Blog Igor_sec

Halo! Selamat datang di blog saya, tempat saya memposting tulisan-tulisan untuk tantangan CTF.

14 Agustus 2023 · Laboratorium rumah

Wazuh | Bagian 2: Menginstal Wazuh dan Mengonfigurasi Server

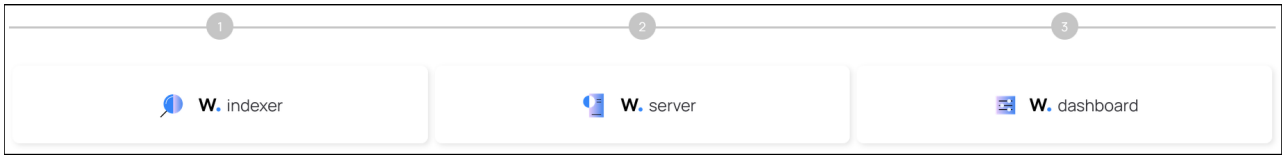
Selamat datang di bagian 2 perjalanan saya menjelajahi Wazuh untuk mendapatkan gambaran pengalaman nyata dalam menggunakan platform pemantauan keamanan tingkat perusahaan.

Pada bagian pertama, saya membahas pengenalan singkat tentang Wazuh, komponen dan kemampuannya sebagai platform pemantauan keamanan sumber terbuka yang menyediakan deteksi ancaman, pemantauan integritas, respons insiden, dan kepatuhan.

Pada bagian kedua seri Wazuh ini, saya akan menginstal Wazuh dan komponen-komponennya, mengonfigurasi server, dan melihat-lihat antarmuka dasbor.

Perkenalan

Ada beberapa metode untuk menginstal Wazuh, tetapi alur kerjanya sama. Metode instalasi mungkin bergantung pada tujuan atau ukuran lingkungan yang membutuhkan pemantauan dan perlindungan. Apa pun metode yang digunakan, alur kerja instalasi di bawah ini akan diikuti.



Demi efisiensi dan kepraktisan, saya akan menginstal server, pengindeks, dan dasbor di host yang sama, atau yang mereka sebut instalasi "all-in-one". Oleh karena itu, referensi saya untuk menginstal Wazuh adalah halaman Quickstart di situs web mereka.

Mulai Cepat

Panduan ini akan menginstal komponen sentral Wazuh pada host yang sama dengan bantuan asisten instalasi. Untuk metode instalasi Wazuh lainnya, Anda

dapat merujuk ke halaman Panduan Instalasi untuk detail selengkapnya dan opsi instalasi lainnya. Instalasi ini akan menginstal Wazuh hanya dalam beberapa menit.

Persyaratan

Berikut adalah persyaratan yang dibutuhkan untuk menginstal Wazuh.

Perangkat keras

Persyaratan ini sangat bergantung pada jumlah titik akhir yang dilindungi dan beban kerja cloud. Jumlah ini dapat membantu memperkirakan berapa banyak data yang akan dianalisis dan berapa banyak peringatan keamanan yang akan disimpan dan diindeks.

Dalam instalasi cepat ini, pengaturan ini biasanya cukup untuk memantau hingga 100 titik akhir dan untuk data peringatan yang dapat dikueri/diindeks selama 90 hari. Tabel di bawah ini menunjukkan perangkat keras yang direkomendasikan untuk penerapan cepat:

Agen	CPU	RAM	Penyimpanan (90 hari)
1–25	4 vCPU	8 GiB	50 GB
25–50	8 vCPU	8 GiB	100 GB
50–100	8 vCPU	8 GiB	200 GB

Untuk lingkungan yang lebih besar, lihat panduan Instalasi .

Sistem operasi

Komponen Wazuh Central dapat diinstal pada sistem operasi Linux 64-bit. Versi

sistem operasi yang direkomendasikan:

Amazon Linux 2	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04

Kompatibilitas peramban

Peramban yang didukung:

- Chrome 95 atau lebih baru
- Firefox 93 atau lebih baru
- Safari 13.7 atau lebih baru

Peramban berbasis Chromium lainnya mungkin juga berfungsi. Catatan: Internet Explorer 11 **tidak** didukung.

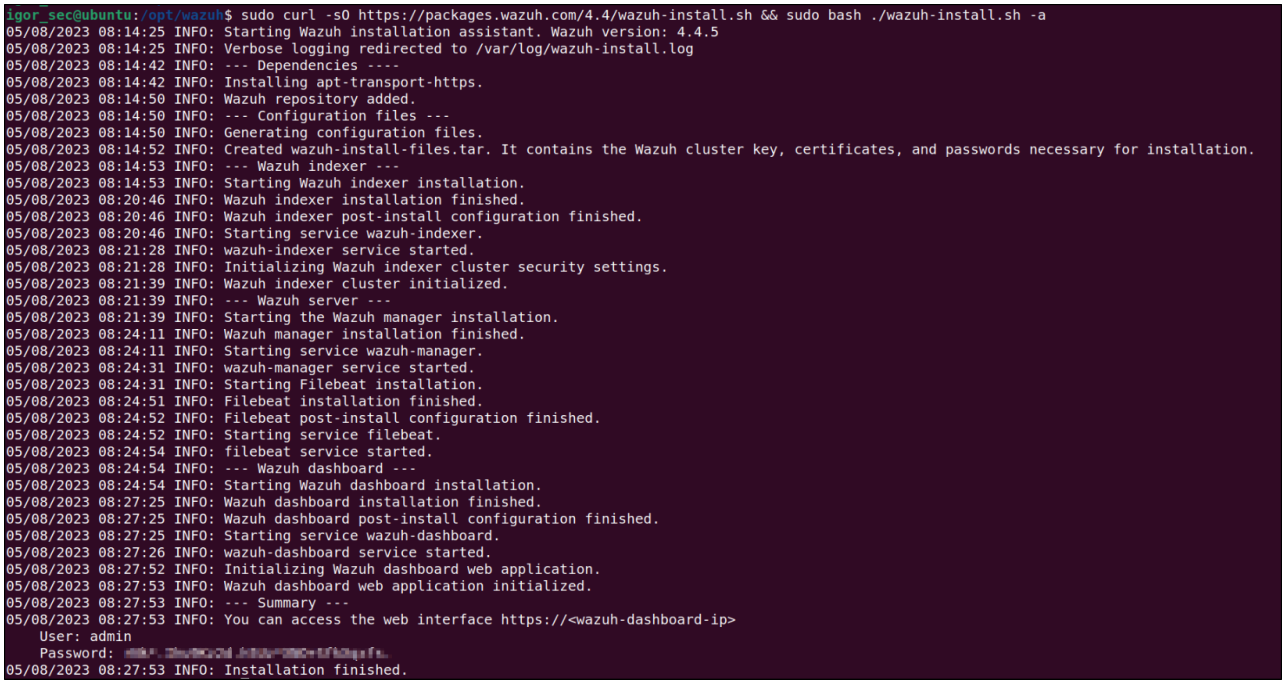
Menginstal Wazuh

Saya menggunakan kembali mesin server Ubuntu saya di lab Snort saya sebelumnya. Saya juga menghapus instalasi Snort di mesin ini karena masalah ketidakcocokan dengan Wazuh. Semua mesin saya dalam proyek ini memiliki antarmuka NAT dan host-only, meskipun saya yakin yang terakhir tidak diperlukan.

Pembuatan dan konfigurasi server Ubuntu awal saya dapat ditemukan di sini .

Untuk memulai, saya mengunduh dan memulai asisten instalasi Wazuh.

```
sudo curl -sO https://packages.wazuh.com/4.4/wazuh-
install.sh && sudo bash ./wazuh-install.sh -a
```



Dari gambar, terlihat bahwa asisten instalasi awalnya menambahkan repositori Wazuh, lalu membuat berkas konfigurasi. Setelah itu, dilanjutkan dengan menginstal komponen inti.

Ini juga menunjukkan di mana mengakses antarmuka web, dan kredensial yang akan digunakan.

Untuk mencetak kredensial semua pengguna pengindeks Wazuh dan API Wazuh, jalankan perintah berikut. Kata sandi terdapat dalam `wazuh-passwords.txt`berkas di dalam `wazuh-install-files.tar`.

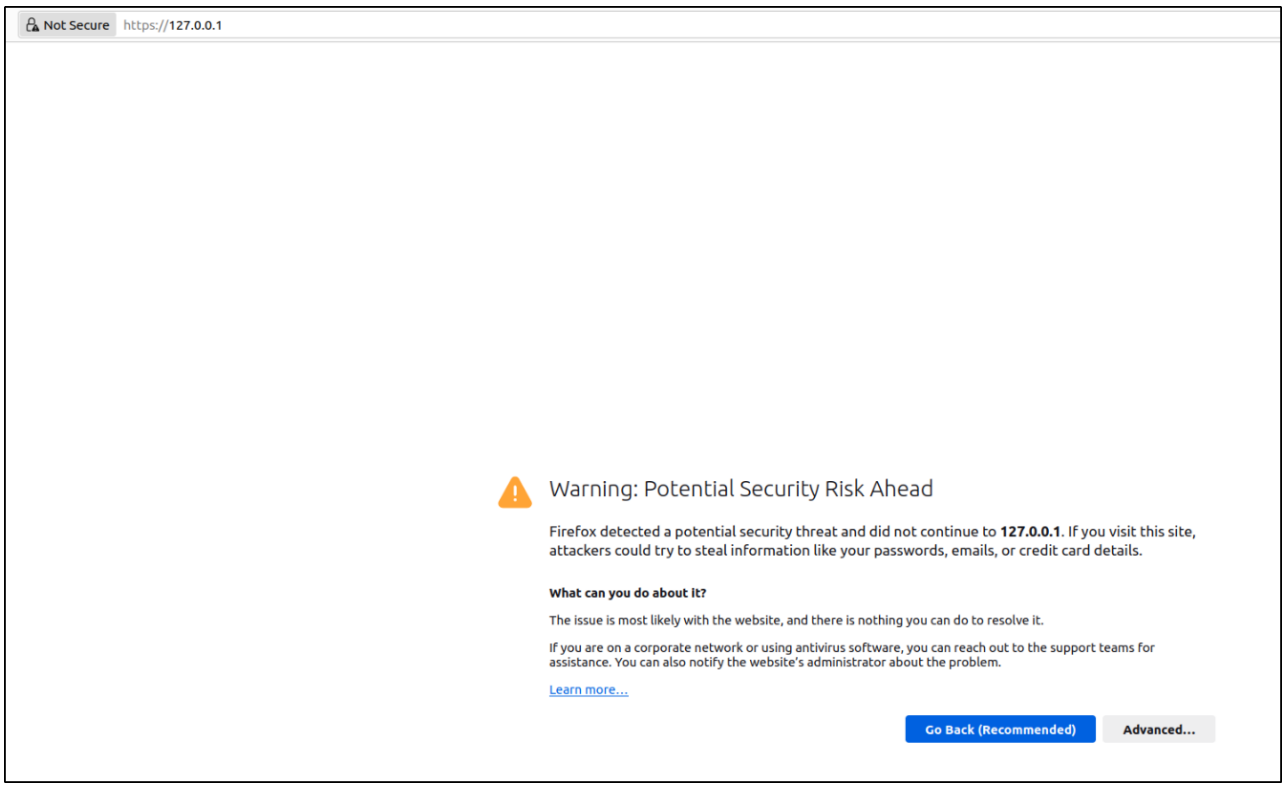
```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

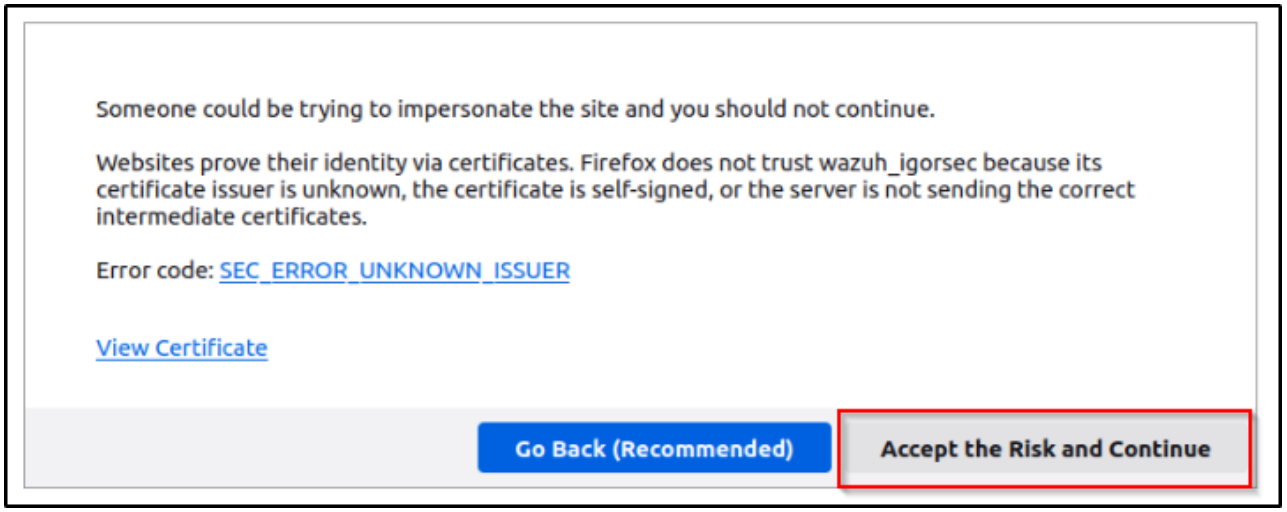
```
igor_sec@ubuntu:/opt/wazuh$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
[sudo] password for igor_sec:
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: '[redacted]'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: '[redacted]'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: '[redacted]'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: '[redacted]'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: '[redacted]'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: '[redacted]'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: '[redacted]'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: '[redacted]'
```

Mencopot komponen pusat Wazuh dapat dilakukan dengan menjalankan asisten instalasi Wazuh menggunakan opsi `-u`atau `—-uninstall`.

Saat pertama kali mengakses antarmuka web, akan muncul pesan peringatan yang menyatakan bahwa sertifikat tidak diterbitkan oleh otoritas tepercaya. Klik "Lanjutan", lalu "Terima Risiko dan Lanjutkan" agar sertifikat yang digunakan oleh Wazuh dikecualikan.

Antarmuka web dapat diakses dengan `https://IP address`. Dalam contoh ini, saya menggunakan host lokal, tetapi juga dapat diakses menggunakan alamat IP NAT atau hanya host.

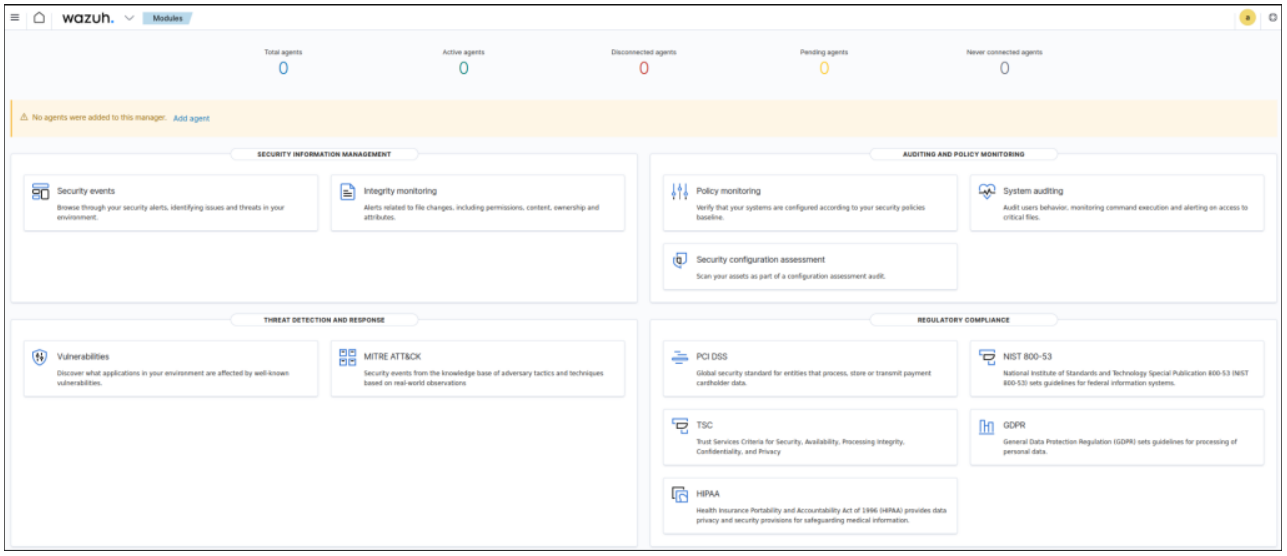




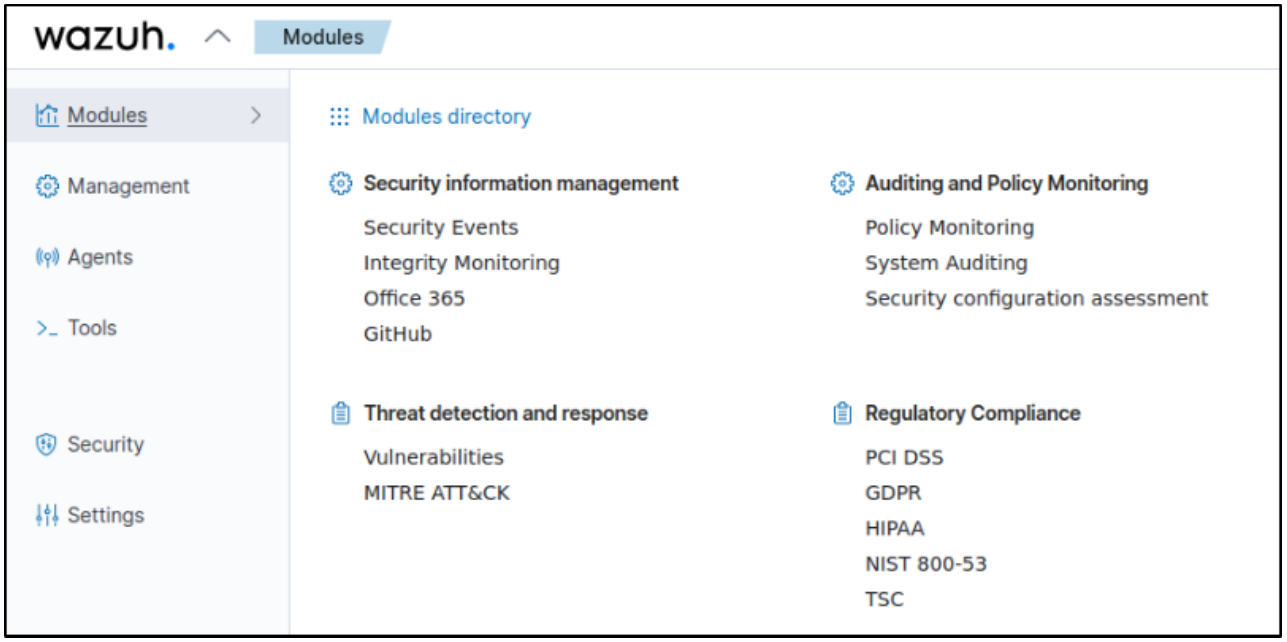
Setelah saya menerima risikonya, saya akan dibawa ke halaman login. Kredensialnya kembali ditemukan di output perintah pertama yang digunakan untuk menginstal Wazuh.

Menjelajahi Dasbor

Terdapat empat modul utama dalam direktori Modul. Modul-modul tersebut adalah Manajemen Informasi Keamanan, Audit dan Pemantauan Kebijakan, Deteksi dan Respons Ancaman, dan Kepatuhan Regulasi.

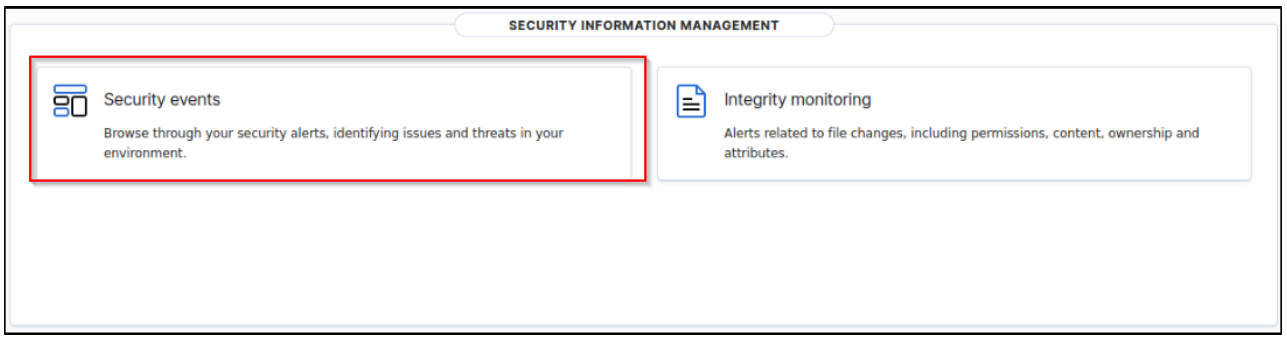


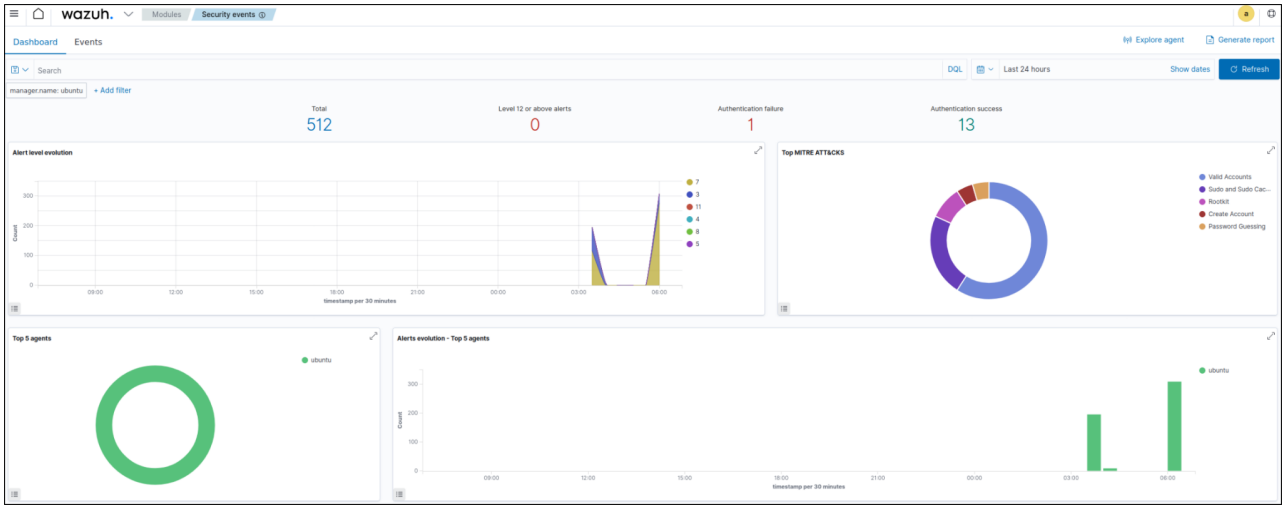
Dalam setiap modul terdapat sub-modul, yang berhubungan dengan beberapa kemampuannya seperti Pemantauan Integritas, Pemantauan Kebijakan, Penilaian Konfigurasi Keamanan, dan Deteksi Kerentanan.



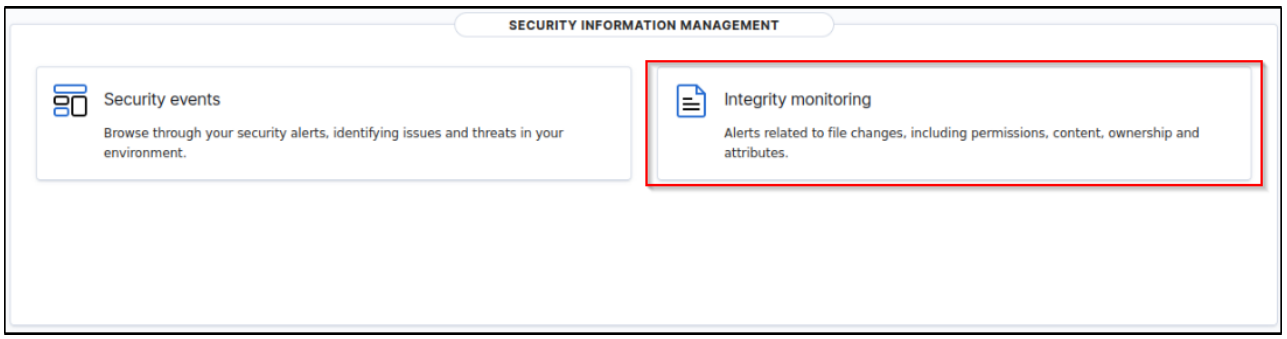
Modul Manajemen Informasi Keamanan berfokus pada pemusatan dan pengelolaan data, peristiwa, dan log terkait keamanan untuk memberikan pandangan komprehensif tentang postur keamanan suatu organisasi.

Submodul Peristiwa keamanan menampilkan ringkasan peristiwa keamanan, menyoroti tingkat keparahan dan statusnya.

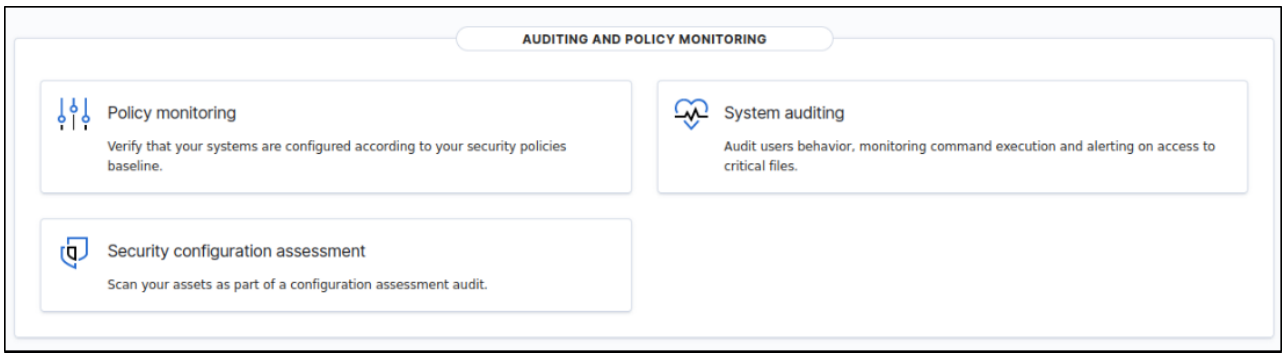


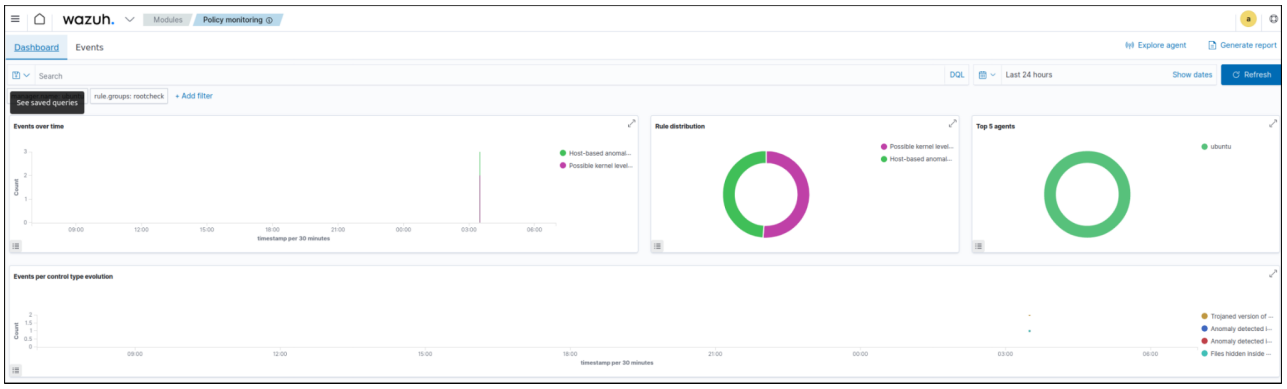


Sub-modul Pemantauan Integritas bertanggung jawab untuk melacak perubahan pada berkas dan konfigurasi sistem guna memastikan integritas dan keamanannya. Ini merupakan alat penting untuk mendeteksi modifikasi yang tidak sah dan potensi pelanggaran keamanan.

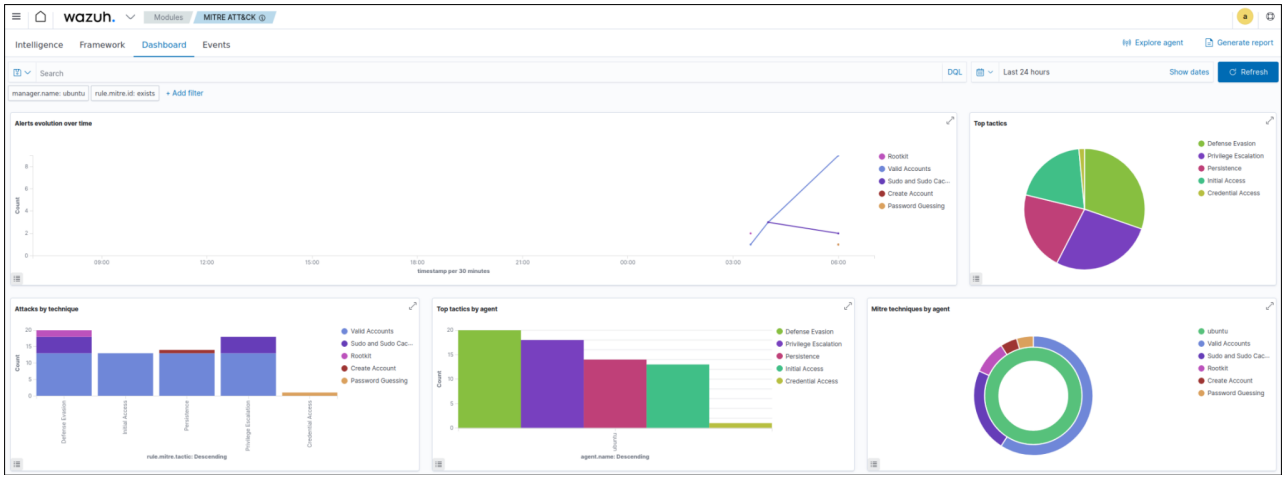


Modul Audit dan Pemantauan Kebijakan berisi sub-modul untuk audit dan pemantauan berkelanjutan terhadap agen untuk kepatuhan terhadap kebijakan, kontrol, proses, dan prosedur guna mendeteksi anomali dan pelanggaran kebijakan.

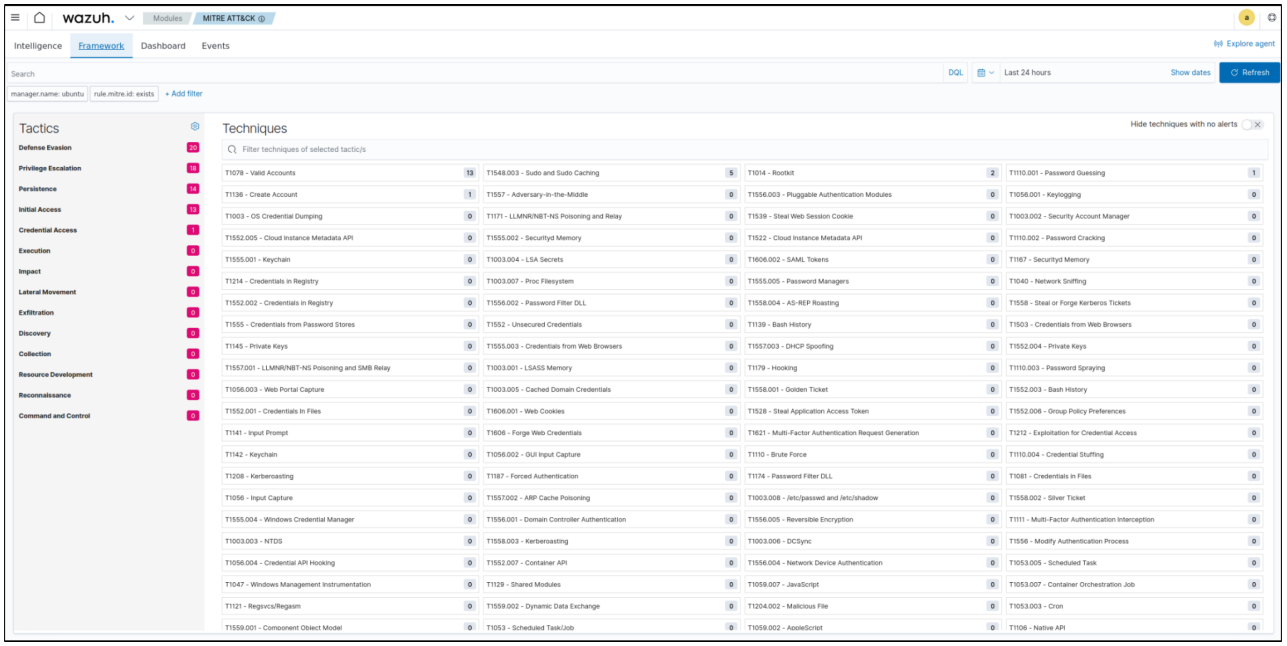




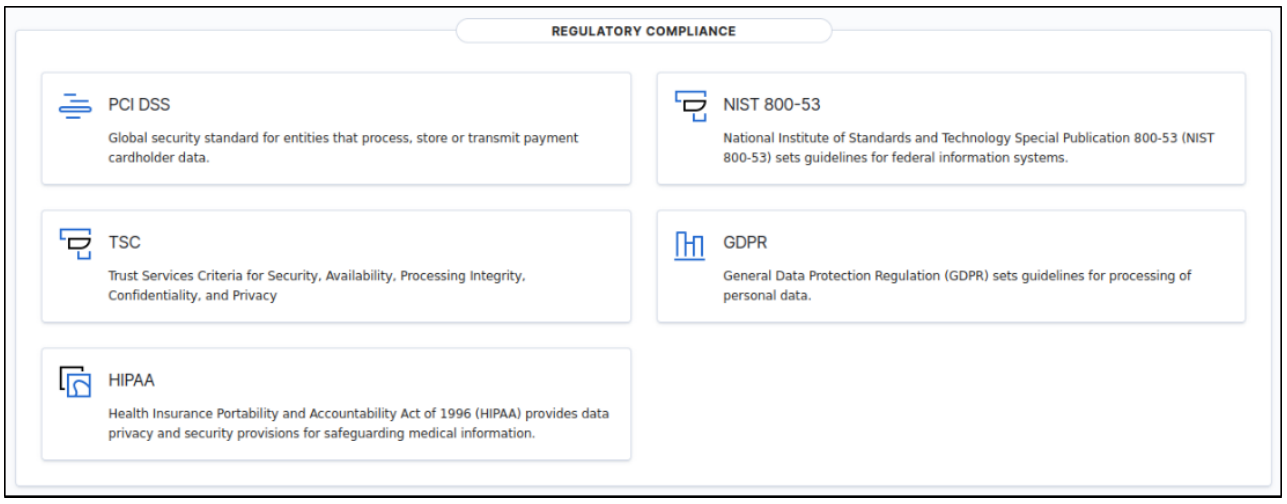
Modul Deteksi dan Respons Ancaman terus memantau lingkungan untuk mencari tanda-tanda kelemahan yang dapat dieksploitasi oleh penyerang. Kerangka kerja MITRE ATT&CK terintegrasi untuk meningkatkan kemampuan Wazuh dalam mendeteksi, menganalisis, dan merespons ancaman dan serangan siber yang canggih. Jika server dikonfigurasi untuk memantau kontainer seperti Docker, yang saat ini belum dikonfigurasi, sub-modul Docker Listener akan muncul di sini.



MITRE ATT&CK menguraikan berbagai taktik, teknik, dan prosedur yang digunakan oleh musuh selama berbagai tahap serangan siber.



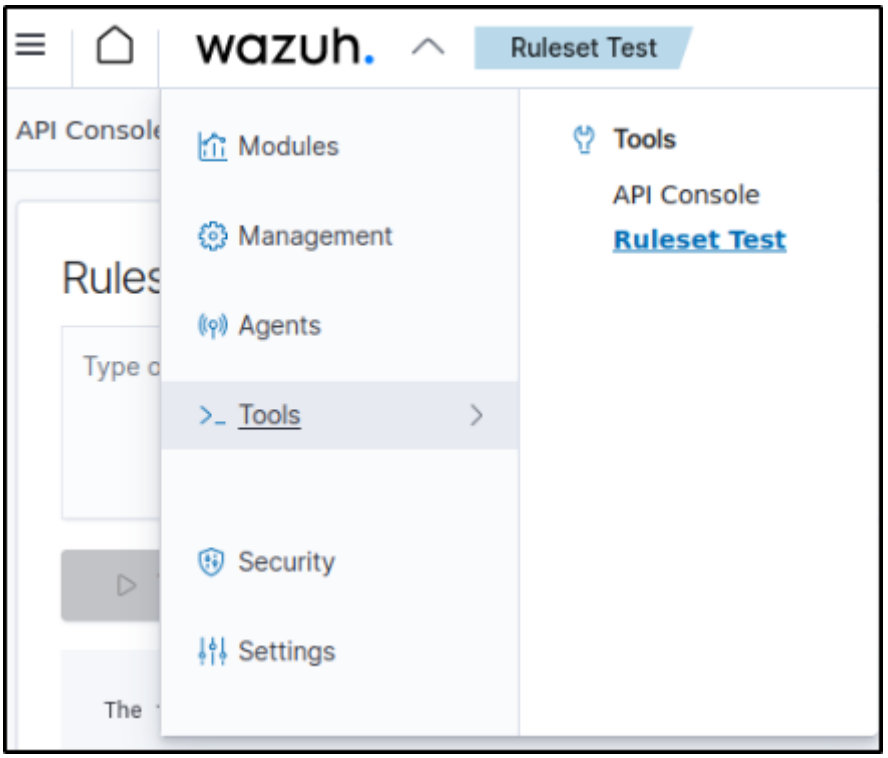
Modul Kepatuhan Regulasi membantu organisasi memenuhi persyaratan kepatuhan dengan menyediakan jejak audit, pelaporan, pemantauan kebijakan sesuai standar seperti PCI DSS, HIPAA, GDPR, dll.



Direktori Manajemen adalah pusat kendali untuk mengelola dan mengoperasikan instalasi Wazuh. Bagian ini didedikasikan untuk mengonfigurasi dan mengelola berbagai komponen platform Wazuh. Direktori ini menyediakan alat dan pengaturan untuk memastikan Wazuh dikonfigurasi, terintegrasi, dan selaras dengan kebutuhan keamanan organisasi.

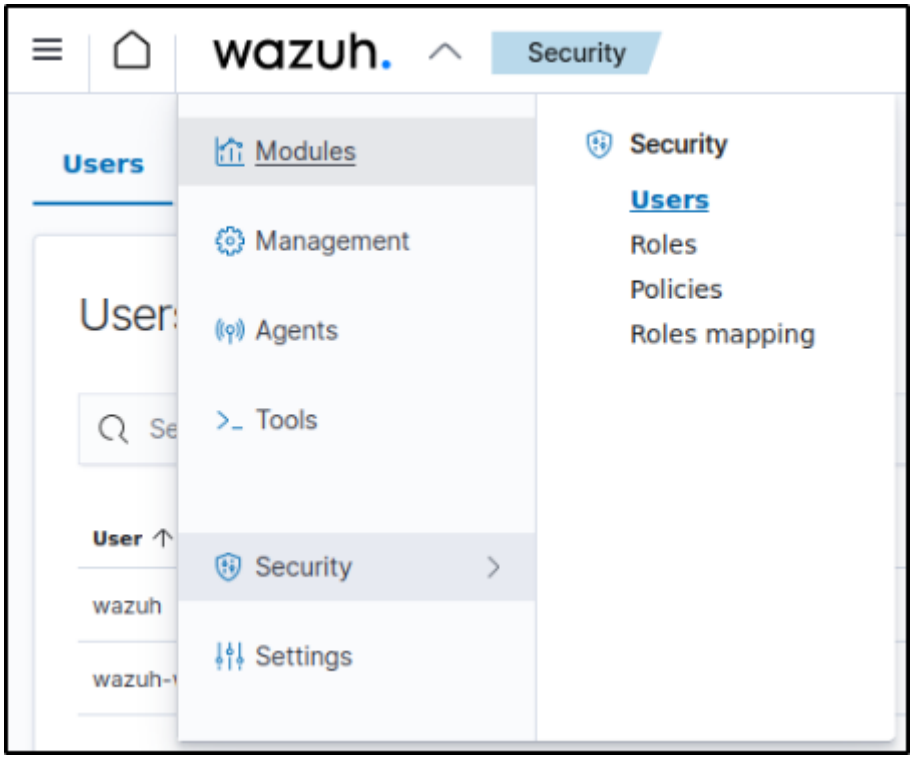
Direktori Agen adalah tempat sumber daya yang dibutuhkan untuk penyebaran, konfigurasi, dan pengelolaan agen Wazuh di seluruh infrastruktur berada. Direktori ini juga digunakan untuk memantau peristiwa dan perilaku titik akhir untuk analisis, deteksi, dan respons.

Direktori alat memiliki dua komponen: konsol API dan Uji Aturan. Konsol API memungkinkan interaksi dengan pengelola Wazuh dari API peramban web untuk mengelola dan memantau instalasi secara terprogram. Konsol menyediakan antarmuka baris perintah untuk melakukan panggilan API tanpa menulis kode. Uji Aturan memungkinkan pengujian aturan Wazuh sebelum menerapkannya ke dalam produksi.

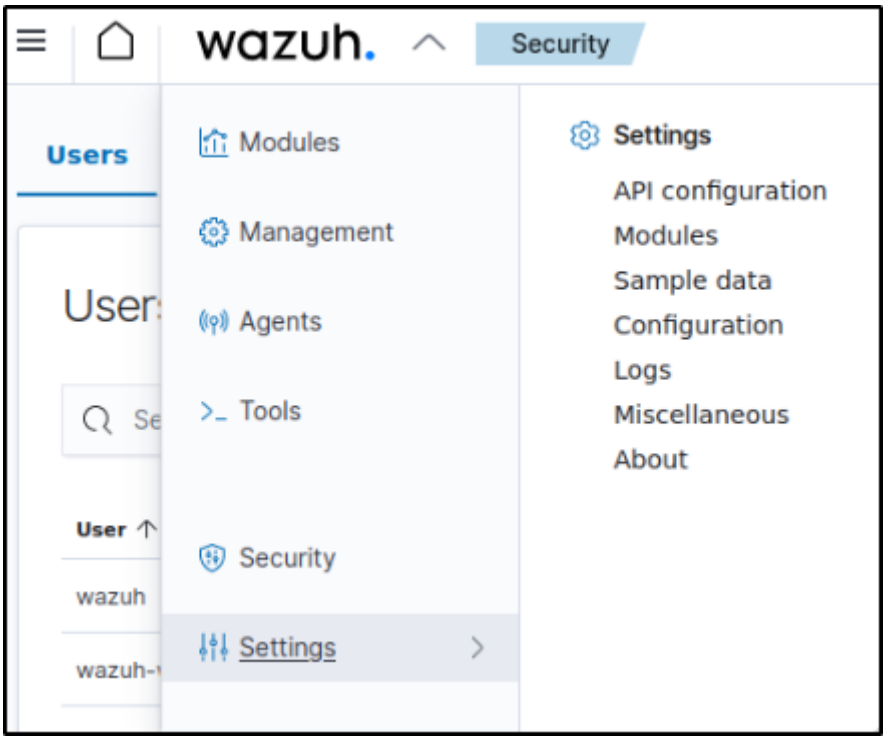


Komponen keamanan ini memungkinkan administrator Wazuh untuk mengatur kontrol akses berbasis peran (RBAC) dengan membuat akun pengguna, menetapkan peran kepada mereka, dan menyusun kebijakan otorisasi yang disesuaikan dengan fungsi masing-masing peran. Hal ini menyediakan manajemen pengguna, kontrol akses, dan pemisahan tugas di

dalam Wazuh.



Folder Pengaturan berisi konfigurasi, log, dan data untuk proses, modul, dan layanan backend inti yang membentuk instalasi Wazuh. Folder ini menyediakan kontrol terpusat atas komponen-komponen di tingkat sistem.

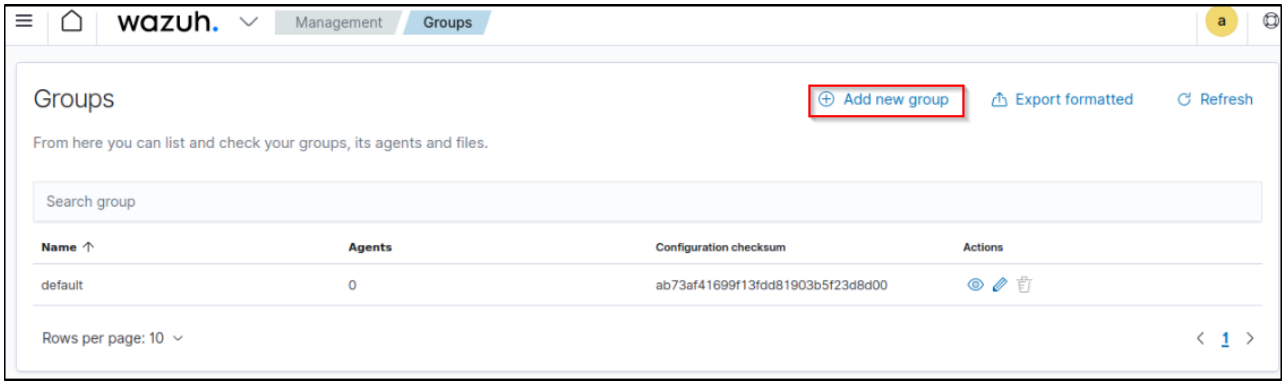


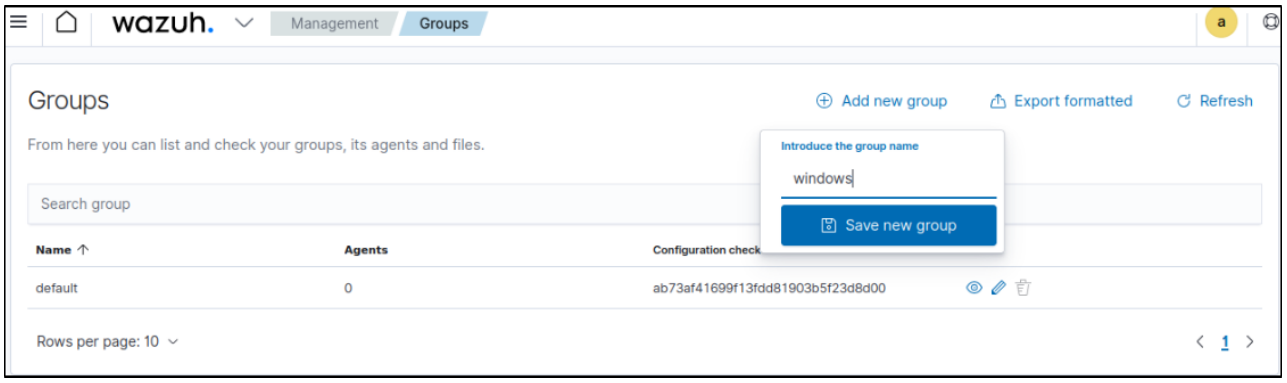
Mengonfigurasi Server Wazuh

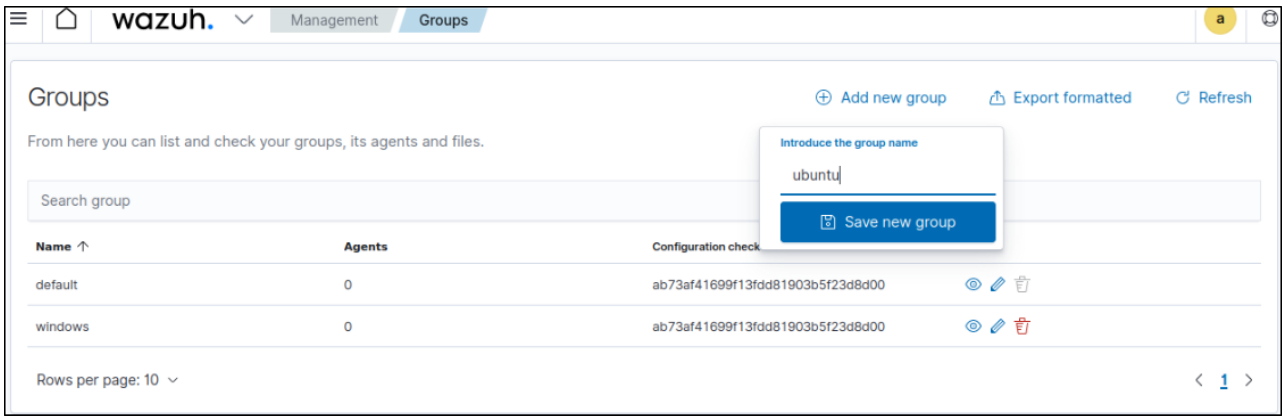
Sebagian besar pengaturan konfigurasi server Wazuh saya didasarkan pada video youtube HackerSploit tentang Menginstal & Mengonfigurasi Wazuh.

Saya membuat dua grup di server saya, satu grup Windows dan satu grup Ubuntu. Pengelompokan agen dengan cara ini memungkinkan saya untuk menyesuaikan pemantauan dan kebijakan khusus untuk titik akhir Windows atau Linux di masa mendatang.

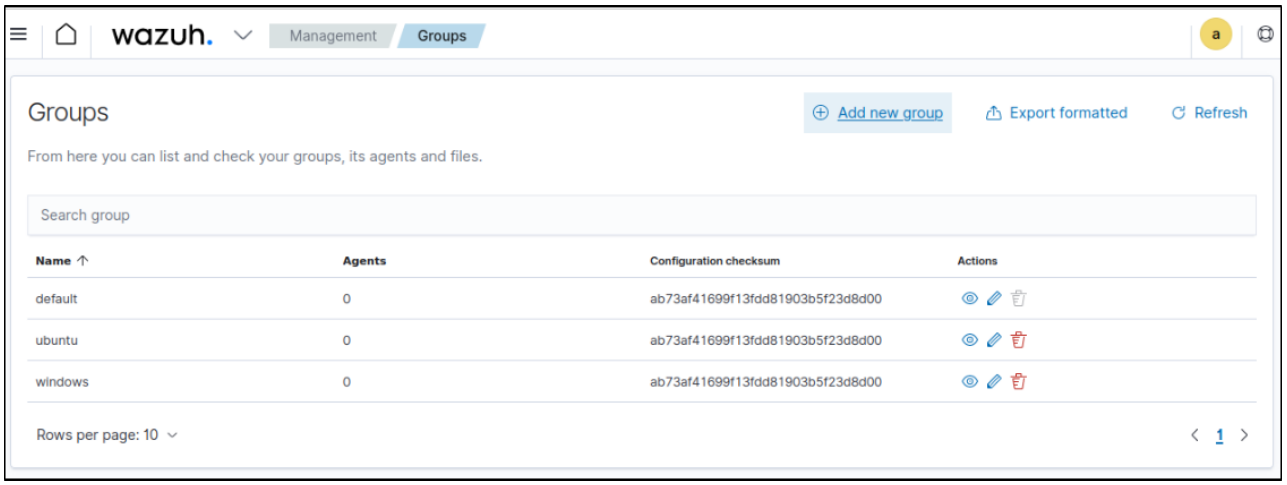
Buka direktori Manajemen dan pilih Grup. Klik "Tambahkan grup baru", lalu ketik nama grup, lalu simpan.







Dua grup baru sekarang ditambahkan selain grup default.

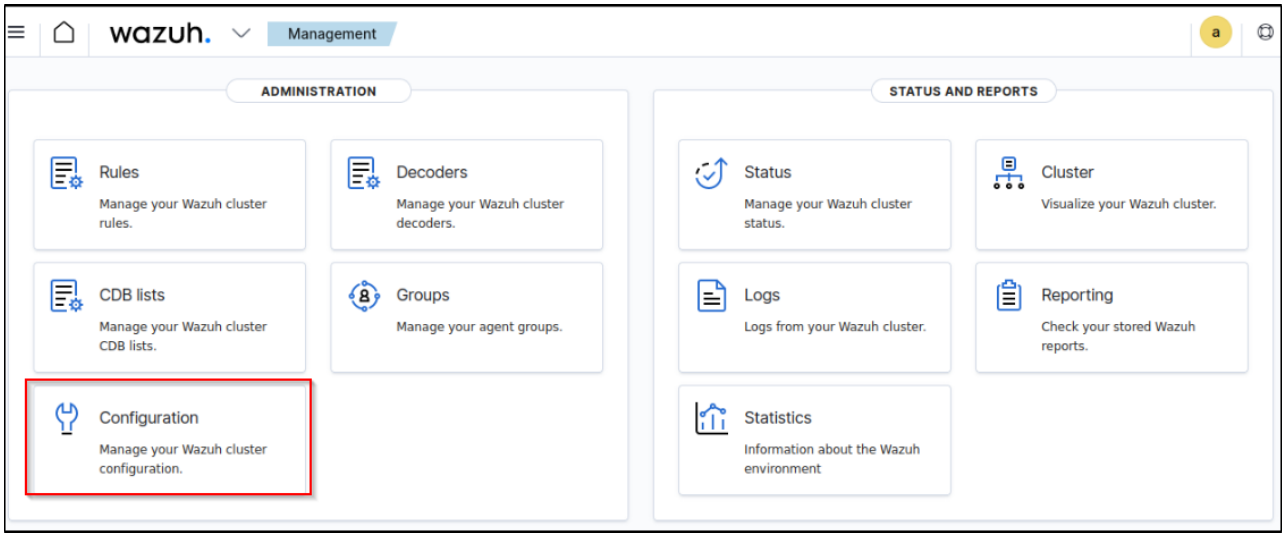


There are six configuration settings that can be configured in this folder, they are main configurations, alerts and output management, auditing and policy monitoring, system threats and incident response, log data analysis, and cloud security monitoring. The following are some settings that can be configured here:

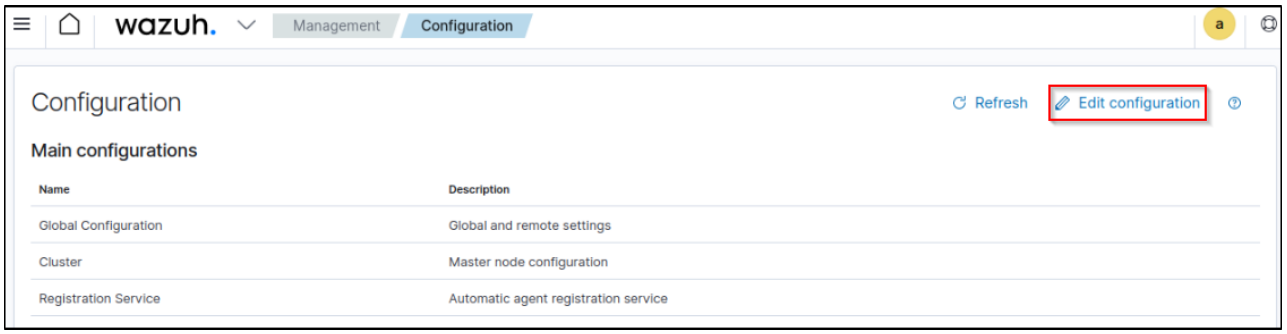
- email notifications,
- log retention policies,
- external integrations,
- API configuration,
- remote command execution,
- cluster settings if applicable,
- agent registration, communication, and synchronization with the

manager

- rules and decoders used by Wazuh for parsing logs and detecting security events.



Click `Edit configuration` to start editing the configuration settings.



Moving forward, the following are the configurations in my Wazuh server.

- I enabled **Wazuh archives**. Wazuh archives are the files that the Wazuh server creates to store logs, alerts, and other security data from monitored devices. They store **everything** that the Wazuh server receives, whether it's a security event that triggers a rule or not.

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

- This setting is for configuring **email notifications**. Wazuh can be configured to send emails of particular logs.

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

- **Policy monitoring** is enabled. I turned on policy monitoring to continuously audit agents against security configuration benchmarks. This lets me identify and fix policy violations.

```
<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>
```

- **Osquery** is enabled. I enabled Osquery that once configured, will use SQL-based queries in exploring the operating system data of the

endpoints.

```
<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>no</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>
```

- **System inventory** is enabled. This will run periodic scans on my endpoints to collect details like installed software, running processes, open network ports, connected hardware, and operating system version.Maintaining an up-to-date inventory provides greater visibility into my environment and is useful for things like vulnerability management. The inventory data will be stored locally on agents and can also be queried centrally via the Wazuh API or dashboard.

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>
```

- **Vulnerability-detector** is enabled. With vulnerability detection enabled, Wazuh will scan my Ubuntu server and agents to detect any vulnerable software packages installed. This prevents overlooked vulnerabilities from turning into exploit targets down the road.

```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>
```

- Enabled **Ubuntu and Debian OS vulnerabilities**. I configured Wazuh to

check multiple sources like Debian, Ubuntu, and Windows advisories for known vulnerabilities. This supplements the vulnerability data from the National Vulnerability Database to provide broader coverage.

```
<!-- Ubuntu OS vulnerabilities -->
<provider name="canonical">
  <enabled>yes</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Debian OS vulnerabilities -->
<provider name="debian">
  <enabled>yes</enabled>
  <os>buster</os>
  <os>bullseye</os>
  <update_interval>1h</update_interval>
</provider>
```

- **Windows OS vulnerabilities** is enabled by default.

```
  <!-- Windows OS vulnerabilities -->
  <provider name="msu">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
  </provider>
```

- We can also add more sources for vulnerability detection.

- **Pemantauan integritas berkas** diaktifkan. Saya mengaktifkan FIM untuk memantau jalur kritis, berkas, dan direktori. FIM akan memberi tahu saya jika ada perubahan tidak sah pada biner sistem, berkas aplikasi, atau berkas log sehingga saya dapat segera menyelidikinya atau meresponsnya tepat waktu.

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
```

- **Konfigurasi respons aktif** . Gambar di bawah ini berisi perintah yang

akan dijalankan Wazuh saat dipicu. Kini, ketika peringatan tingkat keparahan tinggi dipicu dan mengindikasikan ancaman nyata, Wazuh dapat mengambil tindakan seperti memblokir alamat IP atau menghentikan proses secara otomatis. Hal ini mempercepat respons insiden.

```
<!-- Active response -->
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>127.0.0.53</white_list>
</global>

<command>
  <name>disable-account</name>
  <executable>disable-account</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>restart-wazuh</name>
  <executable>restart-wazuh</executable>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>host-deny</name>
  <executable>host-deny</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>route-null</name>
  <executable>route-null</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>win_route-null</name>
  <executable>route-null.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>netsh</name>
  <executable>netsh.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

- **Inventaris Sistem** diaktifkan. Saya mengaktifkan modul Inventaris Sistem di Wazuh untuk mendapatkan visibilitas yang lebih baik ke titik akhir di lingkungan saya. Modul ini akan menjalankan pemindaian

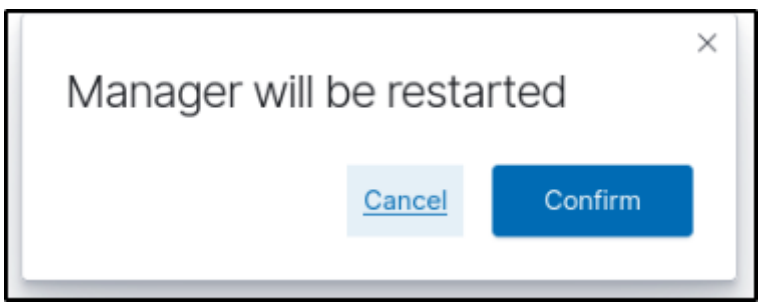
secara berkala untuk mengumpulkan detail seperti perangkat lunak yang terinstal, proses yang berjalan, port jaringan yang terbuka, perangkat keras yang terhubung, dan versi sistem operasi.

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>
```

- Pengaturan ini mengedit konfigurasi **klaster** . Saya membiarkannya apa adanya karena lingkungan saya kecil dan tidak perlu diubah.

```
<cluster>
  <name>wazuh</name>
  <node_name>node01</node_name>
  <node_type>master</node_type>
  <key></key>
  <port>1516</port>
  <bind_addr>0.0.0.0</bind_addr>
  <nodes>
    <node>NODE_IP</node>
  </nodes>
  <hidden>no</hidden>
  <disabled>yes</disabled>
</cluster>
```

Agar perubahan diterapkan, simpan dan mulai ulang pengelola. Proses ini mungkin memakan waktu sekitar satu menit.



Server Wazuh sekarang telah dikonfigurasi, meskipun saya akan kembali mengedit konfigurasinya sesuai kebutuhan di tutorial nanti. Yang masih kurang hanyalah agen-agennya agar eksplorasi kapabilitas Wazuh dapat dimulai.

Kesimpulan

Di bagian kedua seri Wazuh ini, saya menginstal Wazuh dan menjalankan komponen-komponen inti di server Ubuntu. Saya menjelajahi antarmuka dasbor untuk memahami cara menavigasi dan memantau sistem. Saya juga mengonfigurasi beberapa fitur utama Wazuh seperti pemantauan integritas berkas, respons aktif, dan pemindaian kerentanan untuk meningkatkan keamanan dan deteksi.

Setelah fondasinya terpasang, saya siap untuk menerapkan agen dan melihat kemampuan ini beraksi. Wazuh kini telah siap dan siap untuk mulai memproses dan menganalisis data dari titik akhir.

Pada bagian 3, saya akan membuat VM Windows dan mendalami penerapan dan pengelolaan agen di perangkat Ubuntu dan Windows; siap untuk mengeksplorasi kemampuan Wazuh.

Terima kasih sudah membaca!

Sampai jumpa di bagian berikutnya.

Referensi