

Soosan Shabnam

21BCE0172

CYBERSECURITY ASSIGNMENT

TOPIC: Performing file integrity monitoring using WAZUH

GITHUB LINK: <https://github.com/soosan-shabnam/CYBERSECURITY-DA-21BCE0172>

Introduction

File Integrity Monitoring (FIM) is a crucial security process that ensures the integrity of files and systems within an organization's IT infrastructure. As cyber threats evolve, the need for robust monitoring solutions becomes paramount. FIM helps in detecting unauthorized changes to critical system files, configurations, and data, allowing organizations to respond promptly to potential breaches or anomalies. One of the leading solutions for file integrity monitoring is Wazuh, an open-source security information and event management (SIEM) tool that provides comprehensive visibility and control over an organization's security posture. Wazuh leverages host-based agents to monitor file changes in real time, offering insights into file modifications, deletions, and creations across various platforms. This report delves into the implementation of file integrity monitoring using Wazuh, highlighting its functionalities, benefits, and best practices.

Detailed Description

Overview of Wazuh

Wazuh is a powerful open-source security platform that combines security monitoring, incident response, and compliance management. It is designed to provide comprehensive visibility into an organization's security landscape through real-time analysis of logs and alerts. Wazuh consists of three primary components: Wazuh agents, Wazuh manager, and Kibana for visualization. The agents are deployed on endpoints, the manager processes collected data and generates alerts, and Kibana provides a user-friendly interface for monitoring and analysis.

File Integrity Monitoring in Wazuh

File integrity monitoring in Wazuh is accomplished through the deployment of agents on the monitored systems. These agents track changes to specified files and directories using checksums and other integrity verification methods. When a monitored file is altered, created, or deleted, the Wazuh agent generates an alert that is sent to the Wazuh manager for further processing.

Key Features:

1. **Real-time Monitoring:** Wazuh agents continuously monitor the integrity of files, ensuring immediate detection of unauthorized changes. This is crucial for maintaining compliance with security standards and regulations.
2. **Customizable Monitoring Rules:** Users can define which files and directories to monitor, allowing for tailored configurations based on the specific needs of the organization. This flexibility ensures that critical assets are prioritized.
3. **Alerting and Notification:** Wazuh generates alerts based on predefined rules, enabling security teams to respond quickly to potential threats. Alerts can be customized based on severity levels and can trigger notifications via email, Slack, or other channels.
4. **Integration with Other Security Tools:** Wazuh can integrate with other security solutions, enhancing the overall security posture. For instance, it can work alongside firewalls, intrusion detection systems, and threat intelligence platforms.
5. **Compliance Reporting:** Wazuh provides compliance reports to assist organizations in meeting regulatory requirements such as PCI-DSS, HIPAA, and GDPR. The FIM feature helps demonstrate due diligence in protecting sensitive data.

Implementation Steps

To implement file integrity monitoring using Wazuh, the following steps should be followed:

1. **Install Wazuh:** Set up the Wazuh manager using Wazuh cloud and deploy Wazuh agents on all endpoints that need monitoring.
2. **Configure Agents:** Define the file and directory paths that require monitoring in the Wazuh agent configuration file (`ossec.conf`). Specify the types of changes to monitor, such as modifications, deletions, or creations.
3. **Set Up Alert Rules:** Configure alerting rules in the Wazuh manager to determine how alerts are generated and sent. Customize notification settings based on organizational requirements.
4. **Visualize Data in Kibana:** Use Kibana to visualize alerts and file integrity monitoring data. This provides a centralized dashboard for monitoring changes and trends over time.
5. **Review and Respond to Alerts:** Regularly review alerts generated by Wazuh. Implement a response plan to address potential security incidents based on the alerts received.

Benefits of Using Wazuh for File Integrity Monitoring

- **Open Source and Cost-Effective:** Wazuh is an open-source solution, making it accessible to organizations of all sizes without the high costs associated with proprietary tools.
- **Community Support and Development:** Being open-source, Wazuh benefits from a vibrant community that contributes to its development, ensuring continuous improvement and support.
- **Scalability:** Wazuh can scale to monitor large and diverse environments, making it suitable for organizations with complex IT infrastructures.

