

**TUGAS AKHIR
SKEMA MAGANG**

**IMPLEMENTASI MODEL CONTEXT PROTOCOL (MCP)
UNTUK INTEGRASI MULTI-TOOLS OSINT DALAM
ANALISIS THREAT INTELLIGENCE BERBASIS LARGE
LANGUAGE MODEL (LLM)**



JOHAN MAULANA

NIM : 225510014

**PROGRAM STUDI TEKNIK KOMPUTER
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2026**

**TUGAS AKHIR
SKEMA MAGANG**

**IMPLEMENTASI MODEL CONTEXT PROTOCOL (MCP)
UNTUK INTEGRASI MULTI-TOOLS OSINT DALAM
ANALISIS THREAT INTELLIGENCE BERBASIS LARGE
LANGUAGE MODEL (LLM)**

**Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada
Program Sarjana**

Program Studi Teknik Komputer

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Disusun Oleh

JOHAN MAULANA

NIM : 225510014

**PROGRAM STUDI TEKNIK KOMPUTER
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2026**

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul : IMPLEMENTASI MODEL CONTEXT PROTOCOL (MCP) UNTUK INTEGRASI MULTI-TOOLS OSINT DALAM ANALISIS THREAT INTELLIGENCE BERBASIS LARGE LANGUAGE MODEL (LLM)

Nama : Johan Maulana

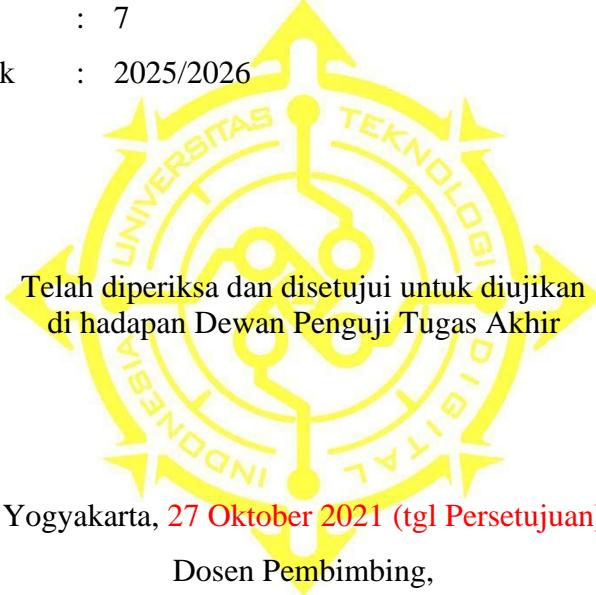
NIM : 225510014

Program Studi : Teknik Komputer

Program : Sarjana

Semester : 7

Tahun Akademik : 2025/2026



Ir. M. Guntara, M.T.
NIDN : 0509066101

HALAMAN PENGESAHAN

IMPLEMENTASI MODEL CONTEXT PROTOCOL (MCP) UNTUK INTEGRASI MULTI-TOOLS OSINT DALAM ANALISIS THREAT INTELLIGENCE BERBASIS LARGE LANGUAGE MODEL (LLM)



Telah dipertahankan di depan Dewan Pengaji dan dinyatakan diterima untuk
memenuhi sebagian persyaratan guna memperoleh
Gelar Sarjana Komputer
Program Studi Teknik Komputer
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia

Yogyakarta, 1 Januari 2022 (tgl Ujian)

Dewan Pengaji

NIDN

Tandatangan

- | | | |
|---------------------------------------|-------|-------|
| 1. Nama Dosen Pengaji (Ketua) | | |
| 2. Nama Dosen Pembimbing (Sekretaris) | | |
| 3. Nama Dosen Pengaji (Anggota) | | |

Mengetahui

Ketua Program Studi Teknik Komputer

Adiyuda Prayitna, S.T, M.T.
NIDN : 0506067901

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 27 Oktober 2021 (tgl Persetujuan)

Tanda tangan mhs

Johan Maulana
NIM: 225510014

HALAMAN PERSEMPAHAN

Dengan penuh rasa syukur, penulis memanjatkan puji dan terima kasih ke hadirat Allah SWT atas limpahan rahmat, kekuatan, serta hidayah-Nya, sehingga penulis dapat menyelesaikan laporan Tugas Akhir ini sebagai salah satu syarat dalam menuntaskan jenjang pendidikan sarjana. Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW, sebagai teladan yang membawa umat manusia menuju kemajuan ilmu pengetahuan dan peradaban yang penuh cahaya seperti saat ini.

Sebagai wujud rasa syukur dan terima kasih, laporan Tugas Akhir ini penulis dedikasikan kepada:

1. Ibu yang selalu memberikan dukungan dan doa dalam setiap proses yang penulis jalani. Terima kasih atas segala kasih sayang, pengorbanan, dan kesabaran yang tidak pernah putus. Doa Ibu adalah kekuatan terbesar yang membantu penulis melewati masa-masa sulit hingga tugas akhir ini selesai.
2. Ayah yang selalu memberikan semangat dan nasihat di setiap tantangan. Terima kasih atas ketegasan dan bimbingannya yang telah membentuk penulis menjadi pribadi yang lebih disiplin, kuat, serta berani dalam mengambil keputusan.
3. Adik yang menjadi salah satu penyemangat bagi penulis. Kehadiranmu menjadi pengingat bagi penulis untuk terus berusaha memberikan hasil yang terbaik dan menjadi contoh yang baik untuk masa depan bersama.
4. Rekan-rekan Magang di PT Solusi 247, yang telah memberikan bantuan, kerja sama, serta pengalaman berharga selama masa magang.

PRAKATA

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini. Tugas Akhir ini disusun untuk memenuhi salah satu syarat dalam memperoleh gelar Sarjana Komputer pada Program Studi Teknik Komputer, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia (UTDI) Yogyakarta.

Penulis menyadari bahwa selesainya Tugas Akhir ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Ibu Sri Redjeki, S.Si., M.Kom., Ph.D., selaku Rektor Universitas Teknologi Digital Indonesia.
2. Bapak Adiyuda Prayitna, S.T., M.T., selaku Ketua Program Studi Teknik Komputer Universitas Teknologi Digital Indonesia.
3. Bapak Ir. M. Guntara, M.T., selaku Dosen Pembimbing yang telah memberikan arahan, waktu, dan bimbingannya dengan penuh kesabaran selama penyusunan Tugas Akhir ini.
4. Keluarga, terutama Ayah, Ibu, dan Adik, yang selalu memberikan doa, kasih sayang, serta dukungan yang luar biasa sehingga penulis dapat menyelesaikan pendidikan ini.
5. HRD PT Solusi 247, yang telah memberikan kesempatan bagi penulis untuk melaksanakan kegiatan magang dan penelitian di lingkungan perusahaan.
6. Bapak Adriyansyah MF, selaku Mentor di PT Solusi 247 yang telah banyak berbagi ilmu serta pengalaman, memberikan arahan, dan membimbing penulis selama masa magang di perusahaan.
7. Seluruh rekan kerja dan teman-teman magang di PT Solusi 247, atas kerja sama, bantuan, serta lingkungan kerja yang positif dan suportif selama masa magang.

8. Teman-teman Teknik Komputer UTDI, atas solidaritas dan setiap momen berharga yang telah dilalui bersama selama menempuh pendidikan, yang menjadi motivasi tersendiri bagi penulis dalam menyelesaikan masa studi.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki keterbatasan dan jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang. Akhir kata, semoga Tugas Akhir ini dapat memberikan manfaat bagi pihak-pihak yang membutuhkan.

Yogyakarta, 3 Januari 2026

Johan Maulana
NIM: 225510014

INTISARI

Proses investigasi ancaman siber pada unit *Security Operations Center* (SOC) PT Solusi 247 menghadapi tantangan efisiensi akibat penggunaan berbagai perangkat *Open-Source Intelligence* (OSINT) yang belum terintegrasi. Kondisi ini menyebabkan alur kerja analis menjadi terpisah-pisah, memakan waktu, dan berisiko pada ketidakkonsistenan data saat memverifikasi *Indicators of Compromise* (IOC). Tugas akhir ini bertujuan untuk mengimplementasikan sistem integrasi berbasis *Model Context Protocol* (MCP) guna menyatukan berbagai layanan OSINT ke dalam antarmuka *Large Language Model* (LLM).

Sistem dibangun dengan menghubungkan layanan intelijen seperti VirusTotal, AbuseIPDB, GreyNoise, dan IPInfo melalui penerapan protokol MCP. Pendekatan ini memungkinkan LLM berinteraksi secara dinamis dengan API eksternal untuk melakukan pengambilan data berdasarkan instruksi analis. Pengujian dilakukan melalui berbagai skenario investigasi, termasuk analisis email *phishing*, verifikasi reputasi alamat IP, URL, dan *file hash* yang mencurigakan.

Hasil penelitian menunjukkan bahwa implementasi MCP berhasil menyederhanakan alur kerja investigasi melalui sentralisasi akses data. Sistem mampu merangkum data format JSON dari berbagai sumber menjadi informasi kontekstual yang mudah dipahami, sehingga mempercepat proses *triage* awal dan membantu analis meminimalkan kesalahan identifikasi (*false positive*). Integrasi ini terbukti efektif dalam meningkatkan efisiensi operasional analis SOC melalui penyederhanaan verifikasi indikator ancaman dalam satu antarmuka tunggal.

Kata kunci: *Model Context Protocol* (MCP), OSINT, *Large Language Model*, *Threat Intelligence*, *Security Operations Center*.

ABSTRACT

The cyber threat investigation process within the Security Operations Center (SOC) unit at PT Solusi 247 faces efficiency challenges due to the use of various unintegrated Open-Source Intelligence (OSINT) tools. This condition results in fragmented analyst workflows, is time-consuming, and poses risks of data inconsistency when verifying Indicators of Compromise (IOC). This final project aims to implement an integration system based on the Model Context Protocol (MCP) to unify various OSINT services into a Large Language Model (LLM) interface.

The system was developed by connecting intelligence services such as VirusTotal, AbuseIPDB, GreyNoise, and IPinfo through the implementation of the MCP protocol. This approach enables the LLM to interact dynamically with external APIs to perform data retrieval based on analyst instructions. Testing was conducted through various investigation scenarios, including phishing email analysis and reputation verification of suspicious IP addresses, URLs, and file hashes.

The research results demonstrate that the MCP implementation successfully streamlines investigation workflows through centralized data access. The system is capable of summarizing JSON format data from multiple sources into easily understandable contextual information, thereby accelerating the initial triage process and assisting analysts in minimizing false positives. This integration has proven effective in increasing the operational efficiency of SOC analysts by simplifying the verification of threat indicators within a single unified interface.

Keywords: Model Context Protocol (MCP), OSINT, Large Language Model, Threat Intelligence, Security Operations Center.

DAFTAR ISI

Hal

TUGAS AKHIR SKEMA MAGANG.....	i
HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
HALAMAN PERSEMBAHAN	v
PRAKATA.....	vi
INTISARI	viii
ABSTRACT.....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Deskripsi Pekerjaan	3
1.3 Tujuan.....	4
1.4 Manfaat.....	5
BAB II PROFIL INSTANSI TEMPAT MAGANG	6
2.1 Sejarah dan Profil Umum Perusahaan	6
2.2 Struktur Organisasi.....	7
2.3 Struktur Organisasi Bidang IT <i>Security</i>	8
2.4 Lokasi Perusahaan	9
2.5 Area Pekerjaan Perusahaan	10
BAB III DESKRIPSI KEGIATAN.....	9
3.1 Persoalan.....	9
3.2 Deskripsi Produk	9
3.3 Analisis dan Rancangan.....	10
3.3.1 Analisis Kebutuhan Sistem	11
3.3.2 Arsitektur Sistem.....	12
3.3.3 Rancangan Diagram Alir.....	14
3.4 Jadwal Kerja	15
BAB IV HASIL DAN PEMBAHASAN	20
4.1 Hasil.....	20
4.1.1 Struktur Implementasi Sistem	20

4.1.2	Implementasi MCP Server (main.py).....	22
4.1.3	Implementasi Modul Integrasi OSINT	27
4.2	Uji coba	33
4.2.1	Metode Pengujian.....	33
4.2.2	Skenario Pengujian.....	34
4.2.3	Hasil <i>Black-Box Testing</i> (Pengujian Fungsionalitas)	35
4.2.4	Hasil <i>Case-Based Scenario Testing</i> (Relevansi Operasional).....	40
4.3	Pembahasan	48
4.3.1	Analisis Efektivitas Integrasi Multi-Tool (OSINT Routing)	49
4.3.2	Analisis Peran LLM dalam Interpretasi Data.....	49
4.3.3	Relevansi dengan Kebutuhan Operasional SOC.....	50
4.3.4	Hambatan dan Batasan Sistem	51
BAB V	PENUTUP	52
5.1	Simpulan.....	52
5.2	Saran	53
DAFTAR	PUSTAKA	54
LAMPIRAN	55

