Nama : Asyrof Hafizh Maulana

INCIDENT INVESTIGATION (SIEM Wazuh)

1. Install VM SIEM Wazuh menggunakan OVA (VirtualBox) berikut

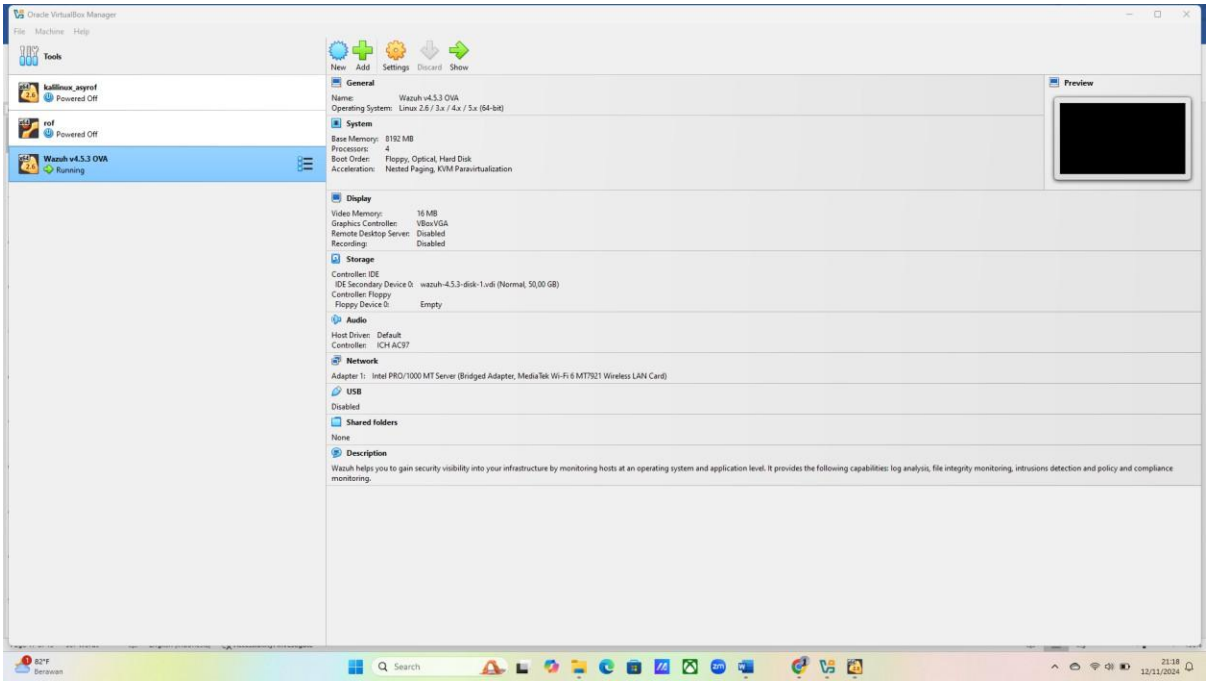
   https://packages.wazuh.com/4.x/vm/wazuh-4.5.3.ova

2. Pelajari fitur fiturnya dan jelaskan dengan bahasa Anda sendiri dengan menunjukkan menu/tampilan Wazuh tersebut
3. Pasang Wazuh-Agent disalah satu mesin/VM lain (dan hubungkan ke SIEM Wazuh) sehingga dapat dimonitor dan audit dari SIEM Wazuh.
   Ref. https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

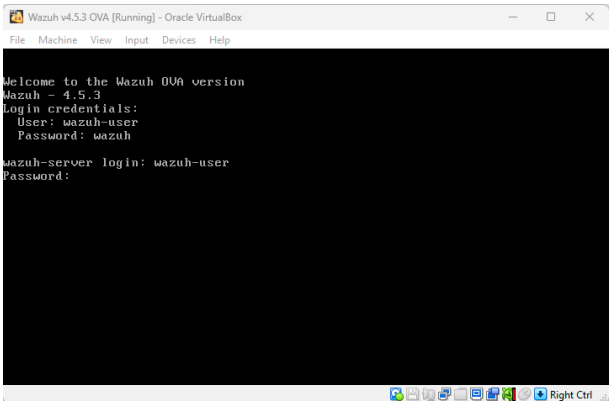
   Jelaskan apa saja yang dapat dimonitor oleh SIEM Wazuh tersebut.

Jawab :

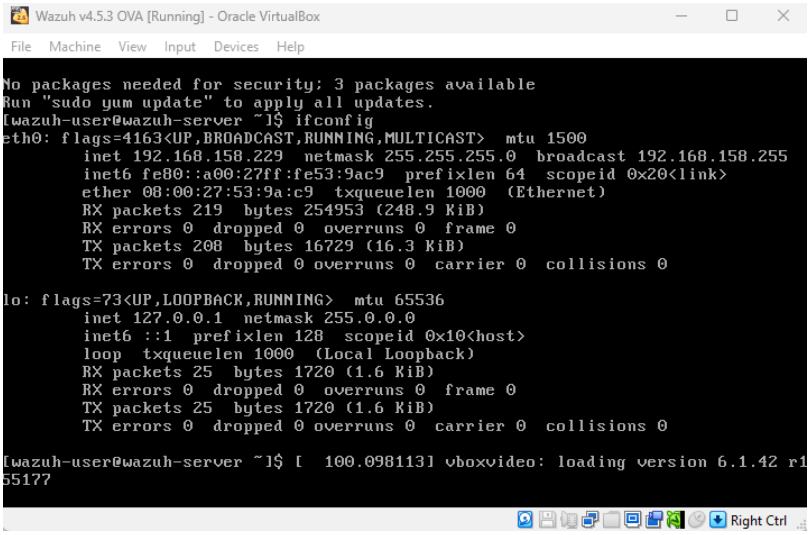
1. Install VM SIEM Wazuh menggunakan OVA di virtualbox :



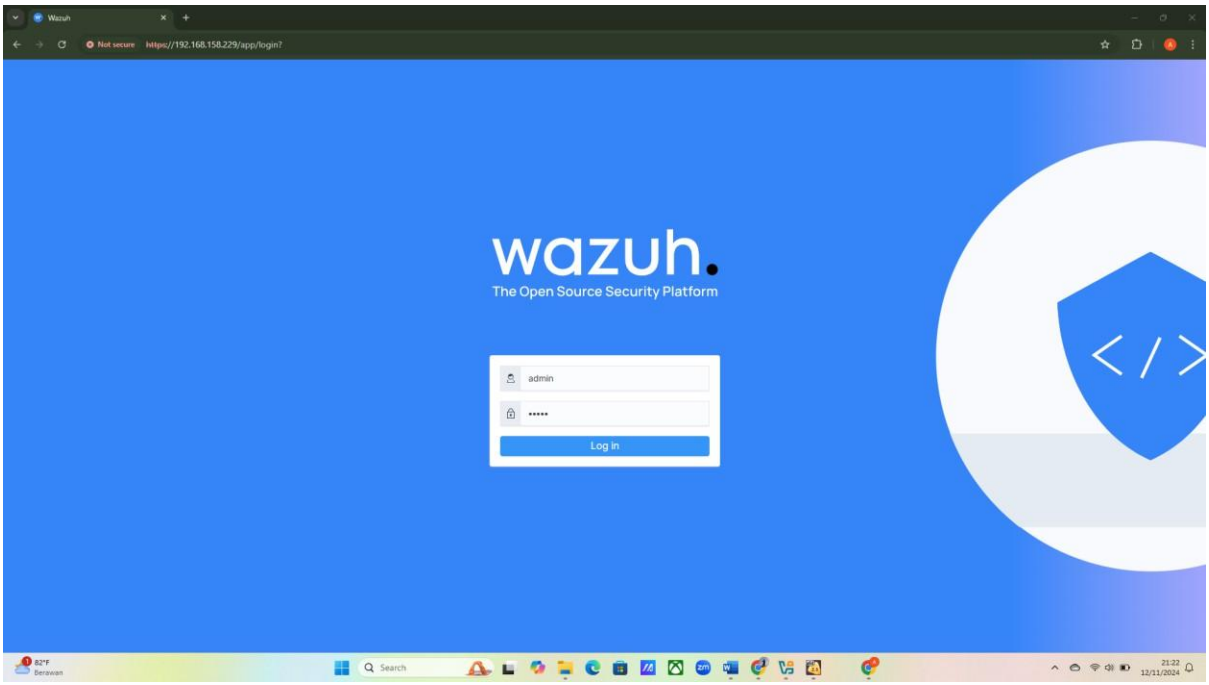
Login wazuh :