- **Enhanced Security Posture:** By providing real-time insights and alerts on file integrity, Wazuh helps organizations enhance their security posture and respond effectively to potential threats.

Description of the Tools Used in the Project

1. Wazuh

Wazuh is an open-source security information and event management (SIEM) tool designed for security monitoring, incident response, and compliance management. It offers features like log analysis, intrusion detection, and file integrity monitoring, making it a comprehensive solution for organizations seeking to enhance their security posture. The key components of Wazuh include:

- **Wazuh Manager:** This is the central server responsible for processing data collected from agents, generating alerts, and providing visualization through Kibana.
- **Wazuh Agents:** Lightweight agents deployed on endpoints to monitor system activity, collect logs, and track file integrity changes.
- **Kibana:** A visualization tool that provides a user-friendly interface for viewing alerts, logs, and reports generated by the Wazuh manager.

2. Linux Environment

The Wazuh environment is typically set up on a Linux operating system. Linux provides a robust platform for deploying server applications and managing agents, allowing for efficient resource utilization and security. Popular distributions used for Wazuh installations include Ubuntu, CentOS, and Debian.

3. Command-Line Interface (CLI)

The Linux command-line interface (CLI) is utilized for installing, configuring, and managing Wazuh agents and the Wazuh manager. The CLI provides powerful commands for system administration, making it essential for setting up and maintaining the Wazuh environment.

Step-by-Step Implementation Details

1. Creating a Wazuh Account

To begin using Wazuh, the first step is to create an account on the Wazuh website. This account allows access to documentation, community resources, and updates on Wazuh.

- **Steps to Create an Account:**
 - Visit the official Wazuh website.
 - Navigate to the registration page.
 - Provide the necessary information, including your name, email address, and organization details.

- Verify your email address by clicking on the confirmation link sent to your inbox.
- Log in to access resources and support related to Wazuh.

Create your account

Already have an account? [Log in](#)

Explore the potential of Wazuh Cloud

Welcome to Wazuh Cloud, your unified solution for XDR and SIEM delivered as a service.

Wazuh Cloud offers easy scalability to match your business growth, flexibility to adapt to your unique needs, and certification to meet industry standards like PCI DSS and SOC2.

Experience advanced threat detection and management with Wazuh Cloud.

Start your Free Trial

Get your 14-day trial. Sign up, register your first agent, and start enjoying Wazuh Cloud. You can cancel the trial at any time, and **no credit card is required**.

[Learn more about Wazuh Cloud](#)

First name: Soosian

Family name: Shabnam

Business email: jacklinkrypton@gmail.com

Phone number: 7595036541

Password:

Company: Student

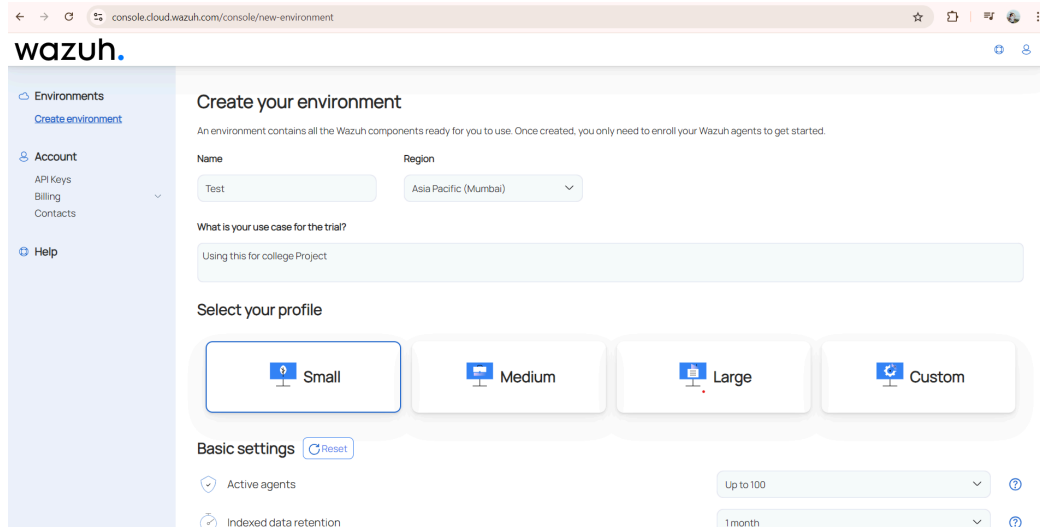
Country: India

[Create account](#)

