

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:

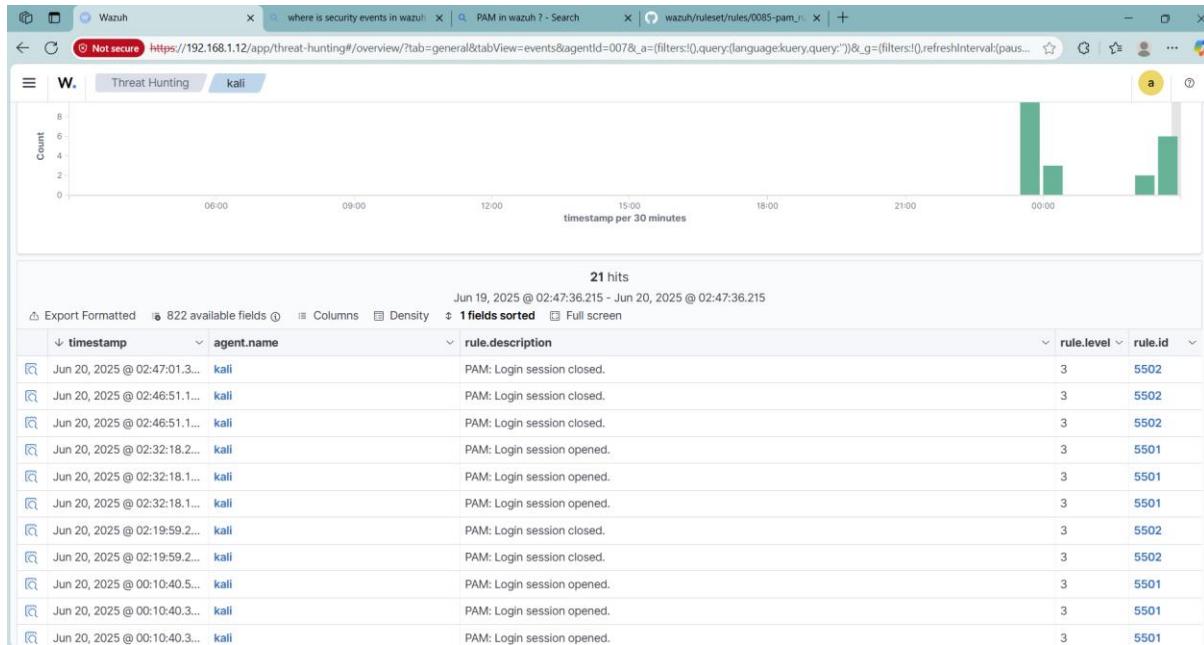
- Go to the "Security Events" module under the Wazuh app.

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:

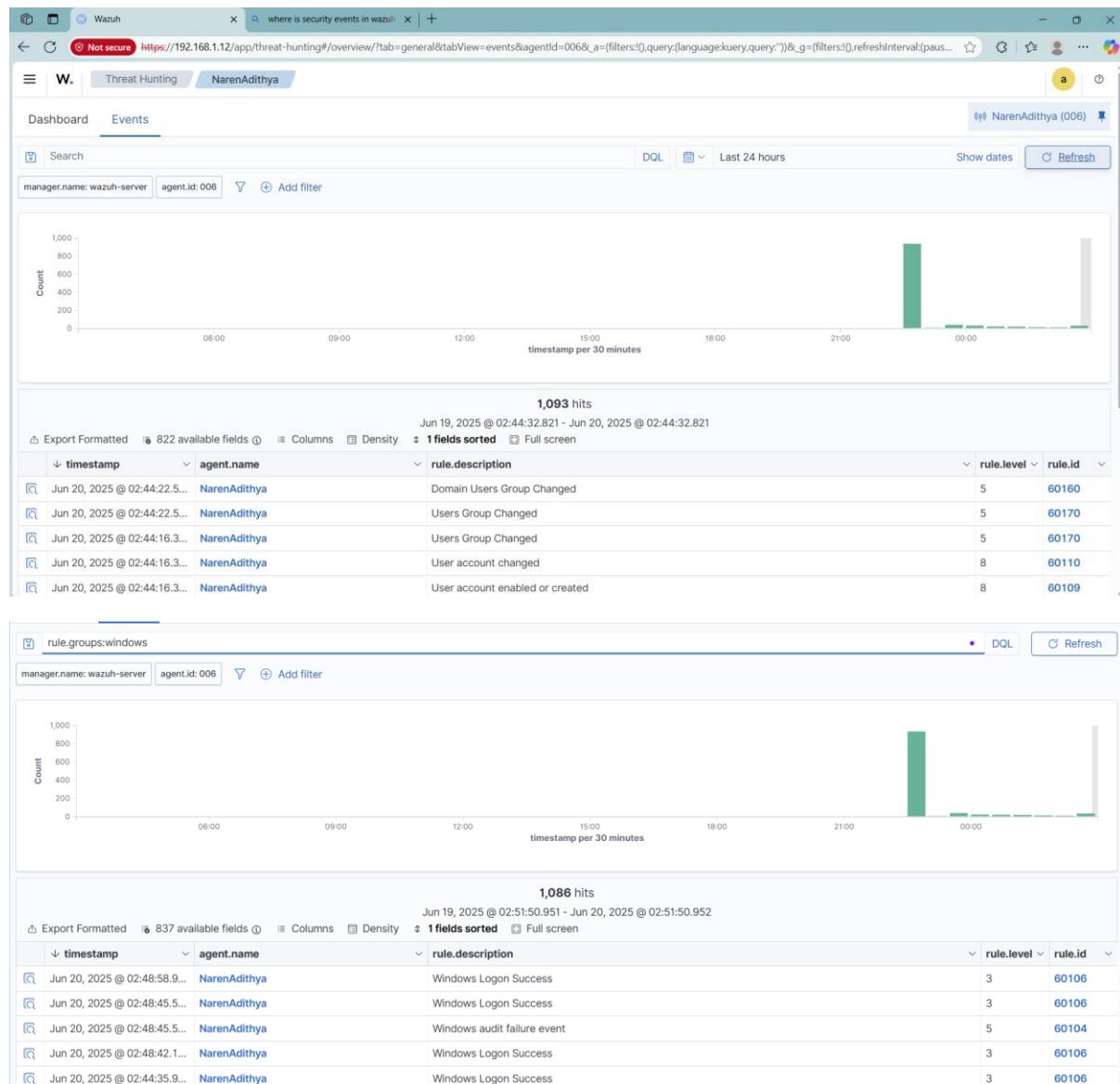
- Click on the "Security Events" module for the selected agent.

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:

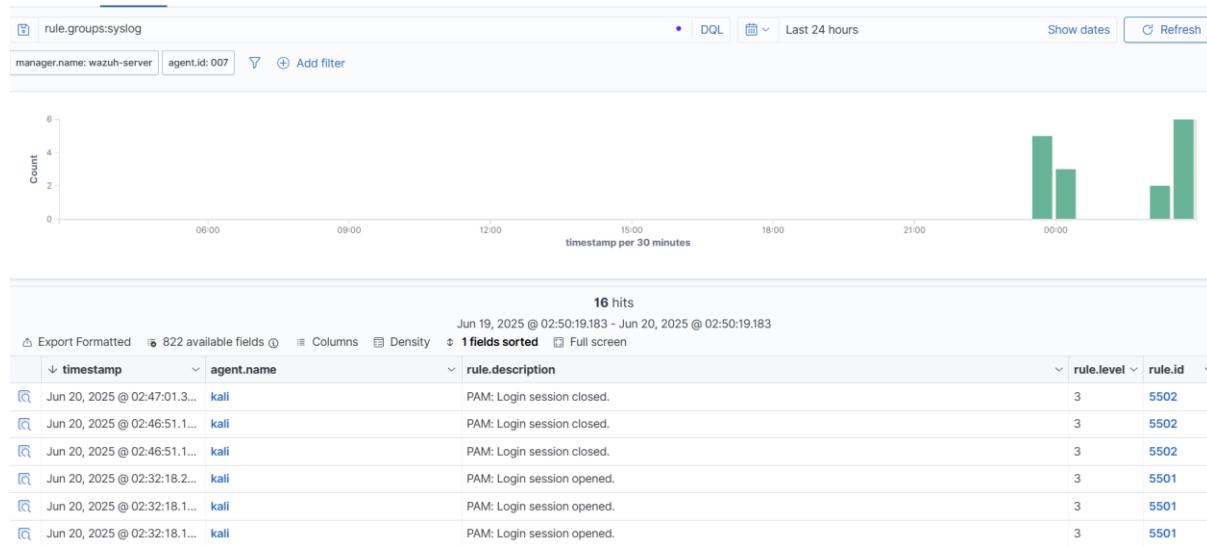
- Access the "Security Events" module for the agent.

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.



Step 4: Filter Alerts by Rule Level and Rule Groups

1. Access Security Events:

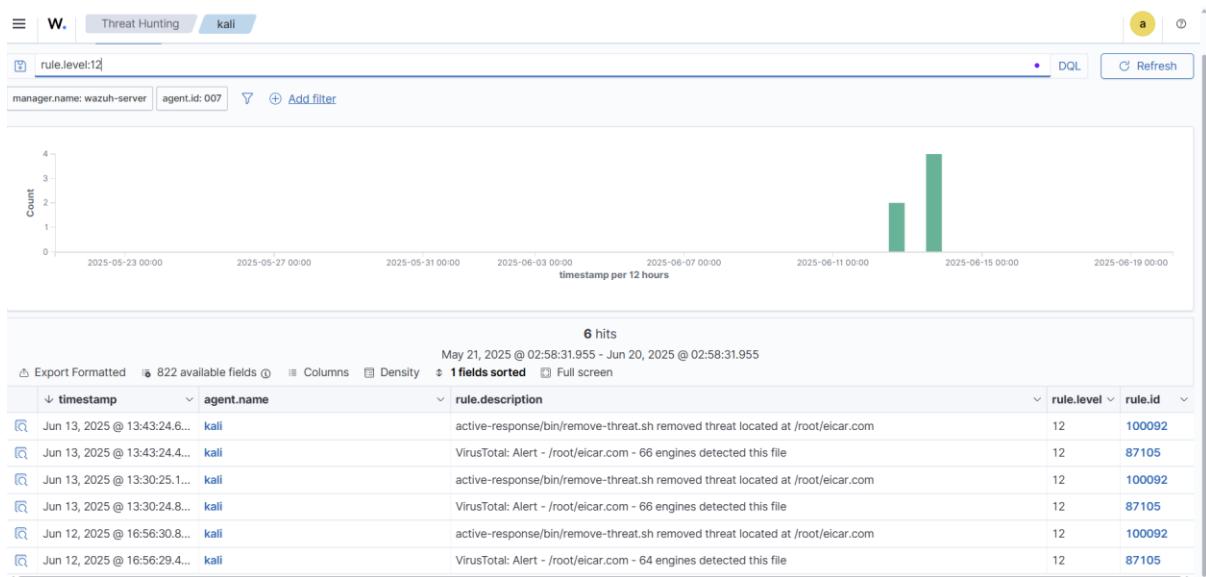
- Navigate to the "Security Events" module in the Wazuh dashboard.

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.

The dashboard shows a table of monitored files under the 'Files (2)' section. The table has columns: File, Last modified, and User.

File	Last modified	User
/etc/hosts	Jun 12, 2025 @ 13:43:48.000	root
/etc/hosts.allow	May 28, 2024 @ 00:32:25.000	root

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.

File Integrity Monitoring Alerts						
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/elcar.com	deleted	File deleted.	7	553
Jun 13, 2025 @ 13:43:22.5...	kali	/root/elcar.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/elcar.com	deleted	File deleted.	7	553
Jun 13, 2025 @ 13:30:21.5...	kali	/root/elcar.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/elcar.com	deleted	File deleted.	7	553
Jun 12, 2025 @ 16:56:28.2...	kali	/root/elcar.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.

The screenshot shows the Wazuh Threat Hunting interface. At the top, there are tabs for 'W.' (selected), 'Threat Hunting' (highlighted in blue), and 'kali'. Below the tabs, there are sections for 'Dashboard' and 'Events'. A search bar contains the query 'rule.id:(553 OR 554 OR 550 OR 87105 OR 100200 OR 100201 OR 100092 OR 100093)'. To the right of the search bar are buttons for 'DQL', 'Last 24 hours', 'Show dates', and 'Refresh'. Below the search bar, there are filters for 'manager.name: wazuh-server' and 'agent.id: 007'. A 'Add filter' button is also present. The main area features a histogram titled 'Count' versus 'timestamp per 30 minutes', showing a single green bar at 15:00 with a value of 4. Below the histogram is a table titled '4 hits' with the following data:

4 hits						
Jun 11, 2025 @ 16:57:28.596 - Jun 12, 2025 @ 16:57:28.596						
Export Formatted 709 available fields Columns Density 1 fields sorted Full screen						
↓ timestamp	agent.name	rule.description	rule.level	rule.id		
Jun 12, 2025 @ 16:56:30.8...	kali	active-response/bin/remove-threat.sh removed threat located at /root/elcar.com	12	100092		
Jun 12, 2025 @ 16:56:29.5...	kali	File deleted.	7	553		
Jun 12, 2025 @ 16:56:29.4...	kali	VirusTotal: Alert - /root/elcar.com - 64 engines detected this file	12	87105		
Jun 12, 2025 @ 16:56:28.2...	kali	File modified in /root directory.	7	100200		