**CodemanBD Internship (December-2023 to January-2024)**

**Topic:** Task-4 (Project-1)

**Submitted By:**
**Student's Id:** 213/48
**Student's Name:** Teresa Jency Bala

**Submitted to:**
**Instructor:** Sanin Ahammed Sifat (Shuvo Ahmed)

**Date:** 04-01-2024
**Day:** Thursday

**Project-1**: Mix tasks 1-2-3 and make a fresh report about Wazuh as SIEM & EDR. **(without installation steps)**

**Wazuh:**
Wazuh is a **free** and **open-source** security monitoring tool that helps organizations detect, respond to, and mitigate cyber threats. It is a **host-based intrusion detection system** (HIDS) that monitors system files, processes, and network traffic for suspicious activity. Wazuh also includes a security information and event management (SIEM) system that collects and analyzes logs from various sources to provide a centralized view of security events.

Wazuh is a popular security monitoring tool because it is:
**Free and open-source:** Wazuh is available to download and use without any licensing fees. This makes it a cost-effective solution for organizations of all sizes.

**Comprehensive:** Wazuh provides a wide range of security monitoring capabilities, including HIDS, SIEM, and log management. This makes it a one-stop shop for security monitoring needs.

**Powerful:** Wazuh is powered by a variety of powerful detection engines, including Random Cut Forest, Local Outlier Factor, and K-Means Clustering. This allows it to detect a wide range of threats, including zero-day attacks and advanced persistent threats (APTs).

**Easy to use:** Wazuh has a user-friendly interface that makes it easy to configure and manage. It also has a large community of users and developers who can provide support and assistance.

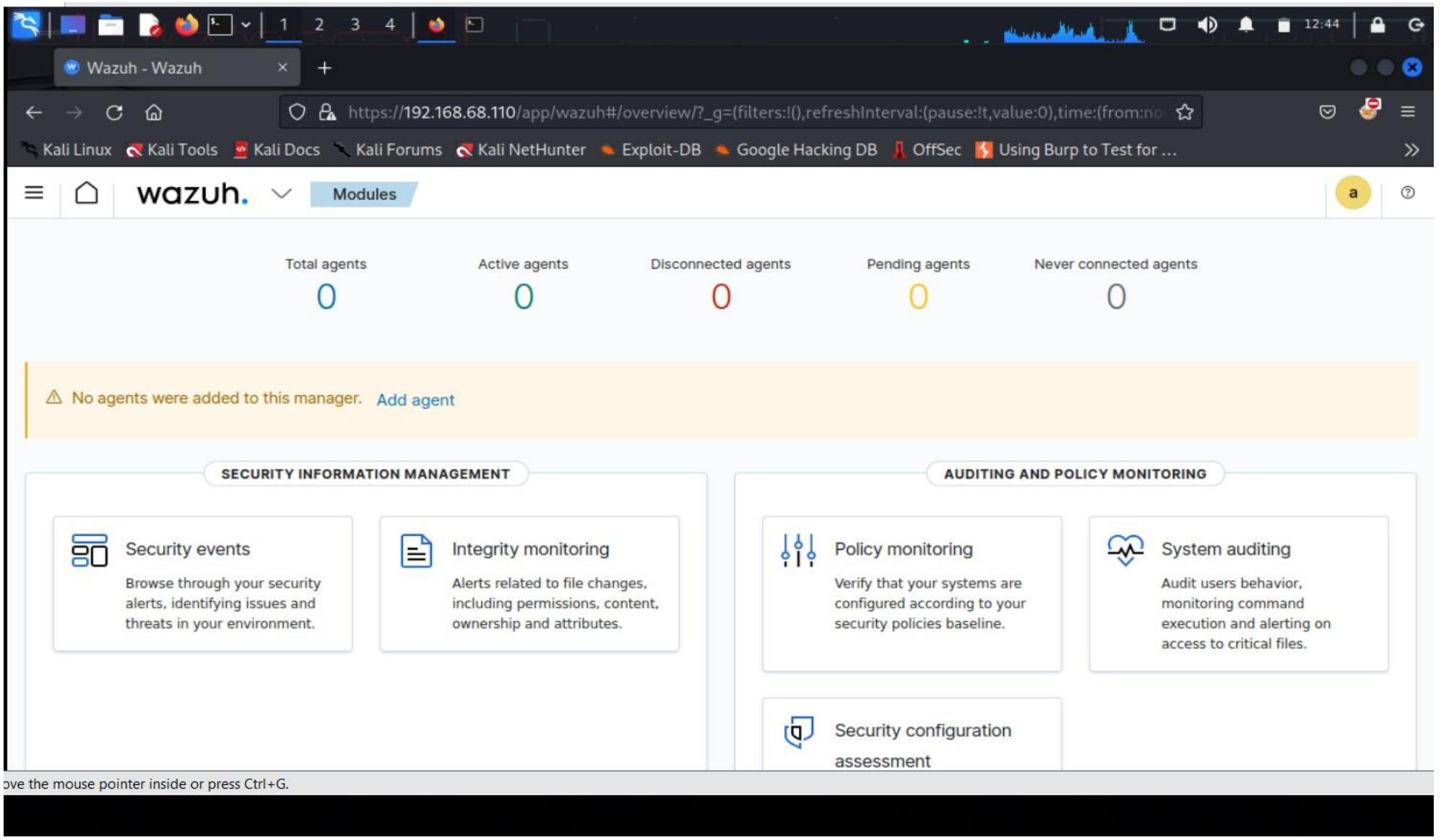
Wazuh is used by a variety of organizations, including government agencies, financial institutions, and healthcare providers. It is a trusted security monitoring tool that can help organizations protect their systems and data from cyber threats.

