LAPORAN

PRAKTEK KERJA LAPANGAN

PERANCANGAN TOOLS MULTI CYBER THREAT INTELLIGENCE MENGGUNAKAN PYTHON DI PT TIRTA NAWASENA TEKNOLOGI

MUHAMMAD ILHAM SUTAMA

2207421028

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

DEPOK

2025

HALAMAN PENGESAHAN LAPORAN
PRAKTIK KERJA LAPANGAN

a.	Judul	: Perancangan Tools Multi Cyber Threat Intelligence Menggunakan Python Di PT Tirta Nawasena Teknologi
b.	Penyusun	
	1) Nama	: Muhammad Ilham Sutama
	2) NIM	: 2207421028
c.	Program Studi	: Teknik Multimedia dan Jaringan
d.	Jurusan	: Teknik Informatika dan Komputer
e.	Waktu Pelaksanaan	: 21 Juli 2025 – 31 Desember 2025
f.	Tempat Pelaksanaan	: PT TirtaNawasena Technology
g.	Alamat Pelaksanaan	: Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec.Serpong Utara, Kota Tangerang Selatan, 15323.

Depok, 31 Desember 2025

Pembimbing PNJ	Pembimbing Perusahaan
Asep Kurniawan, S.Pd., M.Kom.	Nasrullah.
NIP. 199109262019031012	

Mengesahkan,
KPS Teknik Multimedia dan Jaringan

Dr. Indra Hermawan, S.Kom., M.Kom.
NIP. 198703132019031012

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan Praktik Kerja Lapangan ini. Penulisan laporan Praktik Kerja Lapangan ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik.. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Orang tua dan keluarga saya yang telah memberikan bantuan dukungan moral dan material;

b. Bpk. Asep Kurniawan, S.Pd., M.Kom, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan Praktik Kerja Lapangan ini;

c. Dr. Indra Hermawan, S.Kom., M.Kom., selaku Kepala Program Studi Teknik Multimedia dan Jaringan yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan Praktik Kerja Lapangan ini;

d. Pihak PT Tirta Nawasena Teknologi Divisi SOC (Security Operation Center) khususnya kepada Pak Nasrullah selaku mentor saya selama magang dan juga Mas Franz Davidson yang telah banyak membantu dalam usaha memperoleh data yang penulis perlukan;

e. Sahabat dan rekan-rekan seperjuangan dari TMJ Angkatan 2022 yang telah membantu dalam penyusunan laporan Praktik Kerja Lapangan ini.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan Praktik Kerja Lapangan ini membawa manfaat bagi pengembangan ilmu.

Depok, 31 Desember 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang Kegiatan

Dalam era digitalisasi yang berkembang pesat dan luas, keamanan jaringan menjadi aspek penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data di suatu sektor usaha. Seiring dengan peningkatan *cybercrime* yang berpotensi menyebabkan pencurian identitas, kerugian operasional, dan gangguan infrastruktur kritis (Hidayat, Widiyasono and Gunawan, 2025), diperlukan langkah mitigasi yang tepat. Merespons hal tersebut, PT Semen Indonesia Group bekerja sama dengan PT Tirta Nawasena dalam menyediakan fungsi pengawasan, analisis, dan respons melalui tim *SOC (Security Operation Center)*.

Dalam menangani kompleksitas dan intensitas serangan yang terjadi, tim *SOC* dibantu oleh platform keamanan siber berbasis cloud yaitu *XDR Tehtris* dan *CrowdStrike*. Kedua platform ini mengirimkan notifikasi keamanan saat sistem terindikasi melakukan perilaku yang mencurigakan. Indikator dapat berupa artefak digital seperti alamat IP yang mencurigakan, *hash file malware*, pola lalu lintas jaringan yang tidak biasa, atau perilaku pengguna yang tidak wajar. Indikator akan dianalisis skor reputasinya secara manual dan diekskalasi kepada tim *Helpdesk* untuk dilakukan tindakan lebih lanjut berupa pemblokiran *hash file*, alamat IP, dan *domain berbahaya.*

Dewasa ini, tim *SOC* menggunakan berbagai platform *Cyber Threat Intelligence* (*CTI)* seperti *Cyfirma, VirusTotal, CTX,* dan *OTX (AlienVault)* untuk mendapatkan informasi ancaman yang akurat dan terkini. Namun, proses analisis indikator secara manual memakan waktu lama sehingga waktu respons dapat melebihi *SLA (Service Level Agreement)* 30 menit. Keadaan ini dapat mengurangi efisiensi dan dapat memperbesar risiko ancaman.

Dalam rangka memenuhi kebutuhan *SLA* yang diharapkan guna menjamin integritas data, mempercepat deteksi serangan siber, dan mencegah insiden di masa mendatang, penulis memilih judul "Perancangan Tools Multi Cyber Threat Intelligence Menggunakan Python Di PT Tirta Nawasena Teknologi" sebagai

laporan proyek kerja lapangan. Proyek ini menjadi bagian penting dalam meningkatkan performa, efisiensi, dan keamanan pada infrastruktur IT perusahaan.

1.2 Ruang Lingkup Kegiatan

Ruang lingkup kegiatan Praktik Kerja Lapangan (PKL) di PT Tirta Nawasena Teknologi mencakup berbagai aktivitas dalam divisi Security Operation Center (SOC) yang berperan dalam memantau, menganalisis, serta menanggapi berbagai ancaman siber terhadap sistem perusahaan. Selama pelaksanaan magang, mahasiswa berpartisipasi dalam kegiatan pemantauan jaringan menggunakan platform keamanan seperti Tehtris, CrowdStrike, dan Cyfirma, serta melakukan analisis terhadap indikator ancaman (Indicator of Compromise/IoC) dengan memanfaatkan sumber data dari berbagai layanan Cyber Threat Intelligence (CTI) seperti VirusTotal, OTX, dan CTX. Selain itu, mahasiswa juga berkontribusi dalam perancangan *tools* analisis ancaman siber berbasis Multi-CTI API untuk mempercepat proses verifikasi indikator serta meningkatkan efektivitas kerja tim SOC.

1.3 Waktu dan Tempat Pelaksanaan

Adapun waktu dan tempat pelaksanaan praktek kerja lapangan adalah sebagai berikut:

a. Tempat dan pelaksanaan	: Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec. Serpong Utara, Kota Tangerang Selatan, Banten 15323.
b. Penempatan	: Divisi *SOC (Security Operation Center) – SOC Analyst.*
c. Waktu Pelaksanaan	: 21 Juli – 31 Desember 2025.
d. Lama PKL	: 6 Bulan.

1.4.1 Tujuan

Adapun tujuan dari kegiatan ini adalah:

a. Merancang Tools Multi Cyber Threat Intelligence Menggunakan Python Di Pt Tirta Nawasena Teknologi.
b. Menganalisis Tools Multi Cyber Threat Intelligence Menggunakan Python Di Pt Tirta Nawasena Teknologi.

1.4.2 Kegunaan

Adapun kegunaan perancangan dari kegiatan ini adalah:

a. Mempermudah proses pengumpulan skor reputasi secara langsung dari 4 vendor CTI yang digunakan di lingkungan perusahaan (VirusTotal, OTX, CTX, dan Abuse IPDB) menggunakan *tools Multi-CTI.*
b. Mempermudah menganalisis ancaman siber sesuai dengan playbook SOC L1 pada perusahaan, melalui platform keamanan siber *XDR Tehtris* dan *Crowdstrike*.

BAB II
LANDASAN TEORI

2.1 *CTI - Cyber Threat Intelligence*

Cyber Threat Intelligence (CTI) menjadi salah satu pilar keamanan siber yang memungkinkan organisasi untuk secara aktif mendeteksi, mengevaluasi, dan menangani ancaman siber yang muncul. (Soumik *et al.*, 2024)

2.2 *API - Aplicaiton Programming Interface*

Aplicaiton Programming Interface adalah antarmuka untuk entitas perangkat lunak yang dapat digunakan kembali yang digunakan oleh beberapa klien di luar organisasi pengembang, dan dapat didistribusikan secara terpisah dari kode lingkungan (Agil Maulana Nanda Riady, Paniran Paniran and I Made Budi Suksmadana, 2024).

2.3 *IOC – Indicator of Compromise*

Indicator of Compromise adalah artefak forensik yang keberadaannya di dalam suatu sistem merupakan indikator bahwa ada sesuatu yang tidak semestinya (tidak tepat) terjadi dalam sistem tersebut(Asiri *et al.*, 2023). Click or tap here to enter text. Dalam praktik nyata IOC dapat berupa beberapa indikator seperti file hash, IP, dan domain.

2.4 *XDR - Extended Detection and Response*

Extended Detection and Response adalah kategori arsitektur keamanan yang mengintegrasikan tools keamanan ke semua *security-layers* mulai dari *human-layers*, endpoints, email, networks, apps, dan cloud . XDR menyediakan data komprehensif dan kontekstual yang berguna untuk mencegah ancaman, memantau perilaku, mendeteksi, dan mengatasi insiden yag terjadi dengan lebih mudah (Kaur *et al.*, 2024).

2.5 VirusTotal

VirusTotal adalah layanan online yang dapat menganalisis file, IP, dan URL mencurigakan untuk mendeteksi jenis malware dan konten berbahaya menggunakan mesin antivirus dan pemindai situs web. VirusTotal memeriksa item menggunakan lebih dari 70 mesin antivirus dan memiliki VirusTotal Community sebagai jaringan yang memungkinkan berbagi catatan satu sama lain.

Gambar 2. 1 VirusTotal

(Sumber: https://www.virustotal.com/gui/home/upload)

2.6 OTX – Level Blue

Open Threat Exchange (OTX), adalah platform *opensource* untuk berbagi informasi ancaman siber, yang kini dikelola oleh LevelBlue. Data ancaman dikemas dan didistribusikan dalam bentuk laporan yang disebut "Pulse" yang berisi konteks ancaman (seperti jenis malware atau pelaku) beserta daftar IOC terkait, yang dapat mencakup alamat IP, domain, hash file, atau bahkan informasi jaringan seperti ASN (*Autonomous System Number*).

Gambar 2. 2 OTX – Alienvault

(Sumber: https://otx.alienvault.com)

2.7 CTX.io

Cyber Threat eXchange (CTX) adalah platform analisis ancaman siber dari SANDS Lab Co., Ltd. asal Korea Selatan yang menilai reputasi IP, domain, URL, dan file hash dengan indikator malicious atau normal.

Gambar 2. 3 CTX.io

(Sumber: https://www.ctx.io/about/open-source)

2.8 Abuse IPDB

Abuse IPDB adalah *tools* analisis ancaman siber yang bekerja sebagai *community-based IP blacklist database. Tools* ini memiliki spesialisasi dalam dokumentasi dan pemblokiran IP *malicious* yang berpotensi mengandung ancaman siber. Abuse IPDB bekerja dengan cara mengumpulkan laporan ancaman dari komunitas global mengenai IP *address* yang terlibat dalam berbagai tipe penyalahgunaan.

Gambar 2. 4 Abuse IPDB

(Sumber: https://www.abuseipdb.com/)

2.9 Flask

Flask adalah *microframework* web Python yang ringan, fleksibel, dan minimalis. Ia menyediakan dasar-dasar seperti *routing* URL dan *rendering template* HTML, memberikan developer kebebasan penuh untuk menambahkan fitur lain (seperti database) sesuai kebutuhan (Suraya and Sholeh, 2022).

Gambar 2. 5 Flask

(Sumber: https://flask.palletsprojects.com/en/stable/)

2.10 Python

Python merupakan bahasa pemrograman yang berorientasi objek, terinterpretasi, dan interaktif. Python menawarkan struktur data tingkat tinggi seperti daftar, tuple, himpunan, array asosiatif (disebut kamus), tiping dinamis dan pengikatan, modul, kelas, pengecualian, serta pengelolaan memori otomatis (Dhruv, Patel and Doshi, 2022).

Gambar 2. 6 Python
(Sumber: https://www.python.org/)

2.11 XDR Tehtris

Extended Detection and Response Tehtris merupakan platform keamanan *cyber* yang menyatukan berbagai model pertahanan seperti EDR, SIEM, dan Honeypots kedalam satu konsol tunggal. Didukung oleh kecerdasan buatan bernama CYBERIA, yang secara otomatis dapat mendeteksi, menganalisis, dan menetralkan ancaman cyber secara *realtime.*

Gambar *2. 7 Tehtris*
(Sumber: https://tehtris.com/en/company/)

2.12 Crowdstrike

Crowdstrike merupakan platform keamanan siber yang menyatukan berbagai model pertahanan seperti EDR, SIEM, dan Honeypots kedalam satu konsol tunggal. Crowdstrike menggunakan Falcon Exposure Management dan Falcon Cloud Security secara Bersama-sama mendeteksi kerentanan.(‘ebook-2025-MITRE’, 2025)

Gambar 2. 8 Crowdstrike

(Sumber: https://www.crowdstrike.com/en-us/)

2.13 Flowchart

Flowchart dapat didefinisikan sebagai serangkaian langkah untuk memecahkan masalah yang diwakili oleh simbol-simbol khusus. *Flowchart* atau diagram alir ini menggambarkan logika alur program. Diagram alir tidak hanya digunakan sebagai saranakomunikasi, tetapi juga sebagai panduan. Sebelum komponen-komponen dapat dipahami dengan lebih baik.*(Tarsini, 2024)*

Table 1. Symbol and Function Algorithm

No.	Symbol	Name	Function
1		*"Terminal"*	Awal atau akhir dari suatu program (Prosedur).
2		*"Output/Input"*	Proses input atau output
3		*"Process"*	Proses operasional komputer
4		*"Decision"*	Menunjukkan bahwa kondisi tertentu mengarah ke dua kemungkinan, ya/ tidak
5		*"Connector"*	Menghubungkan proses penghubung ke proses lain di halaman yang sama
6		*"Offline Connector"*	Koneksi yang menghubungkan dari satu proses ke proses lain di halaman lain.
7		*"Predefined Process"*	Menunjukkan syarat penyimpanan untuk pemrosesan guna memberikan harga awal
8		*"Punched Card"*	Masukan berasal dari kartu atau keluaran ditulis ke kartu
9		*"Punch Tape"*	input / output yang menggunakan pita berlubang
10		*"Document"*	Cetak keluaran dalam format dokumen (melalui printer)
11		*"Flow"*	Menyatakan jalur alur suatu proses

Explore flowchart and pseudocode concepts in algorithms and programming

Gambar 2. 9 Penjelasan simbol flowchart menurut jurnal

BAB III

HASIL KEGIATAN MAGANG

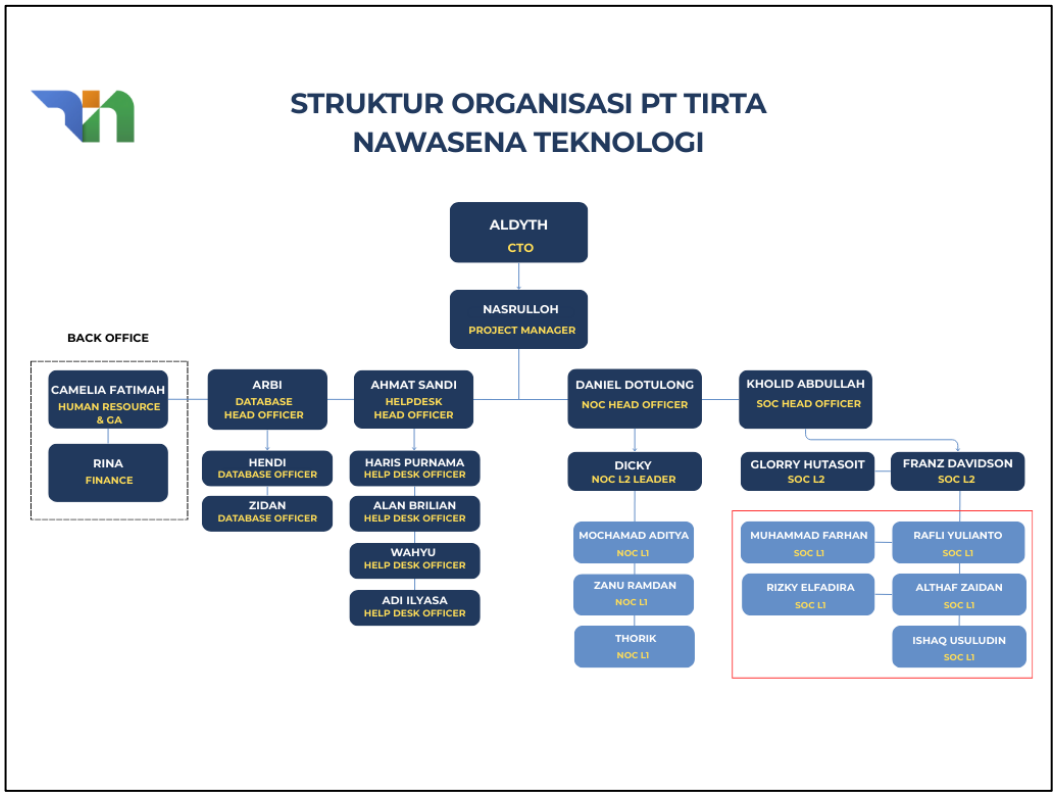
3.1 Profil DUDI

Gambar 3. 1 Logo PT Tirta Nawasena Teknologi

(Sumber https://tirtanawasena.com/)

PT Tirta Nawasena Teknologi adalah penyedia layanan dalam bidang Manajemen xFasilitas dan Solusi *IT End-to-End* yang berfokus pada manajemen keamanan dan teknologi. PT ini terletak di Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec. Serpong Utara, Kota Tangerang Selatan, Banten 15323. PT ini telah tersertifikasi di bidang keamanan *cyber* diantaranya, *ISO 37001:2016 Anti-Bribery Management System* dan *ISO 9001:2015 Quality Management System* serta ini telah menjalin kerja sama dengan beberapa organisasi pemerintahan maupun swasta seperti PLN, SBI (State Bank India), SIG (Semen Indonesia Group), BKN, KBIJ (Kredit Biro Indonesia Jaya), dan Waskita.

PT Tirta Nawasena Teknologi berfokus pada layanan keamanan dan teknologi operasional. Bidang utamanya mencakup manajemen keamanan terintegrasi, cyber security, monitoring dan pengelolaan sistem, serta dukungan infrastruktur teknologi yang menunjang operasional organisasi skala besar. Aktivitasnya erat dengan penerapan kontrol keamanan, tata kelola IT, manajemen risiko, dan pemeliharaan sistem yang berjalan terus-menerus, khususnya pada lingkungan instansi pemerintah dan korporasi. Perusahaan ini bermain di ranah operational security dan managed services, bukan pengembangan produk, sehingga kekuatannya ada pada implementasi, pengawasan, dan keberlangsungan sistem, dan instalasi awal.



Gambar 3. 2 Struktur organisasi PT Tirta Nawasena Teknologi

Selama pelaksanaan magang, penulis ditempatkan pada divisi Security Operations Center (SOC) Level 1. Divisi ini berperan sebagai garda terdepan dalam operasional keamanan informasi dengan fokus pada pemantauan, analisis awal, dan penanganan insiden keamanan siber. Tanggung jawab utama SOC L1 meliputi monitoring aktivitas jaringan dan sistem melalui berbagai tools keamanan, analisis awal terhadap indikasi ancaman, klasifikasi insiden, serta pelaporan dan eskalasi ke level lanjutan apabila ditemukan potensi serangan. Penempatan pada divisi ini memberikan penulis pengalaman langsung dalam proses operasional keamanan, mulai dari pengumpulan dan analisis log, identifikasi anomali, hingga penerapan prosedur standar respons insiden.

3.2 Uraian Kegiatan Magang

Pelaksanaan kegiatan magang dilakukan sepenuhnya secara *WFO (Work from office)* dengan pembagian 2 shift bagi tim magang yaitu shift pertama pada jam 08:00 WIB – 16:00 WIB dan shift kedua pada jam 15:00 WIB – 00:00 WIB. Terdapat 3 orang anggota *SOC* magang dengan pembagian 2 orang pada shift

pertama dan 1 orang pada shift kedua, jadwal shift tersebut selalu dirotasi setiap minggu sehingga setiap anggota magang memiliki kesempatan untuk merasakan shift pertama dan kedua. Berikut adalah log kegiatan harian magang pada tim SOC L1,

Pada bulan pertama (Juli 2025), penulis memasuki masa pengenalan lingkungan kerja serta tools yang digunakan oleh divisi SOC dalam memantau keamanan jaringan SIG. Pada periode ini penulis mempelajari platform Crowdstrike yang menampilkan alert aktivitas mencurigakan melalui VPN SIG. Penulis bertanggung jawab pada menu *Endpoint Detection* untuk mendeteksi malware berupa SHA-256, domain, IP, atau aktivitas mencurigakan lainnya, kemudian SOC menganalisis apakah alert tersebut termasuk *true positive* atau *false positive* yang dianalisis melalui tools CTI.

Pada bulan kedua (Agustus 2025), aktivitas monitoring dan analisis mulai meningkat. Pada awal bulan, tim SOC L2 memberikan tugas baru terkait pengisian data quarantine. Data ini berisi ratusan domain yang diakses oleh tim SIG dan dicurigai sebagai domain malicious oleh sistem keamanan. File diberikan untuk satu minggu penuh dalam bentuk Excel yang terbagi menjadi tujuh file harian. Setiap file berisi 400–800 data yang harus diperiksa reputasinya secara manual menggunakan CTI Cyfirma dan VirusTotal. Rutinitas ini dilakukan bersamaan dengan pemantauan alert pada dashboard Crowdstrike. Penulis juga menyelesaikan pelatihan dasar cybersecurity melalui materi Fortinet Training Institute (NSE 1) dan memperdalam pemahaman terkait playbook tim SOC.

Pada bulan ketiga (September 2025), penulis tetap menjalankan rutinitas pemantauan Crowdstrike dan Tehtris serta pengecekan domain malicious pada file quarantine, namun pada bulan ini tim SOC L2 menambahkan tugas baru berupa pengecekan honeypot dan data breach dari Tehtris dan Cyfirma. Penulis mempelajari proses pembuatan laporan honeypot, laporan data breach, dan cara kerja rule detection pada platform Tehtris. Memasuki pertengahan bulan, tugas pengecekan honeypot dan data breach mulai dialihkan kepada tim magang, dan pada periode yang sama penulis menemukan adanya miskonfigurasi pada VT-Tools dan Chimera yang menyebabkan kedua tools tersebut terkena banned sementara

oleh beberapa layanan CTI, sehingga penulis perlu melakukan konfigurasi ulang agar tools mematuhi batas rate limit API gratis yang digunakan.

Pada bulan keempat (Oktober 2025), penulis menjalankan rutinitas monitoring Crowdstrike dan Tehtris sambil melanjutkan pengembangan fitur Chimera. Fokus kegiatan berada pada penyempurnaan dashboard, integrasi backend–frontend, dan perbaikan error seperti timeout API AbuseIPDB. Penulis juga melakukan troubleshooting GitHub serta pengujian modul CTI. Menjelang akhir bulan, fitur-fitur utama seperti bulk scan, caching, dan tampilan skor reputasi mulai stabil.

Pada Bulan kelima (November 2025), kegiatan difokuskan pada penyempurnaan arsitektur Chimera dan refactoring kode agar lebih efisien. Rutinitas monitoring Crowdstrike, Tehtris, dan SIEM tetap berjalan setiap hari. Penulis mengatasi kendala rate limit API serta memperbaiki integrasi CTI seperti VirusTotal, IBM X-Force, dan OTX. Modul Core Checker disempurnakan dan dashboard diperbaiki. Akhir bulan ditutup dengan penyelesaian dokumentasi dan perbaikan UI.

Pada bulan terakhir kegiatan magang (Desember 2025), Penulis tetap melakukan monitoring Crowdstrike, Tehtris, dan SIEM, bersamaan dengan finalisasi implementasi tools Chimera. Perbaikan dilakukan pada UI/UX, history log, bulk scanning, dan validasi performa terhadap alert nyata. Penulis memastikan seluruh fitur berjalan stabil dan lebih efisien dibanding pengecekan manual. Minggu terakhir difokuskan pada uji operasional dan penyelesaian laporan akhir magang. Ringkasan kegiatan magang ini penulis rangkai dari *logbook* harian yang terdapat pada lampiran II pada halaman 42.

Melalui rangkaian kegiatan tersebut, penulis memperoleh pengalaman langsung dalam pengembangan aplikasi, rekayasa infrastruktur, dan penerapan keamanan siber di lingkungan *enterprise*. Penulis juga mendapatkan pemahaman yang lebih baik mengenai arsitektur sistem, analisis insiden, dan penggunaan platform keamanan.

3.3 Pembahasan Hasil Magang

Selama pelaksanaan kegiatan magang yang dilakukan di PT Tirta Nawasena

Teknologi, penulis berkesempatan untuk menjadi bagian dari divisi *Security Operation Center* (SOC) L1. SOC L1 bertugas menganalisis, melakukan *monitoring*, dan melaporkan insiden terkait ancaman siber pada perusahaan.

Selama kegiatan magang, terdapat tantangan utama pada tim SOC L1 yaitu proses pemeriksaan reputasi IP dan domain yang masih dilakukan secara manual melalui portal tiap CTI vendor. Cara ini memakan waktu lama saat alert meningkat dan perbedaan format antar platform membuat analisis kurang efisien. Kondisi tersebut memperlambat alur pemeriksaan, meningkatkan risiko human error, dan berpotensi menghambat pelaporan insiden.

Sebagai solusi dari permasalahan tersebut penulis mengembangkan sistem pengecekan skor reputasi IOC yang dapat melakukan validasi reputasi IoC kepada 4 vendor utama CTI Agent yang digunakan oleh divisi SOC secara pararel. Selain itu tools ini juga dapat mengotomatisasi pengecekan beberapa domain secara langsung. Penulis berhasil mengoptimalkan proses pengecekan reputasi *IOC dari file hash* berformat *sha 256, IP* dan *domain* yang didapatkan dari log *platform XDR* melalui *tools* Multi-CTI Agent (Chimera).

3.3.1 Gambaran Umum Sistem

Multi-CTI *Agent* Chimera adalah perangkat yang berfungsi melakukan pemindaian reputasi IOC meliputi *hash* SHA-256, IP, dan domain ke berbagai layanan siber eksternal seperti *VirusTotal*, *CTX.IO, OTX LevelBlue*, dan *AbuseIPDB* secara paralel dan otomatis. Sistem ini menggantikan proses pengecekan manual, menampilkan hasil melalui antarmuka web lokal dalam bentuk tabel skor reputasi, serta dirancang sesuai batasan rate limit API gratis. Tujuannya adalah mempermudah analisis reputasi IOC dalam jumlah besar tanpa ketergantungan pada pengecekan manual.

3.3.2 Spesifikasi dan Kebutuhan Sistem

Dalam pengembangan Chimera, beberapa kebutuhan sistem ditetapkan agar proses pemeriksaan berjalan stabil selama berjalan di lingkungan SOC, yaitu, **Kebutuhan Perangkat Lunak (*Software*)** :

a. **Bahasa pemrograman**: Python 3.10 atau lebih baru. (Untuk performa pengecekan yang lebih stabil).
b. **Framework**: Flask (Digunakan karena memiliki integrasi yang mudah dengan pustaka Python lain*)*.
c. **Web server :** Flask Werkzeug Development Server (Web server bawaan flask).
d. **API Vendor CTI tools :** API VirusTotal, OTX, CTX.io, dan Abuse IPDB. (untuk mengakses layanan pengecekan IOC).
e. **Environment** : Python Virtual Environment (venv) (dipilih agar paket Python terisolasi dan menjaga kerahasiaan data).
f. **Frontend**: HTML5, dan CSS3.

Selain kebutuhan perangkat lunak dibutuhkan beberapa spesifikasi minimum untuk dapat menjalankan sistem ini. Berikut adalah deskripsi **kebutuhan perangkat keras** pada perangkat kerja tim SOC L1. Perangkat yang digunakan dalam proses perancangan memiliki spesifikasi minimum seperti berikut :

a. **Processor** : Intel Core i5 gen 10 atau setara (disarankan).
b. **RAM**: 4 GB (disarankan 8 GB untuk multitasking).
c. **Koneksi Internet**: Harus ada dan stabil (untuk mengakses API dari vendor CTI *tools*).

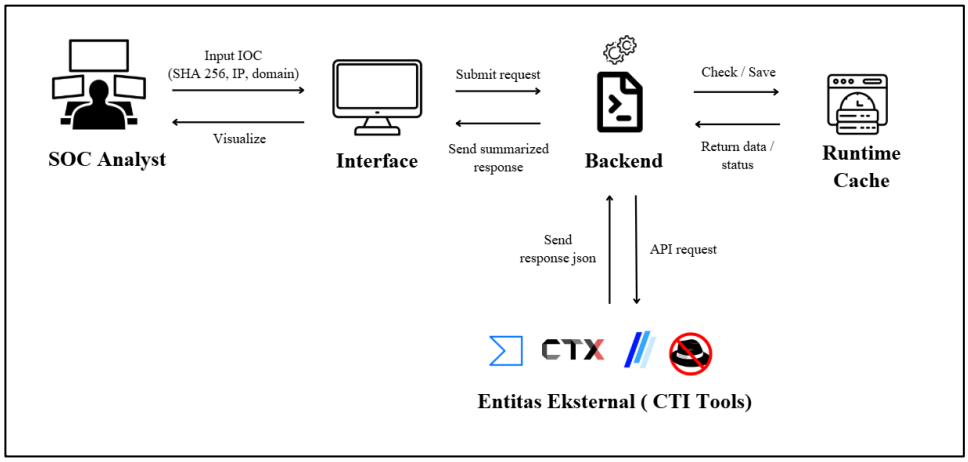
Untuk menghindari kesalahan pada sistem yang dapat membuat konsekuensi seperti ban dan pemrosesan yang lambat berikut ini adalah **kebutuhan fungsional** yang harus dimiliki sistem :

a. Sistem harus dapat menerima input IoC dan mengirim permintaan pemeriksaan ke beberapa platform CTI melalui API.
b. Sistem harus menjalankan proses pemeriksaan secara paralel dan mengatur batas permintaan (rate limit) setiap platform.
c. Sistem harus menampilkan hasil pemeriksaan secara ringkas dan mudah dipahami analis.
d. Sistem harus menyediakan antarmuka web yang hanya dapat diakses oleh pengguna internal dan tetap stabil saat menangani banyak permintaan.

3.3.3 Desain Sistem dan Diagram Alir

a. Data Flow Diagram

Berikut adalah diagram alir data (data flow diagram) dari sistem Multi-CTi tools Chimera :



Gambar 3. 3 Data Flow Diagram

Secara garis besar sistem dirancang dalam bentuk aplikasi web sederhana yang memiliki empat komponen utama:

1) Interface

   Halaman web, digunakan untuk memasukkan indikator ancaman yang akan diperiksa.

2) Backend

   Modul backend menerima request dari UI yang mengatur validasi jenis IOC, mengirim permintaan API ke platform CTI, mengelola batas permintaan (rate limit), mengirim data statistik harian, dan merapikan output menjadi format laporan yang konsisten.

3) Runtime Cache (SQL LRU Cache)

   Cache ini bertujuan untuk menghemat penggunaan API, waktu, jaringan, dan resiko rate limit. Cache disimpan didalam SQLite database dan akan menghapus data yang memiliki masa hidup lebih

dari 48 jam. Cache alan memberikan hasil pengecekan sebelumnya kepada backend sehingga mencegah pemanggilan API berulang untuk IOC yang sama.

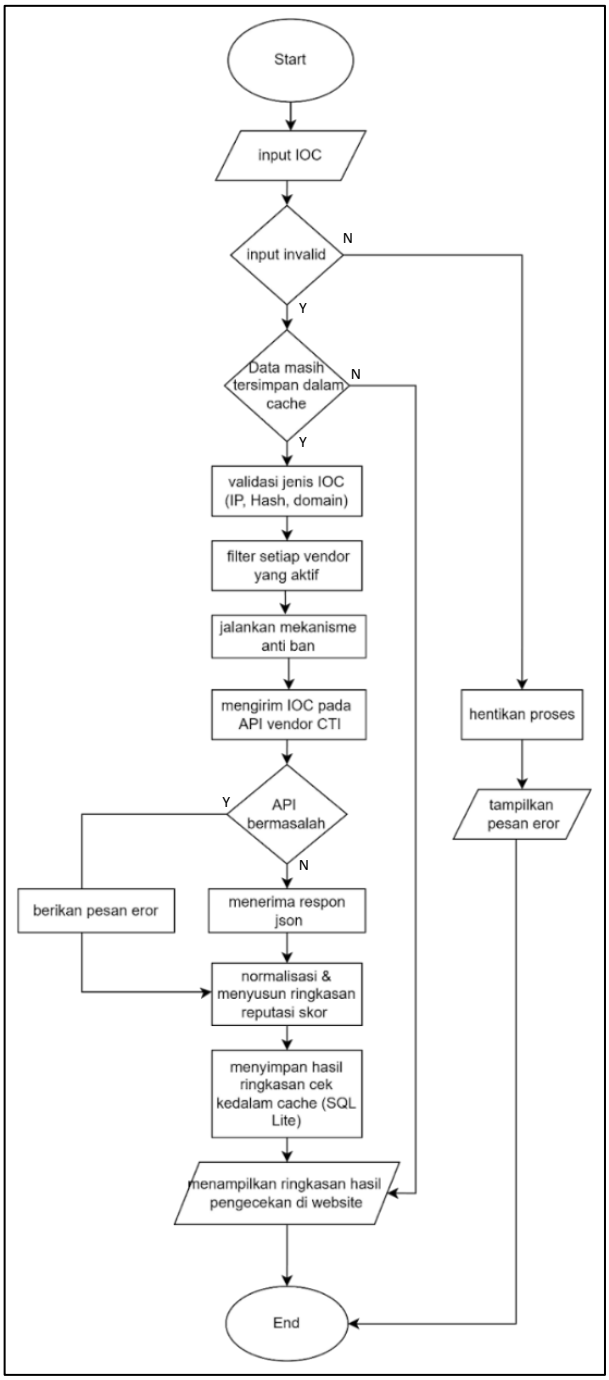
4) External Threat Intelligence Service (CTI tools)

Ini adalah vendor vendor yang menyediakan layanan pengecekan reputasi yang digunakan oleh sistem, vendor tersebut diantaranya OTX, CTX, VIrusTotal, dan Abuse IPDB.

Sistem Multi-CTI Chimera bekerja ketika SOC Analyst memasukan IOC melalui interface web, permintaan tersebut akan diteruskan ke backend untuk diproses. Backend memvalidasi input, membuat cache key, dan memeriksa apakah hasil sebelumnya tersedia di penyimpanan cache. Jika ditemukan dan masih valid, data langsung dikembalikan ke interface web. Jika tidak, backend akan mengirim request API ke beberapa layanan CTI eksternal dan mengatur rate limit.

Setelahnya CTI vendor akan mengirimkan response JSON. Setelah seluruh respons diterima, backend menyusun ringkasan hasil, menyimpannya ke cache sebagai data baru, lalu mengirimkan output kembali ke interface. Terakhir interface akan menampilkan hasil output kepada SOC Analyst sehingga insiden dapat dianalisis lebih lanjut.

b. Flowchart Single Scan



Gambar 3. 4 Flowchart Single Scan

Berikut adalah penjelasan flowchart dari halaman utama dashboard dengan fungsi single scan. Proses dimulai dengan input IOC berupa hash, IP, atau domain dari user. selanjutnya sistem akan melakukan cek apakah input bersifat valid (merupakan salah satu dari jenis IOC) atau tidak, jika input bukan merupakan bagian dari jenis IOC yang ada maka proses akan

dihentikan dan sistem akan menampilkan pesan error pada interface *user.* dan jika tidak, akan dilanjutkan ke proses selanjutnya

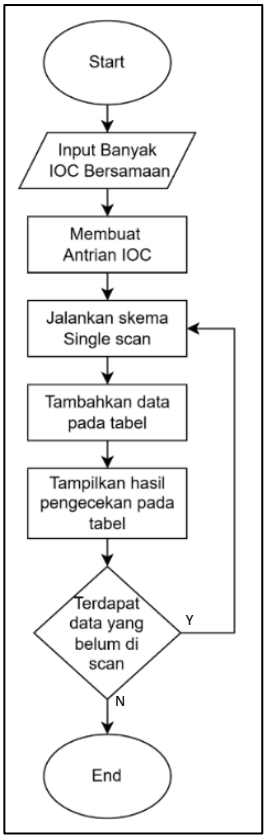
Selanjutnya sistem melakukan cek apakah data IOC sudah pernah di *scan* dan masih tersimpan didalam *cache* atau tidak, jika data yang tersimpan masih berada di dalam *cache* SQLite maka sistem akan menampilkan data yang berasal dari cache tersebut guna menghemat penggunaan API dan jika tidak, akan dilanjutkan ke proses selanjutnya.

Data yang tidak berada di dalam cache akan diseleksi sesuai dengan input yang diberikan yaitu hash, IP, dan domain hal ini dilakukan karena *endpoint* setiap setiap jenis IOC berbeda-beda di setiap url pemanggilan API dari setiap vendor CTI. setelah ditentukan jenis IOC tersebut maka akan dilanjutkan ke tahap selanjutnya.

Sistem memungkinkan pengguna memilih layanan dari CTI vendor dengan mengaktifkan dan menonaktifkan CTI kartu yang aktif dengan menonaktifkan kartu maka proses pengiriman API tidak akan berjalan pada vendor tersebut dan untuk setiap kartu yang akit maka proses akan dilanjutkan ke tahap selanjutnya.

Sebelum mengirimkan request ke setiap API, diperlukan mekanisme load balancing untuk mengatur lalu lintas data dan mencegah terjadinya pembatasan akses akibat lonjakan permintaan secara bersamaan, sebagaimana direkomendasikan dalam penelitian sebelumnya yang menunjukkan bahwa pengelolaan trafik yang buruk dapat menurunkan ketersediaan dan performa sistem. Dalam implementasinya, penulis menggunakan algoritma Round Robin untuk mengatur pergantian API key sebelum request dikirim. Yang terbukti efektif dalam menjaga ketersediaan layanan dan responsivitas sistem ketika menghadapi lonjakan trafik yang signifikan. (Teknologi Informasi Dan Komputer Politeknik Negeri Lhokseumawe, 2024)

c. Flowchart Bulk Scan



Gambar 3. 5Flowchart Bulk Scan

Berikut adalah penjelasan flowchart *bulk scan* diatas, alur flowchart dimulai ketika user memasukan beberapa IOC secara bersamaan pada tabel yang tersedia pada halaman bulk scan. Sistem akan membuat antrian dari beberapa IOC tersebut sehingga tidak terjadi collision atau tabrakan paket yang menyebabkan hang.

Selanjutnya sistem akan meneruskan IOC pada API seperti yang dilakukan pada langkah pengecekan single scan dengan output ringkasan hasil pengecekan. setelah data ringkasan hasil pengecekan berhasil didapatkan maka data akan ditampilkan pada baris baru pada tabel di halaman bulk scan.

langkah selanjutnya adalah melakukan cek apakah masih ada data yang belum diperiksa reputasinya. Jika masih ada, maka ulangi langkah pengecekan sebelumnya hingga seluruh IOC selesai di cek reputasinya.

3.3.4 Desain *Project/produk*

Perancangan tools Chimera dibuat agar dapat menyederhanakan verifikasi ancaman bagi analis SOC dengan sistem web yang terhubung ke berbagai sumber CTI. Aplikasi ini dibangun agar tetap ringan dan cepat, menyajikan ringkasan reputasi IoC yang efektif untuk kebutuhan analisis harian.

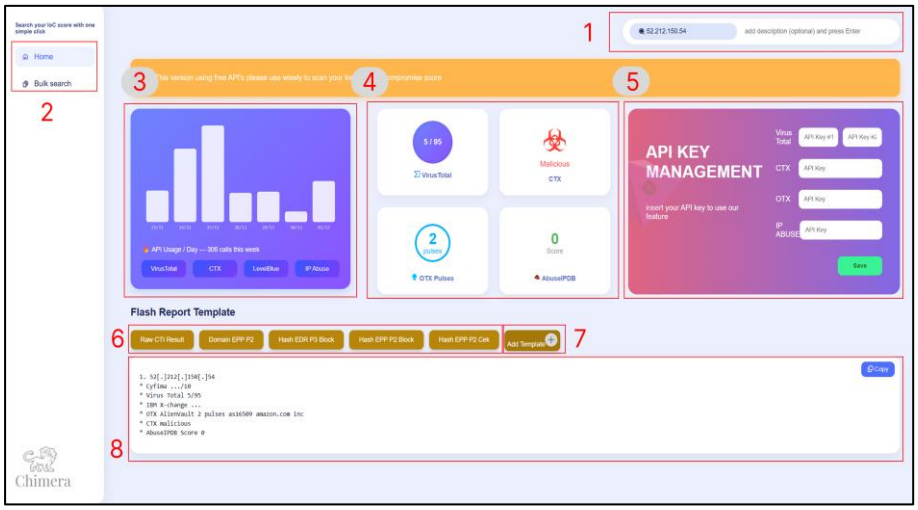
a. Arsitektur Aplikasi

Arsitektur Aplikasi menggunakan arsitektur *Client-Server* dengan pola komunikasi *RESTful API,* yaitu sebuah model arsitektur sistem terdistribusi di mana klien mengirimkan permintaan layanan dan server menerima, memproses, serta merespons permintaan tersebut melalui jaringan (Geofrey *et al.*, 2024).

1) ***Client Side****:* Berkas statis (index.html, style.css, script.js) yang dimuat di browser pengguna. Bertugas mengirimkan input IoC (IP/Domain/Hash) ke server dan memvisualisasikan hasil reputasi yang diterima.

2) **Server Side**: Endpoints API yang dibangun dengan Python (Flask). *app.py* bertindak sebagai entry point yang mengatur rute trafik dan mengorkestrasi permintaan ke berbagai modul CTI eksternal.

b. Desain antarmuka (*Interface*)



Gambar 3. 6 Interface dashboard

Gambar di atas menampilkan halaman utama (dashboard) dari *tools* Multi-CTI. Halaman ini terdiri atas beberapa komponen utama yang masing-masing memiliki fungsi spesifik. Penjelasannya adalah sebagai berikut::

1) *Searchbox*

Searchbox berfungsi sebagai tempat m emasukkan IOC berupa IP, domain, atau hash yang akan diperiksa reputasinya. Sistem akan memproses IOC tersebut ketika pengguna menekan tombol *enter*.

2) *Navigation Bar*

Navigation bar menyediakan dua menu utama, yaitu *Home/Dashboard* untuk pemeriksaan tunggal dan *Bulk Scan* untuk pemeriksaan beberapa IOC secara otomatis.

3) Diagram Statistik

Bagian ini menampilkan diagram batang yang menunjukkan jumlah permintaan (request) yang dilakukan pengguna dalam satu minggu. Statistik membantu pengguna memonitor penggunaan API, terutama ketika memakai layanan dengan kuota terbatas.

4) Kartu CTI (CTI Cards)

Setiap kartu mewakili vendor eksternal penyedia layanan reputasi. Pengguna dapat mengaktifkan atau menonaktifkan vendor tertentu. Jika dinonaktifkan, sistem tidak akan mengirim permintaan API ke vendor tersebut.

5) *API Key Management*

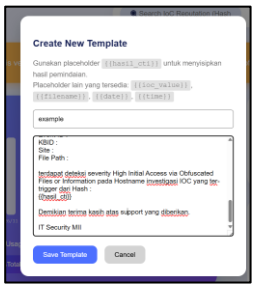
Bagian ini digunakan untuk menambahkan atau mengganti API key yang dibutuhkan oleh masing-masing vendor. Setelah disimpan, sistem akan menggunakan API key yang baru dalam proses pemeriksaan.

6) Flash Report Template

Komponen ini menyediakan fitur pembuatan *flash report* otomatis. Setelah sebuah IOC teridentifikasi sebagai ancaman, sistem dapat menggabungkan template laporan yang dipilih dengan hasil pemeriksaan reputasi, kemudian menampilkannya pada *Result Box*.

7) Add Template Button

Fitur ini berfungsi untuk menambahkan template flash report sesuai dengan yang dibutuhkan oleh *user.* Berikut adalah tampilan *popup menu add flash report template*

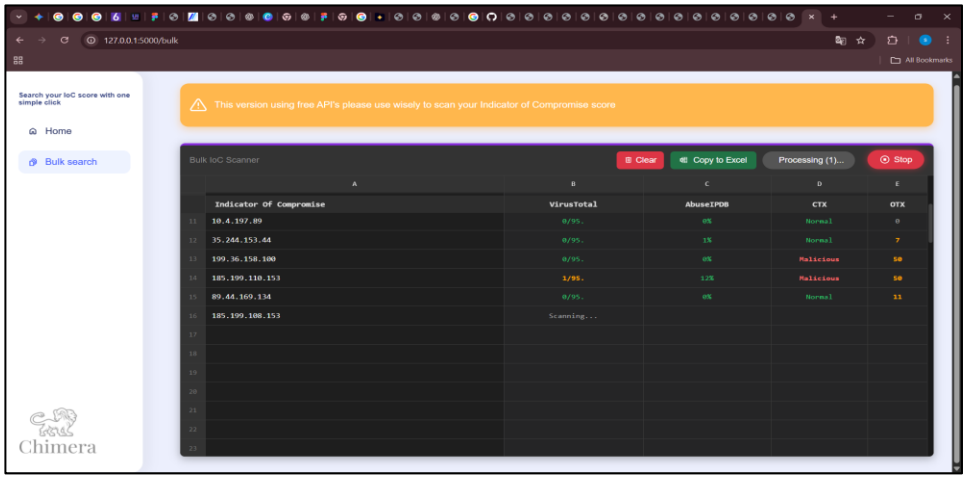


Gambar 3. 7 New Template Bulk Scan

8) Result Box

Result Box menampilkan hasil pemeriksaan baik dalam bentuk ringkasan teks maupun keluaran dari setiap vendor CTI dengan teks yang telah disesuaikan dengan kebutuhan *user*.

Selain fitur utama yang terdapat pada *dashboard. Tools* ini juga dilengkapi dengan pengecekan otomatis beberapa IOC secara bersamaan melalui menu ***bulk scan***. Berikut adalah penjelasannya :



Gambar 3. 8 Halaman Bulk Scan

Gambar di atas menampilkan halaman ***Bulkscan***. Pengguna dapat mengakses menu *bulkscan* melalui *navigation bar*. Pada menu ini pengguna dapat memasukan beberapa IOC secara bersamaan dan akan dicek secara bersama ke semua vendor penyedia layanan pengecekan yang tersedia. Pengguna dapat mengambil beberapa data dari *excel* dan melakukan input secara bersamaan kedalam kolom *indicator of compromise* dan hasil akan di tampilkan pada kolom-kolom lainnya .

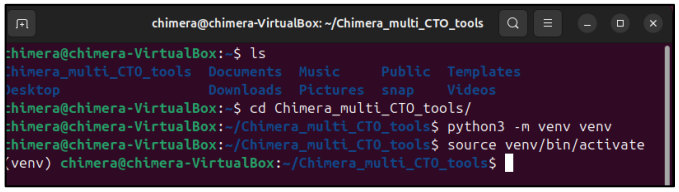
3.3.5 Implementasi

Tahap implementasi adalah tahap merealisasikan rancangan yang telah dijelaskan pada bagian sebelumnya. dalam mengimplementasikan sistem ini penulis membuat sistem secara modular sehingga kode lebih mudah untuk diperbaiki jika terjadi bug / kesalahan sistem. berikut adalah penjelasannya,

a. Implementasi Lingkungan Eksekusi

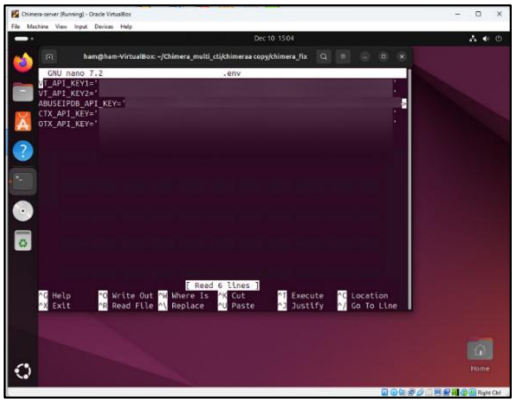
Sistem dijalankan pada perangkat komputer SOC L1 dengan spesifikasi minimum yang telah dijelaskan pada bagian spesifikasi minimum di atas. Sistem dijalankan pada mesin Linux (Ubuntu) menggunakan Python 3.10. Instalasi dilakukan dengan virtual environment untuk memisahkan dependensi

modul CTI tidak menanam kunci kredensial secara langsung pada kode (hardcode) melainkan menggunakan file .env pada direktori utama dan dimuat menggunakan python dotenv. Sehingga aman dan mudah dipakai pada lingkungan berbeda. contoh pemanggilan pada sistem :



Gambar 3. 9 Inisialisasi virtual environment

Untuk mengamankan file sensitif seperti API key dari masing-masing CTI maka file konfigurasi diletakan di dalam file .env. karena saat menangani informasi sensitif seperti kredensial database, menggunakan metode keamanan terbaik adalah hal yang paling penting. (Olabanji, 2023):



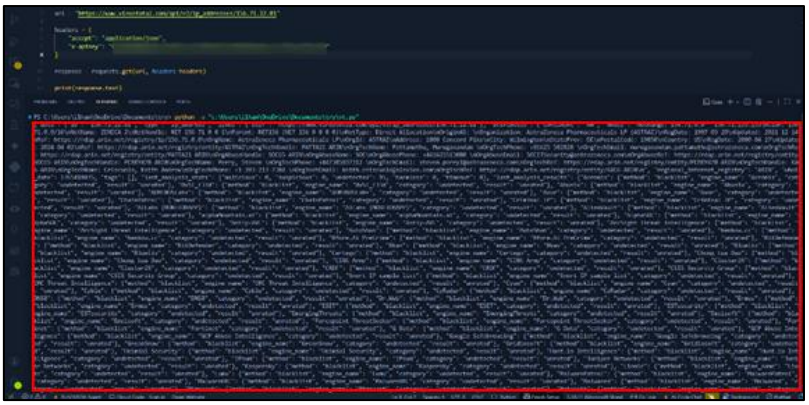
Gambar 3. 10 File Konfigurasi VENV

b. Implementasi Modul CTI (Checkers/)

Modul CTI diimplementasikan secara modular melalui folder checkers/, dimana setiap layanan threat intelligence (VirusTotal, CTX, OTX, dan Abuse IPDB) dipisahkan ke dalam file masing-masing. Dengan menggunakan metode ini modul API satu dan lainnya tidak saling mempengaruhi sehingga mudah diperbaiki, ditambahkan, atau dikembangkan.

Setiap modul memiliki indikator yang berbeda yang dibutuhkan dalam analisis. Karena seluruh CTI vendor akan mengirimkan data berbentuk response JSON dengan format yang lengkap dan panjang, perlu dilakukan normalisasi yaitu proses standarisasi struktur dan skala nilai untuk mengurangi redundansi, meningkatkan konsistensi, dan mendukung proses analisis lebih lanjut, terutama ketika data bersifat kompleks atau datang dari berbagai sumber (Palinggik Allorerung *et al.*, 2024). Untuk menunjukan perbedaan dari output sebelum dan sesudah normalisasi penulis akan memberikan perbandingan berupa gambar seperti dibawah ini.

Berikut adalah data response JSON dari API VirusTotal yang belum di normalisasi.

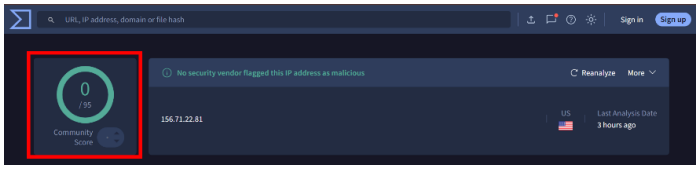


Gambar 3. 11 File response JSON sebelum normalisasi

Berikut adalah data setelah dilakukan normalisasi

Gambar 3. 12 File response JSON setelah normalisasi

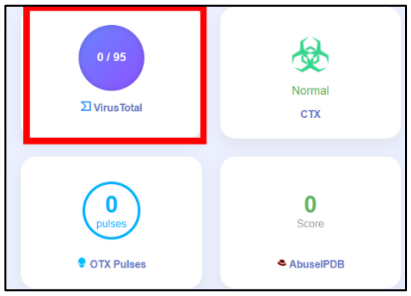
Kedua fungsi memberikan perintah yang sama untuk melakukan request pada API dan menampilkan respon dari API yaitu file response JSON. Dapat dilihat melalui perbedaan kedua gambar di atas bahwa, normalisasi data berhasil mengubah data response JSON yang rumit menjadi data kesimpulan singkat yang lebih mudah dipahami.



Gambar 3. 13 Indikator pada portal website VirusTotal

Gambar di atas merupakan halaman portal dari CTI VirusTotal, data yang ditampilkan setelah normalisasi adalah data yang sesuai dengan kolom score pada portal website virustotal karena kolom ini yang menjadi indikator untuk melakukan analisis kerentanan lebih lanjut.

Dan berikut adalah tampilan pada website chimera



Gambar 3. 14 Halaman dashboard Chimera

Semua CTI dalam sistem mengalami fase yang sama dalam normalisasi data sehingga data yang ditampilkan adalah ringkasan dari setiap CTI report.

c. Implementasi app.py (Controler utama)

File app.py bertindak sebagai pusat pengendali seluruh sistem Chimera. Conttroller ini menerima input IOC melalui interface web berbasis Flask, file ini juga menentukan tipe indikator, lalu mengecek ketersediaan IOC pada cache. Jika tidak ditemukan maka, app.py akan memanggil seluruh modul CTI pada folder *checkers/*, menggabungkan hasil reputasi dari semua vendor aktif, dan menyimpannya kedalam database cache,dan menampilkan hasil pemeriksaan melalui GUI website.

d. Implementasi Cache

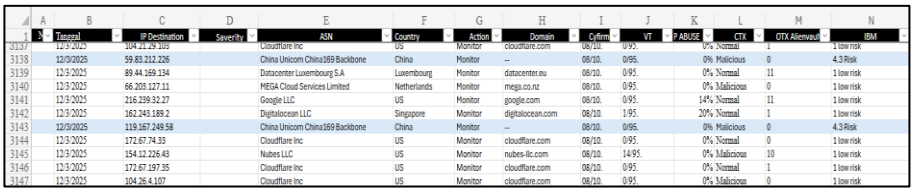
Untuk menghemat penggunaan API chimera menggunakan SQL lite berbasis data cache. Cache diatur batas maksimal penyimpanannya (*TTL*) selama 2 hari atau jika cache sudah berjumlah lebih dari 300 data dan akan dihapus bila telah melewati batas waktu atau maksimal data. tujuannya adalah untuk menghemat penyimpanan db dan agar data yang diberikan tetap relevan dengan data terbaru dari setiap vendor CTI.

e. Implementasi Interface web menggunakan Flask

Bagian antarmuka sistem dibuat sederhana menggunakan Flask dan template HTML Jinja2. Halaman utama hanya menyediakan satu form untuk memasukkan IOC, yang kemudian dikirim ke endpoint Flask untuk diproses. Flask dipilih karena ringan, mudah dikonfigurasi di Linux maupun Windows, serta ideal untuk dashboard sederhana di lingkungan SOC L1. Fokus utama tetap pada fungsi automasi CTI, sehingga UI dibuat minimalis tanpa elemen grafis yang tidak diperlukan.

Interface juga menyediakan data statistik penggunaan API untuk mengetahui konsumsi API yang telah digunakan. Data ini akan bertambah ketika terjadi request API terjadi.

f. implementasi pada lingkungan kerja



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	No	Tanggal	IP Destination	Saverity	ASN	Country	Action	Domain	Cyfirm	VT	P ABUSE	CTX	OTX Alienvault	IBM
3137		12/3/2025	104.21.29.105		Cloudflare Inc	US	Monitor	cloudflare.com	08/10.	0/95.		0% Normal	1	1 low risk
3138		12/3/2025	59.83.212.226		China Unicom China169 Backbone	China	Monitor	--	08/10.	0/95.		0% Malicious	0	4.3 Risk
3139		12/3/2025	89.44.169.134		Datacenter Luxembourg S.A	Luxembourg	Monitor	datacenter.eu	08/10.	0/95.		0% Normal	11	1 low risk
3140		12/3/2025	66.203.127.11		MEGA Cloud Services Limited	Netherlands	Monitor	mega.co.nz	08/10.	0/95.		0% Malicious	0	1 low risk
3141		12/3/2025	216.239.32.27		Google LLC	US	Monitor	google.com	08/10.	0/95.		14% Normal	11	1 low risk
3142		12/3/2025	162.243.189.2		Digitalocean LLC	Singapore	Monitor	digitalocean.com	08/10.	1/95.		20% Normal	1	1 low risk
3143		12/3/2025	119.167.249.58		China Unicom China169 Backbone	China	Monitor	--	08/10.	0/95.		0% Malicious	0	4.3 Risk
3144		12/3/2025	172.67.74.93		Cloudflare Inc	US	Monitor	cloudflare.com	08/10.	0/95.		0% Normal	0	1 low risk
3145		12/3/2025	154.12.226.43		Nubes LLC	US	Monitor	nubes-llc.com	08/10.	14/95.		0% Malicious	10	1 low risk
3146		12/3/2025	172.67.197.35		Cloudflare Inc	US	Monitor	cloudflare.com	08/10.	0/95.		0% Normal	1	1 low risk
3147		12/3/2025	104.26.4.107		Cloudflare Inc	US	Monitor	cloudflare.com	08/10.	0/95.		0% Malicious	0	1 low risk

Gambar 3. 15 Data vulnerability assessment

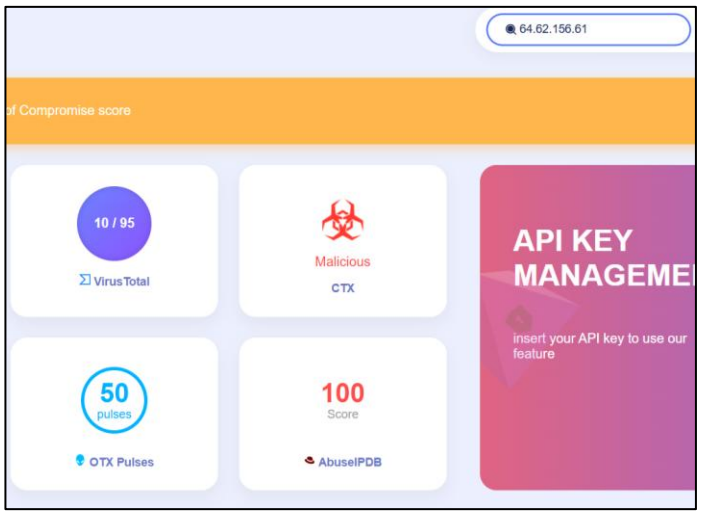
Data IP ini berasal dari sistem manajemen jaringan SIG yaitu SIEM platform Palo Alto dengan kurang lebih 80 IP yang perlu dicek secara manual melalui CTI. Penulis menggunakan menu bulk scan pada *tools* Chimera untuk melakukan pengecekan data secara otomatis kepada beberapa platform CTI yaitu, VIrusTotal, CTX, OTX dan Virus Total.

3.3.6 Pengujian Sistem

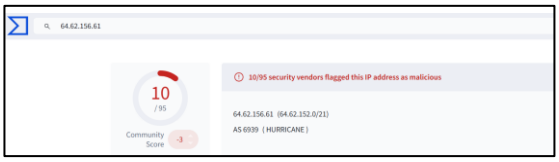
Setelah memahami sistem yang berjalan pada Multi-CTI *tools* tahapan selanjutnya adalah tahap pengujian sistem. pengujian ini sangat berguna sebagai tolak ukur kredibilitas sistem yang telah dirancang. Terdapat lima pengujian yang akan dilakukan yaitu :

a. Pengujian validitas dan akurasi data yang dihasilkan oleh Multi CTI Tools.

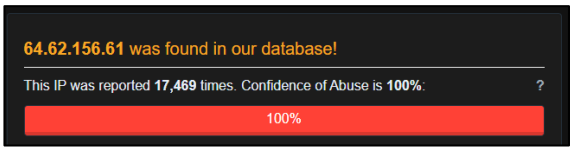
Tujuan utama pengujian ini adalah memastikan bahwa output dari Multi CTI Tools akurat dan dapat dipercaya. Berikut adalah contoh perbandingannya,



Gambar 3. 16 Pengujian pada website Chimera

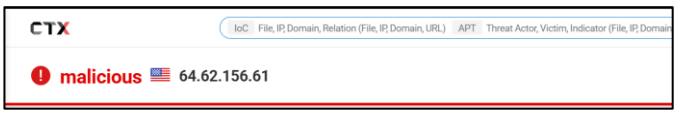


Gambar 3. 17 Score pada portal web VirusTotal



Gambar 3. 18 Score pada portal web Abuse IPDB

Gambar 3. 19 Pulse pada portal web OTX



Gambar 3. 20 State pada portal web CTX

Pengujian dilakukan dengan membandingkan pemindaian reputation score terhadap tiga sampel IOC untuk setiap kategori (IP, hash, domain) melalui portal website dengan melalui sistem Chimera. Tingkat kesesuaian dihitung dengan membandingkan jumlah data yang memiliki hasil identik terhadap total data yang diuji. Digunakan metode *blackbox* testing yaitu pengujian perangkat lunak yang berfokus pada verifikasi fungsionalitas dari sistem perangkat lunak yang Validitas pengujiannya dijamin melalui pemetaan yang konsisten antara spesifikasi sistem dan hasil yang diharapkan (Kawakib Kartono *et al.*, 2025).

Hasil perbandingan kedua metode tersebut dirangkum dalam tabel berikut :

Tabel 3.4.1 Tabel Hasil Pengecekan IOC secara Manual

Parameter	VirusTotal	CTX	OTX (pulse)	IP Abuse
207.46.224.84	3/95.	Normal	4	100%
64.62.156.61	10/95.	Malicious	50	100%
209.85.216.70	0/95.	Normal	2	100%
5b3354069fd3b79f28fdd36507ffc0f3e2422b0b9b2f6ff878ec8e180b8a9a2c	15/62.	Malicious	0	Tidak ditemukan

e4e6c1742f10ceeda74ee11aa7723e06292f7c8ca91168cda2d4d006800df8b6	14/72.	Normal	0	Tidak ditemukan
82d36ec0f74ba240259122268de8ecb4374d82af78406dfa4bd99318a17599f1	29/69.	Malicious	0	Tidak ditemukan
garage-pirenne.be	0/95.	Normal	0	Tidak ditemukan
br-icloud.com.br	14/95.	Malicious	1	Tidak ditemukan
larcadelcarnevale.com	3/95.	Normal	0	Tidak ditemukan

Tabel 3.4.2 Tabel Hasil Pengecekan IOC Menggunakan Fitur Bulk Scan

Parameter	VirusTotal	CTX	OTX (pulse)	IP Abuse
207.46.224.84	3/95.	Normal	4	100%
64.62.156.61	10/95.	Malicious	50	100%
209.85.216.70	0/95.	Normal	2	100%
5b3354069fd3b79f28fdd36507ffc0f3e2422b0b9b2f6ff878ec8e180b8a9a2c	15/62.	Malicious	0	N/A%
e4e6c1742f10ceeda74ee11aa7723e06292f7c8ca91168cda2d4d006800df8b6	14/72.	Normal	0	N/A%
82d36ec0f74ba240259122268de8ecb4374d82af78406dfa4bd99318a17599f1	29/69.	Malicious	0	N/A%
garage-pirenne.be	0/95.	Normal	0	N/A%
br-icloud.com.br	14/95.	Malicious	1	N/A%
larcadelcarnevale.com	3/95.	Normal	0	N/A%

Hasil analisis & kesimpulan pengujian : Berdasarkan hasil pengujian pada kedua tabel, diperoleh tingkat kecocokan yang tinggi antara hasil pengecekan IOC secara manual melalui portal CTI dan pengecekan menggunakan Multi CTI Tools Chimera. Digunakan rumus berikut dalam mengetahui akurasi dari data:

$$Accuracy = \frac{\sum \text{Data yang Sama}}{\text{Total Data}} \times 100\%$$

Hasil perbandingan menunjukkan bahwa seluruh data IOC yang diuji memiliki hasil yang sama, sehingga tingkat kesesuaian mencapai 100%.

Dengan demikian, dapat disimpulkan bahwa Multi CTI Tools Chimera mampu menyajikan data reputasi IOC yang akurat dan konsisten dengan data pada portal CTI masing-masing vendor.

b. Pengujian konfigurasi dalam kode *backend* untuk menangani risiko ban

Tujuan utama pengujian ini adalah menguji efektivitas dari konfigurasi *backend* pada sistem, dengan cara mengimplementasikan rotasi dua API *key* menggunakan logika *Round Robin* dalam menangani tindakan ban oleh penyedia layanan CTI.

Tabel 3.4.3 Tabel Perbandingan Risiko & Efisiensi: VirusTotal API

Parameter	**1 API Key (Tanpa Round Robin)**	**2+ API Keys (Dengan Round Robin)**
Kapasitas Request	Maksimal 4 request / menit.	4 x (Jumlah Key) request / menit. (Misal 2 Key = 8 req/menit).
Skenario: 10 Request Cepat	Request ke-5 akan gagal (HTTP 429). Sistem harus tidur (sleep) 60 detik.	Request 1-8 sukses instan (dibagi ke Key A & B). Hanya request ke-9 yang mungkin perlu menunggu sekitar 5 detik.
Risiko "Soft Ban" (HTTP 429)	Sangat Tinggi. Jika 5 request dikirm dalam 1 detik, API Key langsung terkunci sementara.	Rendah. Karena beban dibagi rata. Key A hanya menerima request dengan urutan ganjil. Key B menerima genap.
Risiko "Hard Ban" (Akun Diblokir)	Sedang. Jika skrip force terus menerus saat kena limit 429 tanpa sleep, VT bisa memblokir akun permanen.	Sangat Rendah. Pola traffic terlihat lebih "wajar" dan tidak agresif pada satu akun saja.
Waktu Tunggu (Idle Time)	Tinggi. Aplikasi sering berhenti total selama 60 detik untuk cooldown.	Hampir 0. Selama jumlah request < (Jumlah Key x 4), aplikasi berjalan terus tanpa henti.
Efisiensi Waktu	Rata-rata 65 detik untuk scan 5 file.	Rata-rata 5 detik untuk scan 5 file.

Hasil analisis & kesimpulan pengujian : Setelah menerapkan konfigurasi tersebut ke dalam kode diketahui bahwa adanya peningkatan kapasitas

request dari 4 request / menit menjadi 8 request / menit pada penggunaan 2 atau lebih API key. Pada 10 request cepat diketahui bahwa ada penurunan waktu tunggu dari sistem selama 60 detik menjadi sekitar 5 detik, menurunkan resiko banned dan menunjukan efisiensi waktu.

Kesimpulan dari pengujian ini adalah, bahwa konfigurasi kode backend menggunakan logika *Round Robin* berhasil mencegah ban pada API dan meningkatkan efisiensi waktu respon sistem.

c. Pengukuran interval antar request (*Inter-Request Gap*)

Pengujian ini memiliki tujuan untuk menganalisis interval penyelesaian pemeriksaan antar IOC, yaitu merupakan selisih waktu yang muncul antara satu hasil pemeriksaan dengan pemeriksaan selanjutnya, sehingga dapat diketahui waktu yang dibutuhkan sistem untuk menganalisis setiap indikator (Terawi *et al.*, 2025). Skenario pengukuran dilakukan menggunakan timestamp yang dicatat terminal saat setiap IOC selesai diproses dengan metode *inter-request gap*. Tabel berikut menyajikan hasil analisis jeda waktu berdasarkan data yang terekam pada terminal Python :

Tabel 3.4.4 Tabel Interval Antar-Request

Indiator of Compromise	Time Stamp	Delay Rate Limit (Log)	Gap ke Request Selanjutnya
207.46.224.84	19:51:44	-	21 detik
64.62.156.61	19:52:05	-	9 detik
209.85.216.70	19:52:14	-	14 detik
5b3354069fd3b79f28fdd36507ffc0f3e2422b0b9b2f6ff878ec8e180b8a9a2c	19:52:28	3.85s	11 detik
e4e6c1742f10ceeda74ee11aa7723e06292f7c8ca91168cda2d4d006800df8b6	19:52:39	4.58s	11 detik
82d36ec0f74ba240259122268de8ecb4374d82af78406dfa4bd99318a17599f1	19:52:50	0.84s	14 detik

garage-pirenne.be	19:53:04	4.54s	11 detik
br-icloud.com.br	19:53:15	-	15 detik
larcadelcarnevale.com	19:53:30	6.94s	(Data Terakhir)
Total Waktu Pengujian			1 Menit 46 detik

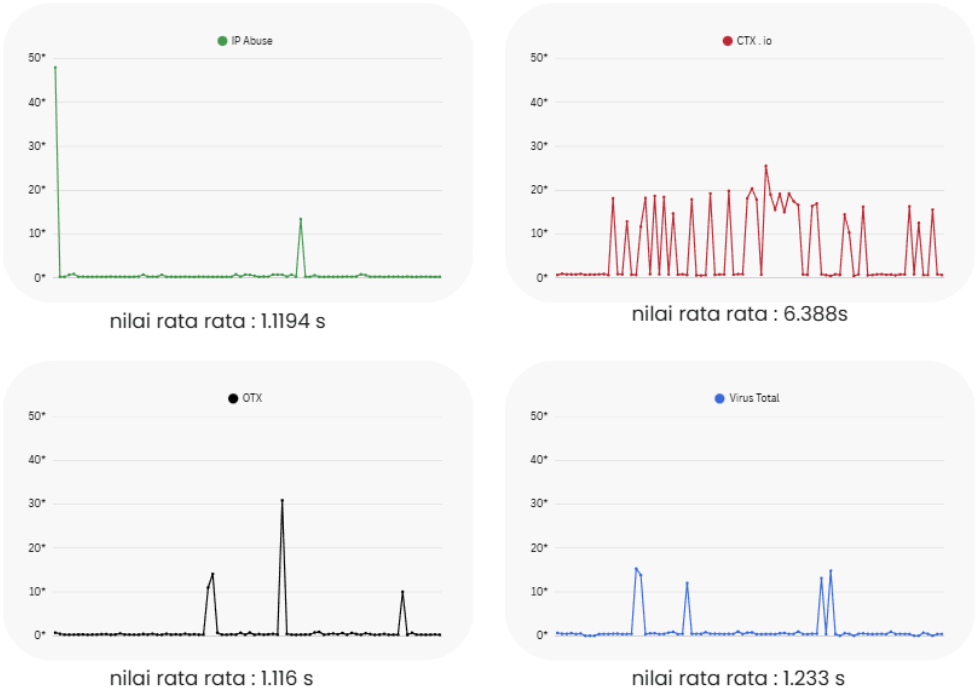
Hasil analisis & kesimpulan pengujian : Sistem menunjukkan stabilitas kinerja dengan rata-rata waktu proses 13,2 detik per request, berkisar antara respon tercepat 9 detik hingga 21 detik saat inisialisasi awal (*cold start*). Dan memiliki total lama waktu pengecekan selama 1 menit 46 detik.

Selain itu implementasi fitur anti banned (rotasi dua API key dengan logika Round Robin) terbukti efektif mengamankan API Key dari risiko banned, terlihat jelas saat sistem secara otomatis menyisipkan delay (seperti 6,94 detik pada VirusTotal) untuk mematuhi batas rate limit tanpa memutus alur pemindaian.

Kesimpulan dari pengujian ini membuktikan sistem bekerja efisien dan stabil, secara cerdas menyeimbangkan kecepatan pemrosesan data dengan kepatuhan terhadap *rate limit* API melalui mekanisme adaptif otomatis.

d. Pengujian Latensi Layanan Threat Intelligence

Pengujian ini merupakan analisis kinerja (*benchmarking*) terhadap empat layanan intelijen ancaman menggunakan 100 sampel IP address, dengan tujuan untuk mengevaluasi efisiensi waktu respons (*response time*) dan stabilitas koneksi API saat menangani permintaan berurutan.

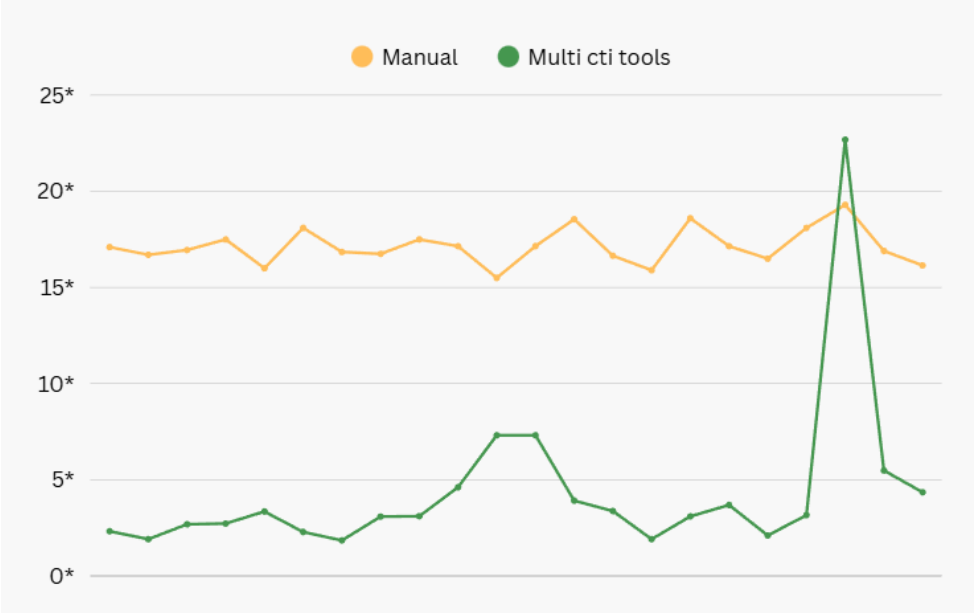


Gambar 3. 21 Perbandingan latensi antar CTI tools

Hasil analisis & kesimpulan pengujian : Pengujian *benchmarking* terhadap empat layanan intelijen ancaman menggunakan 100 sampel IP memakan waktu 12 menit 42 detik. Pengujian ini menunjukkan hasil yang kontras, di mana **OTX** mencatatkan rata-rata tercepat (1,116 detik) diikuti tipis oleh **IP Abuse** (1,1194 detik) dan **Virus Total** (1,233 detik), sementara **CTX.io** justru menjadi layanan paling lambat (6,388 detik). Analisis grafik mengungkap bahwa buruknya performa CTX.io disebabkan oleh ketidakstabilan parah dengan fluktuasi tajam yang terus-menerus (*high jitter*), berbeda dengan IP Abuse yang sebenarnya sangat stabil namun rata-ratanya sedikit terangkat akibat satu anomali lonjakan ekstrem (~48 detik) di awal pengujian. Di sisi lain, OTX mempertahankan posisinya sebagai yang tercepat meski sesekali mengalami *spike* signifikan hingga 30 detik, sedangkan Virus Total menunjukkan latensi yang relatif moderat dengan variabilitas yang lebih terkendali.

e. Pengujian Performa Analisis Manual dengan Automasi Multi-Tools

Pengujian ini bertujuan untuk mengevaluasi efisiensi operasional antara proses analisis manual dibandingkan dengan penggunaan sistem automasi **Multi CTI Tools (Chimera).** Pengujian dilakukan dengan menerapkan metode bulk scan terhadap sampel alamat IP untuk membandingkan efisiensi antara pencarian manual satu per satu dengan sistem automasi Chimera.



Gambar 3. 22 Perbandingan Metode Manual dan Multi CTI tools

Hasil analisis & kesimpulan pengujian : Data perbandingan menunjukkan bahwa sistem Multi CTI Tools (Chimera) secara konsisten memberikan efisiensi waktu yang signifikan dibandingkan metode Manual, yang memerlukan durasi antara 15 hingga 20 detik. Meskipun terdapat lonjakan (spike) latensi hingga mencapai angka 25 detik, hal tersebut merupakan bukti teknis adanya batasan (rate limit) atau mekanisme timeout dari pihak penyedia CTI eksternal, dan bukan disebabkan oleh kegagalan pemrosesan internal. Dengan demikian, sistem Chimera terbukti tetap stabil, sehat, dan memiliki performa kecepatan yang jauh unggul dibandingkan proses manual.

3.4 Identifikasi Kendala yang Dihadapi

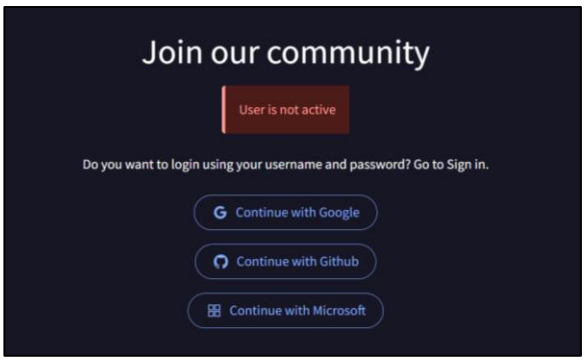
Setelah menjalani kegiatan magang selama enam bulan di PT Tirta Nawasena Teknologi penulis telah memperoleh banyak ilmu pengetahuan, baik yang berasal dari mentor maupun melalui penanganan langsung insiden keamanan yang terjadi. Penulis telah mempelajari berbagai hal teknis seperti analisis ancaman siber melalui platform *enterprise level (Tehtris dan* crowdstrike), identifikasi indikator ancaman melalui CTI *tools* , respon ancaman siber yang terjadi, dan praktik kerja di lingkungan SOC L1.

Selain itu, terdapat beberapa pembelajaran non-teknis yang diperoleh, seperti manajemen waktu untuk menyelesaikan insiden di bawah batas waktu SLA 30 menit, ketelitian dalam menyampaikan informasi kepada tim di luar SOC, koordinasi tim dalam menangani suatu insiden, dan metode kerja yang lebih efisien dalam menyelesaikan setiap tugas.

3.4.1 Kendala Pelaksanaan Tugas

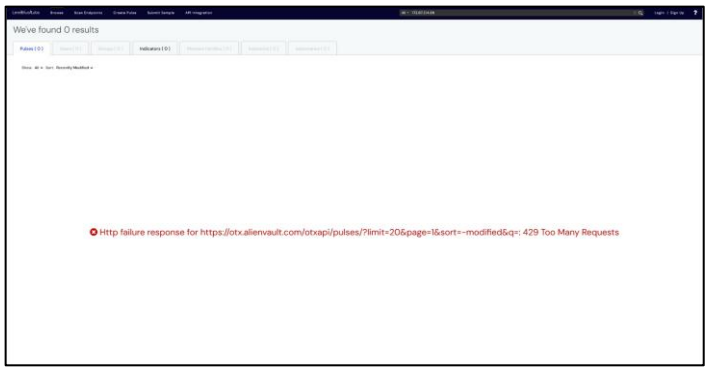
Beberapa kendala yang penulis hadapi selama melaksanakan magang antara lain :

1. Banyaknya jenis ancaman siber yang perlu dipelajari dalam menggunakan platform keamanan XDR Tehtris dan Crowdstrike.
2. *Alert* yang muncul pada platform *monitoring* di awal kegiatan magang sangat banyak dalam rentang waktu yang singkat.
3. API key VirusTotal terkena ban akibat perilaku yang dianggap *abusive* .



Gambar 3. 23 Ban VirusTotal

4. Kesulitan implementasi multi CTI *tools* pada lingkungan kerja SOC L1. OTX API tidak bisa digunakan bersamaan oleh tim L1 karena dianggap melakukan *request abusive* saat *bulk scan*.



Gambar 3. 24 Soft Ban pada OTX

5. Sistem kerja shifting terlebih pada jam malam yang menyita waktu tidur.

3.4.2 Cara Mengatasi Kendala

Beberapa hal yang penulis lakukan untuk mengatasi kendala tersebut antara lain:

1. Mempelajari jenis ancaman siber melalui modul NSE *Fortinate Academy*, memahami aturan *playbook* SOC L1 dan selalu bertukar informasi terbaru terkait ancaman siber bersama anggota dan mentor tim SOC.
2. Untuk menangani kebutuhan analisis yang cepat dalam rentang waktu SLA yang telah ditentukan penulis merancang Multi CTI *tools Chimera* yang juga menjadi produk hasil kegiatan magang ini. Dengan mengimplementasikan *tools* ini membuat proses pengecekan reputasi indikator melalui CTI agent lebih efisien dan pencarian *template flash report* lebih mudah sehingga mengurangi waktu yang dibutuhkan untuk membuat *flash report.*
3. Mengimplementasikan logika pertukaran kunci API menggunakan metode round robin.

4. Penulis memisahkan IP publik tim SOC dan aplikasi Chimera dengan cara menempatkan aplikasi CTI tersebut ke dalam Virtual Machine (VM) yang memiliki VPN (Proton VPN). Hal ini dilakukan karena satu komputer tidak bisa menjalankan dua VPN sekaligus. Dengan cara ini, tim SOC tetap bisa mengakses XDR (via jaringan utama) dan *tools* CTI (via VM) secara bersamaan tanpa harus takut terkena ban oleh CTI *tools* OTX.
5. Dalam mengatasi kendala waktu *shift malam* penulis telah beradaptasi dengan mengganti waktu tidur di siang hari, seiring berjalannya waktu efek dari kelelahan akibat waktu tidur yang kurang telah banyak menurun dibandingkan dengan masa awal kegiatan magang.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan kegiatan magang yang telah dilakukan dengan pengambilan judul laporan " Perancangan Tools Multi Cyber Threat Intelligence Menggunakan Python Di PT Tirta Nawasena Teknologi", dapat disimpulkan sebagai berikut:

1. Permasalahan pengecekan IOC yang lambat dan dapat terjadi human eror karena pengecekan IOC yang masih berjalan manual berhasil ditangani melalui proses perancangan dan implementasi Multi CTI Tools sebagai alat bantu dalam menyelesaikan laporan *vulneribilty assessment* (domain malicious quarentine dan IP malicious 7 layer).
2. Secara fungsional sistem berhasil menangani validasi reputasi IOC secara kredibel, mengotomatisasi pengecekan reputasi IOC dengan akurat dan aman dari risiko pemblokiran IP. Namun implementasi menggunakan API gratis tetap menghadapi kendala waktu proses yang belum cukup cepat saat melakukan pemindaian masif dalam skala *enterprise*.

4.2 Saran

Adapun saran yang dapat disampaikan selama melaksanakan magang adalah sebagai berikut:

1. Guna mendukung operasional skala *enterprise* yang optimal, sangat disarankan untuk menggunakan API Key *premium level / enterprise level* (berbayar) untuk pengembangan selanjutnya guna menghilangkan batasan rate limit dan mempercepat proses pengumpulan data reputasi IOC.
2. Pemeliharaan, pengembangan dan pemantauan keamanan *tools* yang telah dibangun sebaiknya dilakukan secara berkala. Disarankan untuk memahami kebijakan setiap CTI vendor dalam memberikan layanan API

key sehingga tidak ada sanksi yang dijatuhkan akibat *abusing* yang dapat terjadi di masa depan .

3. Multi CTI *tools* yang telah di rancang dapat dikembangkan lebih lanjut seperti proses caching yang berjalan. Disarankan untuk mengintegrasikan cache dengan layanan database seperti postgre karena data cache saat ini masih disimpan di ram, selain itu akses *tools* masih berjalan lokal sehingga dibutuhkan hosting agar layanan dapat diakses secara lebih luas oleh tim SOC L1 di PT Tirta Nawasena Teknologi.
4. Disarankan memanfaatkan waktu luang untuk mempelajari lebih lanjut skill yang berguna pada proses magang saeperti skill *coding* dengan bahasa pemrograman yang dianggap sesuai dengan project yang dikerjakan. Selain itu juga sangat disarankan untuk memanfaatkan kesempatan bertanya dan saling bertukar pengetahuan kepada anggota tim divisi yang sama dalam proses magang, karena penulis mendapatkan banyak keahlian teknis yang dapat dipelajari melalui *sharing knowladge* yang dilaksanakan setiap minggu oleh tim SOC L2.

DAFTAR PUSTAKA

Agil Maulana Nanda Riady, Paniran Paniran and I Made Budi Suksmadana (2024) 'Perancangan Backend Api Berbasis Rest-Api pada Aplikasi Rekomendasi Resep Makanan', *Mars : Jurnal Teknik Mesin, Industri, Elektro Dan Ilmu Komputer*, 2(3), pp. 94–106. doi:10.61132/mars.v2i3.137.

Asiri, M. *et al.* (2023) 'Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective', *ACM Transactions on Cyber-Physical Systems*, 7(2). doi:10.1145/3587255.

Crowdstike .inc (2025) 'Crowdstrike ebook-2025-MITRE'.

Dhruv, A.J., Patel, R. and Doshi, N. (2022) 'Python: The Most Advanced Programming Language for Computer Science Applications'. doi:10.5220/0010307900003051.

Geofrey, M. *et al.* (2024) *Architectural Review of Client-Server Models*, *International Journal of Scientific Research & Engineering Trends*.

Hidayat, M.R.T., Widiyasono, N. and Gunawan, R. (2025) 'OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS', *Jurnal Informatika dan Teknik Elektro Terapan*, 13(1). doi:10.23960/jitet.v13i1.5686.

Kaur, H. *et al.* (2024) 'Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review', in *E3S Web of Conferences*. EDP Sciences. doi:10.1051/e3sconf/202455601006.

Kawakib Kartono, F. *et al.* (2025) *Pengujian Black Box Testing Pada Sistem Website Osha Snack: Pendekatan Teknik Boundary Value Analysis*.

Olabanji, S.O. (2023) 'Advancing Cloud Technology Security: Leveraging High-Level Coding Languages like Python and SQL for Strengthening Security Systems and Automating Top Control Processes', *Journal of Scientific Research and Reports*, 29(9), pp. 42–54. doi:10.9734/jsrr/2023/v29i91783.

Palinggik Allorerung, P. *et al.* (2024) *Analisis Performa Normalisasi Data untuk Klasifikasi K-Nearest Neighbor pada Dataset Penyakit*, *Jurnal Informatika Sunan Kalijaga)*.

Soumik, S. *et al.* (2024) 'Dynamic Risk Scoring of Third-Party Data Feeds and Apis for Cyber Threat Intelligence'. doi:10.32996/jcsts.

Suraya and Sholeh, M. (2022) 'Designing and Implementing a Database for Thesis Data Management by Using the Python Flask Framework', *International*

Journal of Engineering, Science and Information Technology, 2(1), pp. 9–14. doi:10.52088/ijesty.v1i1.197.

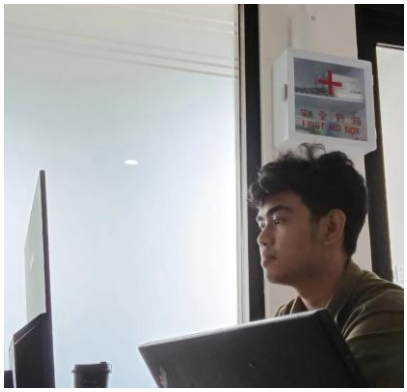
Tarsini, I. (2024) 'Explore flowchart and pseudocode concepts in algorithms and programming', *Indonesian Journal of Multidisciplinary Science, Vol. 3, No. 5*, 3.

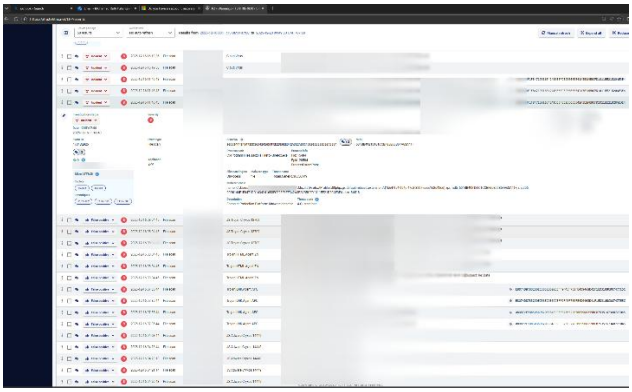
Teknologi Informasi Dan Komputer Politeknik Negeri Lhokseumawe, J. (2024) *ANALISIS KINERJA LOAD BALANCING ROUND ROBIN PADA WEBSITE SKALABEL*, *Journal of Information System Management (JOISM) e-ISSN*.

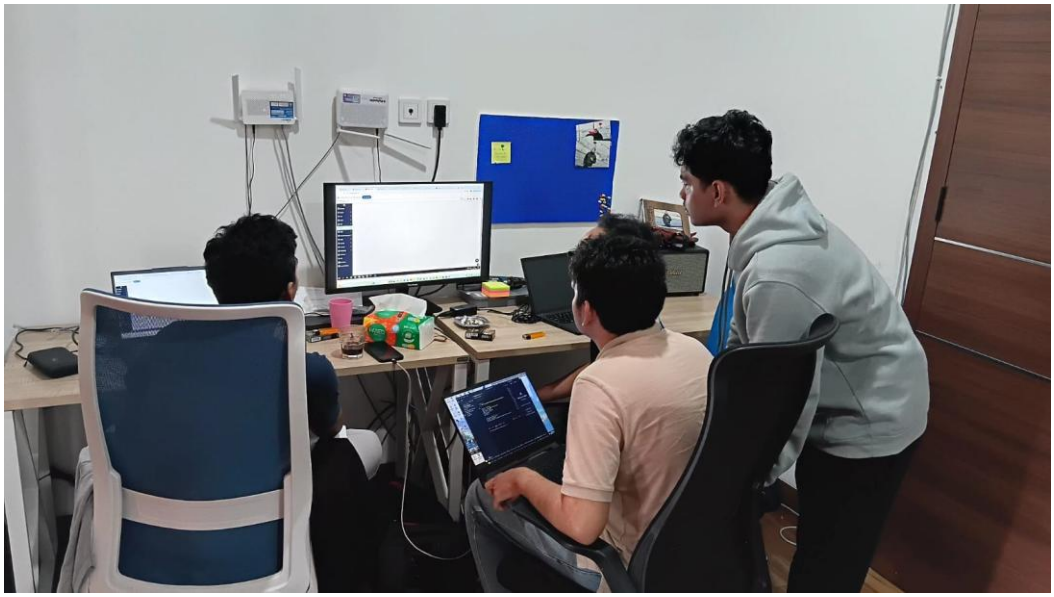
Terawi, N. *et al.* (2025) 'Enhanced Detection of Intrusion Detection System in Cloud Networks Using Time-Aware and Deep Learning Techniques', *Computers*, 14(7). doi:10.3390/computers14070282.

LAMPIRAN

A. Dokumentasi Kegiatan Magang







B. Logbook Harian

KEMENTERIAN PENDIDIKAN TINGGI, RISET, DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
Jl. Prof. DR. G.A. Siwabessy, Kampus UI, Depok 16425
Telp: (021)91274097, Hunting Fax : (021) 7863531, (021)7270036
Laman :http://www.pnj.ac.id, e-mail : tik.pnj@gmail.com

BUKU PENGHUBUNG PEMBIMBING MAGANG INDUSTRI

1. Nama Mahasiswa : Muhammad Ilham Sutama
2. NIM : 2207421028
3. Program Studi : Teknik Multimedia dan Jaringan
4. Nama Perusahaan/Industri : PT. Tirta Nawasena Teknologi
5. Nama Pembimbing Industri : Nasrullah

No.	Hari / Tanggal	Kegiatan Magang	Paraf
1	Senin, 21 Juli 2025	• Pengenalan lingkungan kerja SOC • Pengenalan *tools* & dashboard alert	
2	Selasa, 22 Juli 2025	• Monitoring Crowdstrike • Mempelajari Endpoint Detection (SHA256, domain, IP) • Memahami analisis alert TP/FP	
3	Rabu, 23 Juli 2025	• Monitoring Crowdstrike • Pengecekan reputasi IOC (Cyfirma, OTX, CTX.IO, VirusTotal, IBM-Xchange)	
4	Kamis, 24 Juli 2025	• Monitoring Crowdstrike • Analisis alert TP/FP • Pembuatan flash ticket melalui WhatsApp	
5	Jumat, 25 Juli 2025	• Monitoring Crowdstrike • Evaluasi alert mingguan & alur eskalasi	
6	Senin, 28 Juli 2025	• Monitoring Crowdstrike	

		• Pengecekan quarantine 400–800 domain (Cyfirma & VirusTotal)	
7	Selasa, 29 Juli 2025	• Monitoring Crowdstrike • Pengecekan lanjutan quarantine & update status domain	
8	Rabu, 30 Juli 2025	• Monitoring Crowdstrike • Pengecekan quarantine harian	
9	Kamis, 31 Juli 2025	• Monitoring Crowdstrike • Pelatihan Fortinet academy cybersecurity NSE 1 • Mempelajari playbook SOC	
10	Jumat, 1 Agustus 2025	• Monitoring Crowdstrike • Penyelesaian laporan mingguan quarantine	
11	Senin, 4 Agustus 2025	• Monitoring Crowdstrike • Pengecekan dashboard endpoint detection	
12	Selasa, 5 Agustus 2025	• Monitoring Crowdstrike • Blocking hash berbahaya via IOC Management	
13	Rabu, 6 Agustus 2025	• Monitoring Crowdstrike • Pengenalan XDR Tehtris (EDR & EPP)	
14	Kamis, 7 Agustus 2025	• Monitoring Crowdstrike • Pengenalan fitur Tehtris (EDR, EPP, XDR)	
15	Jumat, 8 Agustus 2025	• Monitoring Crowdstrike • Review blocking hash & dokumentasi	
16	Senin, 11 Agustus 2025	• Monitoring Crowdstrike & Tehtris • Menangani lonjakan alert EDR P3/EPP P2	
17	Selasa, 12 Agustus 2025	• Monitoring Crowdstrike & Tehtris • Eskalasi insiden ke helpdesk	

18	Rabu, 13 Agustus 2025	• Monitoring Crowdstrike & Tehtris • Blocking hash malicious • membuat data screenshoot hasil blokir malicious hash pada Crowdstrike IOC Management dan Tehtris YARA Policy	
19	Kamis, 14 Agustus 2025	• Monitoring Crowdstrike & Tehtris • Koordinasi teknisi & refining IOC	
20	Jumat, 15 Agustus 2025	• Monitoring Crowdstrike & Tehtris • Penyusunan laporan intensitas alert	
21	Senin, 18 Agustus 2025	• Monitoring Tehtris & Crowdstrike • Monitoring EDR P1–P3 & EPP P2	
22	Selasa, 19 Agustus 2025	• Monitoring Tehtris • Shift malam (intesnsitas alert mulai turun) • Pembuatan script otomatisasi IOC Python	
23	Rabu, 20 Agustus 2025	• Monitoring Tehtris • Penyelesaian *tools* otomatisasi VirusTotal	
24	Kamis, 21 Agustus 2025	• Monitoring Tehtris • Perencanaan integrasi CTI OTX & CTX	
25	Jumat, 22 Agustus 2025	• Monitoring Tehtris • Testing awal *tools* & dokumentasi	
26	Senin, 25 Agustus 2025	• Monitoring Tehtris & Crowdstrike • Rutinitas pemantauan harian	
27	Selasa, 26 Agustus 2025	• Monitoring Tehtris & Crowdstrike • Pengecekan quarantine domain	
28	Rabu, 27 Agustus 2025	• Monitoring Tehtris & Crowdstrike • esting VT automation & mempelajari rate limit API	
29	Kamis, 28 Agustus	• Monitoring Tehtris & Crowdstrike	

	2025	• Penanganan lonjakan alert signifikan menggunakan MultiCTI Tools	
30	Jumat, 29 Agustus 2025	• Monitoring Tehtris & Crowdstrike • Optimalisasi tool	
31	Senin, 1 September 2025	• Monitoring Tehtris & Crowdstrike • Pengecekan domain quarantine	
32	Selasa, 2 September 2025	• Monitoring Tehtris • Pengecekan honeypot	
33	Rabu, 3 September 2025	• Monitoring Tehtris • Pengecekan data breach	
34	Kamis, 4 September 2025	• Monitoring Tehtris • Belajar pembuatan detection rule YARA Policy di Tehtris	
35	Senin, 8 September 2025	• Monitoring Tehtris & Crowdstrike • Pengecekan domain	
36	Selasa, 9 September 2025	• Monitoring Tehtris • Pengalihan tugas honeypot & breach	
37	Rabu, 10 September 2025	• Monitoring Tehtris • Analisis data breach (credential leak SIG)	
38	Kamis, 11 September 2025	• Monitoring Tehtris • Troubleshooting VT-Tools & Chimera (API banned)	
39	Jumat, 12 September 2025	• Monitoring Tehtris • inalisasi laporan honeypot & breach	
40	Senin, 15 September 2025	• Rutinitas pemantauan dashboard alert pagi. • Brainstorming arsitektur ulang *tools* internal menjadi "Chimera" (Multi CTI Agent).	
41	Selasa, 16 September 2025	• Perancangan flowchart alur kerja Multi CTI Agent.	

		• Riset library Python untuk integrasi API (Requests, Pandas).	
42	rabu, 17 September 2025	• Analisis alert traffic anomali. • Setup environment development untuk Chimera (Virtualenv, Git init).	
43	Kamis, 18 September 2025	• Penanganan tiket eskalasi user. • Pembuatan kerangka database sederhana untuk log checking IOC.	
44	Jumat, 19 September 2025	• Reporting mingguan • Uji coba koneksi API key VirusTotal & IBM X-Force secara manual.	
45	Senin, 22 September 2025	• Pengecekan karantina domain mingguan. • Coding modul awal: Single IOC Checker (Python script basic).	
46	Selasa, 23 September 2025	• Investigasi phishing campaign baru. • Debugging script parsing JSON dari response API CTI.	
47	rabu, 24 September 2025	• Validasi Hash malicious dari laporan intelijen eksternal. • Integrasi modul OTX AlienVault ke dalam script Chimera.	
48	Kamis, 25 September 2025	• Update YARA rule berdasarkan temuan baru. • Refactoring kode script agar lebih modular (pemisahan class/function).	
49	Jumat, 26 September 2025	• Dokumentasi mingguan. • Evaluasi performa script checking (masih terkendala rate limit).	
50	Senin, 29 September 2025	• Monitoring rutin dashboard. • Inisiasi repositori GitHub untuk backup source code.	

51	Selasa, 30 September 2025	• Mulai eksplorasi framework web (Flask/Next.js) untuk UI Chimera. • Setup struktur backend dasar menggunakan Python Flask.	
52	rabu, 1 Oktober 2025	• Analisis malware variant baru di endpoint. • Menghubungkan script backend Python dengan frontend sederhana.	
53	Kamis, 2 Oktober 2025	• Eskalasi temuan High Severity ke L2. • Troubleshooting error "Push Permission" pada GitHub saat upload code.	
54	Jumat, 3 Oktober 2025	• Review log mingguan. • Finalisasi modul Core Checker v0.1.	
55	Senin, 6 Oktober 2025	• Fokus Dev: Coding intensif integrasi Next.js untuk frontend Chimera. • Implementasi tampilan dashboard skor reputasi IOC.	
56	Selasa, 7 Oktober 2025	• (Periode ini fokus pada perbaikan bug frontend dan sinkronisasi data antar modul CTI).	
57	rabu, 8 Oktober 2025	• Rutinitas pemantauan alert. • Penambahan sumber CTI baru ke dalam Chimera (AbuseIPDB preparation).	
58	Kamis, 9 Oktober 2025	• Menjalankan operasional harian SOC (Analisis, Blocking, Reporting). • Pengembangan fitur History Log pada Chimera untuk menyimpan riwayat pencarian.	
59	Jumat, 10 Oktober 2025	• Pengecekan dashboard awal bulan. • Evaluasi efektivitas Chimera dalam mempercepat analisis alert SOC.	

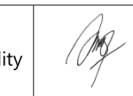
60	Senin, 13 Oktober 2025	• Persiapan environment Linux Ubuntu untuk simulasi serangan/pertahanan.	
61	Selasa, 14 Oktober 2025	• Memastikan environment coding stabil.	
62	rabu, 15 Oktober 2025	• Troubleshooting: Mengatasi isu Timeout terus-menerus pada API AbuseIPDB di Python script. • Simulasi: Riset metode Rotating IP di VM Linux Ubuntu menggunakan Proton VPN untuk bypass limitasi.	
63	Kamis, 16 Oktober 2025	• Implementasi solusi error handling untuk API Timeout. • Testing stabilitas koneksi VPN pada script automation.	
64	Jumat, 17 Oktober 2025	• Kembali ke monitoring rutin. • Dokumentasi hasil troubleshooting API AbuseIPDB.	
65	Senin, 20 Oktober 2025	• Mulai menyusun draft laporan akhir magang/project.	
66	Selasa, 21 Oktober 2025	• Penulisan Laporan: Menyusun Bab Pendahuluan & Latar Belakang	
67	rabu, 22 Oktober 2025	• Rutinitas pengecekan alert awal minggu. • Revisi draft laporan berdasarkan progress *tools*.	
68	Kamis, 23 Oktober 2025	• Fitur Baru: Coding script untuk Bulk Scanning domain ke VirusTotal. • Integrasi Flask: Menggabungkan script bulk scanner ke dalam aplikasi web Flask yang sudah ada.	

		• Debugging logic loop untuk handling list domain dalam jumlah banyak.	
69	Jumat, 24 Oktober 2025	• Validasi hasil scan bulk domain pada kasus real alert. • Pengecekan false positive dari hasil scan otomatis.	
70	Senin, 27 Oktober 2025	• Optimalisasi waktu respon Chimera (caching result). • Update dokumentasi teknis penggunaan *tools*.	
71	Selasa, 28 Oktober 2025	• Finalisasi fitur-fitur utama Chimera sebelum demo. • Penyusunan slide presentasi hasil magang.	
72	rabu, 29 Oktober 2025	• Consulting: Diskusi dan pembuatan Playbook Sederhana untuk Tim SOC L1. • Menyusun SOP penanganan insiden dasar (Phishing, Malware, Unauthorized Access).	
72	Kamis, 30 Oktober 2025	• Implementasi Playbook SOC L1 yang baru dibuat dalam operasional harian. • Monitoring efisiensi penanganan tiket dengan bantuan Chimera.	
73	Jumat, 31 Oktober 2025	• Melengkapi Bab Implementasi dan Pengujian pada laporan akhir. • Memasukkan screenshot "Chimera" ke dalam lampiran laporan.	
74	Senin, 3 November 2025	• Handover pengetahuan *tools* Chimera ke tim internal.	

		• Pengecekan terakhir bug pada fitur export report.	
75	Selasa, 4 November 2025	• Polishing UI/UX Chimera (Next.js) agar lebih user-friendly. • Final commit code ke repository.	
76	rabu, 5 November 2025	• Review mingguan terakhir operasional SOC.	
77	Kamis, 6 November 2025	• Evaluasi keseluruhan project Chimera. • Persiapan materi untuk presentasi sidang/demo *tools* (berdasarkan laporan yang sudah dibuat).	
78	Jumat, 7 November 2025	• Rutinitas pemantauan dashboard alert pagi. • Brainstorming arsitektur ulang *tools* internal menjadi "Chimera" (Multi CTI Agent).	
79	Senin, 10 November 2025	• Perancangan flowchart alur kerja Multi CTI Agent. • Riset library Python untuk integrasi API (Requests, Pandas).	
80	Selasa, 11 November 2025	• Analisis alert traffic anomali. • Setup environment development untuk Chimera (Virtualenv, Git init).	
81	rabu, 12 November 2025	• Penanganan tiket eskalasi user. • Pembuatan kerangka database sederhana untuk log checking IOC.	
82	Kamis, 13 November 2025	• Reporting mingguan. • Uji coba koneksi API key VirusTotal & IBM X-Force secara manual.	
83	Jumat, 14 November 2025	• Pengecekan karantina domain mingguan.	

		• Coding modul awal: Single IOC Checker (Python script basic).	
84	Senin, 17 November 2025	• Investigasi phishing campaign baru. • Debugging script parsing JSON dari response API CTI.	
85	Selasa, 18 November 2025	• Validasi Hash malicious dari laporan intelijen eksternal. • Integrasi modul OTX AlienVault ke dalam script Chimera.	
86	rabu, 19 November 2025	• Update YARA rule berdasarkan temuan baru. • Refactoring kode script agar lebih modular (pemisahan class/function).	
87	Kamis, 20 November 2025	• Dokumentasi mingguan. • Evaluasi performa script checking (masih terkendala rate limit).	
88	Jumat, 21 November 2025	• Monitoring rutin dashboard. • Inisiasi repositori GitHub untuk backup source code.	
89	Senin, 24 November 2025	• Mulai eksplorasi framework web (Flask/Next.js) untuk UI Chimera. • Setup struktur backend dasar menggunakan Python Flask.	
90	Selasa, 25 November 2025	• Analisis malware variant baru di endpoint SIEM dengan Event Type Network.	
91	rabu, 26 November 2025	• Eskalasi temuan High Severity ke L2. • Troubleshooting error "Push Permission" pada GitHub saat upload code.	
92	Kamis, 27 November 2025	• Monitoring Tehtris EDR, EPP, XDR, dan SIEM • Review log mingguan.	

		• Finalisasi modul Core Checker v0.1.	
93	Jumat, 28 November 2025	• Monitoring Tehtris EDR, EPP, XDR, dan SIEM • Implementasi tampilan dashboard skor reputasi IOC.	
95	Senin, 1 Desember 2025	• Rutinitas pemantauan alert.	
96	Selasa, 2 Desember 2025	• Menjalankan operasional harian SOC (Analisis, Blocking, Reporting). • Monitoring Tehtris EDR, EPP, XDR, dan SIEM • Pengembangan fitur History Log pada Chimera untuk menyimpan riwayat pencarian.	
97	rabu, 3 Desember 2025	• Pengecekan dashboard awal bulan. • Monitoring Tehtris EDR, EPP, XDR, dan SIEM • Evaluasi efektivitas Chimera dalam mempercepat analisis alert SOC.	
98	Kamis, 4 Desember 2025	• Monitoring Tehtris EDR, EPP, XDR, dan SIEM	
99	Jumat, 5 Desember 2025	• Mempelajari Zap Analisys tool untuk penetration testing • Monitoring Tehtris EDR, EPP, XDR, dan SIEM	
100	Senin, 8 Desember 2025	• Monitoring Tehtris & Crowdstrike • Pengecekan domain	
101	Selasa, 9 Desember 2025	• Monitoring Tehtris • Pengalihan tugas honeypot & breach	
102	rabu, 10 Desember 2025	• Monitoring Tehtris • Analisis data breach (credential leak SIG)	

103	Kamis, 11 Desember 2025	• Monitoring Tehtris • Mengerjakan laporan vulnerability assessment 7 layer	
104	Jumat, 12 Desember 2025	• Monitoring Tehtris • inalisasi laporan honeypot & breach	

Tangerang Selatan, 17 Desember 2025

Supervisor Perusahaan,

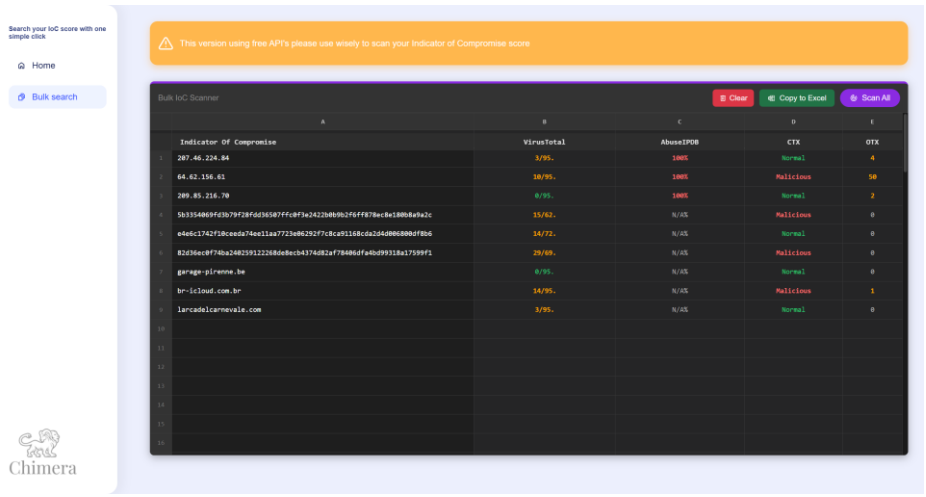
(Nasrullah)
NRK. Tnt002

C. Dokumentasi Pengujian

Inter-Gap Riset Testing

```
[JOB] Memproses: 207.46.224.84 | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
127.0.0.1 - - [06/Dec/2025 19:51:44] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: 64.62.156.61 | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
127.0.0.1 - - [06/Dec/2025 19:52:05] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: 209.85.216.70 | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
127.0.0.1 - - [06/Dec/2025 19:52:14] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: 5b3354069fd3b79f28fdd36507ffc0f3e2422b0b9b2f66ff878ec8e180b8a9a2c | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
   [DELAY] virustotal menunggu 3.85s...
127.0.0.1 - - [06/Dec/2025 19:52:28] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: e4e6c1742f10ceeda74ee11aa7723e06292f7c8ca91168cda2d4d006800df8b6 | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
   [DELAY] virustotal menunggu 4.58s...
127.0.0.1 - - [06/Dec/2025 19:52:39] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: 82d36ec0f74ba240259122268de8ecb4374d82af78406dfa4bd99318a17599f1 | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
   [DELAY] virustotal menunggu 0.84s...
127.0.0.1 - - [06/Dec/2025 19:52:50] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: garage-pirenne.be | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
   [DELAY] virustotal menunggu 4.54s...
127.0.0.1 - - [06/Dec/2025 19:53:04] "POST /api/check HTTP/1.1" 200 -

[JOB] Memproses: br-icloud.com.br | Checkers: ['abuseipdb', 'ctx', 'levelblue', 'virustotal']
127.0.0.1 - - [06/Dec/2025 19:53:15] "POST /api/check HTTP/1.1" 200 -
```

Pengujian Validitas Dan Akurasi Data



Pengujian Latensi API

```
2025-12-20 07:03:46,147.161.161.82,ip,VirusTotal,0.5683,SUCCESS
2025-12-20 07:03:46,147.161.161.82,ip,OTX AlienVault,0.7334,SUCCESS
2025-12-20 07:03:47,147.161.161.82,ip,CTX.io,1.6631,SUCCESS
2025-12-20 07:03:56,147.161.161.82,ip,AbuseIPDB,10.6283,SUCCESS
2025-12-20 07:04:01,165.225.33.6,ip,OTX AlienVault,0.2822,SUCCESS
2025-12-20 07:04:01,165.225.33.6,ip,AbuseIPDB,0.3461,SUCCESS
2025-12-20 07:04:02,165.225.33.6,ip,VirusTotal,1.1604,SUCCESS
2025-12-20 07:04:03,165.225.33.6,ip,CTX.io,2.1013,SUCCESS
2025-12-20 07:04:07,165.225.212.255,ip,OTX AlienVault,0.2405,SUCCESS
2025-12-20 07:04:08,165.225.212.255,ip,AbuseIPDB,0.3493,SUCCESS
2025-12-20 07:04:09,165.225.212.255,ip,CTX.io,2.1250,SUCCESS
2025-12-20 07:04:17,165.225.212.255,ip,VirusTotal,0.9711,SUCCESS
2025-12-20 07:04:19,136.226.64.114,ip,OTX AlienVault,0.2462,SUCCESS
2025-12-20 07:04:19,136.226.64.114,ip,AbuseIPDB,0.3564,SUCCESS
2025-12-20 07:04:21,136.226.64.114,ip,CTX.io,1.9610,SUCCESS
2025-12-20 07:04:23,136.226.64.114,ip,VirusTotal,0.3946,SUCCESS
2025-12-20 07:04:27,165.225.240.79,ip,OTX AlienVault,0.2316,SUCCESS
```

```
2025-12-20 07:04:27,165.225.240.79,ip,AbuseIPDB,0.3275,SUCCESS
2025-12-20 07:04:29,165.225.240.79,ip,CTX.io,2.1180,SUCCESS
2025-12-20 07:04:34,165.225.240.79,ip,VirusTotal,0.3654,SUCCESS
2025-12-20 07:04:39,136.226.77.103,ip,OTX AlienVault,0.2911,SUCCESS
2025-12-20 07:04:39,136.226.77.103,ip,AbuseIPDB,0.3339,SUCCESS
2025-12-20 07:04:41,136.226.77.103,ip,CTX.io,2.0483,SUCCESS
2025-12-20 07:04:42,136.226.77.103,ip,VirusTotal,0.3865,SUCCESS
2025-12-20 07:04:43,165.225.26.101,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:04:43,165.225.26.101,ip,OTX AlienVault,0.2434,SUCCESS
2025-12-20 07:04:45,165.225.26.101,ip,AbuseIPDB,0.3016,SUCCESS
2025-12-20 07:04:45,165.225.26.101,ip,CTX.io,0.8373,SUCCESS
2025-12-20 07:04:47,155.91.45.242,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:04:48,155.91.45.242,ip,OTX AlienVault,0.7260,SUCCESS
2025-12-20 07:04:49,155.91.45.242,ip,AbuseIPDB,0.3659,SUCCESS
2025-12-20 07:04:51,155.91.45.242,ip,CTX.io,2.2399,SUCCESS
2025-12-20 07:04:52,165.225.209.4,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:04:53,165.225.209.4,ip,OTX AlienVault,1.0542,SUCCESS
2025-12-20 07:04:54,165.225.209.4,ip,AbuseIPDB,0.3509,SUCCESS
2025-12-20 07:04:56,165.225.209.4,ip,CTX.io,2.1388,SUCCESS
2025-12-20 07:04:58,147.161.131.1,ip,OTX AlienVault,0.2465,SUCCESS
2025-12-20 07:04:59,147.161.131.1,ip,AbuseIPDB,0.3531,SUCCESS
2025-12-20 07:05:00,147.161.131.1,ip,CTX.io,1.9731,SUCCESS
2025-12-20 07:05:08,147.161.131.1,ip,VirusTotal,0.9339,SUCCESS
2025-12-20 07:05:12,136.226.67.101,ip,OTX AlienVault,0.2240,SUCCESS
2025-12-20 07:05:12,136.226.67.101,ip,AbuseIPDB,0.3146,SUCCESS
2025-12-20 07:05:13,136.226.67.101,ip,CTX.io,1.4730,SUCCESS
2025-12-20 07:05:13,136.226.67.101,ip,VirusTotal,0.3791,SUCCESS
2025-12-20 07:05:16,94.188.248.74,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:05:16,94.188.248.74,ip,OTX AlienVault,0.2376,SUCCESS
2025-12-20 07:05:18,94.188.248.74,ip,AbuseIPDB,0.5263,SUCCESS
2025-12-20 07:05:20,94.188.248.74,ip,CTX.io,2.9381,SUCCESS
2025-12-20 07:05:25,165.225.213.7,ip,AbuseIPDB,0.3490,SUCCESS
2025-12-20 07:05:25,165.225.213.7,ip,OTX AlienVault,0.8358,SUCCESS
2025-12-20 07:05:27,165.225.213.7,ip,CTX.io,2.2327,SUCCESS
2025-12-20 07:05:31,165.225.213.7,ip,VirusTotal,0.4332,SUCCESS
2025-12-20 07:05:36,165.225.8.79,ip,AbuseIPDB,0.3336,SUCCESS
2025-12-20 07:05:36,165.225.8.79,ip,OTX AlienVault,0.4538,SUCCESS
2025-12-20 07:05:38,165.225.8.79,ip,CTX.io,2.0469,SUCCESS
2025-12-20 07:05:40,165.225.8.79,ip,VirusTotal,0.5138,SUCCESS
2025-12-20 07:05:45,136.226.80.97,ip,OTX AlienVault,0.2585,SUCCESS
2025-12-20 07:05:45,136.226.80.97,ip,AbuseIPDB,0.3095,SUCCESS
2025-12-20 07:05:46,136.226.80.97,ip,CTX.io,0.6194,SUCCESS
2025-12-20 07:05:51,136.226.80.97,ip,VirusTotal,0.4405,SUCCESS
2025-12-20 07:05:54,192.241.230.19,ip,AbuseIPDB,0.3372,SUCCESS
2025-12-20 07:05:55,192.241.230.19,ip,CTX.io,0.7971,SUCCESS
2025-12-20 07:06:01,192.241.230.19,ip,VirusTotal,0.5040,SUCCESS
2025-12-20 07:06:06,192.241.230.19,ip,OTX AlienVault,11.8934,SUCCESS
2025-12-20 07:13:18,52.217.201.193,ip,VirusTotal,0.6300,SUCCESS
2025-12-20 07:13:18,52.217.201.193,ip,CTX.io,0.7250,SUCCESS
2025-12-20 07:13:18,52.217.201.193,ip,OTX AlienVault,0.7248,SUCCESS
2025-12-20 07:13:38,52.217.201.193,ip,AbuseIPDB,20.5831,SUCCESS
2025-12-20 07:13:41,3.5.3.152,ip,AbuseIPDB,0.3286,SUCCESS
2025-12-20 07:13:41,3.5.3.152,ip,OTX AlienVault,0.4419,SUCCESS
2025-12-20 07:13:41,3.5.3.152,ip,VirusTotal,0.4604,SUCCESS
2025-12-20 07:13:42,3.5.3.152,ip,CTX.io,0.9850,SUCCESS
2025-12-20 07:13:47,104.21.36.50,ip,OTX AlienVault,0.2534,SUCCESS
2025-12-20 07:13:47,104.21.36.50,ip,AbuseIPDB,0.3002,SUCCESS
2025-12-20 07:13:48,104.21.36.50,ip,CTX.io,0.8589,SUCCESS
2025-12-20 07:13:56,104.21.36.50,ip,VirusTotal,0.4407,SUCCESS
2025-12-20 07:13:58,210.120.17.252,ip,OTX AlienVault,0.2349,SUCCESS
2025-12-20 07:13:58,210.120.17.252,ip,AbuseIPDB,0.7462,SUCCESS
2025-12-20 07:13:58,210.120.17.252,ip,CTX.io,0.8478,SUCCESS
2025-12-20 07:14:02,210.120.17.252,ip,VirusTotal,0.5687,SUCCESS
2025-12-20 07:14:04,61.82.112.249,ip,OTX AlienVault,0.2587,SUCCESS
2025-12-20 07:14:04,61.82.112.249,ip,CTX.io,0.8324,SUCCESS
2025-12-20 07:14:04,61.82.112.249,ip,AbuseIPDB,0.9372,SUCCESS
2025-12-20 07:14:13,61.82.112.249,ip,VirusTotal,0.3917,SUCCESS
2025-12-20 07:14:17,162.243.189.2,ip,OTX AlienVault,0.2770,SUCCESS
2025-12-20 07:14:17,162.243.189.2,ip,AbuseIPDB,0.3207,SUCCESS
2025-12-20 07:14:18,162.243.189.2,ip,CTX.io,0.9498,SUCCESS
2025-12-20 07:14:19,162.243.189.2,ip,VirusTotal,0.4924,SUCCESS
2025-12-20 07:14:21,172.67.153.82,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:14:21,172.67.153.82,ip,OTX AlienVault,0.3159,SUCCESS
2025-12-20 07:14:23,172.67.153.82,ip,AbuseIPDB,0.3449,SUCCESS
2025-12-20 07:14:24,172.67.153.82,ip,CTX.io,0.7492,SUCCESS
2025-12-20 07:14:26,10.4.196.89,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:14:26,10.4.196.89,ip,OTX AlienVault,0.2250,SUCCESS
2025-12-20 07:14:27,10.4.196.89,ip,AbuseIPDB,0.3030,SUCCESS
2025-12-20 07:14:28,10.4.196.89,ip,CTX.io,0.8027,SUCCESS
2025-12-20 07:14:30,104.21.45.44,ip,VirusTotal,0,RATE_LIMIT
2025-12-20 07:14:30,104.21.45.44,ip,OTX AlienVault,0.2811,SUCCESS
2025-12-20 07:14:32,104.21.45.44,ip,AbuseIPDB,0.3102,SUCCESS
2025-12-20 07:14:32,104.21.45.44,ip,CTX.io,0.7990,SUCC
```

Audit Trail

DigiSigner Document ID: 5bde84cc-f368-4534-946d-499747cf99f4

Signer

Email: asep.kurniawan@tik.pnj.ac.id
IP Address: 2404:c0:2420::4f5f:61dd

Signature

Event	User	Time	IP Address
Upload document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/20/2025 10:04:54AM EST	180.252.174.141
Send for signing	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/20/2025 10:05:27AM EST	180.252.174.141
Open document	asep.kurniawan@tik.pnj.ac.id	12/20/2025 6:51:19PM EST	2404:c0:2420::4f5f:61dd
Sign document	asep.kurniawan@tik.pnj.ac.id	12/20/2025 6:51:41PM EST	2404:c0:2420::4f5f:61dd
Close document	asep.kurniawan@tik.pnj.ac.id	12/20/2025 6:51:41PM EST	2404:c0:2420::4f5f:61dd
Open document	asep.kurniawan@tik.pnj.ac.id	12/20/2025 6:51:44PM EST	2404:c0:2420::4f5f:61dd
Download document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/20/2025 7:04:26PM EST	180.252.174.141
Open document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/20/2025 7:04:30PM EST	180.252.174.141
Download document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/22/2025 10:24:31AM EST	103.18.34.162

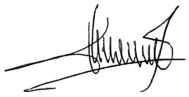
Audit Trail

DigiSigner Document ID: d73e0101-f773-458c-ba0e-aadd1d81fcf4

Signer

Email: indra.hermawan@tik.pnj.ac.id
IP Address: 103.36.14.70

Signature



Event	User	Time	IP Address
Upload document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/23/2025 5:24:35AM EST	103.18.34.162
Send for signing	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/23/2025 5:25:13AM EST	103.18.34.162
Open document	muhammad.ilham.sutama.tik22@mhsw.pnj.ac.id	12/23/2025 5:25:17AM EST	103.18.34.162
Open document	indra.hermawan@tik.pnj.ac.id	12/23/2025 5:30:41AM EST	103.36.14.70
Sign document	indra.hermawan@tik.pnj.ac.id	12/23/2025 5:30:51AM EST	103.36.14.70
Close document	indra.hermawan@tik.pnj.ac.id	12/23/2025 5:30:51AM EST	103.36.14.70