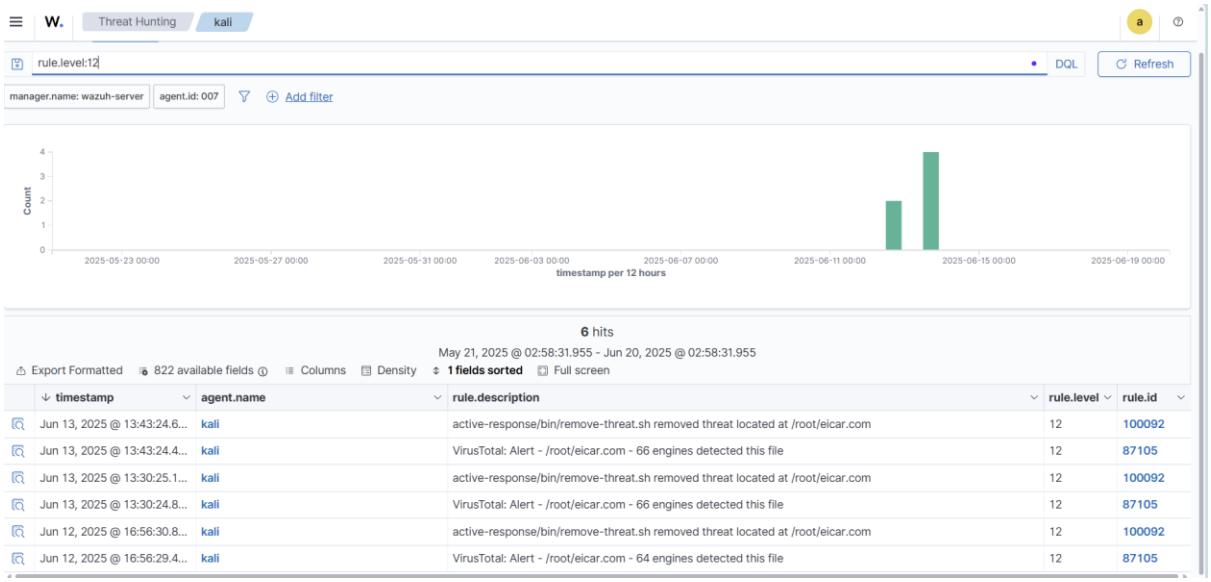
3. **Filter System Logs**:
    - Use a query like agent.os.platform:linux AND rule.groups:syslog to filter system logs.
4. **Review Entries**:
    - Check details such as process name, log message, and timestamp.



timestamp	agent.name	rule.description	rule.level	rule.id
Jun 20, 2025 @ 02:47:01.3...	kali	PAM: Login session closed.	3	5502
Jun 20, 2025 @ 02:46:51.1...	kali	PAM: Login session closed.	3	5502
Jun 20, 2025 @ 02:46:51.1...	kali	PAM: Login session closed.	3	5502
Jun 20, 2025 @ 02:32:18.2...	kali	PAM: Login session opened.	3	5501
Jun 20, 2025 @ 02:32:18.1...	kali	PAM: Login session opened.	3	5501
Jun 20, 2025 @ 02:32:18.1...	kali	PAM: Login session opened.	3	5501

Step 4: Filter Alerts by Rule Level and Rule Groups

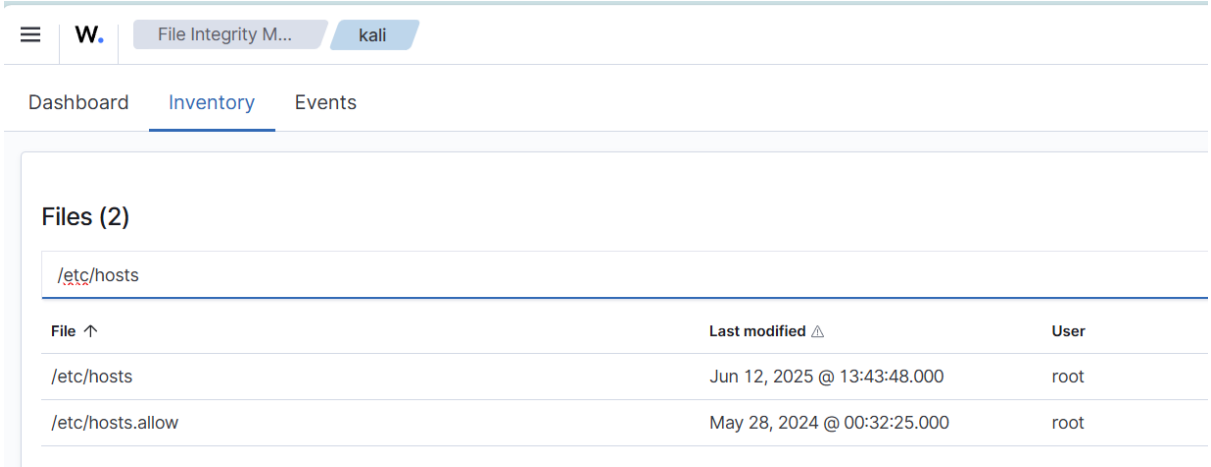
1. **Access Security Events**:
    - Navigate to the "Security Events" module in the Wazuh dashboard.
2. **Filter by Rule Level**:
    - Use a query like rule.level:>7 to show high-severity alerts (level 8 or above).
    - Adjust the level as needed
3. **Review Alerts**:
    - Analyze the filtered alerts for patterns or critical events.