In addition to the features listed above, Wazuh also includes the following:

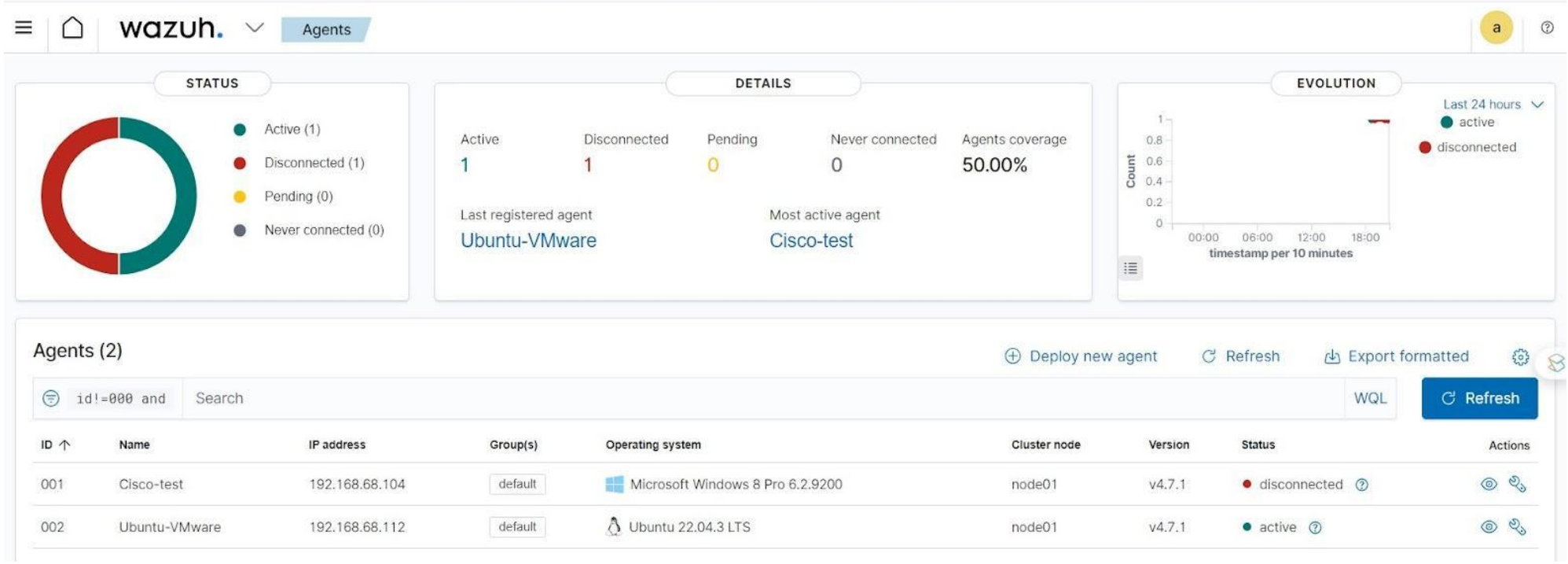
**Real-time monitoring**: Wazuh monitors system activity in real-time, so it can detect threats as they are happening.
**Threat intelligence:** Wazuh includes a threat intelligence feed that provides information about the latest threats and vulnerabilities.
**Incident response:** Wazuh provides tools to help organizations respond to security incidents, such as playbooks and runbooks.
**Compliance reporting:** Wazuh can generate reports that help organizations comply with security regulations, such as PCI DSS and HIPAA.

