BADAN PANGAN NASIONAL

PANDUAN PENGGUNA

RESPIN

SISTEM OTOMASI RESPON INSIDEN

BADAN PANGAN CSIRT

2025

Pendahuluan

Dokumen ini disusun sebagai panduan pengguna untuk mengoperasikan **Sistem Otomasi Respon Insiden**, sebuah sistem terintegrasi yang dirancang untuk mempercepat dan mempermudah proses penanganan insiden keamanan siber. Sistem ini menggabungkan berbagai komponen utama, yaitu **Wazuh** sebagai sistem deteksi dan pemantauan, **Shuffle** sebagai platform orkestrasi otomatis, **DFIR IRIS** untuk manajemen investigasi insiden, serta **MISP** untuk berbagi informasi ancaman (*threat intelligence*). Selain itu, sistem ini juga terhubung dengan tools eksternal seperti **VirusTotal** untuk analisis IoC dan **Telegram** sebagai sarana notifikasi real-time.

Pengembangan sistem ini mengacu pada kerangka kerja **ISO/IEC 27035** yang mengatur tata kelola manajemen insiden keamanan informasi secara sistematis, mulai dari deteksi, analisis, respons, hingga pemulihan. Dengan pendekatan otomatisasi dan integrasi, sistem ini bertujuan untuk mengurangi waktu tanggap insiden, meningkatkan akurasi pengambilan keputusan, serta mendukung dokumentasi dan pelaporan insiden secara efektif.

Panduan ini memberikan petunjuk teknis bagi pengguna dalam menjalankan fungsi-fungsi utama sistem, mulai dari pemantauan insiden hingga eksekusi respon otomatis, serta pengelolaan artefak dan pelaporan hasil investigasi. Panduan ini ditujukan bagi administrator, analis keamanan, dan anggota CSIRT yang terlibat langsung dalam operasional sistem.

Daftar Isi

Instalasi

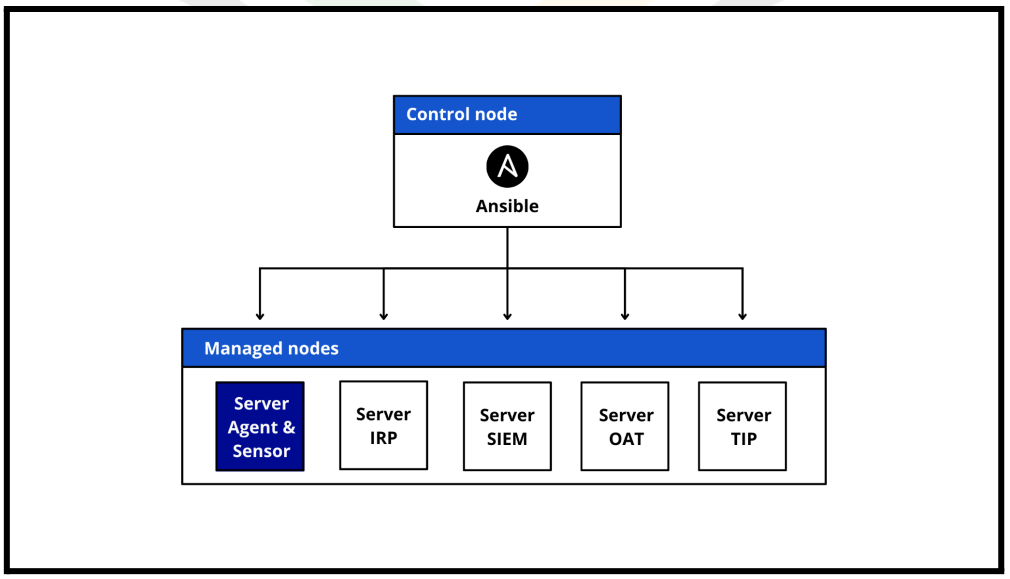
Instalasi sistem dilakukan dengan pendekatan *Infrastructure as Code* menggunakan **Ansible**. Ansible memungkinkan pengguna untuk mendefinisikan infrastruktur dan proses deployment dalam bentuk file YAML yang disebut **playbook**, sehingga proses dapat dijalankan berulang dengan konsisten. Ansible bekerja tanpa agen (*agentless*) dan memanfaatkan koneksi SSH, sehingga mudah diintegrasikan ke dalam berbagai lingkungan sistem.

Environment

Sistem terdiri dari beberapa komponen, diantaranya ***Security Information and Event Management*** (SIEM), **Orchestration and Automation Tools** (OAT), **Incident Response Platform** (IRP), **Threat Intelligence Platform** (TIP), **IoC Analyzer**, dan **Notification Tools**.

Skema Ansible

Seluruh komponen tersebut terintegrasi untuk menjalankan fungsi-fungsi tertentu dalam tahapan penanganan insiden seperti Deteksi, Notifikasi, Triase, Analisis, Respon, dan Pelaporan. Representasi *Infrastructure-as-Code* yang akan digunakan dalam implementasi RESPIN dapat dilihat pada gambar berikut.



Sebuah komputer akan bertindak sebagai **Control Node** yang menjalankan playbook untuk melakukan instalasi dan konfigurasi ke seluruh server komponen RESPIN dan server *victim.*

Spesifikasi Perangkat

Spesifikasi perangkat yang disarankan adalah sebagai berikut.

Nama VM	RAM	Storage	Processor	OS
Control Node	4 GB	50 GB	2	Ubuntu Desktop 22.04
SIEM	8 GB	250 GB	4	Ubuntu 22.04
OAT	4 GB	50 GB	2	Ubuntu 22.04
CTI	4 GB	50 GB	2	Ubuntu 22.04
IRP	4 GB	50 GB	2	Ubuntu 22.04
Victim	4 GB	50 GB	2	Ubuntu 22.04

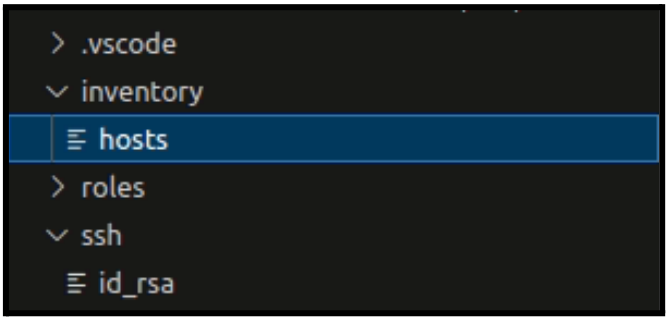
Repository

Script dan *Playbook* yang digunakan dalam instalasi dapat diunduh pada repositori Github berikut.

https://github.com/risetzaki/respin.git

```
$ git clone https://github.com/risetzaki/respin.git
$ cd 'respin/Ansible Playbook'
```

Setelah diunduh, sesuaikan file **/inventory/hosts** berdasarkan informasi server yang digunakan. Apabila menerapkan mekanisme koneksi SSH dengan public dan private key, maka simpan file private key di direktori **/ssh**.



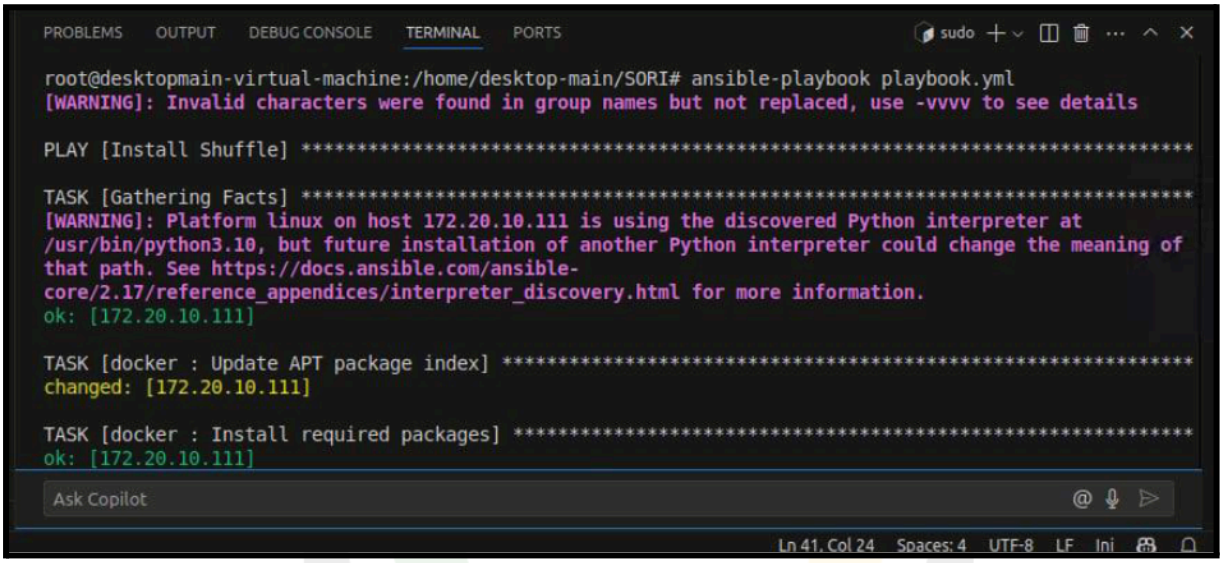
Ansible Automation

Setelah dilakukan penyesuaian, jalankan Ansible *playbook* untuk memulai proses instalasi secara otomatis.

Run Script

Pastikan komputer *control node* sudah menginstall Ansible dan berada di direktori yang benar sebelum menjalankan *playbook*.

```
$ ansible-playbook playbook.yml
```



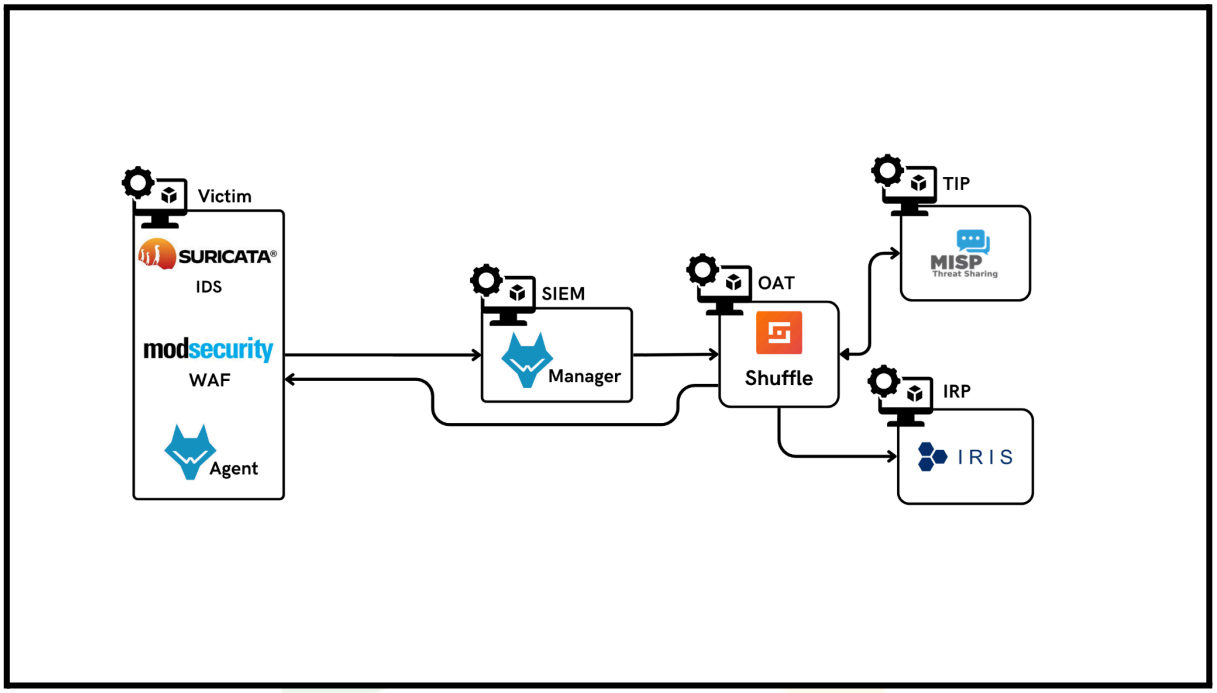
Play Recap

Hasil akhir dari *playbook* ditampilkan dalam Play Recap. Proses instalasi berhasil selama tidak menampilkan status **failed**.

```
PLAY RECAP *********************************************************************************************
172.20.10.105              : ok=19   changed=5    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
172.20.10.109              : ok=21   changed=6    unreachable=0    failed=0    skipped=1    rescued=0
  ignored=0
172.20.10.110              : ok=9    changed=1    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
172.20.10.111              : ok=18   changed=2    unreachable=0    failed=0    skipped=3    rescued=0
  ignored=0
172.20.10.114              : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0
```

Visualisasi Sistem

Berikut adalah visualisasi relasi dan integrasi antar komponen RESPIN.



Akses Komponen Sistem

Wazuh

- URL: https://172.20.10.105/
  *Akses melalui jaringan lokal Badan Pangan CSIRT
- Username: **admin**
- Password: **CGT5GaHf.oLqJ41oYlw.lse?SzC3?7KG**
  *ubah password secara berkala!

Shuffle

- URL: https://172.20.10.111:3443/
  *Akses melalui jaringan lokal Badan Pangan CSIRT
- Username: **nfa-soc**
- Password: **Shufflepass234**
  *ubah password secara berkala!

DFIR IRIS

- URL: https://172.20.10.109/

*Akses melalui jaringan lokal Badan Pangan CSIRT

- Username: **administrator**
- Password: **CreateYourOwnPassword**

  *ubah password secara berkala!

MISP

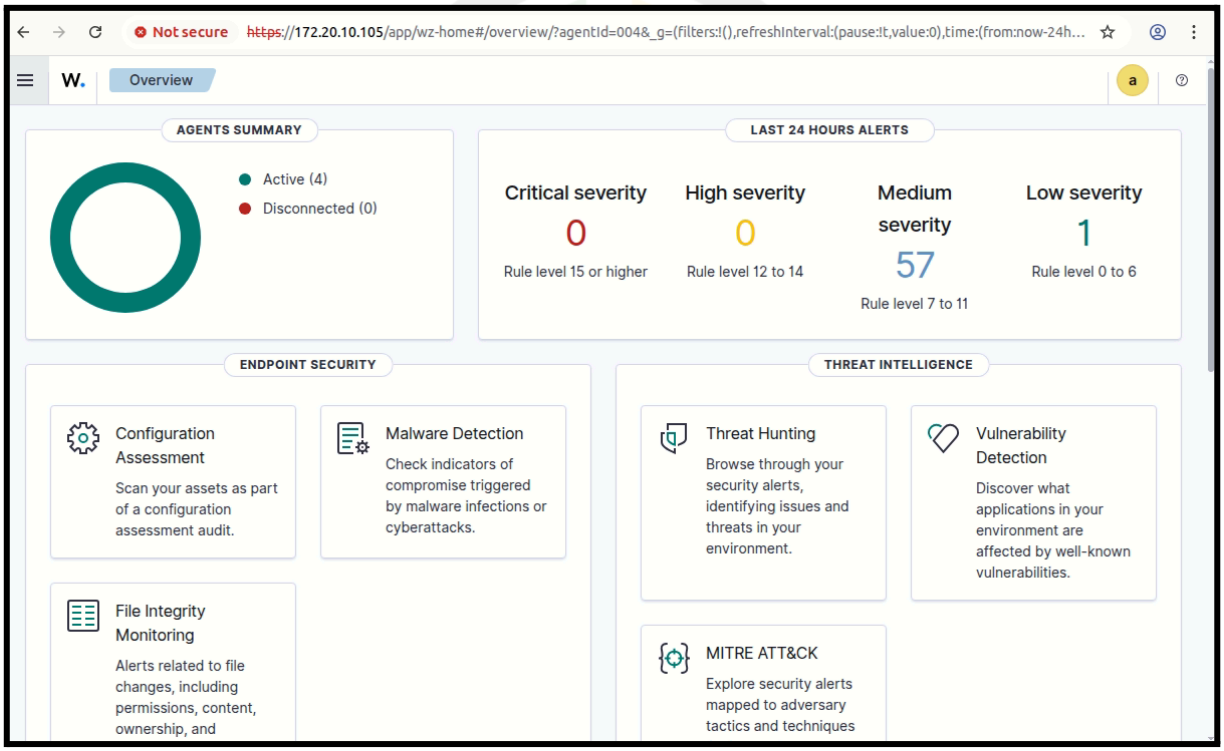
- URL: https://172.20.10.110/users/login

  *Akses melalui jaringan lokal Badan Pangan CSIRT
- Username: **admin@admin.test**
- Password: **adminmisp123!!@!**

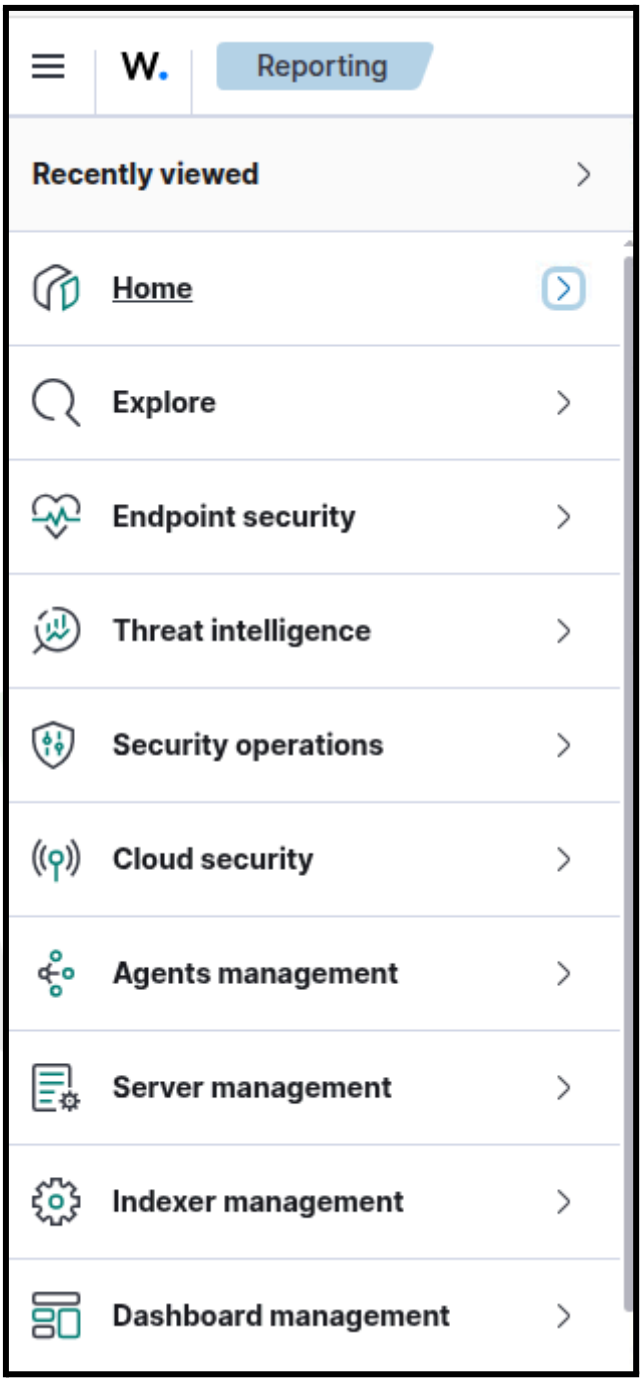
  *ubah password secara berkala!

Wazuh

Wazuh adalah platform keamanan open-source yang berfungsi sebagai sistem deteksi intrusi host-based (HIDS), pengelola informasi dan kejadian keamanan (SIEM), serta alat pemantauan kepatuhan dan integritas file. Wazuh mengumpulkan data dari endpoint dan perangkat jaringan, lalu menganalisisnya untuk mendeteksi aktivitas mencurigakan, celah keamanan, dan pelanggaran kebijakan. Dengan integrasi ke Elastic Stack, Wazuh menyediakan visualisasi log, alerting real-time, serta fitur-fitur seperti konfigurasi assessment, malware detection, dan threat intelligence, sehingga memberikan visibilitas dan kontrol penuh atas postur keamanan sistem TI.



Fitur



Explore

Bagian Explore pada Wazuh berfungsi untuk menganalisis dan memvisualisasikan data keamanan yang dikumpulkan dari berbagai sumber. Secara keseluruhan, Explore membantu pemantauan dan respons keamanan yang lebih cepat dan efisien. Terdapat fitur-fitur di dalamnya, yaitu:

- **Discover:** pengguna dapat menelusuri log secara real-time untuk investigasi insiden
- **Dashboards:** menyajikan data dalam bentuk grafik interaktif
- **Visualize:** menyajikan data dalam bentuk grafik interaktif
- **Reporting:** pembuatan laporan otomatis
- **Alerting:** mendeteksi serta mengirimkan peringatan saat terjadi aktivitas mencurigakan
- **Maps:** menampilkan aktivitas berdasarkan lokasi geografis
- **Notifications:** mendeteksi serta mengirimkan peringatan saat terjadi aktivitas mencurigakan

Endpoint Security

Dashboard ini berfokus pada perlindungan dan pemantauan endpoint, seperti server, workstation, dan perangkat lainnya dalam jaringan. Selain itu dashboard ini juga berperan dalam pengumpulan, analisis, dan penyimpanan data keamanan dari berbagai sumber seperti perangkat jaringan, host dan IDS. Tujuannya adalah untuk memberikan gambaran menyeluruh tentang postur keamanan jaringan, mendeteksi anomali, dan memfasilitasi investigasi insiden. Terdapat fitur-fitur di dalamnya, yaitu:

- **Configuration Assessment**: Memeriksa konfigurasi sistem untuk memastikan kepatuhan terhadap standar keamanan.
- **Malware Detection:** Mendeteksi keberadaan malware pada sistem melalui analisis aktivitas dan file mencurigakan.
- **File Integrity Monitoring:** Memantau perubahan file penting untuk mendeteksi potensi manipulasi atau akses tidak sah.

Threat Intelligence

Dashboard ini berfungsi untuk menampilkan hasil deteksi ancaman sehingga dapat membantu dalam memahami pola serangan, teknik, taktik, dan prosedur (TTP) dari pelaku ancaman. Fungsi ini mencakup analisis data secara real-time untuk mendeteksi pola yang tidak biasa yang dapat mengindikasikan insiden keamanan, dan menyediakan alat untuk respons cepat untuk mengurangi dan menyelesaikan ancaman secepat mungkin. Fitur dalam Threat Intelligence

mencakup Threat Hunting, Vulnerability Detection, MITRE ATT&CK framework, dan integrasi dengan layanan analisis file seperti VirusTotal.

- **Threat Hunting:** Analisis proaktif terhadap log dan aktivitas sistem untuk mendeteksi ancaman tersembunyi.
- **Vulnerability Detection:** Mengidentifikasi celah keamanan dalam sistem berdasarkan data kerentanan terbaru.
- **MITRE ATT&ACK:** Memetakan teknik dan taktik serangan yang terdeteksi, sesuai dengan kerangka kerja berbasis perilaku adversary.

Security Operations

Bagian dashboard ini membantu memastikan bahwa sistem telah mematuhi persyaratan hukum dan peraturan yang relevan. Hal ini mencakup pemantauan kepatuhan terhadap standar seperti GDPR, HIPAA, PCI-DSS, dll., serta menyediakan laporan dan dokumentasi yang diperlukan untuk audit kepatuhan.

Cloud Security

Dashboard ini berfungsi untuk melindungi aset dan data yang disimpan dalam lingkungan cloud dengan pemantauan dan pengawasan terhadap berbagai layanan cloud. Layanan cloud diantaranya adalah:

- Docker
- Amazon Web Services (AWS)
- Google Cloud
- Github
- Office 365

Agent Management

Dashboard ini pada Wazuh adalah fitur yang digunakan untuk mengelola agen-agen yang terpasang di endpoint seperti server, workstation, dan perangkat lainnya dalam jaringan. Melalui fitur ini, pengguna dapat melakukan instalasi, registrasi, konfigurasi, serta memantau status dan aktivitas masing-masing agen secara terpusat. Agent Management juga memungkinkan pengelompokan agen berdasarkan peran atau lokasi, memudahkan dalam penerapan kebijakan keamanan yang konsisten. Selain itu, fitur ini menyediakan informasi detail seperti

sistem operasi, alamat IP, versi agen, serta status konektivitas, sehingga tim keamanan dapat memastikan semua endpoint terpantau dan dilindungi secara optimal.

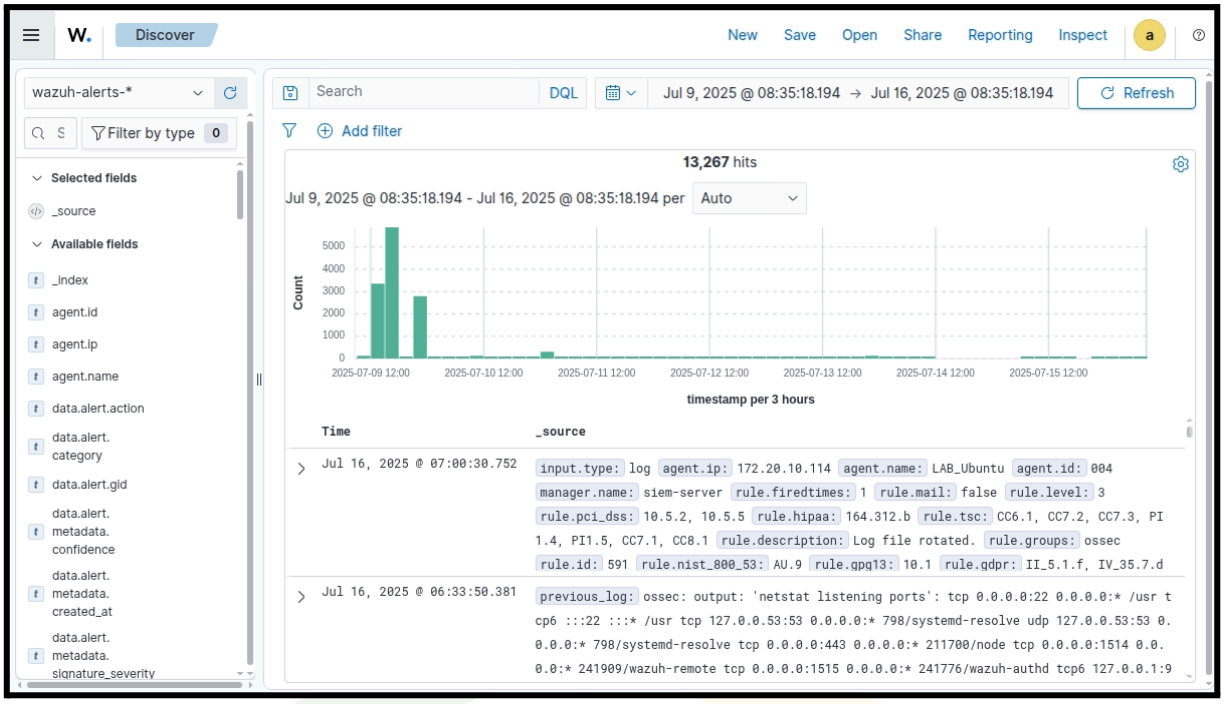
Fungsi

[Explore] Security Event / Discovery

Fitur ini memungkinkan Wazuh untuk mengumpulkan dan menganalisis log keamanan dari berbagai sumber, seperti sistem operasi, firewall, dan aplikasi. Dengan ini, pengguna dapat mendeteksi aktivitas mencurigakan, anomali, dan percobaan serangan secara real-time.

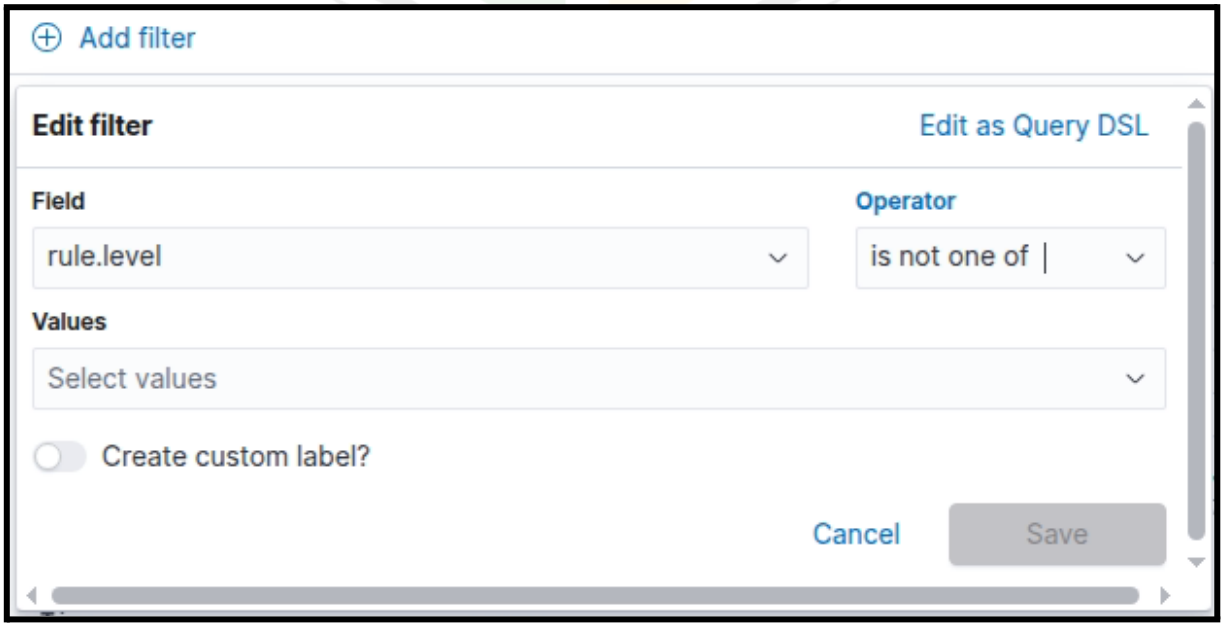
Filtering Security Event

Dalam fitur Security Event / Discovery, fungsi ini berfungsi untuk mempermudah analis dalam membaca informasi dan event keamanan. Pada panel sebelah kiri, analis dapat memilih kolom apa saja yang ingin ditampilkan di daftar event, sepeti **agent.name, rule.id, rule.description, full.log, timestamps, dll.**

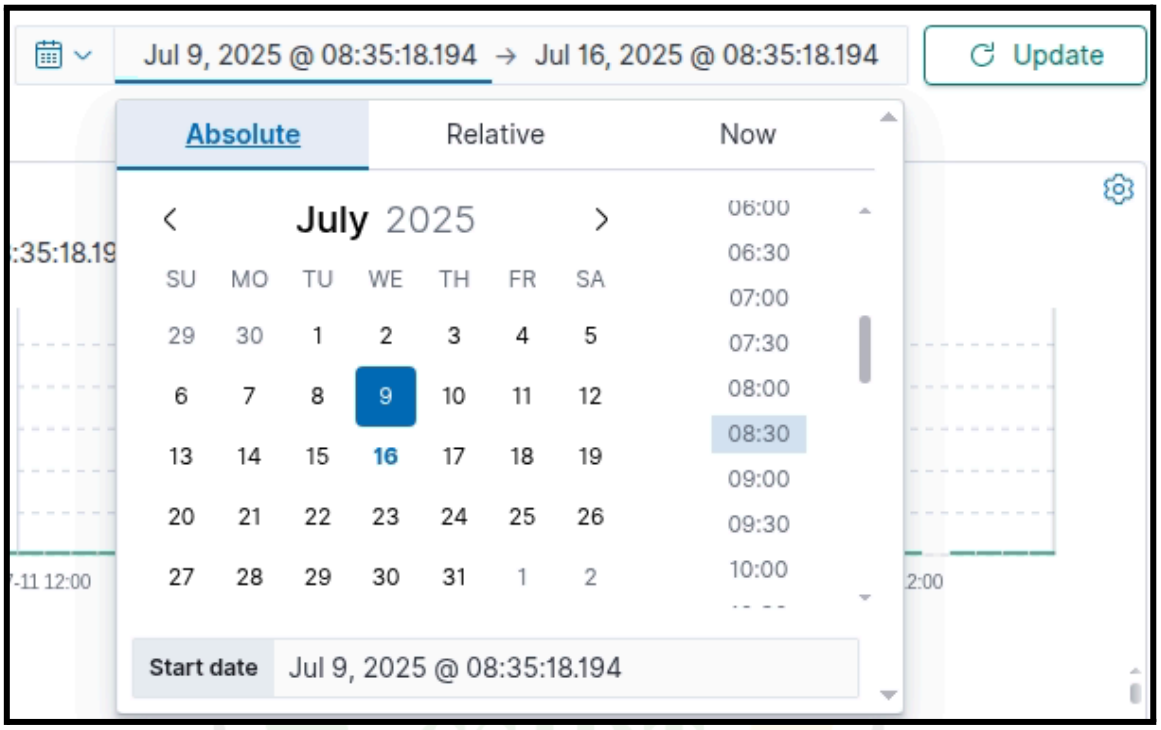


Pada bagian **tengah atas**, terdapat tombol **Add Filter** yang dapat diatur untuk menyaring informasi agar sesuai dengan yang diinginkan analis. Fungsi ini juga dapat menspesifikkan indikator insiden dalam kumpulan *event* yang sangat banyak

Field diisi dengan variabel yang ingin ditampilkan, **Operator** diisi dengan mode operasi yang diinginkan, dan **Values** diisi dengan nilai yang diinginkan.



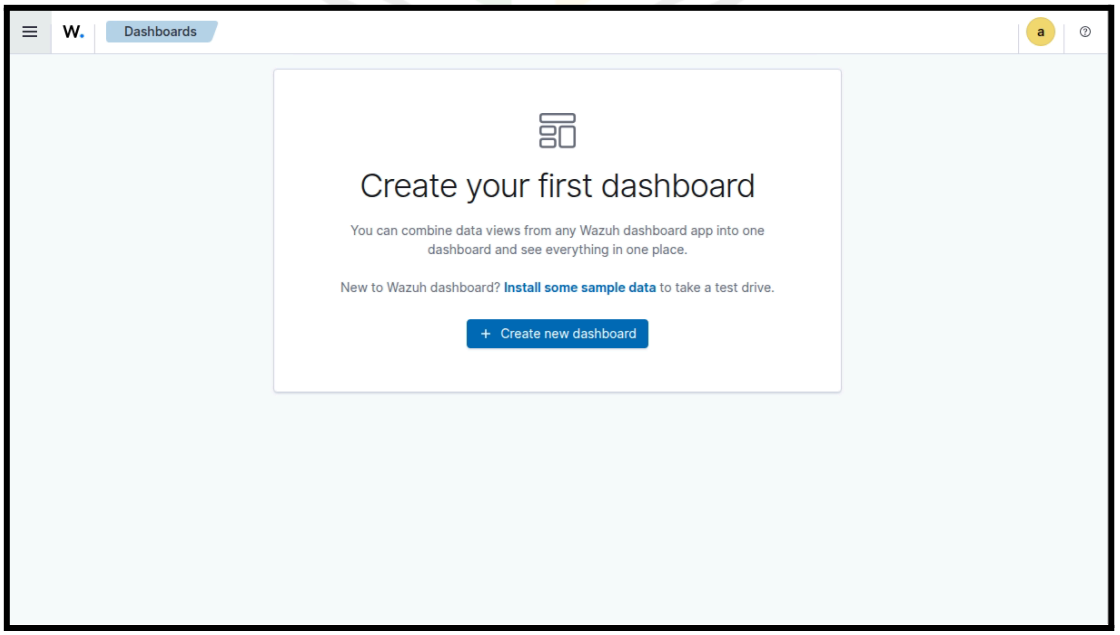
Pada bagian **kanan atas**, dapa dilakukan pengaturan rentang waktu tertentu agar informasi yang ditampilkan dapat dikerucutkan dan tidak terlalu banyak.



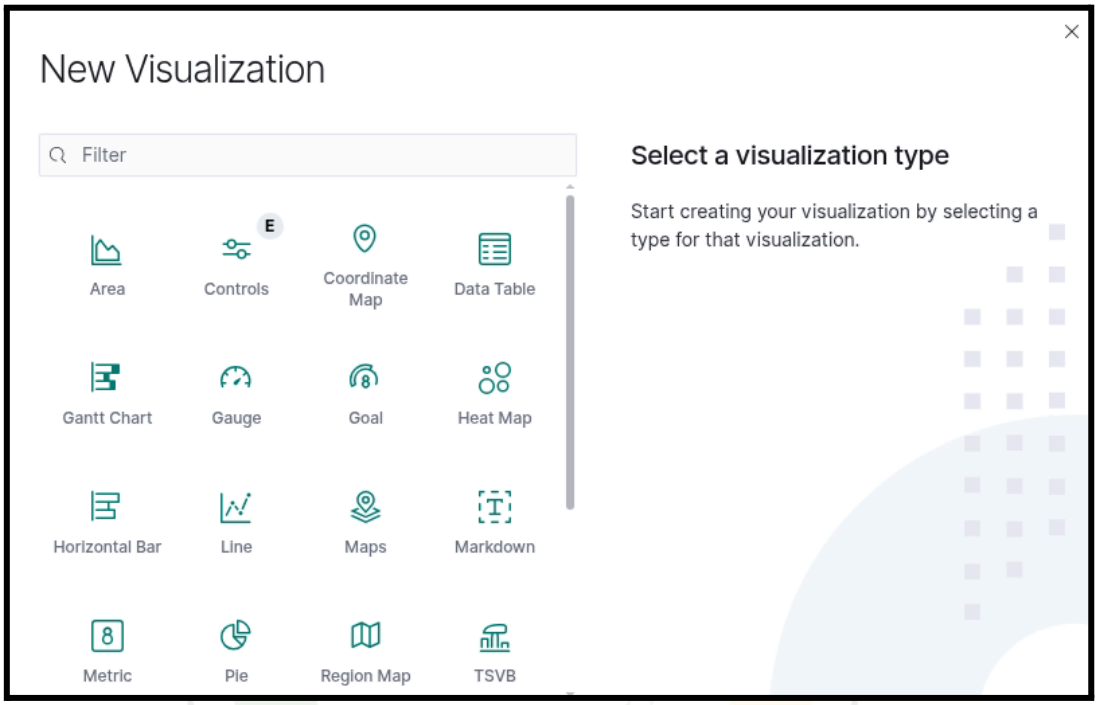
[Explore] Dashboard

Create Dashboard

Analis dapat memuat dashboard sendiri sesuai dengan jenis informasi yang ingin dianalisis.

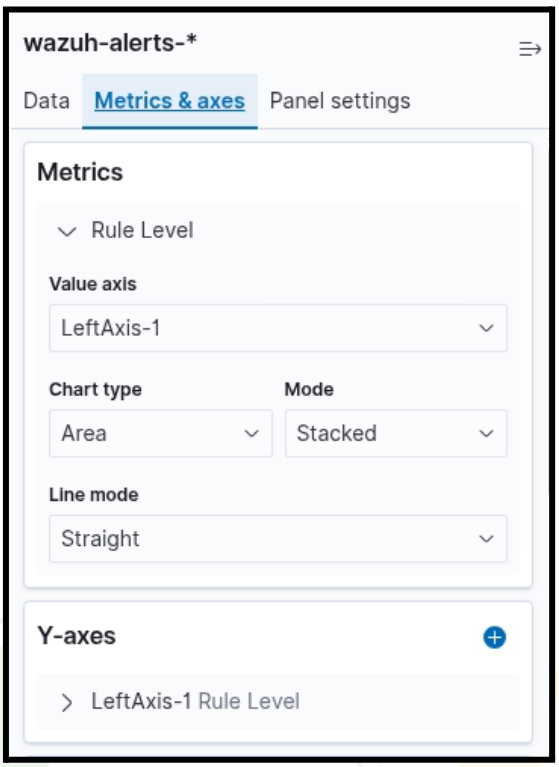


Visualisasi dashboard yang didukung Wazuh cukup banyak, seperti **Area, Gantt Chart, Line, Metric, Pie, dll**



Setelah jenis visualisasi dipilih, selanjutnya adalah menentukan kelompok informasi apa yang ingin dijadikan data input dalam dashboard. Contoh pilihan *data source* diantaranya adalah **wazuh-alerts**, **wazuh-monitoring**, atau *custom view* seperti **main** yang dibuat sendiri oleh analis.

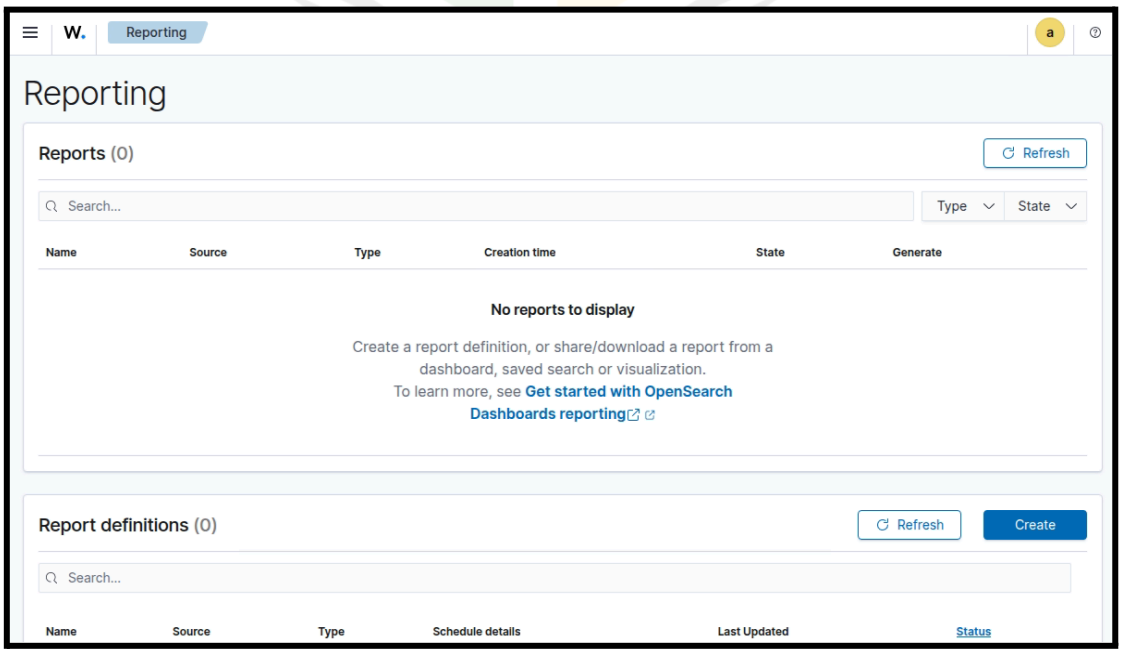
Sebagai contoh, dipilih *source* **wazuh-alerts**, atur Metrics yang akan digunakan dalam dashboard sesuai dengan kebutuhan analisis.



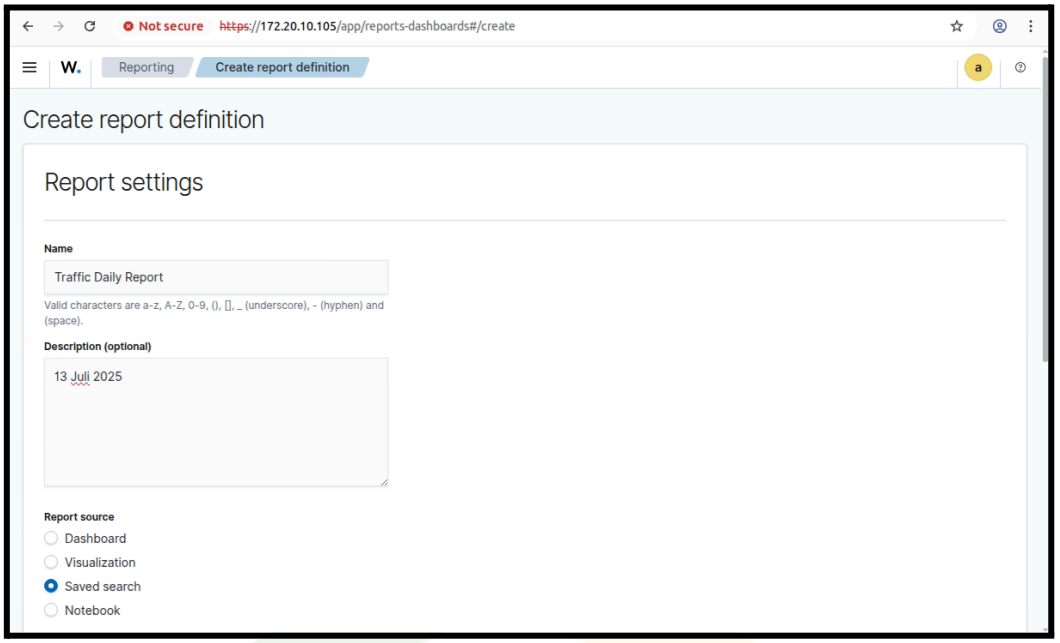
[Explore] Reporting

Create Report in XLSX or CSV Format

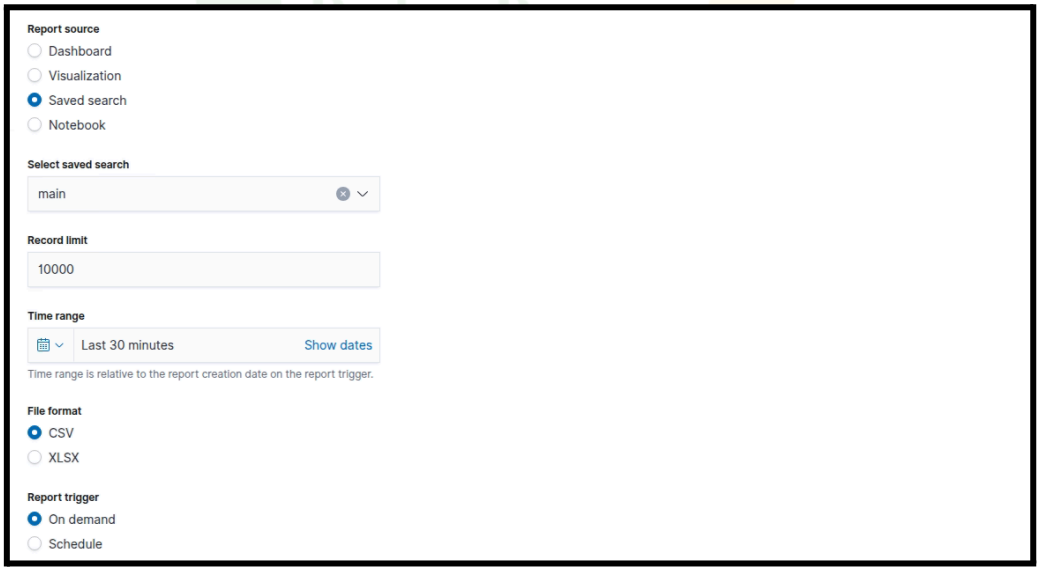
Wazuh dapat melakukan pembuatan laporan dalam format **csv** atau **xlsx.** Pada menu **Reporting,** pilih **Create** → atur pengaturan Report → **Create**



Isi sesuai keinginan dan ketentuan.

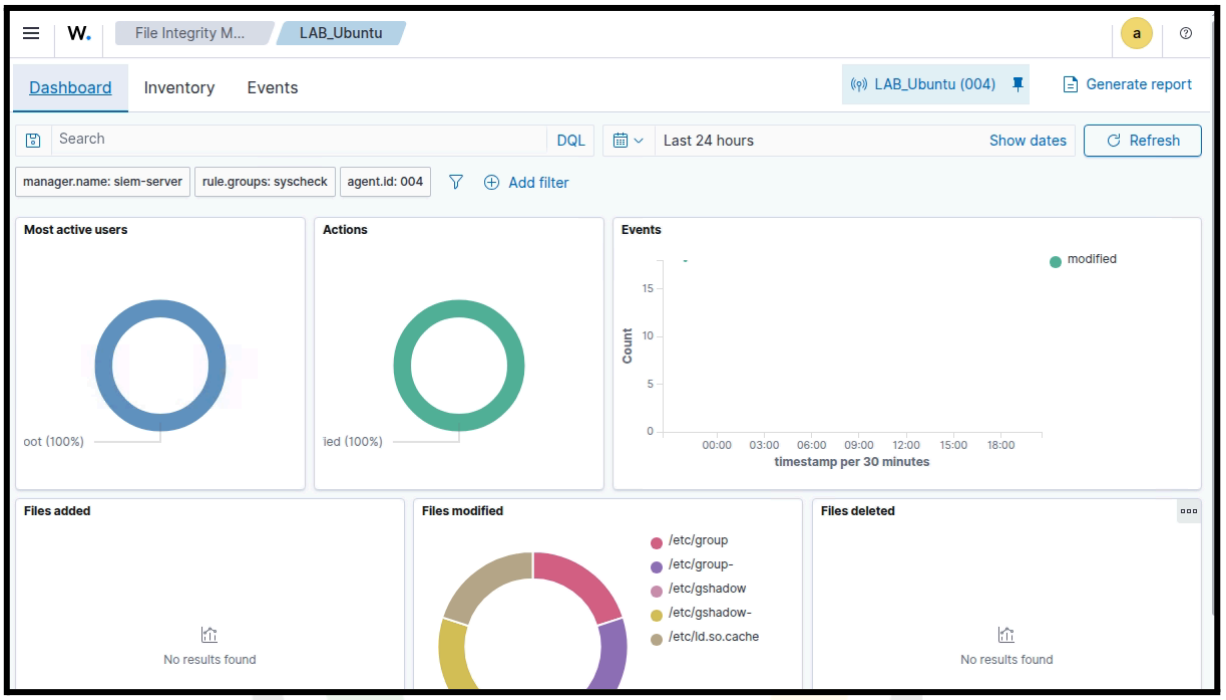


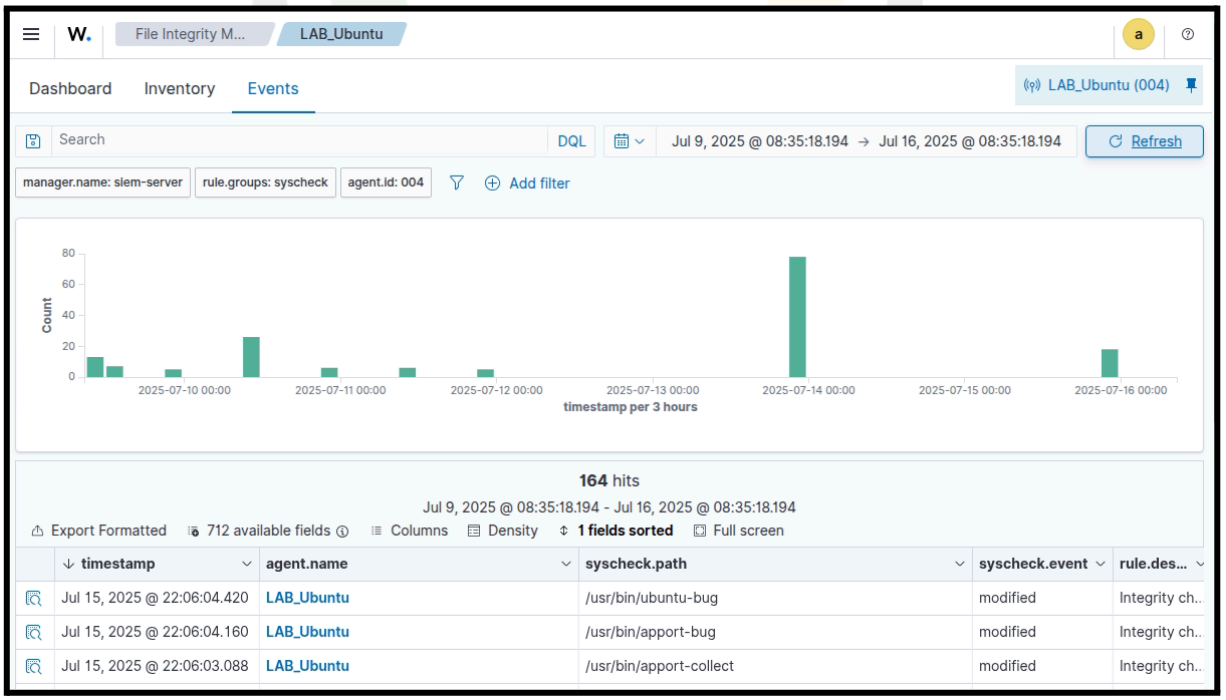
Setelah diisi, pilih **Create** pada bagian kanan atas.



[Endpoint Security] File Integrity Monitoring

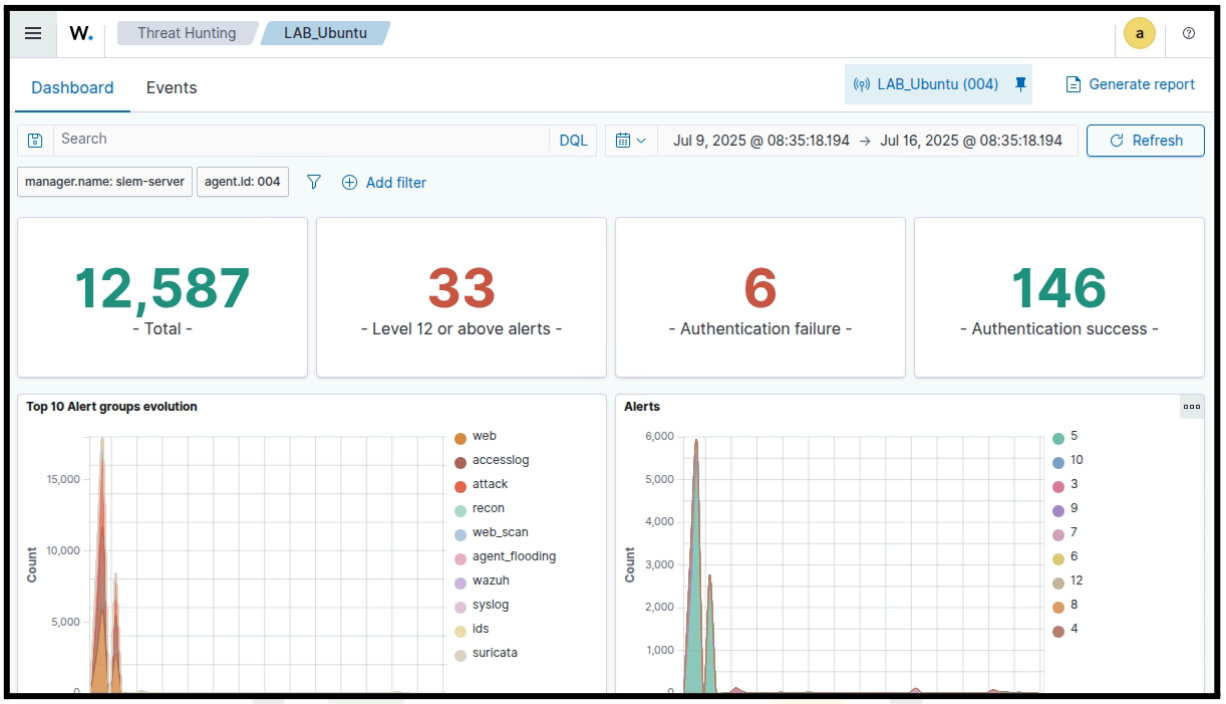
Wazuh memantau perubahan file penting pada sistem, termasuk modifikasi, penghapusan, atau penambahan file. Ini berguna untuk mendeteksi indikasi kompromi (IoC), seperti perubahan tak sah pada file konfigurasi, skrip, atau executable

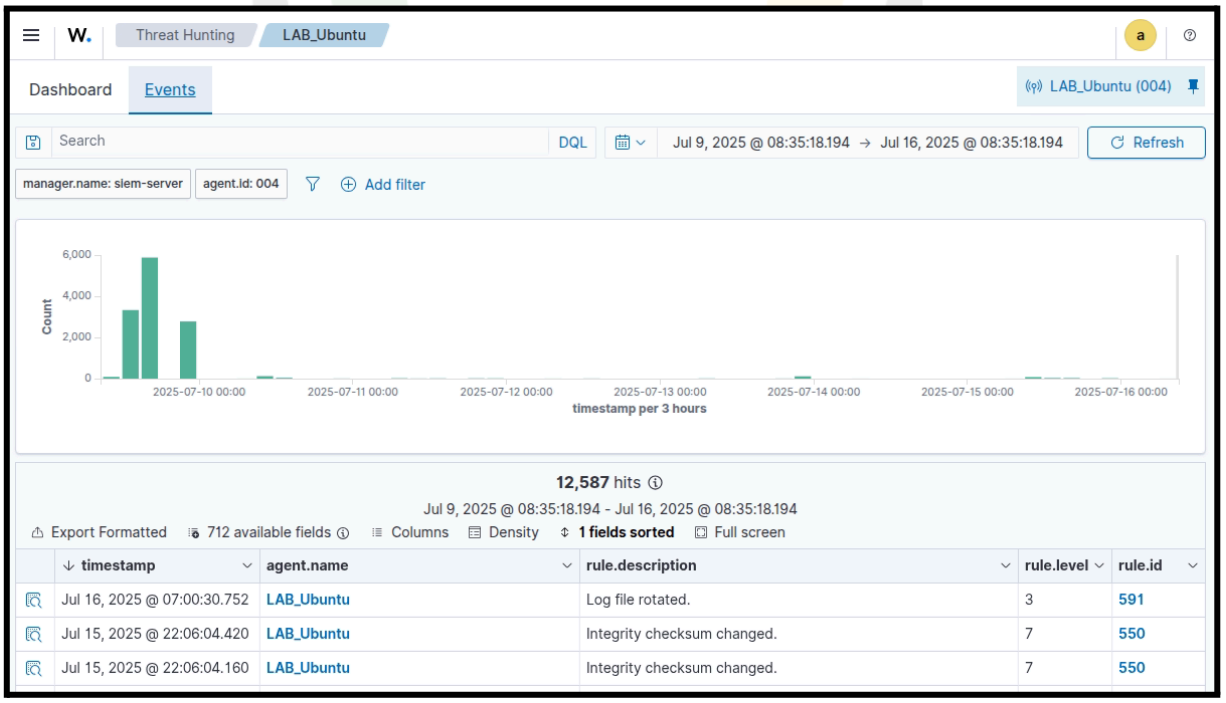




[Threat Intelligence] Threat Hunting

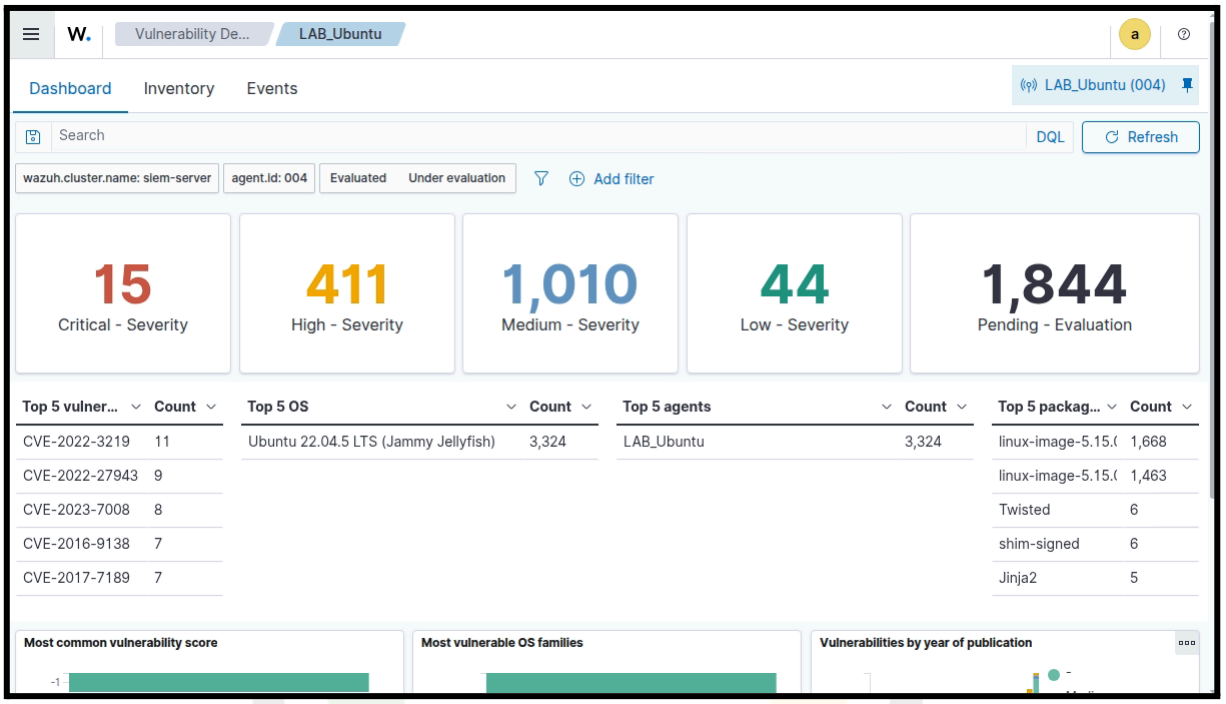
Wazuh menyediakan kemampuan analisis log yang mendalam dan pencarian berbasis aturan untuk melakukan threat hunting secara proaktif. Pengguna dapat mencari pola serangan, aktivitas command-and-control, atau eksploitasi sistem berdasarkan indikator ancaman yang diketahui.

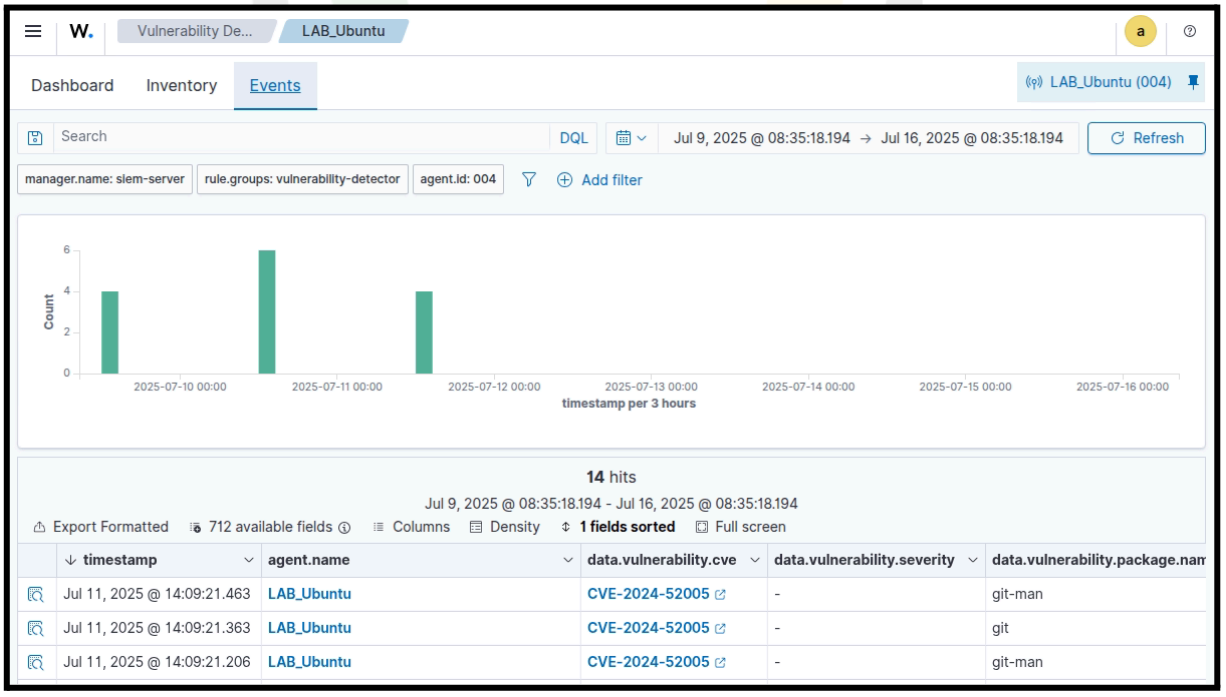




[Threat Intelligence] Vulnerability Detection

Wazuh secara berkala memindai sistem dan perangkat lunak untuk mendeteksi kerentanan (CVE) yang belum ditambal. Informasi ini membantu tim keamanan untuk melakukan mitigasi proaktif sebelum kerentanan tersebut dieksploitasi oleh pihak tidak bertanggung jawab.

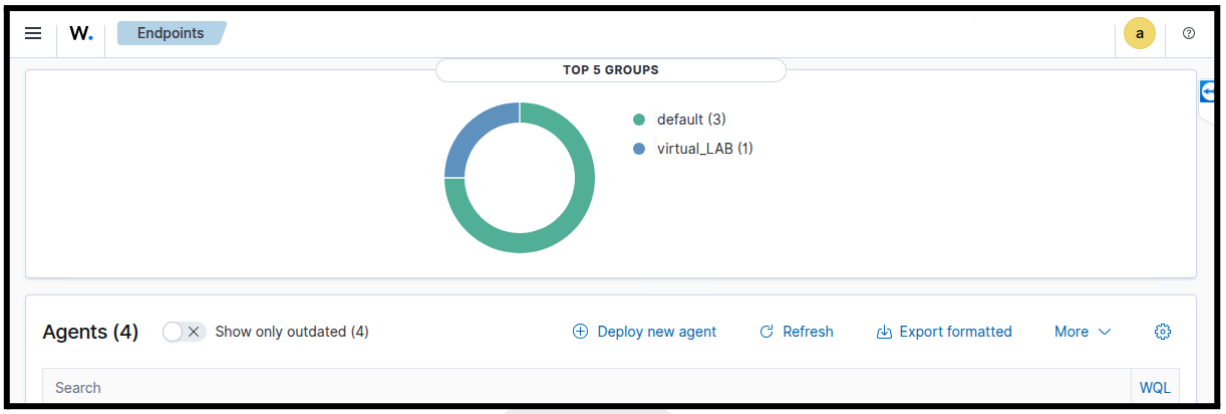




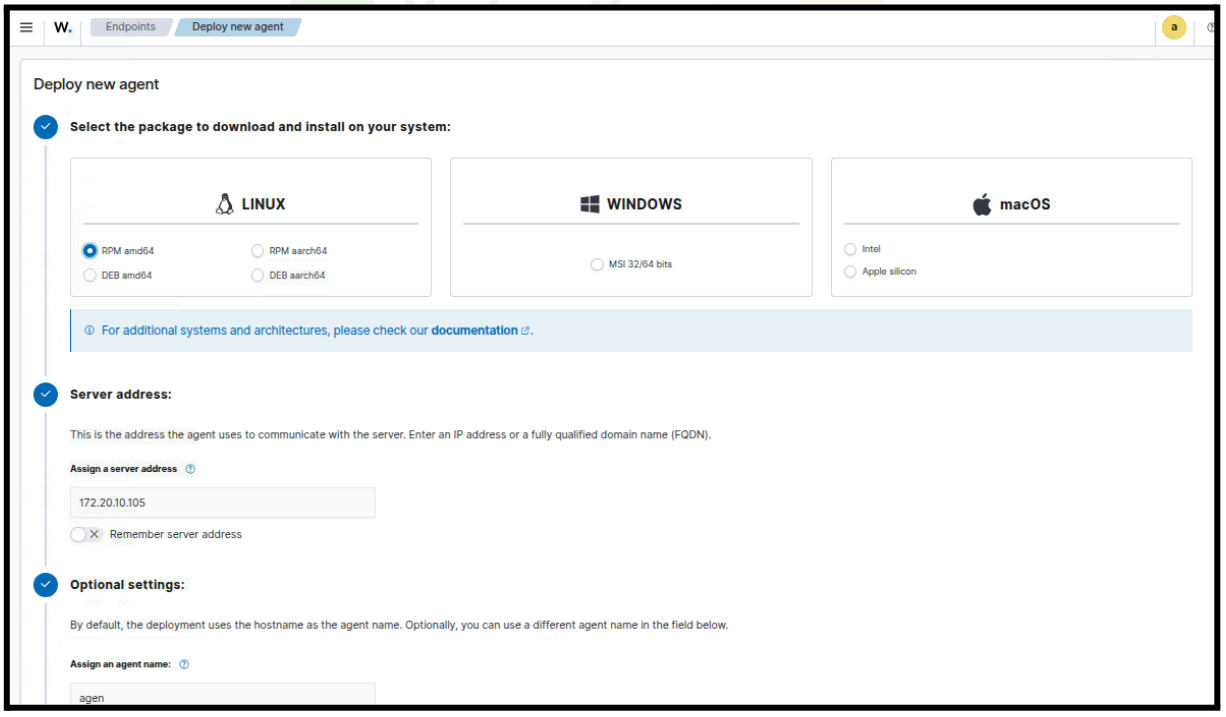
[Agent Management] Summary

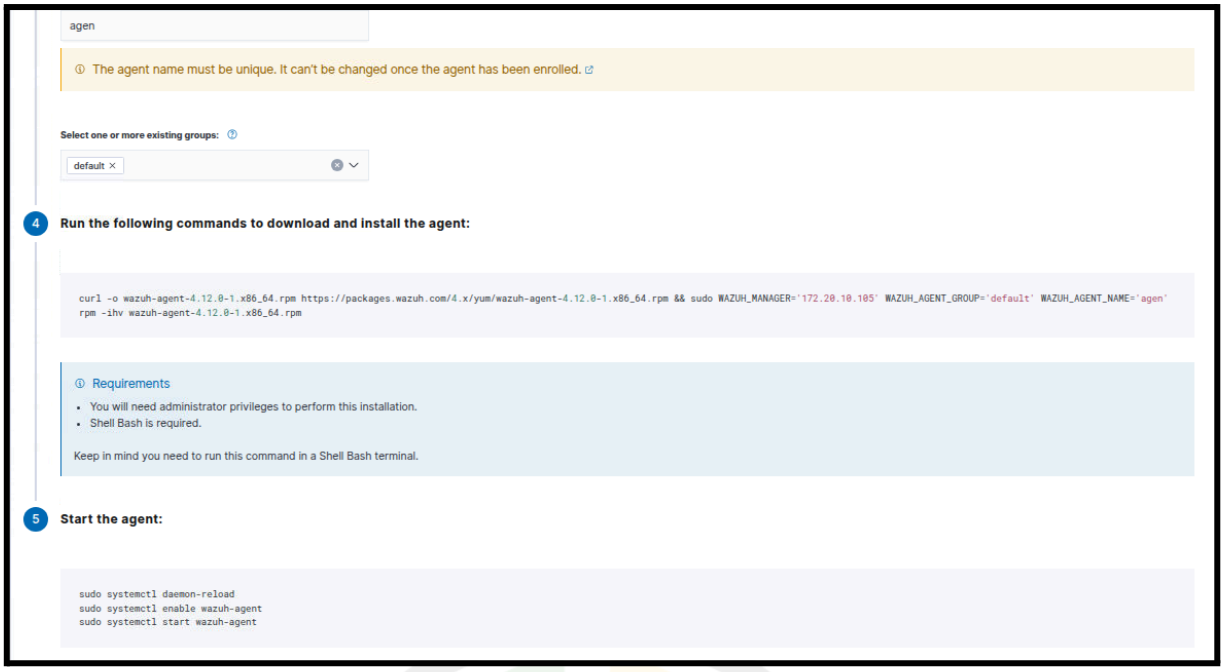
Add New Agent

Untuk menambahkan agent, klik ***Deploy new agent.***

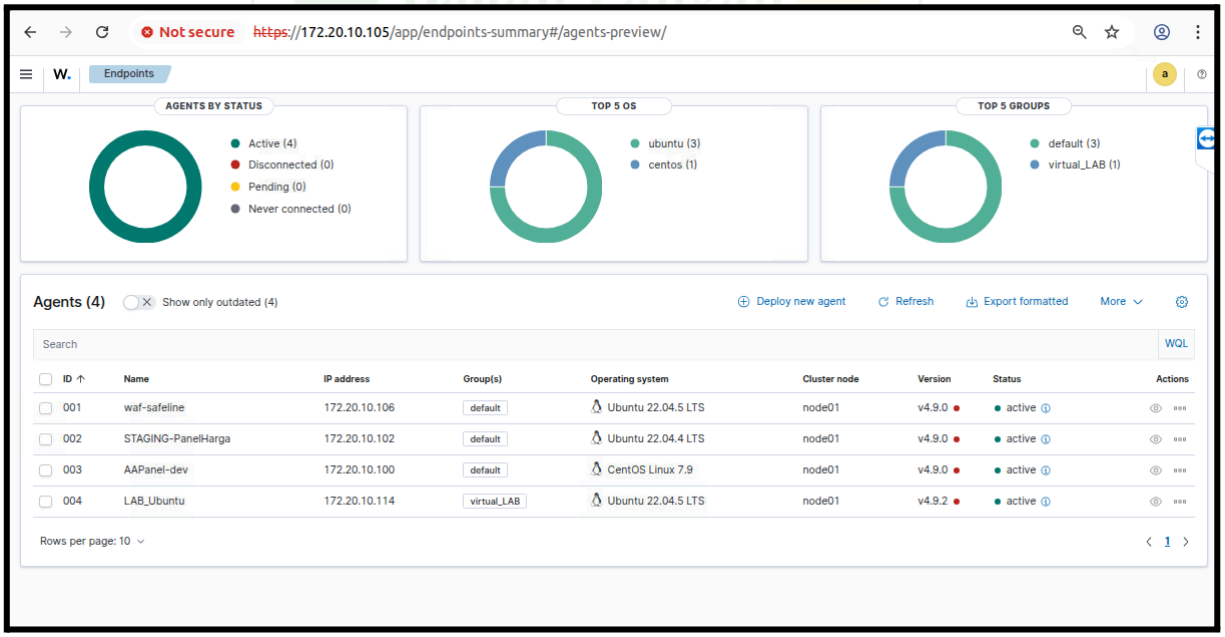


Isi kolom sesuai informasi agen dan server. Pada bagian paling bawah akan muncul perintah/*command* yang perlu dijalankan pada mesin agent untuk men-*deploy* agent. Lakukan sesuai petunjuk.





Periksa bahwa agent berhasil di-*deploy* dan muncul pada daftar agent di halaman awal.



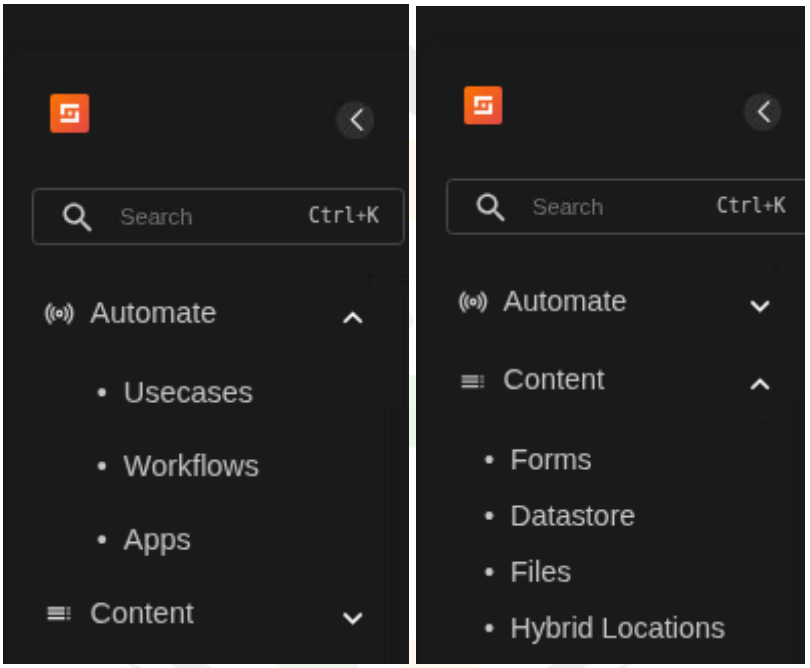
Dokumentasi Resmi

https://documentation.wazuh.com/current/index.html

Shuffle

Shuffle adalah platform *Open Source* SOAR (*Security Orchestration, Automation, and Response*) yang dikembangkan oleh Netflix. SOAR adalah pendekatan yang mengintegrasikan keamanan, otomatisasi, dan tanggapan kejadian keamanan untuk membantu organisasi mengelola dan merespons ancaman keamanan dengan lebih efisien.

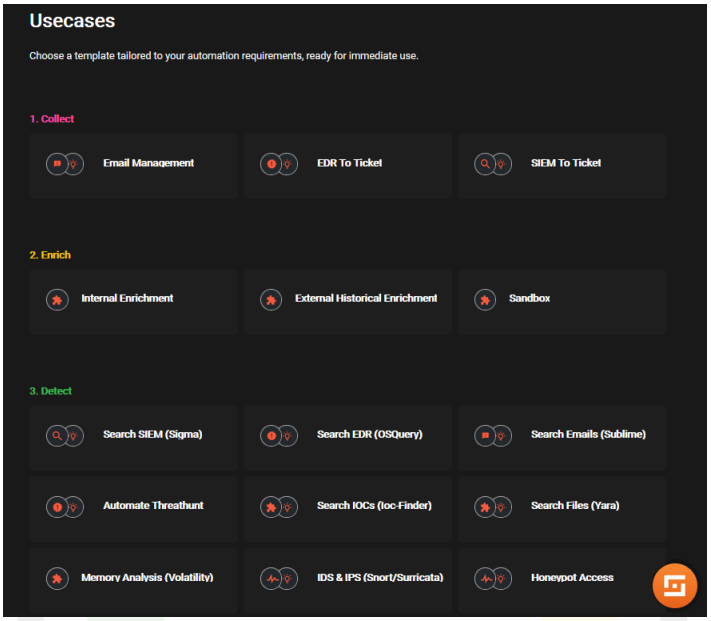
Fitur



Automate

Use cases

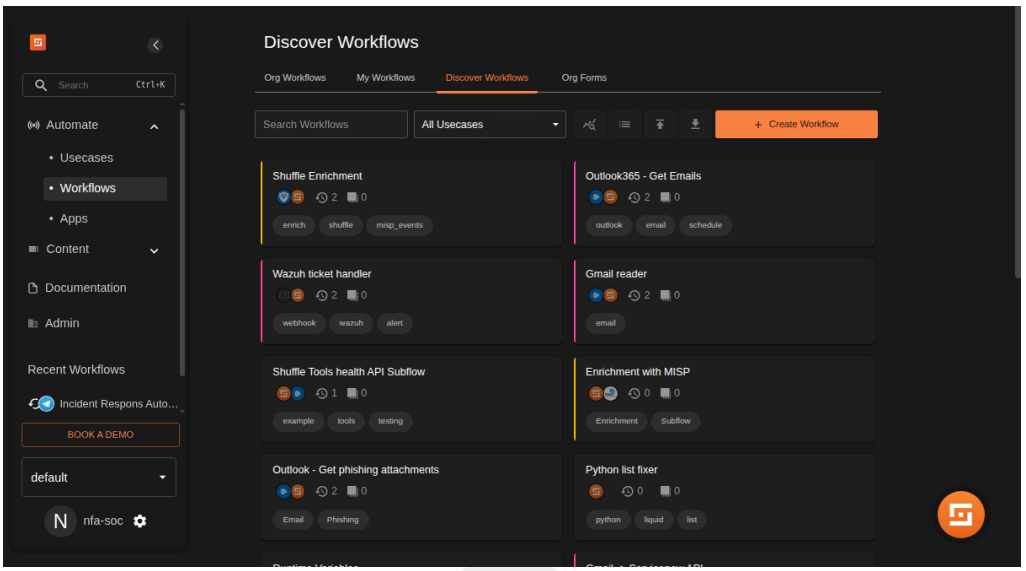
Use Case adalah workflow yang dibuat secara otomatis yang melakukan suatu tugas secara bersama-sama. Hal ini dapat berupa hal-hal seperti menangani peringatan EDR, melakukan analisis phishing, atau menggunakan aturan deteksi dengan Sigma dengan SIEM.



Workflows

Workflows adalah komponen utama Shuffle yang mengotomatiskan berbagai tugas dengan antarmuka yang sederhana. Workflow menggunakan **Apps**, **Trigger**, **Condition**, dan **Variable** untuk membuat otomatisasi yang kuat dalam waktu singkat.

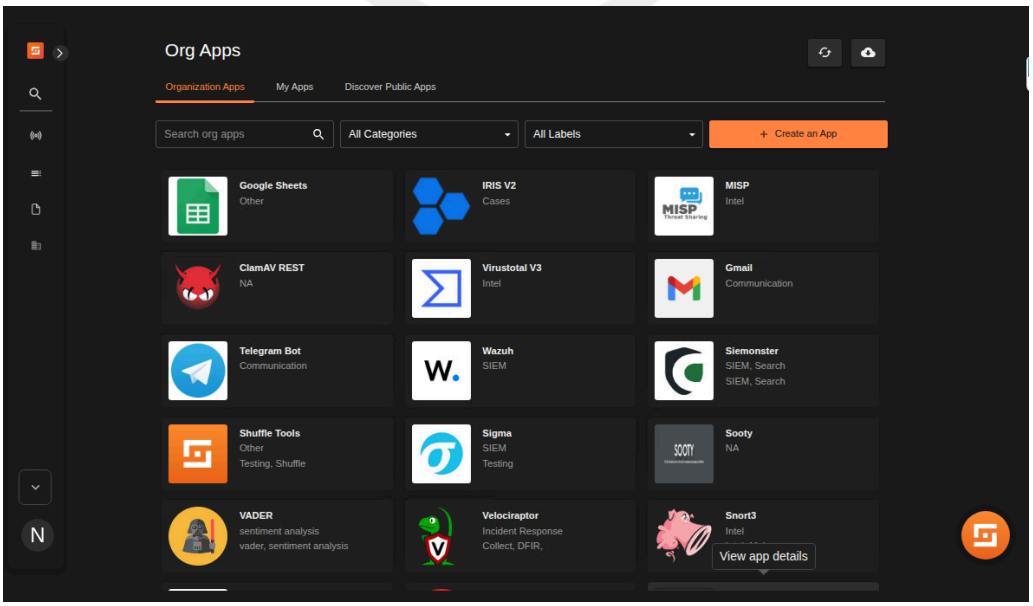
- **Apps:** komponen dalam Shuffle yang memberikan akses ke pustaka fungsi (*library*) dan dibuat menggunakan OpenAPI atau Python
- **Trigger:** operator yang digunakan untuk menjalankan workflow secara otomatis. Pemicu sering kali menjadi simpul awal pada workflow. Trigger biasanya mengambil argumen eksekusi yang akan digunakan untuk menjalankan workflow yang dimaksud.
- **Condition:** Menentukan aliran eksekusi node dalam workflow. Sebuah *condition* didefinisikan pada cabang/baris antara dua node.



Apps

Apps atau Aplikasi adalah blok pembangun utama dalam workflow. Apps dapat dibuat secara otomatis dari spesifikasi OpenAPI atau menggunakan SDK aplikasi Shuffle. Untuk menegakkan stabilitas dan kegunaan, Shuffle menggunakan sistem versi untuk mencegah pembaruan mendadak pada aplikasi.

Aplikasi dapat berisi beberapa tindakan, yang dapat mengambil beberapa variabel. Aplikasi dibuat untuk dapat berinteraksi satu sama lain dengan menggunakan data masing-masing. Aplikasi memiliki kemampuan untuk berada di berbagai lingkungan dengan data yang berbeda (misalnya kredensial yang berbeda), sebelum menyebarkannya.



Content

Forms

Formulir input manual dari pengguna sebagai bagian dari alur kerja automasi.

Datastore

Tempat menyimpan data secara persisten yang dapat diakses dan digunakan kembali dalam berbagai workflow.

Hybrid Locations

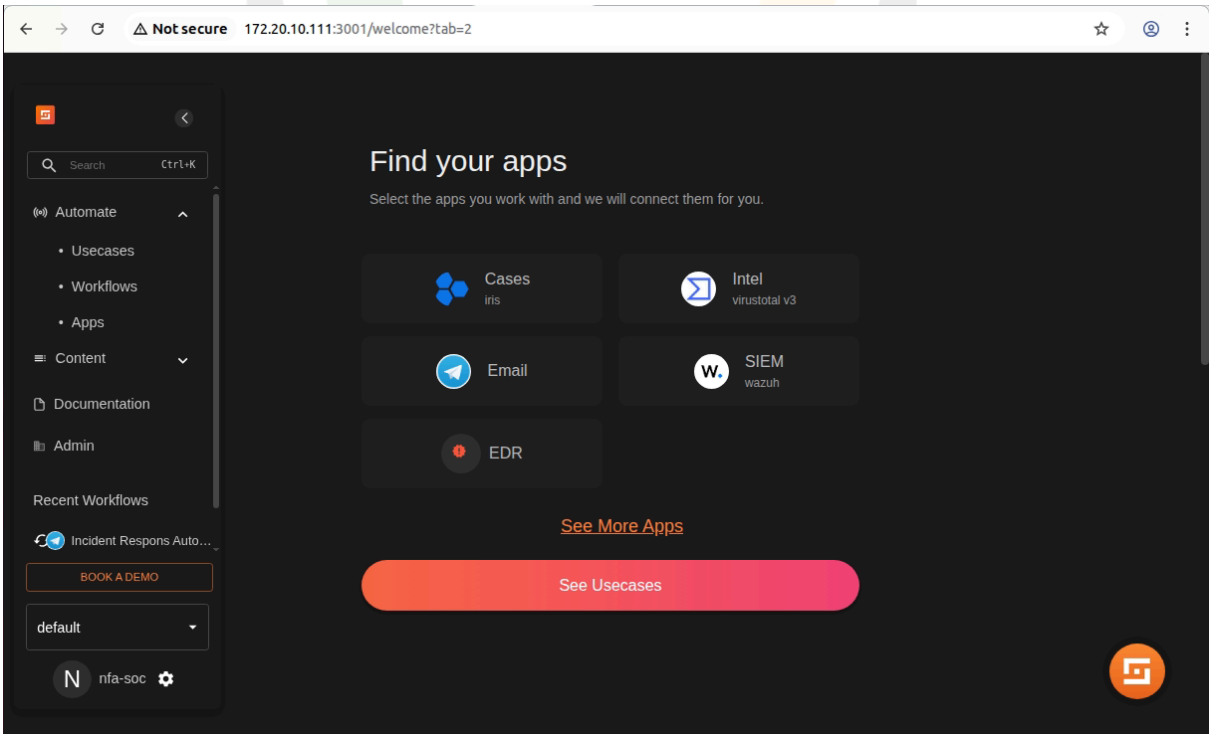
Mendukung integrasi antara lingkungan cloud dan lokal, memungkinkan eksekusi aplikasi atau workflow di lokasi hybrid secara fleksibel.

Fungsi

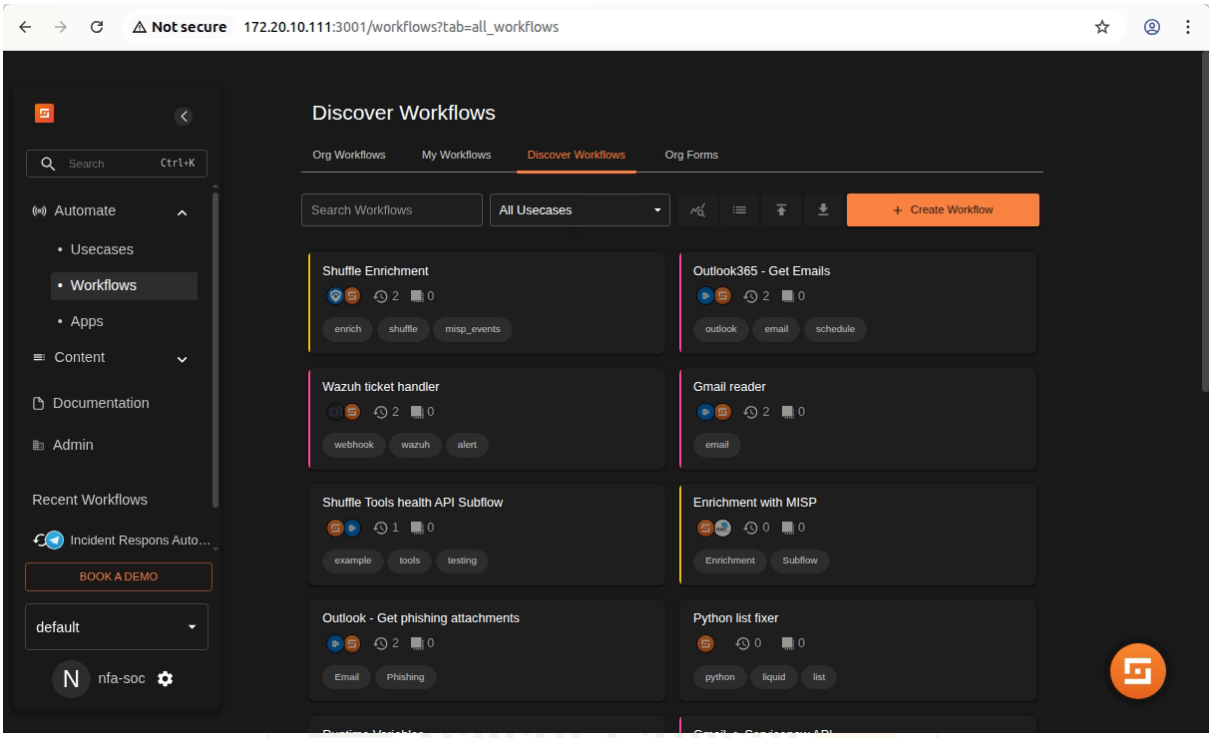
[Automate] Workflows

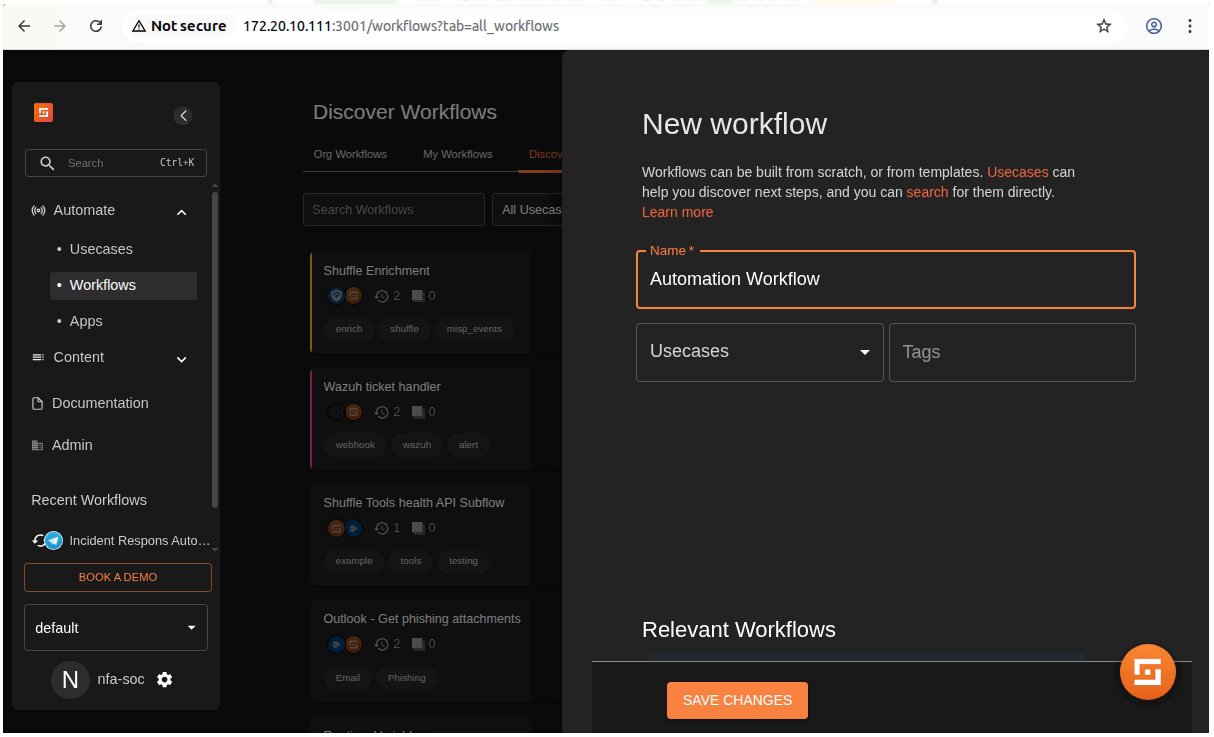
Create New Workflow

Pada halaman awal setelah Login **(Home)**, pilih **Automate** → **Workflows** yang berada di bar sebelah kiri.

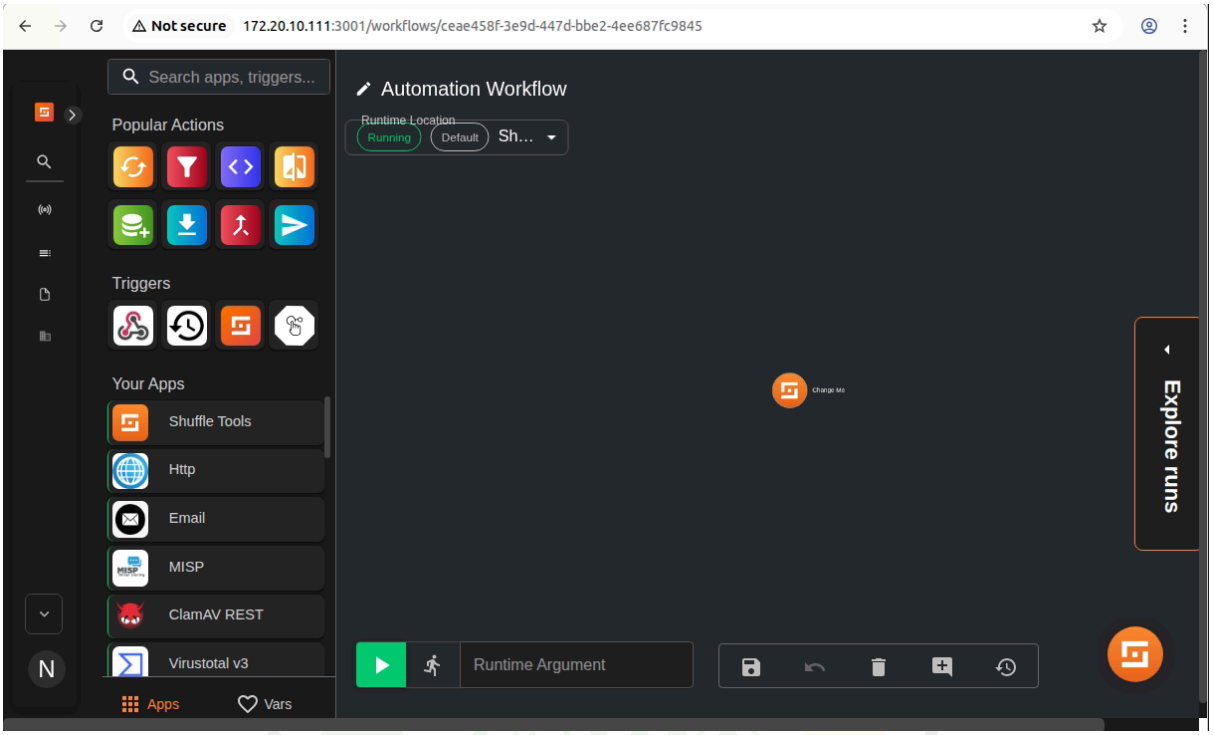


Pilih **+ Create Workflow** dan beri nama *workflow* yang akan dibuat. Isi **Usecases** dan **Tags** bila perlu. **Save Changes** untuk mengonfirmasi pembuatan *workflow*.





Berikut adalah tampilan awal *workflow* yang baru dibuat. Bagian sebelah kiri adalah daftar *Popular Actions*, *Triggers*, dan aplikasi yang bisa diintegrasikan menggunakan Shuffle,.

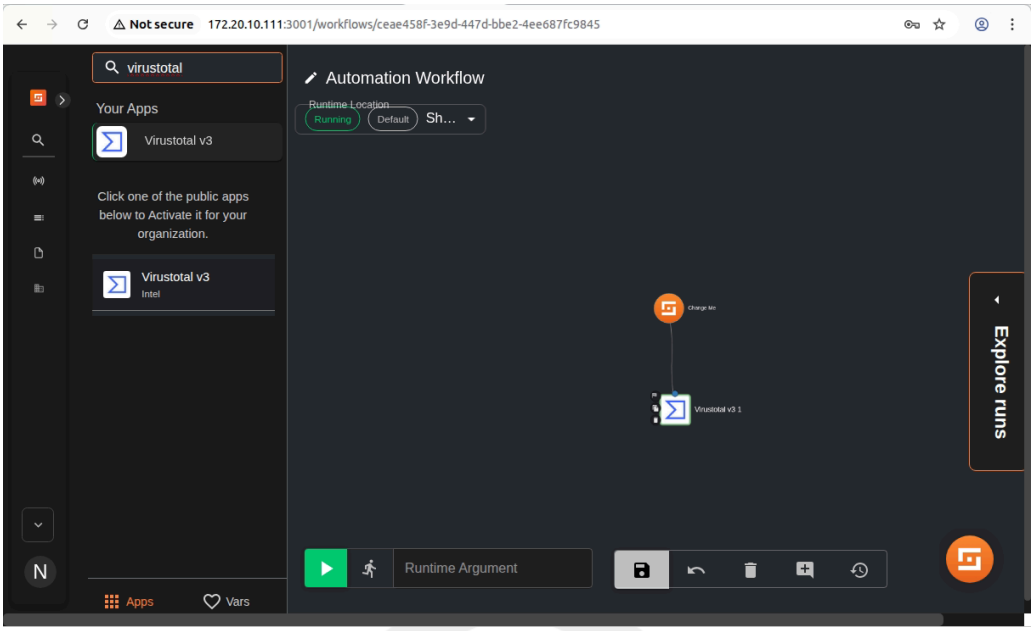


Connect with External Tools/Apps

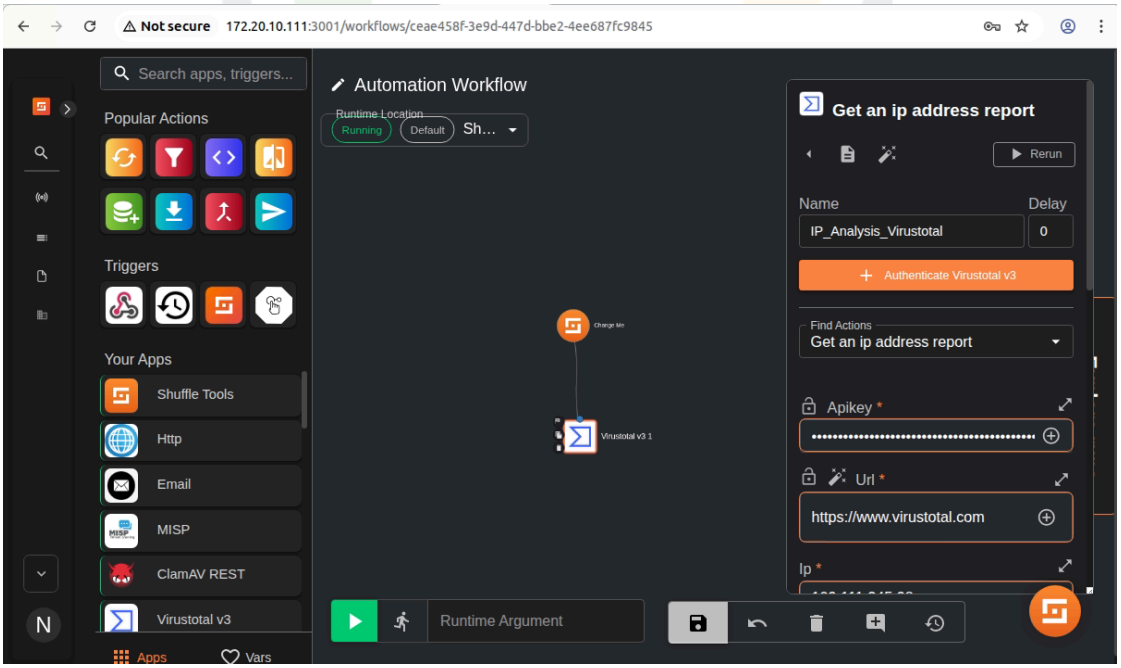
Workflow mendukung banyak aplikasi/*tools* untuk diintegrasikan, beberapa tools external yang dapat digunakan pada *workflow* Shuffle melalui API adalah Virustotal, MISP, Wazuh, dll. Pembuatan workflow dapat dimulai dengan drag and drop pada apps/trigger yang dibutuhkan.

Berikut adalah contoh koneksi dari Shuffle ke *tools* eksternal Virustotal untuk pemeriksaan alamat IP yang mencurigakan.

Pada ***search bar*** di kanan atas, cari aplikasi Virustotal, lalu *drag & drop* ke bagian *workflow*.



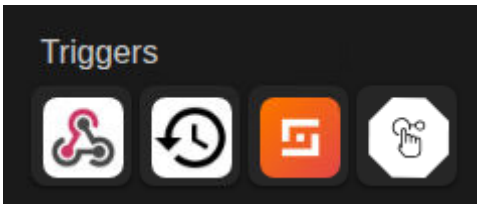
Klik node **Virustotal** lalu pilih ***Actions*** yang akan dilakukan. Pada contoh ini akan dilakukan aksi pemeriksaan laporan alamat IP. Isi parameter yang diperlukan, seperti **API key** Virustotal, **URL**, dan **alamat IP** yang akan diperiksa.
Selain mengisi parameter, dapat pula dilakukan pengubahan nama node pada kolom **Name**.



Setiap **node** dan setiap **action** memiliki required parameter yang berbeda-beda sesuai dengan kondisi dan kebutuhan aplikasi/tools.

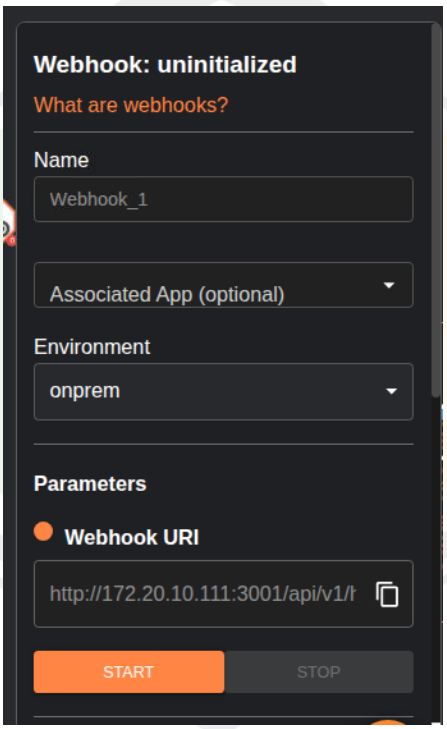
Configure Triggers

Terdapat 4 tipe *Triggers* yang dapat digunakan di Shuffle, diantaranya **Webhook**, **Schedule**, **Shuffle Workflow**, dan **User Input**.



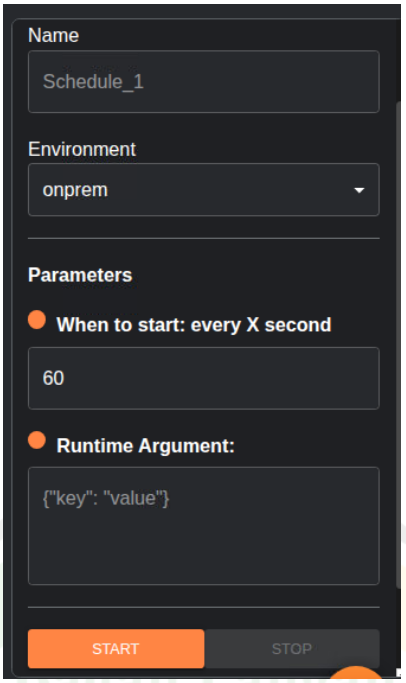
- **Webhook**

  Trigger Webhook mengharuskan **Webhook URL** dari Shuffle dikonfigurasikan pada target hook, seperti Wazuh.



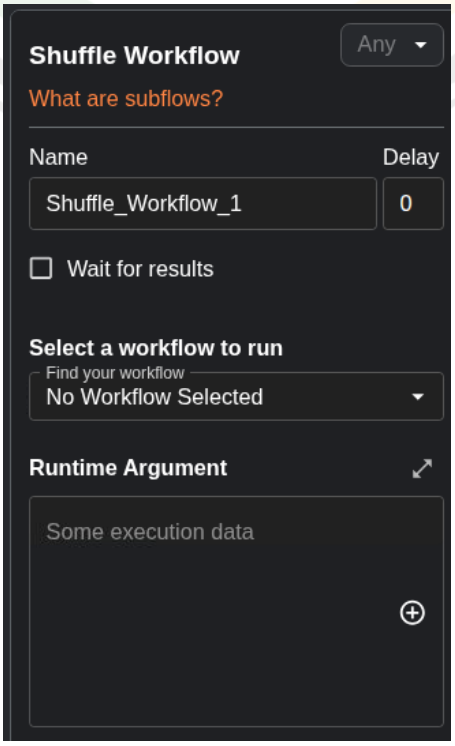
- **Schedule**

  Pada trigger Schedule dapat diatur waktu dimulainya *workflow* dan Argumen yang diberikan.



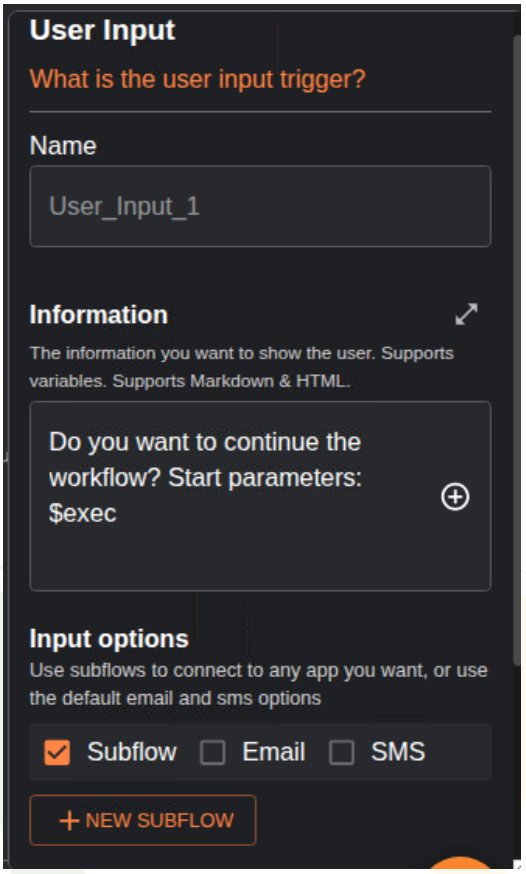
- **Shuffle Workflow**

  Workflow pada Shuffle dapat dijadikan Trigger untuk workflow lainnya sebagai Subflow.



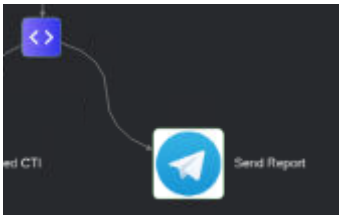
- **User Input**

  Pengguna dapat memberikan input tertentu untuk menentukan dijalankan atau tidaknya suatu workflow.

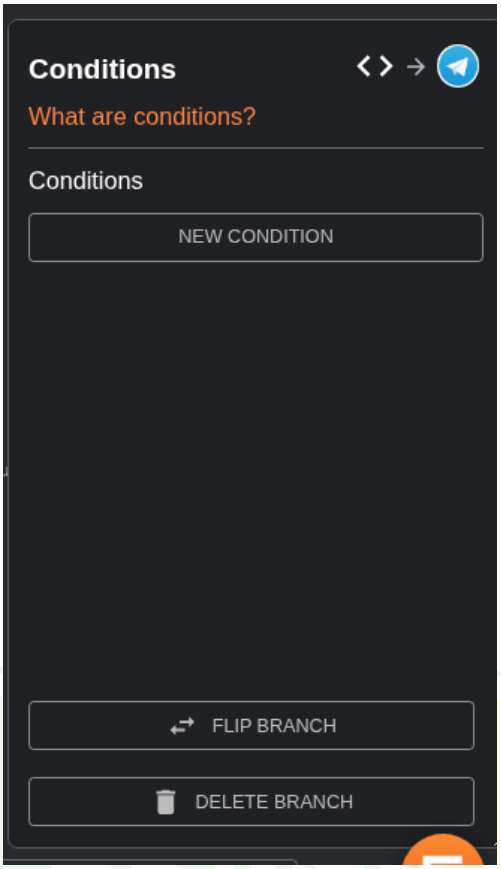


Setting Conditions

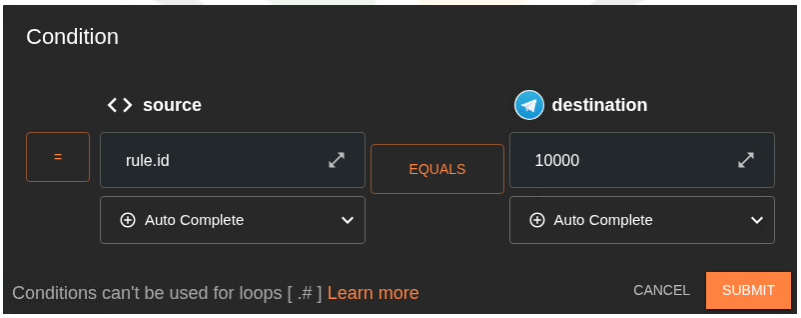
digunakan untuk mengatur percabangan logika dalam sebuah workflow automasi berdasarkan nilai atau hasil tertentu. Misalnya pada percabangan antara dua node di bawah.



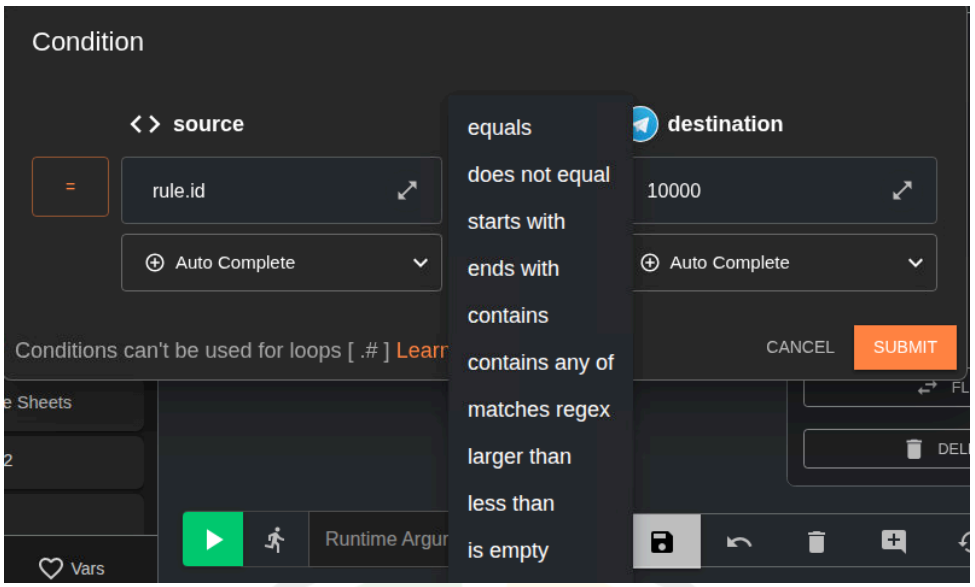
Klik **New Condition** untuk membuat condition.



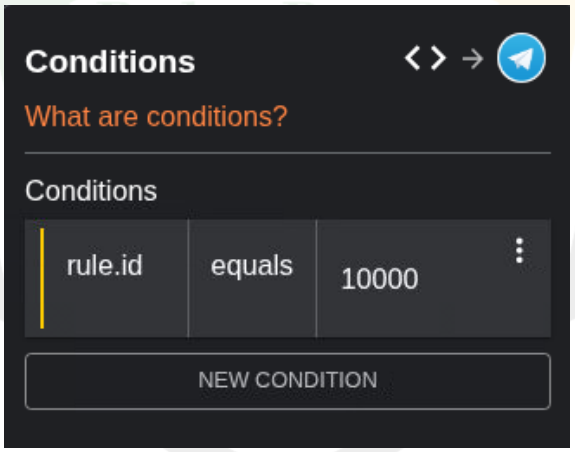
Atur parameter **key** dan **value** seperti di bawah (key: **rule.id** & value: **10000**) yang menandakan bahwa percabangan ini akan berjalan apabila rule.id pada Runtime Argument bernilai 10000.



Selain operator **Equals**, terdapat operator lain seperti **does not equal, contains, matches regex, dll**. Seperti pada gambar di bawah.

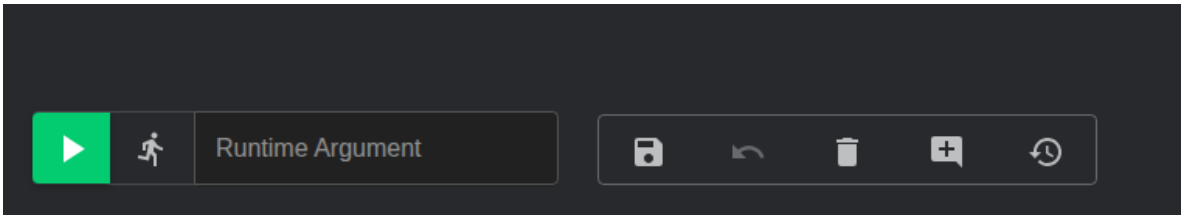


Berikut adalah hasil Conditions yang berhasil dibuat.

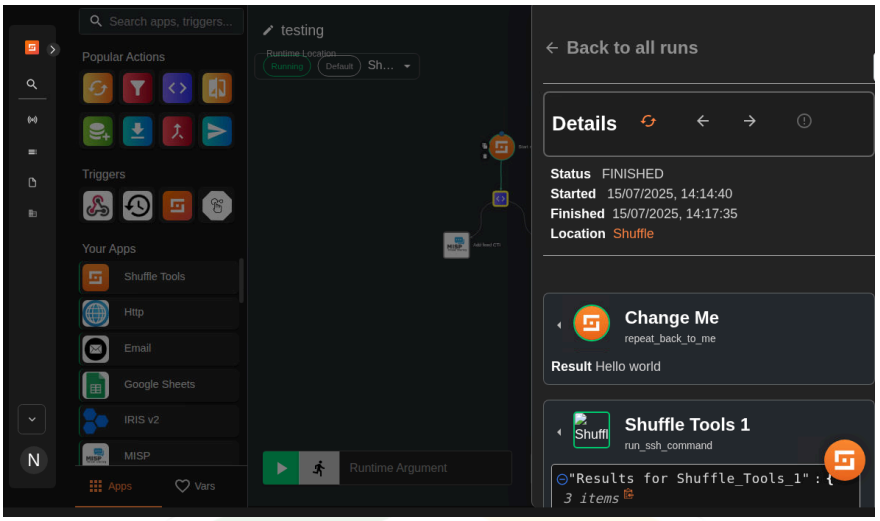


Running and Testing Workflow

Sebelum menjalankannya, pastikan *workflow* sudah tersimpan (Save). Klik icon *save* di bar bagian bawah.



Jalankan workflow dengan menekan tombol *play* berwarna hijau di bagian kiri bawah. Workflow dapat dijalankan menggunakan trigger tertentu atau menggunakan argumen (**Runtime Argument**) sebagai data input.

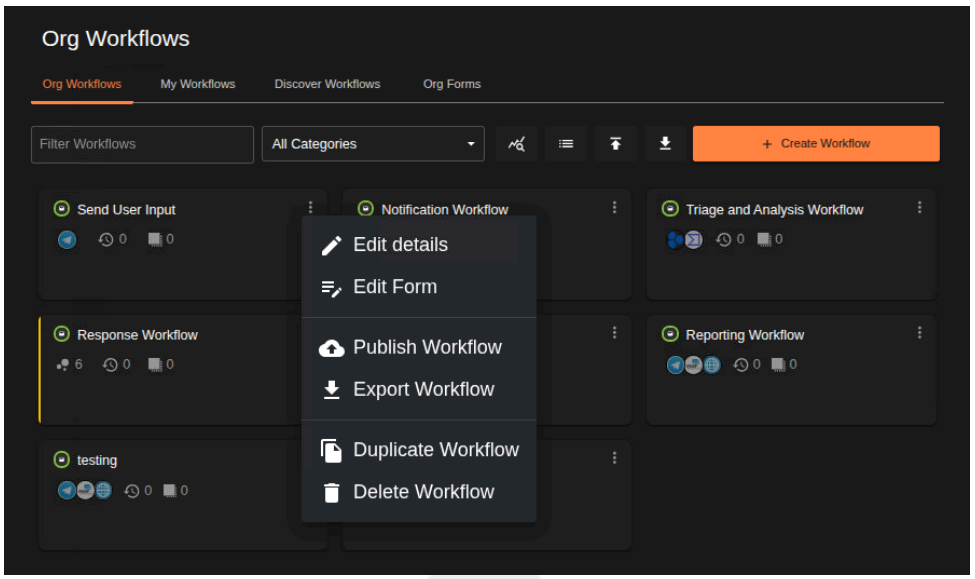


Saat *workflow* berjalan, akan muncul tampilan monitoring di sebelah kanan yang menampilkan **Details** dari *workflow*. Status *workflow* yang dijalankan terdiri dari **Executing**, **Finished**, **Waiting**, dan **Aborted**. Executing menandakan *workflow* sedang berjalan, Finished menandakan *workflow* sudah selesai, Waiting menandakan *workflow* sedang menunggu proses/*workflow* lain, dan Aborted menandakan *workflow* dihentikan sebelum selesai.

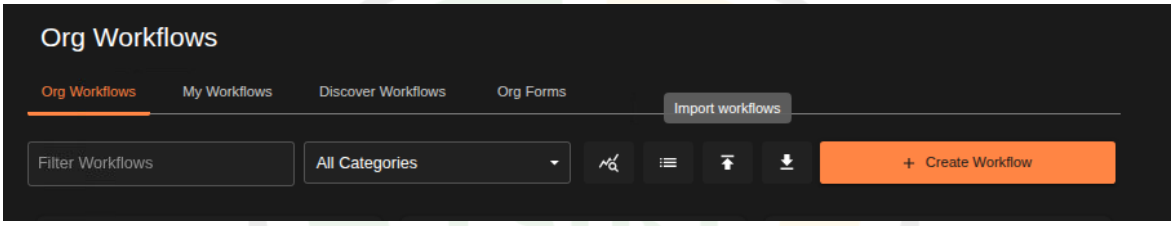
Export / Import Workflow

Shuffle mendukung ***export*** dan ***import*** *workflow* dalam format JSON. Untuk melakukan *export* atau pengunduhan, dapat dilakukan melalui langkah berikut

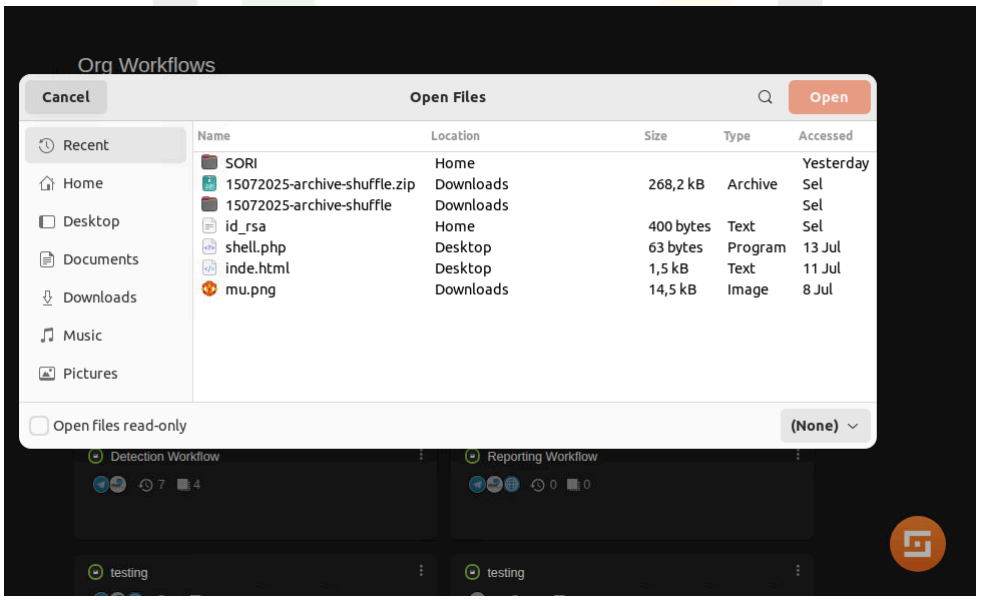
Klik **tiga titik** atau klik kanan pada workflow yang ingin di-*export*, lalu pilih **Export Workflow.**



Untuk melakukan *import*, klik icon **panah atas** pada bar sebelah atas.



Pilih file *workflow* berekstensi JSON yang ingin di-*import*.

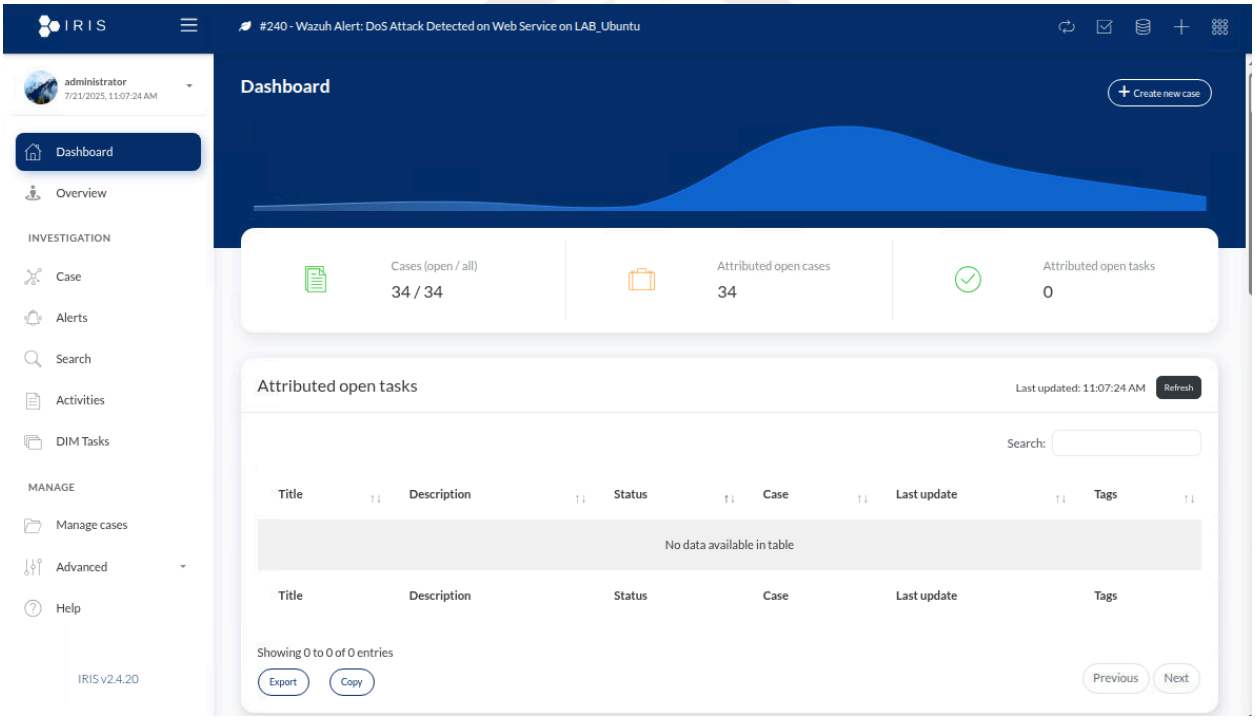


Dokumentasi Resmi

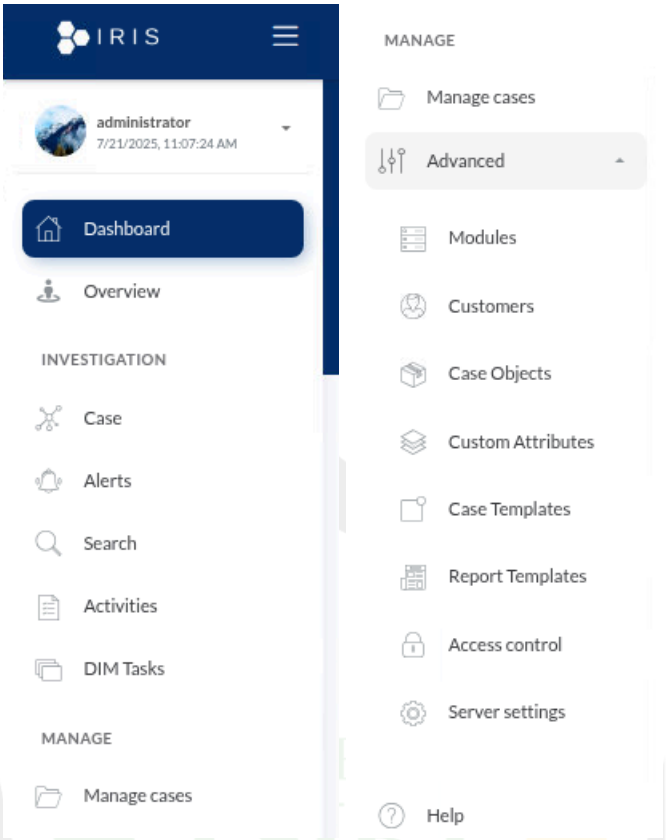
https://shuffler.io/docs/

DFIR IRIS

DFIR-IRIS adalah platform open-source yang dirancang khusus untuk membantu proses **Digital Forensics and Incident Response (DFIR)**. IRIS berfungsi sebagai sistem manajemen insiden yang memungkinkan tim keamanan mendokumentasikan, melacak, dan mengkoordinasikan respons terhadap insiden siber secara terstruktur. Dengan fitur seperti timeline insiden, manajemen bukti, korelasi artefak, serta integrasi dengan alat forensik lainnya, DFIR-IRIS memperkuat proses investigasi dan pelaporan insiden, sehingga mempermudah tim dalam memahami skenario serangan dan meresponsnya dengan cepat dan efisien.

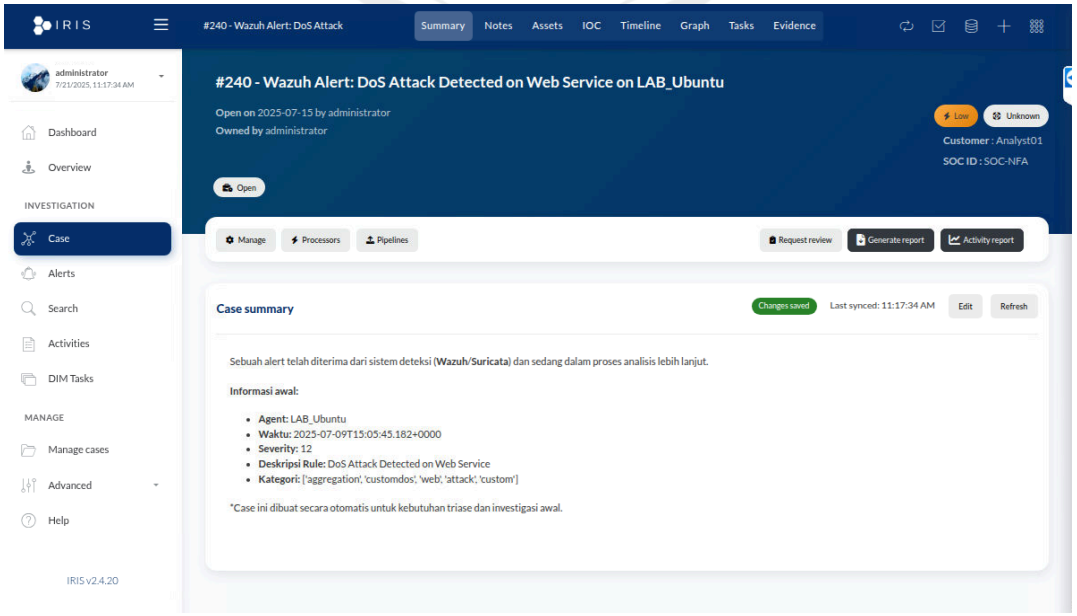


Fitur



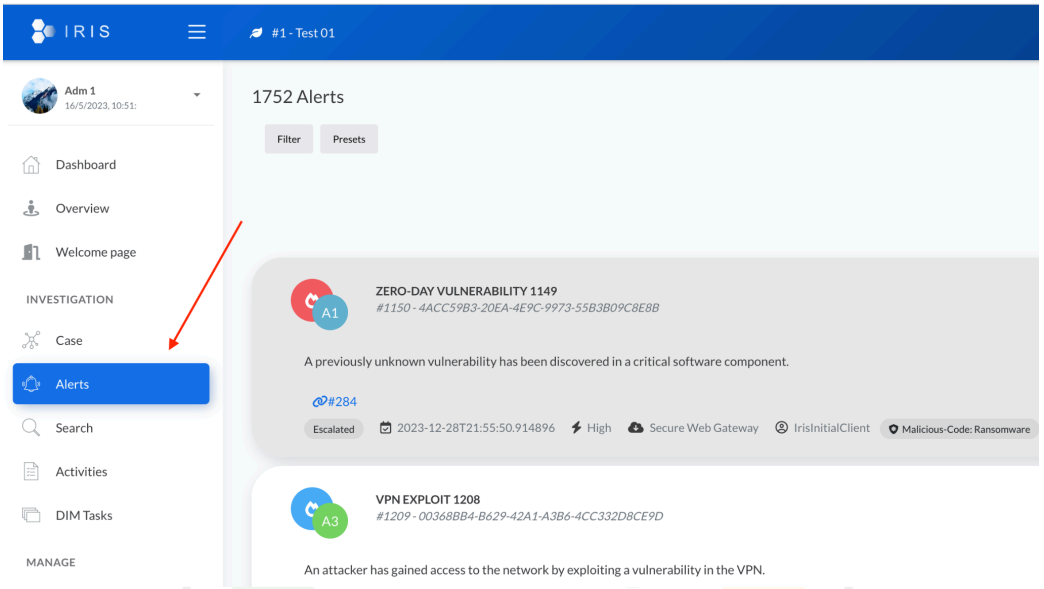
Case Management

Membuat, mengelola, dan melacak insiden siber secara terstruktur. Fitur ini memfasilitasi dokumentasi lengkap terkait kronologi, artefak, tindakan, dan status penanganan kasus.



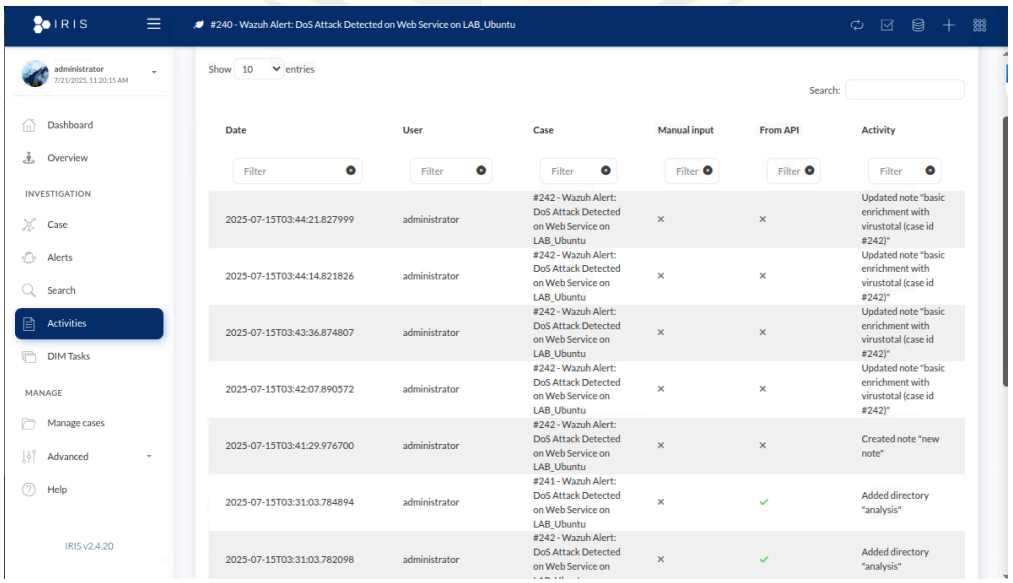
Alerts Management

mengelola peringatan (alerts) yang masuk dari berbagai sumber deteksi. Alerts ini dapat ditinjau dan dihubungkan langsung ke kasus yang relevan untuk ditindaklanjuti lebih lanjut.



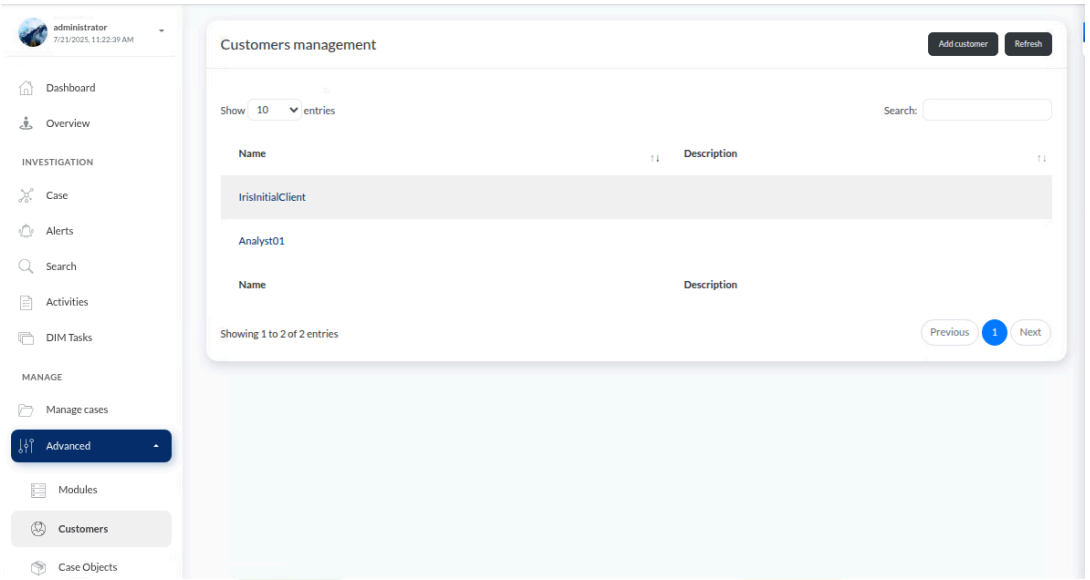
Activities Management

Menyediakan log aktivitas terkait setiap kasus atau entitas yang ditangani. Hal ini membantu pelacakan tindakan tim dan audit trail selama investigasi berlangsung.



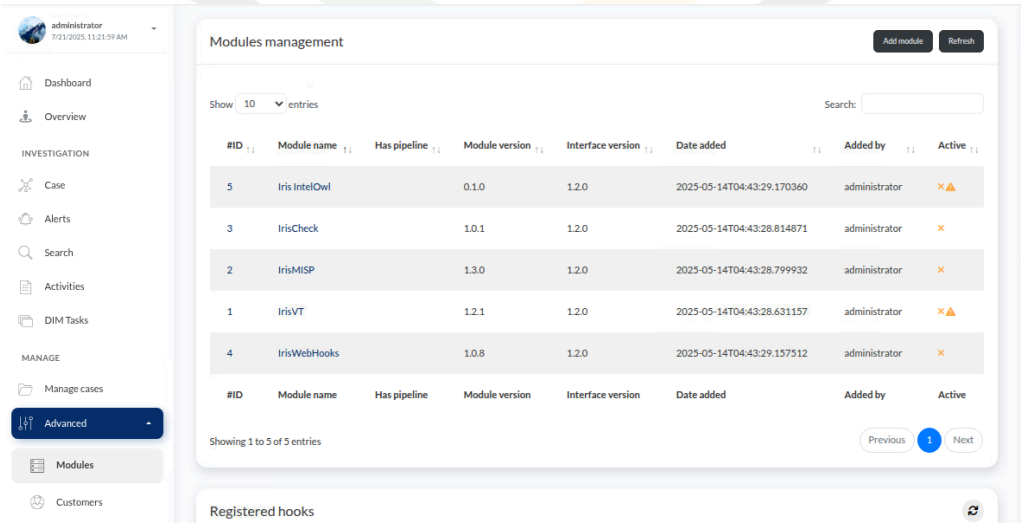
Customer Management

Memungkinkan manajemen informasi pelanggan atau entitas yang terkait dengan insiden. Fitur ini bermanfaat dalam konteks penyedia layanan keamanan atau organisasi multi-klien.



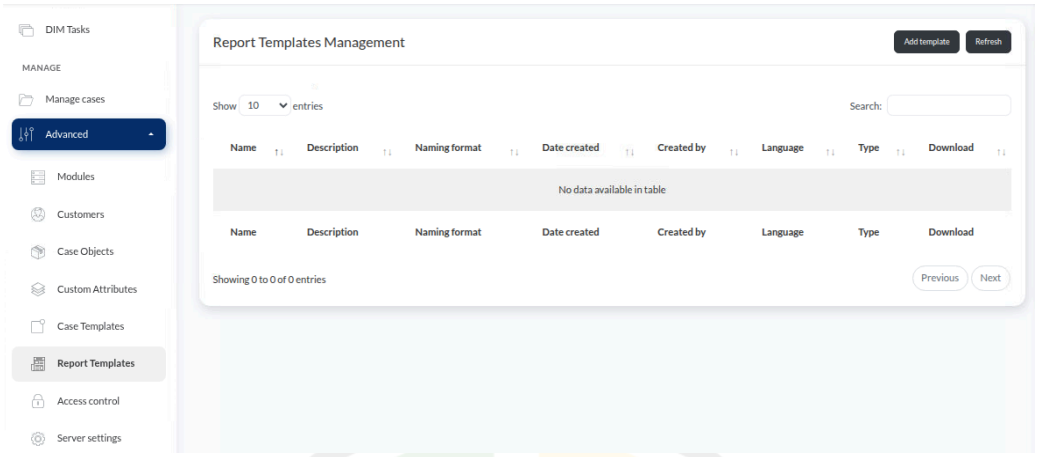
Modules Management

mengelola integrasi dan fungsionalitas tambahan dalam IRIS, seperti plugin atau koneksi ke sistem eksternal. Ini memberikan fleksibilitas dalam memperluas kapabilitas platform.



Report Management

Memfasilitasi pembuatan dan pengelolaan laporan insiden secara otomatis atau manual. Laporan ini dapat disesuaikan dan diekspor untuk dokumentasi resmi atau pelaporan ke manajemen/pihak eksternal.

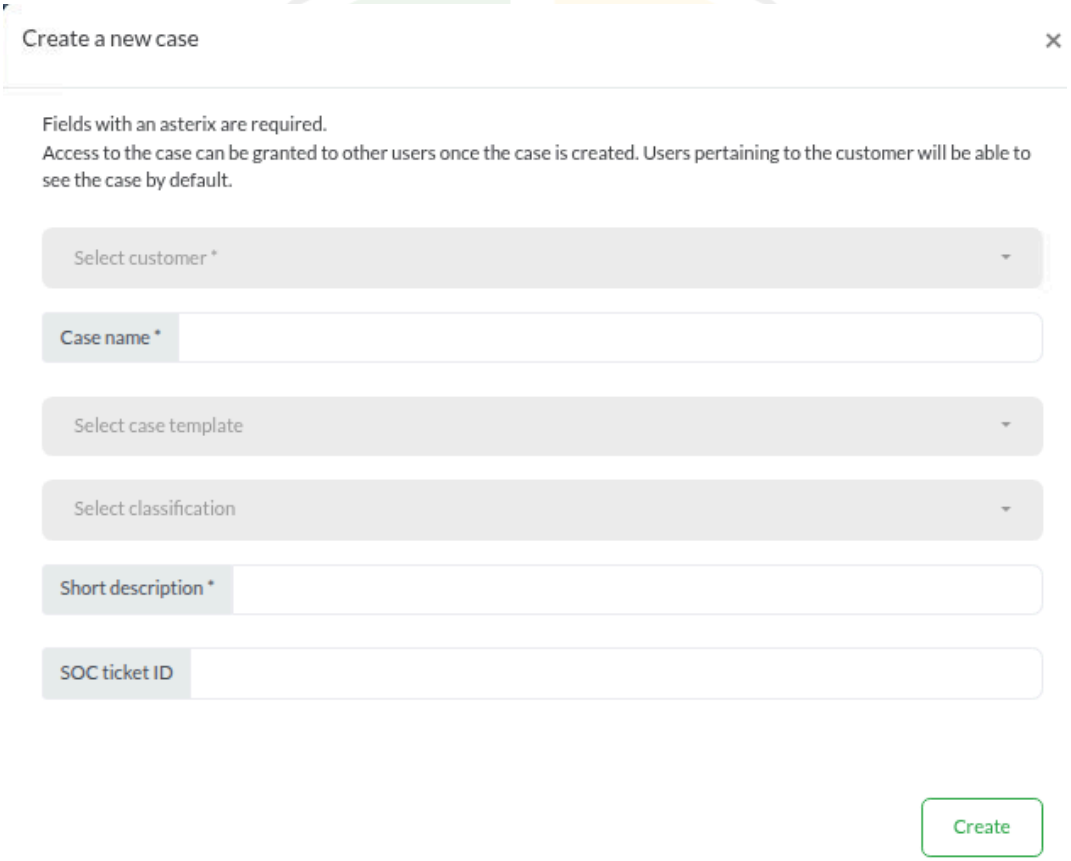


Fungsi

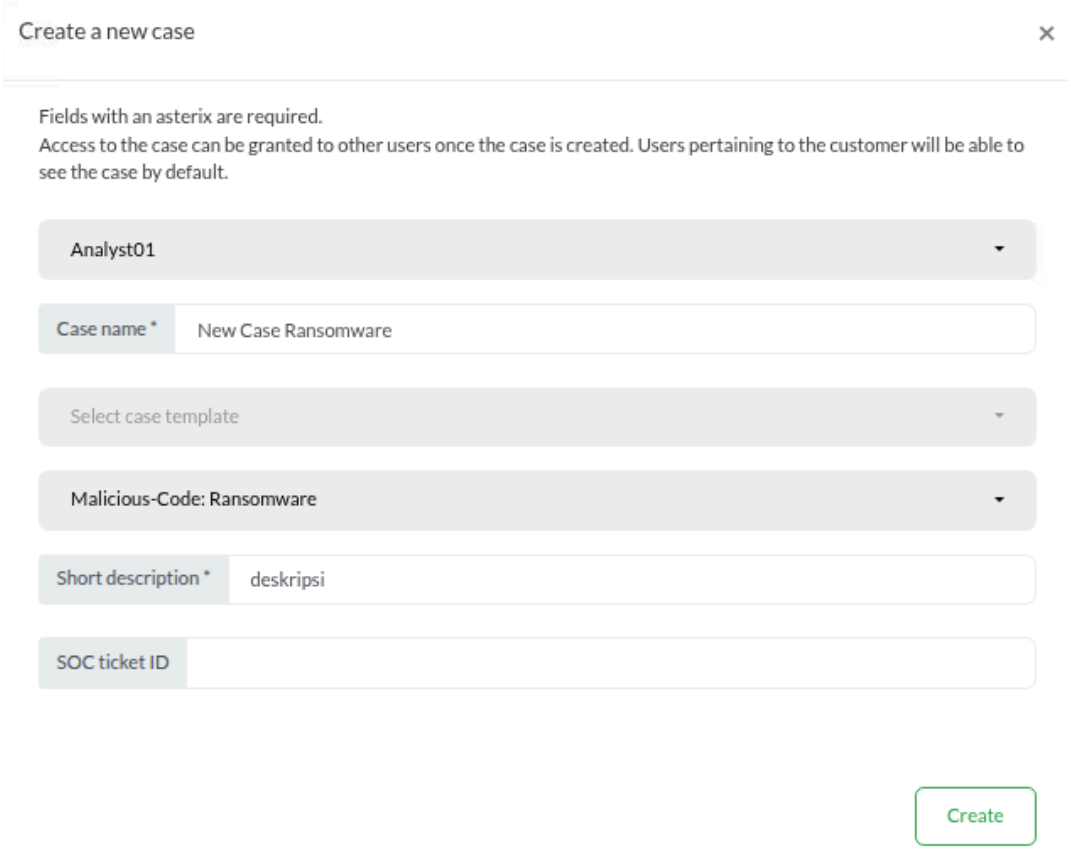
[Case Management] Create new Case

Pada halaman dashboard, klik **+Create New Case** pada bagian kanan atas.

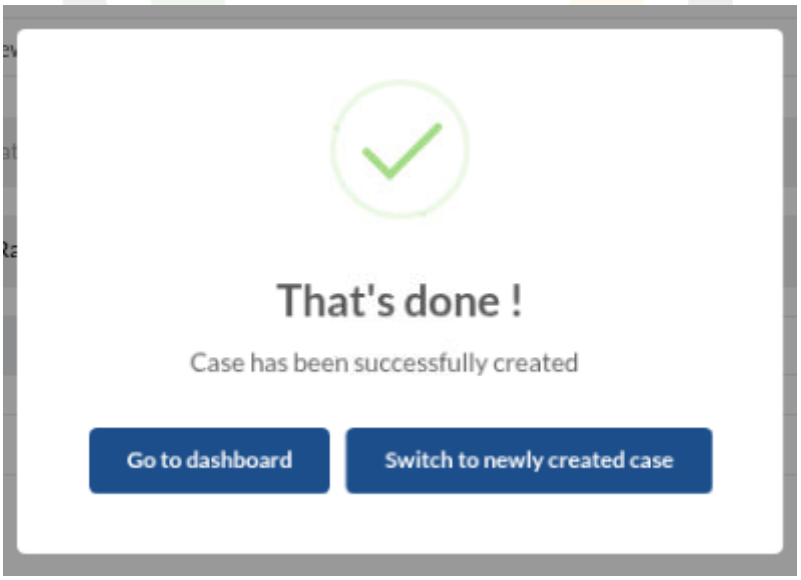
Akan muncul pop up halaman form informasi Case yang akan dibuat. Isi formulir sesuai kebutuhan dan keinginan.



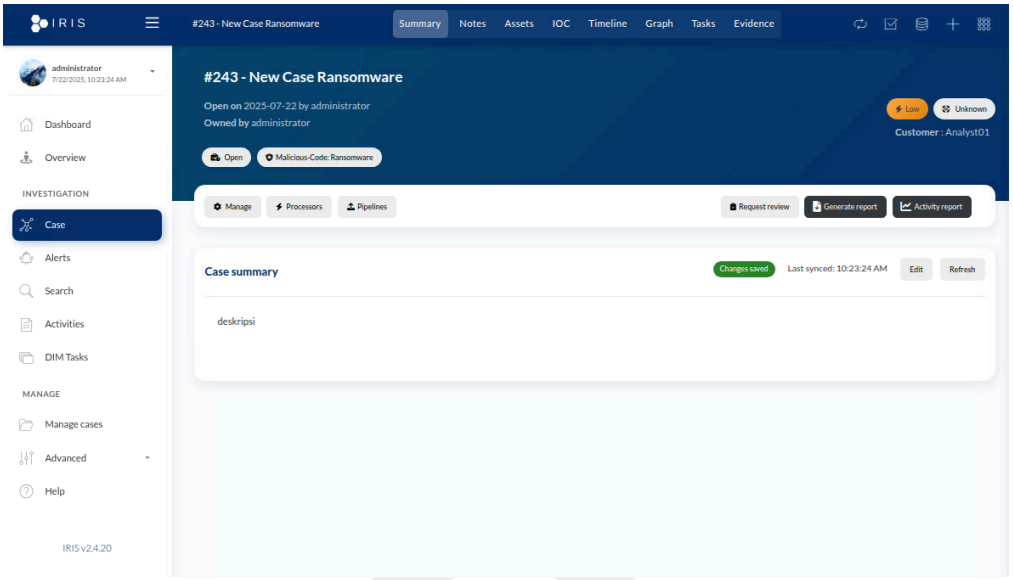
Berikut adalah contoh pengisian form informasi Case.



Akan muncul pesan konfirmasi apabila Case berhasil dibuat.



Berikut adalah halaman Case yang baru dibuat.

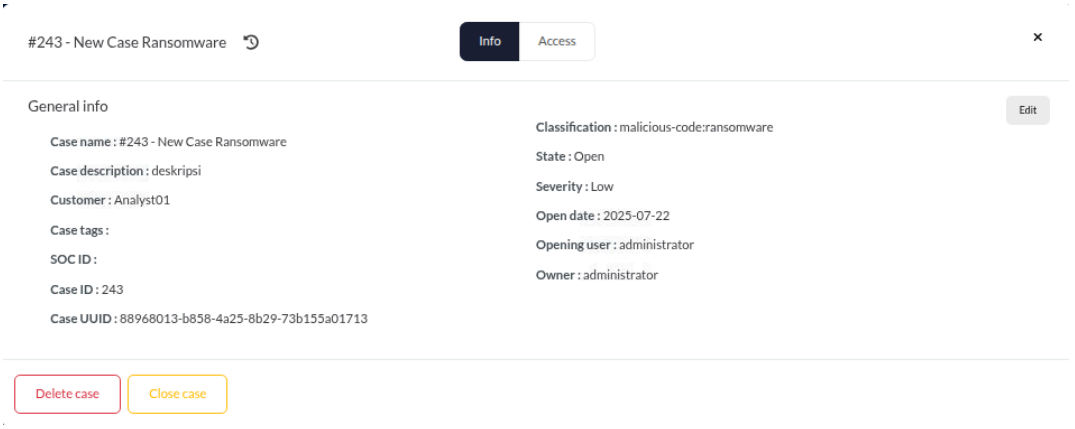


[Case Management] Update and Enrich Case

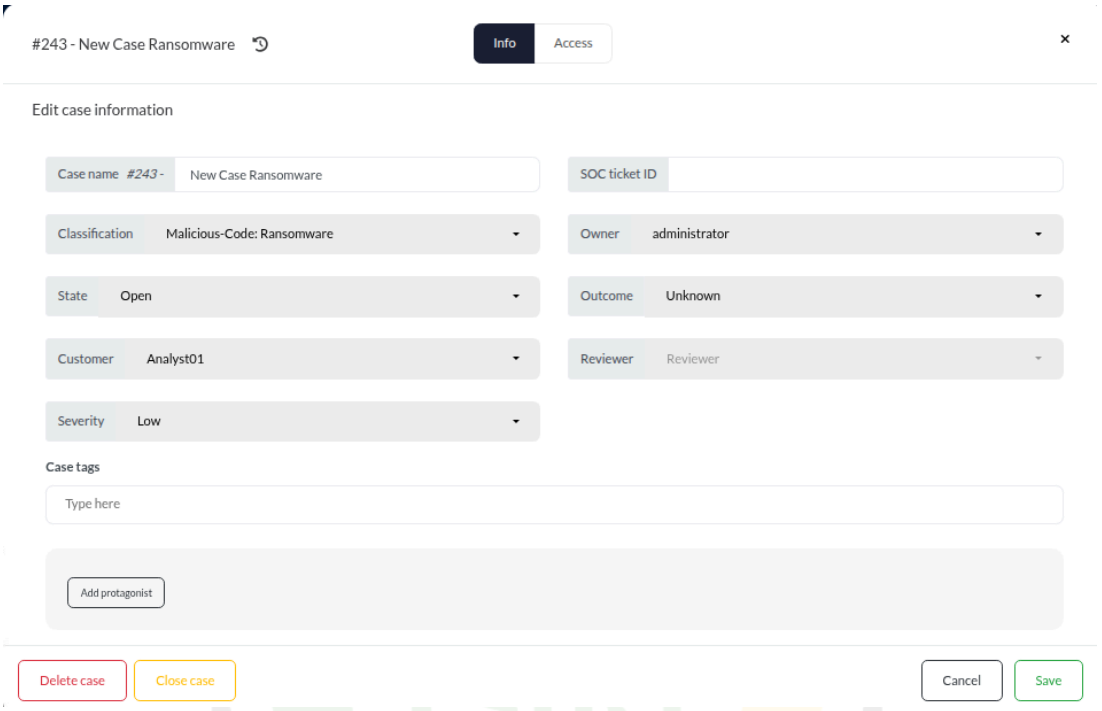
Update Case Information

Pada halaman Case, klik **Manage** pada bagian kiri atas

Akan muncul pop up halaman informasi Case, klik **Edit** pada bagian kanan atas.

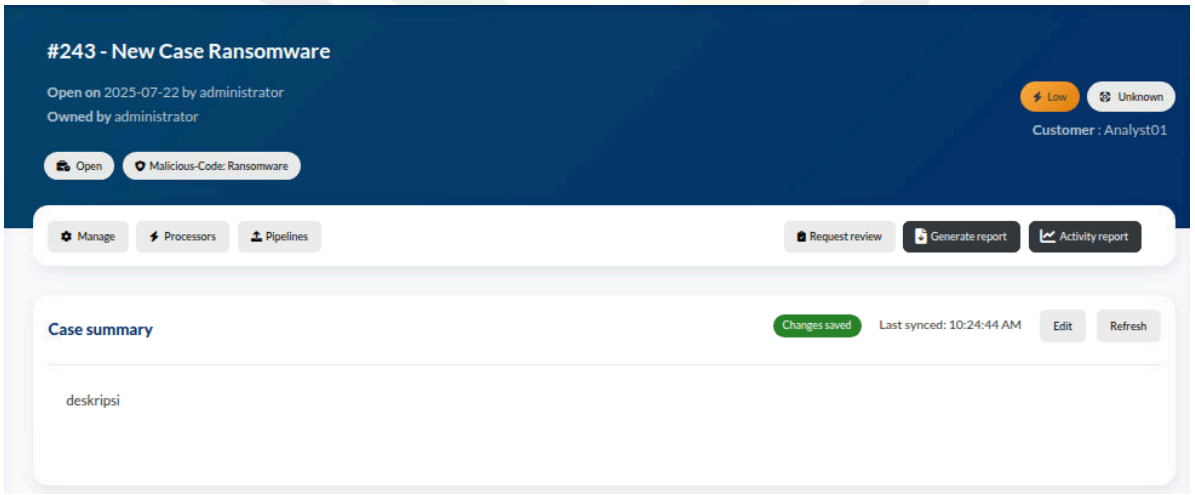


Isi atau Pilih informasi yang ingin diperbarui atau ditambahkan pada Case, seperti Severity, Classification, State, Customer, dll. Klik **Save** apabila ingin mengonfirmasi pembaruan.

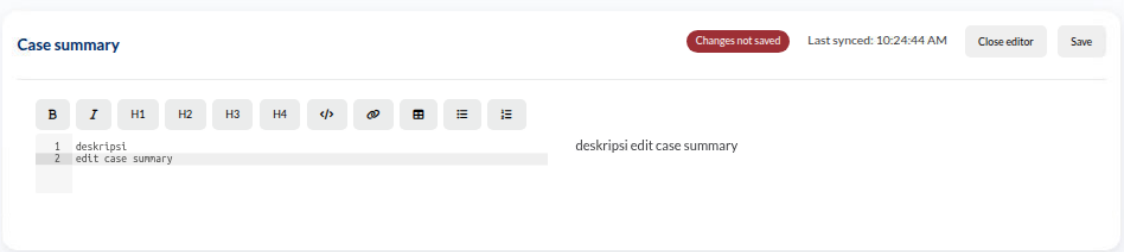


Summary

Pada halaman Case, klik **Edit** pada bagian kanan di panel **Case summary**.



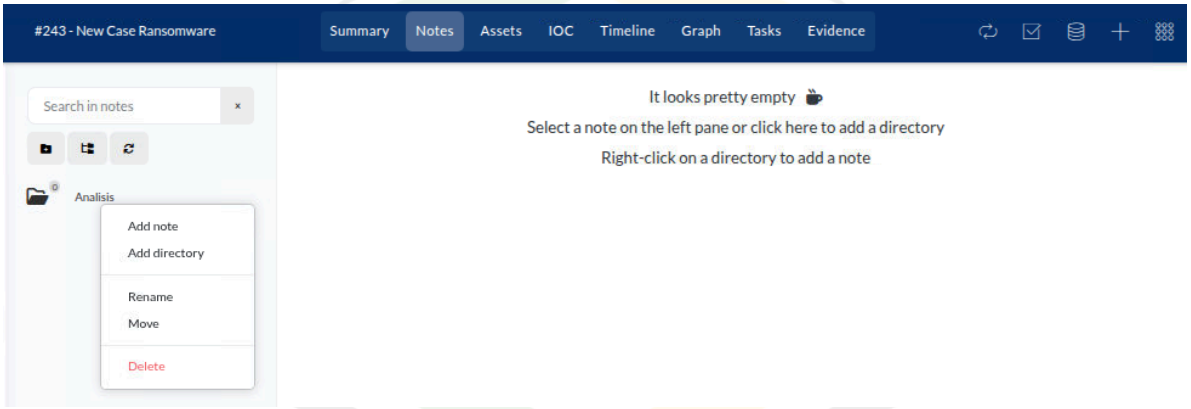
Tuliskan case summary, lalu klik **Save**.



Notes

Pada tab **Notes**, klik kanan pada suatu Folder (cth. **Analisis**) → **Add note**. Note bisa berisi informasi apa saja yang berkaitan dengan Case insiden keamanan siber.

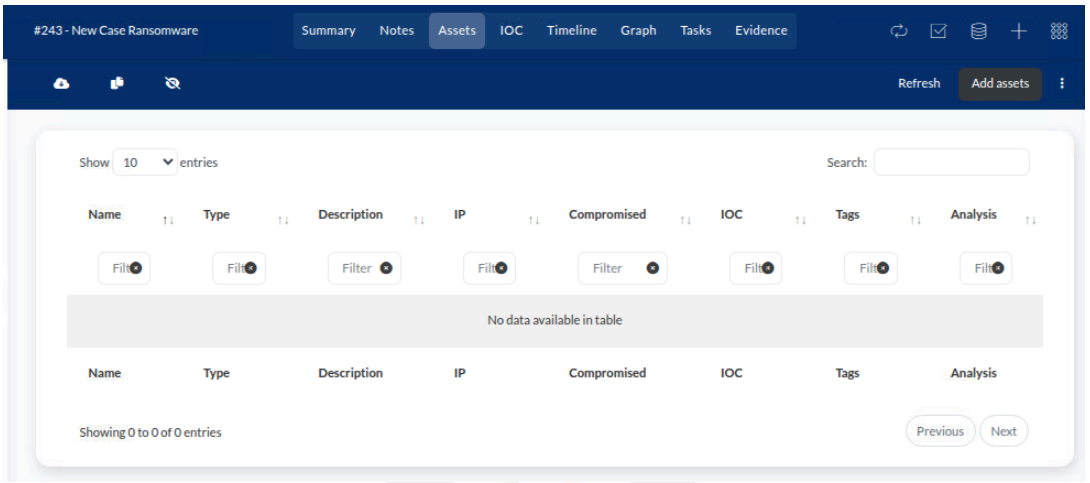
*jika belum ada folder, buat dahulu dengan klik icon Folder di bawah *search bar*.



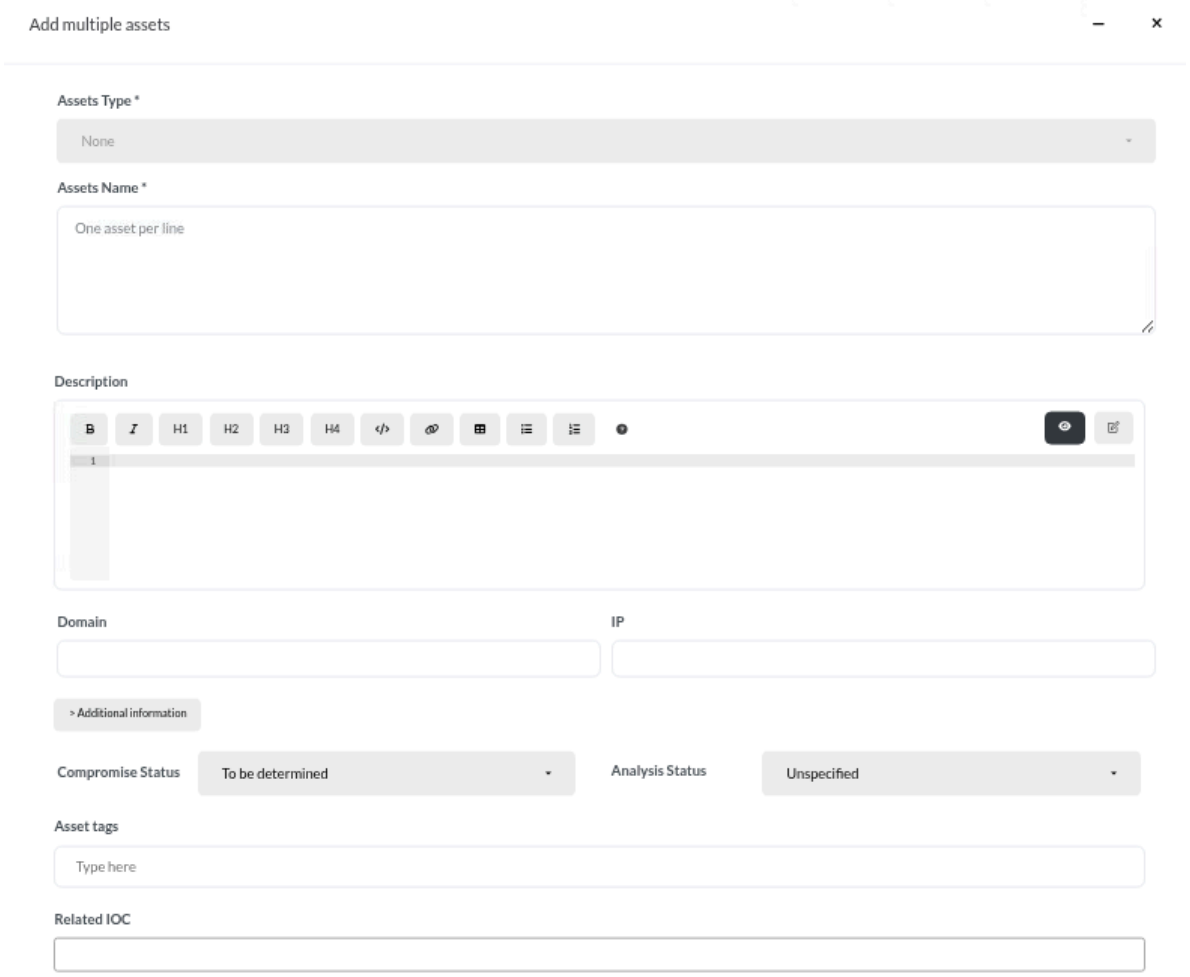
Tuliskan notes, beri nama notes, lalu klik **Save note**.

Assets

Pada tab **Assets**, klik **Add assets** pada bagian kanan atas.



Isi form informasi aset yang ingin ditambahkan, lalu klik **Save**.

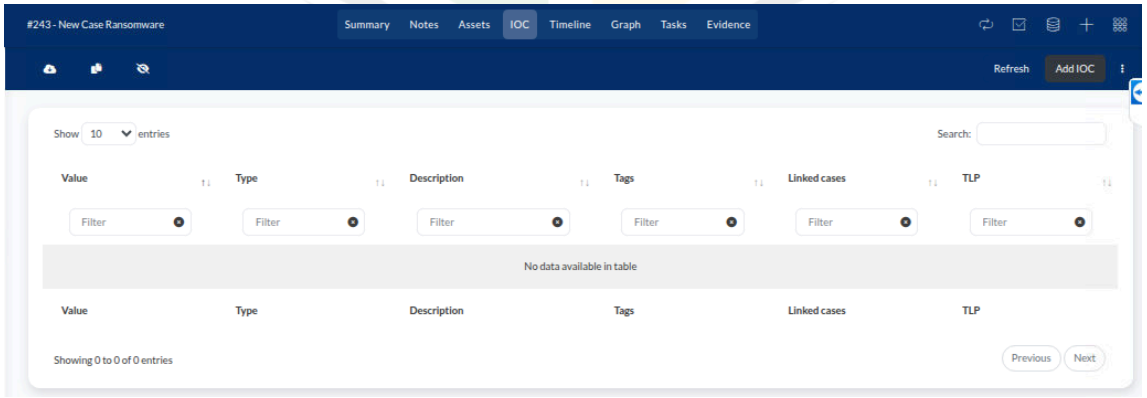


Entitas/Komponen yang dapat dikategorikan dan ditambahkan sebagai Aset pada Case DFIR IRIS diantaranya:

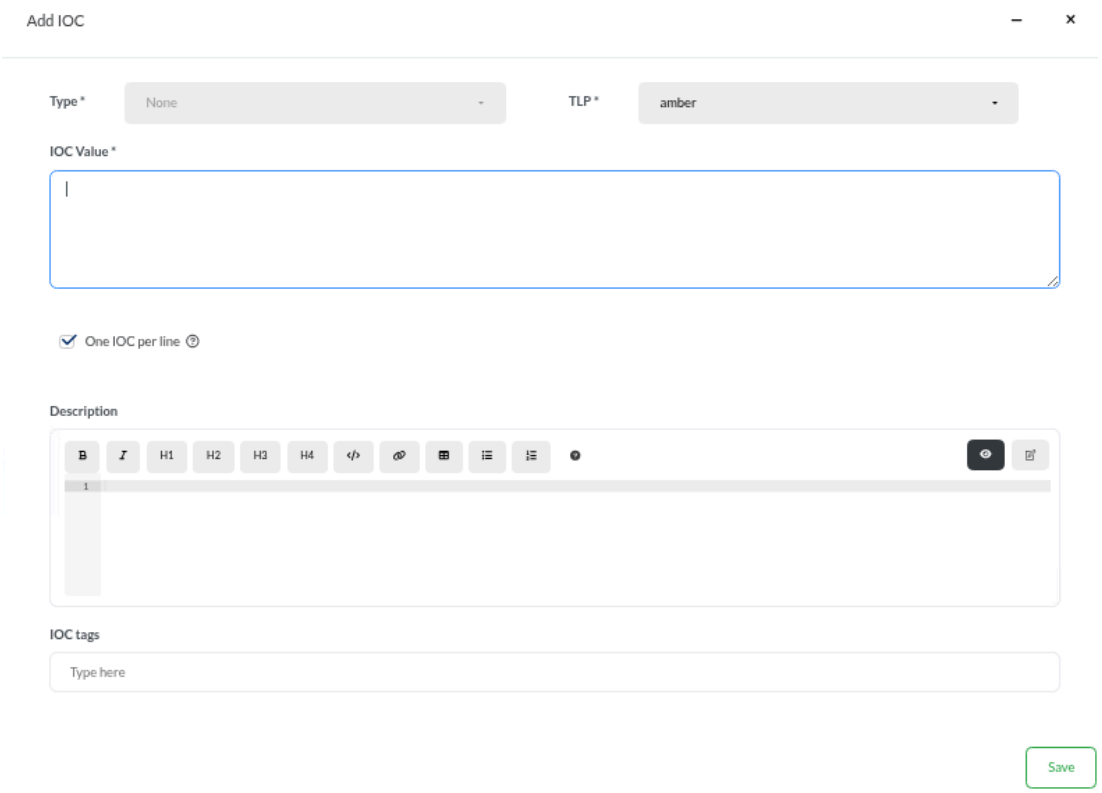
- **Hostname atau Nama Server** – Sistem atau perangkat yang menjadi target atau sumber insiden.
- **Alamat IP** – Alamat IP internal/eksternal yang terlibat dalam aktivitas mencurigakan atau serangan.
- **User Account** – Identitas pengguna yang terlibat atau disalahgunakan dalam insiden (misalnya akun admin yang dikompromi).
- **Email Address** – Alamat email terkait phishing, spoofing, atau komunikasi berbahaya.
- **Domain atau URL** – Nama domain atau URL yang terkait dengan command & control, phishing, atau aktivitas berbahaya lainnya.
- **Perangkat Keras** – Laptop, server fisik, atau perangkat jaringan yang terdampak.
- **Aplikasi atau Sistem Layanan** – Aplikasi atau layanan TI (misalnya Active Directory, VPN, database) yang terkait atau terdampak.
- **UUID atau Device ID** – Identifier unik dari perangkat atau sistem dalam organisasi.

IOC

Pada tab **IOC**, klik **Add IOC** pada bagian kanan atas.



Isi form informasi IOC yang ingin ditambahkan, lalu klik **Save**.

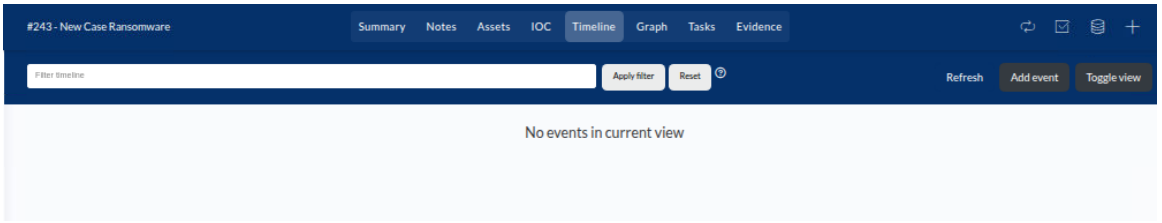


Entitas/Komponen yang dapat dikategorikan dan ditambahkan sebagai IoC (*Indicator of Compromise*) pada Case DFIR IRIS diantaranya:

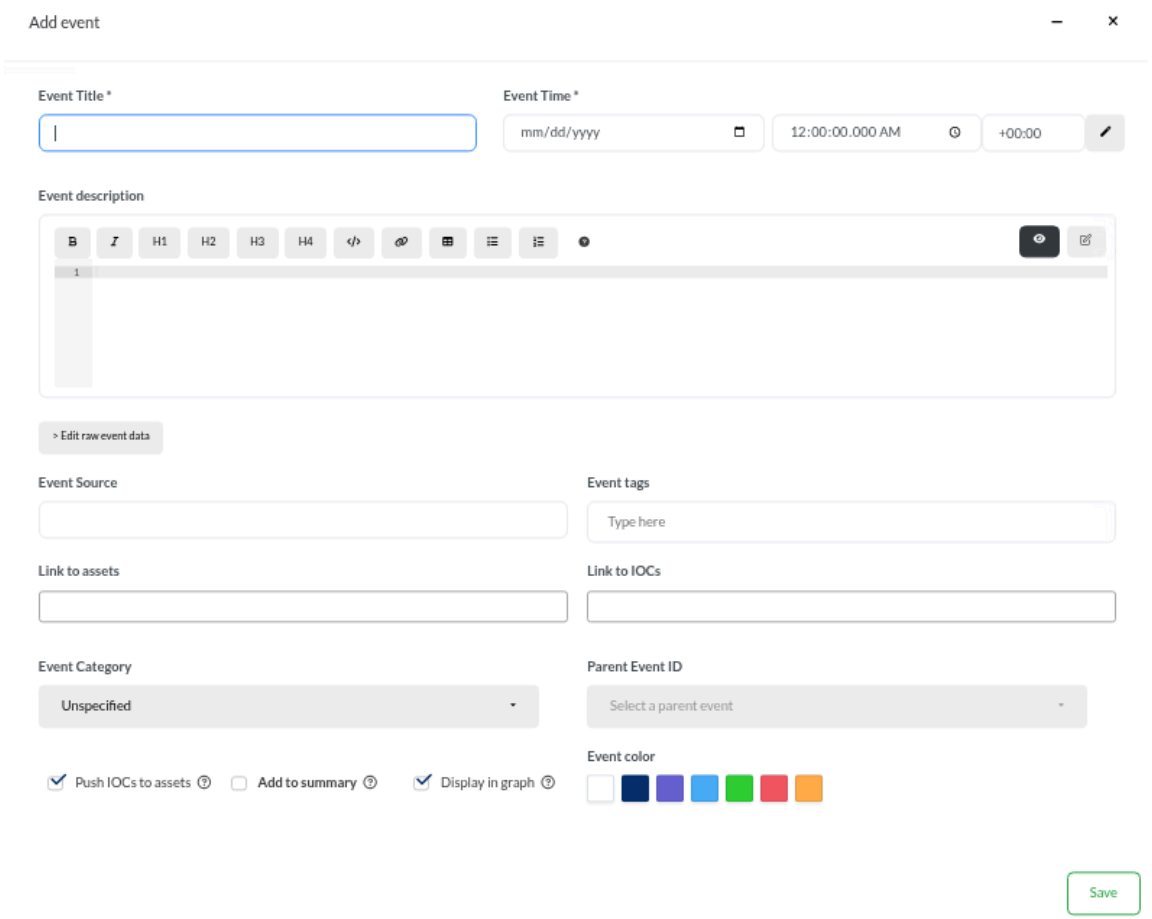
- **Alamat IP berbahaya** – IP yang digunakan oleh attacker untuk C2 (command & control) atau eksploitasi.
- **Domain atau URL mencurigakan** – Sumber phishing, malware download, atau komunikasi outbound tidak sah.
- **Hash file (MD5, SHA1, SHA256)** – Identifikasi unik file berbahaya seperti malware atau script eksploitasi.
- **Nama file atau path** – Lokasi file mencurigakan di sistem yang terinfeksi.
- **Signature antivirus atau YARA rules** – Pola deteksi yang cocok dengan file atau aktivitas berbahaya.
- **Email header atau subject** – Digunakan dalam kasus phishing atau social engineering.
- **Registry keys atau proses mencurigakan** – Pada sistem Windows, bisa menunjukkan persistence atau malware aktif.

Timeline

Pada tab **Timeline**, klik **Add event** pada bagian kanan atas.



Isi form informasi Event yang ingin ditambahkan, lalu klik **Save**.



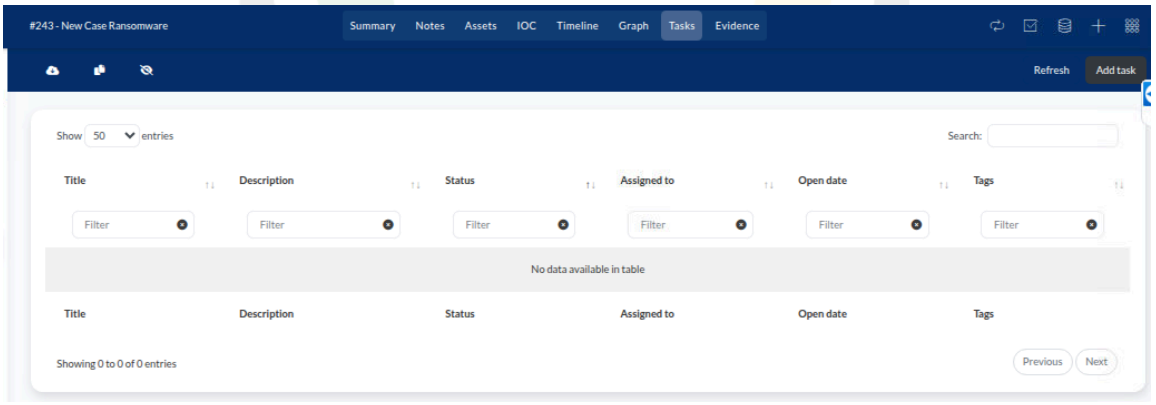
Kolom yang perlu diisi antara lain:

- **Event Title** *(wajib)*: Judul singkat untuk mendeskripsikan event, seperti "Malware Detected" atau "User Disabled".
- **Event Time** *(wajib)*: Tanggal dan waktu terjadinya event. Waktu ini akan digunakan untuk menempatkan event secara kronologis di timeline.
- **Event Description**: Penjelasan rinci mengenai event. Bisa mencakup kronologi, analisis teknis, atau hasil tindakan yang dilakukan.

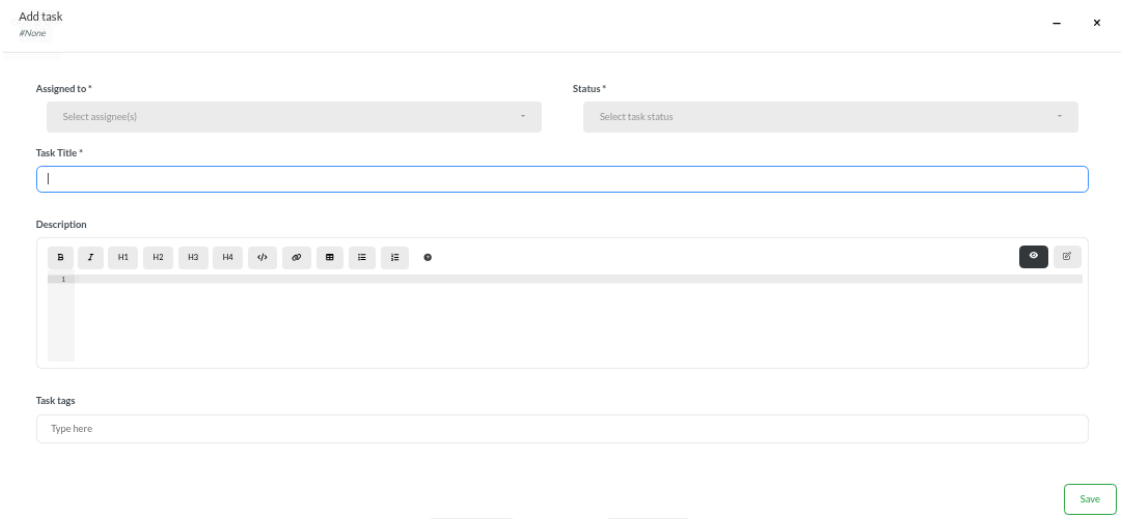
- **Event Source**: Sumber data atau alat yang mendeteksi atau mencatat event, misalnya "Wazuh", "Firewall", atau "Analyst Manual Input".
- **Event Tags**: Label atau kata kunci untuk mengelompokkan atau mempermudah pencarian event serupa, misalnya "initial-access", "remediation".
- **Link to Assets**: Menautkan event ke aset terkait (misalnya IP, hostname, atau perangkat yang terdampak).
- **Link to IOCs**: Menautkan event ke IOC (Indicators of Compromise) yang relevan, seperti hash file, IP, domain, dll.
- **Event Category**: Kategori umum dari event, seperti "Detection", "Response", "Containment", dsb., untuk klasifikasi otomatis.
- **Parent Event ID**: Jika event ini merupakan turunan atau bagian dari event lain, dapat ditautkan ke *parent* untuk membangun struktur naratif.
- **Event Color**: Pilihan warna untuk menandai visualisasi event dalam timeline agar lebih mudah dibedakan antar jenis atau fase insiden.

Tasks

Pada tab **Tasks**, klik **Add task** pada bagian kanan atas.



Isi form informasi Task yang ingin ditambahkan, lalu klik **Save**.

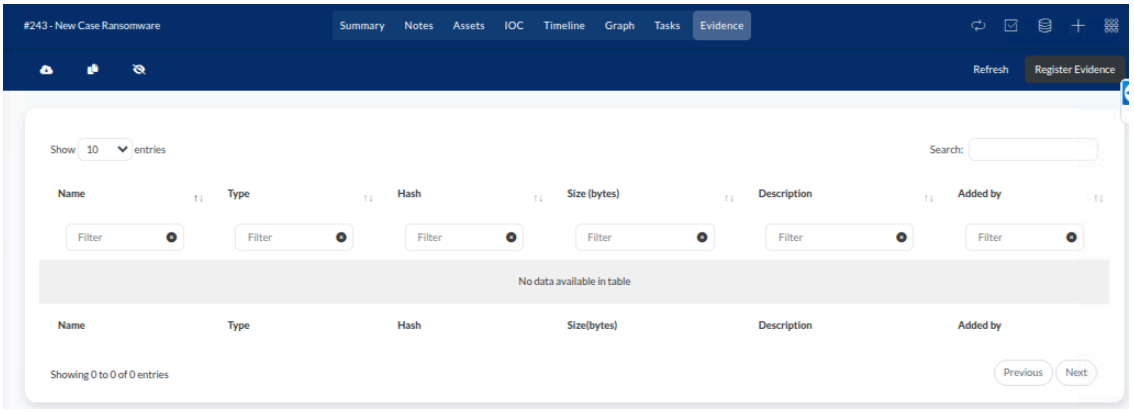


Kolom yang perlu diisi antara lain:

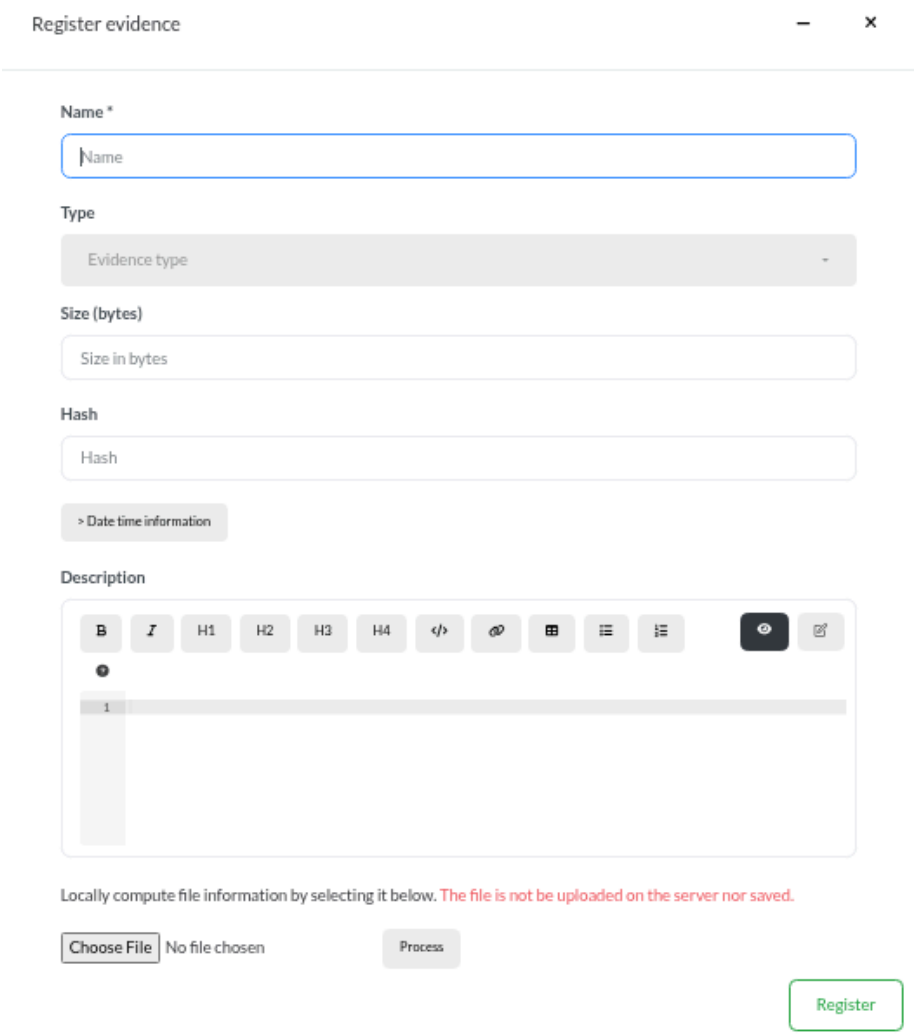
- **Assigned to** *(wajib)*: Pilihan untuk menetapkan siapa (user atau anggota tim) yang bertanggung jawab menjalankan tugas tersebut.
- **Status** *(wajib)*: Menentukan status saat ini dari tugas, seperti *To Do*, *In Progress*, *Blocked*, atau *Done*, untuk memantau progres pengerjaan.
- **Task Title** *(wajib)*: Judul singkat dan jelas dari tugas, contohnya "Analisis malware pada endpoint A" atau "Kumpulkan artefak disk".
- **Description**: Penjelasan rinci mengenai ruang lingkup tugas, instruksi teknis, atau catatan tambahan yang relevan bagi assignee.
- **Task tags**: Label/kata kunci untuk mengelompokkan tugas berdasarkan tema, jenis pekerjaan, atau prioritas (misalnya: "remediation", "triage", "low-priority").

Evidence

Pada tab **Evidence**, klik **Register Evidence** pada bagian kanan atas.



Isi form informasi Register Evidence yang ingin ditambahkan, lalu klik **Save**.

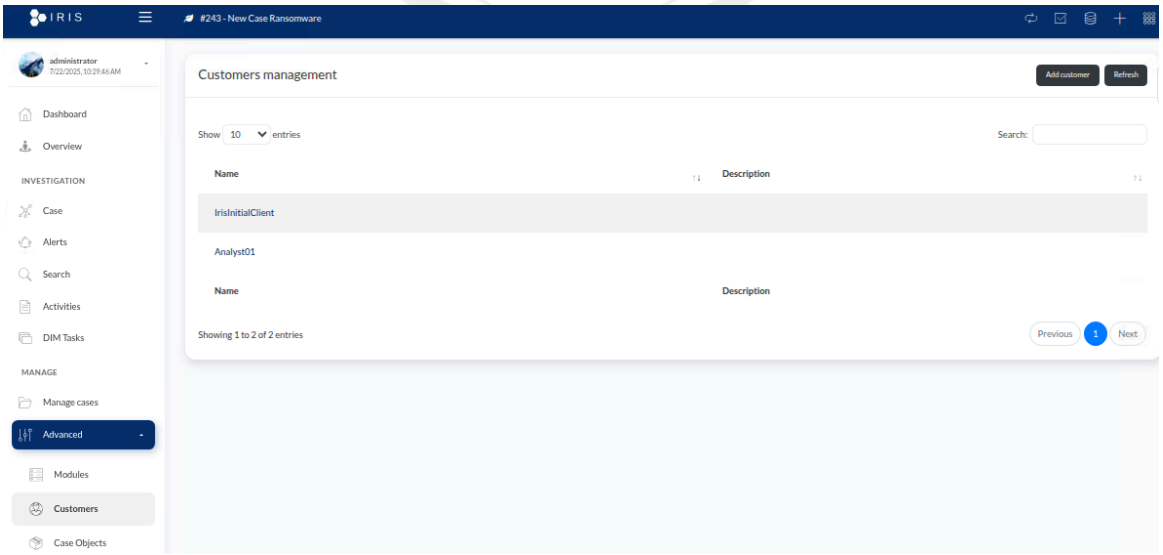


Kolom yang perlu diisi antara lain:

- **Name** *(wajib)*: Nama atau label unik untuk bukti, misalnya “Disk image server A” atau “Email phishing 01”.
- **Type**: Jenis bukti, seperti file log, image disk, dokumen, email, memori dump, dsb. Digunakan untuk klasifikasi.
- **Size (bytes)**: Ukuran file bukti dalam satuan byte, yang membantu dalam validasi integritas.
- **Hash**: Nilai hash (MD5/SHA1/SHA256) dari file bukti untuk memastikan tidak terjadi modifikasi. Hash dapat dihitung otomatis dari file.
- **Date time information**: Opsional, untuk menambahkan informasi waktu terkait bukti (misalnya waktu pengambilan atau penemuan).
- **Description**: Penjelasan mendetail tentang bukti, konteks pengumpulan, dan relevansinya terhadap insiden yang ditangani.
- **Choose File** & **Process**: Tombol ini digunakan untuk memilih file dari sistem lokal dan menghitung nilai hash serta ukurannya. Catatan penting di bawah menyatakan bahwa **file tidak akan diunggah atau disimpan di server**, hanya diproses secara lokal untuk keperluan pencatatan metadata.

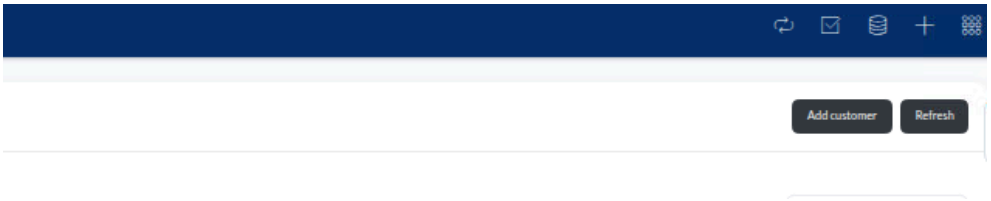
[Customer Management] Add and Delete Customer

Pada panel sebelah kiri, masuk ke halaman **Advanced** → **Customer**. Halaman ini menampilkan daftar customer yang ada.

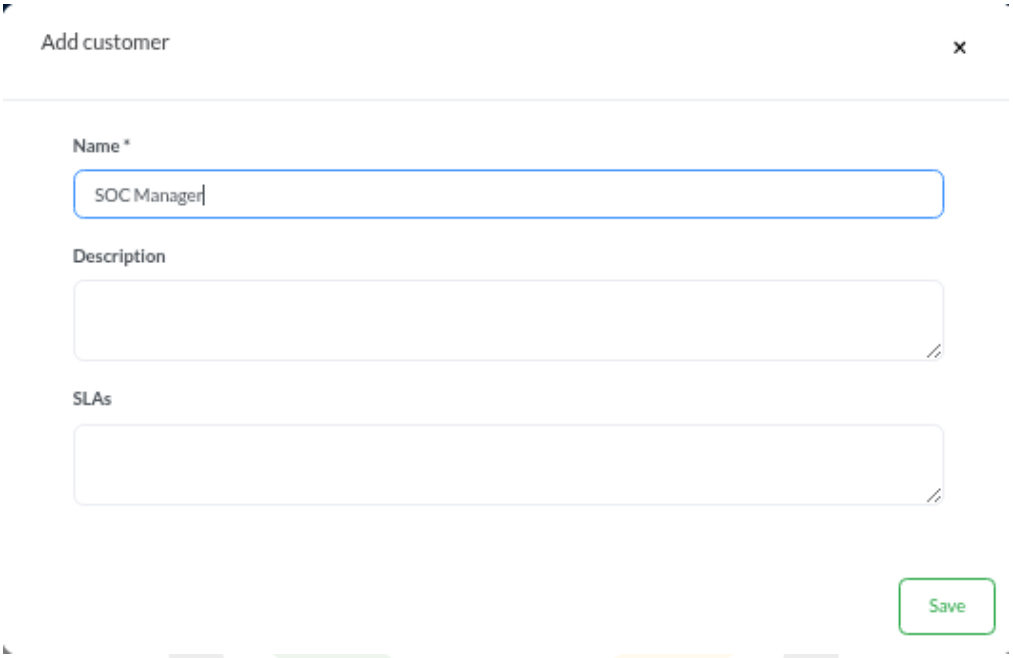


Add Customer

Untuk menambahkan *customer*, klik **Add customer** pada bagian kanan atas.

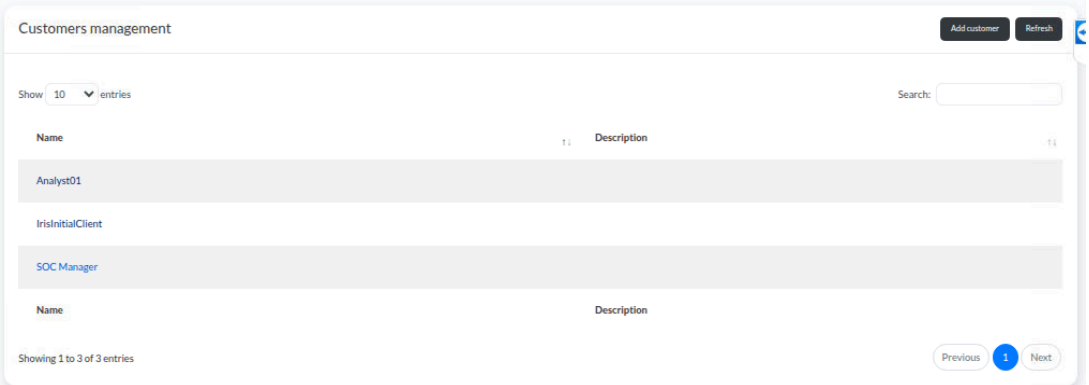


Isi form informasi Customer yang akan ditambahkan, lalu klik **Save**.

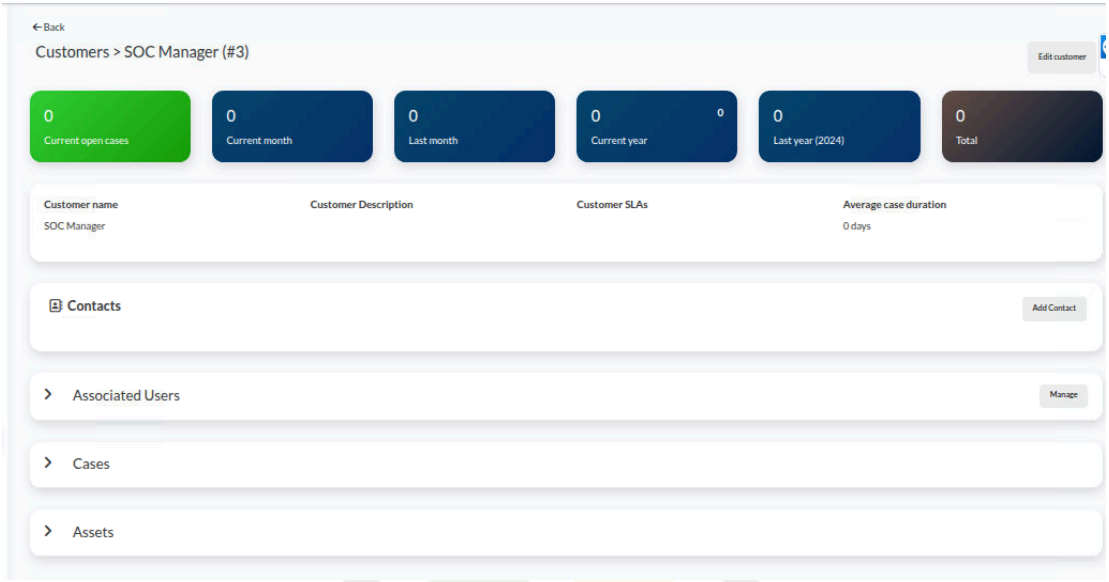


Edit & Delete Customer

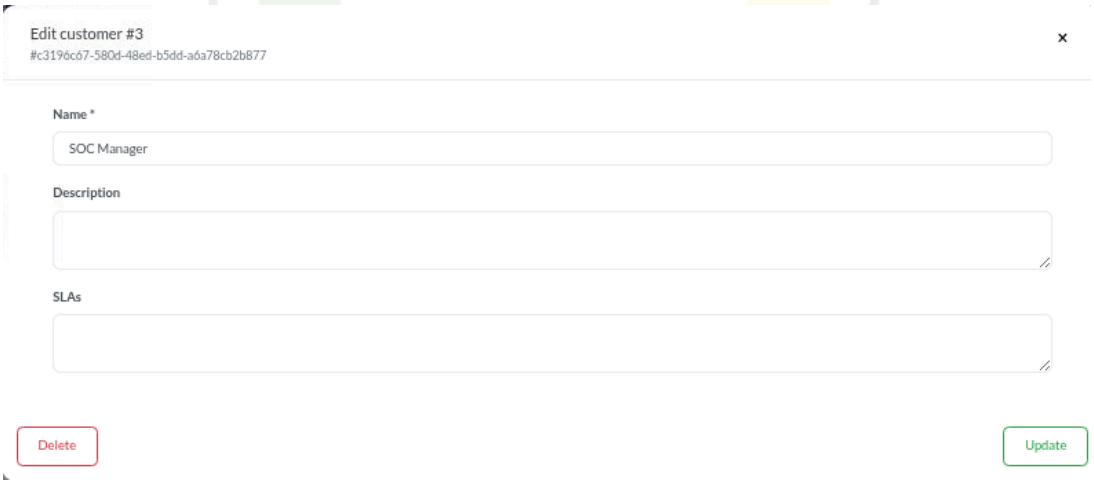
Klik pada **Nama Customer** yang ingin diedit/dihapus (cth. SOC Manager).



Akan diarahkan ke halaman Customer yang berisi informasi terkait aktivitas Customer. Klik **Edit customer** pada bagian kanan atas.

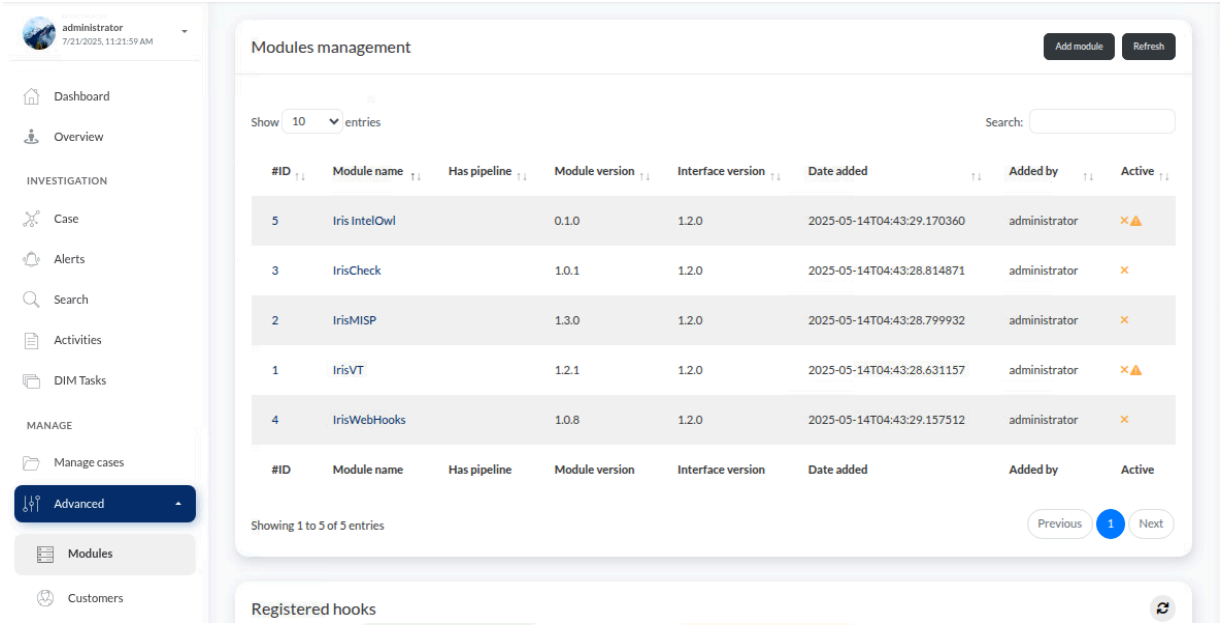


Sesuaikan form informasi customer, klik **Update** bila ingin menerapkan perubahan. Namun apabila ingin menghapus Customer, klik **Delete**.

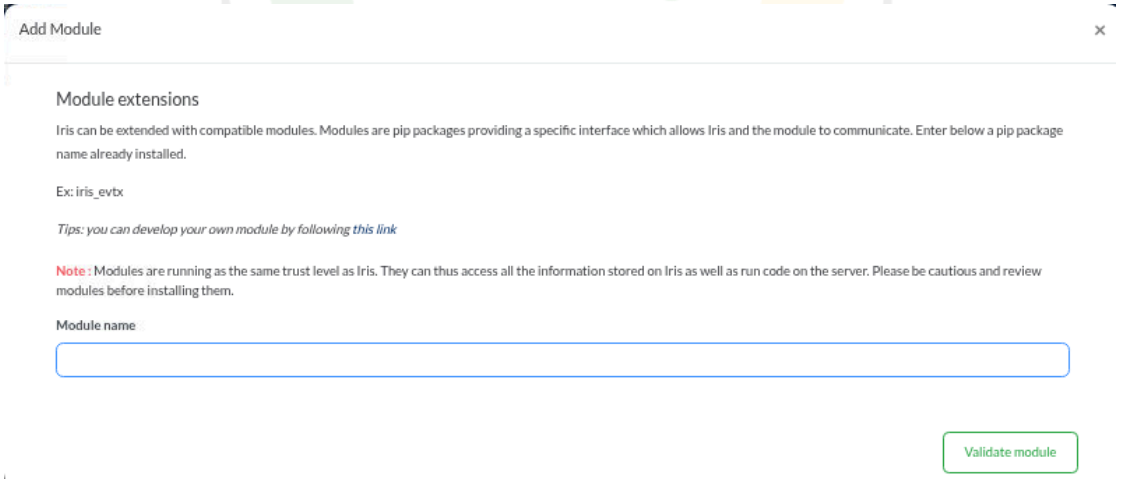


[Modules Management] Add Module

Pada halaman **Modules**, klik **Add module** pada bagian kanan atas.



Akan muncul halaman Module Extension berikut.



Masukkan nama modul pada kolom **"Module name"**.

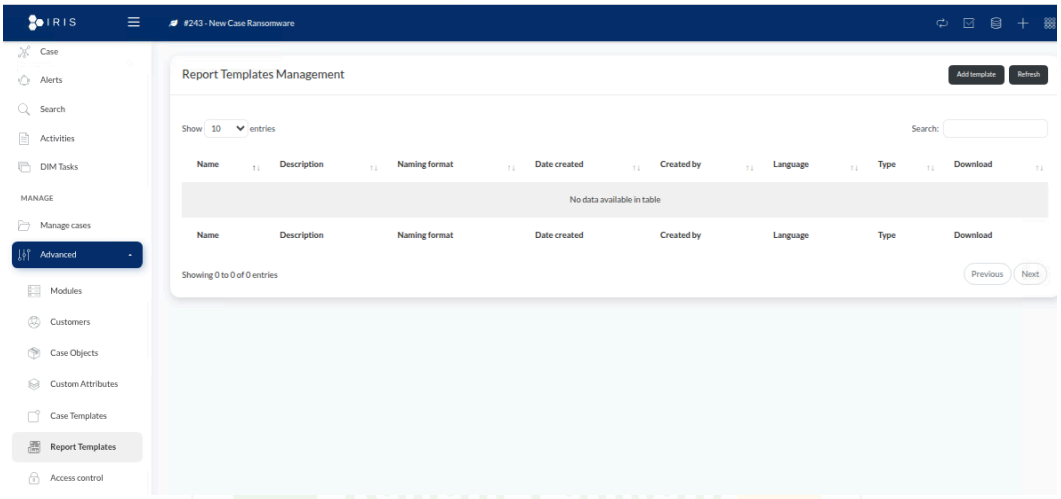
- Contoh: `iris_evtx` (untuk parsing log EVTX), atau modul lain yang sesuai.
- Modul tersebut **harus sudah diinstal** di lingkungan Python IRIS terlebih dahulu.

Klik tombol "Validate module" untuk memverifikasi bahwa modul valid, kompatibel, dan dapat dihubungkan dengan sistem IRIS.

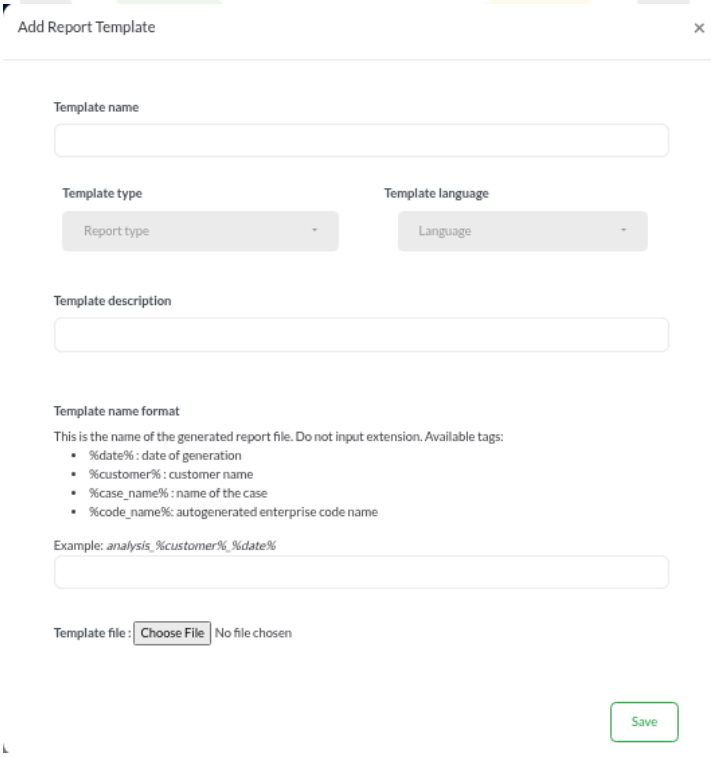
[Report Management] Generate Incident Report

Add Template

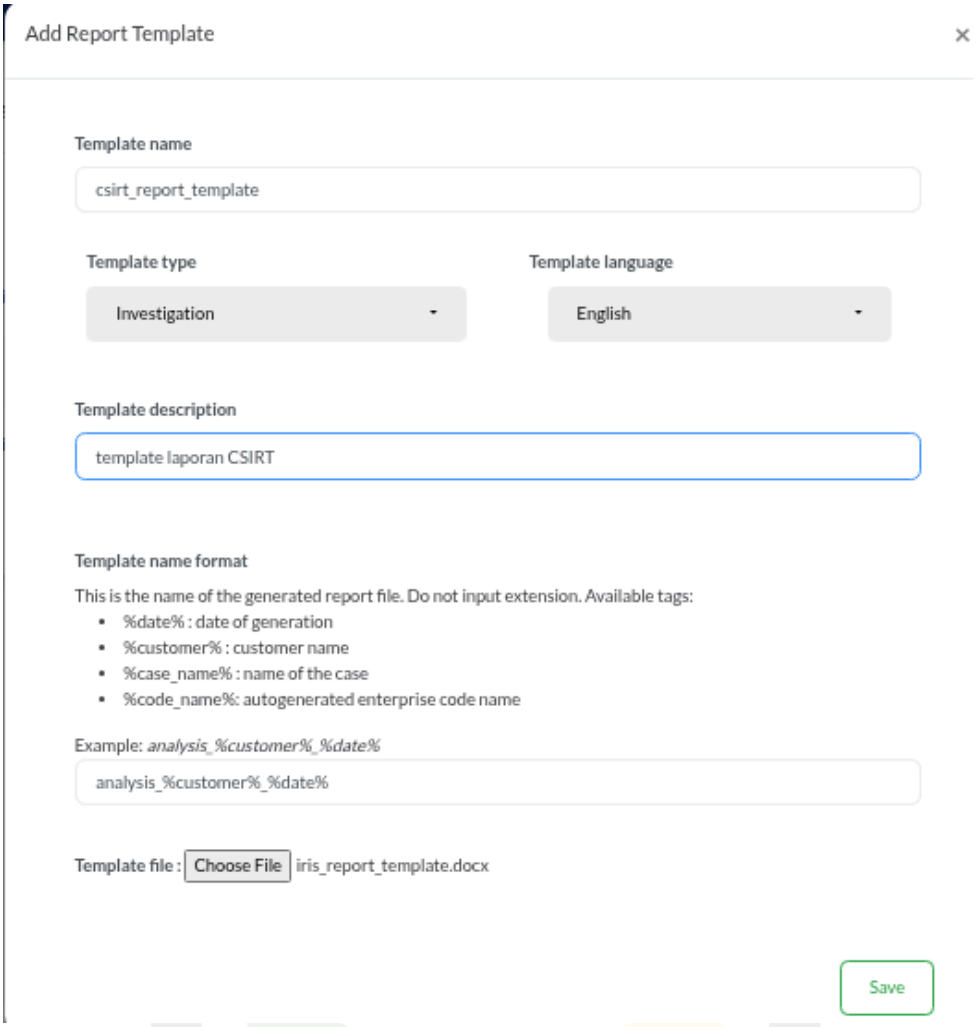
Secara bawaan, DFIR IRIS tidak memiliki default template report, sehingga perlu dilakukan pengunggahan format dokumen laporan ke platform. Namun DFIR IRIS telah menyediakan format dokumen di situs dokumentasinya dan dapat digunakan pada platform.



Isi form pengunggahan Template Report seperti Template name, Template type, Template language, Template description, Template name format, dan Template file.

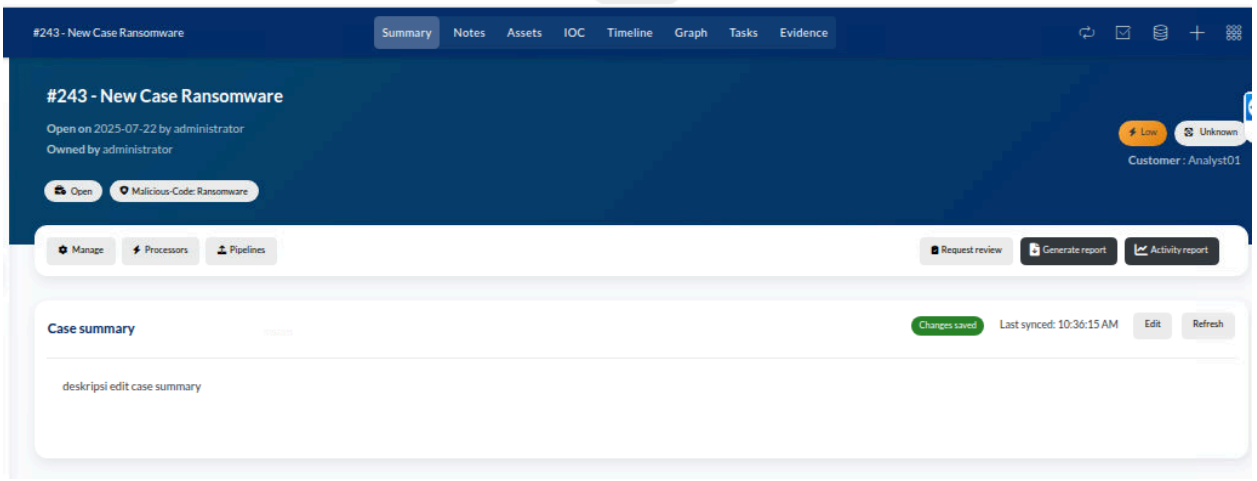


Berikut contoh pengisian form pengunggahan Template Report. Klik **Save**.

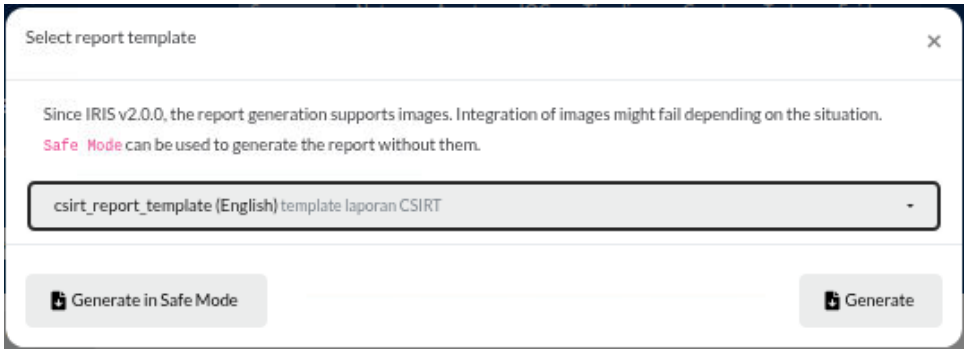


Generate Report

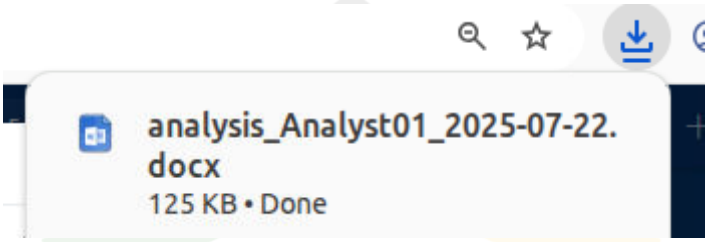
Setelah berhasil mengunggah template, lakukan pembuatan laporan. Pada halaman Case, klik **Generate report** pada bagian kanan atas.



Pilih template report yang akan digunakan.



Report akan otomatis terunduh dengan ekstensi .docx

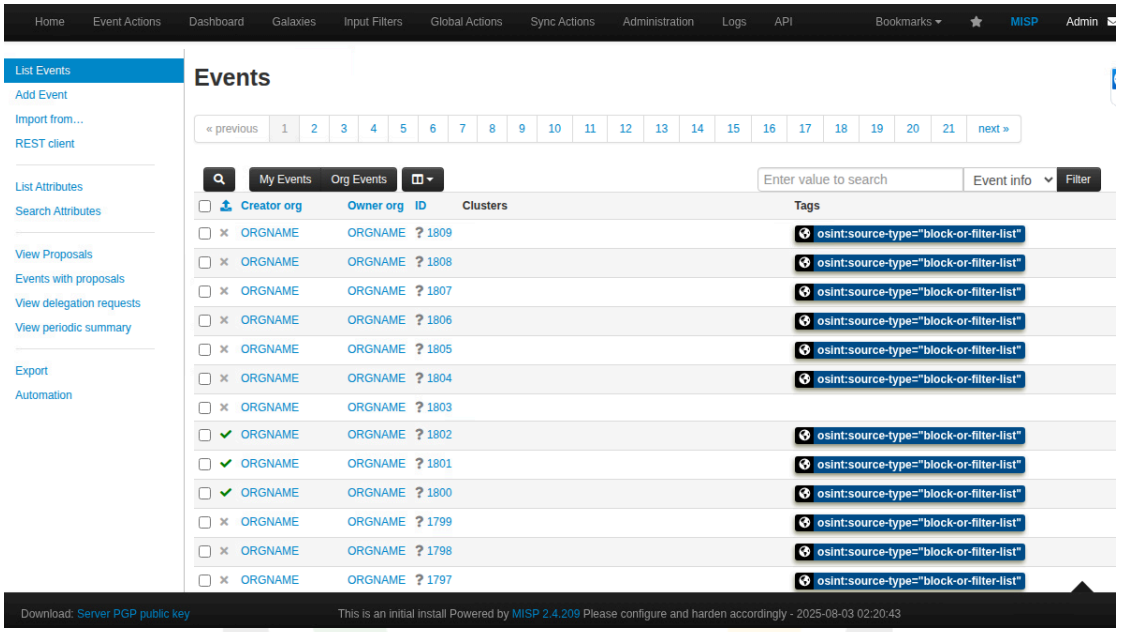


Dokumentasi Resmi

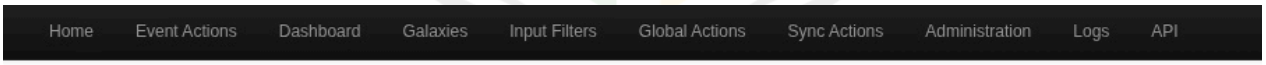
https://docs.dfir-iris.org/latest/

MISP

MISP (Malware Information Sharing Platform) adalah platform open-source untuk mengelola dan berbagi informasi ancaman siber secara terstruktur. MISP memfasilitasi kolaborasi antar organisasi dengan menyimpan indikator ancaman (seperti IP, domain, hash), mendukung visualisasi, tagging, dan integrasi otomatis guna meningkatkan deteksi dan respons terhadap serangan.

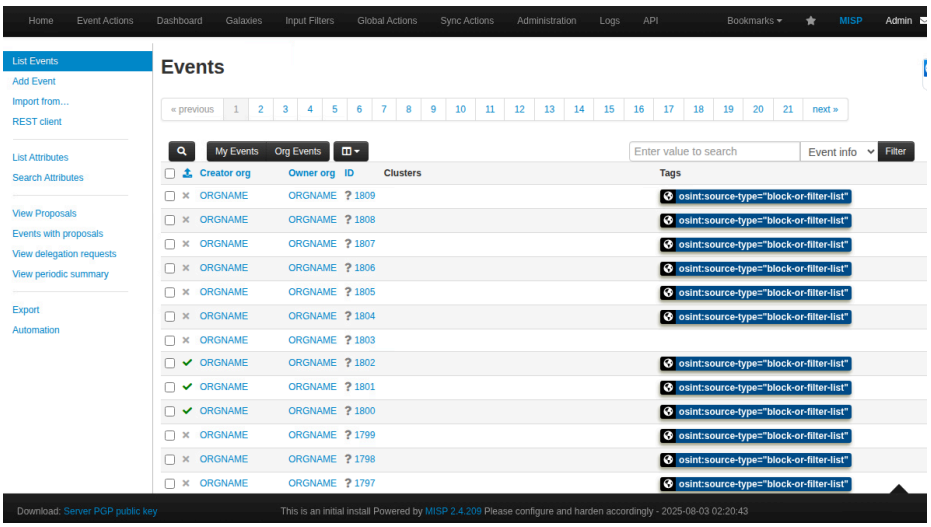


Fitur



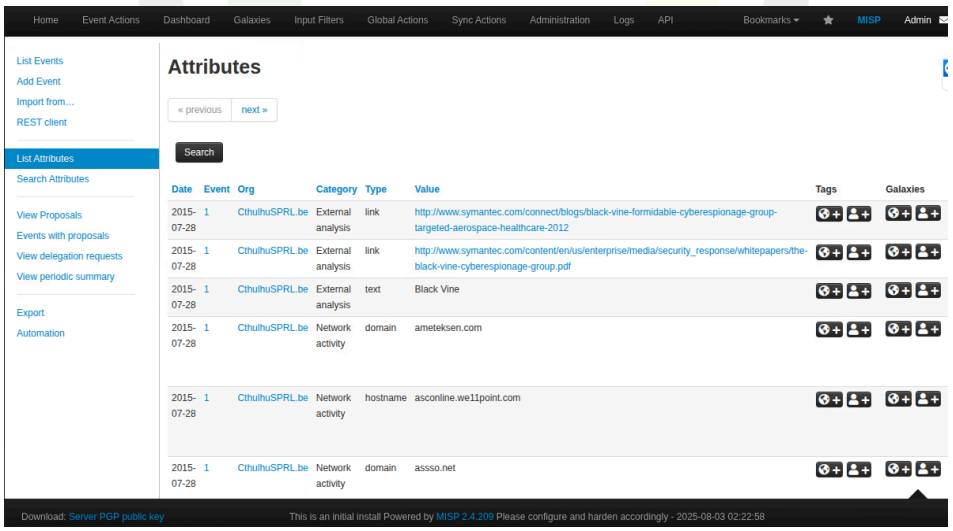
Events

Fitur Events adalah jantung dari MISP. Di sinilah semua informasi ancaman (threat intelligence) dikumpulkan, dikelola, dan dibagikan. Pengguna membuat event baru untuk setiap insiden atau kampanye serangan, lalu menambahkan berbagai atribut (seperti IP, domain, hash, URL, file info) yang terkait. Events juga dapat ditandai dengan threat level, TLP, dan taksonomi lain. Fitur ini penting karena menjadi wadah utama untuk mengkonsolidasikan dan menyusun informasi intelijen. Fitur ini berada di halaman **Event Actions**.



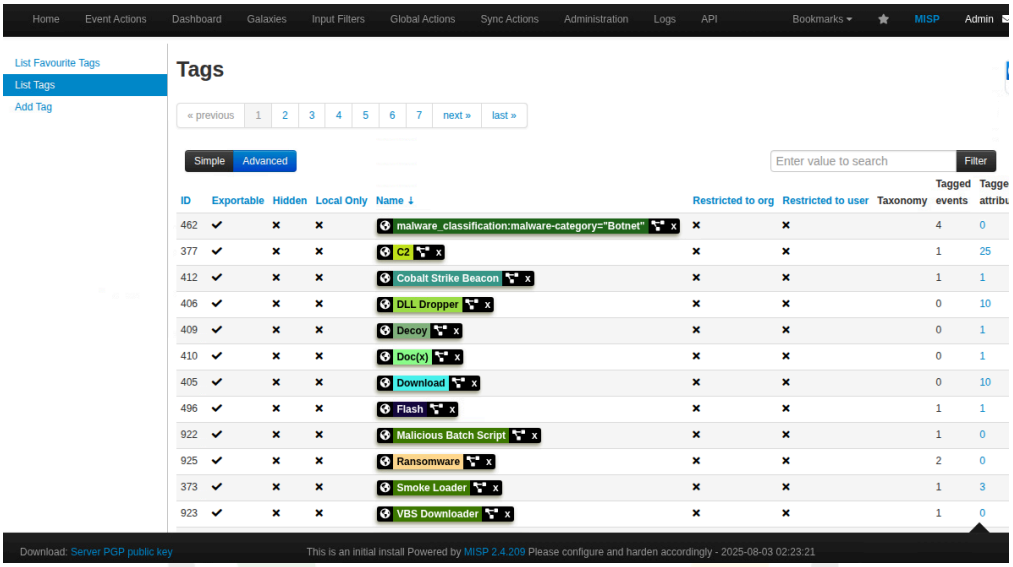
Attributes

Attributes adalah elemen-elemen data detail (Indicators of Compromise/IoCs) yang terhubung dengan suatu event. Halaman Attributes memungkinkan pengguna melihat seluruh indikator dalam sistem secara terpusat dan cepat mencari nilai spesifik seperti hash file, IP address, atau domain. Ini sangat penting dalam operasi tim keamanan seperti analyst, responder, atau threat hunter yang ingin mengecek apakah suatu artefak sudah diketahui sistem. Fitur ini berada di halaman **Event Actions**.



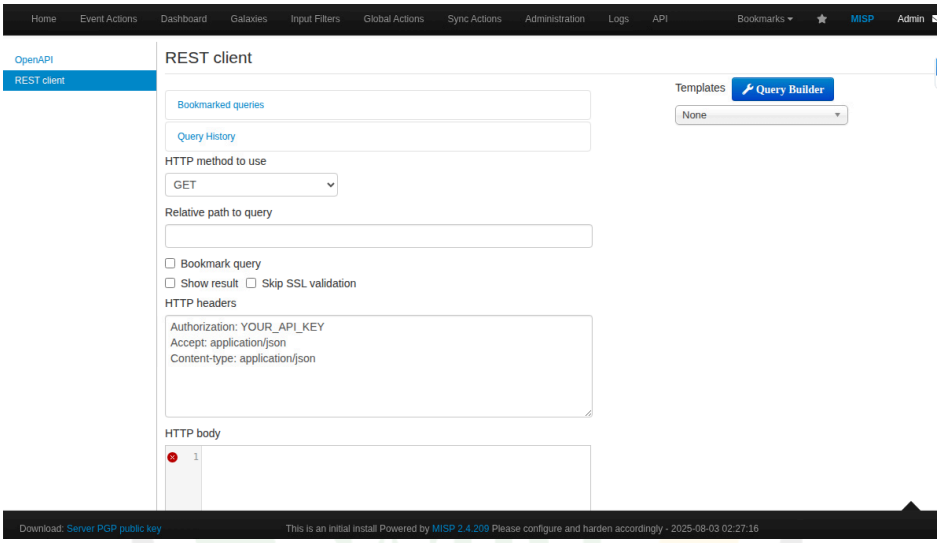
Tags

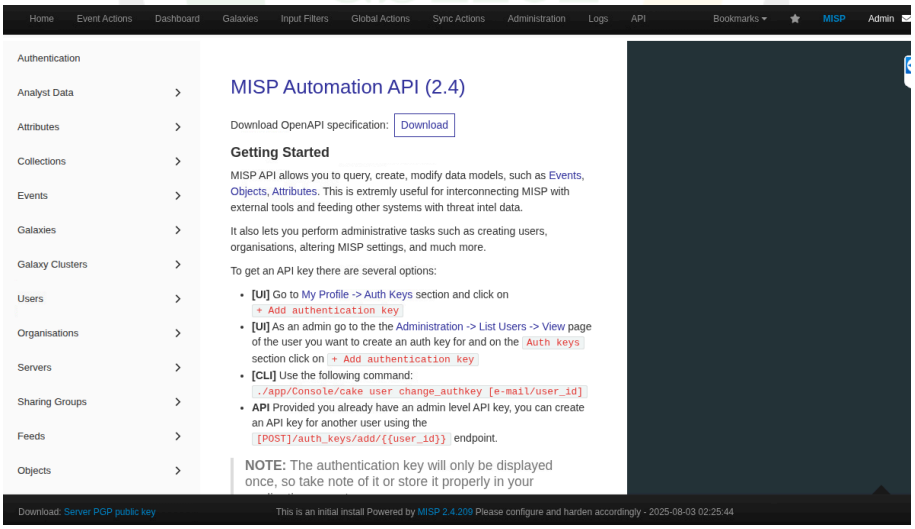
Fitur Tags digunakan untuk memberi label klasifikasi pada event dan atribut, seperti TLP (Traffic Light Protocol), malware type, threat actor, atau mitre tactic. Tag sangat penting untuk mengatur visibilitas data, menyaring hasil pencarian, dan mengatur distribusi informasi ke pihak lain. Tanpa tagging, intelijen akan menjadi tidak terstruktur dan sulit dianalisis secara efektif. Fitur ini berada di halaman **Event Actions**.



API

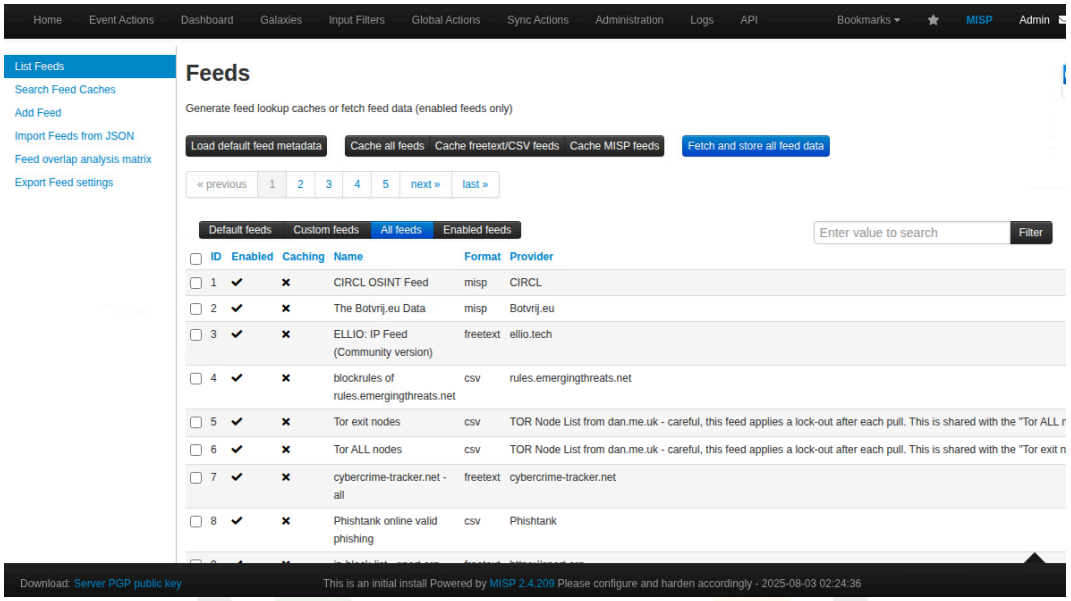
MISP mendukung REST API dan OpenAPI (Swagger) untuk integrasi otomatis dengan sistem lain seperti SIEM atau SOAR. API ini memungkinkan akses penuh ke event, atribut, tagging, dan manajemen pengguna secara programatik, serta menyediakan dokumentasi interaktif langsung di web MISP untuk memudahkan pengujian dan integrasi.





Feeds

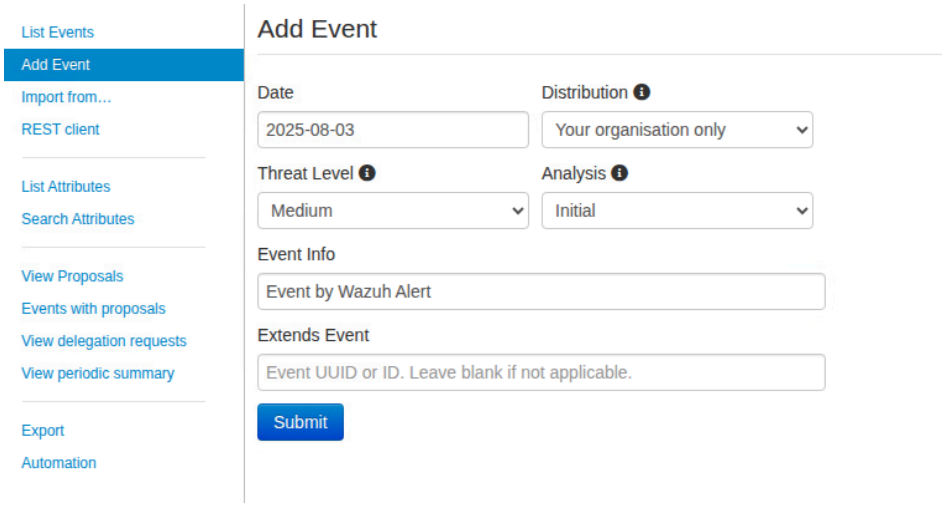
Feeds memungkinkan MISP mengambil data ancaman secara otomatis dari berbagai sumber publik atau komunitas. Dengan mengaktifkan feeds, organisasi dapat terus mendapatkan update IoC dari sumber tepercaya (misalnya CIRCL OSINT, abuse.ch, dll) tanpa perlu input manual. Ini penting untuk menjaga intelijen tetap terkini dan memperkuat pertahanan proaktif. Fitur ini berada pada halaman **Sync Actions**.



Fungsi

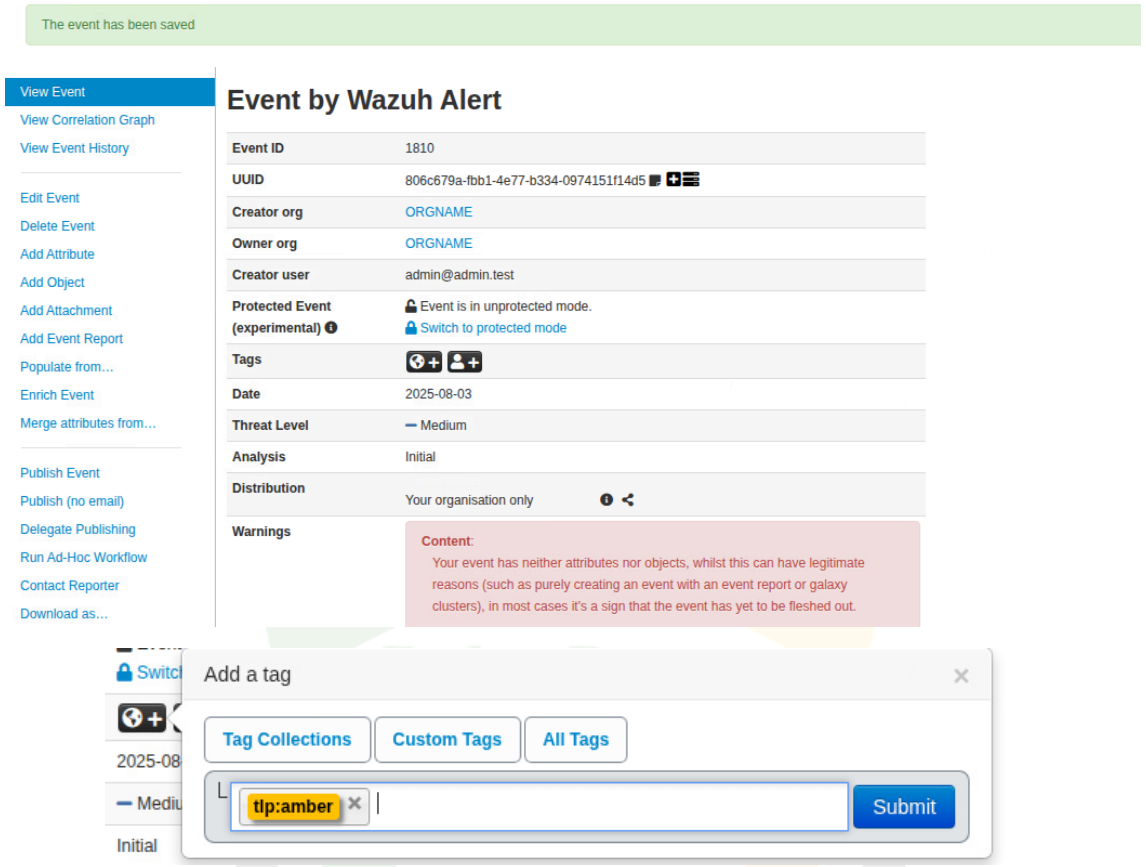
Add MISP Events

Masuk ke **Events Actions** → **Add Events,** lalu isi metadata terkait event yang akan ditambahkan. Klik **Submit**.



Add Tags to Events

Setelah Event terbuat, akan muncul tampilan seperti di bawah, pilih icon **"+"** pada baris **Tags** untuk menambahkan Tags.

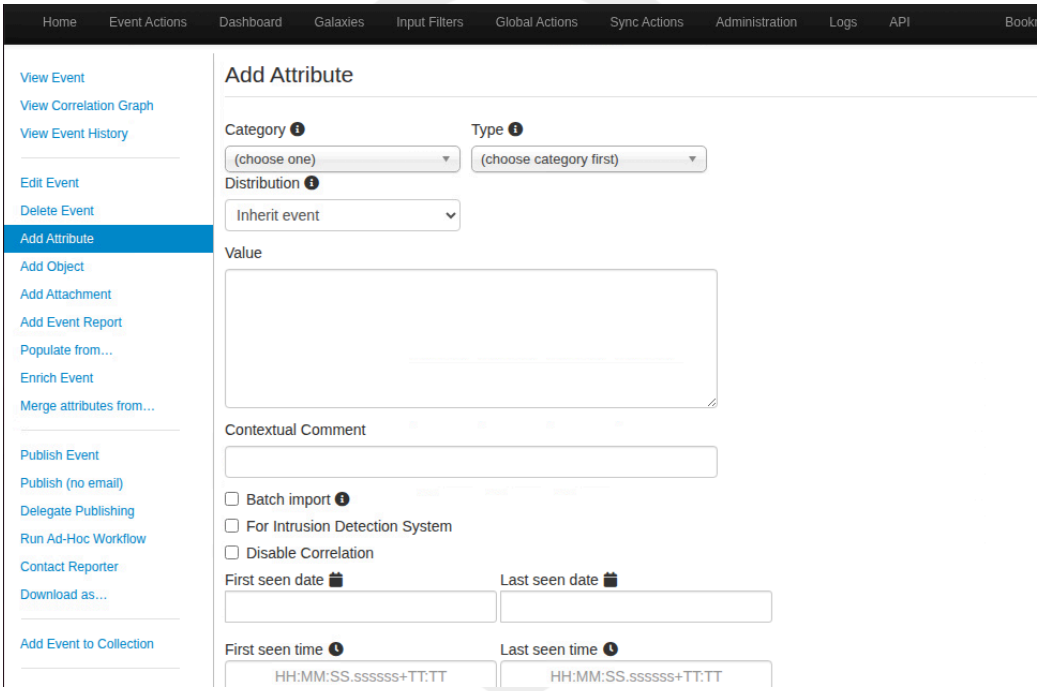


Add Attributes to Events

Attribut dapat berupa alamat IP, domain, filehash, atau data lain. Pada panel sebelah kiri, pilih **Add Attributes**. Isi form penambahan atribut sesuai konteks atribut yang ditambahkan. Lalu klik **Submit**.

- **Category**: Kategori atribut (misalnya: Network activity, Payload delivery, External analysis).
- **Type**: Jenis data yang dimasukkan (misalnya: ip-src, domain, sha256, url). Opsi ini tergantung kategori yang dipilih.
- **Distribution**: Pengaturan visibilitas data (Inherit event, This community only, etc).
- **Value**: Isi utama dari atribut, contohnya IP `8.8.8.8`, domain `example.com`, atau file hash.

- **Contextual Comment**: Catatan atau konteks tambahan terkait atribut tersebut.
- **Batch import**: Untuk menambahkan beberapa atribut sekaligus dalam satu form.
- **For Intrusion Detection System**: Tandai agar atribut ini diekspor sebagai rule IDS (misalnya Suricata/Snort).
- **Disable Correlation**: Nonaktifkan korelasi otomatis antara atribut ini dan atribut lain di MISP.
- **First seen date/time** dan **Last seen date/time**: Waktu pertama dan terakhir atribut ini diamati dalam sistem atau jaringan. Berguna untuk analisis temporal dan korelasi.

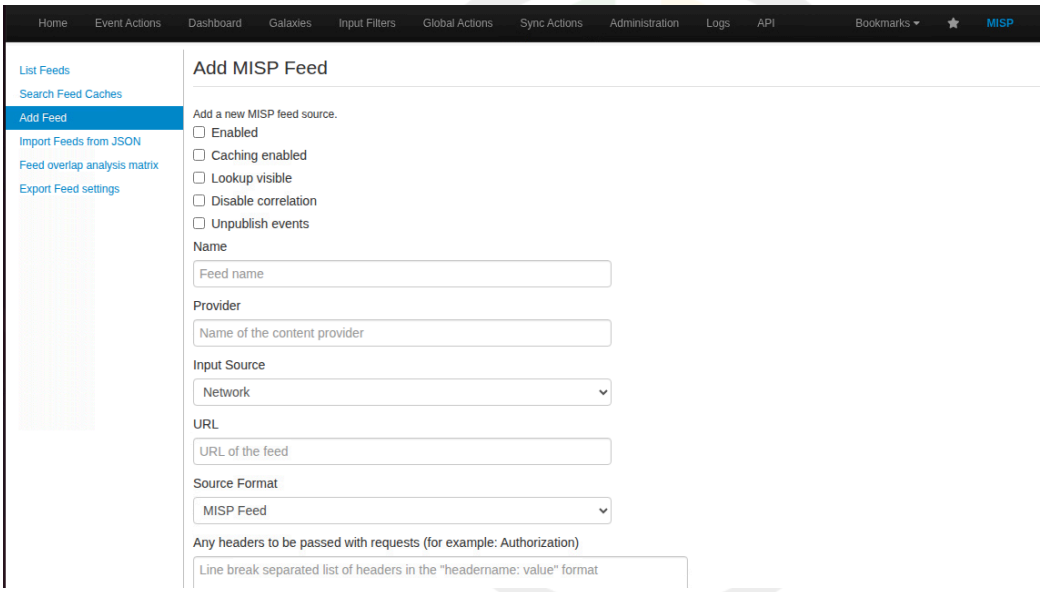


Add Threat Feed

Buka halaman **Sync Actions** → **Feed** → **Add Feed**. Isi form penambahan Feed sesuai konteks Feed yang ingin ditambahkan.

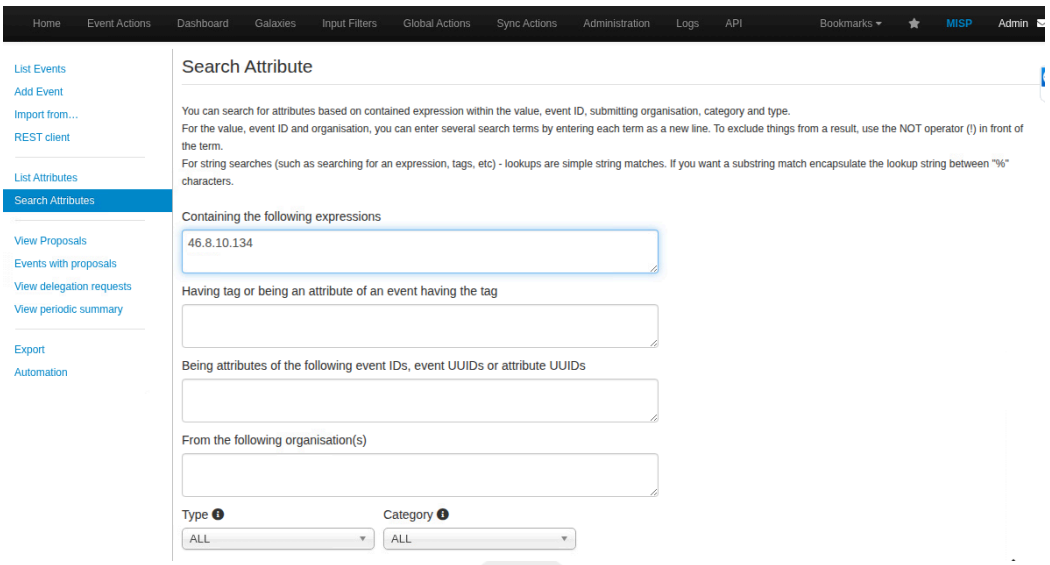
- **Enabled**: Mengaktifkan feed agar dapat digunakan.
- **Caching enabled:** Menyimpan data feed secara lokal untuk akses cepat.
- **Lookup visible:** Memungkinkan feed digunakan saat pencarian atribut.
- **Disable correlation**: Menonaktifkan korelasi otomatis antar data feed dan event.

- **Unpublish events**: Feed tidak akan mempublikasikan event ke server lain.
- **Name**: Nama feed (bebas ditentukan).
- **Provider:** Nama penyedia data ancaman.
- **Input Source:** Sumber data, biasanya dipilih “Network”.
- **URL:** Alamat URL feed (misalnya dari CIRCL, abuse.ch, dll).
- **Source Format:** Format feed, misalnya "MISP Feed", "CSV", "FreeText", dll.
- **Headers:** Tambahan header HTTP jika diperlukan (contohnya Authorization untuk feed privat).
- **Add Basic Auth:** Untuk menambahkan otentikasi HTTP Basic jika feed memerlukannya.
- **Distribution:** Siapa saja yang dapat mengakses data dari feed ini.

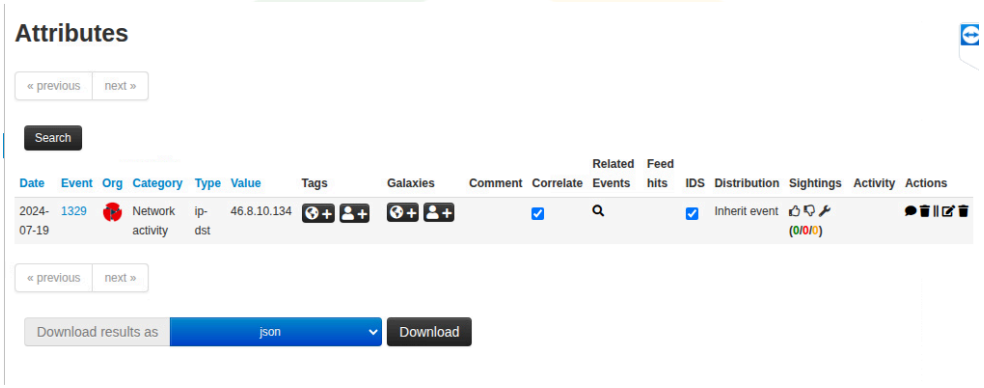


Search and Lookup IoC

Dalam konteks MISP, IoC seringkali dikaitkan dengan **Attributes** dari suatu Event. Untuk melakukan pemeriksaan IoC, buka halaman **Event Actions** → **Search Attributes** dan isi form pencarian sesuai konteks IoC yang ingin diperiksa.



Hasilnya akan menampilkan daftar **Event** yang memiliki/mengandung **Attributes** yang dicari/diperiksa.



Lakukan pemeriksaan Event untuk mengetahui informasi ancaman yang berkaitan dengan IoC/Attributes yang diperiksa.

Dokumentasi Resmi

https://www.misp-project.org/documentation/

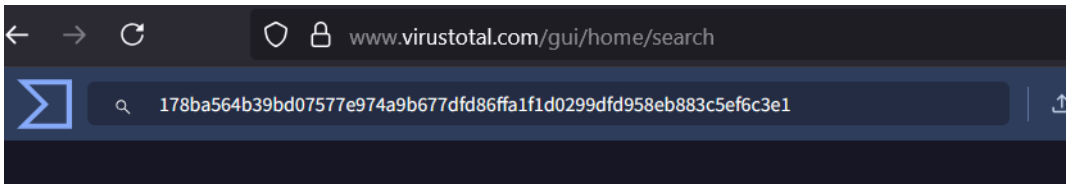
VirusTotal

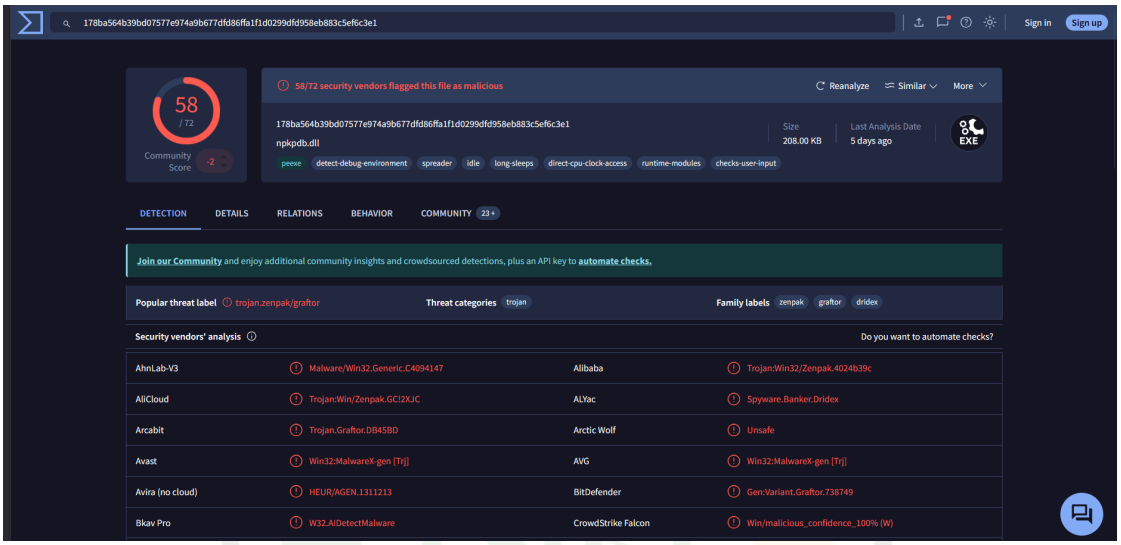
VirusTotal adalah layanan online yang digunakan untuk menganalisis file, IP dan IoC lainnya guna mendeteksi malware, virus, worm, trojan, dan ancaman keamanan lainnya. Layanan ini bekerja dengan cara mengirimkan file atau tautan ke lebih dari 70 mesin antivirus dan berbagai alat analisis keamanan untuk mendapatkan hasil deteksi dari berbagai vendor secara bersamaan. Dalam sistem ini, Virustotal digunakan untuk melakukan analisis dasar terkait IoC insiden siber yang terjadi, seperti alamat IP sumber dan file tidak sah. Sistem memanfaatkan API key Virustotal untuk melakukan pemanggilan layanan melalui API.

Fitur

IoC Analysis

Input yang dapat diberikan bisa berupa File, Filehash, URL, IP, maupun domain. Berikut adalah contoh tampilan hasil analisis Filehash pada Virustotal.

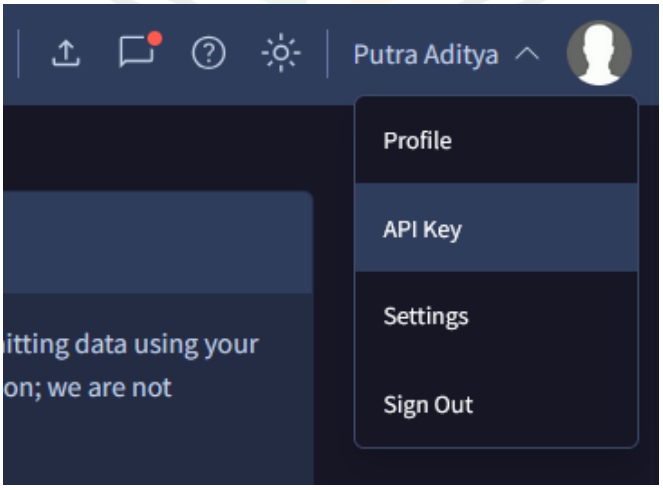


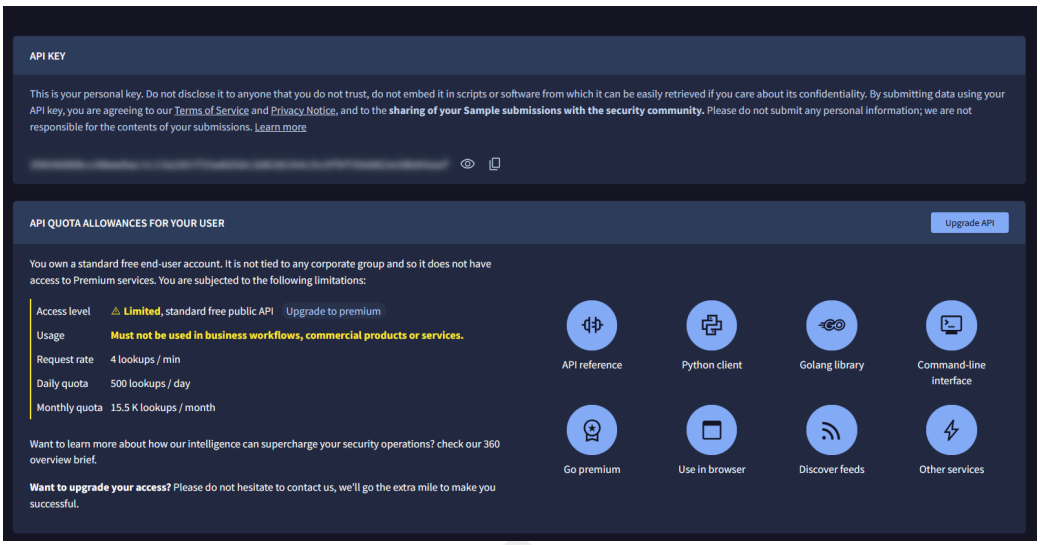


Fungsi

Periksa API Key Virustotal

Pada ikon Profile di kanan atas, klik dan pilih API Key.

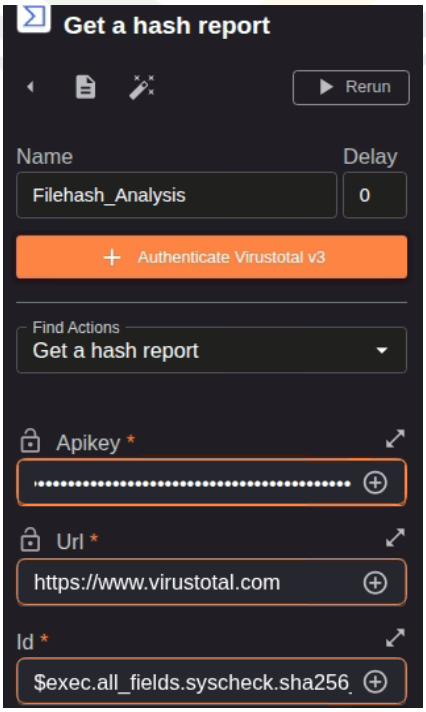




Akun gratis standar (*standard free end-user account*) tidak terhubung dengan grup perusahaan atau layanan premium, sehingga memiliki akses terbatas hanya pada API publik standar. Penggunaan akun dibatasi dengan maksimum 4 permintaan (lookup) per menit, 500 permintaan per hari, dan 15.500 permintaan per bulan.

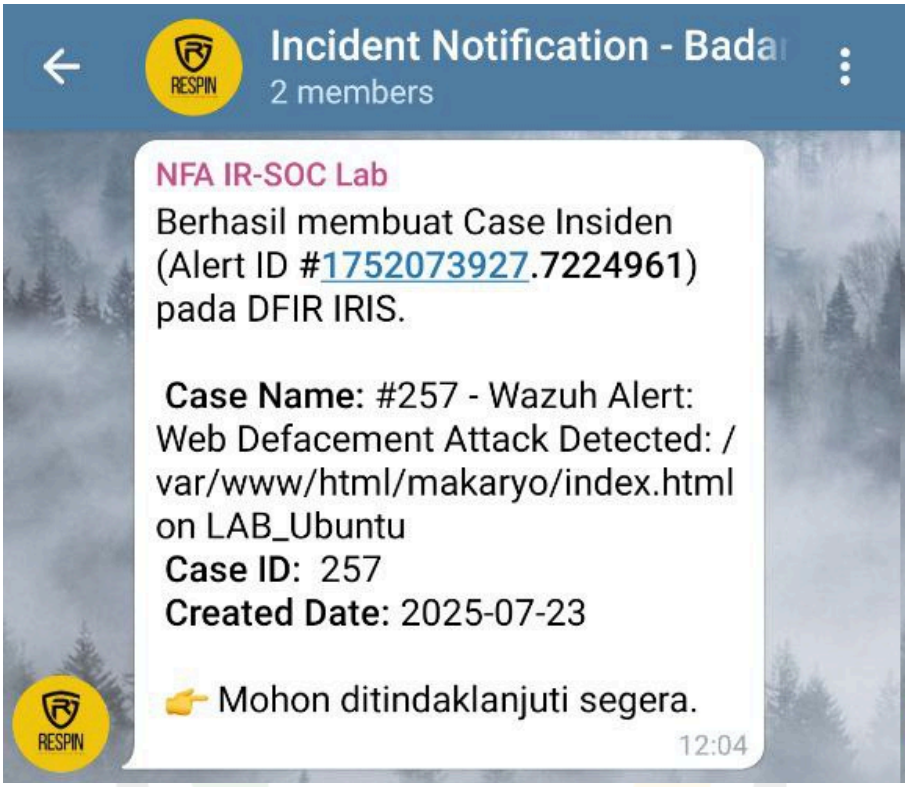
API Usage & Setting

Simpan **API Key** Virustotal, lalu gunakan pada konfigurasi node **Virustotal** pada Shuffle.



Telegram BOT (Notifikasi)

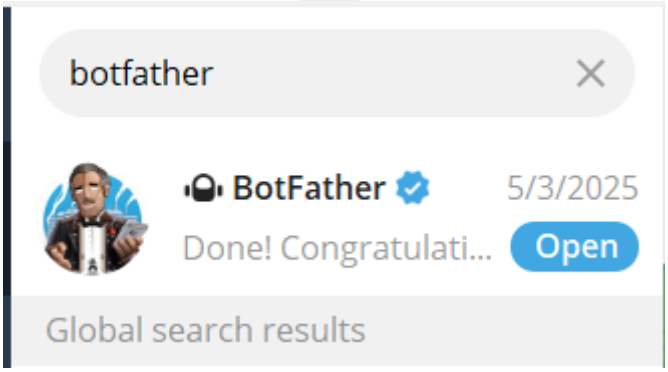
Telegram Bot digunakan untuk mengirimkan notifikasi insiden siber secara otomatis dan *realtime*.



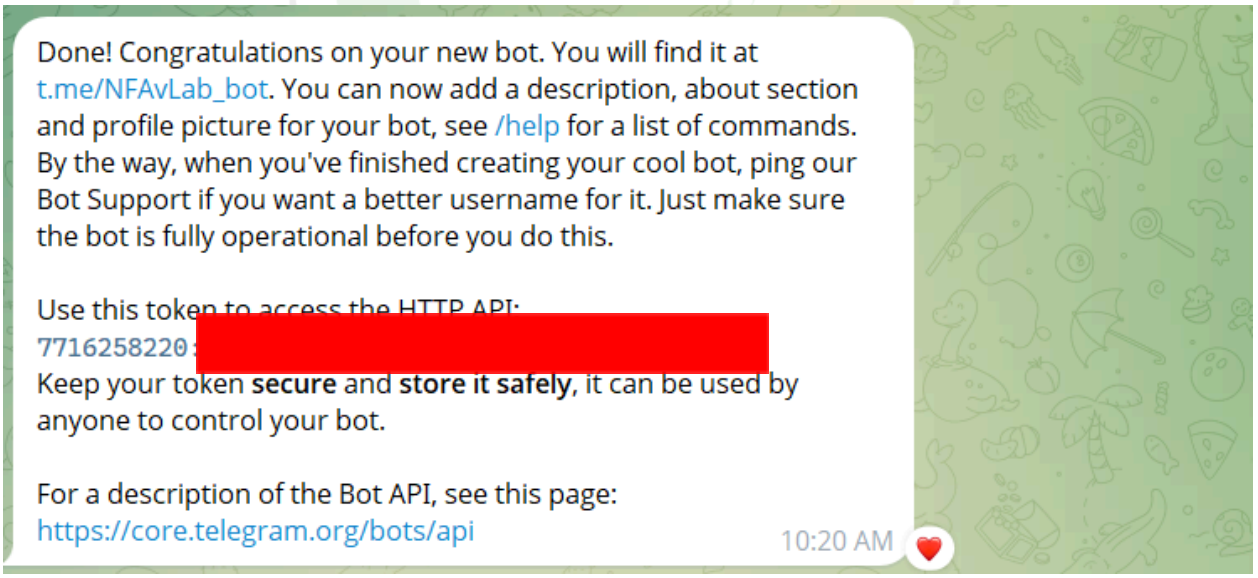
Fungsi

Membuat BOT Telegram

Akses akun official **@BotFather** di **Telegram** (Cari melalui fitur Pencarian di Telegram)

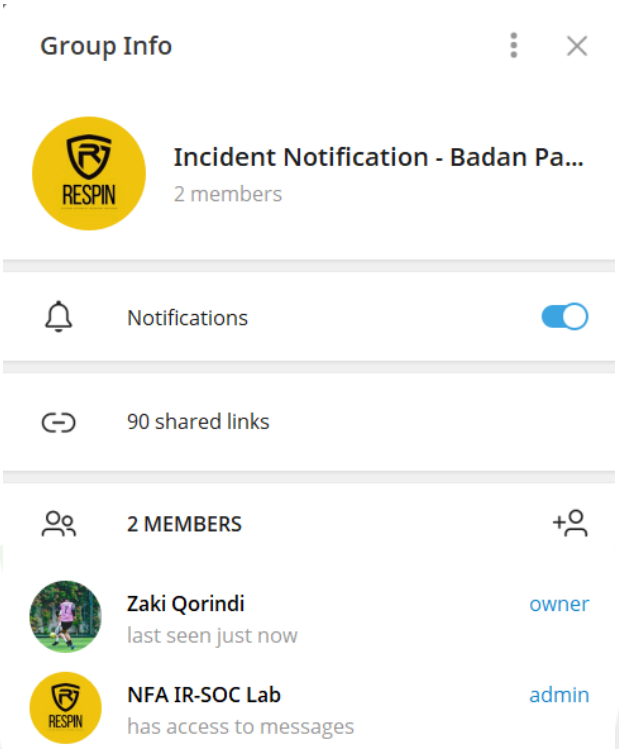


Lakukan pembuatan BOT baru sesuai langkah-langkah yang diberikan. Simpan API Tokennya.



Menambahkan BOT ke Grup Telegram

Setelah BOT dibuat, undang ke dalam sebuah Grup sebagai anggota (Buat Grup terlebih dahulu jika belum ada). Beri hak akses administrator agar BOT dapat mengirim pesan ke Grup.

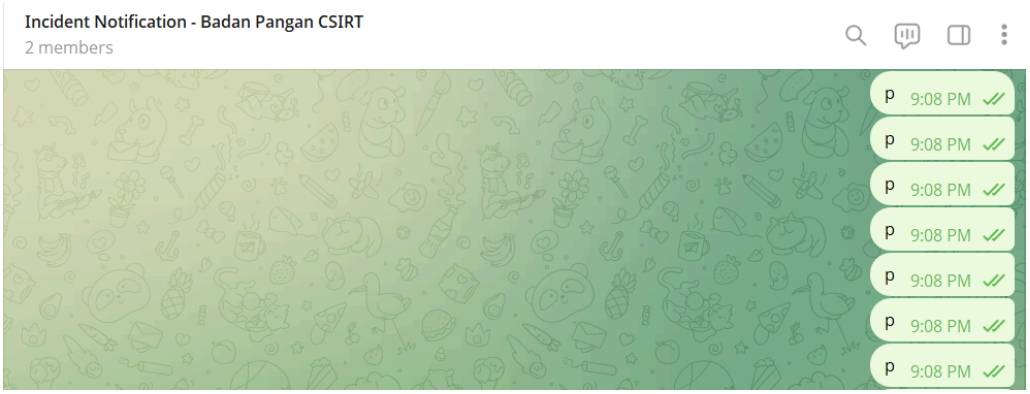


Mendapatkan CHAT ID dari BOT Telegram

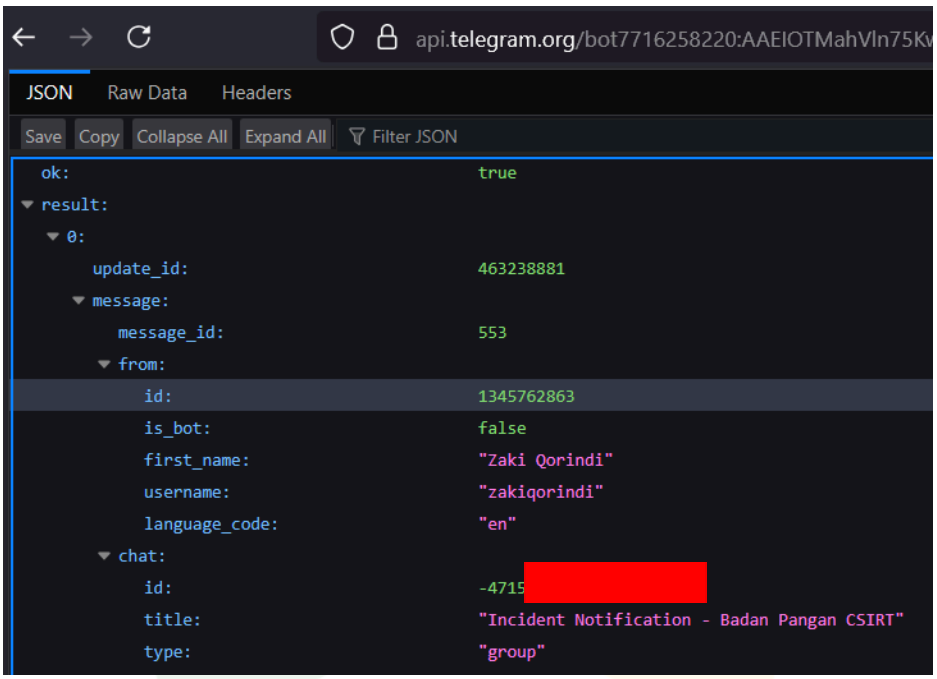
Akses url https://api.telegram.org/bot{TOKEN}/getUpdates

*isi {TOKEN} sesuai BOT yang dibuat

Lakukan pengiriman pesan sembarang ke grup

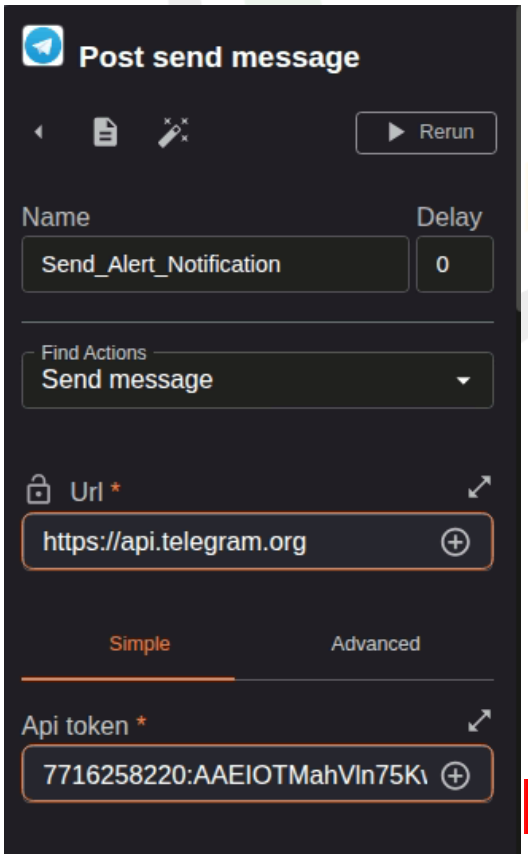


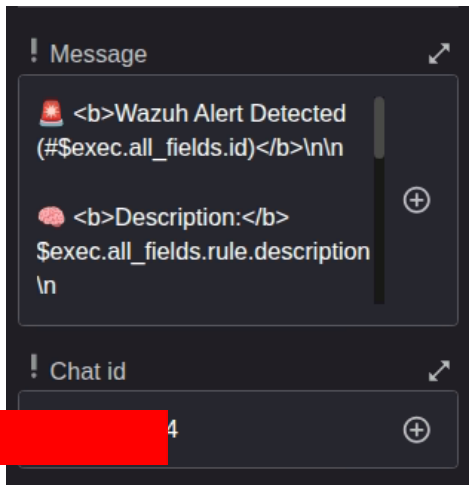
Periksa **CHAT ID** grup, ditandai dengan tanda **"-" (negatif).** Simpan CHAT ID tersebut.



API Usage & Setting

Lakukan konfigurasi **API Token** dan **Chat ID** pada node Telegram di Shuffle.





Penutup

Sebagai penutup, sistem otomasi respon insiden yang telah dijelaskan dalam panduan ini diharapkan dapat membantu Badan Pangan CSIRT dalam merespons insiden dengan lebih cepat, terstruktur, dan efisien. Dengan memanfaatkan fitur-fitur utama dari setiap komponen seperti Wazuh, Shuffle, DFIR IRIS, dan MISP, organisasi dapat meningkatkan ketahanan siber secara signifikan. Penggunaan sistem ini juga mendorong konsistensi dalam penanganan insiden serta meminimalkan risiko human error. Diharapkan panduan ini dapat menjadi referensi praktis bagi seluruh pihak yang terlibat dalam pengelolaan dan penanganan insiden keamanan informasi.

Salam hormat,

Penyusun

Kontak Penyusun

Untuk pertanyaan, masukan, atau diskusi lebih lanjut terkait panduan ini, silakan hubungi:

Nama: Zaki Qorindi
Email: riset.zakiq@gmail.com