5. File Integrity Monitoring (FIM)

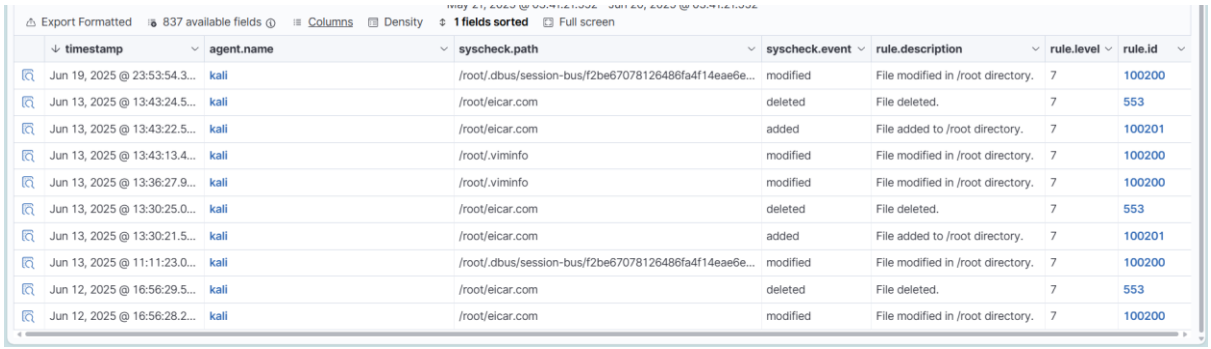
Step 1: Configure FIM on Sensitive Directories

1. **Edit Agent Configuration**:
    - On the Wazuh manager, edit the agent configuration file /var/ossec/etc/ossec.conf or use centralized configuration via the dashboard.
2. **Add FIM Directory**:
    - Add a directory to monitor, such as /etc or C:\Program Files for Windows. Example configuration:
    - <syscheck>
    - <directories check_all="yes" realtime="yes">/etc</directories>
    - </syscheck>
3. **Verify Configuration**:
    - In the Wazuh dashboard, go to the "File Integrity Monitoring" module to confirm the directory is monitored.



Step 2: Trigger an Alert by Modifying a File

1. **Check FIM Alerts**:
    - In the Wazuh dashboard, navigate to the "File Integrity Monitoring" module.
    - Look for an alert indicating the file modification, including details like file path, timestamp, and change type.
2. **Review Alert Details**:
    - Click the alert to view specifics, such as the modified content or checksum.



Export Formatted | 837 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jun 19, 2025 @ 23:53:54.3...	kali	/root/.dbus/session-bus/f2be67078126486fa4f14eae6e...	modified	File modified in /root directory.	7	100200
Jun 13, 2025 @ 13:43:24.5...	kali	/root/eicar.com	deleted	File deleted.	7	553
Jun 13, 2025 @ 13:43:22.5...	kali	/root/eicar.com	added	File added to /root directory.	7	100201
Jun 13, 2025 @ 13:43:13.4...	kali	/root/.viminfo	modified	File modified in /root directory.	7	100200
Jun 13, 2025 @ 13:36:27.9...	kali	/root/.viminfo	modified	File modified in /root directory.	7	100200
Jun 13, 2025 @ 13:30:25.0...	kali	/root/eicar.com	deleted	File deleted.	7	553
Jun 13, 2025 @ 13:30:21.5...	kali	/root/eicar.com	added	File added to /root directory.	7	100201
Jun 13, 2025 @ 11:11:23.0...	kali	/root/.dbus/session-bus/f2be67078126486fa4f14eae6e...	modified	File modified in /root directory.	7	100200
Jun 12, 2025 @ 16:56:29.5...	kali	/root/eicar.com	deleted	File deleted.	7	553
Jun 12, 2025 @ 16:56:28.2...	kali	/root/eicar.com	modified	File modified in /root directory.	7	100200

Also, I have added a trigger situation for a malicious file, which gets detected using virus total, also removing the malicious file with a help of a bash script.