Wazuh is a comprehensive and powerful security monitoring tool that can help organizations protect their systems and data from cyber threats. It is free and open-source, easy to use, and has a large community of users and developers.

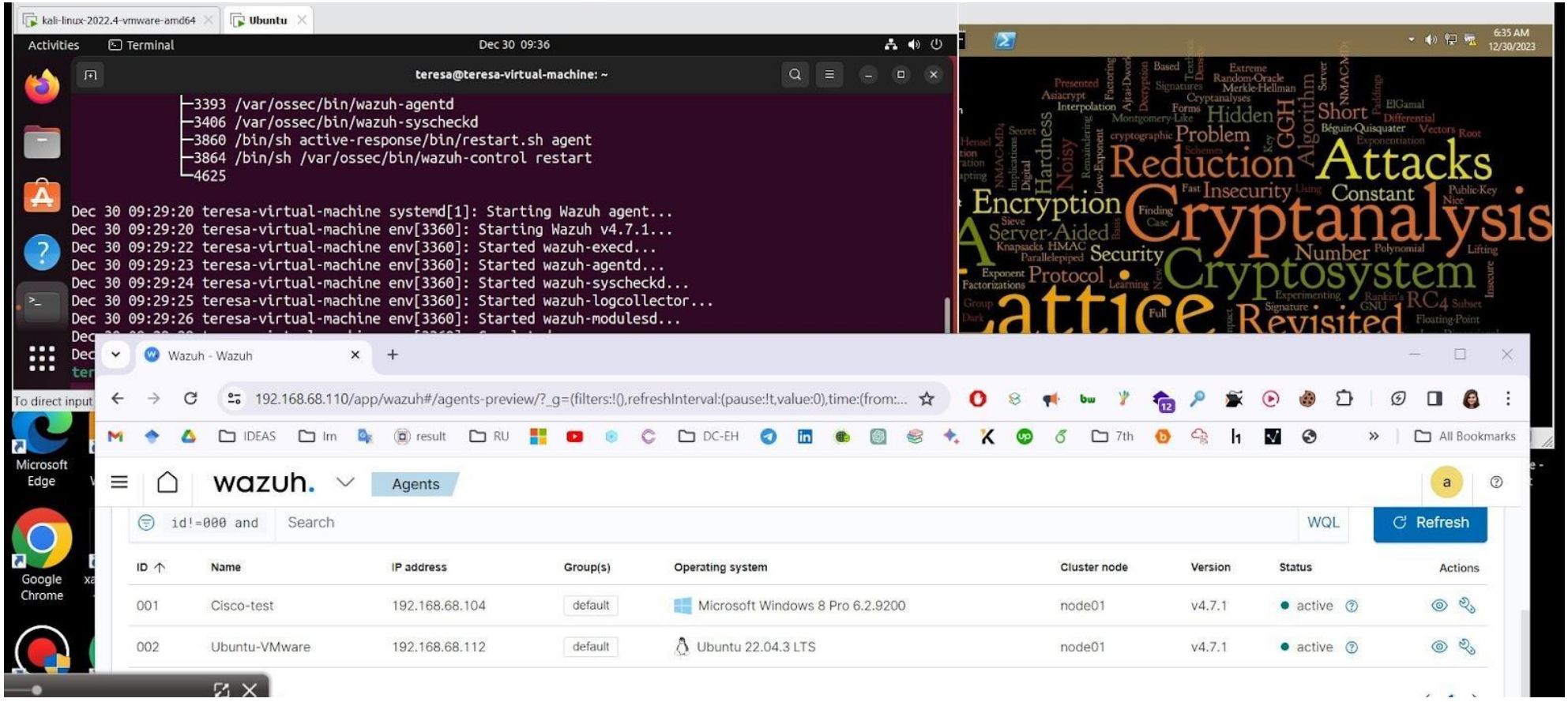
**Wazuh Dashboard** before integrating agents(hosts) for monitoring:



**Wazuh Dashboard** after integrating agents(hosts) for monitoring: Here One agent (ubuntu) active

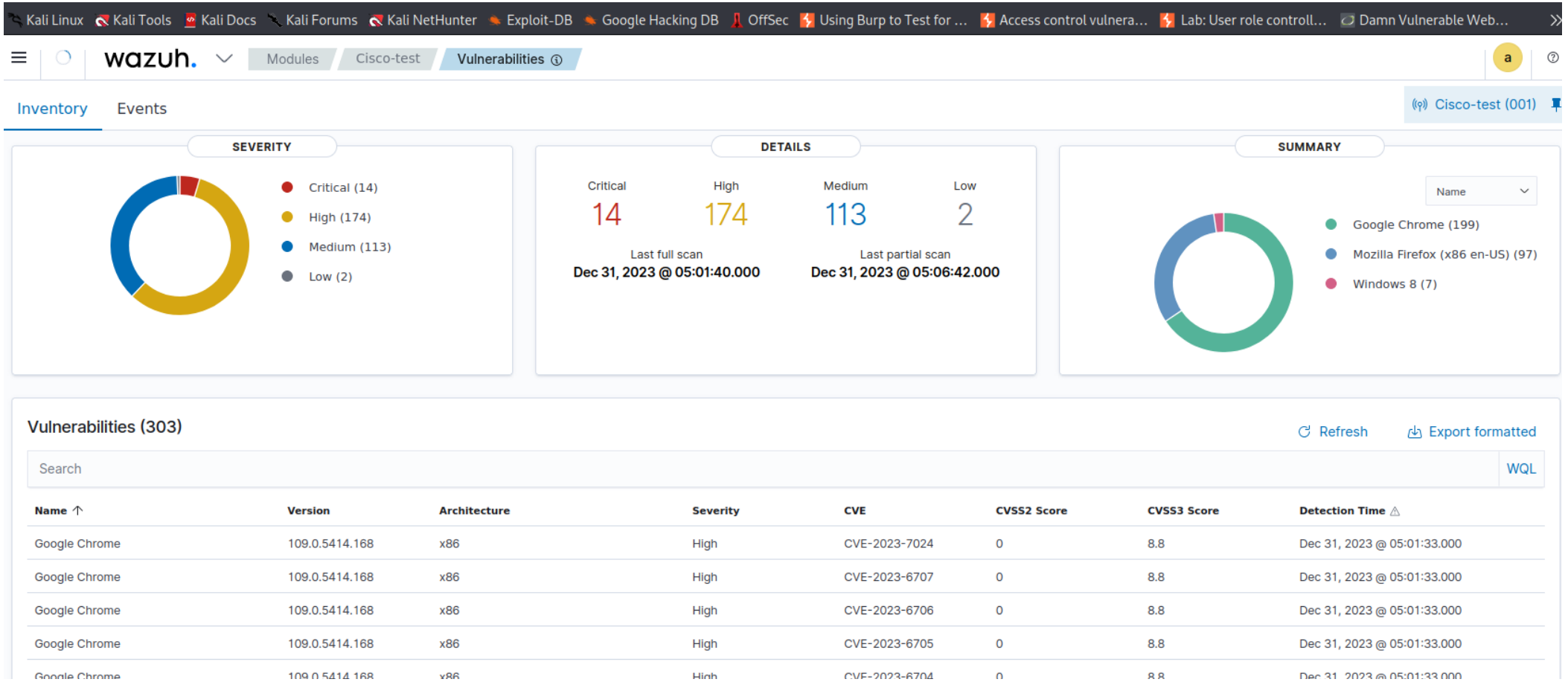


**Wazuh Dashboard** after integrating agents(hosts) for monitoring: Here both Linux and Windows Host