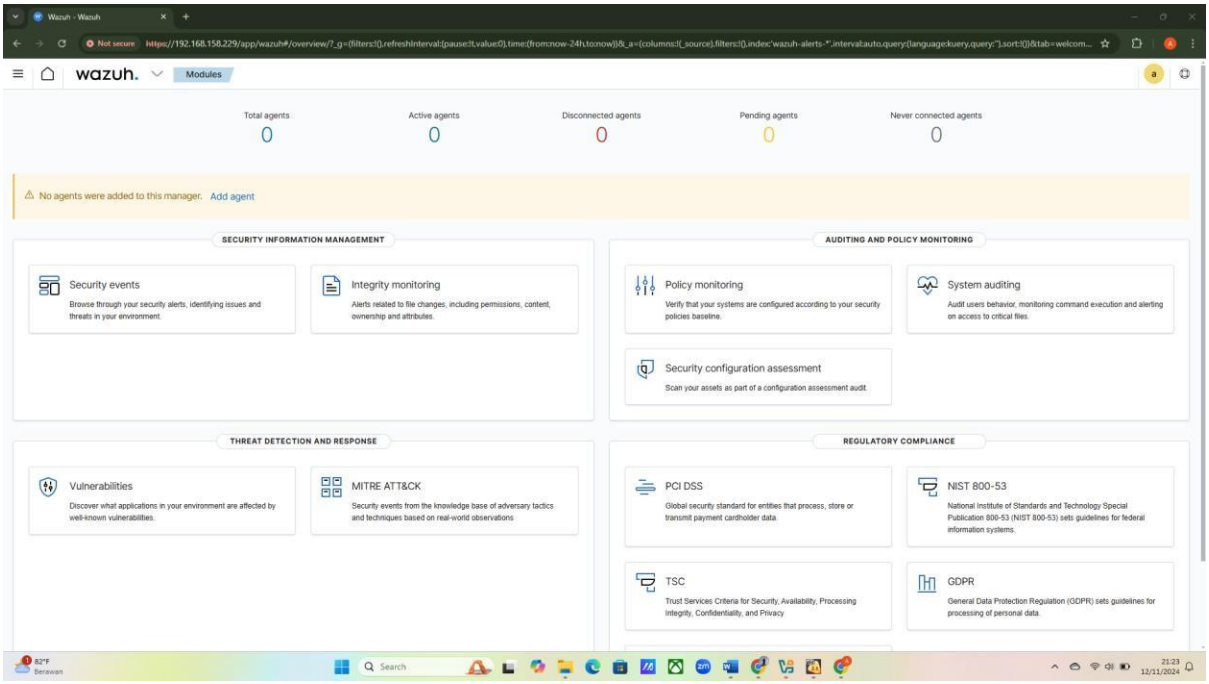
Setelah login cek ip web wazuh dengan perintah ifconfig :



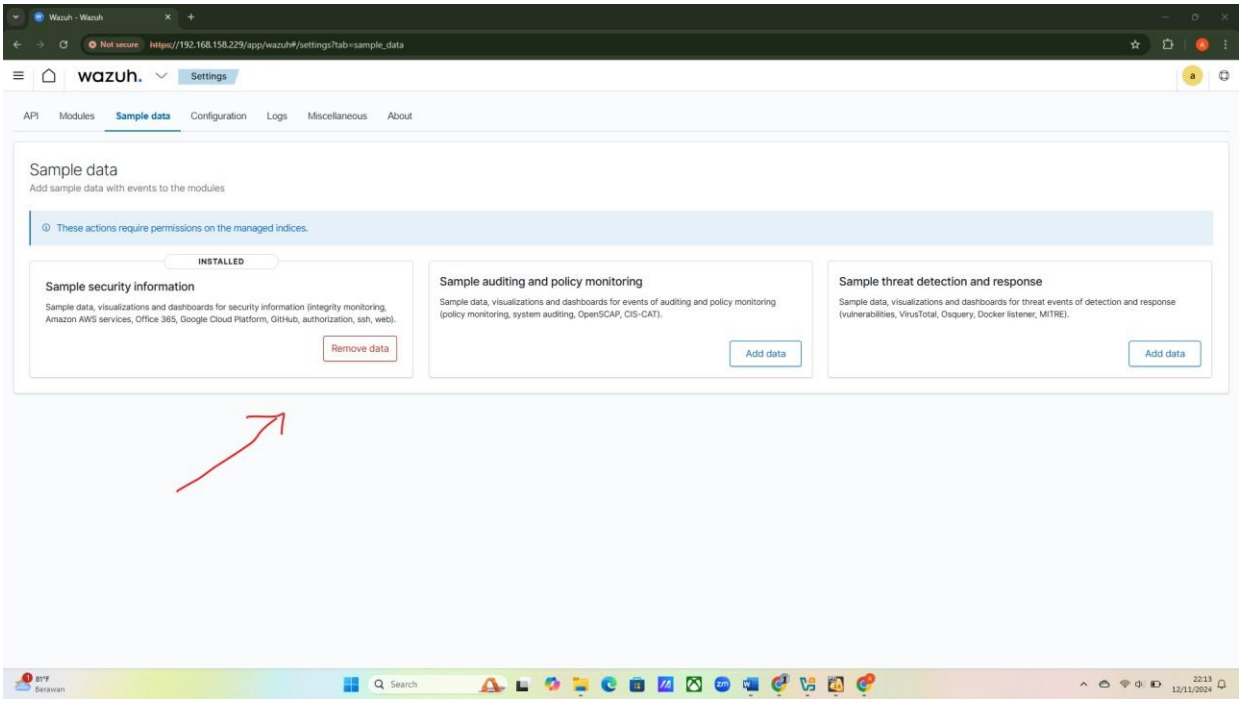
Akses web wazuh denga nip yang sudah didapatkan :



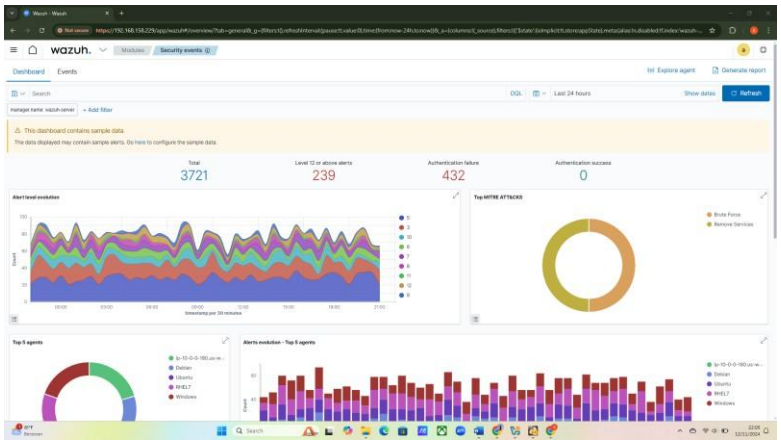
Tampilan awal web wazuh :



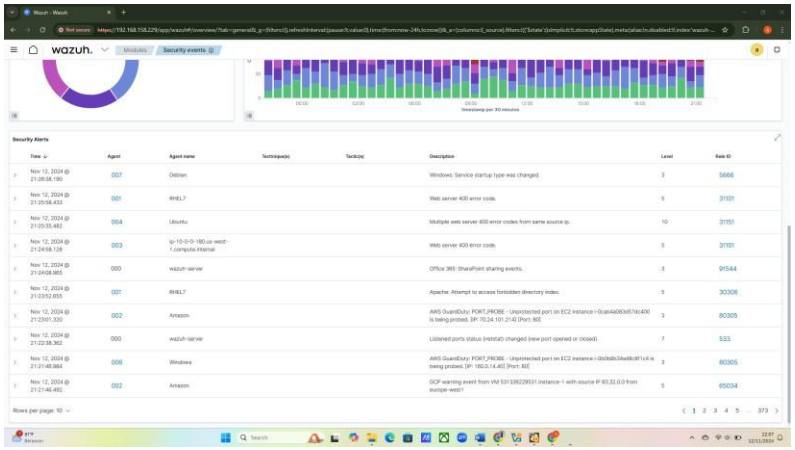
2. Penjelasan beberapa fitur/tampilan dashboard pada wazuh, Saya sudah download sample data :