2. Creating a Wazuh Environment (Linux)

Setting up a Wazuh environment typically involves deploying the Wazuh manager and agents on a Linux system. This environment will serve as the backbone for monitoring file integrity across various endpoints.

- **Steps to Create a Wazuh Environment:**
 - Choose a Linux distribution (e.g., Ubuntu, CentOS).
 - Install the necessary packages and dependencies required for Wazuh.
 - Download and install the Wazuh manager using the official installation guide.
 - Configure network settings to allow communication between the Wazuh manager and agents.



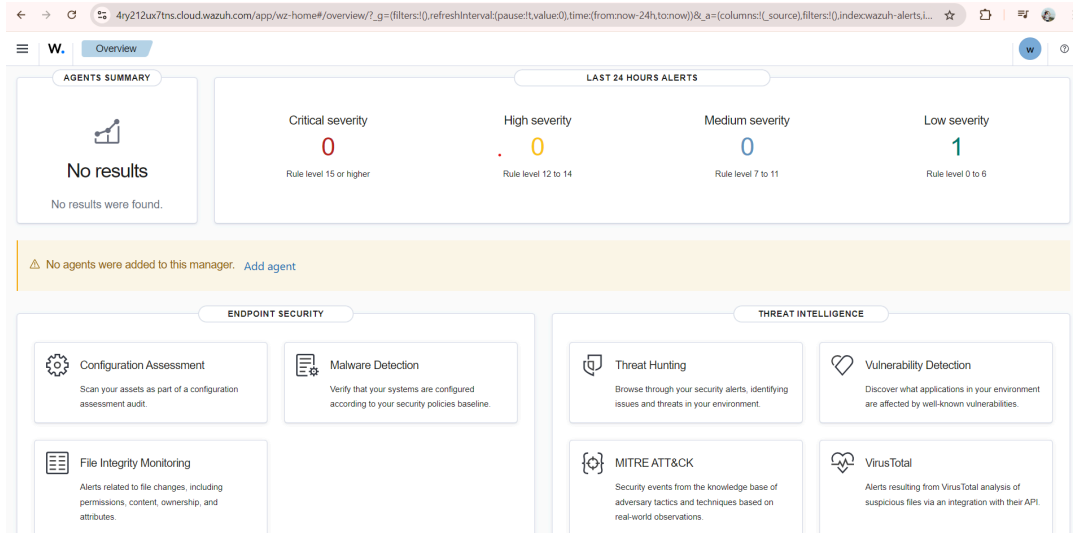
The screenshot displays the 'Create your environment' page in the Wazuh Cloud console. The page is titled 'Create your environment' and includes a sub-header: 'An environment contains all the Wazuh components ready for you to use. Once created, you only need to enroll your Wazuh agents to get started.' The form contains the following elements:

- Name:** A text input field with the value 'Test'.
- Region:** A dropdown menu with the selected value 'Asia Pacific (Mumbai)'.
- What is your use case for the trial?:** A text input field with the value 'Using this for college Project'.
- Select your profile:** Four buttons labeled 'Small', 'Medium', 'Large', and 'Custom'. The 'Small' button is highlighted with a blue border.
- Basic settings:** A section with a 'Reset' button and two settings:
 - Active agents:** A dropdown menu with the value 'Up to 100'.
 - Indexed data retention:** A dropdown menu with the value '1 month'.

3. Wazuh Overview and Agent Summary

Wazuh provides comprehensive security monitoring capabilities, focusing on log analysis, intrusion detection, and file integrity monitoring.