active

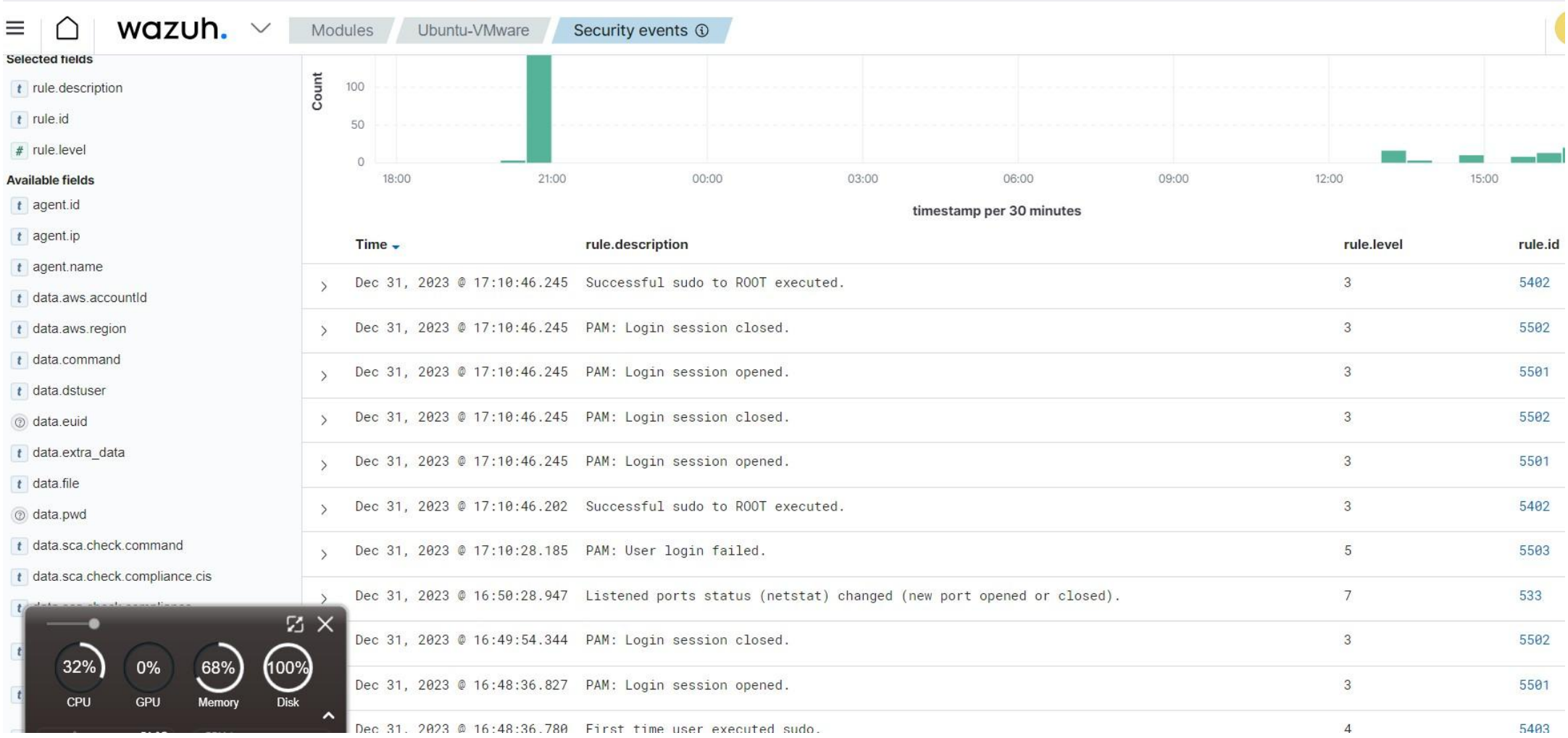


After enabling the vulnerability detector in the Wazuh configuration files through wazuh dashboard we are able to detect vulnerabilities and do study on information from all the agent devices.