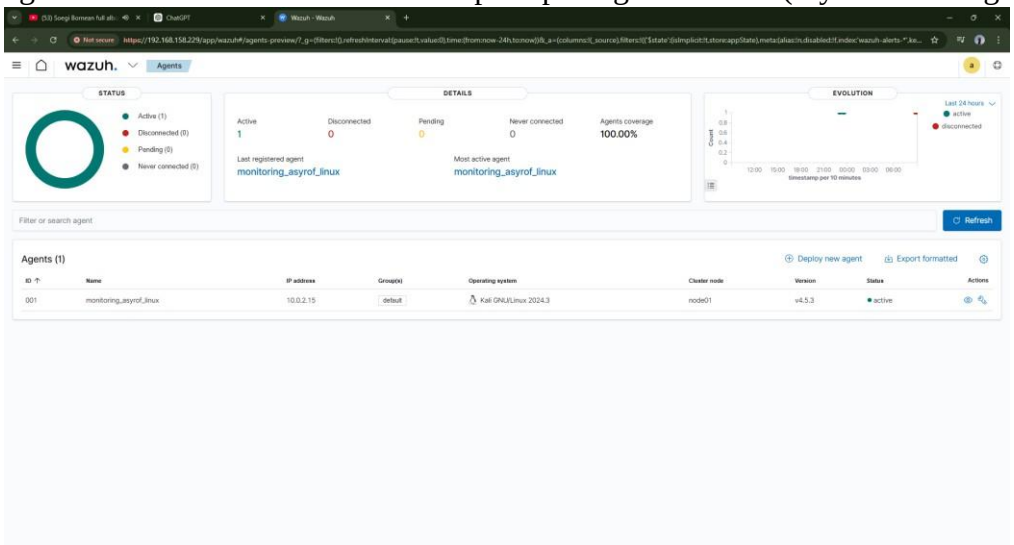
1. Dashboard Overview:
   Berisi data-data dari agen (perangkat) berupa diagram dan keterangannya



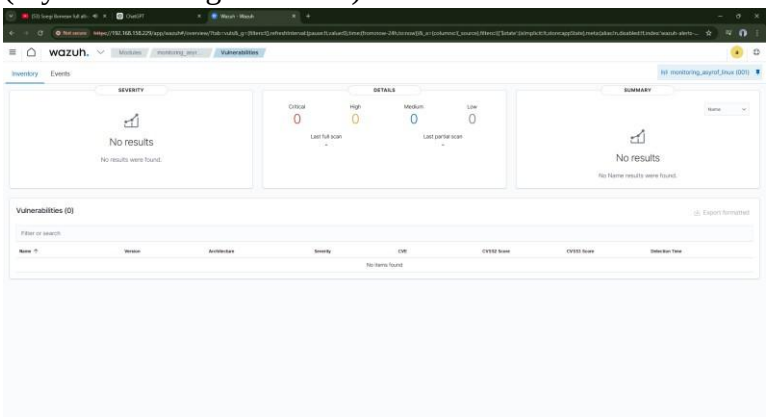
2. Security Events:
   Daftar peringatan keamanan secara rinci,penjelasam bagaimana setiap alert memberikan informasi tentang jenis serangan,sumber,dan waktu kejadian.



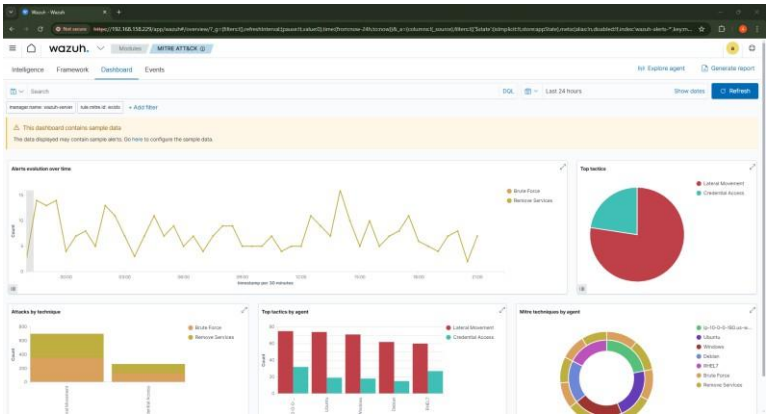
3. Agent Management:
   Menampilkan daftar agen (perangkat atau server) yang terhubung dengan Wazuh. Setiap agen memonitor aktivitas keamanan pada perangkat tertentu (saya monitoring kali linux) :



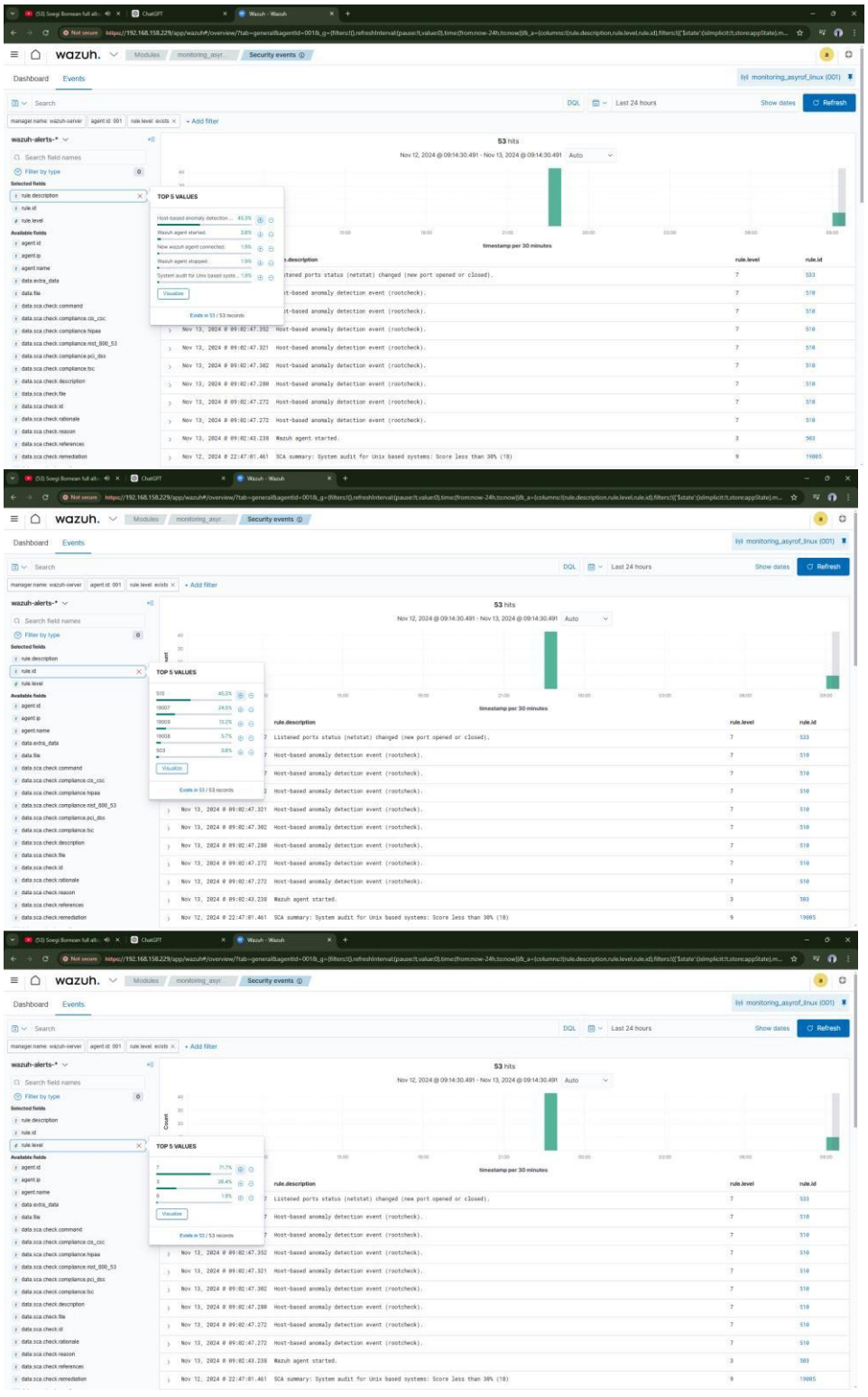
4. Vulnerability Detection:
   Memindai sistem untuk mendeteksi kerentanan atau celah keamanan. Bagian ini memberikan informasi detail tentang kerentanan yang ditemukan, seperti versi software yang rentan, sehingga membantu dalam menilai risiko dan mengambil langkah perbaikan (saya monitoring kali linux) :



