



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

Pendahuluan.....	1
Daftar Isi.....	2
Instalasi.....	3
Environment.....	3
Ansible Automation.....	5
Akses Komponen Sistem.....	6
Wazuh.....	8
Fitur.....	9
Fungsi.....	12
Dokumentasi Resmi.....	22
Shuffle.....	23
Fitur.....	23
Fungsi.....	26
Dokumentasi Resmi.....	36
DFIR IRIS.....	37
Fitur.....	38
Fungsi.....	42
Dokumentasi Resmi.....	60
MISP.....	61
Fitur.....	61
Fungsi.....	65
Dokumentasi Resmi.....	69
VirusTotal.....	70
Fitur.....	70
Fungsi.....	71
API Usage & Setting.....	72
Telegram BOT (Notifikasi).....	73
Fungsi.....	73
API Usage & Setting.....	76
Penutup.....	77

Instalasi

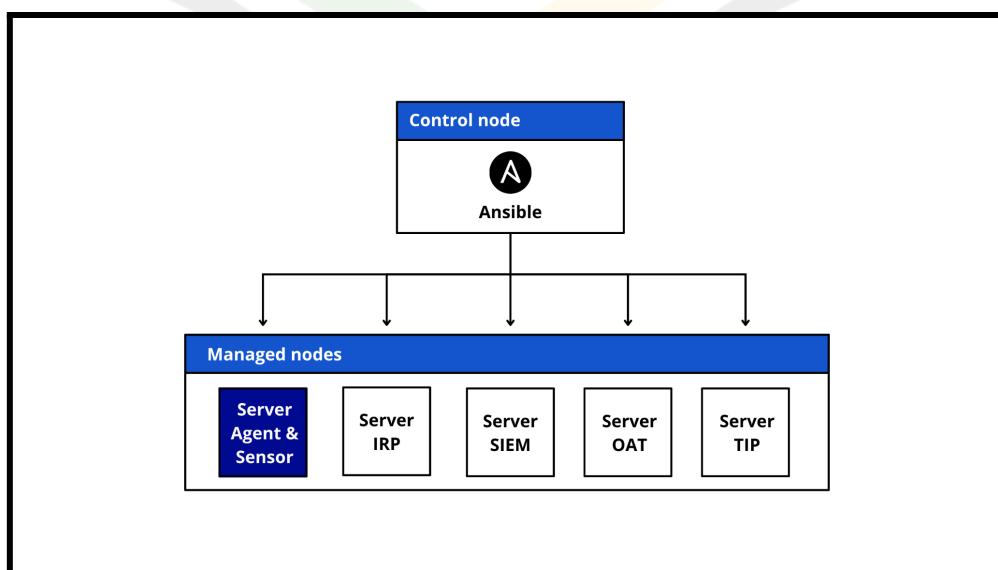
Instalasi sistem dilakukan dengan pendekatan *Infrastructure as Code* menggunakan **Ansible**. Ansible memungkinkan pengguna untuk mendefinisikan infrastruktur dan proses deployment dalam bentuk file YAML yang disebut **playbook**, sehingga proses dapat dijalankan berulang dengan konsisten. Ansible bekerja 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

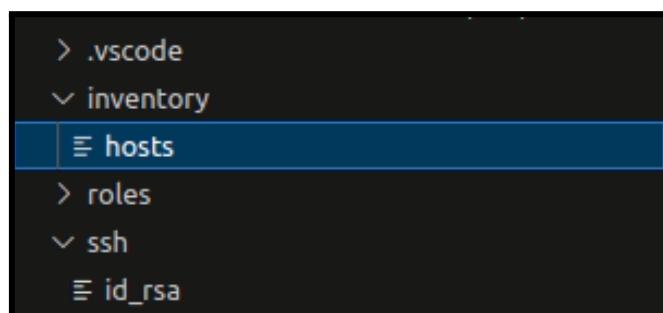
Repository

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**.





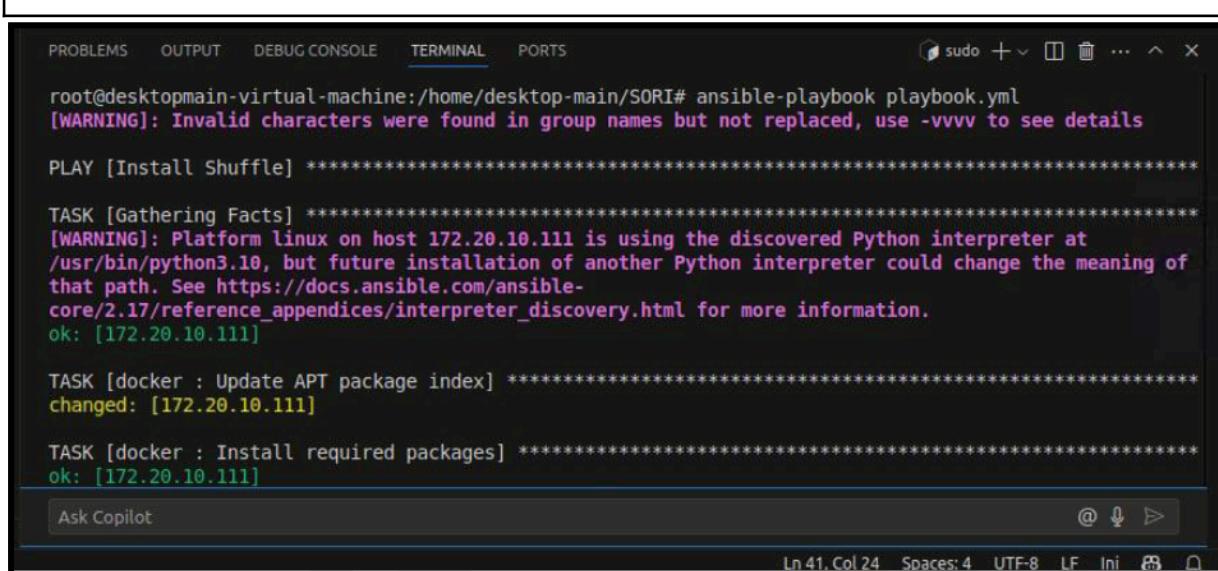
Ansible Automation

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
```



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
root@desktopmain-virtual-machine:/home/desktop-main/SORI# ansible-playbook playbook.yml
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details

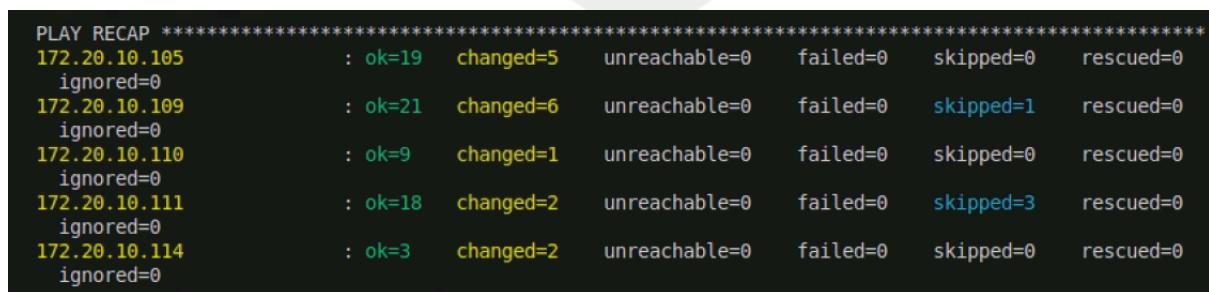
PLAY [Install Shuffle] ****
TASK [Gathering Facts] ****
[WARNING]: Platform linux on host 172.20.10.111 is using the discovered Python interpreter at
/usr/bin/python3.10, but future installation of another Python interpreter could change the meaning of
that path. See https://docs.ansible.com/ansible-
core/2.17/reference_appendices/interpreter_discovery.html for more information.
ok: [172.20.10.111]

TASK [docker : Update APT package index] ****
changed: [172.20.10.111]

TASK [docker : Install required packages] ****
ok: [172.20.10.111]
Ask Copilot @ ↴ ▶
Ln 41. Col 24 Spaces: 4 UTF-8 LF Ini ⌂ ⌂
```

Play Recap

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

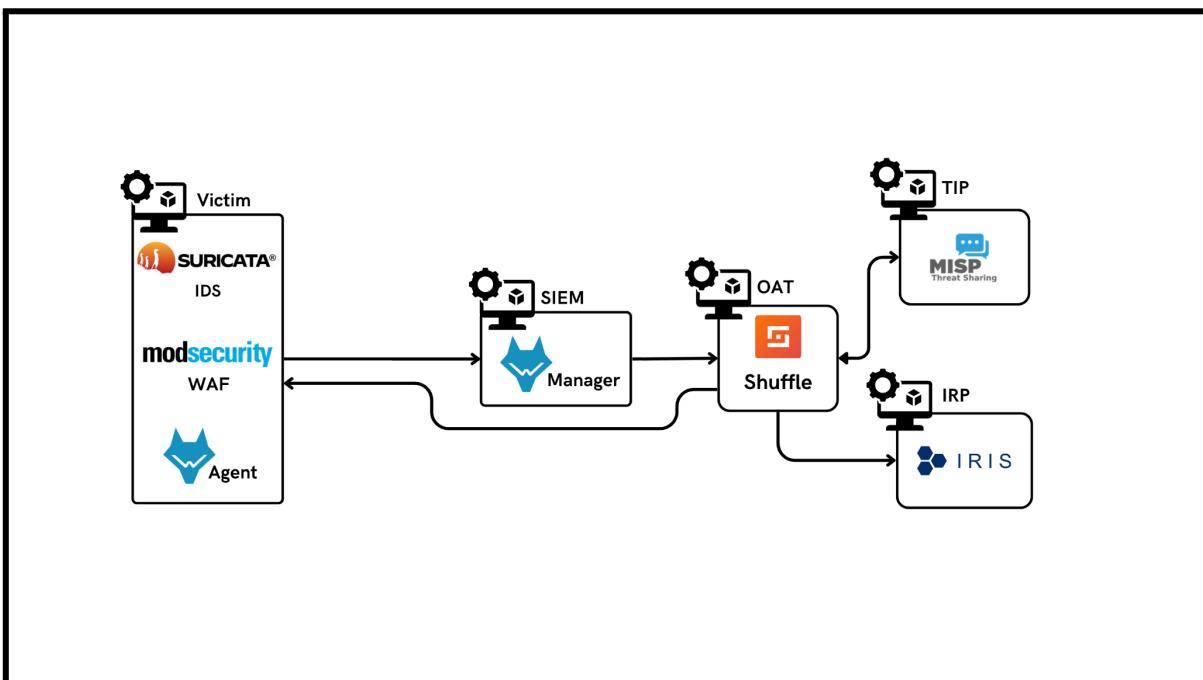


```
PLAY RECAP ****
172.20.10.105      : ok=19   changed=5    unreachable=0   failed=0    skipped=0   rescued=0
                      ignored=0
172.20.10.109     : ok=21   changed=6    unreachable=0   failed=0    skipped=1   rescued=0
                      ignored=0
172.20.10.110     : ok=9    changed=1    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.oLqJ4loYlw.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

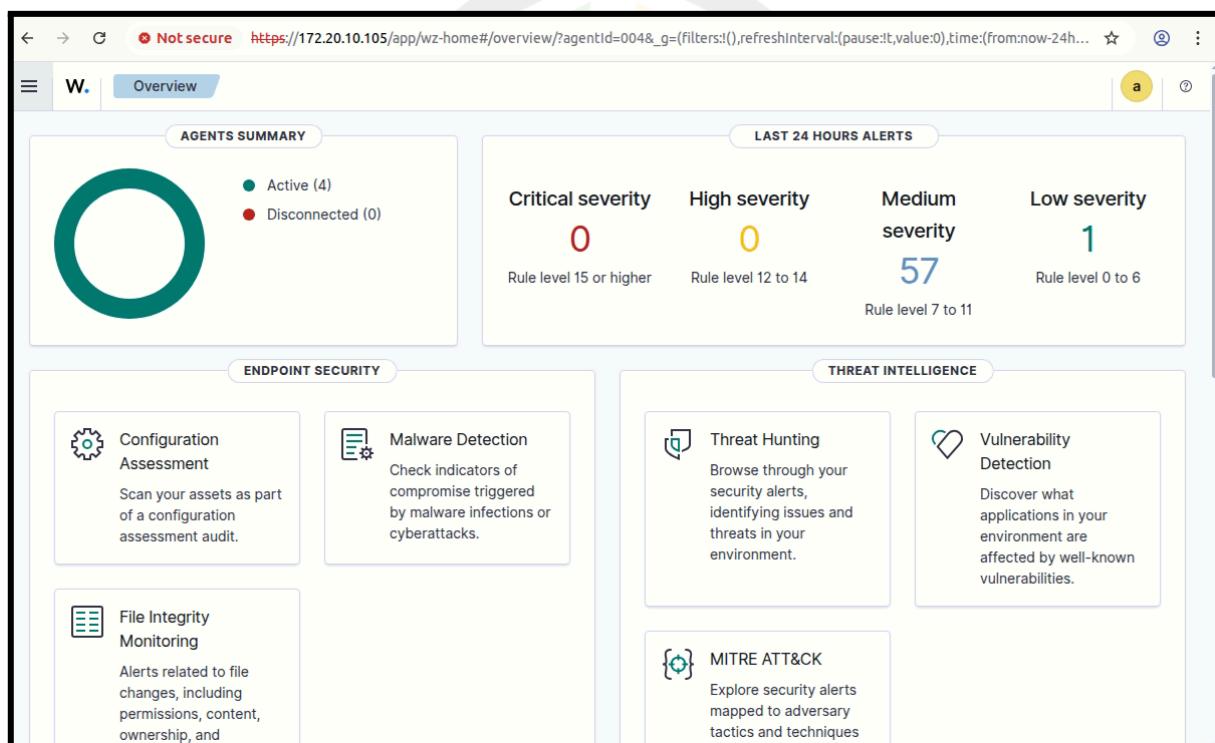
- URL: <https://172.20.10.110/users/login>
*Akses melalui jaringan lokal Badan Pangan CSIRT
- Username: admin@admin.test
- Password: **adminmisp123!!@!**
*ubah password secara berkala!



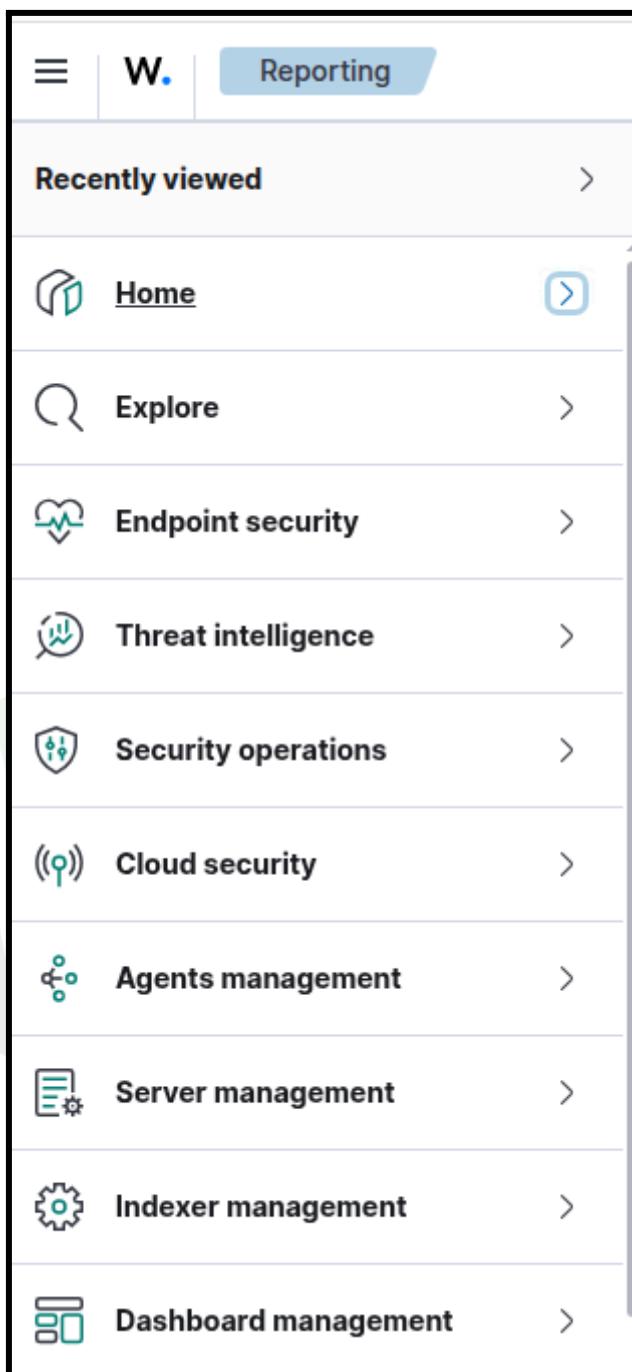


Wazuh

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

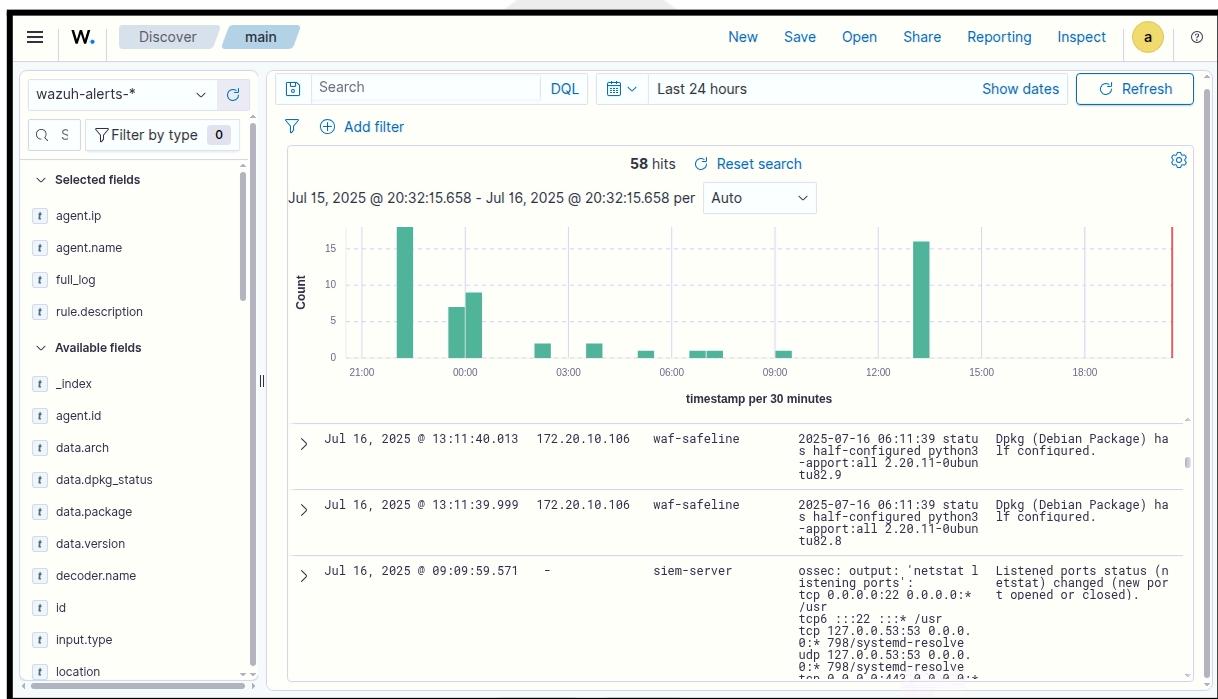


sistem operasi, alamat IP, versi agen, serta status koneksi, sehingga tim keamanan dapat memastikan semua endpoint terpantau dan dilindungi secara optimal.

Fungsi

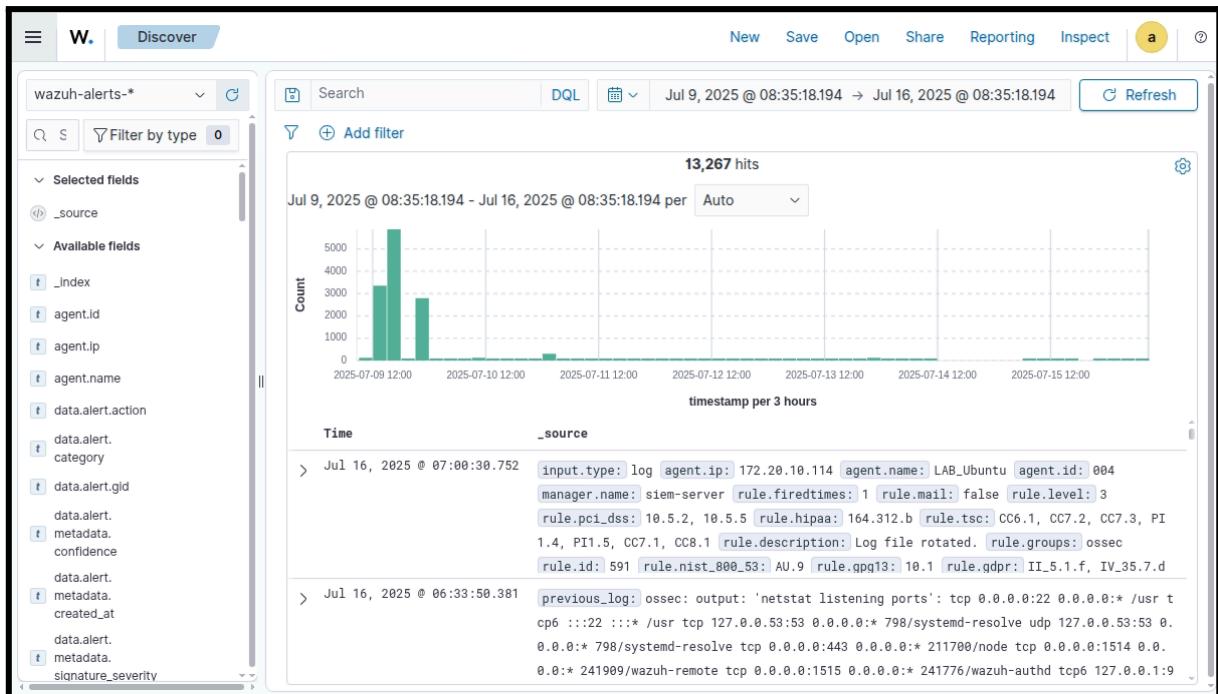
[Explore] Security Event / Discovery

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, seperti **agent.name**, **rule.id**, **rule.description**, **full.log**, **timestamps**, dll.

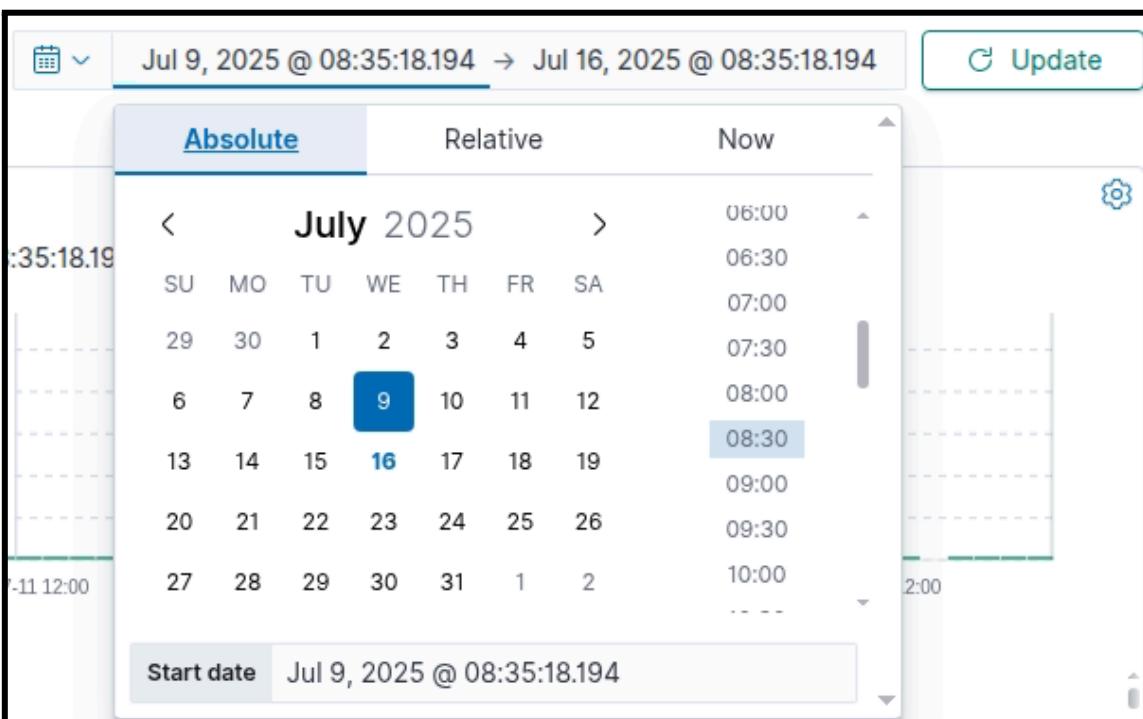


Pada bagian **tengah atas**, terdapat tombol **Add Filter** yang dapat diatur untuk menyaring informasi agar sesuai dengan yang diinginkan analisis. Fungsi ini juga dapat menspesifikasi indikator insiden dalam kumpulan event yang sangat banyak

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

The screenshot shows the "Edit filter" dialog box. It includes fields for "Field" (set to "rule.level"), "Operator" (set to "is not one of"), "Values" (with a "Select values" button), and a "Create custom label?" checkbox. At the bottom are "Cancel" and "Save" buttons.

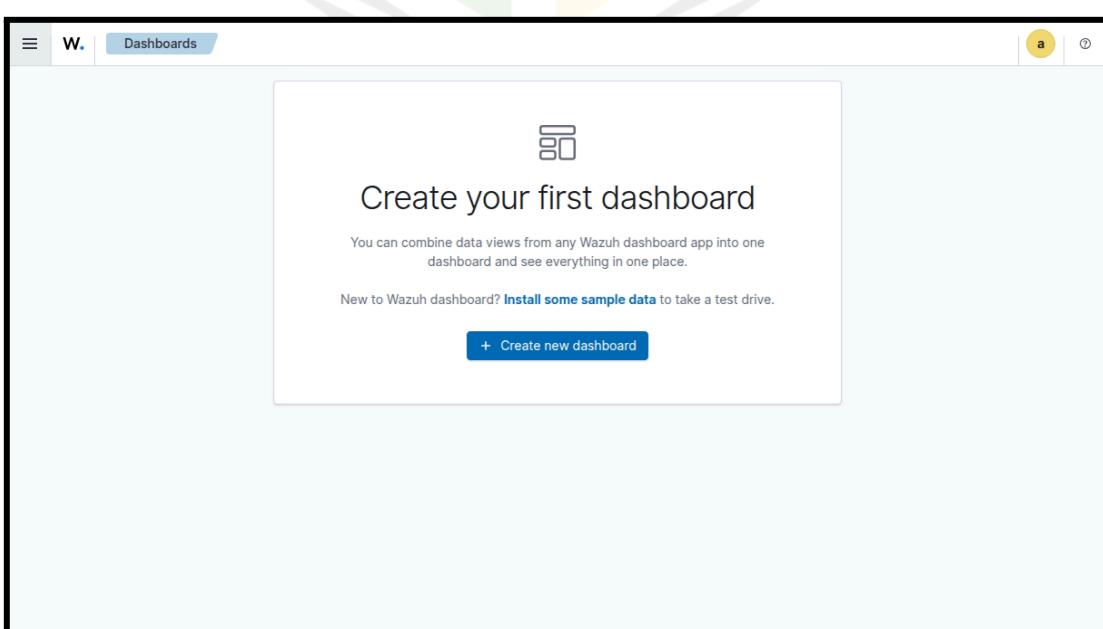
Pada bagian **kanan atas**, dapat dilakukan pengaturan rentang waktu tertentu agar informasi yang ditampilkan dapat dikerucutkan dan tidak terlalu banyak.



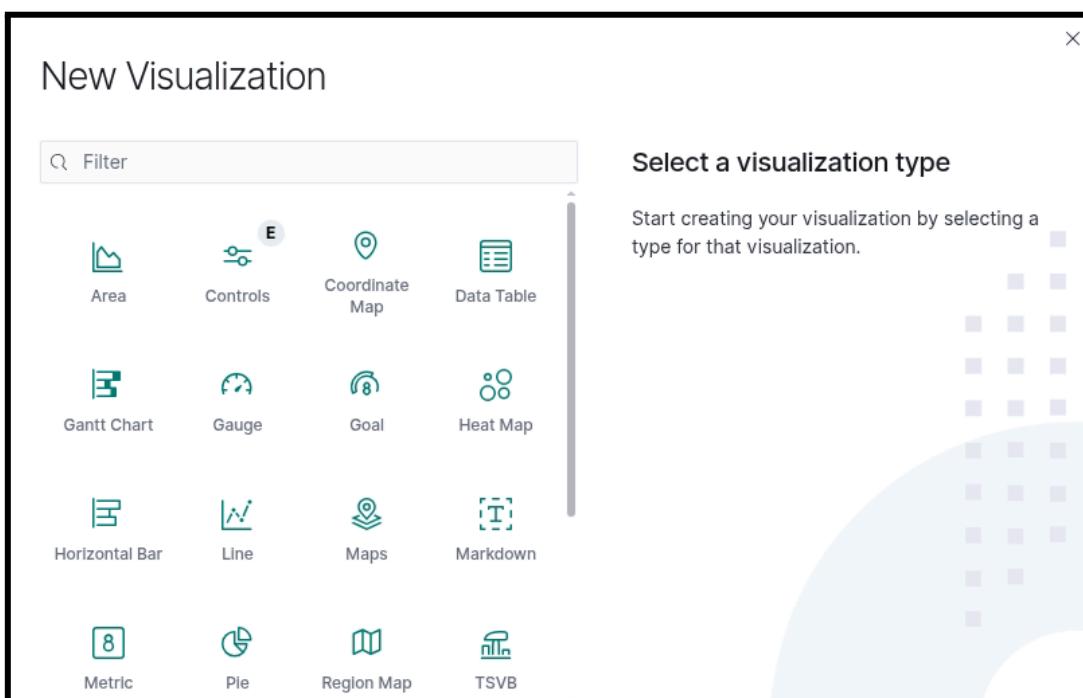
[Explore] Dashboard

Create Dashboard

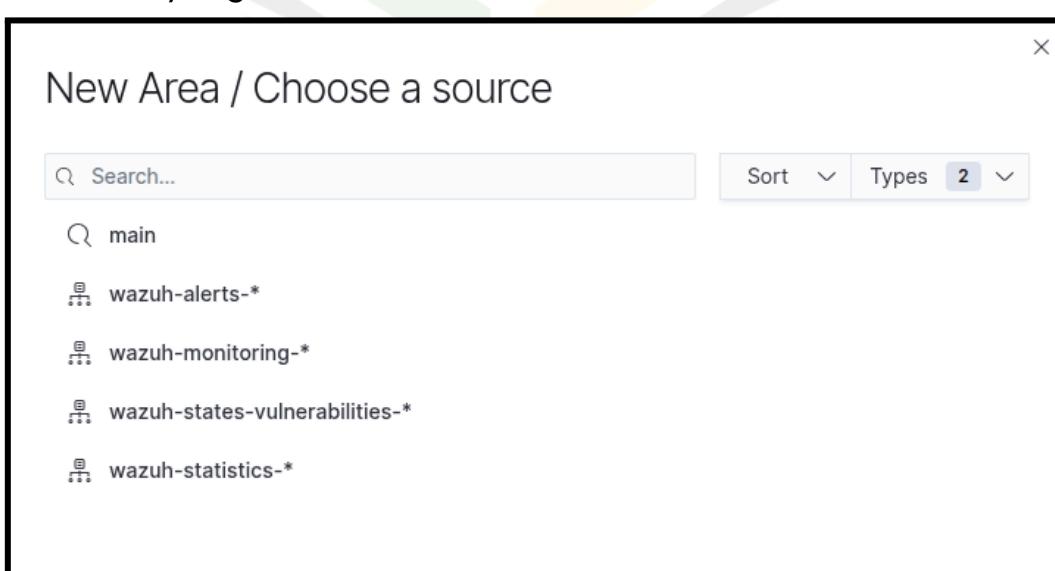
Analis dapat memuat dashboard sendiri sesuai dengan jenis informasi yang ingin dianalisis.



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.

The screenshot shows the 'Metrics & axes' tab selected in the top navigation bar. Under the 'Metrics' section, 'Rule Level' is expanded. The 'Value axis' dropdown is set to 'LeftAxis-1'. The 'Chart type' dropdown is set to 'Area' and the 'Mode' dropdown is set to 'Stacked'. The 'Line mode' dropdown is set to 'Straight'. In the 'Y-axes' section, there is a list containing 'LeftAxis-1 Rule Level' with a '+' button to its right.

[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**

The screenshot shows the 'Reporting' interface with the 'Create' report definition screen. The top section is titled 'Reporting' and has a 'Reports (0)' heading. It includes a search bar, a 'Refresh' button, and filters for 'Type' and 'State'. Below this, a message states 'No reports to display' and provides instructions to 'Create a report definition, or share/download a report from a dashboard, saved search or visualization.' A link to 'Get started with OpenSearch Dashboards reporting' is provided. The bottom section is titled 'Report definitions (0)' and includes a search bar, a 'Refresh' button, and a 'Create' button. It has a table header with columns: Name, Source, Type, Schedule details, Last Updated, and Status.



Isi sesuai keinginan dan ketentuan.

Not secure https://172.20.10.105/app/reports-dashboards#/create

Reporting Create report definition

Create report definition

Report settings

Name

Traffic Daily Report

Valid characters are a-z, A-Z, 0-9, (), _ (underscore), - (hyphen) and (space).

Description (optional)

13 Juli 2025

Report source

Dashboard

Visualization

Saved search

Notebook

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

Report source

Dashboard

Visualization

Saved search

Notebook

Select saved search

main

Record limit

10000

Time range

Last 30 minutes Show dates

Time range is relative to the report creation date on the report trigger.

File format

CSV

XLSX

Report trigger

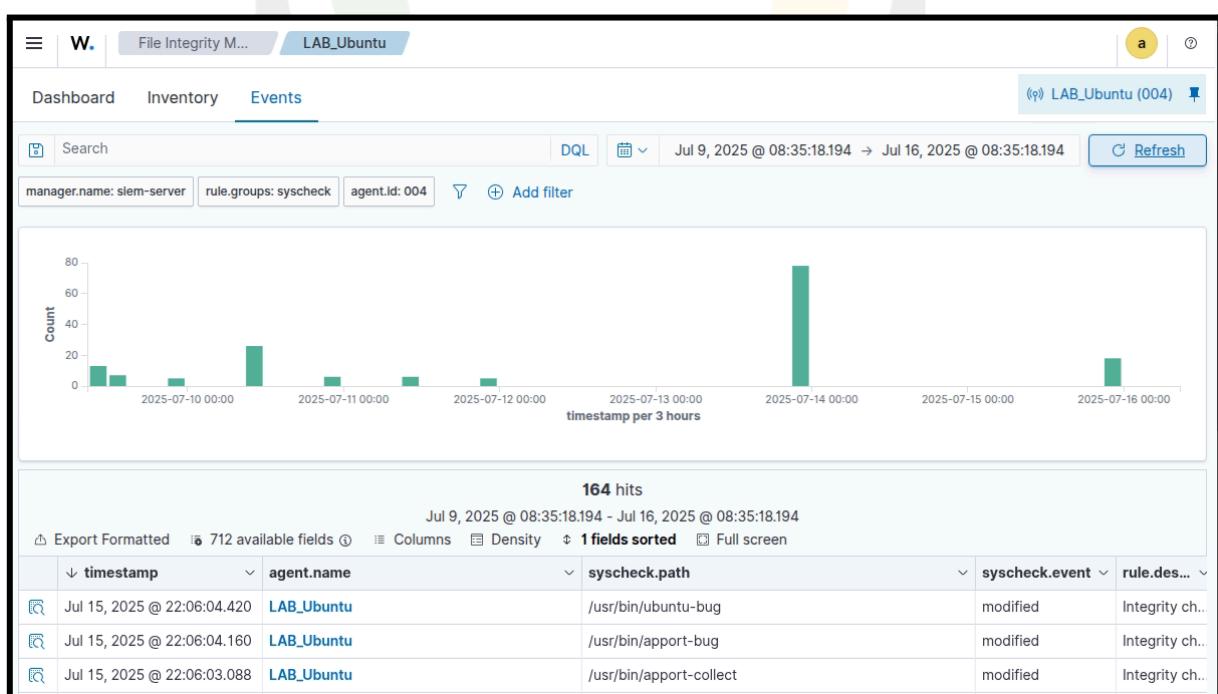
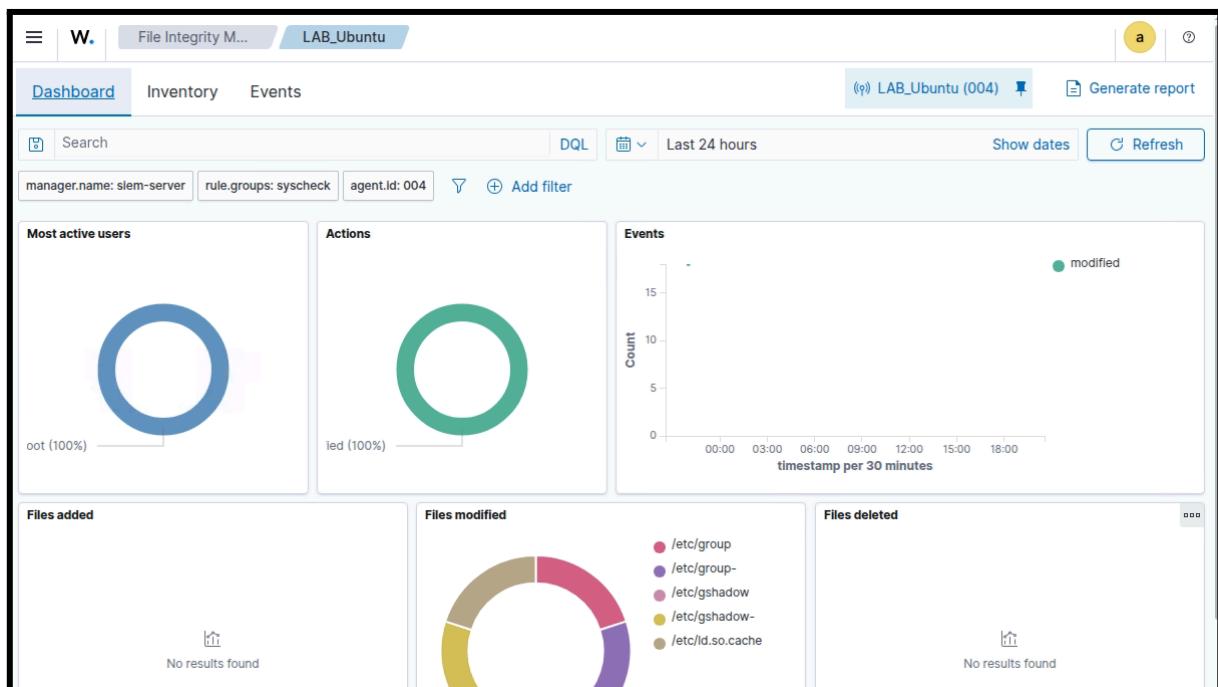
On demand

Schedule



[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.

The screenshot displays two views of the Wazuh Threat Hunting interface. The top view shows a dashboard with four large numerical metrics: 12,587 (Total), 33 (Level 12 or above alerts), 6 (Authentication failure), and 146 (Authentication success). Below these are two charts: 'Top 10 Alert groups evolution' and 'Alerts'. The bottom view shows an 'Events' section with a histogram of event counts over time, followed by a table of 12,587 hits from July 9 to July 16, 2025. The table includes columns for timestamp, agent.name, rule.description, rule.level, and rule.id.

timestamp	agent.name	rule.description	rule.level	rule.id
Jul 16, 2025 @ 07:00:30.752	LAB_Ubuntu	Log file rotated.	3	591
Jul 15, 2025 @ 22:06:04.420	LAB_Ubuntu	Integrity checksum changed.	7	550
Jul 15, 2025 @ 22:06:04.160	LAB_Ubuntu	Integrity checksum changed.	7	550

[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 dieksplorasi oleh pihak tidak bertanggung jawab.

The screenshot shows the Wazuh Vulnerability Detection interface for the LAB_Ubuntu agent. At the top, there are five large numerical displays representing different severity levels:

- Critical - Severity: 15
- High - Severity: 411
- Medium - Severity: 1,010
- Low - Severity: 44
- Pending - Evaluation: 1,844

Below these are four tables of data:

- Top 5 vulnerabilities by count:**

Vulnerability ID	Count
CVE-2022-3219	11
CVE-2022-27943	9
CVE-2023-7008	8
CVE-2016-9138	7
CVE-2017-7189	7
- Top 5 OS:**

OS	Count
Ubuntu 22.04.5 LTS (Jammy Jellyfish)	3,324
- Top 5 agents:**

Agent	Count
LAB_Ubuntu	3,324
- Top 5 packages by count:**

Package	Count
linux-image-5.15.0-1668	1,668
linux-image-5.15.0-1463	1,463
Twisted	6
shim-signed	6
Jinja2	5

At the bottom, there are three small charts: "Most common vulnerability score", "Most vulnerable OS families", and "Vulnerabilities by year of publication".

The screenshot shows the Wazuh Events tab for the LAB_Ubuntu agent. It displays a histogram of event counts over time:

Timestamp	Count
2025-07-10 00:00	4
2025-07-11 00:00	6
2025-07-12 00:00	4
2025-07-13 00:00	0
2025-07-14 00:00	0
2025-07-15 00:00	0
2025-07-16 00:00	0

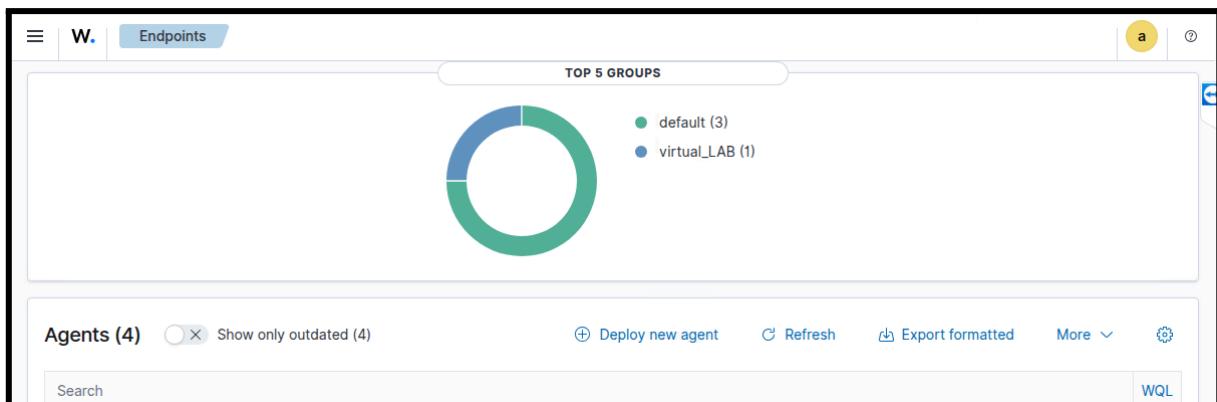
Below the histogram is a table of 14 detected vulnerabilities:

timestamp	agent.name	data.vulnerability.cve	data.vulnerability.severity	data.vulnerability.package.name
Jul 11, 2025 @ 14:09:21.463	LAB_Ubuntu	CVE-2024-52005	-	git-man
Jul 11, 2025 @ 14:09:21.363	LAB_Ubuntu	CVE-2024-52005	-	git
Jul 11, 2025 @ 14:09:21.206	LAB_Ubuntu	CVE-2024-52005	-	git-man

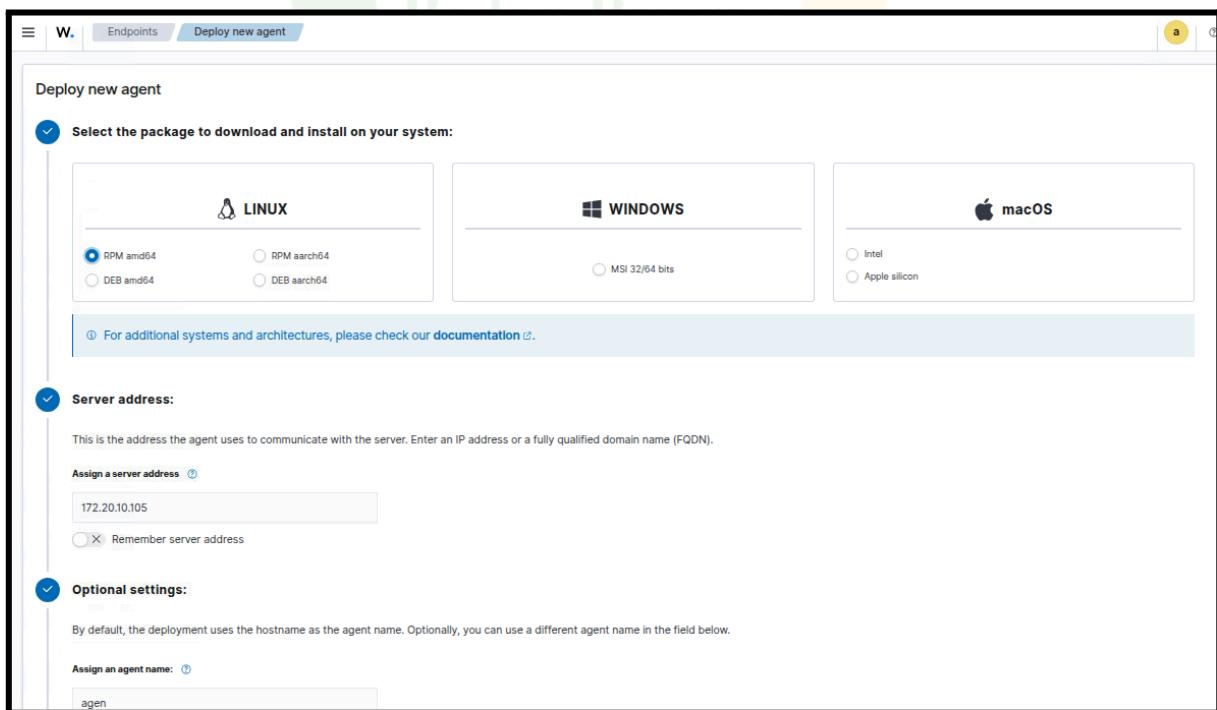
[Agent Management] Summary

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.





agen

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

default

Run the following commands to download and install the agent:

```
curl -o wazuh-agent-4.12.0-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.12.0-1.x86_64.rpm && sudo WAZUH_MANAGER='172.20.10.105' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='agen' rpm -ihv wazuh-agent-4.12.0-1.x86_64.rpm
```

Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

Start the agent:

```
sudo systemctl daemon-reload  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent
```

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

Not secure <https://172.20.10.105/app/endpoints-summary#/agents-preview/>

Endpoints

W Agents by status

- Active (4)
- Disconnected (0)
- Pending (0)
- Never connected (0)

TOP 5 OS

- ubuntu (3)
- centos (1)

TOP 5 GROUPS

- default (3)
- virtual_LAB (1)

Agents (4) Show only outdated (4)

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	waf-safeline	172.20.10.106	default	Ubuntu 22.04.5 LTS	node01	v4.9.0	active	...
002	STAGING-PanellHarga	172.20.10.102	default	Ubuntu 22.04.4 LTS	node01	v4.9.0	active	...
003	AAPanel-dev	172.20.10.100	default	CentOS Linux 7.9	node01	v4.9.0	active	...
004	LAB_Ubuntu	172.20.10.114	virtual_LAB	Ubuntu 22.04.5 LTS	node01	v4.9.2	active	...

Rows per page: 10 < 1 >

Dokumentasi Resmi

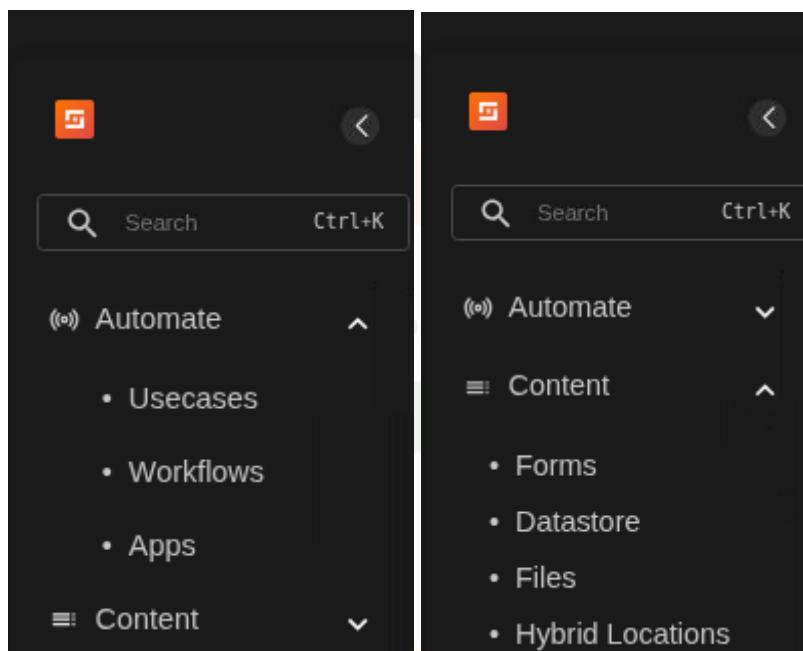
<https://documentation.wazuh.com/current/index.html>



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

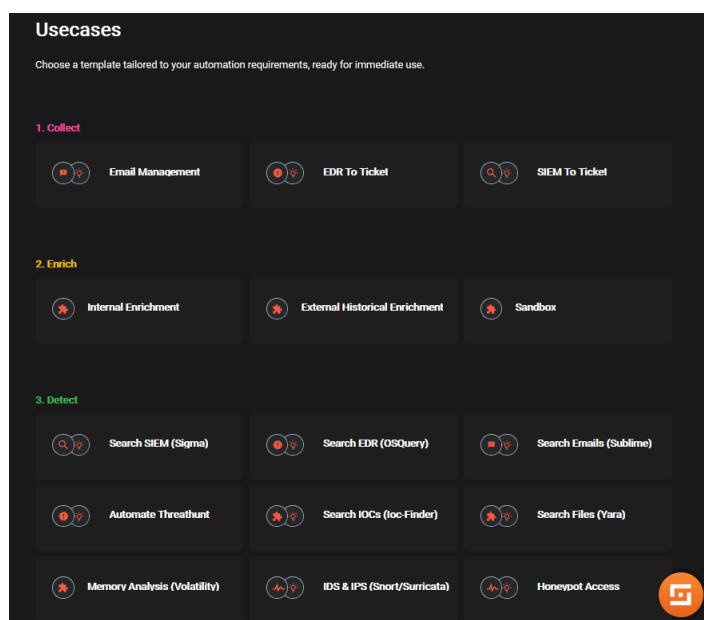




Automate

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.





The screenshot shows the 'Discover Workflows' section of a software interface. On the left, there's a sidebar with navigation links like 'Automate', 'Content', 'Documentation', and 'Admin'. Below that is a 'Recent Workflows' section with a card for 'Incident Response Auto...'. At the bottom of the sidebar are buttons for 'BOOK A DEMO' and a dropdown menu. The main area is titled 'Discover Workflows' and contains several cards for different workflows:

- Shuffle Enrichment
- Outlook365 - Get Emails
- Wazuh ticket handler
- Gmail reader
- Shuffle Tools health API Subflow
- Enrichment with MISP
- Outlook - Get phishing attachments
- Python list fixer

Each card displays icons for different actions and metrics.

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.

The screenshot shows the 'Org Apps' section of a software interface. On the left, there's a sidebar with navigation links like 'Organization Apps', 'My Apps', and 'Discover Public Apps'. Below that is a 'Search org apps' field and dropdown menus for 'All Categories' and 'All Labels'. At the bottom of the sidebar are buttons for 'BOOK A DEMO' and a dropdown menu. The main area is titled 'Org Apps' and contains a grid of application cards:

Google Sheets Other	IRIS V2 Cases	MISP Intel
ClamAV REST NA	Virustotal V3 Intel	Gmail Communication
Telegram Bot Communication	Wazuh SIEM	Siemonster SIEM, Search
Shuffle Tools Other, Testing, Shuffle	Sigma SIEM, Testing	Sooty NA
VADER sentiment analysis	Velociraptor Incident Response, Collect, DFIR,	Snort3 Intel

Each card displays icons for different features and providers.



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

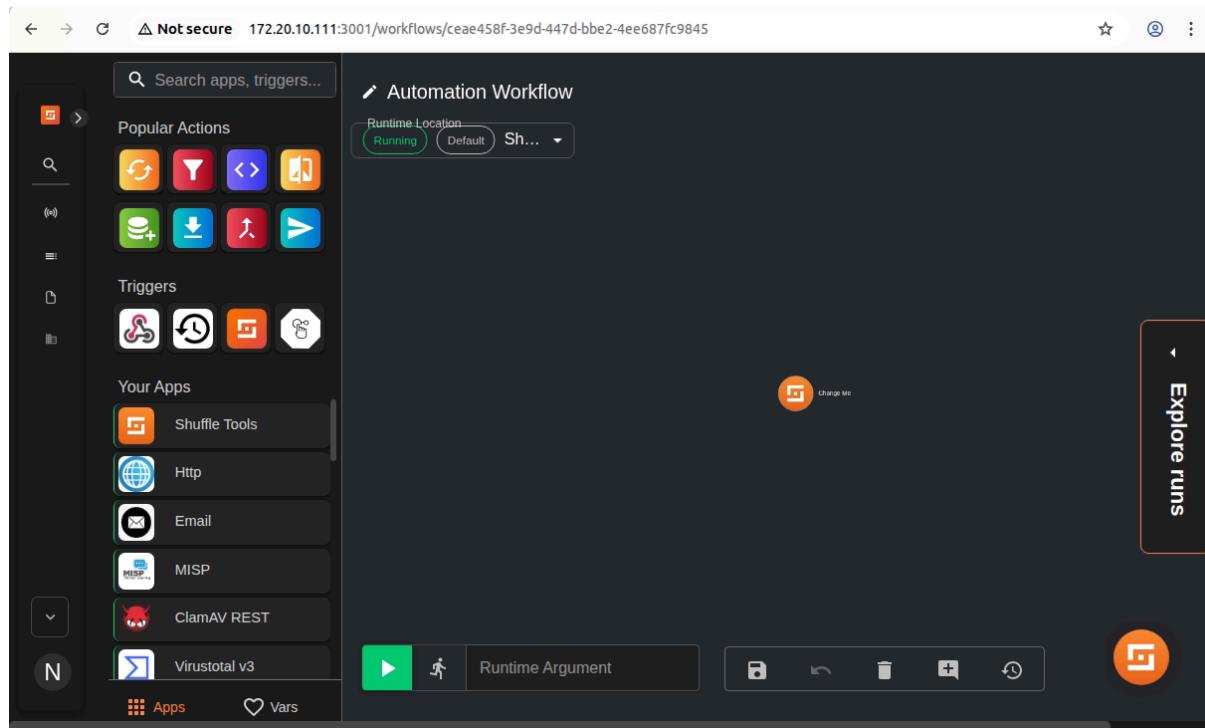
Pada halaman awal setelah Login (**Home**), pilih **Automate → Workflows** yang berada di bar sebelah kiri.

The screenshot shows a web-based application interface for managing workflows. On the left, there is a sidebar with navigation links: 'Automate' (selected), 'Usecases', 'Workflows', 'Apps', 'Content' (expanded), 'Documentation', and 'Admin'. Below this is a 'Recent Workflows' section with a link to 'Incident Response Autom...'. At the bottom of the sidebar are buttons for 'BOOK A DEMO' and a dropdown menu set to 'default'. The main content area has a dark background with a light-colored header bar. The header bar includes a back arrow, forward arrow, refresh icon, and a URL bar showing 'Not secure 172.20.10.111:3001/welcome?tab=1'. To the right of the URL bar are three small icons: a star, a person, and a three-dot menu. The main content area features a heading 'Find your apps' with the sub-instruction 'Select the apps you work with and we will connect them for you.' Below this are several app cards: 'Cases iris' (blue hexagonal icon), 'Email' (envelope icon), 'EDR' (red circle with a white exclamation mark), 'Intel virustotal v3' (Intel logo), and 'SIEM wazuh' (Wazuh logo). At the bottom of this section are two buttons: 'See More Apps' and 'See Usecases'. In the bottom right corner of the main area, there is a small orange circular icon with a white 'G' symbol.

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

The screenshot shows two views of a workflow management interface. The top view displays the 'Discover Workflows' page with several workflow cards listed under categories like 'Shuffle Enrichment', 'Outlook365 - Get Emails', 'Wazuh ticket handler', etc. The bottom view shows the 'New workflow' creation dialog, where a new workflow named 'Automation Workflow' is being created. The 'Usecases' dropdown is set to 'Automation Workflow' and the 'Tags' field is empty. A 'SAVE CHANGES' button is visible at the bottom right of the dialog.

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

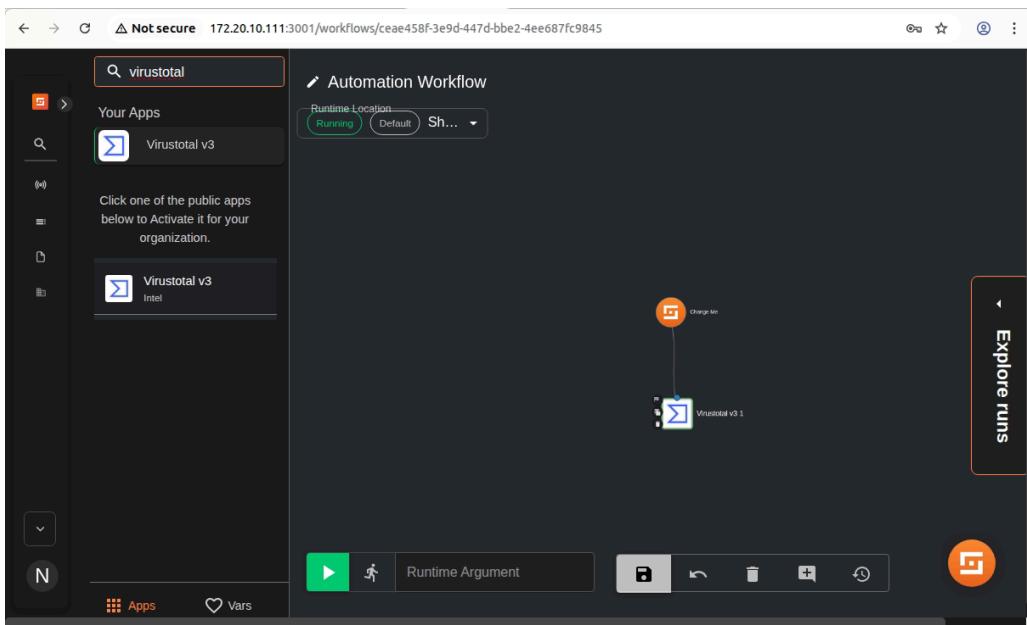


Connect with External Tools/Apps

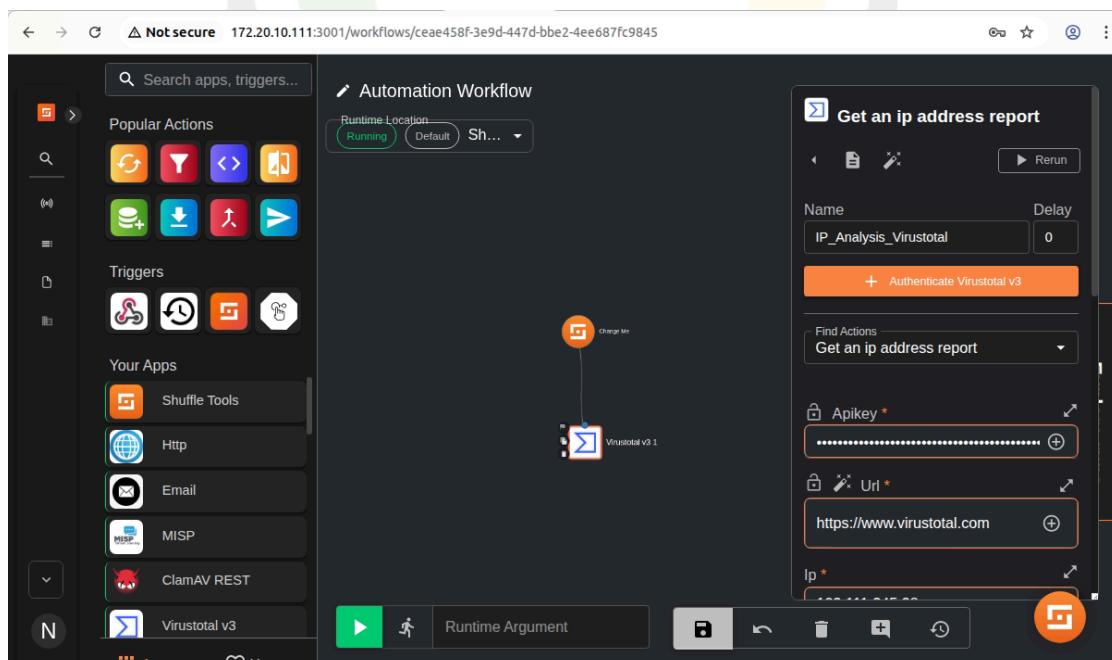
Workflow mendukung banyak aplikasi/tools untuk diintegrasikan, beberapa tools external yang dapat digunakan pada workflow Shuffle melalui API adalah Virustotal, MISP, Wazuh, dll. Pembuatan workflow dapat dimulai dengan drag and drop pada apps/trigger yang dibutuhkan.

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**.

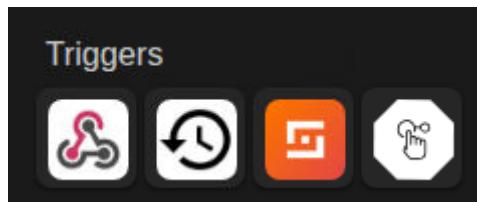


Setiap **node** dan setiap **action** memiliki required parameter yang berbeda-beda sesuai dengan kondisi dan kebutuhan aplikasi/tools.



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.

Webhook: uninitialized

What are webhooks?

Name: Webhook_1

Associated App (optional)

Environment: onprem

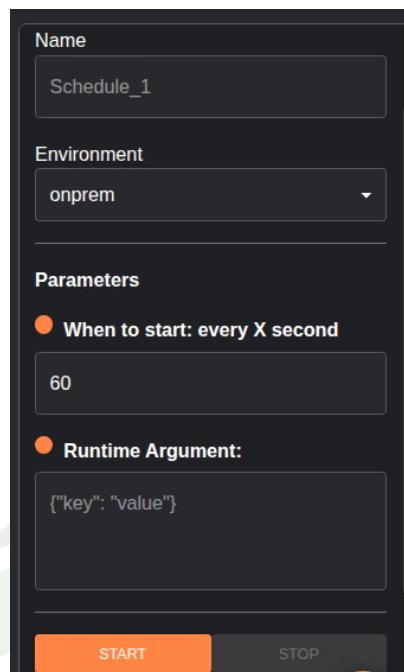
Parameters

Webhook URI: http://172.20.10.111:3001/api/v1/l

START STOP

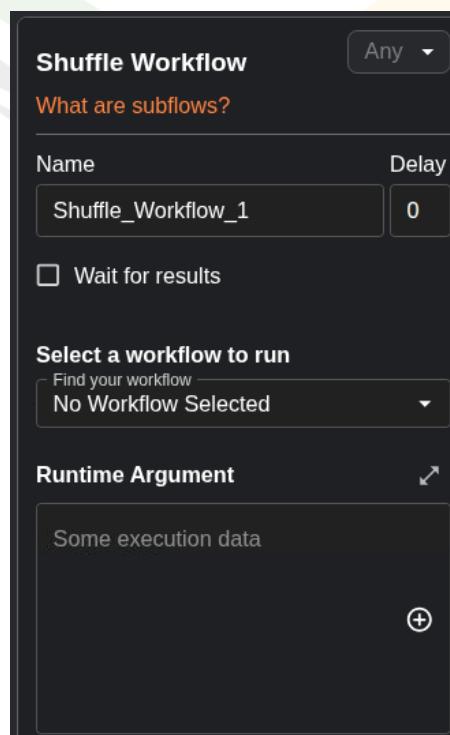
- **Schedule**

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



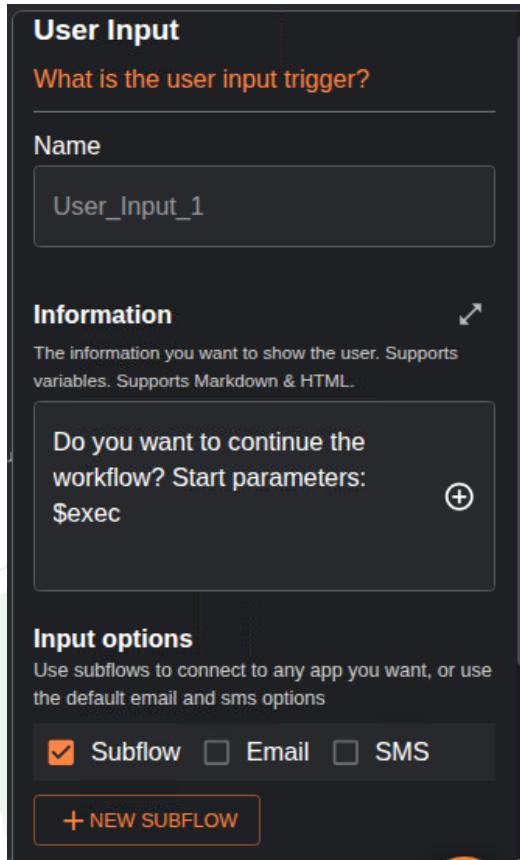
- **Shuffle Workflow**

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



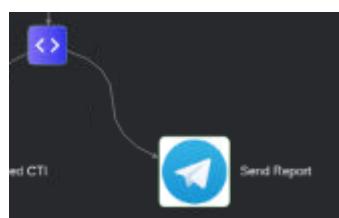
- **User Input**

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

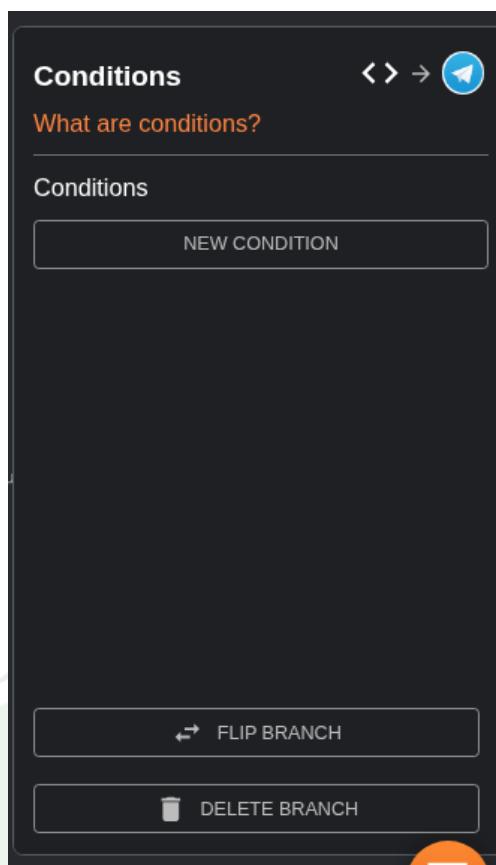


Setting Conditions

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.

Condition

Condition

source destination

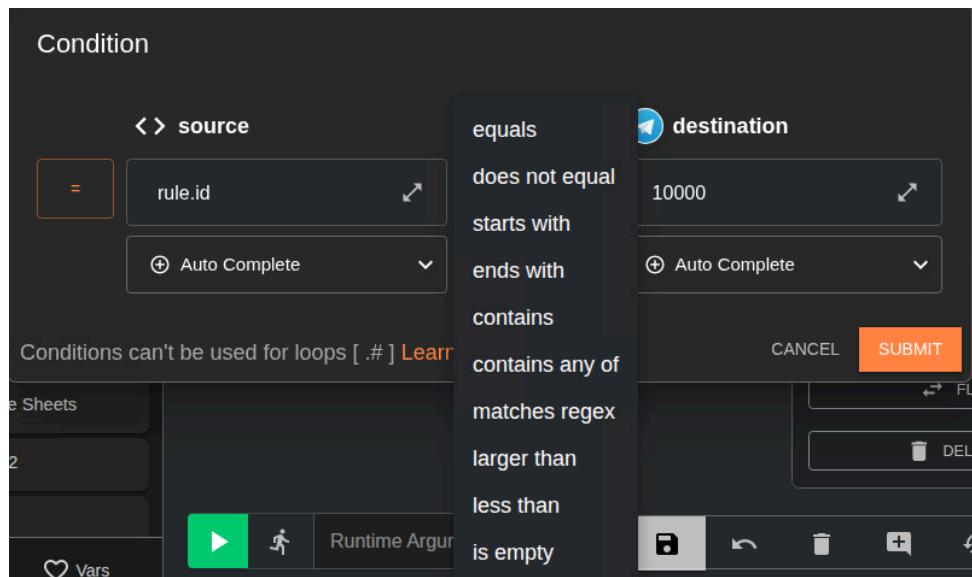
= rule.id EQUALS 10000

Auto Complete Auto Complete

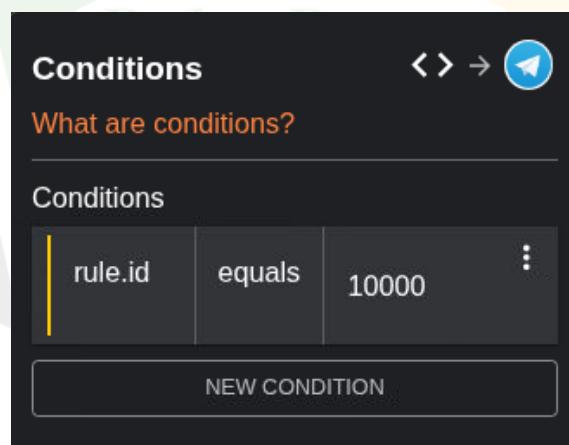
Conditions can't be used for loops [.#] [Learn more](#)

CANCEL SUBMIT

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

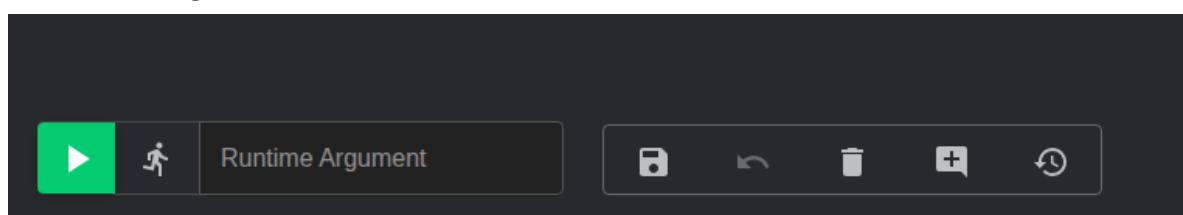


Berikut adalah hasil Conditions yang berhasil dibuat.

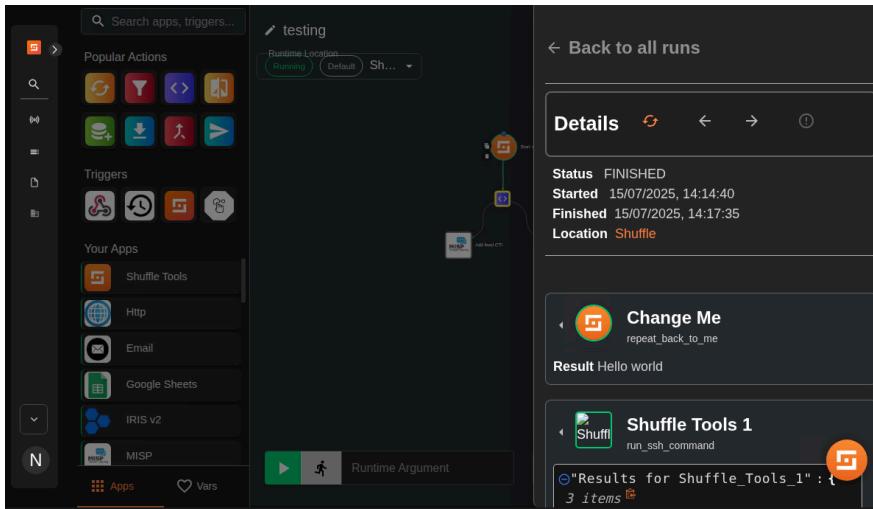


Running and Testing Workflow

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**.



Org Workflows

Org Workflows My Workflows Discover Workflows Org Forms

Filter Workflows All Categories ⌂ ⌄ ⌅ ⌆ + Create Workflow

Send User Input (0) Response Workflow (6) testing (0)

Notification Workflow (0) Triage and Analysis Workflow (0)

Publish Workflow Export Workflow Duplicate Workflow Delete Workflow

Send User Input (0) Response Workflow (6) testing (0)

Notification Workflow (0) Triage and Analysis Workflow (0)

Publish Workflow Export Workflow Duplicate Workflow Delete Workflow

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

Org Workflows

Org Workflows My Workflows Discover Workflows Org Forms Import workflows

Filter Workflows All Categories ⌂ ⌄ ⌅ ⌆ + Create Workflow

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

Org Workflows

Cancel Open Files ⌂ ⌄ ⌅ ⌆ Open

Recent

- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures

Name Location Size Type Accessed

Name	Location	Size	Type	Accessed
SORI	Home	268,2 kB	Archive	Yesterday
15072025-archive-shuffle.zip	Downloads			Sel
15072025-archive-shuffle	Downloads			Sel
id_rsa	Home	400 bytes	Text	Sel
shell.php	Desktop	63 bytes	Program	13 Jul
inde.html	Desktop	1,5 kB	Text	11 Jul
mu.png	Downloads	14,5 kB	Image	8 Jul

Open files read-only (None) ▾

Detection Workflow (0) Reporting Workflow (0)

testing (0) testing (0)

Dokumentasi Resmi

<https://shuffler.io/docs/>

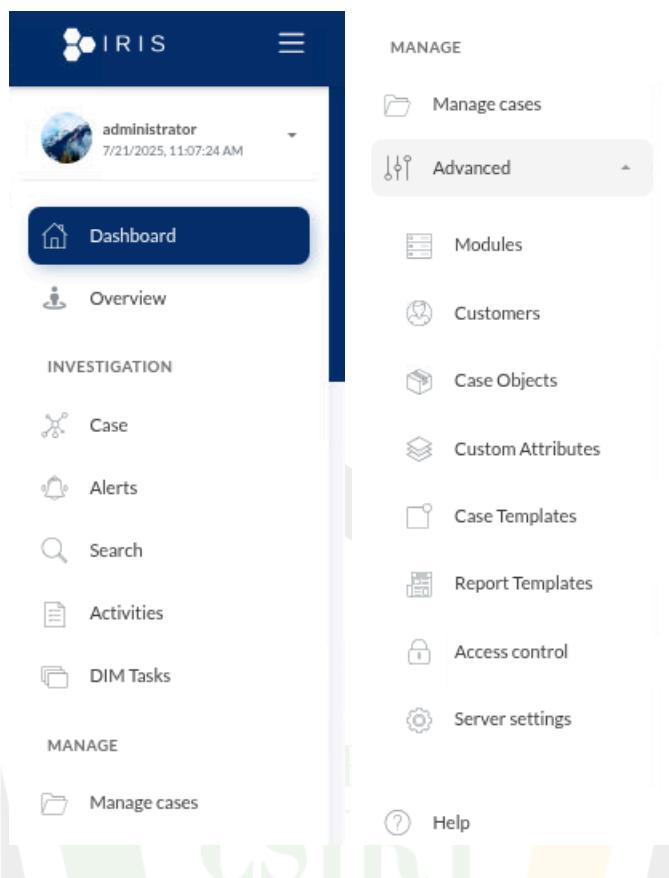


DFIR IRIS

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.

The screenshot shows the DFIR IRIS web interface. At the top, there's a header bar with the title '#240 - Wazuh Alert: DoS Attack Detected on Web Service on LAB_Ubuntu'. Below the header is a navigation sidebar on the left containing links for 'Dashboard', 'Overview', 'INVESTIGATION' (Case, Alerts, Search, Activities, DIM Tasks), and 'MANAGE' (Manage cases, Advanced, Help). The main area is titled 'Dashboard' and displays three summary cards: 'Cases (open / all) 34 / 34', 'Attributed open cases 34', and 'Attributed open tasks 0'. Below these cards is a section titled 'Attributed open tasks' with a table header for 'Title', 'Description', 'Status', 'Case', 'Last update', and 'Tags'. A message 'No data available in table' is displayed. At the bottom of this section, it says 'Showing 0 to 0 of 0 entries' and has 'Export' and 'Copy' buttons. There are also 'Previous' and 'Next' navigation buttons. The footer of the page shows 'IRIS v2.4.20'.

Fitur



Case Management

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

This screenshot shows a detailed view of a case summary for incident #240. The summary states: 'Sebuah alert telah diterima dari sistem deteksi (Wazuh/Suricata) dan sedang dalam proses analisis lebih lanjut.' Below this, there's a section for 'Informasi awal' (Initial Information) which lists: Agent: LAB_Ubuntu, Waktu: 2025-07-09T15:05:45.182+0000, Severity: 12, Deskripsi Rule: DoS Attack Detected on Web Service, and Kategori: ['aggregation', 'customdos', 'web', 'attack', 'custom']. A note at the bottom says: '*Case ini dibuat secara otomatis untuk kebutuhan triase dan investigasi awal.' The bottom of the screen shows the IRIS version 'IRIS v2.4.20'.

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.

The screenshot shows the IRIS interface with a sidebar navigation. The 'Alerts' button in the sidebar is highlighted with a blue background and white text. The main content area displays two alert cards. The first alert is titled 'ZERO-DAY VULNERABILITY 1149' with ID #1150-4ACC59B3-20EA-4E9C-9973-55B3B09C8E8B. It describes a previously unknown vulnerability discovered in a critical software component. The second alert is titled 'VPN EXPLOIT 1208' with ID #1209-00368BB4-B629-4A21-A3B6-4CC332D8CE9D. It describes an attacker gaining access to the network by exploiting a vulnerability in the VPN. Both alerts show their status as 'Escalated', the date (2023-12-28T21:55:50.914896), severity ('High'), source ('Secure Web Gateway'), and related entities ('IrisInitialClient' and 'Malicious-Code: Ransomware').

Activities Management

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

The screenshot shows the IRIS interface with a sidebar navigation. The 'Activities' button in the sidebar is highlighted with a blue background and white text. The main content area displays a table of activities for a specific case. The table has columns for Date, User, Case, Manual input, From API, and Activity. Each row in the table provides a timestamp, the user who performed the action, the case it's associated with, and the source of the activity (Manual input or From API). The 'Activity' column contains detailed notes such as 'Updated note "basic enrichment with virustotal (case id #242)"', 'Created note "new note"', 'Added directory "analysis"', and 'Added directory "analysis"'. The notes also mention specific alert IDs like '#242 - Wazuh Alert: Dos Attack Detected on Web Service on LAB_Ubuntu'.



Customer Management

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

The screenshot shows the 'Customers management' section of the IRIS platform. On the left, there is a sidebar with navigation links for Dashboard, Overview, INVESTIGATION (Case, Alerts, Search, Activities, DIM Tasks), and MANAGE (Manage cases, Advanced, Modules, Customers, Case Objects). The main area is titled 'Customers management' and displays a table with two entries: 'IrisInitialClient' and 'Analyst01'. The table has columns for 'Name' and 'Description'. At the bottom, it says 'Showing 1 to 2 of 2 entries' and includes 'Previous' and 'Next' buttons.

Modules Management

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

The screenshot shows the 'Modules management' section of the IRIS platform. The sidebar is identical to the previous screenshot. The main area is titled 'Modules management' and displays a table with five entries: IrisIntelOwl, IrisCheck, IrisMISP, IrisVT, and IrisWebHooks. The table has columns for '#ID', 'Module name', 'Has pipeline', 'Module version', 'Interface version', 'Date added', 'Added by', and 'Active'. At the bottom, it says 'Showing 1 to 5 of 5 entries' and includes 'Previous' and 'Next' buttons. Below the table, it says 'Registered hooks'.



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.

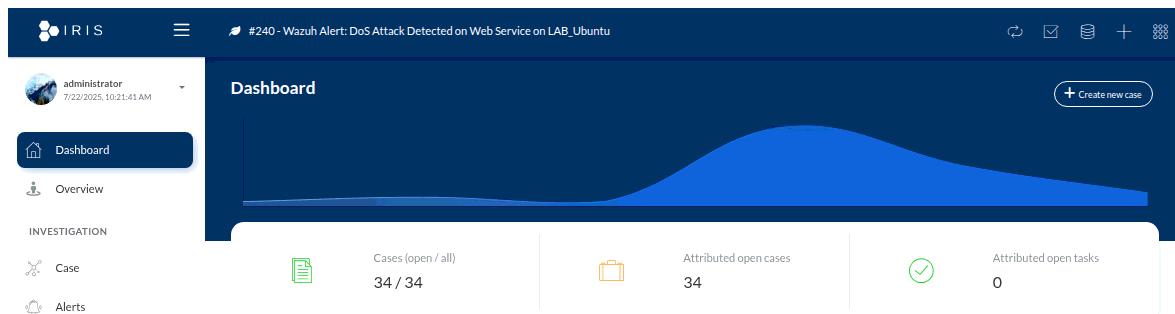
The screenshot shows a user interface for managing report templates. On the left, there's a sidebar with navigation options: DIM Tasks, Manage cases (selected), Advanced (dropdown menu), Modules, Customers, Case Objects, Custom Attributes, Case Templates, Report Templates (selected), Access control, and Server settings. The main area is titled "Report Templates Management". It includes a search bar, a dropdown for "Show 10 entries", and a "Search:" input field. A table lists report templates with columns: Name, Description, Naming format, Date created, Created by, Language, Type, and Download. Below the table, it says "No data available in table". At the bottom, it shows "Showing 0 to 0 of 0 entries" and buttons for "Previous" and "Next".



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.

A screenshot of a 'Create a new case' modal window. The window has a title bar 'Create a new case' with a close button. Inside, there's a note: 'Fields with an asterisk are required.' and 'Access to the case can be granted to other users once the case is created. Users pertaining to the customer will be able to see the case by default.' Below the note are several input fields: 'Select customer *' (a dropdown menu), 'Case name *' (a text input field), 'Select case template' (a dropdown menu), 'Select classification' (a dropdown menu), 'Short description *' (a text input field), and 'SOC ticket ID' (a text input field). In the bottom right corner of the modal, there's a green 'Create' button.



Berikut adalah contoh pengisian form informasi Case.

Create a new case X

Fields with an asterix are required.
Access to the case can be granted to other users once the case is created. Users pertaining to the customer will be able to see the case by default.

Analyst01

Case name * New Case Ransomware

Select case template

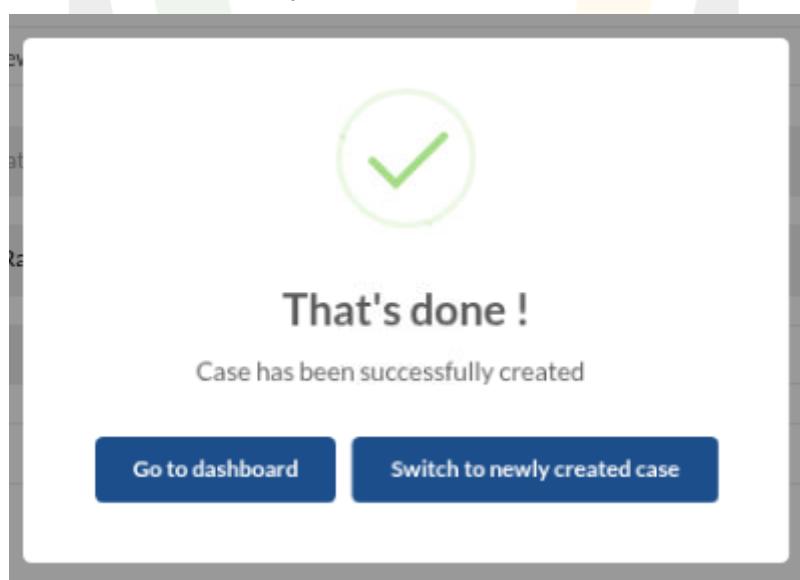
Malicious-Code: Ransomware

Short description * deskripsi

SOC ticket ID

Create

Akan muncul pesan konfirmasi apabila Case berhasil dibuat.





Berikut adalah halaman Case yang baru dibuat.

The screenshot shows the IRIS Case Management interface. On the left, there's a sidebar with navigation links: Dashboard, Overview, INVESTIGATION (with Case selected), Alerts, Search, Activities, DIM Tasks, MANAGE (with Manage cases selected), Advanced, and Help. The main area displays a case summary for '#243 - New Case Ransomware'. The summary includes the case number, opened date (2025-07-22), owner (administrator), classification (Malicious-Code: Ransomware), and a brief description ('deskripsi'). There are tabs for Manage, Processors, and Pipelines, along with buttons for Request review, Generate report, and Activity report. A status bar at the bottom indicates 'Changes saved' and 'Last synced: 10:23:4 AM'.

[Case Management] Update and Enrich Case

Update Case Information

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

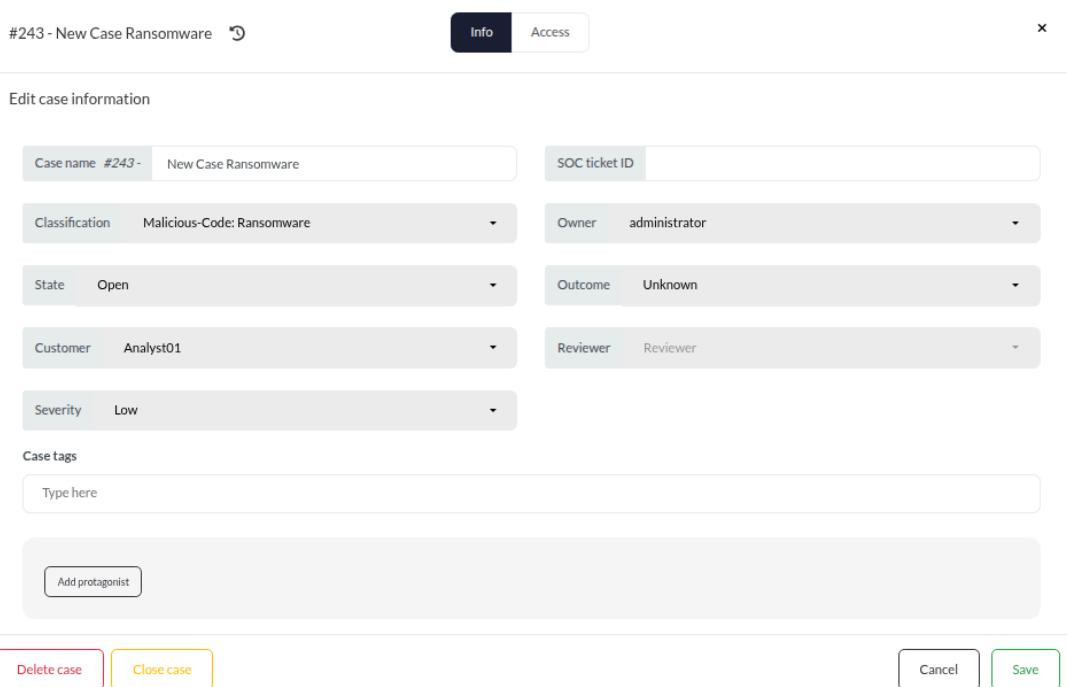
This screenshot is similar to the one above, showing the case summary for '#243 - New Case Ransomware'. The 'Manage' button in the sidebar is highlighted, indicating it has been clicked. The rest of the interface and case details are identical to the first screenshot.

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

The screenshot shows a 'Case Info' pop-up window for case #243. It has tabs for Info and Access. The Info tab is active, displaying 'General info' with fields like Case name, Case description, Customer, Case tags, SOC ID, Case ID, and Case UUID. To the right, there's a section for 'Classification' (malicious-code:ransomware), 'State' (Open), 'Severity' (Low), 'Open date' (2025-07-22), 'Opening user' (administrator), and 'Owner' (administrator). An 'Edit' button is located in the top right corner of this section. At the bottom, there are buttons for 'Delete case' (red) and 'Close case' (yellow).



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



#243 - New Case Ransomware

Info Access X

Edit case information

Case name #243 - New Case Ransomware

SOC ticket ID

Classification Malicious-Code: Ransomware

Owner administrator

State Open

Outcome Unknown

Customer Analyst01

Reviewer Reviewer

Severity Low

Case tags

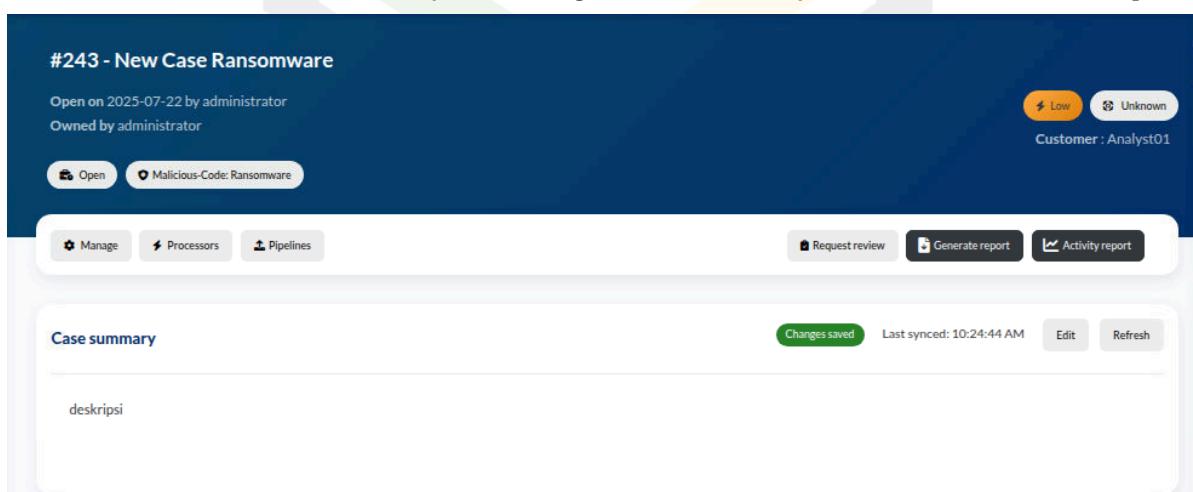
Type here

Add protagonist

Delete case Close case Cancel Save

Summary

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



#243 - New Case Ransomware

Open on 2025-07-22 by administrator
Owned by administrator

Malicious-Code: Ransomware

Severity: Low | Outcome: Unknown
Customer: Analyst01

Open Manage Processors Pipelines Request review Generate report Activity report

Case summary Changes saved Last synced: 10:24:44 AM Edit Refresh

deskripsi

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.

#243 - New Case Ransomware

Summary Notes Assets IOC Timeline Graph Tasks Evidence

Refresh Add assets

Show 10 entries Search:

Name	Type	Description	IP	Compromised	IOC	Tags	Analysis
No data available in table							

Name Type Description IP Compromised IOC Tags Analysis

Showing 0 to 0 of 0 entries Previous Next

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

Add multiple assets

Assets Type *

None

Assets Name *

One asset per line

Description

B I H1 H2 H3 H4 </> ⌂ ⌂ ⌂ ⌂

Domain IP

> Additional information

Compromise Status To be determined Analysis Status Unspecified

Asset tags

Type here

Related IOC

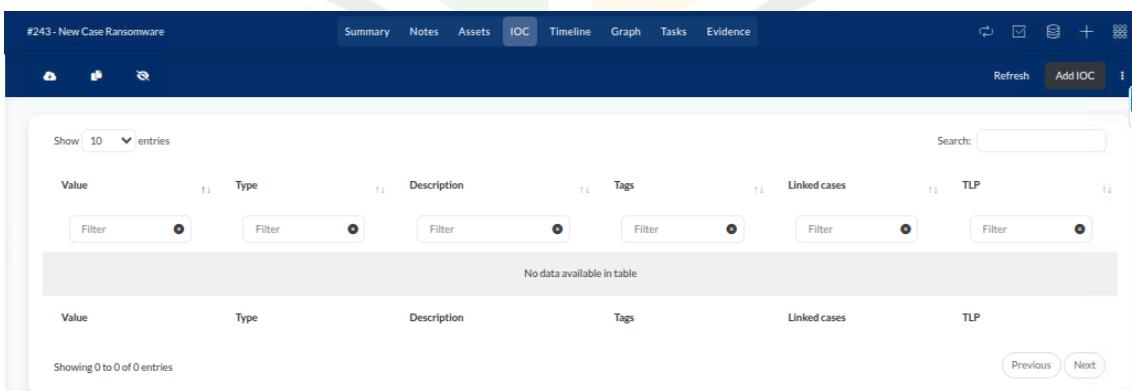


Entitas/Komponen yang dapat dikategorikan dan ditambahkan sebagai Aset pada Case DFIR IRIS diantaranya:

- **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**.



Add IOC

Type *

TLP *

IOC Value *

One IOC per line ⓘ

Description


IOC tags

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 eksloitasi.
 - **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 eksloitasi.
 - **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 persistency atau malware aktif.



Timeline

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

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

Add event

Event Title *

Event Time *

Event description

Event Source

Event tags

Link to assets

Link to IOCs

Event Category

Parent Event ID

Event color

Push IOCs to assets Add to summary Display in graph

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 asset 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**.

Add task

#None

Assigned to *

Select assignee(s)

Status *

Select task status

Task Title *

|

Description

B I H1 H2 H3 H4 ⌂ ⌂ ⌂ ⌂

1

Task tags

Type here

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 penggerjaan.
 - **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.

The screenshot shows the 'Evidence' tab of a software interface. At the top, there are tabs for Summary, Notes, Assets, IOC, Timeline, Graph, Tasks, and Evidence. The Evidence tab is selected. Below the tabs is a toolbar with icons for cloud, file, search, and refresh, followed by a 'Register Evidence' button. The main area contains a table with the following columns: Name, Type, Hash, Size(bytes), Description, and Added by. There are filter dropdowns for each column. A message 'No data available in table' is displayed below the table. At the bottom, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Register evidence' form. It includes fields for Name (with a required asterisk), Type (a dropdown menu labeled 'Evidence type'), Size (bytes) (a text input field), Hash (a text input field), and Description (a rich text editor with a toolbar). Below the rich text editor is a note: 'Locally compute file information by selecting it below. The file is not be uploaded on the server nor saved.' At the bottom, there is a 'Choose File' button with the message 'No file chosen', a 'Process' button, and a large green 'Register' button.



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

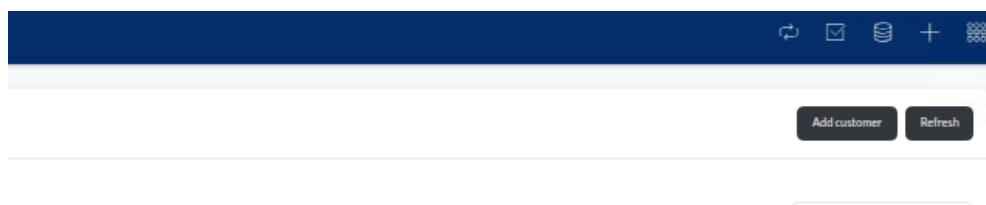
Pada panel sebelah kiri, masuk ke halaman **Advanced → Customer**. Halaman ini menampilkan daftar customer yang ada.

Name	Description
IrisInitialClient	
Analyst01	



Add Customer

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



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

Add customer ×

Name *
SOC Manager

Description

SLAs

Save

Edit & Delete Customer

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

Customers management			
		Add customer Refresh	
Show:	10 entries	Search:	
Name	Description		
Analyst01			
IrisInitialClient			
SOC Manager			
Name	Description		
Showing 1 to 3 of 3 entries		Previous	Next



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

The screenshot shows the 'Customers > SOC Manager (#3)' page. At the top, there are six cards displaying metrics: Current open cases (0), Current month (0), Last month (0), Current year (0), Last year (2024) (0), and Total (0). Below these are sections for Customer name (SOC Manager), Customer Description, Customer SLAs, and Average case duration (0 days). A large 'Edit customer' button is located in the top right corner. Below the main stats are sections for Contacts, Associated Users, Cases, and Assets, each with a 'Manage' button.

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

The screenshot shows the 'Edit customer #3' form. It includes fields for Name (SOC Manager), Description (empty), and SLAs (empty). At the bottom are two buttons: a red 'Delete' button and a green 'Update' button.

[Modules Management] Add Module

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

#ID	Module name	Has pipeline	Module version	Interface version	Date added	Added by	Active
5	IrisIntelOwl		0.1.0	1.2.0	2025-05-14T04:43:29.170360	administrator	
3	IrisCheck		1.0.1	1.2.0	2025-05-14T04:43:28.814871	administrator	
2	IrisMISP		1.3.0	1.2.0	2025-05-14T04:43:28.799932	administrator	
1	IrisVT		1.2.1	1.2.0	2025-05-14T04:43:28.631157	administrator	
4	IrisWebHooks		1.0.8	1.2.0	2025-05-14T04:43:29.157512	administrator	

Akan muncul halaman Module Extension berikut.

Add Module

Module extensions

Iris can be extended with compatible modules. Modules are pip packages providing a specific interface which allows Iris and the module to communicate. Enter below a pip package name already installed.

Ex: iris_evtx

Tips: you can develop your own module by following [this link](#)

Note : Modules are running as the same trust level as Iris. They can thus access all the information stored on Iris as well as run code on the server. Please be cautious and review modules before installing them.

Module name

Validate module

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

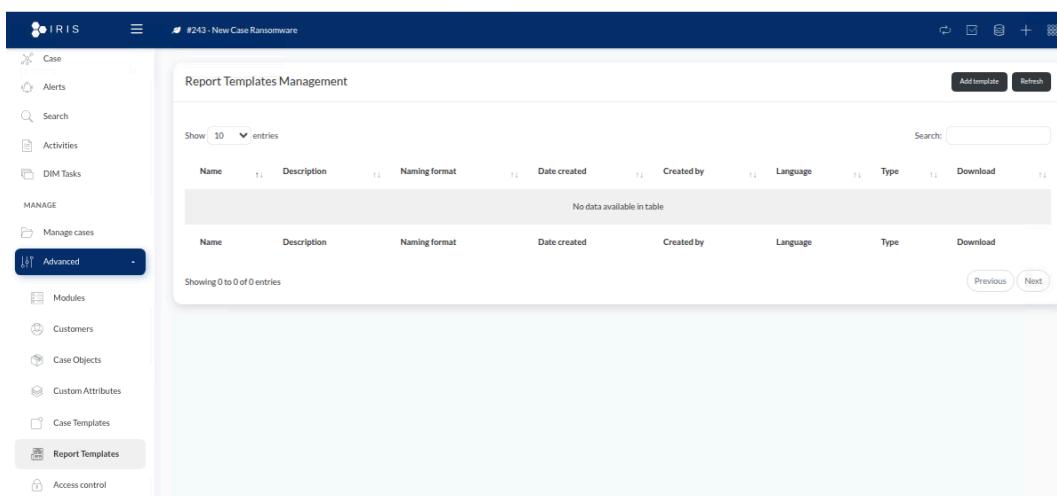
- Contoh: `iris_evtx` (untuk parsing log EVTX), atau modul lain yang sesuai.
- Modul tersebut **harus sudah diinstal** di lingkungan Python IRIS terlebih dahulu.

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

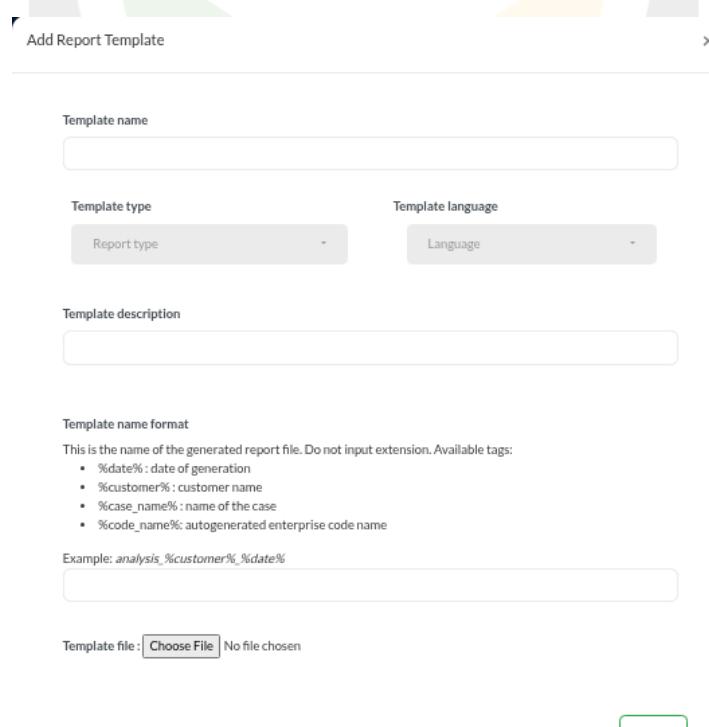
[Report Management] Generate Incident Report

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.



Add Report Template

Template name

Template type

Template language

Template description

Template name format

This is the name of the generated report file. Do not input extension. Available tags:

- %date% : date of generation
- %customer% : customer name
- %case_name% : name of the case
- %code_name% : autogenerated enterprise code name

Example: analysis_%customer%_%date%

Template file : No file chosen

Save

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



Add Report Template

Template name: csirt_report_template

Template type: Investigation

Template language: English

Template description: template laporan CSIRT

Template name format:
This is the name of the generated report file. Do not input extension. Available tags:

- %date% : date of generation
- %customer% : customer name
- %case_name% : name of the case
- %code_name%: autogenerated enterprise code name

Example: analysis_%customer%_%date%

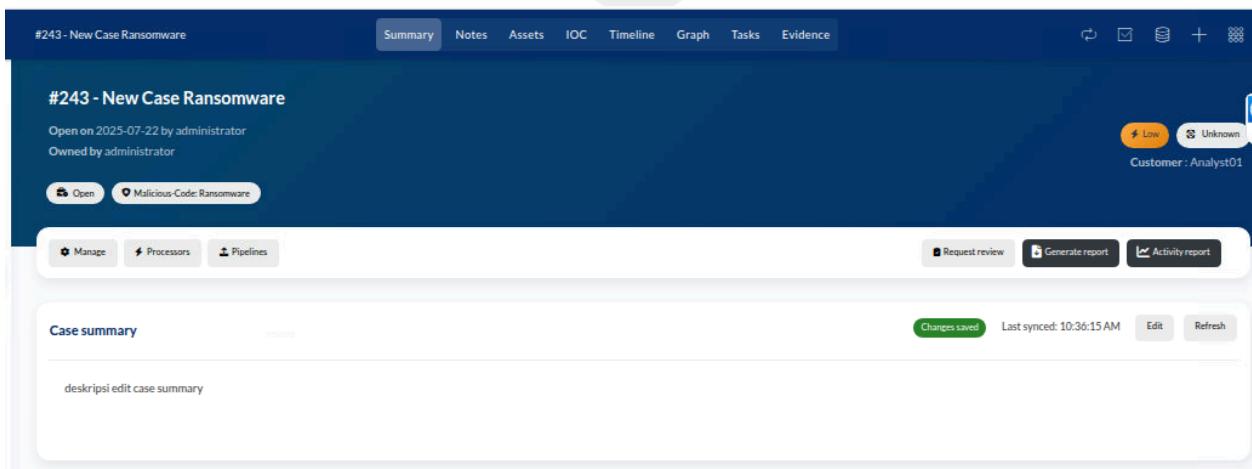
analysis_%customer%_%date%

Template file: Choose File iris_report_template.docx

Save

Generate Report

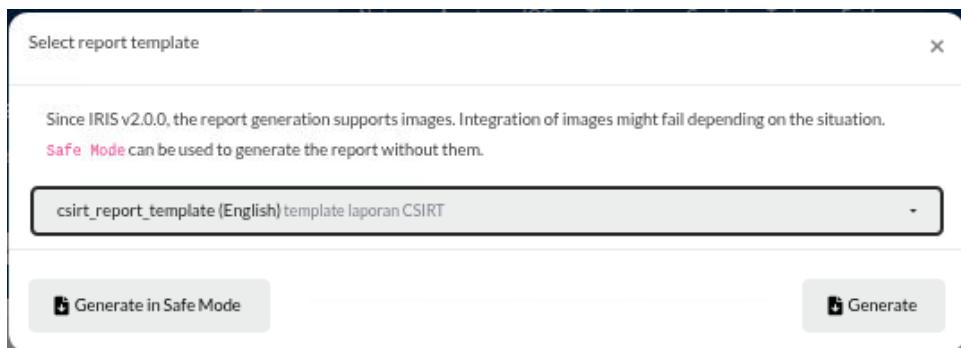
Setelah berhasil mengunggah template, lakukan pembuatan laporan. Pada halaman Case, klik **Generate report** pada bagian kanan atas.



The screenshot shows the IRIS platform interface for a case titled '#243 - New Case Ransomware'. The top navigation bar includes tabs for Summary, Notes, Assets, IOC, Timeline, Graph, Tasks, and Evidence. On the right side of the header, there are status indicators for 'Low' and 'Unknown' risks, and a note that the case is owned by 'Analyst01'. Below the header, there are buttons for 'Open', 'Malicious-Code: Ransomware', 'Manage', 'Processors', and 'Pipelines'. A 'Request review' button is also present. The main content area displays a 'Case summary' section with a text input field containing 'deskripsi edit case summary'. At the bottom right of this section, there are buttons for 'Changes saved', 'Last synced: 10:36:15 AM', 'Edit', and 'Refresh'. A decorative graphic of overlapping green and yellow triangles is visible behind the main content area.



Pilih template report yang akan digunakan.



Report akan otomatis terunduh dengan ekstensi .docx





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.

The screenshot shows the MISP web interface with a dark-themed header bar containing links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, Bookmarks, MISP (highlighted with a star), and Admin. The main content area has a left sidebar with sections for List Events (Add Event, Import from..., REST client), List Attributes, Search Attributes, View Proposals, Events with proposals, View delegation requests, View periodic summary, Export, and Automation. The main panel displays a table titled "Events" with columns for Creator org, Owner org, ID, Clusters, and Tags. The table lists 19 rows of event data, each with a checkbox, a delete icon, and a link like "ORNAME ? 1809". A search bar at the top right allows entering values to search. At the bottom of the page, there are download links for "Server PGP public key" and a note: "This is an initial install Powered by MISP 2.4.209 Please configure and harden accordingly - 2025-08-03 02:20:43".

Fitur

The screenshot shows the MISP web interface with a dark-themed header bar containing links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. The main content area has a section titled "Events" in red. Below it, a large paragraph describes the purpose of the Events feature: "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**."



Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks MISP Admin

List Events Add Event Import from... REST client

List Attributes Search Attributes

View Proposals Events with proposals View delegation requests View periodic summary

Export Automation

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

	Creator org	Owner org	ID	Clusters	Tags
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1809		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1808		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1807		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1806		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1805		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1804		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1803		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 1802		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	ORGNAME	ORGNAME	? 1801		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	ORGNAME	ORGNAME	? 1800		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1799		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1798		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"
<input type="checkbox"/>	x ORGNAME	ORGNAME	? 1797		<input checked="" type="checkbox"/> osint:source-type="block-or-filter-list"

Download: Server PGP public key This is an initial install Powered by MISP 2.4.209 Please configure and harden accordingly - 2025-08-03 02:20:43

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**.

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks MISP Admin

List Events Add Event Import from... REST client

List Attributes Search Attributes

View Proposals Events with proposals View delegation requests View periodic summary

Export Automation

Attributes

« previous next »

Date	Event	Org	Category	Type	Value	Tags	Galaxies
2015- 07-28	1	CthulhuSPRL.be	External analysis	link	http://www.symantec.com/connect/blogs/black-vine-formidable-cyberespionage-group-targeted-aerospace-healthcare-2012	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2015- 07-28	1	CthulhuSPRL.be	External analysis	link	http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2015- 07-28	1	CthulhuSPRL.be	External analysis	text	Black Vine	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2015- 07-28	1	CthulhuSPRL.be	Network activity	domain	ameteksen.com	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2015- 07-28	1	CthulhuSPRL.be	Network activity	hostname	asconline.wellpoint.com	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2015- 07-28	1	CthulhuSPRL.be	Network activity	domain	assso.net	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Download: Server PGP public key This is an initial install Powered by MISP 2.4.209 Please configure and harden accordingly - 2025-08-03 02:22:58

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**.

The screenshot shows the 'Tags' page in the MISP interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, Bookmarks, MISp, Admin, and a user icon. On the left, there's a sidebar with 'List Favourite Tags' and buttons for 'List Tags' (which is selected) and 'Add Tag'. The main content area has a title 'Tags' and a search bar. Below is a table with columns: ID, Exportable, Hidden, Local Only, Name (sorted by name), Restricted to org, Restricted to user, Taxonomy, events, and attrib. The table lists 13 tags:

ID	Exportable	Hidden	Local Only	Name	Restricted to org	Restricted to user	Taxonomy	events	attrib
462	✓	✗	✗	malware_classification:malware-category="Botnet"	✗	✗		4	0
377	✓	✗	✗	C2	✗	✗		1	25
412	✓	✗	✗	Cobalt Strike Beacon	✗	✗		1	1
406	✓	✗	✗	DLL Dropper	✗	✗		0	10
409	✓	✗	✗	Decoy	✗	✗		0	1
410	✓	✗	✗	Docx	✗	✗		0	1
405	✓	✗	✗	Download	✗	✗		0	10
496	✓	✗	✗	Flash	✗	✗		1	1
922	✓	✗	✗	Malicious Batch Script	✗	✗		1	0
925	✓	✗	✗	Ransomware	✗	✗		2	0
373	✓	✗	✗	Smoke Loader	✗	✗		1	3
923	✓	✗	✗	VBS Downloader	✗	✗		1	0

At the bottom, there are links for 'Download: Server PGP public key' and 'This is an initial install Powered by MISp 2.4.209 Please configure and harden accordingly - 2025-08-03 02:23:21'.



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.

The image contains two screenshots of the MISP web interface. The top screenshot shows the 'REST client' section of the 'OpenAPI' tab. It includes fields for 'HTTP method to use' (set to GET), 'Relative path to query' (empty), and 'HTTP headers' (containing Authorization: YOUR_API_KEY, Accept: application/json, Content-type: application/json). The bottom screenshot shows the 'MISP Automation API (2.4)' documentation page, which provides instructions for generating an API key and includes a note about its display. Both screenshots include a navigation bar at the top with links like Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, Bookmarks, MISp, and Admin.





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**.

The screenshot shows the 'Feeds' section of the MISP interface. On the left, there's a sidebar with links like 'List Feeds', 'Search Feed Caches', 'Add Feed', 'Import Feeds from JSON', 'Feed overlap analysis matrix', and 'Export Feed settings'. The main area has tabs for 'Default feeds', 'Custom feeds', 'All feeds' (which is selected), and 'Enabled feeds'. Below these tabs is a table listing eight feeds:

ID	Enabled	Caching	Name	Format	Provider
1	✓	✗	CIRCL OSINT Feed	misp	CIRCL
2	✓	✗	The Botvrij.eu Data	misp	Botvrij.eu
3	✓	✗	ELLIOT: IP Feed (Community version)	freetext	elliotech
4	✓	✗	blockrules of rules.emergingthreats.net	csv	rules.emergingthreats.net
5	✓	✗	Tor exit nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL" feed.
6	✓	✗	Tor ALL nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed.
7	✓	✗	cybercrime-tracker.net - all	freetext	cybercrime-tracker.net
8	✓	✗	Phishtank online valid phishing	csv	Phishtank

At the bottom of the page, there are two status messages: 'Download: Server PGP public key' and 'This is an initial install Powered by MISP 2.4.209 Please configure and harden accordingly - 2025-08-03 02:24:36'.

Fungsi

Add MISP Events

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

The screenshot shows the 'Add Event' form. On the left, there's a sidebar with links for 'List Events', 'Add Event' (which is selected), 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'View periodic summary', 'Export', and 'Automation'. The main form has fields for 'Date' (set to 2025-08-03), 'Distribution' (set to 'Your organisation only'), 'Threat Level' (set to 'Medium'), 'Analysis' (set to 'Initial'), 'Event Info' (containing 'Event by Wazuh Alert'), and 'Extends Event' (containing 'Event UUID or ID. Leave blank if not applicable'). At the bottom is a 'Submit' button.

Add Tags to Events

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

The screenshot shows the Wazuh interface for managing events. On the left, there's a sidebar with various navigation options like 'View Event', 'Edit Event', and 'Add Attribute'. The main area displays an event titled 'Event by Wazuh Alert' with details such as Event ID (1810), UUID (806c679a-fbb1-4e77-b334-0974151f14d5), Creator org (ORNAME), and Owner org (ORNAME). A 'Protected Event' section indicates the event is in unprotected mode. The 'Tags' field contains two entries: 'tipp:amber' and 'tipp:yellow'. A 'Warnings' section provides a note about the event having neither attributes nor objects, which is common for certain types of events. Below this, a modal window titled 'Add a tag' is open, showing tabs for 'Tag Collections', 'Custom Tags', and 'All Tags'. The 'Custom Tags' tab is selected, and the input field contains 'tipp:amber'. A 'Submit' button is visible at the bottom right of the modal.

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.

The screenshot shows the 'Add Attribute' page in the MISP interface. The left sidebar has a blue highlight over 'Add Attribute'. The main form fields include:

- Category:** (choose one) dropdown
- Type:** (choose category first) dropdown
- Distribution:** Inherit event dropdown
- Value:** Text input field
- Contextual Comment:** Text input field
- Checkboxes:** Batch import, For Intrusion Detection System, Disable Correlation
- Date/Time Fields:** First seen date, Last seen date, First seen time, Last seen time. Each has a calendar icon and a dropdown for time format (HH:MM:SS.ssssss+TT:TT).

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.

The screenshot shows the MISP web interface with a navigation bar at the top containing links like Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, Bookmarks, and a MISP logo. On the left, there's a sidebar with links for List Feeds, Search Feed Caches, Add Feed (which is selected), Import Feeds from JSON, Feed overlap analysis matrix, and Export Feed settings. The main content area has a title 'Add MISP Feed' and a sub-instruction 'Add a new MISP feed source.' Below this are several input fields and dropdown menus:

- Enabled (checkbox)
- Caching enabled (checkbox)
- Lookup visible (checkbox)
- Disable correlation (checkbox)
- Unpublish events (checkbox)
- Name (text input field labeled 'Feed name')
- Provider (text input field labeled 'Name of the content provider')
- Input Source (dropdown menu currently set to 'Network')
- URL (text input field labeled 'URL of the feed')
- Source Format (dropdown menu currently set to 'MISP Feed')
- Any headers to be passed with requests (for example: Authorization) (text input field labeled 'Line break separated list of headers in the "headername: value" format')

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.





Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks Admin MISP

List Events Add Event Import from... REST client

List Attributes **Search Attributes**

View Proposals Events with proposals View delegation requests View periodic summary

Export Automation

Search Attribute

You can search for attributes based on contained expression within the value, event ID, submitting organisation, category and type. For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To exclude things from a result, use the NOT operator (!) in front of the term. For string searches (such as searching for an expression, tags, etc) - lookups are simple string matches. If you want a substring match encapsulate the lookup string between "%" characters.

Containing the following expressions
46.8.10.134

Having tag or being an attribute of an event having the tag

Being attributes of the following event IDs, event UUIDs or attribute UUIDs

From the following organisation(s)

Type i Category i
ALL ALL

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

Attributes

« previous next »

Search

Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Events	hits	IDS	Distribution	Sightings	Activity	Actions
2024-07-19	1329	Network activity	ip-dst	46.8.10.134										Inherit event	(0/0/0)	

« previous next »

Download results as json Download

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

The screenshot shows the VirusTotal website's home page. At the top, there is a search bar with the placeholder "URL, IP address, domain or file hash". Below the search bar is the VirusTotal logo, which consists of a blue square with a white Greek sigma symbol followed by the word "VIRUSTOTAL" in blue capital letters. A sub-instruction below the logo reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches; automatically share them with the security community." There are three tabs at the top: "FILE" (which is underlined), "URL", and "SEARCH". Below these tabs is a file upload area with a "Choose file" button. A small note below the file input says: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the [sharing of your sample submission with the security community](#). Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)." At the bottom of the page, there is a link: "Want to automate submissions? Check our API, or access your API key." On the right side of the page, there is a blue circular icon with a white outline of a person's head.





IoC Analysis

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

The screenshot shows the Virustotal analysis page for the file hash 178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1. The main summary indicates that 58 out of 72 security vendors flagged the file as malicious. The file is identified as an EXE file, 208.00 KB in size, and was last analyzed 5 days ago. Threat categories listed include peexe, detect-debug-environment, spreader, idle, long-sleeps, direct-cpu-clock-access, runtime-modules, and checks-user-input. Below this, a table lists vendor detections:

Vendor	Result	Category
AhnLab-V3	Malware/Win32.Generic.C.4094147	Alibaba
AliCloud	Trojan/Win/Zenpak.GC12KJC	ALYac
Arcabit	Trojan/Grafor.DB45BD	Arctic Wolf
Avast	Win32:MalwareX.gen [Tr]	AVG
Avira (no cloud)	HEUR/AGEN.1311213	BitDefender
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon

Fungsi

Periksa API Key Virustotal

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

The screenshot shows the user profile menu for Putra Aditya. The 'API Key' option is highlighted in the list, which also includes Profile, Settings, and Sign Out.





This screenshot shows the VirusTotal API key page. At the top, it says "API KEY" and provides a personal key for submission. Below that, it states: "This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the sharing of your Sample submissions with the security community. Please do not submit any personal information; we are not responsible for the contents of your submissions. [Learn more](#)". A "Upgrade API" button is available.

The next section, "API QUOTA ALLOWANCES FOR YOUR USER", indicates a standard free end-user account with the following limits:

- Access level: **Limited**, standard free public API. Upgrade to premium.
- Usage: **Must not be used in business workflows, commercial products or services.**
- Request rate: 4 lookups / min
- Daily quota: 500 lookups / day
- Monthly quota: 15.5 K lookups / month

Below these, there are links to "Go premium", "Use in browser", "Discover feeds", and "Other services". There is also a note: "Want to learn more about how our intelligence can supercharge your security operations? check our 360 overview brief." and a "Want to upgrade your access?" contact link.

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.

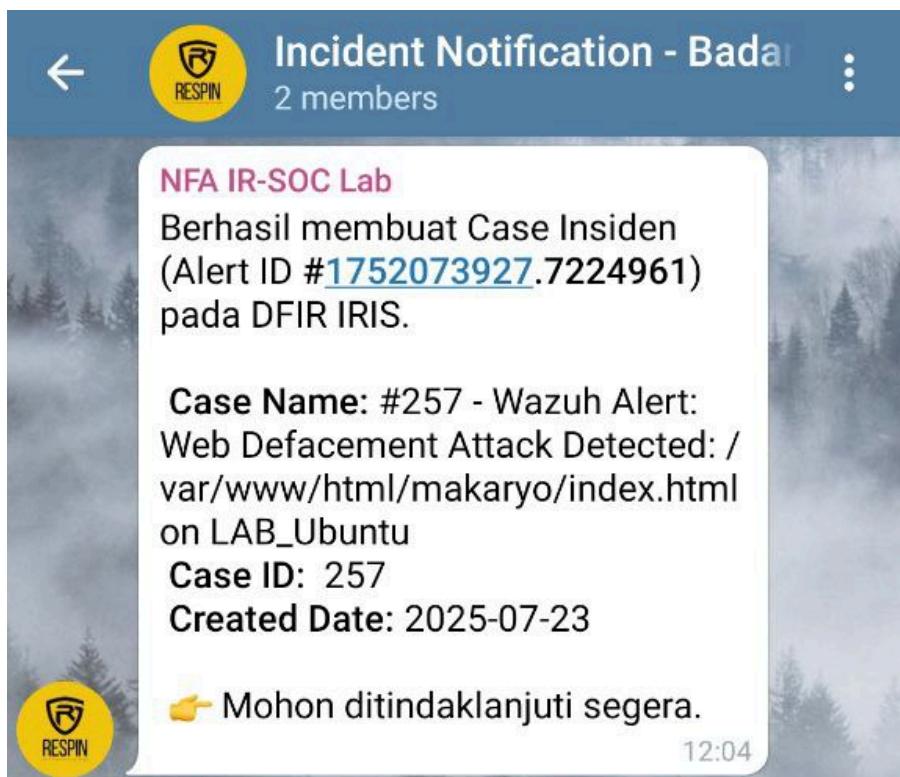
This screenshot shows the configuration interface for a "Get a hash report" node in Node-RED. The node has the following settings:

- Name: Filehash_Analysis
- Delay: 0
- Action: Get a hash report
- Authenticating: Authenticate Virustotal v3
- Fields:
 - Apikey *: An input field containing a redacted API key.
 - Url *: An input field containing the URL <https://www.virustotal.com>.
 - Id *: An input field containing the expression `$exec.all_fields.syscheck.sha256`.



Telegram BOT (Notifikasi)

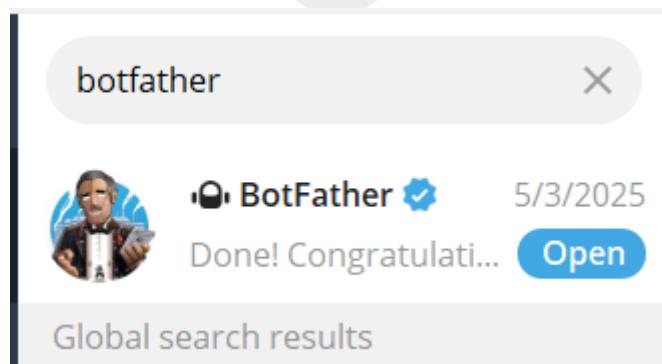
Telegram Bot digunakan untuk mengirimkan notifikasi insiden siber secara otomatis dan *realtime*.



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.



Done! Congratulations on your new bot. You will find it at t.me/NFAvLab_bot. You can now add a description, about section and profile picture for your bot, see [/help](#) for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:
`7716258220:XXXXXXXXXXXXXX`

Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

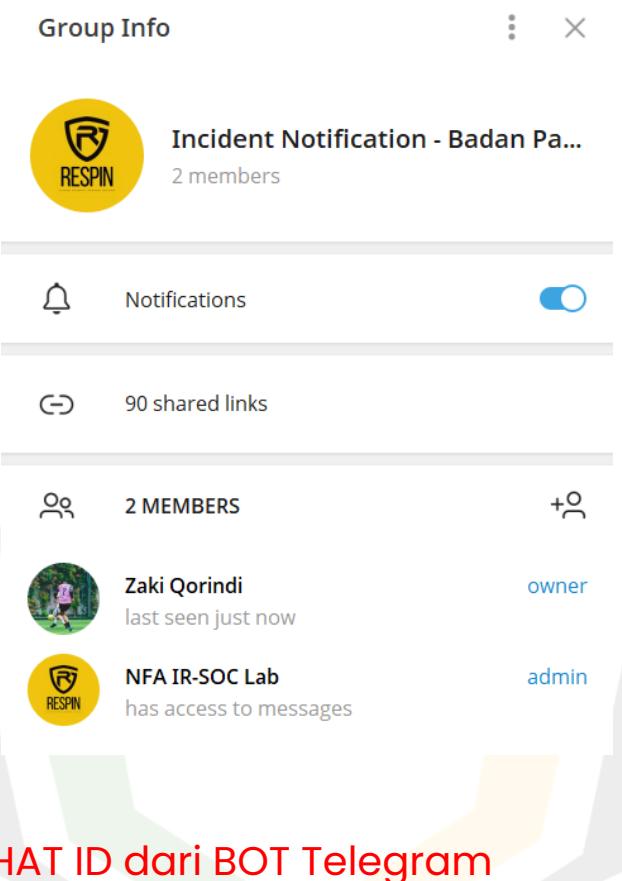
For a description of the Bot API, see this page:
<https://core.telegram.org/bots/api>

10:20 AM



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.



```
ok: true
result:
  0:
    update_id: 463238881
    message:
      message_id: 553
      from:
        id: 1345762863
        is_bot: false
        first_name: "Zaki Qorindi"
        username: "zakiqorindi"
        language_code: "en"
      chat:
        id: -4715 [REDACTED]
        title: "Incident Notification - Badan Pangang CSIRT"
        type: "group"
```

API Usage & Setting

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



The image shows two screenshots of the Shuffle app interface. The left screenshot displays the 'Post send message' configuration screen. It includes fields for 'Name' (Set to 'Send_Alert_Notification'), 'Delay' (Set to '0'), 'Find Actions' (Set to 'Send message'), 'Url' (Set to 'https://api.telegram.org'), and 'Api token' (Set to '7716258220:AAEiOTMahVln75Kv'). Below these, tabs for 'Simple' and 'Advanced' are visible. The right screenshot shows the expanded 'Send message' action configuration, revealing the message template: '**Wazuh Alert Detected** (#\$exec.all_fields.id)
Description: \$exec.all_fields.rule.description'. The 'Chat id' field is also visible, showing a redacted value.



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