For example the windows 8 device has many vulnerabilities in the Chrome exe file. So it has to be updated to latest release:

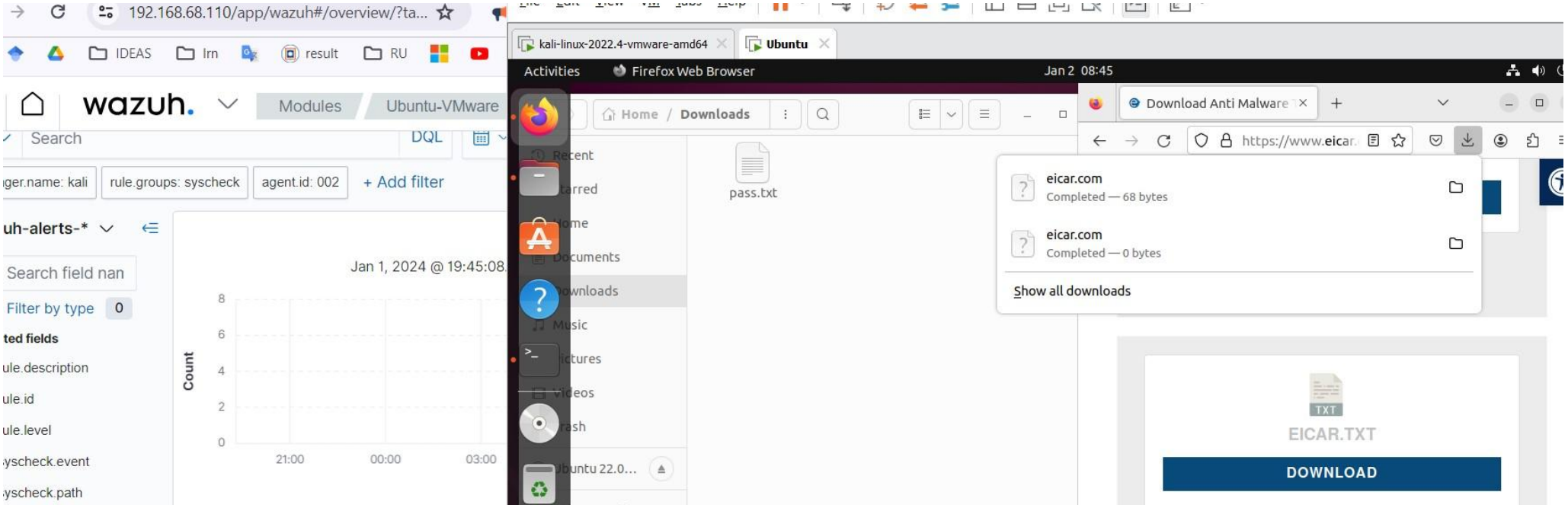


For the **Ubuntu device** since there we didn't find any vulnerabilities we can use AtomicRedTeam to apply some tactics on the device and those will also get monitored on the wazuh. Any sort of operations getting executed in the agent devices will get recorded in real time in the wazuh dashboard.