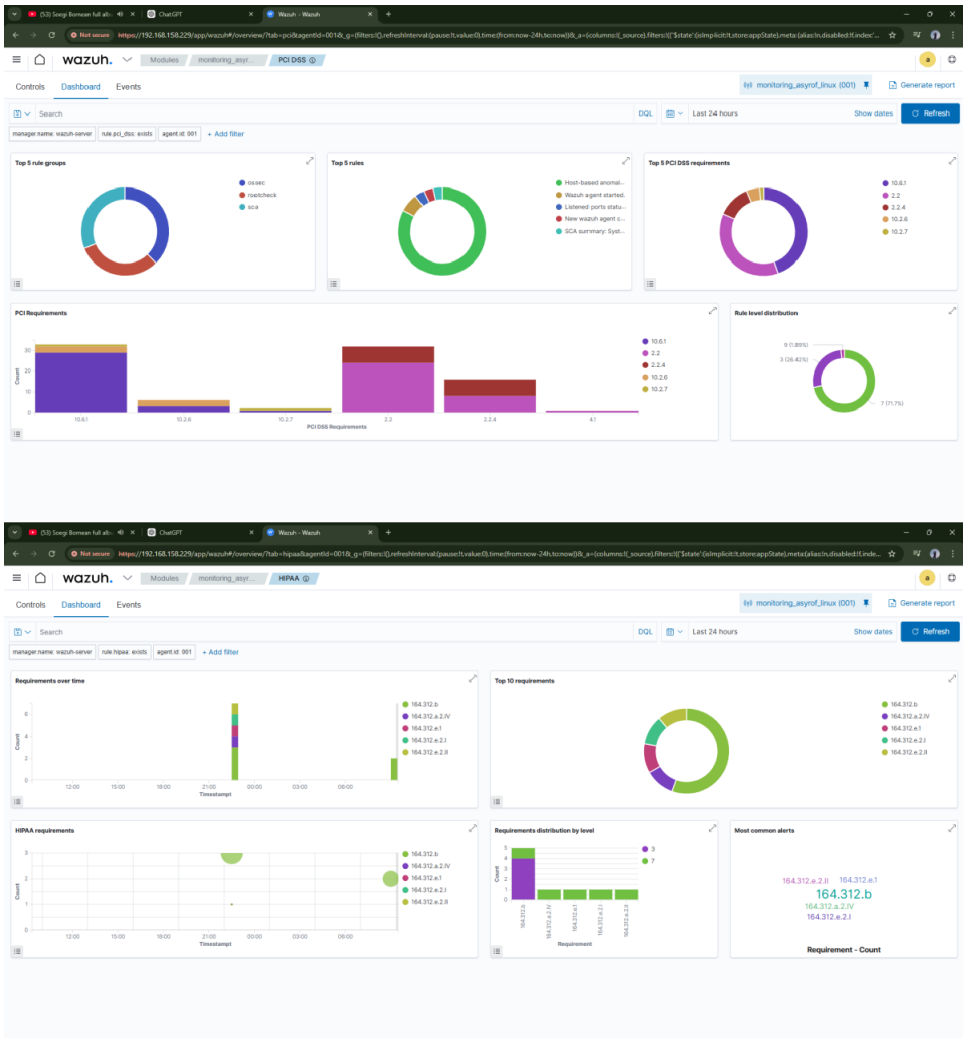
5. MITRE ATT&CK Framework:
   Memberikan rincian tentang jenis serangan yang teridentifikasi berdasarkan MITRE ATT&CK.



6. File Integrity Monitoring (FIM):
   Melacak perubahan pada file penting dalam sistem. Fitur ini bisa ditunjukkan melalui log atau tampilan FIM di Wazuh untuk memperlihatkan file mana yang diubah, kapan, dan oleh siapa.
7. Log Data Analysis:
   Mengumpulkan dan menganalisis log dari berbagai perangkat untuk mencari pola atau indikasi serangan (monitoring kali linux) :



8. Compliance Monitoring:
   Menyediakan fitur untuk memastikan bahwa sistem mematuhi standar kepatuhan (seperti PCI-DSS atau HIPAA) (monitoring kali linux) :



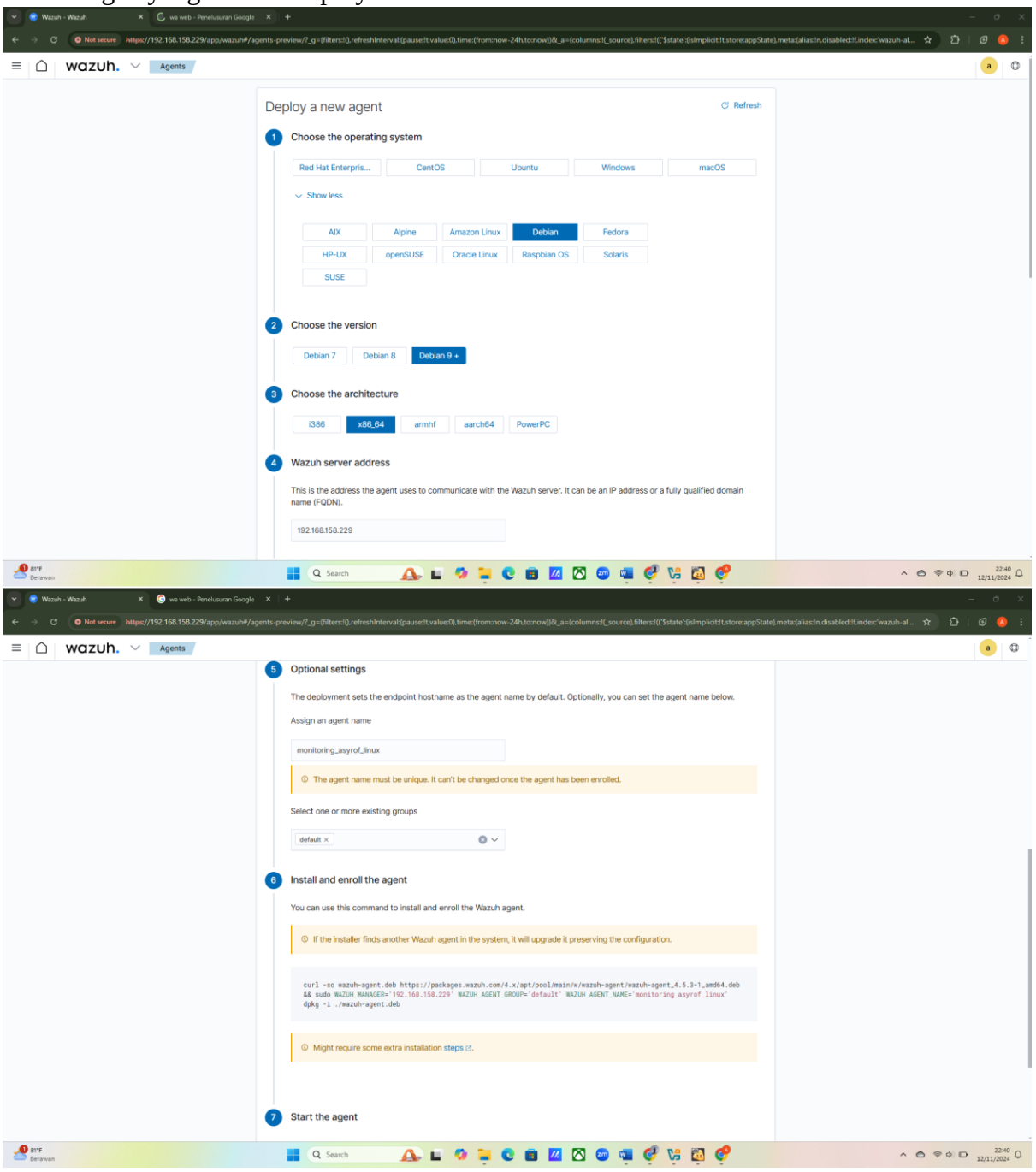
3. Memasang Wazuh-Agent di virtual box agar bisa dimonitoring dan penjelasan apa saja yang dapat dimonitor oleh SIEM Wazuh tersebut :

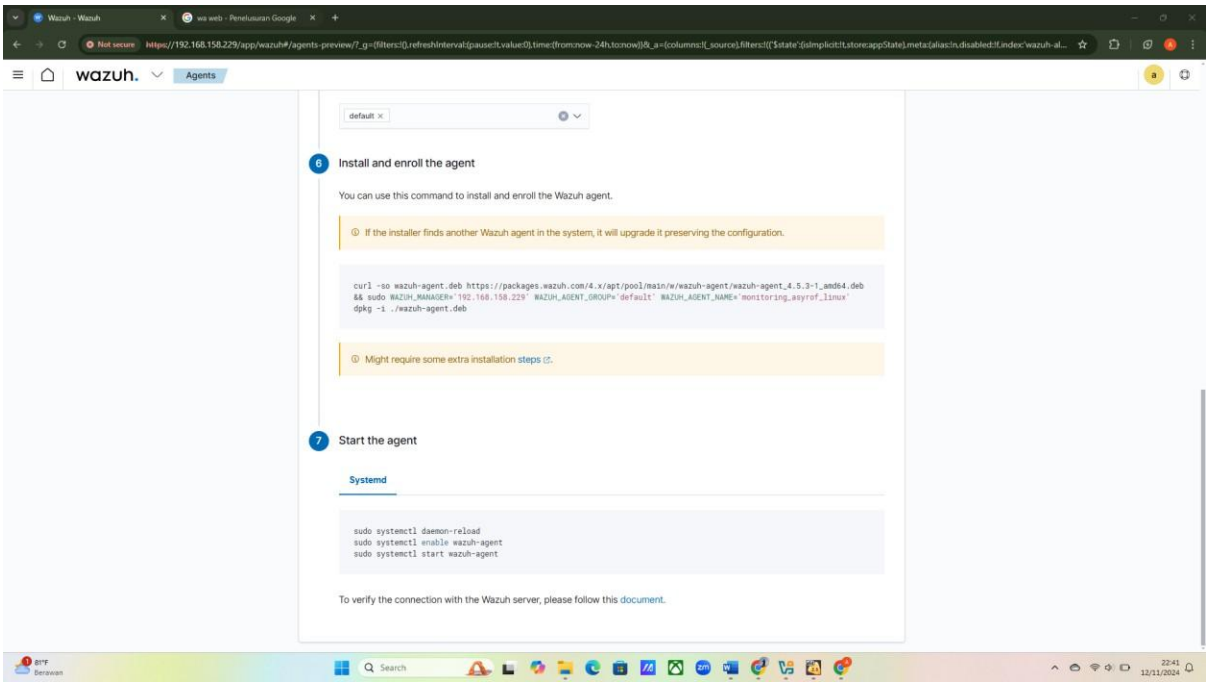
Cek ip pada kali linux :

```
┌──(root㉿asyrof)-[/home/asyrof]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::d215:2f85:fb99:cff8  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe7c:a37a  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::a00:27ff:fe7c:a37a  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:7c:a3:7a  txqueuelen 1000  (Ethernet)
        RX packets 456  bytes 234919 (229.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 413  bytes 56498 (55.1 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Isi data agen yang akan di deploy :



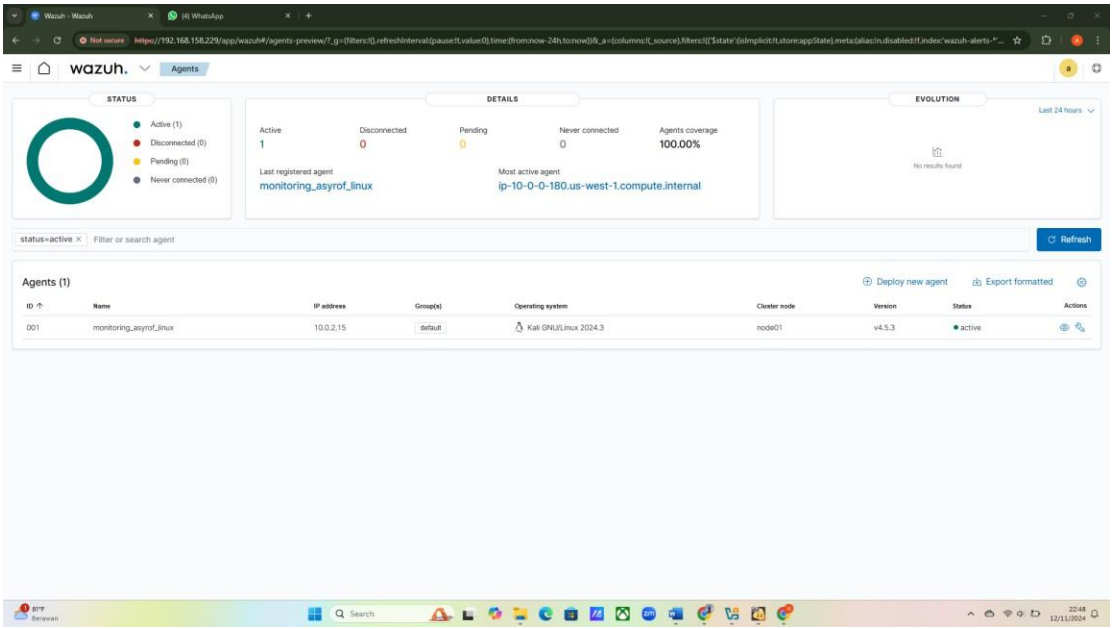


Copy enroll the agent pada kali linux :

```
curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.3-1_amd64.deb
&& sudo WAZUH_MANAGER='192.168.158.229' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='monitoring_asyrof_linux'
dpkg -i ./wazuh-agent.deb
```

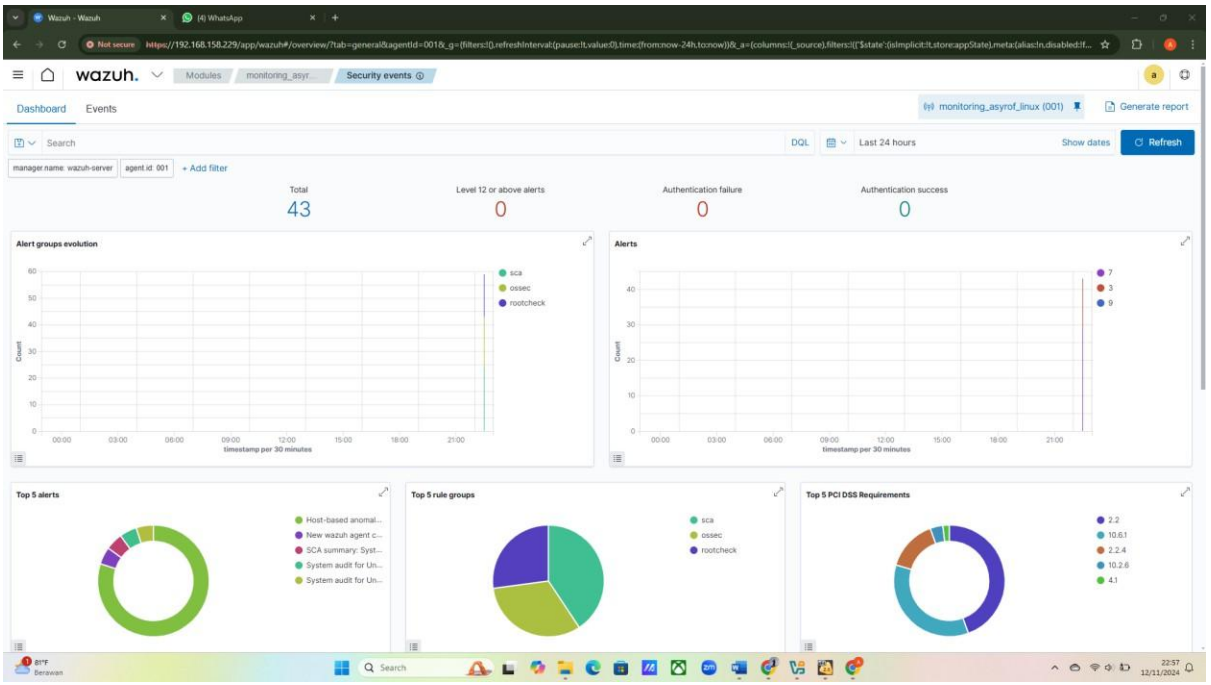
Start wazuh agen pada kali linux :

Monitoring kali linux sudah berhasil:
Fitur ini secara keseluruhan berguna untuk memantau status, aktivitas, dan koneksi dari setiap agen yang berhubungan dengan Wazuh Manager, sehingga memudahkan dalam pengelolaan dan pemantauan sistem.

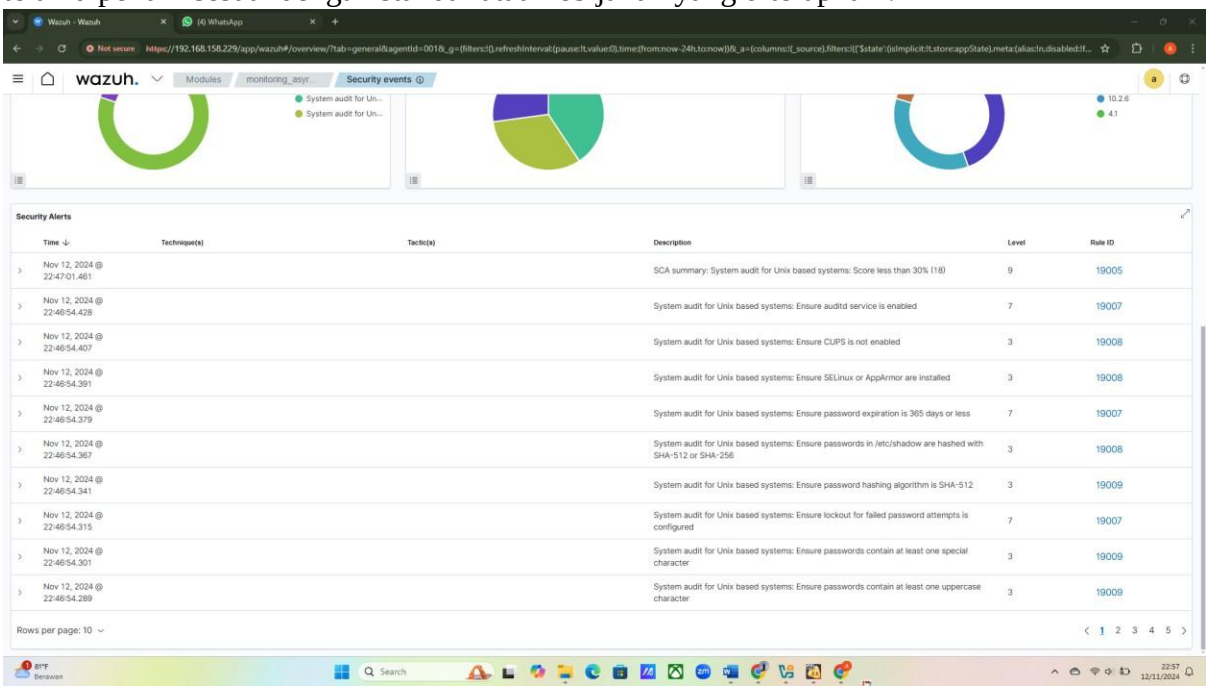


Penjelasan apa saja yang dapat dimonitoring :
Secara keseluruhan, dashboard ini berfungsi untuk memberikan gambaran menyeluruh tentang aktivitas keamanan dari agen yang terhubung, membantu dalam identifikasi ancaman, dan memantau kepatuhan terhadap kebijakan keamanan yang berlaku.

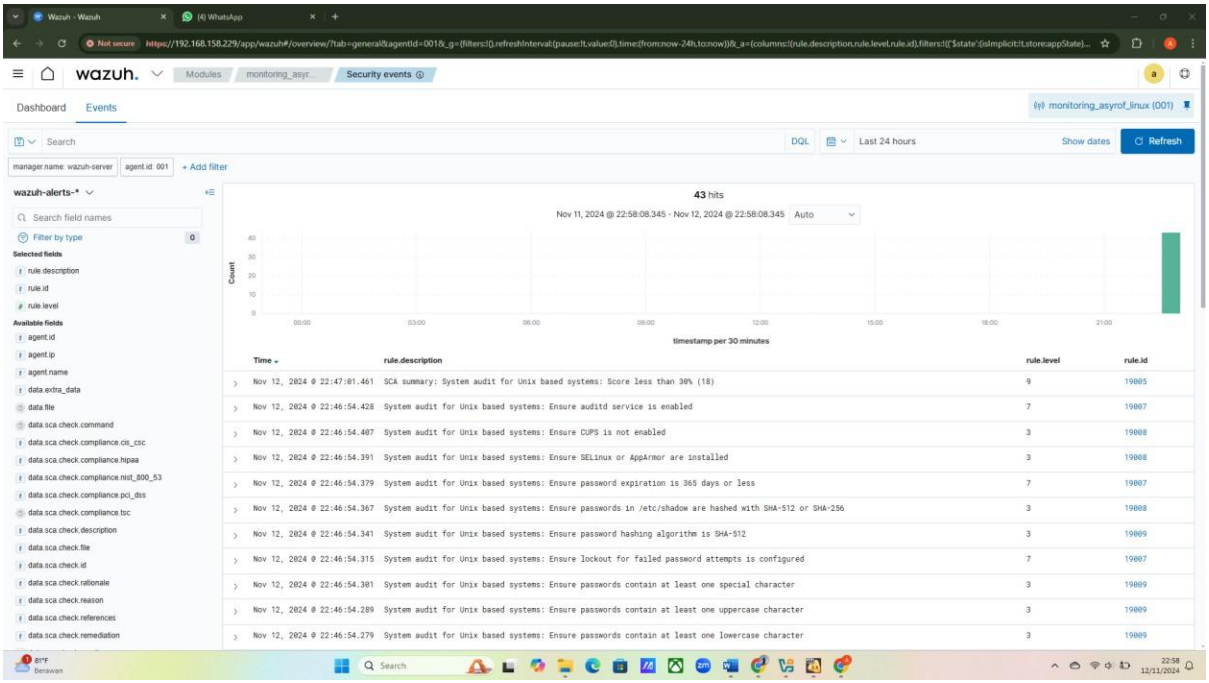
- Disini terlihat ada total alert nya 43
- Level 12 or above alerts pada angka 0 yang berarti tidak memiliki potensi ancaman yang tinggi
- Authentication failure pada angka 0 yang berarti usaha login yang gagal
- Authentication success pada angka 0 yang berarti ada 1 usaha login yang berhasil
- Top MITRE ATT&CKS menampilkan jenis serangan yang paling sering terjadi.
- Top 5 alert menunjukkan 5 agen (perangkat) teratas yang sering mengirim allert :



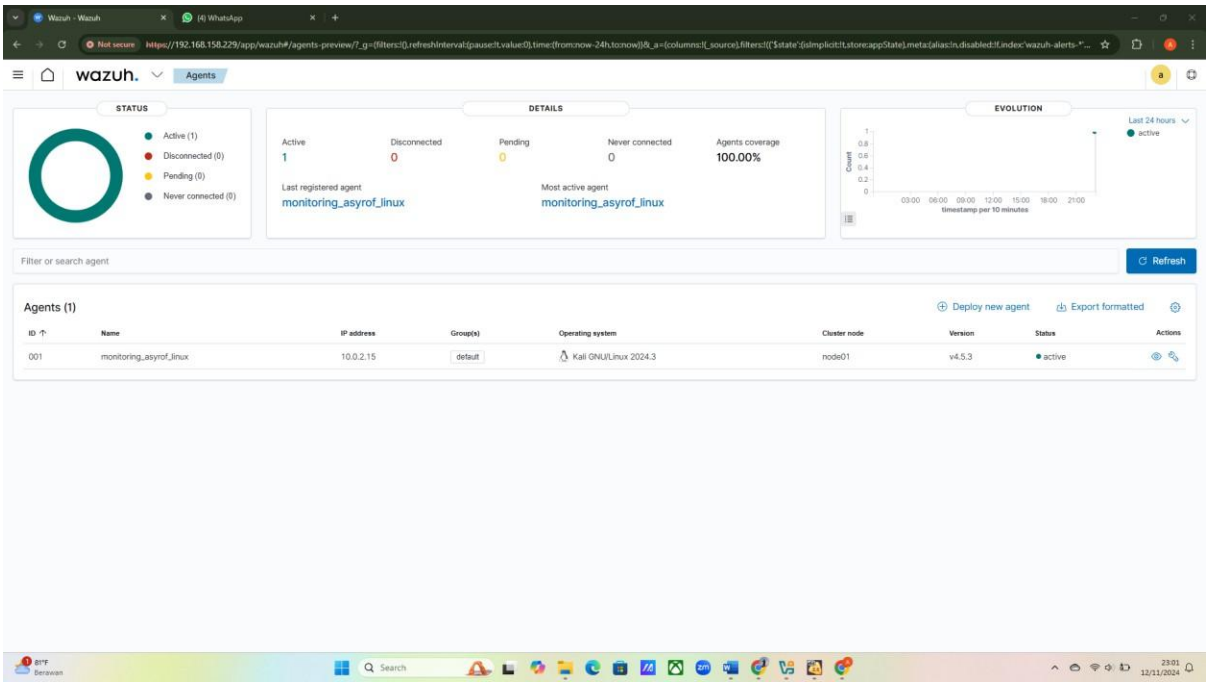
Secara keseluruhan, daftar **Security Alerts** ini memungkinkan administrator untuk meninjau masalah keamanan yang teridentifikasi pada sistem, prioritas penanganannya berdasarkan tingkat keparahan, serta memastikan bahwa semua persyaratan konfigurasi dan keamanan telah dipenuhi sesuai dengan standar atau kebijakan yang diterapkan :



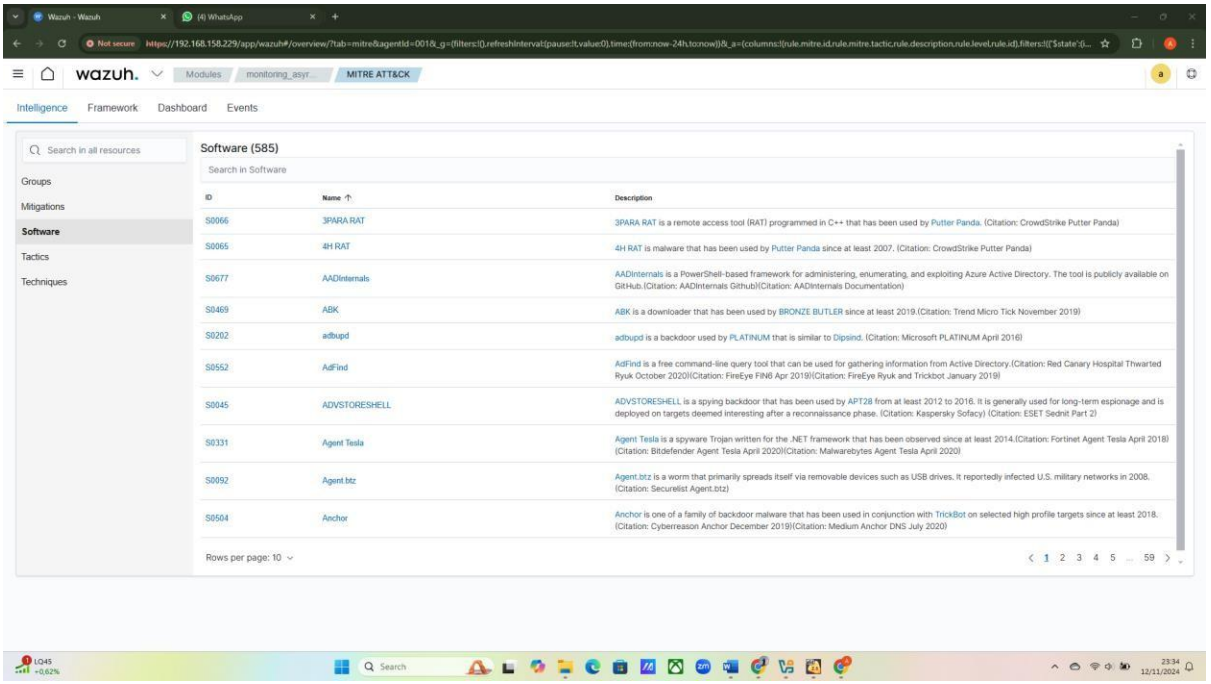
Gambar ini menunjukkan dashboard Wazuh pada tab Events, yang menampilkan log hasil audit keamanan sistem. Masing-masing aturan memiliki level prioritas yang menunjukkan tingkat keparahannya, serta ID unik untuk identifikasi. Grafik di atasnya memperlihatkan jumlah kejadian dalam rentang waktu tertentu, membantu mendeteksi pola aktivitas keamanan di sistem:



Pada dasarnya, gambar ini menunjukkan bahwa agen monitoring_asyrof_linux berhasil terhubung dengan Wazuh Server dan aktif untuk monitoring, dengan informasi terkait sistem operasi dan status koneksi yang stabil :



Tampilan ini berguna untuk memberikan pemahaman tentang jenis-jenis ancaman perangkat lunak yang mungkin terdeteksi di jaringan atau mesin yang dimonitor oleh Wazuh. Dengan informasi ini, administrator dapat mengidentifikasi jenis malware atau trojan tertentu dan memahami taktik yang mungkin digunakan oleh penyerang :

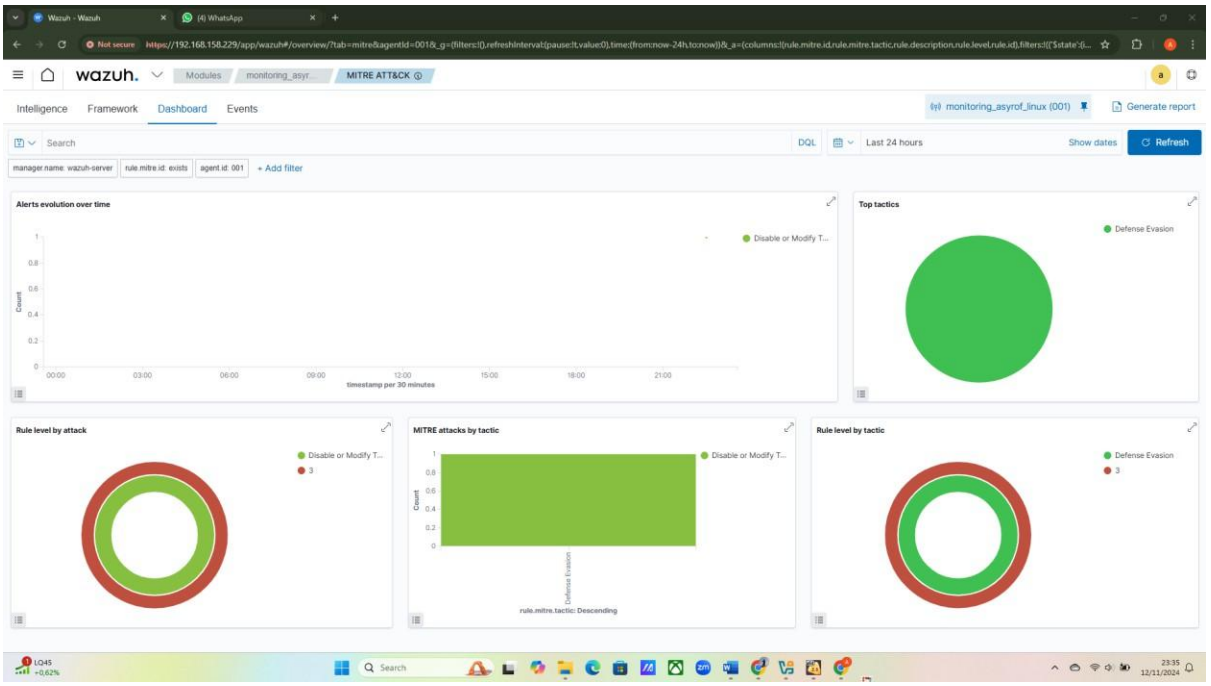


Gambar ini adalah tampilan **MITRE ATT&CK Dashboard** di Wazuh, yang menunjukkan statistik tentang ancaman dan aktivitas terkait taktik keamanan yang terjadi pada agen yang dimonitor (dalam hal ini, agen bernama monitoring_asyrof_linux). Dashboard ini memberikan visualisasi terkait pola ancaman dan informasi mengenai teknik yang digunakan dalam serangan.

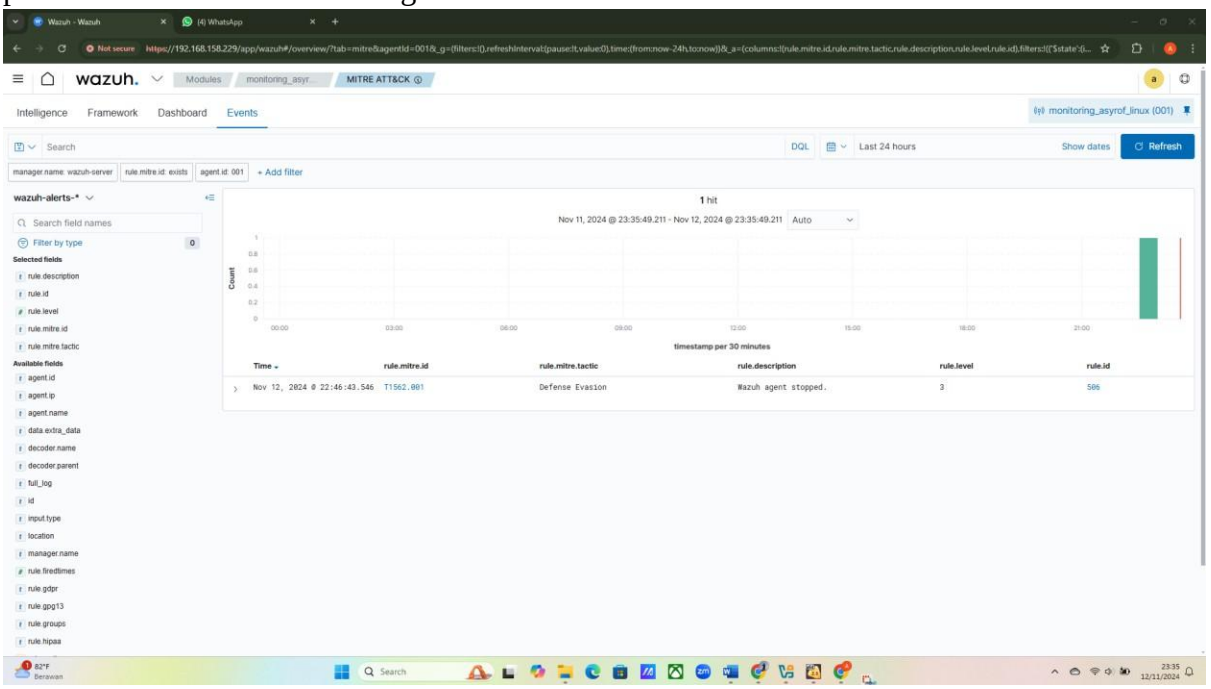
Dashboard ini memberikan wawasan tentang taktik yang digunakan oleh penyerang dan bagaimana aturan keamanan diatur untuk mengatasi taktik-taktik tersebut. Tampilan ini mempermudah administrator untuk:

- Mengidentifikasi pola taktik serangan yang paling sering digunakan.
- Melihat jenis ancaman dan metode penghindaran deteksi yang digunakan oleh penyerang.
- Memahami efektivitas aturan keamanan dalam mendeteksi dan mengatasi ancaman berdasarkan taktik MITRE ATT&CK.

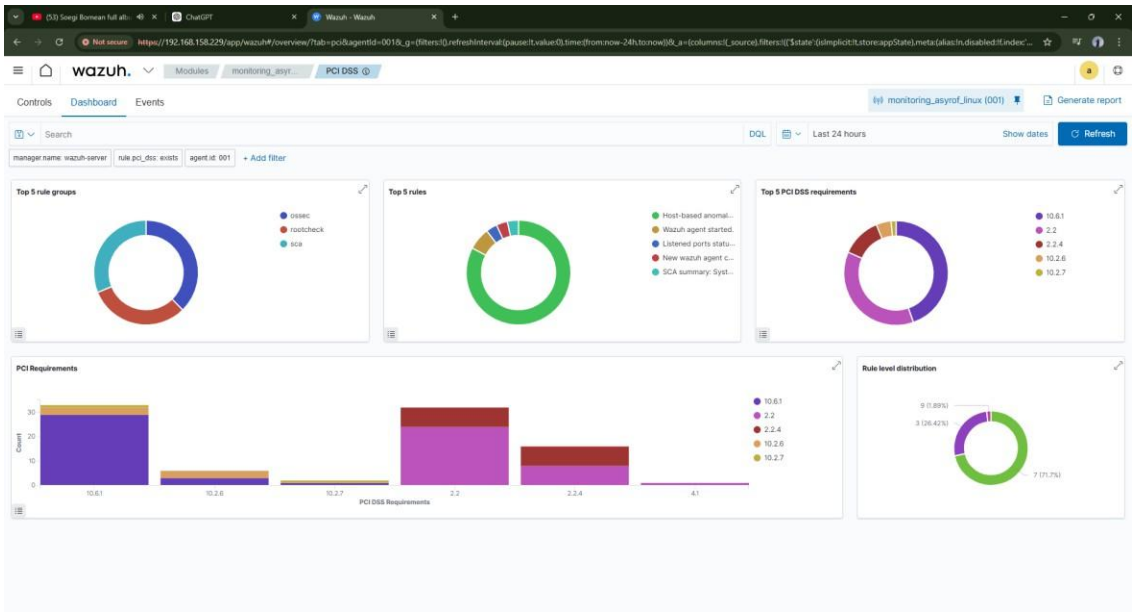
Dengan informasi ini, admin dapat mengoptimalkan aturan atau strategi pertahanan untuk mencegah serangan yang lebih spesifik di masa mendatang :



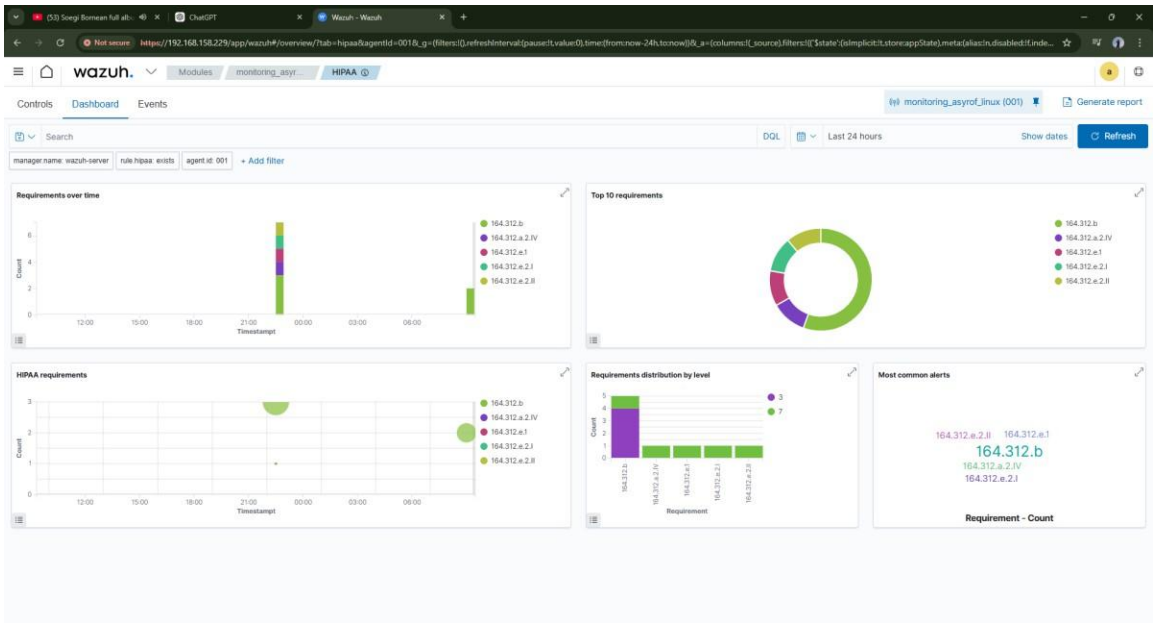
Gambar ini menunjukkan bahwa pada 12 November 2024, agen Wazuh di perangkat yang dipantau tiba-tiba berhenti. Ini dianggap sebagai upaya Defense Evasion (menghindari deteksi), karena mungkin ada seseorang atau sesuatu yang mencoba menghentikan pemantauan Wazuh untuk menghindari terdeteksi :



Gambar ini menunjukkan dashboard Wazuhyang memantau kepatuhan terhadap standar keamanan PCI DSS.Dashboard ini berisi beberapa grafik yang memberikan gambaran aturan yang diaudit, seperti kelompok aturan utama (ossec, rootcheck, sca), lima aturan yang paling sering muncul, serta lima persyaratan PCI DSS yang paling sering diaudit. Ada juga grafik yang menunjukkan jumlah kejadian berdasarkan persyaratan PCI DSS dan distribusi tingkat keparahan aturan. Secara keseluruhan, dashboard ini membantu memantau seberapa patuh sistem terhadap standar keamanan PCI DSS :



Gambar ini menunjukkan dashboard Wazuhyang memantau kepatuhan terhadap standar HIPAA.Dashboard ini menampilkan berbagai grafik untuk memantau persyaratan yang perlu dipenuhi, seperti jumlah persyaratan HIPAA yang terdeteksi seiring waktu, persyaratan yang paling sering muncul, dan distribusi tingkat keparahan aturan. Grafik ini juga memperlihatkan peringatan yang paling sering muncul, membantu mengidentifikasi area yang paling sering melanggar aturan. Secara keseluruhan, dashboard ini membantu memastikan bahwa sistem mengikuti standar keamanan data sesuai ketentuan HIPAA :


wazuh.
Modules
monitoring_asyr...
HIPAA
Controls
Dashboard
Events
monitoring_asyrof_linux (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.hipaa: exists
agent.id: 001
+ Add filter
Requirements over time
Count
Timestamp
12:00
15:00
18:00
21:00
00:00
03:00
06:00
164.312.b
164.312.a.2.IV
164.312.e.1
164.312.e.2.I
164.312.e.2.II
Top 10 requirements
HIPAA requirements
Requirements distribution by level
Requirement
Most common alerts
164.312.e.2.II
164.312.e.1
164.312.b
164.312.a.2.IV
164.312.e.2.I
Requirement - Count