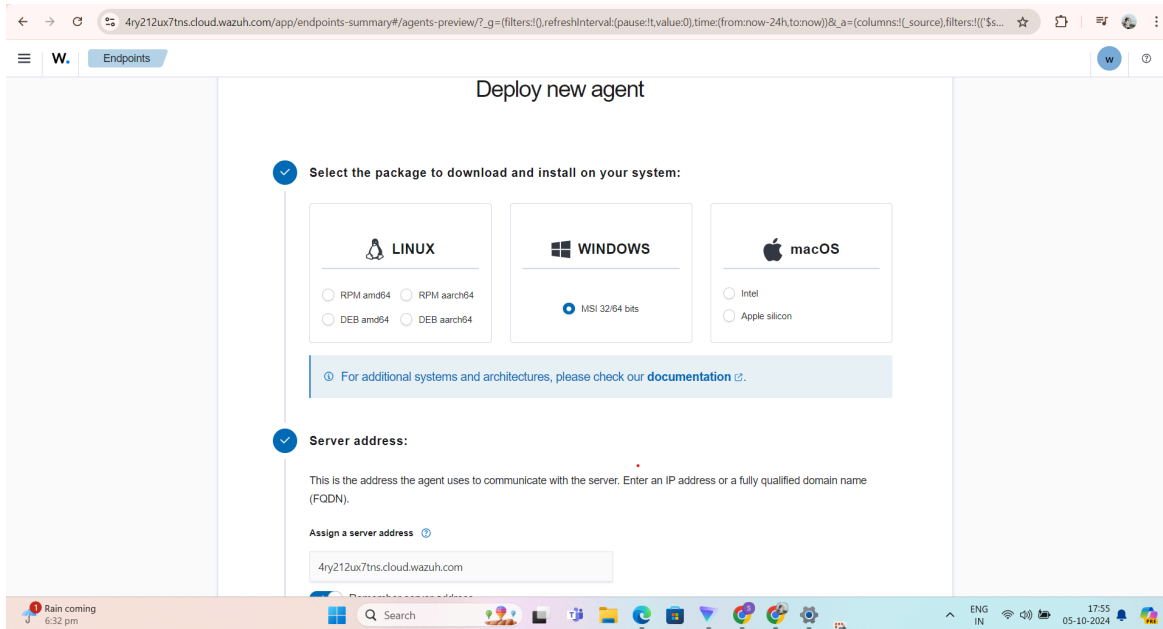
- **Key Components:**
 - **Wazuh Manager:** The central server that processes data from agents, manages alerts, and provides a user interface through Kibana.
 - **Wazuh Agents:** Lightweight agents installed on monitored endpoints that collect data, perform log analysis, and monitor file integrity.
- **Agent Summary:**
 - Each agent runs a local daemon that collects security-related events and sends them to the Wazuh manager.
 - Agents can be deployed on various operating systems, including Linux, Windows, and macOS, allowing for cross-platform monitoring.



4. Deploying the Agent

Deploying the Wazuh agent involves installing it on the target systems that need to be monitored. This process ensures that the agents can send logs and alerts back to the Wazuh manager.

- **Steps to Deploy the Agent:**
 - Access the target Linux machine via SSH or direct terminal access.
 - Download the Wazuh agent package for your Linux distribution from the official Wazuh repository.
 - Install the agent using the package manager (e.g., apt for Debian-based systems or yum for Red Hat-based systems).
 - Start the Wazuh agent service and enable it to start on boot.



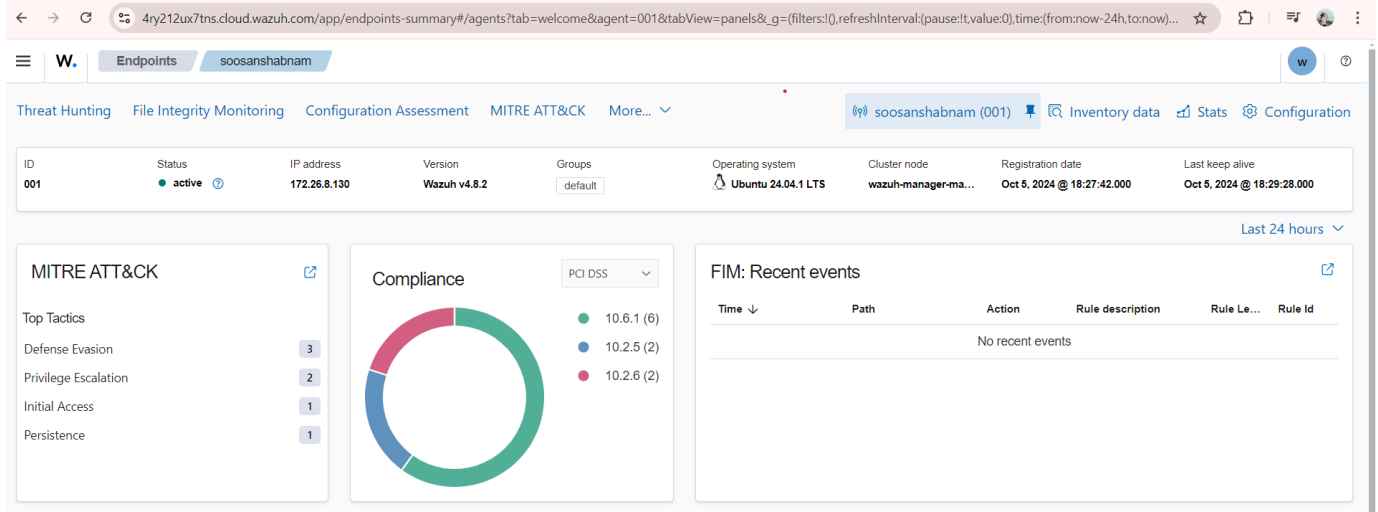
```
soosan@DESKTOP-M5FIOA0: ~  
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.  
soosan@DESKTOP-M5FIOA0:~$ sudo systemctl status wazuh-agent  
● wazuh-agent.service - Wazuh agent  
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2024-10-05 12:57:48 UTC; 30s ago  
     Tasks: 43 (limit: 18989)  
    Memory: 127.6M ()  
    CGroup: /system.slice/wazuh-agent.service  
            └─2013 /var/ossec/bin/wazuh-execd  
              └─2023 /var/ossec/bin/wazuh-agentd  
                └─2037 /var/ossec/bin/wazuh-syscheckd  
                  └─2108 /var/ossec/bin/wazuh-logcollector  
                    └─2122 /var/ossec/bin/wazuh-modulesd  
  
Oct 05 12:57:41 DESKTOP-M5FIOA0 systemd[1]: Starting wazuh-agent.service - Wazuh agent...  
Oct 05 12:57:41 DESKTOP-M5FIOA0 env[1732]: Starting Wazuh v4.8.2...  
Oct 05 12:57:42 DESKTOP-M5FIOA0 env[1732]: Started wazuh-execd...  
Oct 05 12:57:43 DESKTOP-M5FIOA0 env[1732]: Started wazuh-agentd...  
Oct 05 12:57:44 DESKTOP-M5FIOA0 env[1732]: Started wazuh-syscheckd...  
Oct 05 12:57:45 DESKTOP-M5FIOA0 env[1732]: Started wazuh-logcollector...  
Oct 05 12:57:46 DESKTOP-M5FIOA0 env[1732]: Started wazuh-modulesd...  
Oct 05 12:57:48 DESKTOP-M5FIOA0 env[1732]: Completed.  
Oct 05 12:57:48 DESKTOP-M5FIOA0 systemd[1]: Started wazuh-agent.service - Wazuh agent.  
soosan@DESKTOP-M5FIOA0:~$
```

5. Details on Agent Configuration Through Linux CLI on PC

After deploying the Wazuh agent, it must be configured to communicate with the Wazuh manager. Configuration is done through the command line interface (CLI).

- **Steps to Configure the Agent:**
 - Open the agent configuration file located at `/var/ossec/etc/ossec.conf` using a text editor (e.g., nano or vi).

- Update the <server> section to specify the IP address or hostname of the Wazuh manager.
- Modify other settings as needed, such as log collection and file integrity monitoring rules.
- Save the changes and restart the Wazuh agent service to apply the new configuration.



6. Changing `ossec.conf`, Creating, and Deleting Files to Reflect on Wazuh Dashboard

The `ossec.conf` file can be modified to specify which directories and files to monitor for integrity changes. This allows for customization based on the organization's security requirements.

- **Steps to Change `ossec.conf`:**
 - Open the `ossec.conf` file for editing.
 - Add or modify <directories> and <files> tags to include the specific paths to monitor.
 - Save and close the file, then restart the agent.
- **Creating and Deleting Files:**
 - Use command line commands such as `touch` to create a new file or `rm` to delete an existing file in the monitored directories.
 - For example, to create a file: `touch /path/to/monitored/file.txt`
 - To delete a file: `rm /path/to/monitored/file.txt`


```
root@DESKTOP-M5FIOA0: /var/ossec/etc
Oct 05 12:57:43 DESKTOP-M5FIOA0 env[1732]: Started wazuh-agentd...
Oct 05 12:57:44 DESKTOP-M5FIOA0 env[1732]: Started wazuh-syscheckd...
Oct 05 12:57:45 DESKTOP-M5FIOA0 env[1732]: Started wazuh-logcollector...
Oct 05 12:57:46 DESKTOP-M5FIOA0 env[1732]: Started wazuh-modulesd...
Oct 05 12:57:48 DESKTOP-M5FIOA0 env[1732]: Completed.
Oct 05 12:57:48 DESKTOP-M5FIOA0 systemd[1]: Started wazuh-agent.service - Wazuh agent.
soosan@DESKTOP-M5FIOA0:~$ sudo -i
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 5.15.153.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sat Oct 5 13:07:40 UTC 2024

System load: 0.0          Processes:              38
Usage of /:  0.1% of 1006.85GB Users logged in:       1
Memory usage: 3%          IPv4 address for eth0: 172.26.8.130
Swap usage:  0%

This message is shown once a day. To disable it please create the
/root/.hushlogin file.
root@DESKTOP-M5FIOA0:~# cd /var/ossec/
root@DESKTOP-M5FIOA0:/var/ossec# /var/ossec# ls
-bash: /var/ossec#: No such file or directory
root@DESKTOP-M5FIOA0:/var/ossec# ls
active-response  agentless  backup  bin  etc  lib  logs  queue  ruleset  tmp  var  wodles
root@DESKTOP-M5FIOA0:/var/ossec# cd etc/
root@DESKTOP-M5FIOA0:/var/ossec/etc# nano os
```

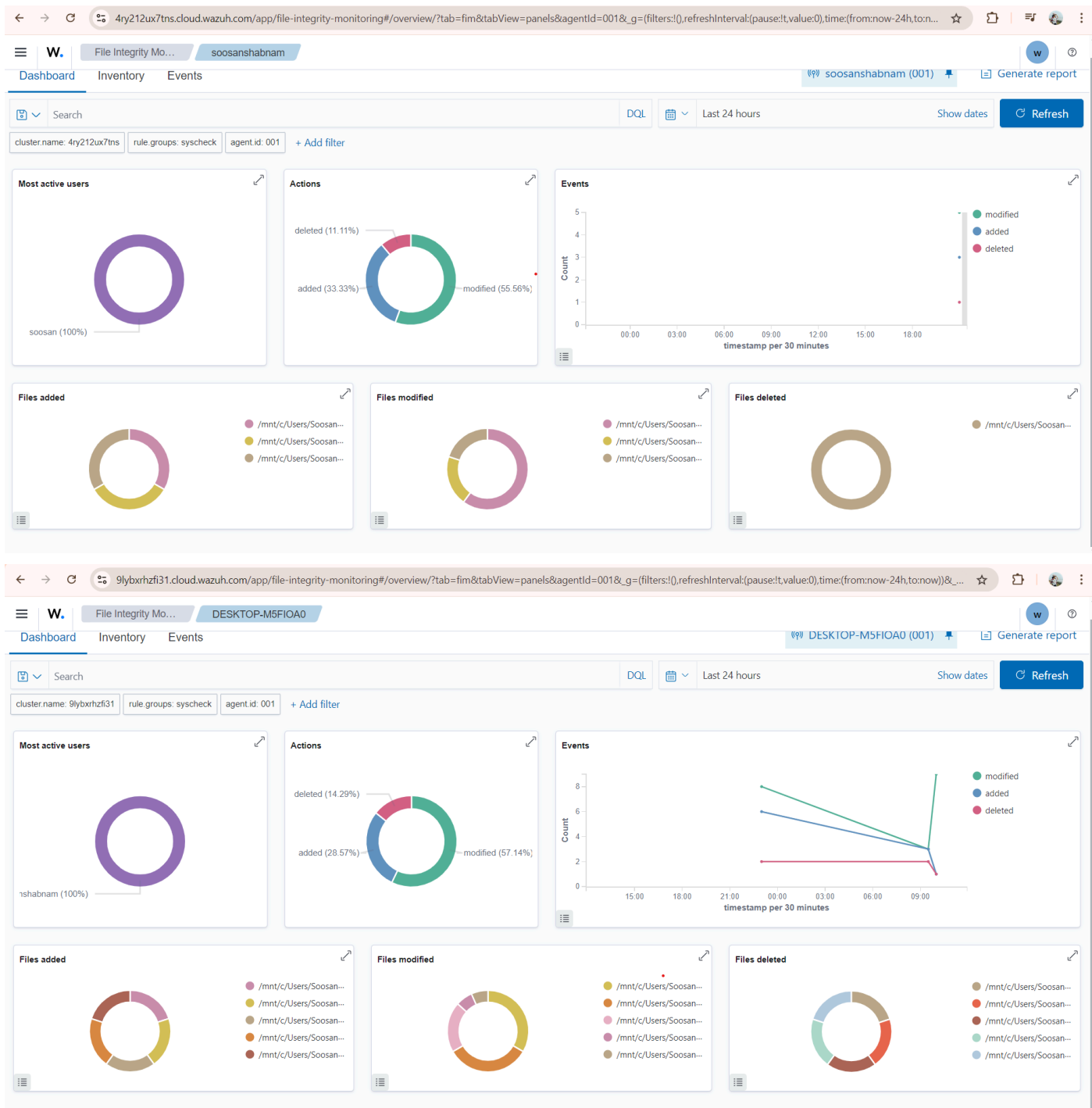
7. Changes on Wazuh Dashboard About Files Created, Deleted, Modified, and the Timestamps for These Actions

Once the agent is properly configured and files are created or deleted, Wazuh will reflect these changes on the dashboard in real time.

- **Monitoring Changes:**
 - Access the Wazuh dashboard via Kibana to view alerts and changes detected by the agents.
 - The dashboard will display alerts for files that have been created, deleted, or modified, along with relevant details such as:
 - File path
 - Action type (created, deleted, modified)
 - Timestamp of the change
 - The source of the change (e.g., user or process)
- **Example View on Wazuh Dashboard:**
 - Alerts may show entries like:
 - "File created: /path/to/monitored/file.txt at [timestamp]"
 - "File deleted: /path/to/monitored/file.txt at [timestamp]"
 - "File modified: /path/to/monitored/another_file.txt at [timestamp]"

This comprehensive approach to file integrity monitoring using Wazuh not only enhances the security of systems but also ensures compliance with various regulatory requirements by providing auditable logs and alerts for all critical changes.

SCREENSHOTS OF FINAL CHANGES REFLECTED ON DASHBOARD



Recent Research on File Integrity Monitoring Using Wazuh

File Integrity Monitoring (FIM) is a critical aspect of cybersecurity that helps organizations detect unauthorized changes to files and directories, ensuring compliance with regulatory standards and protecting sensitive information. Wazuh, as an open-source security monitoring tool, has gained popularity for its capabilities in file integrity monitoring. Recent research and studies have focused on various aspects of implementing Wazuh for FIM, highlighting its effectiveness and advancements in this domain.

1. Enhancing Detection Capabilities

Recent studies have shown that integrating Wazuh with machine learning algorithms enhances its ability to detect anomalies in file modifications. By analyzing historical file change patterns, researchers have developed models that can distinguish between normal and suspicious changes, reducing false positives and improving the accuracy of alerts.

- **Key Findings:**
 - The incorporation of machine learning techniques, such as clustering and classification, enables Wazuh to learn from historical data and adapt to normal behavior over time.
 - Anomaly detection systems built on Wazuh can identify potential security incidents more efficiently than traditional signature-based methods.

2. Compliance and Regulatory Standards

Research has emphasized the role of Wazuh in helping organizations meet compliance requirements such as PCI-DSS, HIPAA, and GDPR. By continuously monitoring file changes and generating detailed reports, Wazuh assists organizations in maintaining compliance with data protection regulations.

- **Key Findings:**
 - Wazuh's logging and alerting features provide comprehensive documentation of file integrity changes, which is crucial during audits.
 - The system's ability to automate compliance reporting significantly reduces the administrative burden on IT security teams.

3. Cloud and Virtualized Environments

With the rise of cloud computing and virtualization, research has explored how Wazuh can be deployed effectively in these environments for file integrity monitoring. Studies demonstrate that Wazuh's lightweight agents can efficiently monitor file integrity across multiple cloud instances and virtual machines.

- **Key Findings:**
 - Wazuh's architecture allows for centralized management of agents deployed in distributed environments, ensuring consistent monitoring and reporting.

- Integration with cloud-native tools and services enhances the scalability of file integrity monitoring solutions.

4. Performance Optimization

Recent research has addressed performance challenges associated with file integrity monitoring in high-traffic environments. Researchers have proposed optimization strategies for Wazuh to reduce resource consumption while maintaining effective monitoring capabilities.

- **Key Findings:**
 - Techniques such as adjusting the frequency of file checks and optimizing the configuration of monitoring rules can lead to significant performance improvements.
 - Load balancing across multiple Wazuh managers can enhance the scalability of the FIM solution.

5. User Behavior Analytics

Studies have begun to explore the integration of user behavior analytics (UBA) with Wazuh's file integrity monitoring capabilities. By analyzing user interactions with files, organizations can identify potentially malicious behavior or policy violations.

- **Key Findings:**
 - Combining UBA with FIM allows organizations to gain deeper insights into user activity, making it easier to detect insider threats and data exfiltration attempts.
 - Enhanced correlation rules in Wazuh can trigger alerts based on unusual user behavior related to file modifications.

6. Case Studies and Real-World Implementations

Recent case studies have documented successful implementations of Wazuh for file integrity monitoring across various industries, including finance, healthcare, and government sectors. These studies illustrate the practical benefits of deploying Wazuh and its impact on enhancing security posture.

- **Key Findings:**
 - Organizations report improved incident response times and reduced risks of data breaches following the deployment of Wazuh for FIM.
 - The community support and extensive documentation associated with Wazuh facilitate faster implementation and troubleshooting.

BIBLIOGRAPHY:

1. **Wazuh Documentation.** (2024). *Wazuh Documentation*. Retrieved from <https://documentation.wazuh.com>
2. **Moiz, S., Majid, A., Basit, A., & Ebrahim, M.** (2024). *Security and Threat Detection through Cloud-Based Wazuh Deployment*. In *Proceedings of the 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*. DOI: 10.1109/KHI-HTC60760.2024.10482206.
3. **Islam, Md R., & Rafique, R.** (2024). *Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries*. *International Journal of Engineering Materials and Manufacture*, 9(4), 136–144. DOI:10.26776/ijemm.09.04.2024.02.
4. **SANS Institute.** (2023). *Understanding File Integrity Monitoring in SIEM Systems*. Retrieved from <https://www.sans.org>
5. **Sankar, N. A., & K. A., F.** (2023). *Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring*. In *Proceedings of the 2023 9th International Conference on Smart Computing and Communications (ICSCC)*. DOI:10.1109/ICSCC59169.2023.10334992.