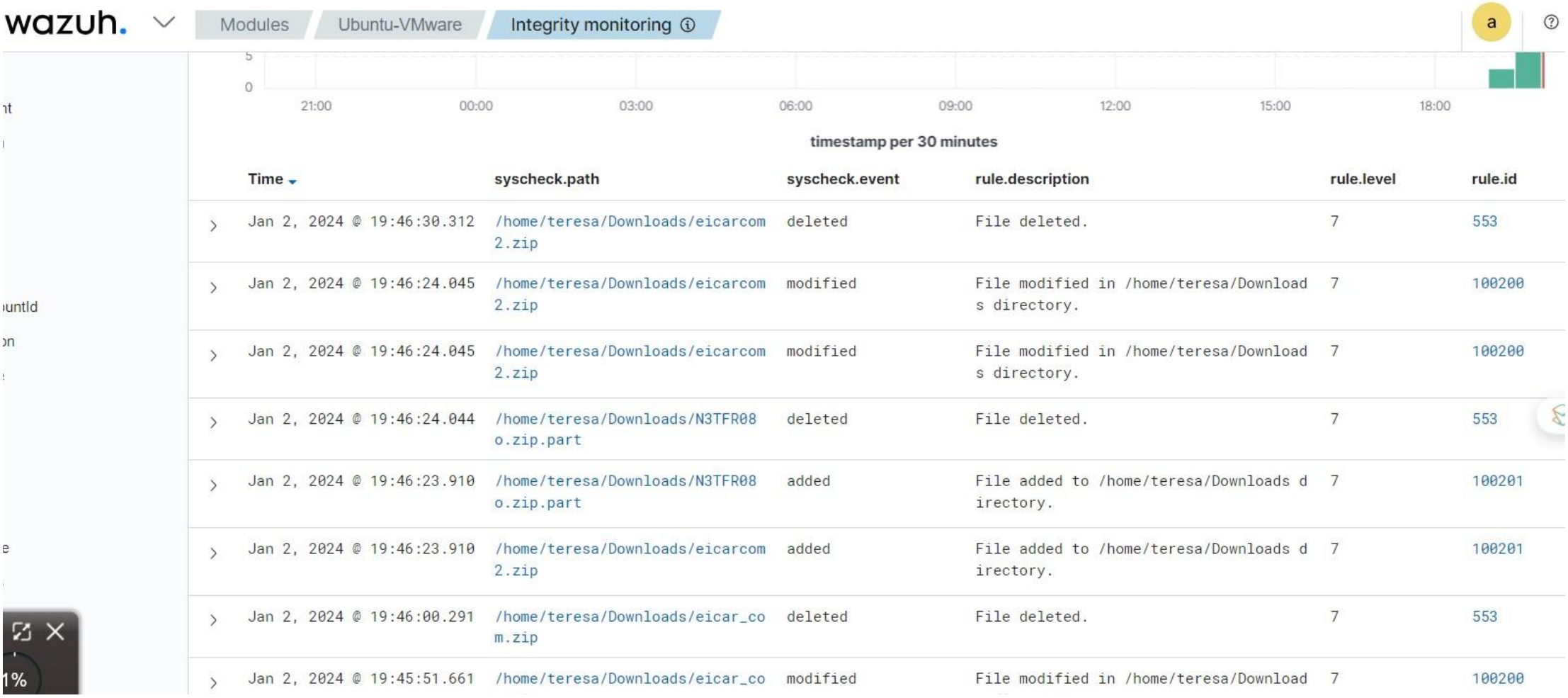


For getting **real-time updates** and Setting up **Active Responses** for the whole system or for a specific directory in Ubuntu we can integrate **Virustotal API** for malware detection and realtime removal.
For demonstration purpose here in the Ubuntu (Linux system) we will set up VirusTotal API and have Real-time Active response for downloading Malicious softwares.

After following directives and completing the setup following the Wazuh Virustotal API integration system from the Official website for the Server and the wazuh-agent device here is an example of how Wazuh with VirusTotal API integration, instantly removes malicious files downloaded from the web.



Files after downloading from eicar. com website are automatically getting deleted within seconds as they contain malicious codes and are listed in Virustotal as malicious files.




| Time | syscheck.path | syscheck.event | rule.description | rule.level | rule.id |
|---|---|---|---|---|---|
| Jan 2, 2024 @ 19:46:30.312 | /home/teresa/Downloads/eicarcom2.zip | deleted | File deleted. | 7 | 553 |
| Jan 2, 2024 @ 19:46:24.045 | /home/teresa/Downloads/eicarcom2.zip | modified | File modified in /home/teresa/Downloads directory. | 7 | 100200 |
| Jan 2, 2024 @ 19:46:24.045 | /home/teresa/Downloads/eicarcom2.zip | modified | File modified in /home/teresa/Downloads directory. | 7 | 100200 |
| Jan 2, 2024 @ 19:46:24.044 | /home/teresa/Downloads/N3TFR08o.zip.part | deleted | File deleted. | 7 | 553 |
| Jan 2, 2024 @ 19:46:23.910 | /home/teresa/Downloads/N3TFR08o.zip.part | added | File added to /home/teresa/Downloads directory. | 7 | 100201 |
| Jan 2, 2024 @ 19:46:23.910 | /home/teresa/Downloads/eicarcom2.zip | added | File added to /home/teresa/Downloads directory. | 7 | 100201 |
| Jan 2, 2024 @ 19:46:00.291 | /home/teresa/Downloads/eicar_com.zip | deleted | File deleted. | 7 | 553 |
| Jan 2, 2024 @ 19:45:51.661 | /home/teresa/Downloads/eicar_co | modified | File modified in /home/teresa/Download | 7 | 100200 |

Wazuh is an SIEM solution where we can monitor, collect, and analyze logs from various sources to provide a centralized view of security events. It can be used for threat prevention, detection, and response. Our work here is done with the Wazuh- server being installed in Kali Linux device and we have two agents - ubuntu and Windows 8. Furthermore, Wazuh is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments.