

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>

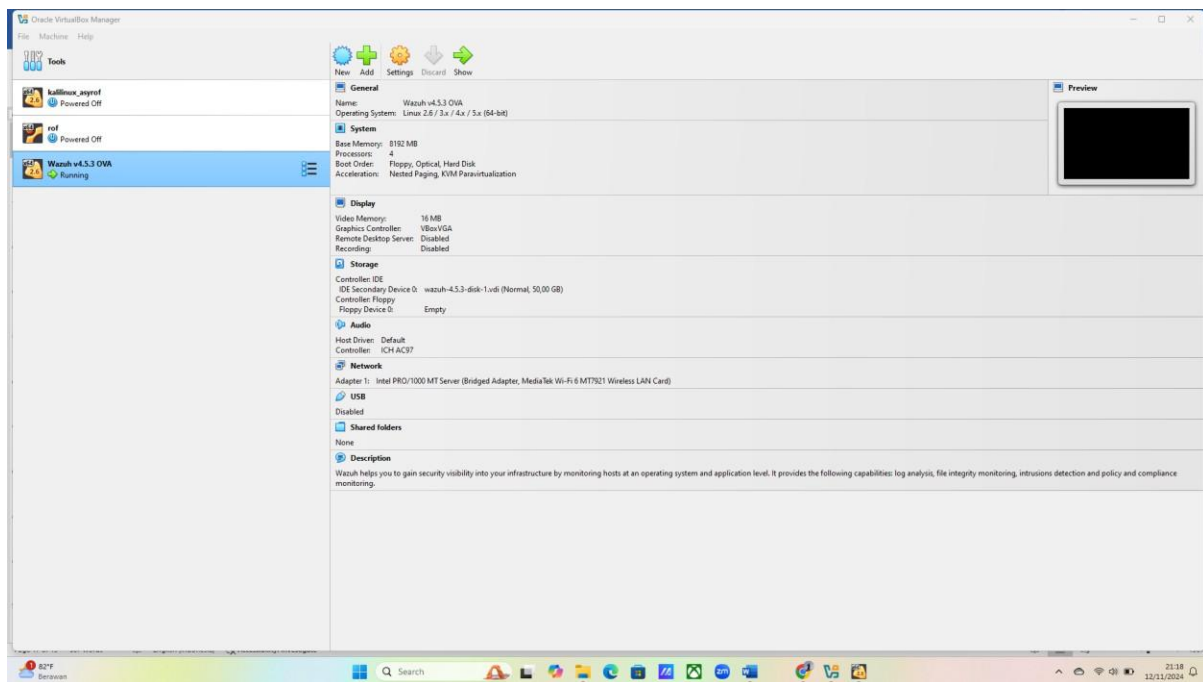
2. Pelajari fitur fiturnya dan jelaskan dengan bahasa Anda sendiri dengan menunjukkan menu/tampilan Wazuh tersebut
3. Pasang Wazuh-Agent disalah satu mesin/VM lain (dan hubungkan ke SIEM Wazuh) sehingga dapat dimonitor dan audit dari SIEM Wazuh.

Ref. <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>

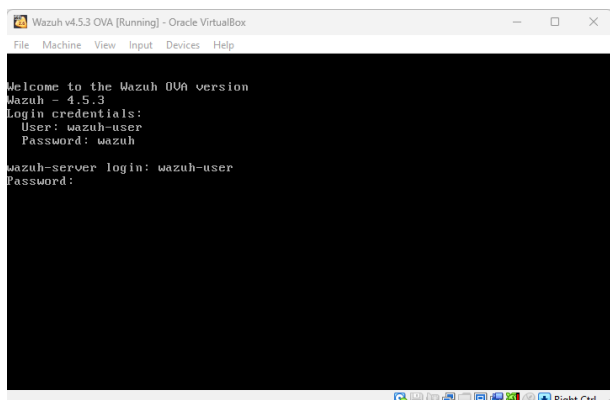
Jelaskan apa saja yang dapat dimonitor oleh SIEM Wazuh tersebut.

Jawab :

1. Install VM SIEM Wazuh menggunakan OVA di virtualbox :



Login wazuh :



Setelah login cek ip web wazuh dengan perintah ifconfig :

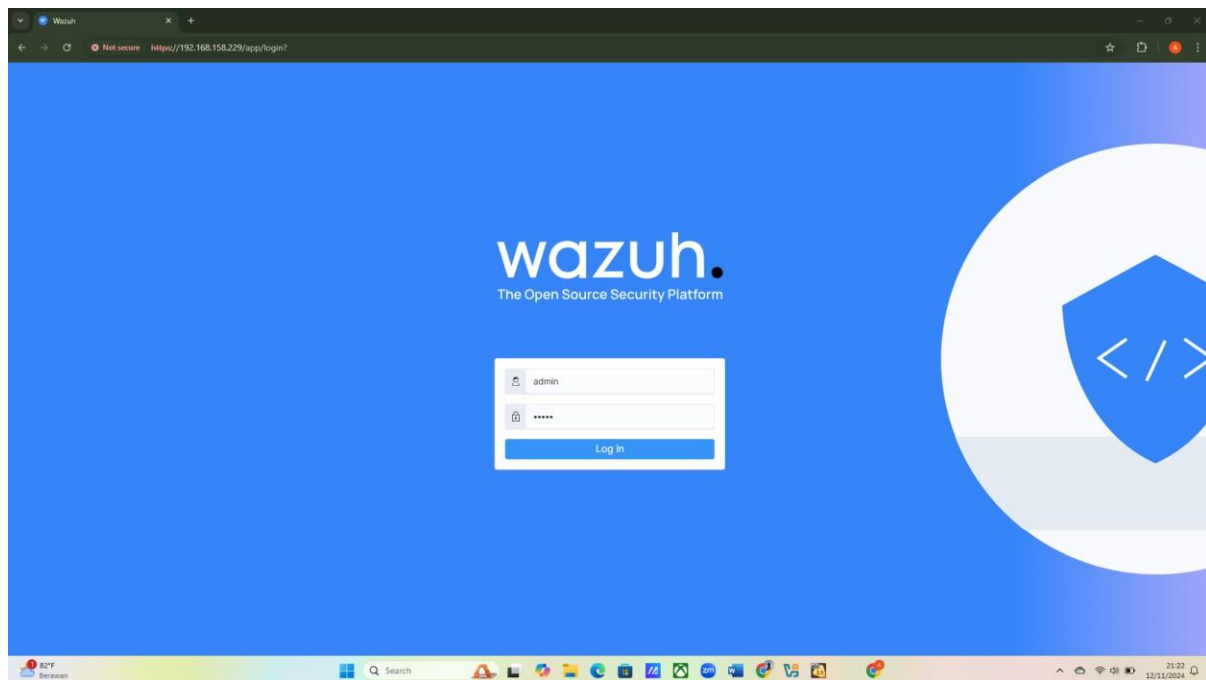
```
Wazuh v4.5.3 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help

No packages needed for security; 3 packages available
Run "sudo yum update" to apply all updates.
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.158.229 netmask 255.255.255.0 broadcast 192.168.158.255
    inet6 fe80::a00:27ff:fe53:9ac9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:53:9a:c9 txqueuelen 1000 (Ethernet)
    RX packets 219 bytes 254953 (248.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 208 bytes 16729 (16.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

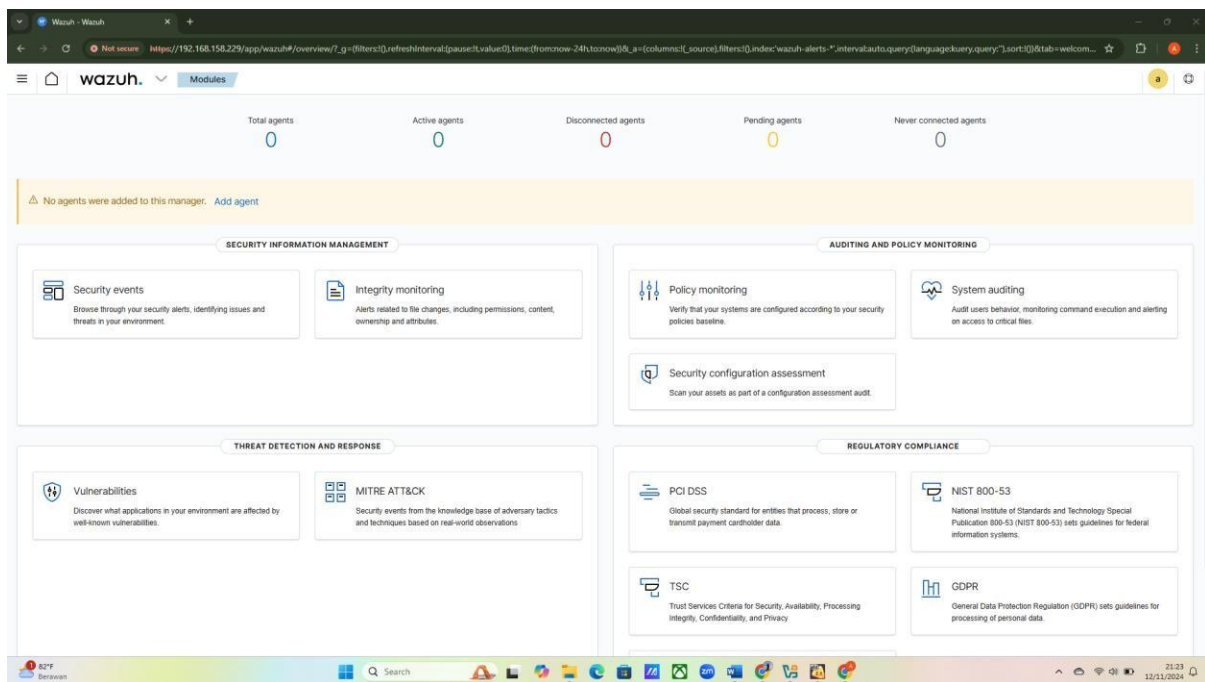
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 25 bytes 1720 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 1720 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[wazuh-user@wazuh-server ~]$ [ 100.098113] vboxvideo: loading version 6.1.42 r1
55177
```

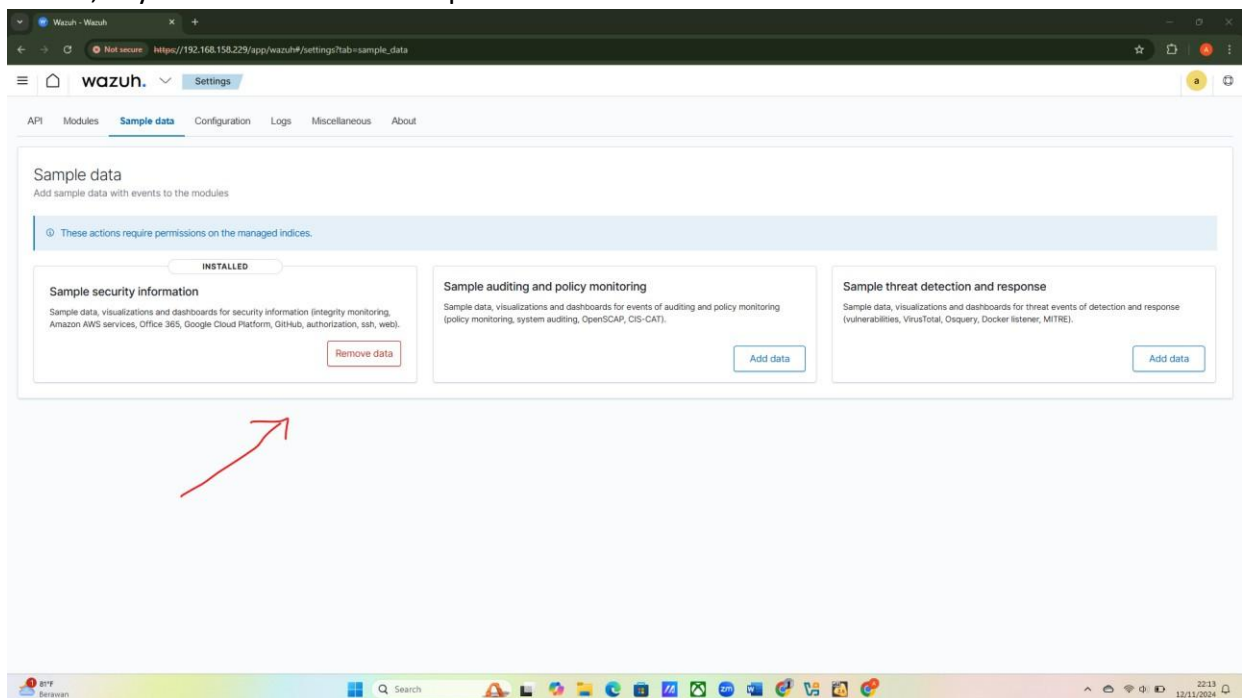
Akses web wazuh denga nip yang sudah didapatkan :



Tampilan awal web wazuh :

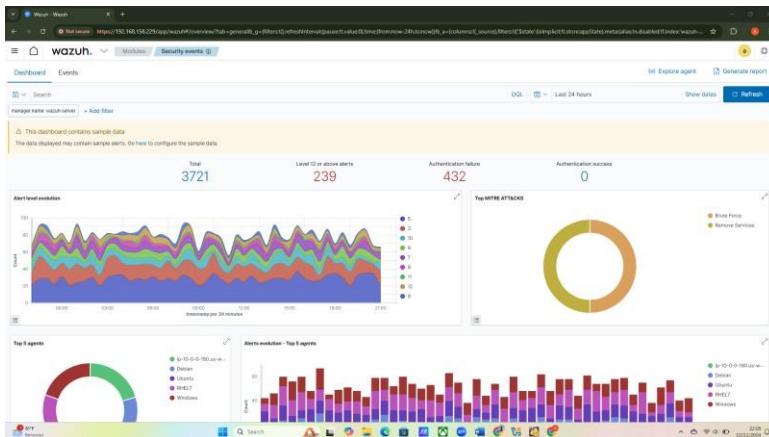


2. Penjelasan beberapa fitur/tampilan dashboard pada wazuh, Saya sudah download sample data :



1. Dashboard Overview:

Berisi data-data dari agen (perangkat) berupa diagram dan keterangannya



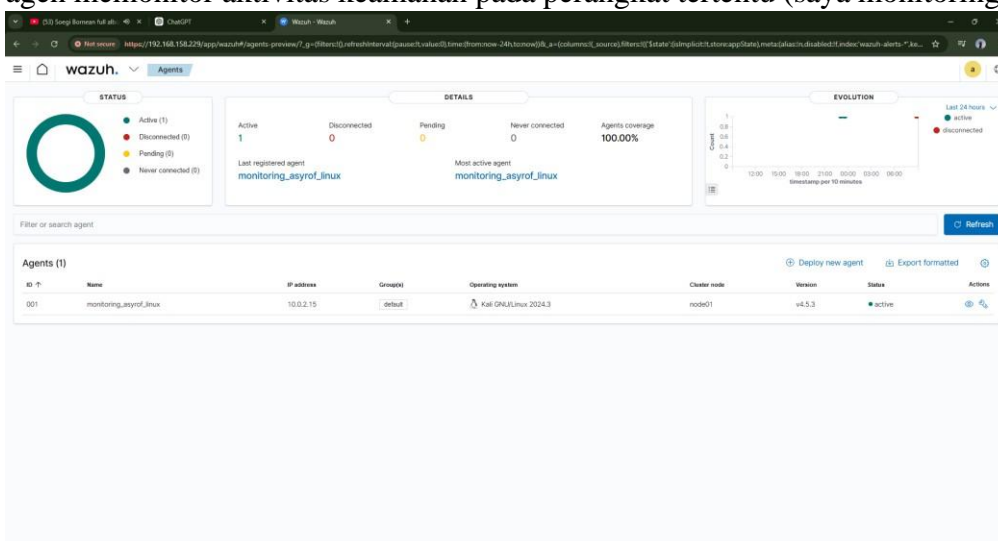
2. Security Events:

Daftar peringatan keamanan secara rinci, penjabaran bagaimana setiap alert memberikan informasi tentang jenis serangan, sumber, dan waktu kejadian.

Time	Agent	Agent name	Source	Target	Description	Level	Rule ID
Nov 12, 2024 @ 21:20:58.180	001	Debian	Windows	Service startup type was changed.		5	5698
Nov 12, 2024 @ 21:20:58.453	001	DEBIAN	Web server	403 error code.		5	3101
Nov 12, 2024 @ 21:20:58.482	004	Ubuntu	Multiple web server	403 error codes from same source ip.		10	3101
Nov 12, 2024 @ 21:20:58.519	003	ip-10-0-0-100.us-east-1-compute.internal	Web server	403 error code.		5	3101
Nov 12, 2024 @ 21:24:08.865	000	wazuh-server	Office 365	SharePoint sharing events.		3	91544
Nov 12, 2024 @ 21:25:01.855	001	DEBIAN	Apache	Attempt to access forbidden directory index.		5	30308
Nov 12, 2024 @ 21:25:01.855	002	Amazon	AWX	SwanProxy PORT_PROBE - Unresponsive port on EC2 instance i-0c4a6b3d07b14400 is being probed. EP: 10.24.101.2143 (Port: 80).		5	80305
Nov 12, 2024 @ 21:25:39.762	000	wazuh-server	Unresponsive port	on EC2 instance i-0c4a6b3d07b14400 is being probed. EP: 10.24.101.2143 (Port: 80).		7	533
Nov 12, 2024 @ 21:21:45.864	008	Windows	AWX	SwanProxy PORT_PROBE - Unresponsive port on EC2 instance i-0c4a6b3d07b14400 is being probed. EP: 10.24.101.2143 (Port: 80).		5	80305
Nov 12, 2024 @ 21:21:46.482	002	Amazon	SCP	warning event from IAM 101.139.29313 instance - with source IP 10.24.101.2143 from wazuh-agent.		5	65034

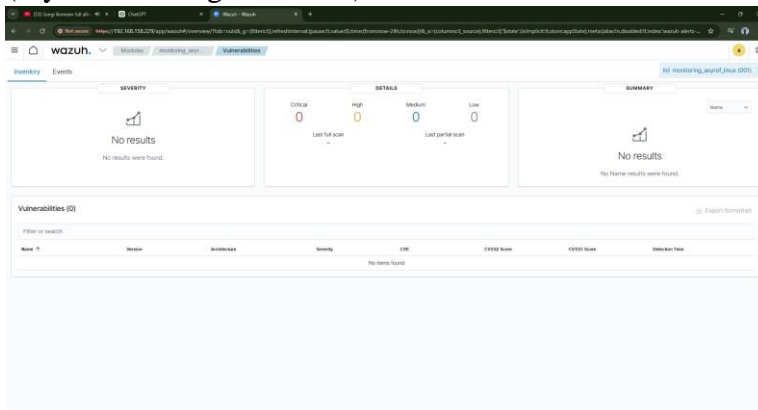
3. Agent Management:

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



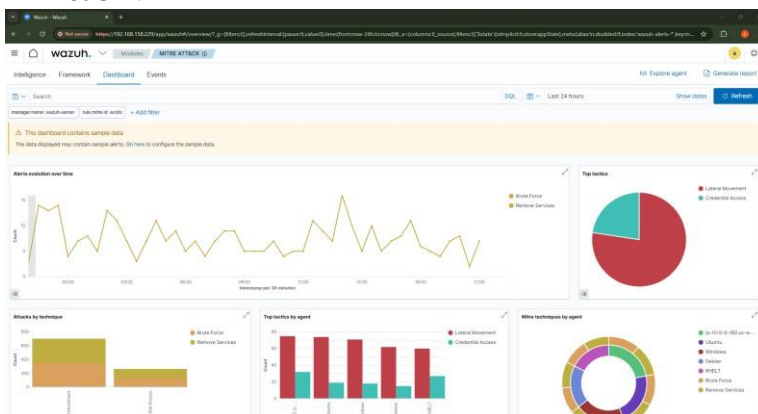
4. Vulnerability Detection:

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.

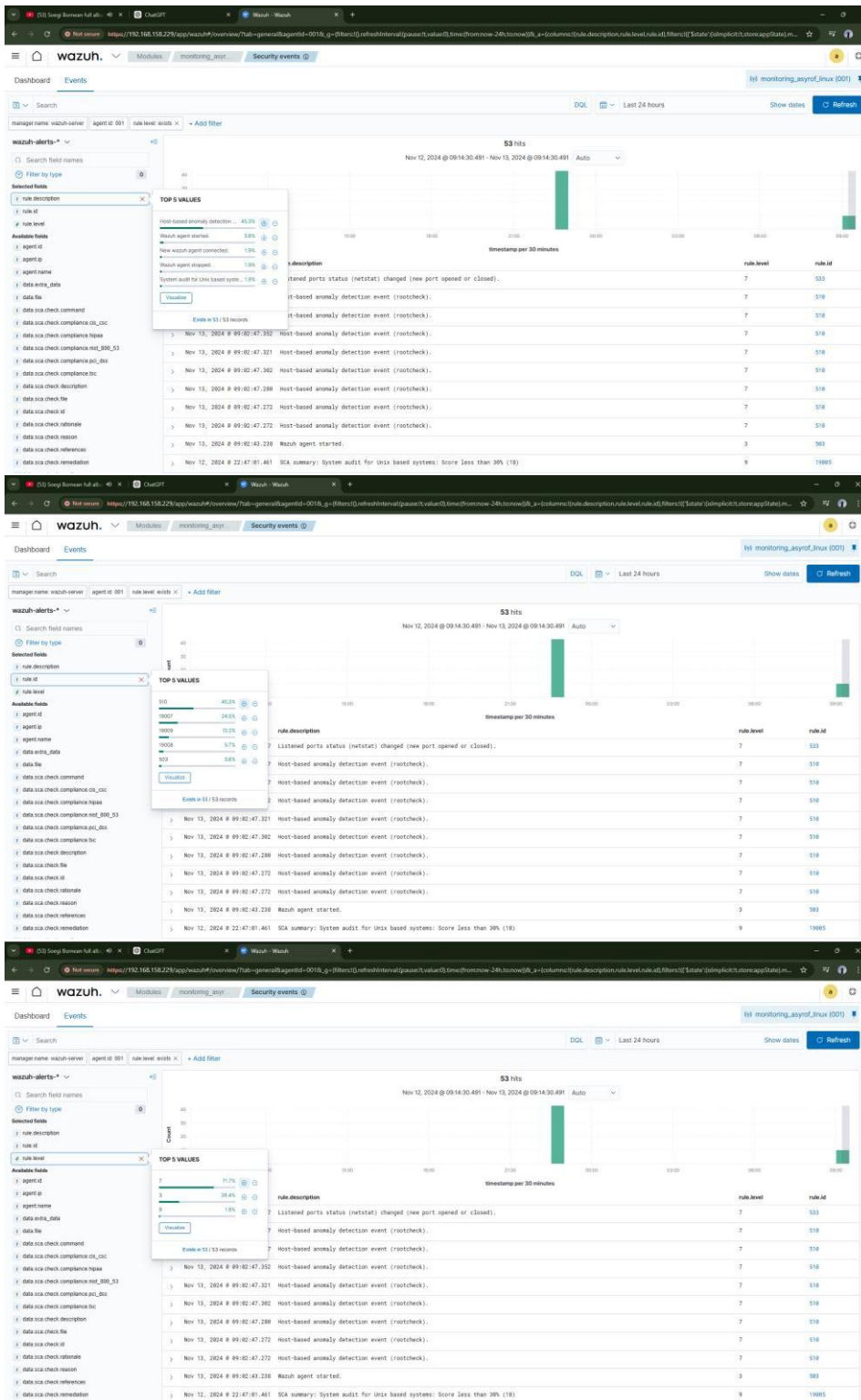


6. File Integrity Monitoring (FIM):

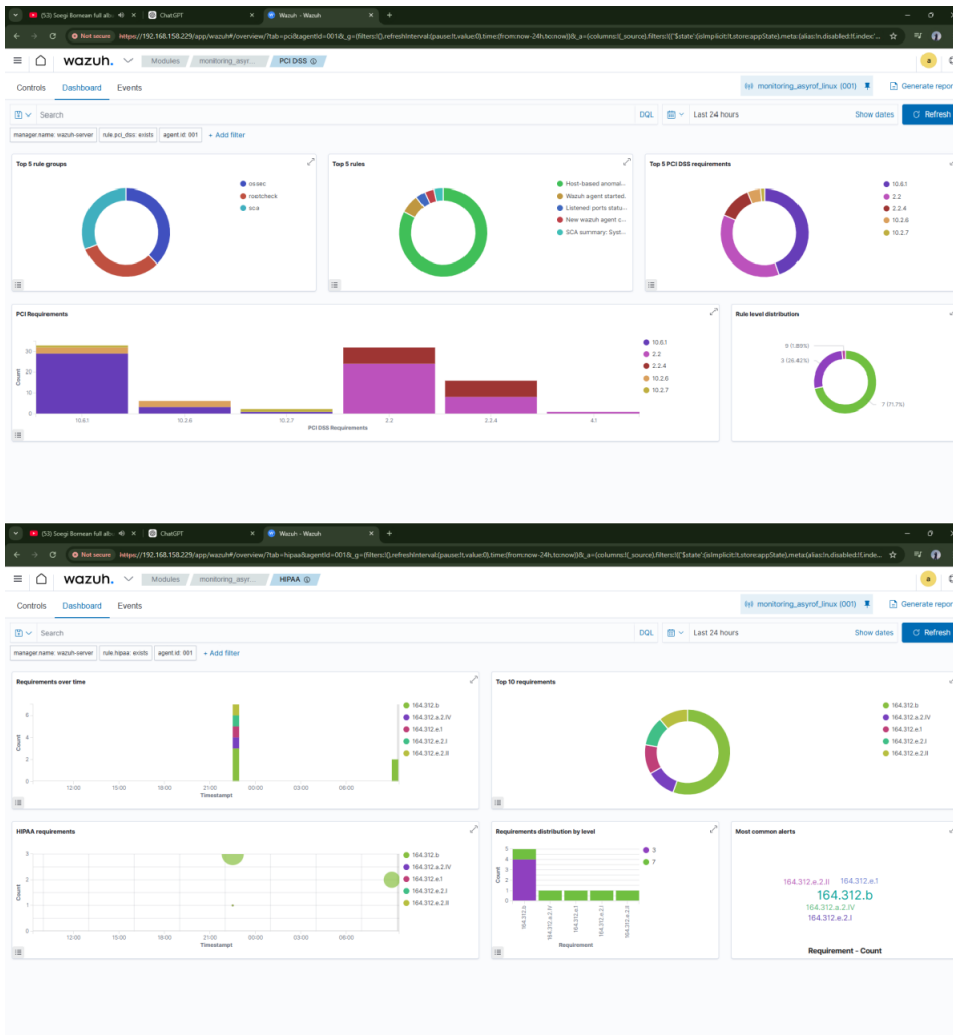
Melacak perubahan pada file penting dalam sistem. Fitur ini bisa ditunjukkan melalui log atau tampilan FIM di Wazuh untuk memperlihatkan file mana yang diubah, kapan, dan oleh siapa.

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) :



- 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:~# 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 :

The screenshot displays the Wazuh Agents deployment wizard, which is a multi-step process for installing and configuring Wazuh agents. The interface is clean and modern, with a light blue header and a white main content area. The steps are numbered 1 through 7, and the current step is highlighted with a blue circle and a blue bar on the right side of the step indicator.

Step 1: Choose the operating system

This step allows the user to select the operating system for the agent. The options are presented in a grid of buttons. The selected option, **Debian**, is highlighted with a blue border. Below the grid, there is a "Show less" link.

Step 2: Choose the version

This step allows the user to select the version of the agent. The options are presented in a row of buttons. The selected option, **Debian 9 +**, is highlighted with a blue border.

Step 3: Choose the architecture

This step allows the user to select the architecture of the agent. The options are presented in a row of buttons. The selected option, **x86_64**, is highlighted with a blue border.

Step 4: Wazuh server address

This step allows the user to enter the Wazuh server address. The text below the input field states: "This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN)." The input field contains the address **192.168.158.229**.

Step 5: Optional settings

This step allows the user to configure optional settings for the agent. The text below the input field states: "The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below." The input field contains the name **monitoring_asyrof_linux**. Below the input field, there is a warning message: "The agent name must be unique. It can't be changed once the agent has been enrolled." Below the warning message, there is a section for "Select one or more existing groups" with a dropdown menu showing **default**.

Step 6: Install and enroll the agent

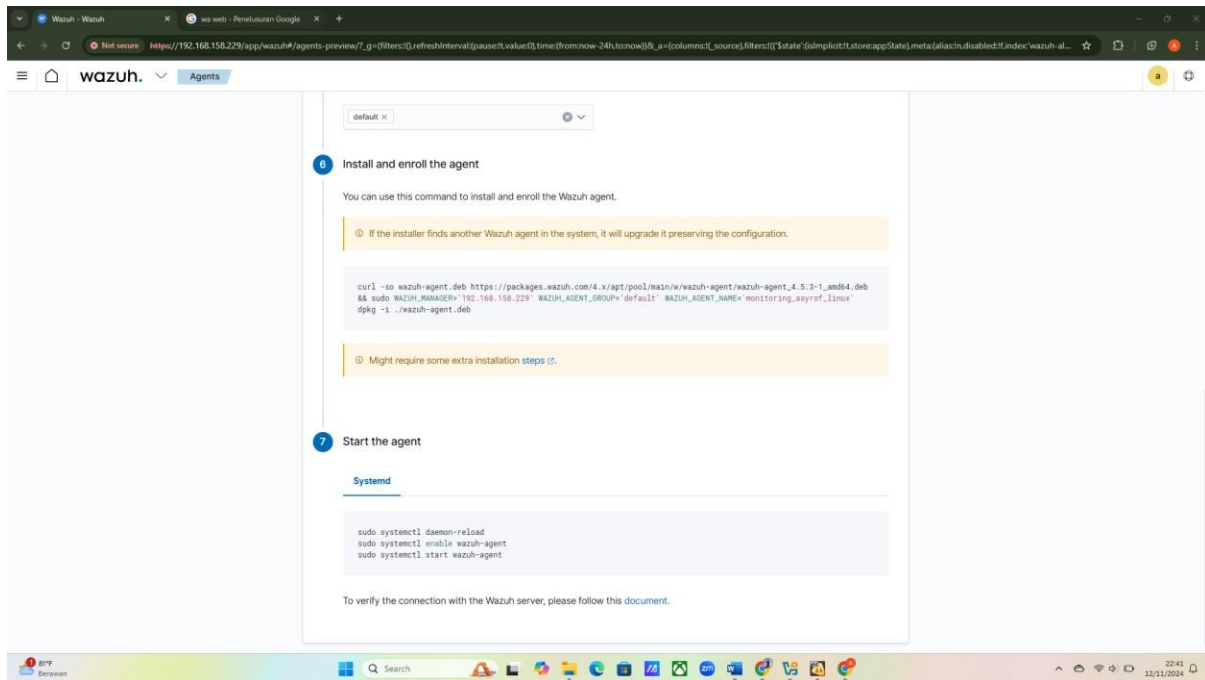
This step provides the command to install and enroll the agent. The text below the code block states: "You can use this command to install and enroll the Wazuh agent." Below the code block, there is a warning message: "If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration." Below the warning message, there is a code block containing the command:

```
curl -s -o 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
```

Below the code block, there is a warning message: "Might require some extra installation steps." Below the warning message, there is a link to "steps".

Step 7: Start the agent

This step is the final step in the deployment process. It is currently not visible in the screenshot.



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
```

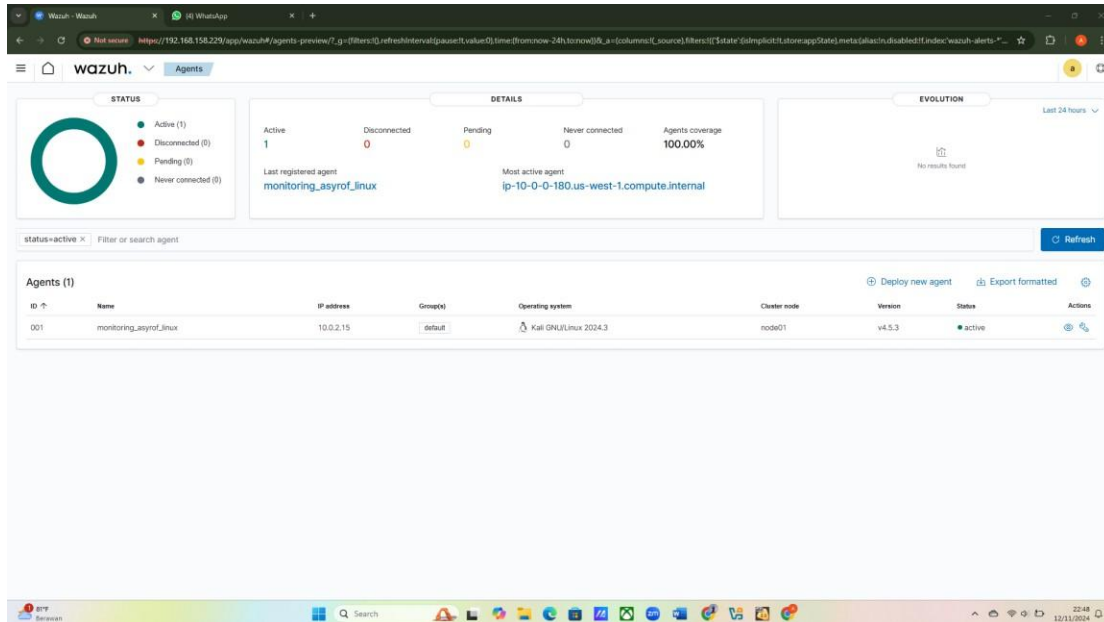
```
(root@asyrof)~[/home/asyrof]
# curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.3-1_amd64.deb 66 sudo WAZUH_MANAGER='192.168.158.229' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='monitoring_asyrof_linux' dpkg -i ./wazuh-agent.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 438153 files and directories currently installed.)
Preparing to unpack ./wazuh-agent.deb ...
Unpacking wazuh-agent (4.5.3-1) ...
Setting up wazuh-agent (4.5.3-1) ...
```

Start wazuh agen pada kali linux :

```
(root@asyrof)~[/home/asyrof]
# service wazuh-agent start
```

Monitoring kali linux sudah berhasil:

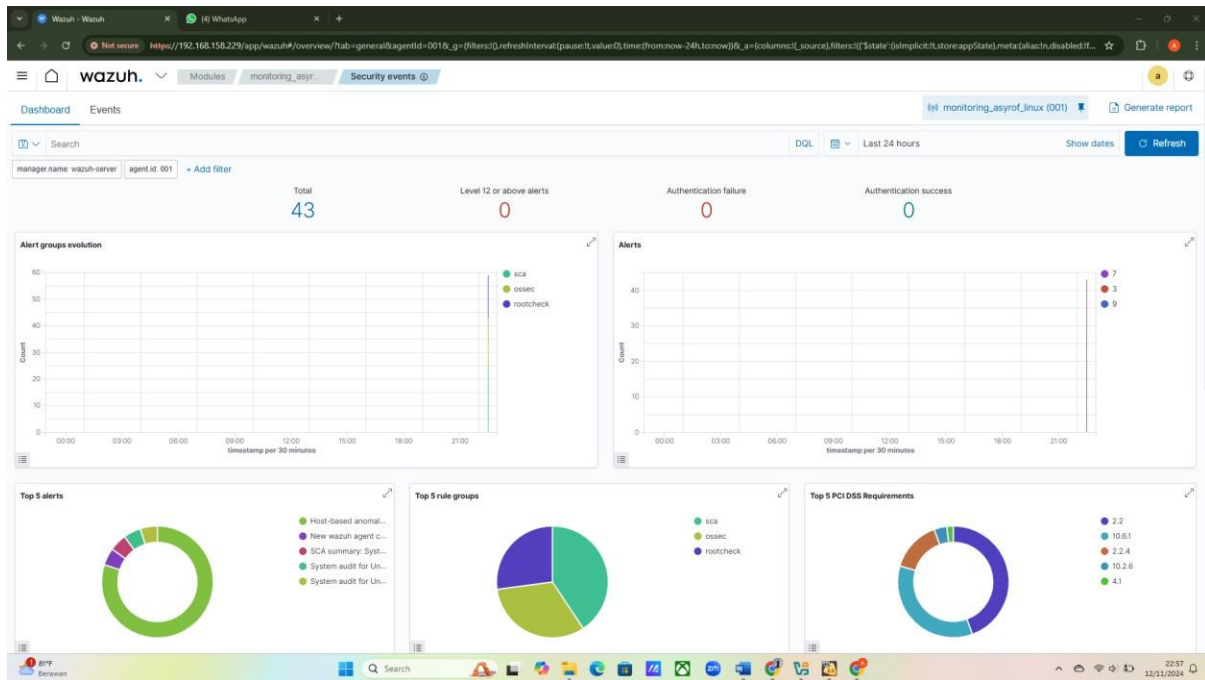
Fitur ini secara keseluruhan berguna untuk memantau status, aktivitas, dan koneksi dari setiap agen yang berhubungan dengan Wazuh Manager, sehingga memudahkan dalam pengelolaan dan pemantauan sistem.



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 :

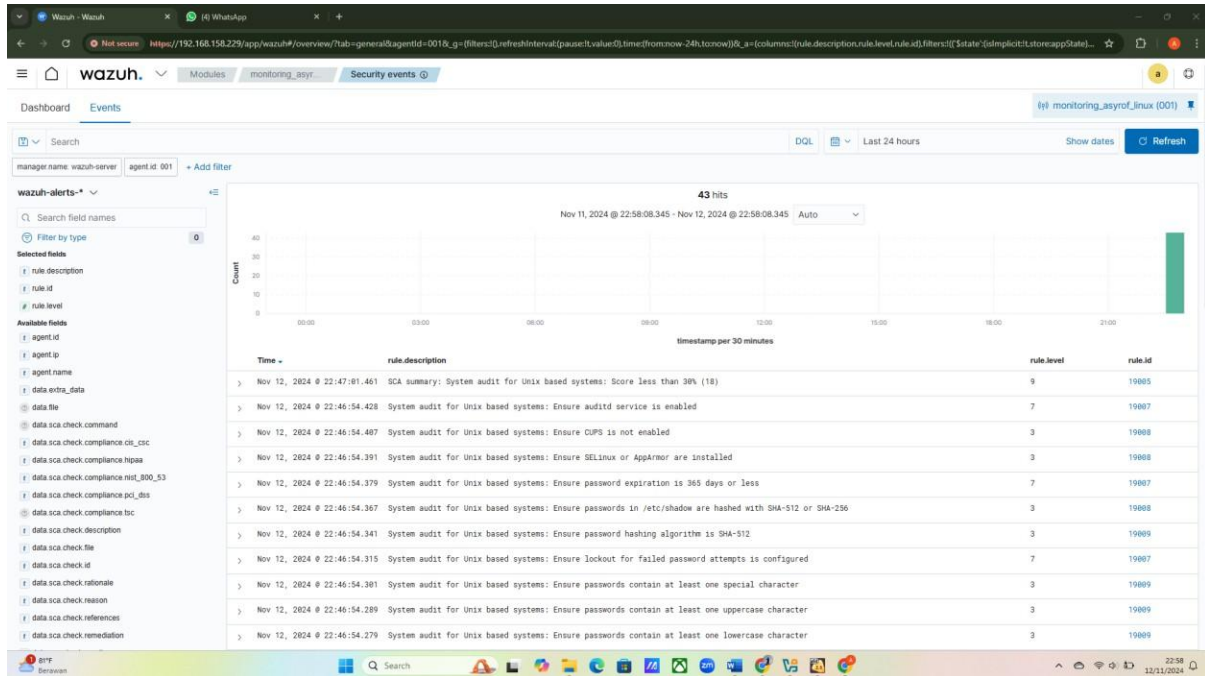


Secara keseluruhan, daftar **Security Alerts** ini memungkinkan administrator untuk meninjau masalah keamanan yang teridentifikasi pada sistem, prioritas penanganannya berdasarkan tingkat keparahan, serta memastikan bahwa semua persyaratan konfigurasi dan keamanan telah dipenuhi sesuai dengan standar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

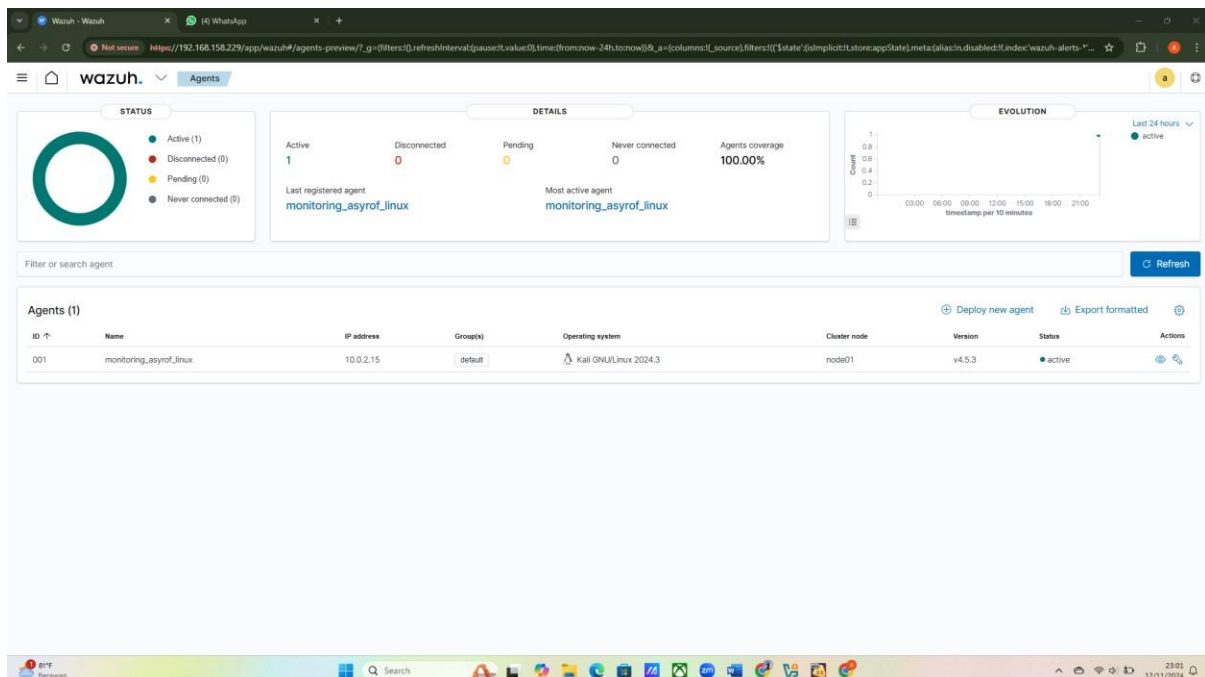
The screenshot displays the Wazuh Security Alerts table. The table has columns for Time, Technique(s), Tactics, Description, Level, and Rule ID. The table lists 10 alerts, each with a timestamp, a description of the alert, a level, and a rule ID. The alerts are related to system audit for Unix based systems, including checks for auditd service, CLUPS, SELinux, AppArmor, password expiration, password hashing, password lockout, password complexity, and password case requirements.

Time	Technique(s)	Tactics	Description	Level	Rule ID
Nov 12, 2024 @ 22:47:01.461			SCA summary: System audit for Unix based systems: Score less than 30% (18)	9	19005
Nov 12, 2024 @ 22:46:54.428			System audit for Unix based systems: Ensure auditd service is enabled	7	19007
Nov 12, 2024 @ 22:46:54.407			System audit for Unix based systems: Ensure CLUPS is not enabled	3	19008
Nov 12, 2024 @ 22:46:54.391			System audit for Unix based systems: Ensure SELinux or AppArmor are installed	3	19008
Nov 12, 2024 @ 22:46:54.379			System audit for Unix based systems: Ensure password expiration is 365 days or less	7	19007
Nov 12, 2024 @ 22:46:54.367			System audit for Unix based systems: Ensure passwords in /etc/shadow are hashed with SHA-512 or SHA-256	3	19008
Nov 12, 2024 @ 22:46:54.341			System audit for Unix based systems: Ensure password hashing algorithm is SHA-512	3	19009
Nov 12, 2024 @ 22:46:54.315			System audit for Unix based systems: Ensure lockout for failed password attempts is configured	7	19007
Nov 12, 2024 @ 22:46:54.301			System audit for Unix based systems: Ensure passwords contain at least one special character	3	19009
Nov 12, 2024 @ 22:46:54.289			System audit for Unix based systems: Ensure passwords contain at least one uppercase character	3	19009

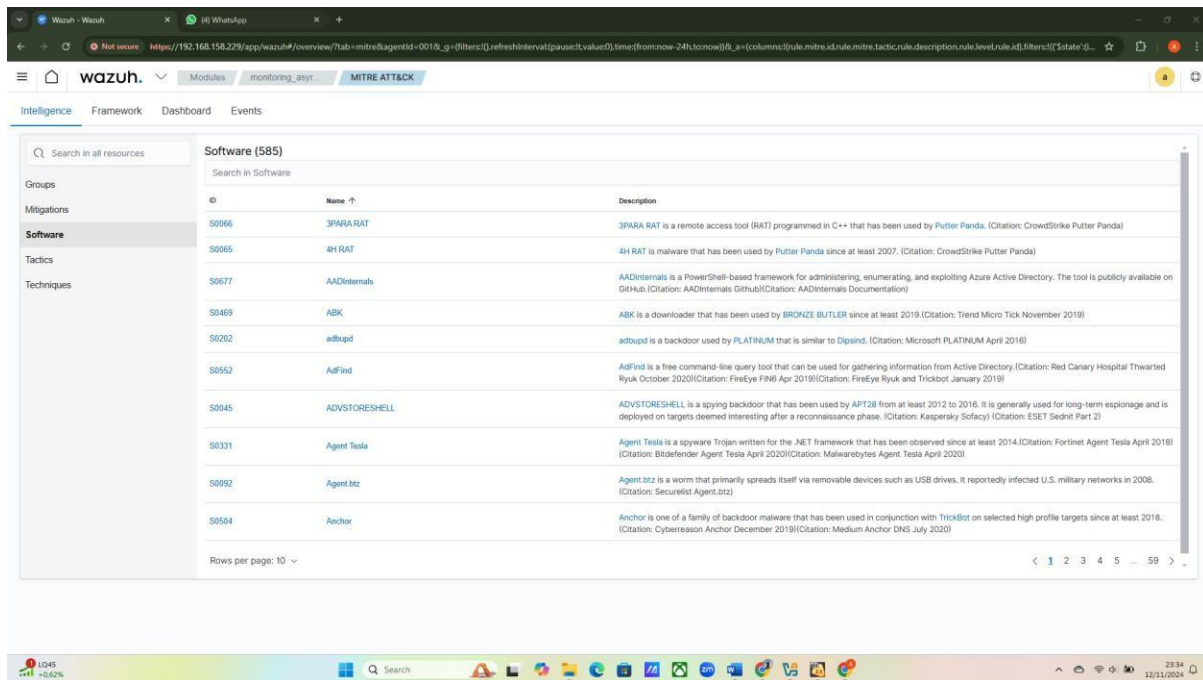
Gambar ini menunjukkan dashboard Wazuh pada tab Events, yang menampilkan log hasil audit keamanan sistem. Masing-masing aturan memiliki level prioritas yang menunjukkan tingkat keparahannya, serta ID unik untuk identifikasi. Grafik di atasnya memperlihatkan jumlah kejadian dalam rentang waktu tertentu,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

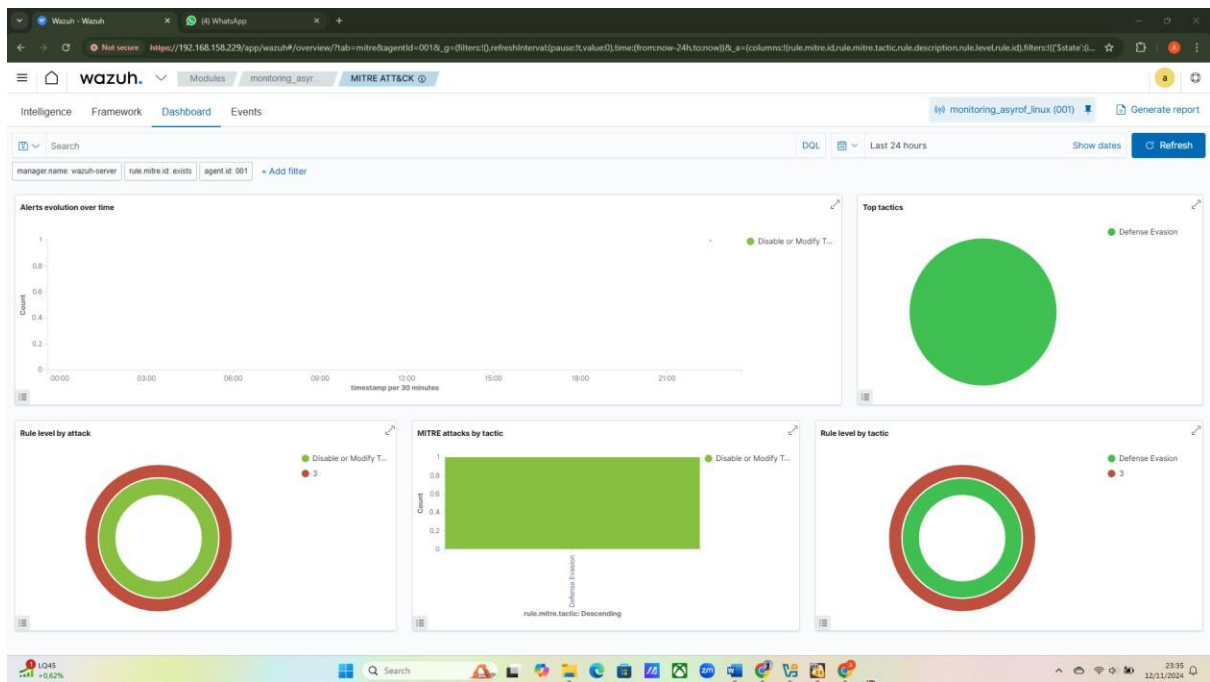


Gambar ini adalah tampilan **MITRE ATT&CK Dashboard** di Wazuh, yang menunjukkan statistik tentang ancaman dan aktivitas terkait taktik keamanan yang terjadi pada agen yang dimonitor (dalam hal ini, agen bernama `monitoring_asyrof_linux`). Dashboard ini memberikan visualisasi terkait pola ancaman dan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

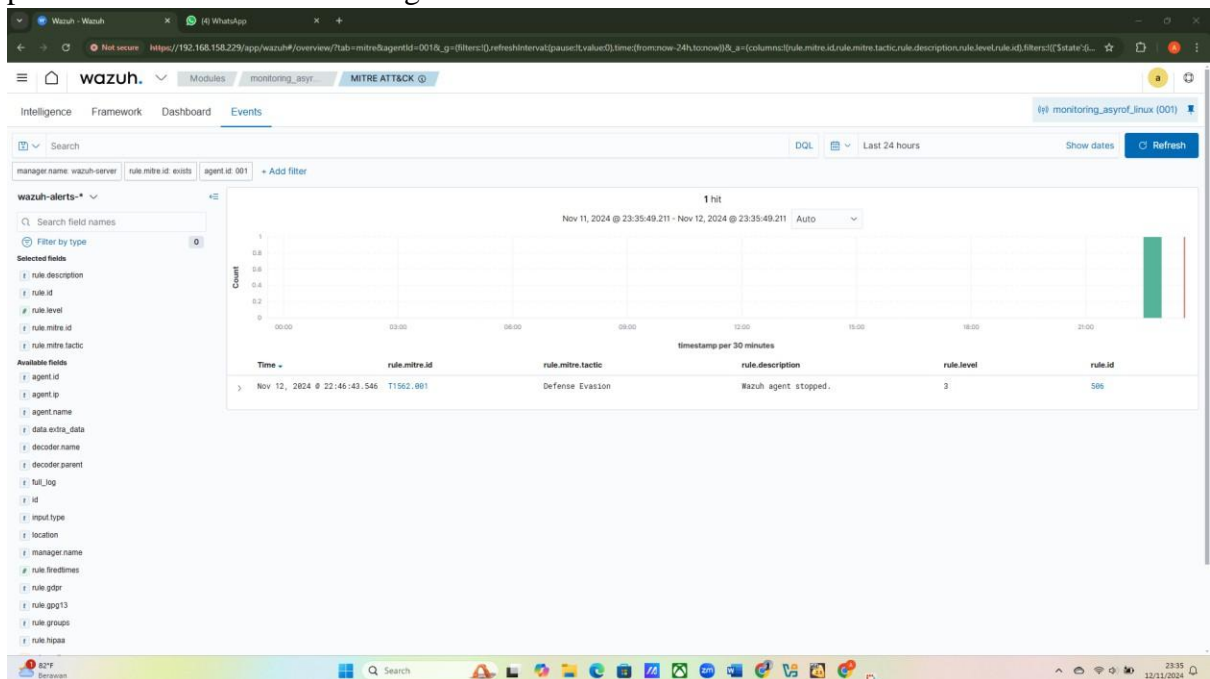
Dashboard ini memberikan wawasan tentang taktik yang digunakan oleh penyerang dan bagaimana aturan keamanan diatur untuk mengatasi taktik-taktik tersebut. Tampilan ini mempermudah administrator untuk:

- 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.

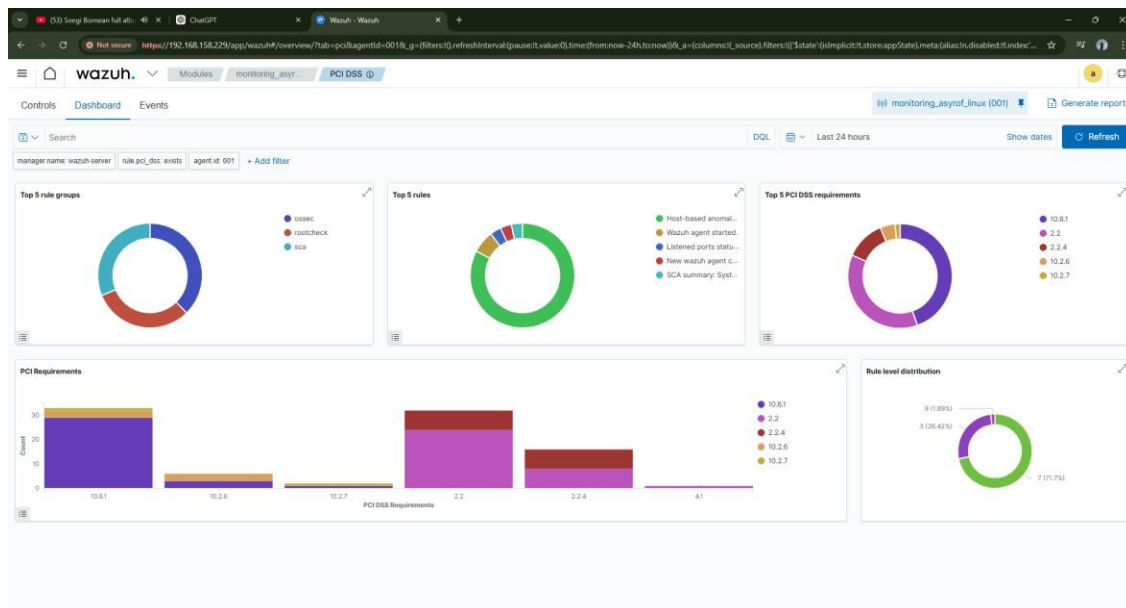
Dengan informasi ini, admin dapat mengoptimalkan aturan atau strategi pertahanan untuk mencegah serangan yang lebih spesifik di masa mendatang :



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 Wazuh yang 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 Wazuh yang 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 :