DAFTAR GAMBAR

	Hal
Gambar 2. 1 Struktur Organisasi PT Solusi247	7
Gambar 2. 2 Struktur Organisasi Bidang IT Security	8
Gambar 3. 1 Arsitektur Sistem.....	13
Gambar 3. 2 Diagram Alir	14
Gambar 4. 1 Struktur Direktori Sistem	21
Gambar 4. 2 Fungsi handle_list_tools.....	23
Gambar 4. 3 Fungsi handle_call_tool	26
Gambar 4. 4 Konfigurasi MCP di Developer Settings Claude Desktop	27
Gambar 4. 5 virustotal_tool.py	29
Gambar 4. 6 abuseipdb_tool.py	30
Gambar 4. 7 greynoise_tool.py	31
Gambar 4. 8 ipinfo_tool.py	33
Gambar 4. 9 Input user dan Pemicuan Tool Call JSON	36
Gambar 4. 10 Input Pengguna dan Pemicuan routing sistem	37
Gambar 4. 11 Formatted JSON Response Summary	38
Gambar 4. 12 Deteksi Error Format Input	39
Gambar 4. 13 Respons LLM untuk Penanganan Error Format	39
Gambar 4. 14 Ringkasan Keamanan dan Hasil Analisis Awal	41
Gambar 4. 15 Hasil Analisis Tambahan	42
Gambar 4. 16 Kesimpulan dari LLM	42
Gambar 4. 17 Hasil ringkasan deteksi malware.....	43
Gambar 4. 18 Ringkasan Keamanan dan Hasil Deteksi VirusTotal	44
Gambar 4. 19 Analisis Risiko dan Identifikasi Red Flags	45
Gambar 4. 20 Kesimpulan Akhir dan Rekomendasi Mitigasi	45
Gambar 4. 21 Hasil dari LLM.....	47
Gambar 4. 22 Hasil lanjutan dari LLM.....	48
Gambar 4. 23 Kesimpulan akhir	48

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan *Large Language Models* (LLM) seperti GPT-3 telah memungkinkan otomatisasi berbagai tugas berbasis bahasa, mulai dari menjawab pertanyaan hingga menulis laporan teknis (Bommasani et al., 2022). Namun, LLM bersifat *static* terhadap pengetahuan, artinya model ini tidak dapat mengakses informasi di luar data pelatihannya dan tidak memiliki kemampuan bawaan untuk berinteraksi dengan sumber eksternal secara *real-time* (Mialon et al., 2023). Akibatnya, meskipun mampu menghasilkan respons yang koheren, LLM tidak dapat secara langsung mengambil data terkini dari internet, memanggil API, atau menjalankan alat eksternal tanpa mekanisme integrasi tambahan.

Untuk mengatasi keterbatasan akses eksternal pada LLM, berbagai pendekatan integrasi telah dikembangkan. Salah satunya adalah *tool augmentation*, yaitu pemberian kemampuan kepada LLM untuk berinteraksi dengan alat bantu eksternal seperti *Application Programming Interface* (API), basis data, atau skrip analisis. Pendekatan ini memungkinkan LLM memperluas fungsinya di luar pemrosesan bahasa murni, misalnya dengan mengambil data terkini dari internet atau menjalankan fungsi khusus sesuai kebutuhan konteks (Mialon et al., 2023). Salah satu standar terkini yang mendukung integrasi tersebut adalah *Model Context Protocol* (MCP), sebuah spesifikasi komunikasi terbuka yang memungkinkan LLM berinteraksi secara dinamis dengan layanan eksternal melalui antarmuka standar berbasis JSON-RPC (*JavaScript Object Notation-Remote Procedure Call*) (Model Context Protocol, n.d.). MCP memisahkan logika model dari alat eksternal, sehingga kredensial, *API key*, dan logika bisnis tetap berada di luar model. Dengan demikian, sistem menjadi lebih modular, aman, dan mudah dipelihara, karena setiap *tool* dapat dikembangkan, diperbarui, atau diganti tanpa mengubah inti model bahasa.

Dalam ranah keamanan siber, *Open-Source Intelligence* (OSINT) memainkan peran kritis dalam mengumpulkan dan menganalisis data publik yang relevan dengan ancaman digital, seperti alamat IP berbahaya atau aktivitas *phishing*. Sumber-sumber umum meliputi media sosial (terutama Twitter), forum daring, basis data kerentanan publik publik seperti *National Vulnerability Database* (NVD), serta layanan intelijen ancaman terbuka seperti *feed* reputasi IP dan deteksi lalu lintas anomali. Namun, praktik OSINT saat ini sering mengandalkan berbagai alat terpisah, misalnya Shodan untuk pemetaan perangkat, VirusTotal untuk analisis malware, atau TheHarvester untuk pengumpulan email, yang umumnya dioperasikan secara manual dan memerlukan koordinasi antar platform. Studi sistematis menunjukkan bahwa sebagian besar penelitian berbasis AI dalam OSINT masih fokus pada tahap pemrosesan dan analisis data, sementara integrasi dengan alat OSINT yang sudah ada (*pre-existing OSINT tools*) masih sangat terbatas. Kondisi ini menunjukkan bahwa potensi integrasi antara sistem berbasis AI dan alat OSINT yang telah digunakan di lapangan belum dimanfaatkan secara optimal, suatu peluang yang dapat memberikan manfaat signifikan bagi pengguna OSINT (Browne et al., 2024).

Dalam magang sebagai *Security Operations Center* (SOC) Analyst di PT Solusi 247, teridentifikasi sejumlah tantangan dalam proses investigasi ancaman, khususnya terkait kurangnya integrasi berbagai alat OSINT terbuka dan kompleksitas dalam mengoordinasikan alur kerja analisis. Berdasarkan observasi tersebut, Tugas Akhir ini dikembangkan untuk memberi solusi agar dapat mempercepat identifikasi dan korelasi *Indicators of Compromise* (IOC). Penelitian ini mengusulkan penerapan MCP sebagai mekanisme integrasi antara LLM dan sejumlah *tools* OSINT dalam satu sistem terpadu. Sistem ini dirancang agar LLM dapat mengakses data intelijen terkini, seperti infrastruktur jaringan dan reputasi aset, sehingga proses analisis IOC dapat dilakukan secara lebih efisien dan terstruktur. Meskipun belum diterapkan selama kegiatan magang, solusi ini diharapkan dapat menjadi pertimbangan pengembangan alur kerja SOC di masa depan.

1.2 Deskripsi Pekerjaan

Pelaksanaan kegiatan magang dilakukan pada divisi SOC di PT Solusi 247 dengan peran utama sebagai *SOC Analyst*. Kegiatan magang berfokus pada pemantauan keamanan jaringan, deteksi ancaman, serta analisis insiden siber. Deskripsi pekerjaan berikut difokuskan pada aktivitas yang relevan dengan topik penelitian, khususnya dalam konteks integrasi data OSINT dan analisis indikator ancaman/IOC.

1. Pemantauan Log dan Alert Keamanan

Melakukan pemantauan harian terhadap log dari server dan perangkat jaringan menggunakan platform *Security Information and Event Management* (SIEM) untuk mendeteksi aktivitas mencurigakan. Aktivitas ini bertujuan mengidentifikasi potensi ancaman seperti upaya *brute-force*, *port scanning*, serta koneksi ke alamat IP berisiko atau indikator ancaman lainnya. Data hasil pemantauan tersebut menjadi sumber utama dalam proses analisis dan korelasi indikator ancaman.

2. Pembuatan *Rules* dan *Detektor Anomali*

Mengembangkan dan menguji *rules* pada sistem SIEM untuk mendeteksi pola serangan spesifik. Selain itu, merancang detektor berbasis anomali guna mengenali aktivitas tidak normal yang tidak terdeteksi oleh aturan konvensional. Proses ini mendukung penelitian terkait penerapan pendekatan terintegrasi antara analisis log keamanan dan pemanfaatan konteks data dalam sistem berbasis LLM.

3. Analisis Email *Phishing*

Melakukan analisis terhadap laporan email mencurigakan untuk mengidentifikasi ciri-ciri *phishing* seperti URL berbahaya, *spoofed header*, dan lampiran berisiko. Data hasil analisis, termasuk alamat IP, file hash, serta pola tautan, berkontribusi dalam pembangunan konteks ancaman yang dapat diolah lebih lanjut oleh sistem OSINT terpadu.

Melalui rangkaian pekerjaan tersebut, diperoleh pemahaman praktis mengenai tantangan integrasi data dari berbagai sumber keamanan, terutama terkait

ketergantungan pada *tools* OSINT yang terpisah serta proses manual dalam verifikasi IOC. Temuan ini menjadi dasar dalam perancangan dan implementasi MCP untuk integrasi multi-*tools* OSINT dengan LLM dalam penelitian ini.

1.3 Tujuan

Tujuan yang diharapkan dari pelaksanaan kegiatan magang sebagai *SOC Analyst* di PT Solusi 247 adalah memperoleh pengalaman praktis dalam operasional SOC dan memperdalam pemahaman mengenai mekanisme pertahanan siber berbasis *Blue Team*. Adapun tujuan yang ingin dicapai selama kegiatan magang adalah sebagai berikut:

1. Menguasai praktik pemantauan log sistem dan *security alert* menggunakan platform SIEM untuk mendeteksi aktivitas mencurigakan, seperti upaya *brute-force*, *port scanning*, dan koneksi ke asset berisiko.
2. Mampu merancang, menguji, dan mendokumentasikan *rules* deteksi serta mekanisme deteksi anomali yang efektif dalam mengidentifikasi pola serangan yang tidak tercakup oleh aturan konvensional.
3. Mampu menganalisis insiden keamanan yang dilaporkan, khususnya terkait email *phishing*, melalui identifikasi indikator ancaman seperti URL berbahaya, alamat IP mencurigakan, dan manipulasi *header* email.
4. Mampu menyusun laporan insiden yang komprehensif, mencakup ringkasan kejadian, bukti teknis, analisis risiko, serta rekomendasi mitigasi yang jelas dan aplikatif.
5. Memperoleh wawasan mengenai kolaborasi antar anggota tim keamanan, alur respons insiden, serta kebutuhan industri dalam menjaga ketahanan siber organisasi.

1.4 Manfaat

Kegiatan magang sebagai SOC *Analyst* di PT Solusi 247 memberikan sejumlah manfaat dalam pengembangan kompetensi teknis dan pemahaman operasional keamanan siber. Manfaat tersebut antara lain:

1. Peningkatan kemampuan dalam analisis *log* dan deteksi ancaman, melalui pemantauan harian terhadap *log* sistem dan *security alert*, sehingga mampu mengenali pola aktivitas mencurigakan, mengidentifikasi IOC, serta memprioritaskan insiden berdasarkan tingkat risiko.
2. Pemahaman praktis terhadap penerapan platform SIEM dalam mengelola alur kerja keamanan, termasuk pengembangan *detection rules* dan detektor anomali untuk memperluas cakupan deteksi di luar pola serangan konvensional.
3. Pengembangan keterampilan analisis insiden siber, khususnya dalam menangani kasus email *phishing*, mulai dari identifikasi tautan berbahaya, verifikasi reputasi alamat IP, hingga analisis *header* email untuk mendukung investigasi lebih lanjut.
4. Peningkatan kesadaran akan tanggung jawab profesional dalam menangani data sensitif, termasuk pentingnya kerahasiaan, integritas, dan akuntabilitas dalam setiap tahap respons insiden.
5. Penguatan orientasi solusi berbasis kebutuhan nyata, di mana pengalaman lapangan mendorong pengembangan Tugas Akhir berupa sistem integrasi OSINT dan LLM sebagai upaya menjawab tantangan efisiensi dalam investigasi ancaman.

BAB II

PROFIL INSTANSI TEMPAT MAGANG

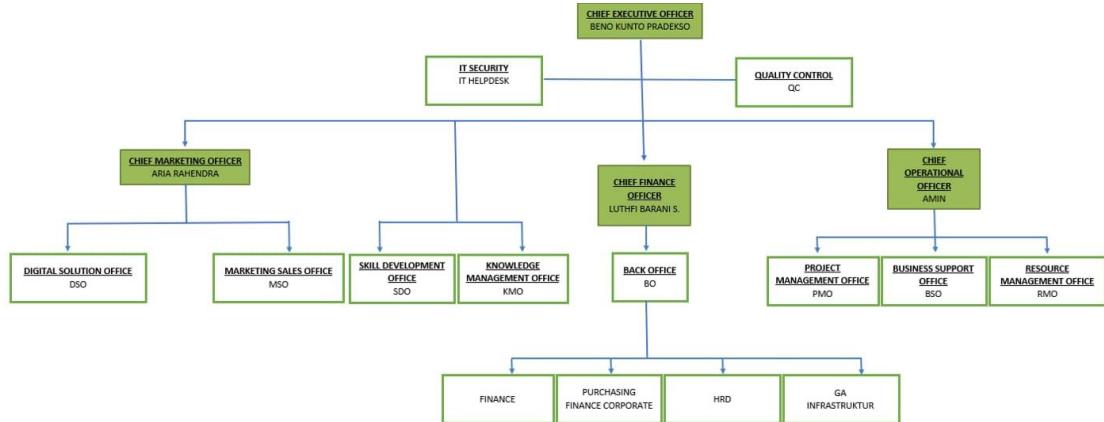
2.1 Sejarah dan Profil Umum Perusahaan

PT Dua Empat Tujuh (Solusi 247) merupakan perusahaan teknologi informasi dan data yang didirikan pada tahun 2000, dengan fokus utama pada pemrosesan data skala besar (*big data*) dan sistem berbasis teknologi tinggi. Dengan pengalaman lebih dari 20 tahun dalam proyek-proyek data serta sebagai perusahaan pertama dan terbesar yang mengimplementasikan klaster *big data* di Indonesia, PT Solusi 247 telah dikenal dan dipercaya sebagai penyedia solusi *big data* terkemuka di tanah air(*Home - Solusi247*, n.d.).

Perusahaan berkomitmen untuk menghadirkan produk dan solusi bernilai tinggi bagi pelanggan. Untuk mewujudkan hal tersebut, PT Solusi 247 mengalokasikan 20 persen dari sumber dayanya untuk kegiatan penelitian dan pengembangan (*research and development*), guna memastikan pelanggan memperoleh produk dan layanan mutakhir yang berkualitas.

Berdasarkan pengalaman panjang tersebut, PT Solusi 247 meyakini bahwa investasi teknologi dan implementasi yang tepat merupakan dua pilar utama yang menopang keberhasilan bisnis. Perusahaan memahami bahwa investasi teknologi saja tidak cukup untuk menjamin kesuksesan bisnis. Diperlukan pula upaya serius dalam proses implementasinya. Oleh karena itu, PT Solusi 247 tidak hanya mengembangkan teknologi, tetapi juga berkomitmen memberikan solusi terbaik yang disesuaikan dengan kebutuhan setiap pelanggan.

2.2 Struktur Organisasi



Gambar 2. 1 Struktur Organisasi PT Solusi247

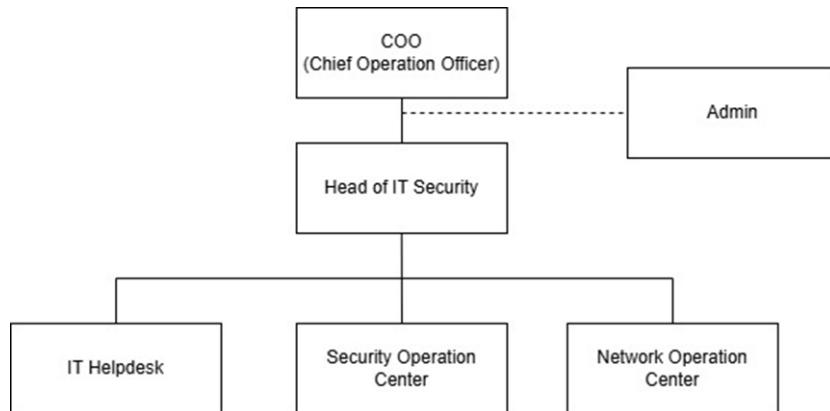
Gambar 2.1 merupakan struktur organisasi PT Solusi 247 yang dirancang untuk mendukung operasional yang efisien dan kolaboratif. Struktur organisasi Perusahaan meliputi :

1. *Chief Executive Officer (CEO)*: Beno Kunto Pradekso, bertugas mengambil keputusan strategis, mengawasi kinerja setiap divisi, serta mewakili perusahaan dalam hubungan dengan pihak luar seperti mitra, klien, dan investor.
2. *IT Security*: Bertugas menjaga dan meningkatkan keamanan informasi perusahaan dengan melindungi sistem, jaringan, dan data dari ancaman siber. Divisi ini juga mencakup layanan *IT Helpdesk* yang berperan dalam memberikan dukungan teknis, penanganan insiden, serta pemeliharaan operasional teknologi informasi bagi seluruh pengguna di lingkungan perusahaan.
3. *Quality Control (QC)*: Mengawasi standar kualitas di setiap aspek perusahaan.
4. *Chief Marketing Officer (CMO)*: Aria Rahendra, memimpin *Digital Solution Office (DSO)* dan *Marketing Sales Office (MSO)*.
5. *Skill Development Office (SDO)*: Berdiri langsung di bawah *CEO*, bertugas merancang, mengelola, dan mengevaluasi program pelatihan untuk

meningkatkan kompetensi karyawan.

6. *Knowledge Management Office (KMO)*: Langsung di bawah *CEO*, bertugas untuk mengelola pengetahuan organisasi.
7. *Chief Finance Officer (CFO)*: Luthfi Barani S, memimpin *Back Office (BO)* yang mencakup *Finance, Purchasing Finance Corporate, Human Resources Development (HRD)* dan *General Affairs (GA)* Infrastruktur.
8. *Chief Operational Officer (COO)*: Amin, memimpin *Project Management Office (PMO)*, *Business Support Office (BSO)*, dan *Resource Management Office (RMO)*.

2.3 Struktur Organisasi Bidang IT Security



Gambar 2. 2 Struktur Organisasi Bidang IT Security

Gambar 2.2 menampilkan struktur organisasi Divisi *Security* PT Solusi247 yang menggambarkan alur koordinasi, wewenang, dan tanggung jawab dalam pengelolaan teknologi informasi serta keamanan sistem guna mendukung efektivitas operasional dan keamanan data perusahaan.

Berikut penjelasan struktur organisasi berdasarkan diagram tersebut:

1. COO (*Chief Operation Officer*) adalah pimpinan yang bertanggung jawab atas operasional organisasi secara keseluruhan. Semua fungsi yang berkaitan dengan pengelolaan *IT Security* berada di bawah pengawasan dan kebijakan COO. Pada struktur ini, COO juga memiliki hubungan koordinatif

dengan bagian Admin, yang ditunjukkan dengan garis putus-putus. Artinya, Admin tidak langsung berada di bawah jalur komando, namun tetap memberikan dukungan operasional bila diperlukan.

2. *Head of IT Security* berada langsung di bawah COO dan bertanggung jawab untuk memimpin, mengawasi, dan mengembangkan kebijakan keamanan IT di perusahaan. Posisi ini bertugas memastikan bahwa sistem, jaringan, dan data perusahaan terlindungi dari ancaman keamanan.

Head of IT Security menjadi pusat koordinasi dari tiga unit operasional berikut:

- a. *IT Helpdesk* : Bertanggung jawab menangani keluhan, permintaan bantuan teknis, serta permasalahan pengguna internal guna memastikan layanan IT berjalan lancar.
- b. *Security Operation Center (SOC)* : Bertugas memantau dan menganalisis keamanan sistem serta jaringan, mendeteksi dan menangani insiden siber, serta melakukan monitoring log dan aktivitas mencurigakan menggunakan sistem SIEM.
- c. *Network Operation Center (NOC)* : Bertanggung jawab mengelola, memantau, dan memelihara infrastruktur jaringan guna menjamin ketersediaan, stabilitas, dan kualitas konektivitas perusahaan.

2.4 Lokasi Perusahaan

PT Solusi 247 didirikan pada tahun 2000, dengan kantor pusat yang berlokasi di Segitiga Emas Business Park, Jl. Prof. Dr. Satrio KAV 6, Jakarta Selatan, 12940, Indonesia. Selain kantor pusat di Jakarta, perusahaan ini juga memiliki kantor cabang di Yogyakarta, yang berlokasi di Jl. Cantel No.352, Muja Muju, Kec. Umbulharjo, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55221, yang turut mendukung kegiatan operasional perusahaan dalam pengolahan Big Data dan pengembangan solusi teknologi informasi dan komunikasi (TIK).

2.5 Area Pekerjaan Perusahaan

Sebagai perusahaan yang bergerak di bidang pengembangan TIK, PT Solusi 247 memiliki sejumlah area pekerjaan utama yang menjadi fokus operasionalnya. Bidang-bidang tersebut dikembangkan secara terintegrasi guna mendukung ketangguhan dan inovasi dalam ekosistem digital. Adapun area-area tersebut adalah sebagai berikut:

1. Pengolahan *Big Data*

PT Solusi 247 menyediakan layanan pengelolaan, pemrosesan, dan analisis data skala besar (*large-scale data*) untuk berbagai sektor industri guna menghasilkan nilai strategis bagi klien.

2. Keamanan Siber

PT Solusi 247 mengembangkan solusi deteksi ancaman (*threat detection*), pemantauan keamanan (*security monitoring*), serta manajemen risiko berbasis indikator dan perilaku (*indicator- and behavior-based detection*).

3. Sistem Informasi dan Infrastruktur IT

PT Solusi 247 melayani perancangan, pengembangan, dan pemeliharaan sistem informasi serta infrastruktur teknologi informasi untuk menjamin keandalan dan keamanan operasional sistem klien.

4. Riset dan Pengembangan Teknologi

Kegiatan riset dan pengembangan (*research and development/R&D*) merupakan salah satu pilar strategis perusahaan. Sekitar 20% dari total sumber daya dialokasikan untuk inisiatif R&D, dengan fokus pada penciptaan produk dan teknologi baru yang inovatif, relevan dengan kebutuhan pasar, serta mendukung kemajuan ekosistem TIK nasional.

5. Digital Solution dan Layanan IT

Perusahaan juga menawarkan layanan pendukung transformasi digital, mencakup pengembangan aplikasi, integrasi sistem lintas platform, serta manajemen layanan teknologi informasi (*IT service management*). Pendekatan terpadu ini dirancang untuk mempercepat adopsi teknologi serta meningkatkan efisiensi operasional klien.

BAB III

DESKRIPSI KEGIATAN

3.1 Persoalan

Selama kegiatan magang di divisi *Security Operations Center* (SOC) di PT Solusi 247, ditemukan tantangan utama berupa alur kerja investigasi yang tidak terintegrasi akibat penggunaan berbagai *tools Open-Source Intelligence* (OSINT) secara terpisah. Ketika menganalisis insiden seperti email *phishing* atau aktivitas jaringan mencurigakan, analis keamanan harus memverifikasi *Indicators of Compromise* (IOC), seperti alamat IP, URL, atau *file hash*, dengan mengakses beberapa platform berbeda secara bergantian. Proses ini memerlukan perpindahan antar-antarmuka, serta penggabungan informasi yang memakan waktu, terutama saat beban insiden meningkat. Selain itu, hasil investigasi cenderung kurang konsisten karena sangat bergantung pada metode kerja masing-masing analis, serta berisiko terhadap *human error*. Kondisi ini menghambat kemampuan tim SOC untuk memberikan respons yang cepat dan terstandar, sekaligus menambah beban kerja operasional analis dalam menjalankan tugas sehari-hari.

3.2 Deskripsi Produk

Sebagai respons terhadap tantangan yang diamati selama magang di divisi SOC PT Solusi 247, dikembangkan sebuah prototipe sistem berbasis *Model Context Protocol* (MCP). Sistem ini dirancang untuk membantu analis keamanan dalam memverifikasi IOC, seperti alamat IP, URL, dan *file hash*, menggunakan sumber OSINT yang relevan dengan tugas SOC. Alih-alih membuka beberapa platform secara terpisah, sistem memungkinkan *Large Language Model* (LLM) untuk mengambil data dari empat layanan OSINT:

1. VirusTotal

Digunakan untuk analisis reputasi IP, URL, dan *file hash* berdasarkan agregasi berbagai mesin pemindai keamanan global.

2. AbuseIPDB

Digunakan untuk penilaian risiko IP berdasarkan jumlah laporan pelanggaran dari komunitas pengguna.

3. GreyNoise

Digunakan untuk memfilter lalu lintas jaringan umum (seperti *scanner*, *crawler*) yang tidak berbahaya, sehingga analis dapat fokus pada ancamannya.

4. IPinfo

Digunakan untuk konteks jaringan dan geografis, seperti negara, ISP, ASN, dan lokasi fisik.

Arsitektur sistem bersifat modular, dengan MCP sebagai protokol perantara standar yang menjembatani LLM dengan layanan eksternal, sehingga integrasi dapat dilakukan tanpa mengubah inti model bahasa. Sistem hanya menerima *input* berupa indikator teknis yang didukung oleh layanan tersebut. Prototipe ini dikembangkan secara lokal selama magang dan belum diimplementasikan di lingkungan operasional perusahaan. Meski demikian, pengujian terbatas menunjukkan bahwa sistem mampu mempercepat proses verifikasi awal IOC, khususnya dalam kasus email *phishing* dan koneksi jaringan mencurigakan.

3.3 Analisis dan Rancangan

Bagian ini menjelaskan kebutuhan sistem serta rancangan prototipe sistem yang dikembangkan untuk menjawab tantangan tersebut. Sistem dibangun menggunakan MCP sebagai protokol perantara antara LLM dan layanan OSINT yang digunakan. Tujuannya adalah mempercepat proses verifikasi awal IOC (IP, URL, dan *file hash*) melalui penggabungan informasi yang lebih terpusat.

Penjelasan mencakup kebutuhan fungsional dan non-fungsional, arsitektur sistem, serta rancangan diagram alir. Semua disusun secara sederhana, sesuai dengan ruang lingkup pengembangan selama magang dan kemampuan prototipe sebagai *proof of concept*.

3.3.1 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem bertujuan untuk mengidentifikasi apa yang diperlukan agar sistem dapat menyelesaikan persoalan investigasi yang diamati selama magang. Proses ini dilakukan dengan memahami alur kerja investigasi di SOC, mengamati hambatan operasional yang terjadi, serta menentukan fitur dan kriteria yang dibutuhkan. Fokus utama analisis ini terbagi ke dalam dua aspek utama, yaitu kebutuhan fungsional yang mendefinisikan apa yang harus mampu dilakukan oleh sistem, serta kebutuhan non-fungsional yang menentukan bagaimana sistem tersebut seharusnya bekerja dan beroperasi untuk mendukung pengguna.

Kebutuhan fungsional:

1. Menerima *input* berupa IOC, seperti IP, URL, atau *file hash*.
2. Menentukan sumber OSINT yang relevan berdasarkan jenis IOC yang dimasukkan.
3. Mengambil data dari sumber OSINT melalui protokol MCP.
4. Menyusun hasil menjadi ringkasan dalam bahasa alami yang mudah dipahami.

Kebutuhan non-fungsional:

1. Modularitas
Setiap komponen dapat dikembangkan atau diganti tanpa mengganggu sistem secara keseluruhan.
2. Keamanan
Kredensial API dikelola melalui *developer settings* di Claude Desktop dan tidak muncul dalam respons, sehingga risiko kebocoran dapat diminimalkan.
3. Kemudahan penggunaan
Pengguna hanya berinteraksi melalui Claude Desktop dengan mengetikkan pertanyaan dalam bahasa alami, tanpa perlu antarmuka atau sintaks

tambahan.

4. Keandalan

Jika salah satu sumber OSINT tidak merespons, sistem tetap memberikan hasil dari sumber lain atau menyampaikan pesan bahwa data tersebut tidak tersedia, sehingga alur investigasi tetap dapat berlanjut.

3.3.2 Arsitektur Sistem

Arsitektur sistem menggambarkan komponen utama dalam prototipe yang dikembangkan selama magang. Sistem memanfaatkan MCP sebagai standar komunikasi antara LLM dan layanan eksternal. MCP merupakan protokol terbuka yang digunakan sebagai penghubung antara LLM dan layanan eksternal, dan tidak dikembangkan dalam penelitian ini.

Komponen utama sistem terdiri dari:

1. User

User berperan sebagai aktor eksternal yang memasukkan IOC seperti alamat IP, URL, atau *file hash*, ke dalam sistem. User juga menjadi pihak yang menerima hasil analisis yang dihasilkan oleh sistem.

2. Claude

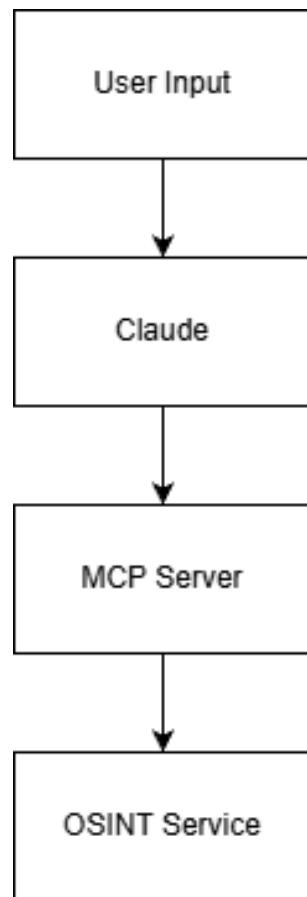
Claude berfungsi sebagai antarmuka pengguna sekaligus lingkungan eksekusi LLM. User berinteraksi dengan sistem melalui Claude dengan mengetikkan perintah atau IOC dalam bahasa alami. Claude bertanggung jawab untuk menganalisis *input*, menentukan apakah dibutuhkan data eksternal, serta mengorkestrasi pemanggilan tool melalui protokol MCP.

3. MCP Server

MCP Server dijalankan melalui skrip Python (main.py) dan bertindak sebagai penghubung antara Claude dan layanan OSINT eksternal. Server ini menerima permintaan dari Claude, menerjemahkannya ke dalam pemanggilan API OSINT sesuai spesifikasi MCP, lalu mengembalikan hasilnya ke Claude.

4. OSINT Service

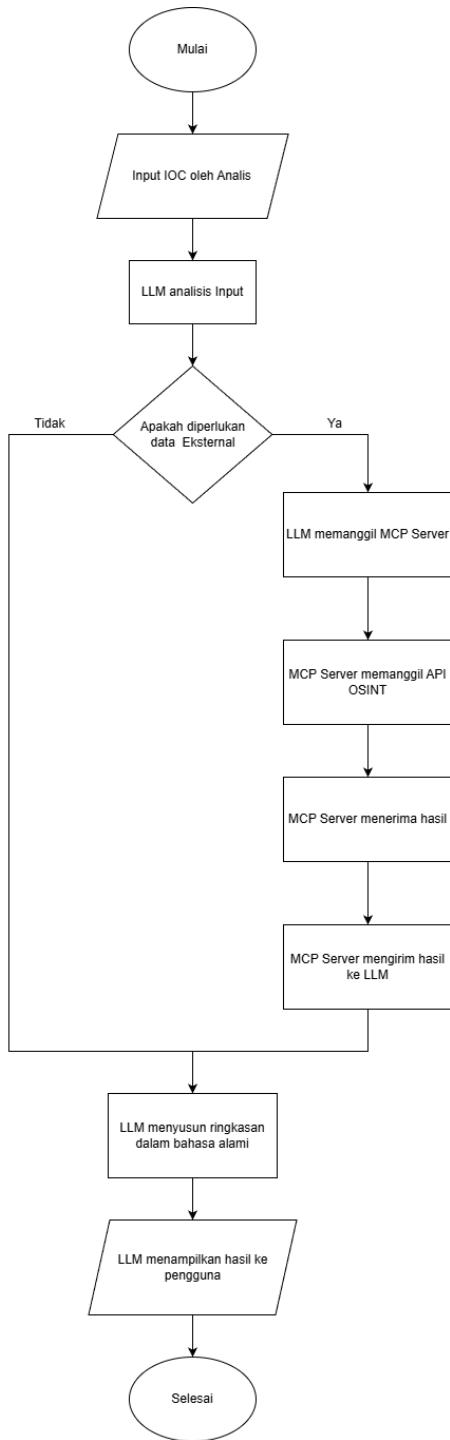
OSINT *Service* merupakan kumpulan layanan intelijen keamanan publik, seperti VirusTotal, AbuseIPDB, Greynoise dan IPinfo, yang menyediakan data reputasi dan informasi ancaman. Layanan ini diakses oleh MCP Server untuk memperoleh data yang dibutuhkan dalam proses analisis IOC.



Gambar 3. 1 Arsitektur Sistem

Gambar 3.1 menunjukkan hubungan antar komponen utama. Pengguna memberikan perintah melalui Claude, yang kemudian diteruskan ke MCP *Server*. Selanjutnya, MCP *Server* mengakses Integrasi OSINT untuk mengambil data dari layanan eksternal sebelum dikembalikan kembali ke pengguna dalam bentuk informasi yang sudah terolah.

3.3.3 Rancangan Diagram Alir



Gambar 3. 2 Diagram Alir

Gambar 3.2 menunjukkan diagram alir sistem yang menggambarkan urutan proses dari *input* pengguna hingga respons akhir. Proses dimulai ketika analis

memasukkan sebuah IOC, seperti alamat IP, URL, atau *file hash*, ke dalam antarmuka Claude Desktop. LLM kemudian menganalisis *input* tersebut untuk mengidentifikasi jenis IOC serta menentukan apakah diperlukan data tambahan dari sumber eksternal. Apabila data eksternal diperlukan, LLM akan mengirimkan permintaan ke MCP Server, yang berfungsi sebagai perantara antara LLM dan berbagai layanan OSINT. MCP Server kemudian memanggil modul OSINT yang sesuai, seperti VirusTotal atau AbuseIPDB, untuk melakukan pencarian data intelijen terhadap IOC tersebut. Setelah hasil dari API OSINT diterima, MCP Server mengirimkan data tersebut kembali ke LLM. LLM kemudian mengolah dan menginterpretasikan data teknis tersebut menjadi ringkasan analisis dalam bahasa alami, termasuk *verdict* dan tingkat risiko IOC. Tahap terakhir adalah LLM menampilkan hasil analisis kepada pengguna dalam bentuk laporan yang mudah dipahami, sehingga analis dapat dengan cepat mengambil keputusan berdasarkan informasi yang diperoleh.

3.4 Jadwal Kerja

Kegiatan magang dilaksanakan dengan penugasan sebagai *SOC Analyst*, yang mencakup pemantauan, analisis, dan penanganan insiden keamanan informasi. Gambaran jadwal kegiatan selama magang ditunjukkan pada Tabel 3.1.

Table 3. 1 Gambaran Jadwal Kegiatan Magang

No	Bulan	Minggu	Keterangan
1	September 2025	3	<ol style="list-style-type: none"> 1. Tanda tangan perjanjian kebijakan, pengenalan perusahaan, penjelasan tata tertib perusahaan, dan explorasi <i>Security Information and Event Management</i> (SIEM) Wazuh. 2. Penyampaian materi <i>cyber security</i> dan SIEM Wazuh oleh mentor. 3. Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh. 4. Melakukan Analisis Log yang diberikan oleh mentor.

			<p>5. Mengembangkan dan menambahkan <i>rules</i> Wazuh.</p>
		4	<ol style="list-style-type: none"> 1. Melakukan analisis log yang diberikan oleh mentor dan mengembangkan <i>rulesnya</i>. 2. Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh. 3. Melakukan <i>meeting</i> divisi cyber security. 4. Git clone repositori ELK Stack dan website vulnerable dari mentor untuk kebutuhan pengujian
2	Oktober 2025	1	<ol style="list-style-type: none"> 1. Melakukan Latihan sebagai <i>Offensive</i> dan <i>Defensive</i>. 2. Melakukan instalasi dan konfigurasi dasar Rocky Linux (update, SSH, firewall) pada VM. 3. Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh. 4. Melakukan analisis file .pcap dan .eml yang diberikan oleh mentor.
		2	<ol style="list-style-type: none"> 1. Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”
		3	<ol style="list-style-type: none"> 1. Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)” 2. Mempelajari dan membuat detector di anomaly detection pada Wazuh. 3. Melakukan analisis statis terhadap file malware yang diberikan untuk memeriksa struktur file dan metadata. 4. Membuat laporan hasil analisis statis.

		4	<ol style="list-style-type: none"> 1. Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan <i>sandbox</i>.
		5	<ol style="list-style-type: none"> 1. Membuat laporan hasil analisis dinamis terkait perilaku sistem, aktivitas jaringan, dan IoC. 2. Menganalisis File Malware menggunakan IT Hygiene Wazuh berdasarkan prosesnya. 3. Membuat laporan analisis Malware berdasarkan proses IT Hygiene yang ditemukan.
3	November 2025	1	<ol style="list-style-type: none"> 1. Membuat script untuk integrasi Wazuh dengan MISP
		2	<ol style="list-style-type: none"> 1. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”
		3	<ol style="list-style-type: none"> 1. Melakukan monitoring insiden menggunakan SIEM Wazuh. 2. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”
		4	<ol style="list-style-type: none"> 1. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”
4	Desember 2025	1	<ol style="list-style-type: none"> 1. Melakukan <i>Penetration Testing</i> terhadap target dari mentor 2. Reconnaissance: Berhasil mengumpulkan informasi awal, pemetaan subdomain, dan identifikasi infrastruktur dasar pada target. 3. Service Enumeration: Melakukan pemindaian port dan identifikasi versi

			<p>layanan (<i>banner grabbing</i>) untuk memetakan titik masuk potensial.</p> <ol style="list-style-type: none"> 4. Vulnerability Assessment: Melakukan analisis celah keamanan secara manual pada aplikasi web dan layanan jaringan yang aktif. 5. Exploitation & Validation: Melakukan validasi temuan untuk memastikan kerentanan benar-benar dapat dieksloitasi (<i>Proof of Concept</i>). 6. Post-Exploitation & Evidence: Mengumpulkan bukti-bukti pengujian, <i>log</i> aktivitas, dan <i>screenshot</i> temuan sebagai data pendukung utama.
		2	<ol style="list-style-type: none"> 1. Risk Analysis: Melakukan penilaian dampak dari setiap temuan dan menentukan skor tingkat keparahan berdasarkan standar CVSS. 2. Mitigation Planning: Menyusun langkah-langkah remediasi dan saran perbaikan teknis untuk setiap celah keamanan yang ditemukan. 3. Drafting Report: Menyusun draf laporan teknis yang mencakup metodologi pengujian, detail temuan, dan bukti-bukti pendukung. 4. Final Review: Melakukan pengecekan ulang terhadap laporan untuk memastikan akurasi data dan kerapuhan format dokumen. 5. Reporting & Submission: Menyerahkan laporan akhir kepada mentor dan melakukan diskusi terkait hasil evaluasi keamanan target.
		3	<ol style="list-style-type: none"> 1. Melakukan monitoring insiden menggunakan SIEM Wazuh. 2. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam

			Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”
		4	<ol style="list-style-type: none"> 1. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)” 2. Melakukan monitoring insiden menggunakan SIEM Wazuh.
		5	<ol style="list-style-type: none"> 1. Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)” 2. Melakukan monitoring insiden menggunakan SIEM Wazuh.
5	Januari 2026	1	<ol style="list-style-type: none"> 1. Melakukan monitoring insiden menggunakan SIEM Wazuh. 2. Menyusun Laporan Akhir Magang
		2	<ol style="list-style-type: none"> 1. Menyusun Laporan Akhir Magang

BAB IV

HASIL DAN PEMBAHASAN

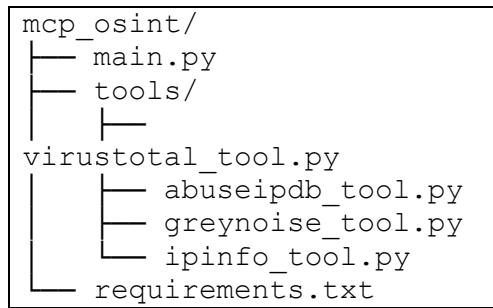
Pengembangan prototipe sistem ini dilakukan berdasarkan arahan dan kebutuhan yang diidentifikasi bersama mentor *Security Operations Center* (SOC), khususnya dalam mempercepat verifikasi *Indicators of Compromise* (IOC). Gagasan integrasi berbasis *Model Context Protocol* (MCP) muncul dari observasi terhadap alur kerja investigasi harian yang selama ini dilakukan melalui berbagai *platform* terpisah. Meskipun prototipe ini belum diuji langsung di lingkungan operasional perusahaan, perancangannya telah disesuaikan dengan tugas harian analis SOC, seperti analisis *phishing*, investigasi koneksi mencurigakan, dan penyusunan laporan teknis.

Selama proses pengembangan, tantangan utama yang dihadapi adalah keterbatasan akses terhadap layanan data berbayar serta batasan penggunaan (*rate limit*) pada layanan gratis yang tersedia secara terbuka. Hal tersebut direspon dengan menyeleksi beberapa penyedia *Open-Source Intelligence* (OSINT) publik yang lebih fleksibel serta menyesuaikan cakupan pengujian agar tetap fungsional tanpa melampaui kuota akses yang tersedia. Pemahaman terhadap karakteristik IOC yang umum ditemui dalam investigasi harian menjadi dasar utama dalam pengembangan sistem, sehingga solusi yang dihasilkan tetap relevan dengan kebutuhan operasional analis.

4.1 Hasil

4.1.1 Struktur Implementasi Sistem

Sistem dikembangkan dalam satu direktori utama, `mcp_osint/`. Struktur direktori sengaja dibuat ringkas untuk mendukung sifat proof of concept dan kemudahan pengujian local. Struktur direktori ditunjukkan pada Gambar 4.1 berikut.



Gambar 4. 1 Struktur Direktori Sistem

Penjelasan masing-masing komponen adalah sebagai berikut:

1. main.py

Berfungsi sebagai *entry point* sistem dan mengimplementasikan MCP *Server* sesuai spesifikasi resmi protocol MCP. Skrip ini menangani pendaftaran *tools*, validasi parameter, eksekusi pemanggilan *Application Programming Interface* (API) secara asinkron, serta penanganan *error* terpusat. Seluruh logika koordinasi antara *Large Language Model* (LLM) dan layanan OSINT terpusat di sini, sehingga integrasi dapat dilakukan tanpa mengubah inti model bahasa.

2. virustotal_tool.py

Merupakan modul khusus untuk berinteraksi dengan VirusTotal API v3. Modul ini mampu memproses berbagai jenis IOC, termasuk alamat IP, URL, serta *file hash* (MD5, SHA1, SHA256). Modul akan mengekstrak informasi kunci seperti jumlah laporan ancaman dan memformatnya menjadi teks ringkas untuk LLM.

3. abuseipdb_tool.py

Bertugas memverifikasi reputasi alamat IPv4 melalui AbuseIPDB API. Modul ini mengambil data berupa jumlah laporan pelanggaran, skor risiko, kategori ancaman, serta informasi ISP. Hasil ini membantu analis membedakan antara koneksi berbahaya dan normal.

4. greynoise_tool.py

Mengintegrasikan sistem dengan GreyNoise Community API. Fungsinya adalah mengklasifikasikan lalu lintas jaringan apakah termasuk kategori *benign* (aman), *malicious* (berbahaya), atau *unknown*. Informasi ini

berguna dalam menyaring *false positive* pada SIEM.

5. ipinfo_tool.py

Menyediakan konteks jaringan dan geografis seperti negara, kota, *Autonomous System Number* (ASN), serta nama organisasi pemilik jaringan. Data ini digunakan untuk memperkaya konteks investigasi tanpa menilai ancaman secara langsung.

6. requirements.txt

Mencantumkan dependensi utama yaitu mcp versi 1.15.0 (untuk kompatibilitas protokol) dan requests versi 2.31.0 (untuk komunikasi HTTP). Tidak ada dependensi tambahan karena sistem tidak menggunakan basis data, antarmuka grafis, atau fitur berat lainnya, hal ini mempercepat instalasi dan mengurangi *attack surface*.

Sistem ini dirancang tanpa folder tambahan seperti logs/, cache/, atau reports/ karena sistem berjalan dalam sesi lokal tanpa menyimpan data persisten. Hal ini sesuai dengan prinsip keamanan SOC yang membatasi penyimpanan informasi sensitif di luar lingkungan yang terkontrol.

4.1.2 Implementasi MCP Server (main.py)

Skrip main.py berfungsi sebagai *MCP Server* yang menjembatani komunikasi antara LLM dan layanan OSINT eksternal. Implementasi ini mengikuti spesifikasi resmi MCP, sehingga kompatibel dengan antarmuka LLM yang mendukung MCP, seperti Claude Desktop. Server diinisialisasi menggunakan objek *Server* dari *library* mcp, dengan identitas sistem ditetapkan sebagai *osint-mcp-server* versi 1.0.0, dan dijalankan dalam mode stdio untuk komunikasi standar.

1. Detail fungsi *handle_list_tool*

Fungsi ini berperan sebagai *gateway discovery*, titik awal di mana LLM memahami kemampuan eksternal yang tersedia. Tanpa fungsi ini, LLM tidak akan tahu tools apa saja yang dapat dipanggil, sehingga integrasi

tidak dapat dimulai. Detail pendefinisian alat pada fungsi ini ditunjukkan pada Gambar 4.2 berikut.

```
@server.list_tools()
async def handle_list_tools():
    return [
        Tool(
            name="virustotal_lookup",
            description="Lookup IP, URL, or file hash on VirusTotal",
            inputSchema={"type": "object", "properties": {"ioc": {"type": "string"}}, "required": ["ioc"]}),
        Tool(
            name="abuseipdb_check",
            description="Check IPv4 reputation on AbuseIPDB",
            inputSchema={"type": "object", "properties": {"ip": {"type": "string"}}, "required": ["ip"]}),
        Tool(
            name="greynoise_check",
            description="Check IP on GreyNoise (no API key needed)",
            inputSchema={"type": "object", "properties": {"ip": {"type": "string"}}, "required": ["ip"]}),
        Tool(
            name="ipinfo_lookup",
            description="Get geolocation/ISP for IPv4 via IPinfo.io",
            inputSchema={"type": "object", "properties": {"ip": {"type": "string"}}, "required": ["ip"]}),
        Tool(
            name="auto_osint_router",
            description="Run all IP tools for an IPv4 address",
            inputSchema={"type": "object", "properties": {"query": {"type": "string"}}, "required": ["query"]})
    ]
```

Gambar 4. 2 Fungsi *handle_list_tools*

Kode ini mengikuti spesifikasi MCP dengan mendaftarkan setiap *tool* sebagai objek *Tool* yang berisi tiga elemen wajib seperti *name*, *description*, dan *inputSchema*. Nama bersifat unik dan menjadi

identifier dalam pemanggilan. Deskripsi ditulis dalam bahasa alami agar LLM dapat memahami konteks penggunaan tanpa pelatihan ulang. Skema input berbasis JSON Schema memaksa validasi struktural di sisi LLM misalnya, jika abuseipdb_check meminta ip, LLM tidak akan mengirim ioc atau nilai kosong, sehingga mengurangi error di sisi server.

2. Detail fungsi *handle_call_tool*

Fungsi ini merupakan *executor* utama sistem yang bertugas menerjemahkan instruksi LLM menjadi aksi nyata terhadap layanan eksternal. Ia beroperasi sebagai *router dinamis* yang tidak hanya mendelegasikan ke modul spesifik, tetapi juga mampu memicu alur kerja komposit seperti analisis IP menyeluruh. Logika pemrosesan dan perutean instruksi tersebut dapat dilihat pada Gambar 4.3.


```

        output = ["IP Analysis Summary", "—" * 30]
        for res in results:
            if isinstance(res, Exception):
                output.append(f"Error: {res}")
            elif isinstance(res, list) and res:
                output.append(res[0].text)
        return [TextContent(type="text", text="\n".join(output))]

    else:
        raise McpError(code="method_not_found",
                      message=f"Unknown tool: {tool_name}")

except McpError:
    raise
except Exception as e:
    logger.exception("Tool execution error")
    return [TextContent(type="text", text=f"Internal
error: {str(e)}")]

```

Gambar 4. 3 Fungsi handle_call_tool

Logika fungsi ini terbagi menjadi tiga lapis yaitu validasi, eksekusi, dan penggabungan hasil. Di lapis validasi, sistem memastikan parameter wajib tersedia dan sesuai format (misal: ioc tidak kosong, input mengandung pola IPv4). Di lapis eksekusi, pemanggilan ke modul OSINT dilakukan secara *thread-safe* via `asyncio.to_thread()` untuk mencegah pemblokiran *event loop*. Lapis terakhir hanya muncul pada `auto_osint_router`, empat *tool* dijalankan secara konkuren dengan `asyncio.gather()`, lalu hasil termasuk error parsial digabung ke dalam satu daftar keluaran. Penggunaan `return_exceptions=True` memastikan satu kegagalan tidak menghentikan seluruh proses, sesuai prinsip *graceful degradation*.

3. Integrasi dengan Claude

Prototipe diintegrasikan ke Claude Desktop melalui *developer settings* dengan berbasis JSON. Konfigurasi ini mendefinisikan perintah eksekusi (python), lokasi skrip (main.py), serta kredensial API yang diperlukan oleh modul OSINT. Detail file konfigurasi JSON untuk integrasi tersebut disajikan pada Gambar 4.4.

```

"osint": {
    "command": "python",
    "args": ["C:\\Users\\ASUS\\Desktop\\MCP-OSINT\\mcp_osint\\main.py"],
    "env": {
        "VIRUSTOTAL_API_KEY": "9a7316f6b5b32dca1459c5bd6b925a8caa8f1d41a2a45c9cbf85784eb620e161",
        "ABUSEIPDB_API_KEY": "561bfb113cbce63372a768a1dc03ebe8a697257aec125026bdd0ce87e1341a0f1ad1ddc093bff3f8",
        "IPINFO_API_KEY": "27b81b20aa4539"
    }
}

```

Gambar 4. 4 Konfigurasi MCP di Developer Settings Claude Desktop

Konfigurasi ini mengaktifkan tool calling dengan protokol MCP. Saat pengguna memasukkan permintaan berbasis IOC, Claude memicu eksekusi main.py secara *on-demand* melalui *subprocess*. Penggunaan variabel lingkungan (env) memastikan kredensial API tidak tersimpan dalam percakapan, sehingga risiko kebocoran dapat diminimalkan.

4.1.3 Implementasi Modul Integrasi OSINT

Setiap layanan OSINT diintegrasikan melalui modul terpisah di dalam direktori tools/. Keempat modul mengikuti prinsip modularitas, namun masing-masing memiliki logika spesifik sesuai karakteristik layanan yang diintegrasikan.

1. VirusTotal (virustotal_tool.py)

Modul ini mengintegrasikan sistem dengan VirusTotal API v3 untuk analisis IOC multi-jenis seperti *file hash*, alamat IP, dan URL. Fungsi vt_lookup_ioc() mendeteksi jenis IOC berdasarkan pola teks, lalu memetakan ke *endpoint* API yang sesuai. Respons diformat menjadi ringkasan yang mencakup verdict (*malicious/suspicious/clean*), jumlah mesin pelapor, konteks geografis, serta tautan ke laporan lengkap.

Cuplikan kode modul VirusTotal dapat dilihat pada Gambar 4.5 berikut.

```
def vt_lookup_ioc(ioc: str) -> dict:
    headers = {"x-apikey": VT_API_KEY}
    ioc = ioc.strip()

    # 1. Logika Deteksi Jenis IOC (Regex)
    if re.fullmatch(r"[a-fA-F0-9]{64}", ioc):
        endpoint = f"/files/{ioc}"

    elif re.fullmatch(r"\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}", ioc):
        endpoint = f"/ip_addresses/{ioc}"

    elif ioc.startswith(("http://", "https://")):
        url_id =
base64.urlsafe_b64encode(ioc.encode()).decode().rstrip(
"=")

        endpoint = f"/urls/{url_id}"

    # 2. Ekstraksi Data & Penentuan Verdict
    response = requests.get(VT_BASE_URL + endpoint,
headers=headers)

    if response.status_code == 200:
        attrs = response.json().get("data",
{}).get("attributes", {})

        stats = attrs.get("last_analysis_stats", {})
        malicious = stats.get("malicious", 0)

        if malicious > 0:
            verdict = "🔴 Malicious"
        else:
            verdict = "🟢 Clean"

    # 3. Format Hasil untuk LLM
    result_lines = [
        f"🔍 VirusTotal Lookup: {ioc}",
        f"Verdict: {verdict}",
        f"Detection: {malicious} malicious /
```

```

{total} engines",
        f"🔗 Full Report:
https://www.virustotal.com/gui/{endpoint.lstrip('/')}"
    ]
    return {"result": "\n".join(result_lines)}

```

Gambar 4. 5 virustotal_tool.py

2. AbuseIPDB (abuseipdb_tool.py)

Modul memverifikasi reputasi alamat IPv4 berdasarkan laporan komunitas. Fungsi `check_ip_abuseipdb()` mengambil data *abuse confidence score*, lalu mengkategorikannya ke dalam tingkat risiko, *High Risk* ($\geq 80\%$), *Medium Risk* (30–79%), atau *Low Risk* (<30%). Hasil mencakup informasi ISP, negara, dan tautan ke laporan lengkap. Cuplikan kode modul AbuseIPDB dapat dilihat pada Gambar 4.6 berikut.

```

def check_ip_abuseipdb(ip: str, max_age_in_days: int = 90) -> dict:
    """Check an IP address against AbuseIPDB."""
    # 1. Validasi Input & Pemanggilan API
    headers = {"Accept": "application/json", "Key": ABUSEIPDB_API_KEY}
    params = {"ipAddress": ip, "maxAgeInDays": max_age_in_days}

    response = requests.get(ABUSEIPDB_URL,
                           headers=headers, params=params)

    if response.status_code == 200:
        data = response.json()["data"]
        score = data.get("abuseConfidenceScore", 0)

        # 2. Kategorisasi Tingkat Risiko
        # (Classification Logic)
        if score >= 80:
            risk = "🔴 High Risk"
        else:
            risk = "🟡 Medium Risk"
        else:
            risk = "🟢 Low Risk"
    else:
        risk = "⚪ Unknown Risk"
    return {
        "ip": ip,
        "score": score,
        "risk": risk,
        "isp": data.get("isp"),
        "country": data.get("country"),
        "url": data.get("url")
    }

```

```

        elif score >= 30:
            risk = "🔴 Medium Risk"
        else:
            risk = "🟢 Low Risk"

    # 3. Format Hasil untuk LLM
    result = (
        f"🔍 AbuseIPDB Report for {ip}\n"
        f"Risk Level: {risk} ({score}% confidence)\n"
        f"Total Reports: {data.get('totalReports', 0)}\n"
        f"ISP: {data.get('isp', 'N/A')}\n"
        f"Country: {data.get('countryName', 'N/A')}\n"
        f"🔗 Full Report:\n"
        f"https://www.abuseipdb.com/check/{ip}"
    )
    return {"result": result}

```

Gambar 4. 6 abuseipdb_tool.py

3. GreyNoise (greynoise_tool.py)

Modul memanfaatkan *GreyNoise Community API* untuk mengklasifikasikan lalu lintas jaringan seperti *benign* (scanner korporat), *malicious* (aktor ancaman aktif), atau *unknown* (belum terkласifikasi). Fungsi greynoise_lookup_ip() memberikan konteks tambahan seperti nama *scanner* dan waktu terakhir terlihat informasi yang membantu menyaring *false positive* dalam investigasi. Cuplikan kode modul GreyNoise dapat dilihat pada Gambar 4.7 berikut.

```

def greynoise_lookup_ip(ip: str) -> dict:
    """Lookup an IPv4 address using GreyNoise
    Community API."""
    # 1. Endpoint & Pemanggilan API (Tanpa API Key)
    url =
    f"https://api.greynoise.io/v3/community/{ip}"
    try:

```

```

        response = requests.get(url, timeout=10)

        if response.status_code == 200:
            data = response.json()

            classification =
data.get("classification", "unknown").lower()

            # 2. Logika Klasifikasi (Noise Filtering)
            if classification == "benign":
                verdict = "🟢 Benign (Known Scanner - Not Malicious)"
            elif classification == "malicious":
                verdict = "🔴 Malicious"
            else:
                verdict = "❓ Unknown"

            # 3. Format Output Hasil Investigasi
            result = (
                f"🔍 GreyNoise Community Lookup: {ip}\n"
                f"Classification: {verdict}\n"
                f"Scanner Name: {data.get('name', 'N/A')}\n"
                f"Last Seen: {data.get('last_seen', 'N/A')}\n"
                f"🔗 Full Report: https://www.greynoise.io/viz/ip/{ip}"
            )
        return {"result": result}
    
```

Gambar 4. 7 greynoise_tool.py

4. IPinfo

Modul ipinfo_tool.py menyediakan konteks geografis dan jaringan untuk alamat IP, termasuk kota, wilayah, negara, koordinat, dan waktu zona. Fitur uniknya adalah parsing otomatis field org (misal: "AS15169 Google LLC") menjadi nomor ASN (AS15169) dan nama ISP (Google

LLC), yang mendukung identifikasi asal koneksi mencurigakan. Cuplikan kode modul IPinfo dapat dilihat pada Gambar 4.8 berikut.

```
def ipinfo_lookup(ip: str) -> dict:
    """Lookup IPv4 address on IPinfo.io for
    geolocation and network info."""

    url =
f"{IPINFO_BASE_URL}/{ip}?token={IPINFO_API_KEY}"


    try:
        response = requests.get(url, timeout=10)
        if response.status_code == 200:
            data = response.json()

            # 1. Penanganan IP Privat (Bogon)
            if data.get("bogon") is True:
                return {"result": f"IPinfo:
{ip}\nStatus: 🟡 Private/reserved IP."}

            # 2. Logika Parsing ASN dan ISP (Feature
            # Unik)
            org = data.get("org", "N/A")
            asn, isp = "N/A", "N/A"
            if org != "N/A" and org.startswith("AS"):
                parts = org.split(" ", 1)
                asn = parts[0]
                isp = parts[1] if len(parts) > 1 else
"N/A"

            # 3. Format Output Konteks Investigasi
            result = (
                f"🌐 IPinfo Lookup: {ip}\n"
                f"Location: {data.get('city')}, "
                f"{data.get('region')}, {data.get('country')}\n"
                f"Coordinates: {data.get('loc')}\n"
                f"ASN: {asn}\n"
                f"ISP: {isp}\n"
            )
    except requests.exceptions.RequestException as e:
        result = f"Error: {e}"
    return result
```

```

        f"🔗 Full Report:  

        https://ipinfo.io/{ip}"  

    )  

    return {"result": result}

```

Gambar 4. 8 ipinfo_tool.py

4.2 Uji coba

Pengujian prototipe sistem MCP-OSINT dilakukan secara lokal menggunakan data intelijen yang relevan dengan kasus harian di SOC, yang mencakup analisis email *phishing* dan investigasi koneksi jaringan mencurigakan. Sumber IOC berasal dari log aktivitas mencurigakan yang terekam di Wazuh SIEM dan data dari tugas investigasi dan simulasi ancaman (seperti *file hash malware* asli dan skenario *sextortion scam*) yang diberikan dan diverifikasi oleh mentor SOC.

4.2.1 Metode Pengujian

Pengujian sistem ini menggunakan dua metode utama untuk memverifikasi fungsionalitas teknis dan relevansi operasional:

1. *Black-Box Testing* (Pengujian Fungsionalitas) :
 - a. Fokus dari pengujian ini adalah untuk memverifikasi fungsionalitas alur kerja antara Claude dan *MCP Server*, serta memastikan setiap modul OSINT bekerja sesuai spesifikasi teknis.
 - b. Tujuan utama pengujian ini adalah untuk memastikan bahwa LLM berhasil memicu *tool calling*, *MCP Server* berhasil merutekan permintaan, dan setiap modul API mengembalikan data tanpa *error* dalam format JSON yang valid.
 - c. Hasil kunci yang diharapkan meliputi *Pass/Fail* pada setiap alur fungsional dan validasi format data.

2. *Case-Based Scenario Testing* (Pengujian Relevansi Operasional) :
 - a. Fokus dari pengujian ini bertujuan untuk memverifikasi bahwa sistem memberikan nilai tambah yang signifikan dan efisiensi waktu dalam konteks kerja Analis SOC.
 - b. IOC yang digunakan dalam pengujian ini berasal dari sumber yang relevan dengan pekerjaan harian meliputi log aktivitas jaringan mencurigakan yang terekam di Wazuh SIEM dan data dari tugas investigasi dan simulasi ancaman yang diberikan oleh mentor SOC.
 - c. Tujuan pengujian ini adalah untuk mengukur peningkatan kecepatan investigasi menggunakan IOC nyata dan menilai kualitas *verdict* yang dihasilkan LLM sebagai bahan *decision-making* yang *actionable*.

4.2.2 Skenario Pengujian

Untuk membuktikan efektivitas sistem dalam alur kerja SOC, tiga skenario pengujian utama dilakukan, yang masing-masing mereplikasi tugas investigasi harian:

1. **Skenario 1: Investigasi IP Mencurigakan (*Malicious*)**
 Pengujian ini menggunakan alamat IP yang dicurigai sebagai berbahaya (*malicious*) untuk memverifikasi kemampuan sistem dalam memberikan *verdict* yang cepat dan komprehensif. Verifikasi ini dilakukan dengan memanggil *tools* AbuseIPDB, GreyNoise, dan IPinfo secara konkuren.
2. **Skenario 2: Investigasi File Hash (*Malware*)**
 Skenario ini menguji *file hash* (SHA-256) yang berasal dari sampel *malware* yang digunakan saat pelatihan. Tujuannya adalah untuk memverifikasi kemampuan sistem merutekan permintaan ke VirusTotal dan merangkum rasio deteksi *malware* dari sampel yang digunakan saat pelatihan.
3. **Skenario 3: Verifikasi Reputasi URL (*Phishing/Malicious*)**
 Pengujian ini menggunakan tautan (URL) yang terindikasi sebagai situs *phishing* atau penyebar konten berbahaya. Tujuannya adalah untuk

memverifikasi kemampuan sistem dalam memicu fungsi analisis pada VirusTotal guna mendapatkan informasi mengenai kategori situs dan tingkat risiko berdasarkan laporan berbagai mesin keamanan.

4. Skenario 4: Pengujian *False Positive* Filtering.

Pengujian ini menggunakan alamat IP yang diketahui aman (*benign*) untuk memverifikasi bahwa sistem dapat mengidentifikasi aktivitas yang sah. Hal ini penting untuk mencegah pemblokiran yang salah (*false positive*) dengan memanfaatkan data klasifikasi dari GreyNoise.

4.2.3 Hasil *Black-Box Testing* (Pengujian Fungsionalitas)

Pengujian ini fokus pada verifikasi fungsionalitas dan interaksi teknis antara komponen utama sistem, yaitu LLM (*Claude*) dan *MCP Server*, serta kemampuan sistem untuk menjalankan *multi-API* secara konkuren.

1. Pengujian Interaksi *Model Context Protocol* (MCP)

Pengujian interaksi MCP memverifikasi mekanisme komunikasi dan pertukaran data antara Claude dan *tool server* melalui protokol MCP. Tiga tahapan kunci dalam protokol ini diuji untuk memastikan sistem bekerja secara *end-to-end*.

A. Verifikasi Pemanggilan *Tool* oleh LLM (*Tool Calling*)

Tahap ini bertujuan memastikan LLM di Claude berhasil mendeteksi dan memicu pemanggilan *tool* (*osint_tool*) secara otomatis ketika menerima IOC dengan format valid. Keberhasilan ini membuktikan bahwa konfigurasi JSON *Schema* MCP sudah valid dan LLM dapat berinteraksi dengan layanan eksternal. Bukti pemicuan *tool call* oleh LLM saat menerima *input* pengguna ditunjukkan pada Gambar 4.9.

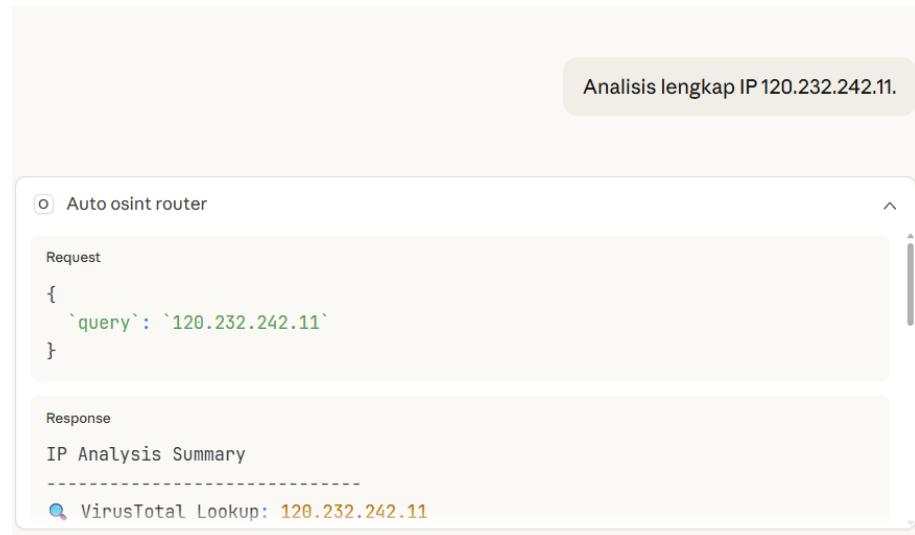


The screenshot shows a user interface for a security tool. At the top, there is a text input field containing the command "Cek hash ini:" followed by a hash value: "7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5". Below this, there is a date indicator "Dec 16" and some icons. A dropdown menu is open, showing the option "VirusTotal lookup" which is selected. Under the "Request" section, there is a JSON object: { "ioc": "7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5" }. In the "Response" section, it shows the results from VirusTotal: "VirusTotal Lookup" with the hash "7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5" and a "Verdict: Malicious".

Gambar 4. 9 Input user dan Pemicuan Tool Call JSON

B. Verifikasi Penerimaan Permintaan dan *Routing Server*

Setelah LLM memanggil *tool*, *MCP Server* (*main.py*) harus berhasil menerima parameter IOC, mem-parsing *input* dari LLM, dan merutekannya ke fungsi *auto_osint_router*. Pada tahap ini diverifikasi bahwa setiap modul API (seperti AbuseIPDB, VirusTotal, dll.) berhasil diuji dan mengembalikan respons yang valid. Hal ini membuktikan bahwa jalur komunikasi antara sistem MCP-OSINT dengan penyedia data OSINT pihak ketiga telah terjalin dengan benar. Proses pemicuan *routing* sistem diperlihatkan pada Gambar 4.10, sementara detail data mentah JSON yang berhasil ditarik dari berbagai sumber API disajikan pada Gambar 4.11.



Gambar 4. 10 Input Pengguna dan Pemicuan routing sistem

<p>Request</p> <pre> { `query`: `120.232.242.11` } </pre>	<p>Response</p> <p>IP Analysis Summary</p> <hr/> <p> VirusTotal Lookup: 120.232.242.11</p> <p>Verdict: ● Malicious</p> <p>Detection: 6 malicious, 3 suspicious / 95 engines</p> <p>Country: CN AS Owner: China Mobile communications corporation</p> <p> Full Report:</p> <p>https://www.virustotal.com/gui/ip_addresses/120.232.242.11</p> <p> AbuseIPDB Report for 120.232.242.11</p> <p>Risk Level: ● High Risk (87% confidence)</p> <p>Total Reports: 68</p> <p>Last Reported: 2025-12-15T17:21:34+00:00</p> <p>ISP: China Mobile Communications Corporation</p> <p>Domain: chinamobile.com</p> <p>Usage Type: Fixed Line ISP Country: China</p>
---	---

```
🔗 Full Report:  
https://www.abuseipdb.com/check/120.232.242.11  
GreyNoise: 120.232.242.11  
Status: ✅ Not seen in GreyNoise (likely clean or private IP).  
🔍 IPinfo Lookup: 120.232.242.11  
Location: Guangzhou, Guangdong, CN  
Postal: 510000 | Timezone: Asia/Shanghai  
Coordinates: 23.1167,113.2500  
Hostname: N/A ASN: AS56040  
ISP: China Mobile communications corporation  
🔗 Full Report: https://ipinfo.io/120.232.242.11
```

Gambar 4. 11 Formatted JSON Response Summary

C. Verifikasi Penanganan Error (*Error Handling*)

Pengujian ketahanan (*robustness*) sistem dilakukan dengan mengirimkan *input* yang tidak valid (misalnya, alamat IP dengan format salah) ke LLM. Hasil pengujian menunjukkan bahwa sistem berhasil menangani *error* ini. *Tool* mengembalikan pesan *error* yang jelas dan informatif kepada LLM, yang kemudian diteruskan kepada pengguna, alih-alih mengalami *server crash*. Deteksi kesalahan format oleh sistem dapat dilihat pada Gambar 4.12, dan penyampaian pesan *error* yang informatif kepada pengguna oleh LLM ditunjukkan pada Gambar 4.13.



Gambar 4. 12 Deteksi Error Format Input

Error: Format IP Tidak Valid

Masalah yang Terdeteksi:
 IP address **192.168.A.1** bukanlah format IP yang valid karena mengandung karakter huruf "A".

Format IP Address yang Benar
 IP address IPv4 harus menggunakan format:
 XXX.XXX.XXX.XXX
 Dimana setiap **XXX** adalah angka antara **0-255**.

Contoh IP yang valid:

- **192.168.0.1** (private IP - router)
- **192.168.1.1** (private IP - router)
- **8.8.8.8** (public IP - Google DNS)
- **1.1.1.1** (public IP - Cloudflare DNS)

Contoh IP yang TIDAK valid:

- **192.168.A.1** (mengandung huruf)
- **192.168.256.1** (angka > 255)
- **192.168..1** (format salah)

Gambar 4. 13 Respons LLM untuk Penanganan Error Format

Berdasarkan pengujian interaksi di atas, seluruh alur fungsional antara antarmuka pengguna dan server dinyatakan Pass, karena seluruh mekanisme *routing* dan validasi data bekerja sesuai dengan spesifikasi yang diharapkan.

4.2.4 Hasil Case-Based Scenario Testing (Relevansi Operasional)

Pengujian ini bertujuan memverifikasi kinerja sistem MCP-OSINT dalam mereplikasi empat tugas investigasi keamanan siber harian yang sudah didefinisikan dalam skenario pengujian. Fokus utama dari bagian ini adalah validasi *output* akhir yang dihasilkan sistem dalam mendukung proses pengambilan keputusan (*decision-making*) oleh analis SOC.

1. Skenario 1: Investigasi IP Mencurigakan (*Malicious*)

Skenario ini menguji kemampuan sistem dalam memberikan *verdict* yang cepat dan komprehensif untuk alamat IP yang dicurigai sebagai berbahaya (*malicious*). Analis memasukkan IP Address, dan sistem berhasil memicu *tool call* yang merutekan permintaan secara konkuren ke empat API sekaligus, yaitu VirusTotal, AbuseIPDB, GreyNoise, dan IPinfo. Hasil pengujian menunjukkan bahwa LLM mampu memproses data teragregasi untuk menghasilkan Ringkasan Keamanan yang mencakup rasio deteksi mesin (VirusTotal), *confidence score* (AbuseIPDB), status *noise* (GreyNoise), dan konteks geografis (IPinfo) secara terpadu. Output ini memastikan analis dapat mengambil keputusan blokir yang cepat dan terinformasi tanpa harus membandingkan laporan dari banyak sumber secara manual.

Hasil analisis komprehensif terhadap alamat IP mencurigakan yang mencakup ringkasan keamanan, data intelijen dari berbagai sumber, hingga rekomendasi tindakan dapat dilihat pada Gambar 4.14 sampai Gambar 4.16

Analisis lengkap IP 120.232.242.11.

Auto osint router ▾

Analisis Lengkap IP: 120.232.242.11

Ringkasan Keamanan: **HIGH RISK**

IP ini teridentifikasi sebagai **berbahaya** dan **berisiko tinggi** berdasarkan multiple intelligence sources.

VirusTotal Analysis

- Verdict:** Malicious (Berbahaya)
- Detection Rate:** 6 engine mendeteksi sebagai malicious, 3 engine mendeteksi sebagai suspicious dari 95 total engines
- Country:** China (CN)
- AS Owner:** China Mobile Communications Corporation
- Report:** [Lihat Detail](#)

AbuseIPDB Report

- Risk Level:** HIGH RISK
- Confidence Score:** 87% (Sangat tinggi)
- Total Reports:** 68 laporan abuse
- Last Reported:** 15 Desember 2025 (17:21:34 UTC) - Sangat baru!
- Domain:** chinamobile.com
- Usage Type:** Fixed Line ISP
- Report:** [Lihat Detail](#)

Gambar 4. 14 Ringkasan Keamanan dan Hasil Analisis Awal

GreyNoise Analysis

- **Status:** Tidak terdeteksi di GreyNoise
- **Interpretasi:** IP ini mungkin tidak melakukan internet-wide scanning atau bukan bagian dari noise internet yang umum. Ini bisa berarti aktivitas yang lebih targeted.

Geolocation & Network Info (IPinfo)

- **Location:** Guangzhou, Guangdong, China
- **Postal Code:** 510000
- **Timezone:** Asia/Shanghai
- **Coordinates:** 23.1167°N, 113.2500°E
- **ASN:** AS56040
- **ISP:** China Mobile Communications Corporation
- **Hostname:** Tidak tersedia

Gambar 4. 15 Hasil Analisis Tambahan

Kesimpulan & Rekomendasi

Tingkat Ancaman: ● TINGGI

IP ini menunjukkan karakteristik berbahaya dengan indikator kuat:

1. Dilaporkan 68 kali di AbuseIPDB dengan confidence 87%
2. Terdeteksi sebagai malicious/suspicious oleh 9 security vendors di VirusTotal
3. Aktivitas abuse masih sangat aktif (laporan terakhir kemarin)
4. Berasal dari China Mobile network di Guangzhou

Rekomendasi Tindakan:

- Blokir IP ini di firewall Anda
- Investigasi log untuk melihat aktivitas dari IP ini
- Periksa apakah ada komunikasi keluar ke IP ini
- Jika ada koneksi, lakukan incident response dan malware scanning
- Monitor terus untuk aktivitas mencurigakan

Kemungkinan Aktivitas: Brute force attack, scanning, malware C&C, atau aktivitas abuse lainnya.

Gambar 4. 16 Kesimpulan dari LLM

2. Skenario 2: Investigasi File Hash (Malware)

Skenario ini berfokus pada File Hash (SHA-256) yang berasal dari sampel *malware*, memverifikasi kemampuan sistem merutekan permintaan ke VirusTotal. Setelah *input* Hash diberikan, sistem berhasil

merutekan permintaan langsung ke API VirusTotal. Hasilnya, LLM menghasilkan ringkasan yang fokus pada rasio deteksi (*detection ratio*) dan klasifikasi ancaman. Sistem terbukti mampu merangkum informasi kunci yang diperlukan analis untuk *triage* file *malware* awal secara efektif, dengan tetap menyediakan akses langsung ke laporan lengkap untuk validasi mendalam. Hasil ringkasan deteksi *malware* dan klasifikasi ancaman berdasarkan pengujian file hash dapat dilihat pada Gambar 4.17 berikut.

The screenshot shows a user interface for VirusTotal's file lookup service. At the top, there is a text input field containing the SHA-256 hash: `7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5`. Below the input field, a button labeled "Cek hash ini!" is visible. The main content area displays a warning message: "**PERINGATAN: File Berbahaya Terdeteksi!**" followed by the text "Hash yang Anda berikan teridentifikasi sebagai **malicious** (berbahaya) di VirusTotal". A section titled "Detail Deteksi:" lists the following information:

- Status:** ● Malicious (Berbahaya)
- Deteksi:** 58 antivirus mendeteksi sebagai malicious dari 71 engine yang menganalisis
- Nama File:** PO_278_285Units_.exe
- Hash SHA-256:** `7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5`

A section titled "Analisis:" provides context: "File ini adalah executable (.exe) yang sangat mencurigakan dengan nama yang menyerupai dokumen purchase order (PO), yang merupakan taktik umum malware untuk mengelabui korban. Dengan 58 dari 71 antivirus mendeteksinya sebagai malicious, ini adalah indikator kuat bahwa file tersebut adalah malware."

A section titled "Rekomendasi:" lists the following recommendations:

- Jangan jalankan file ini
- Jika sudah terdownload, hapus segera dari sistem Anda
- Jika sudah dijalankan, lakukan scan penuh dengan antivirus dan pertimbangkan untuk melakukan investigasi lebih lanjut terhadap sistem

At the bottom, a note states: "Anda bisa melihat laporan lengkap di: <https://www.virustotal.com/gui/files/7f29f1dac72cfbf27f3537bec5b6cedc10f90f2b6b0cdaa503983f43d3bcf1d5>".

Gambar 4. 17 Hasil ringkasan deteksi malware

3. Skenario 3: Pengujian Verifikasi Reputasi URL (*Phishing/Malicious*)

Skenario ini menguji kemampuan sistem dalam melakukan analisis terhadap tautan (URL) yang dicurigai sebagai ancaman keamanan. Setelah analis memasukkan URL, sistem berhasil memicu *tool call* yang merutekan permintaan ke API VirusTotal. Hasil pengujian menunjukkan bahwa LLM mampu mentransformasi data mentah mengenai kategori situs, reputasi vendor, dan detail teknis URL menjadi ringkasan analisis risiko yang terstruktur. Kemampuan ini memungkinkan analis untuk memvalidasi ancaman pada tautan secara lebih mendalam, termasuk memahami karakteristik infrastruktur yang digunakan oleh penyerang. *Output* ini memberikan dukungan keputusan bagi analis dalam menentukan tingkat bahaya suatu tautan secara efisien. Hasil verifikasi URL, analisis risiko, hingga rekomendasi tindakan yang dihasilkan oleh sistem dapat dilihat pada Gambar 4.18 sampai Gambar 4.20

The screenshot shows a user interface for analyzing URLs. At the top, there is a search bar labeled "Analisa url ini" with the URL <https://ipfs.io/ipfs/bafkreast2ifwp4kuzhp4pjtgph46xb4bjueqkeezw34jh> entered. Below the search bar is a dropdown menu set to "virustotal_lookup". The main content area displays the analysis results:

Analisis URL: IPFS Gateway

Ringkasan Keamanan: MALICIOUS - HIGH RISK

URL ini terdeteksi sebagai **berbahaya** oleh multiple security vendors!

VirusTotal Analysis

- Verdict: **Malicious (Berbahaya)**
- Detection Rate: 13 malicious + 1 suspicious = 14 dari 98 security engines
- Last Analyzed: 9 Oktober 2025 (09:05 UTC)
- Full Report: [Lihat Detail](#)

Gambar 4. 18 Ringkasan Keamanan dan Hasil Deteksi VirusTotal

Red Flags & Risk Analysis

Mengapa URL Ini Berbahaya?

1. **Deteksi Malicious yang Tinggi:**
 - 13 security vendors mendeteksi sebagai malicious
 - 1 vendor mendeteksi sebagai suspicious
 - Total: **14.3% detection rate** (cukup tinggi untuk URL)
2. **IPFS Abuse Pattern:** IPFS sering disalahgunakan untuk:
 - **Malware distribution** - file executable berbahaya
 - **Phishing pages** - fake login pages
 - **Crypto scams** - fake wallet/investment sites
 - **C&C infrastructure** - malware command & control
 - **Spam campaigns** - malicious links in emails

Gambar 4. 19 Analisis Risiko dan Identifikasi Red Flags

Kesimpulan Akhir

URL
<https://ipfs.io/ipfs/bafkrelast2ifwp4kuzhp4pjtghp46xb4bjueyqkeezw34ljhmm63od4xy>

Risk Score: 8.5/10 (Very High Risk)

Threat Level: **CRITICAL**

Final Recommendations:

- **DO NOT ACCESS** this URL under any circumstances
- **BLOCK** in your security infrastructure
- **REPORT** to security team jika menemukan di network Anda
- **INVESTIGATE** jika ada user yang sudah mengakses
- **EDUCATE** users tentang IPFS security risks

Jika Anda menerima URL ini via email, chat, atau social media: Ini kemungkinan besar bagian dari **targeted attack campaign**. Report sebagai phishing/malware dan delete immediately!

PERINGATAN: Jangan coba untuk "test" atau "verify" URL ini dengan mengaksesnya langsung. Gunakan tools seperti VirusTotal atau sandbox environment jika absolutely necessary.

Gambar 4. 20 Kesimpulan Akhir dan Rekomendasi Mitigasi

4. Skenario 4: Pengujian False Positive Filtering

Pengujian ini bertujuan memverifikasi kemampuan sistem dalam mengidentifikasi aktivitas yang sah (*benign*) untuk mencegah *false positive*. Analis memasukkan alamat IP milik layanan publik terpercaya, yaitu 8.8.8.8 (Google *Public DNS*). Melalui proses *tool call*, data klasifikasi dari GreyNoise berhasil mengembalikan status "Benign". LLM secara eksplisit menyatakan *verdict* risiko yang RENDAH, dan memberikan informasi kontekstual bahwa IP tersebut merupakan layanan DNS publik yang aman. Hasil ini membuktikan bahwa sistem efektif dalam memfilter *false positive*, sehingga mencegah analis melakukan pemblokiran terhadap layanan penting yang dapat mengganggu operasional jaringan. Hasil identifikasi IP dengan klasifikasi *benign* serta penyajian *verdict* berisiko rendah dapat dilihat pada Gambar 4.21 sampai Gambar 4.23.

analisa ip ini 8.8.8.8

Auto osint router

Analisis Lengkap IP: 8.8.8.8

Ringkasan Keamanan: COMPLETELY SAFE - LEGITIMATE SERVICE

IP ini adalah **Google Public DNS** - salah satu layanan DNS publik paling populer dan terpercaya di dunia!

VirusTotal Analysis

- Verdict:** Clean (Bersih)
- Detection Rate:** 0 dari 95 security engines mendeteksi ancaman
- Country:** United States (US)
- AS Owner:** GOOGLE
- Report:** [Lihat Detail](#)

AbuseIPDB Report

- Risk Level:** Low Risk
- Confidence Score:** 0%
- Total Reports:** 153 laporan (false reports)
- Last Reported:** 17 Desember 2025 (16:02:18 UTC)
- Domain:** google.com
- Usage Type:** Content Delivery Network
- Country:** United States
- ISP:** Google LLC
- Report:** [Lihat Detail](#)

Gambar 4. 21 Hasil dari LLM

GreyNoise Analysis

- Classification: Benign (Known Scanner - Not Malicious)
- Scanner Name: Google Public DNS
- Last Seen: 18 Desember 2025 (Hari ini!)
- Status: Known non-malicious service
- Report: [Lihat Detail](#)

Geolocation & Network Info (IPinfo)

- Location: Mountain View, California, United States
- Postal Code: 94043 (Google HQ area)
- Timezone: America/Los_Angeles
- Coordinates: 38.0088°N, 122.1175°W
- Hostname: dns.google
- ASN: AS15169
- ISP: Google LLC
- Report: [Lihat Detail](#)

Gambar 4. 22 Hasil lanjutan dari LLM

Kesimpulan Akhir

IP **8.8.8.8** adalah **100% LEGITIMATE dan SAFE**

Ini adalah **Google Public DNS**, salah satu infrastructure internet paling penting dan dipercaya di dunia. Digunakan oleh ratusan juta orang setiap hari untuk DNS resolution.

Risk Score: 0/10 (Completely Safe)

Rekomendasi:

- AMAN** untuk digunakan sebagai DNS server
- WHITELIST** di firewall (jangan blokir!)
- TRUSTED** service dari Google

Jika Anda melihat traffic ke 8.8.8.8 di network Anda, ini adalah **normal DNS queries** dan bukan ancaman keamanan.

Gambar 4. 23 Kesimpulan akhir

4.3 Pembahasan

Berdasarkan hasil pengujian yang telah dipaparkan pada sub-bab sebelumnya, bagian ini membahas analisis mengenai efektivitas sistem MCP-OSINT dalam menyatukan berbagai sumber intelijen, peran LLM dalam pengolahan data, serta nilai praktisnya dalam operasional keamanan siber.

4.3.1 Analisis Efektivitas Integrasi Multi-Tool (OSINT Routing)

Sistem ini menggunakan metode perutean otomatis (automated routing) untuk memastikan setiap indikator ancaman (IOC) diperiksa oleh sumber yang tepat. Berdasarkan hasil pengujian, metode ini memberikan keuntungan sebagai berikut:

1. Konsolidasi Data yang Komprehensif

Pada Skenario 1 (IP Malicious), sistem berhasil menarik data dari VirusTotal, AbuseIPDB, dan GreyNoise secara bersamaan. Hal ini menutupi kekurangan jika hanya menggunakan satu sumber saja. Misalnya, jika VirusTotal hanya mendekripsi reputasi buruk, GreyNoise menambahkan konteks apakah IP tersebut merupakan scanner massal atau serangan tertarget.

2. Efisiensi Tool-Call

Sistem mampu mengenali format *input*. Jika *input* berupa File Hash, sistem secara cerdas hanya memanggil modul VirusTotal (Skenario 2) dan tidak memanggil modul IPinfo. Hal ini membuktikan bahwa sistem efisien dalam penggunaan kuota API dan sumber daya komputasi.

4.3.2 Analisis Peran LLM dalam Interpretasi Data

Salah satu fitur utama sistem ini adalah penggunaan LLM untuk merangkum data format JSON menjadi informasi yang mudah dipahami oleh analis. Manfaat yang teramat adalah :

1. Penyajian Informasi Kontekstual

LLM tidak hanya menampilkan angka deteksi, tetapi juga memberikan arti dari angka tersebut. Contohnya pada Skenario 4, LLM mampu menjelaskan bahwa meskipun ada laporan *abuse*, IP 8.8.8.8 adalah layanan tepercaya (Google DNS), sehingga analis tidak perlu melakukan blokir.

2. Sintesis Verdict Akhir

LLM membantu analis dalam menentukan *severity* (tingkat bahaya) dengan cepat melalui ringkasan di awal jawaban. Hal ini mengurangi beban kognitif analis dalam membaca baris demi baris data teknis dari berbagai API yang berbeda formatnya.

4.3.3 Relevansi dengan Kebutuhan Operasional SOC

Sesuai dengan tujuan pengembangan untuk meningkatkan efisiensi di unit kerja, sistem MCP-OSINT memberikan solusi praktis sebagai berikut:

1. Sentralisasi Alur Investigasi

Analis tidak perlu lagi mengakses berbagai *tools* OSINT secara terpisah untuk memeriksa satu alamat IP atau indikator ancaman lainnya. Melalui satu antarmuka tunggal, sistem ini mengintegrasikan data dari berbagai platform sehingga seluruh informasi intelijen tersaji secara terpadu. Hal ini menyederhanakan langkah-langkah dalam proses *triage* awal tanpa harus berpindah-pindah antar aplikasi atau layanan OSINT.

2. Mitigasi *Alert Fatigue*

Dengan adanya fitur pemfilteran *false positive* (seperti pada Skenario 3), sistem membantu analis untuk membedakan antara aktivitas mencurigakan dan layanan yang sah, sehingga analis dapat lebih fokus pada ancaman nyata yang memerlukan tindakan segera.

3. Analisis Komparatif Efisiensi Alur Kerja

Sistem ini mengubah model investigasi dari sekvensial (berurutan) menjadi paralel. Jika sebelumnya analis perlu menggunakan beberapa *tools* OSINT secara terpisah satu per satu untuk mendapatkan informasi yang komprehensif, maka melalui penggunaan *server-side concurrency* (metode `asyncio.gather`), sistem MCP-OSINT mampu mengeksekusi seluruh permintaan API secara bersamaan. Konsolidasi alur kerja ini memungkinkan analis untuk segera mendapatkan gambaran ancaman

secara utuh dalam satu antarmuka tunggal, sehingga mempercepat proses pengambilan keputusan.

4.3.4 Hambatan dan Batasan Sistem

Meskipun sistem telah berhasil berjalan sesuai skenario, terdapat beberapa hambatan dan batasan yang ditemukan:

1. Variasi Struktur Respons API

Tantangan teknis utama adalah mengolah berbagai format JSON dari penyedia API yang berbeda. Dibutuhkan penyesuaian kode (*parsing*) yang spesifik agar LLM dapat menerima data dalam format yang bersih dan terstruktur.

2. Ketergantungan pada Pihak Ketiga dan Internet

Karena sistem ini berbasis API, kinerja dan ketersediaan data sangat bergantung pada stabilitas koneksi internet serta *uptime* dari layanan pihak ketiga (VirusTotal, AbuseIPDB, dll).

3. Limitasi Kuota API

Penggunaan sistem ini dibatasi oleh kuota gratis (*free tier*) dari masing-masing penyedia OSINT. Jika kuota harian habis, modul terkait tidak dapat memberikan data hingga kuota diperbarui, yang dapat membatasi jumlah investigasi dalam satu hari.

BAB V

PENUTUP

5.1 Simpulan

Berdasarkan hasil pelaksanaan kegiatan magang di PT Solusi 247 serta proses pengembangan sistem MCP-OSINT, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Pengalaman Operasional SOC: Pelaksanaan magang memberikan pemahaman praktis mengenai alur kerja di unit *Security Operations Center* (SOC). Kegiatan ini memberikan wawasan nyata mengenai cara verifikasi *Indicators of Compromise* (IOC) dilakukan dalam prosedur investigasi keamanan siber, seperti pada analisis email *phishing* dan pemantauan aktivitas jaringan.
2. Keberhasilan Implementasi Protokol: Sistem MCP-OSINT berhasil dikembangkan dengan memanfaatkan *Model Context Protocol* (MCP) untuk mengintegrasikan berbagai layanan intelijen (VirusTotal, AbuseIPDB, GreyNoise, dan IPinfo). Protokol ini terbukti efektif dalam menghubungkan logika kecerdasan buatan dengan sumber data eksternal secara stabil.
3. Sentralisasi Alur Investigasi: Pengembangan sistem ini berhasil mengatasi kendala penggunaan banyak perangkat investigasi yang terpisah. Melalui satu antarmuka tunggal, data dari berbagai sumber intelijen dapat disajikan secara terpadu, sehingga menyederhanakan proses *triage* awal dan mengurangi penggunaan *tools* yang bersifat repetitif.
4. Kualitas Analisis Berbasis AI: Integrasi LLM dalam sistem ini memberikan kemampuan untuk merangkum data terstruktur dari berbagai modul OSINT menjadi informasi yang kontekstual. Sistem mampu membantu pemilahan tingkat bahaya (*severity*) dan mempermudah identifikasi layanan tepercaya guna meminimalkan kesalahan analisis (*false positive*).

5.2 Saran

Beberapa saran yang diajukan untuk perbaikan proses magang maupun pengembangan sistem di masa mendatang adalah sebagai berikut:

1. Saran untuk Organisasi Mitra (PT Solusi 247)
 - A. Penyediaan Sampel Indikator Ancaman yang Lebih Variatif:
Disarankan agar pihak perusahaan dapat memberikan penambahan variasi sampel ancaman atau dataset log dari skenario serangan yang telah dihilangkan data sensitifnya. Hal ini akan membantu meningkatkan akurasi pengujian perangkat agar lebih selaras dengan kebutuhan industri.
 - B. Pelaksanaan *Sharing Session* Rutin: Disarankan diadakannya diskusi berkala mengenai tren ancaman siber terbaru untuk memperluas wawasan praktis peserta magang.
2. Saran untuk Pengembangan Sistem
 - A. Pengembangan Fitur Pemindaian Log Mentah (Raw Log Parsing):
Disarankan untuk menambahkan kemampuan pemrosesan teks yang lebih luas agar sistem dapat secara mandiri mengekstrak indikator ancaman (IOC) dari potongan baris log mentah yang dimasukkan oleh analis. Hal ini akan mempercepat alur kerja karena analis tidak perlu lagi memisahkan alamat IP atau hash secara manual sebelum melakukan pencarian.
 - B. Implementasi LLM Lokal: Eksplorasi penggunaan model bahasa lokal (seperti Llama 3 melalui Ollama) disarankan agar seluruh proses analisis data tetap berada di dalam jaringan internal perusahaan untuk menjaga kerahasiaan informasi sensitif.
 - C. Manajemen Kuota API: Penambahan fitur penyimpanan data sementara (*caching*) pada hasil pencarian diperlukan untuk mengoptimalkan penggunaan kuota harian API, terutama saat menghadapi indikator acaman yang muncul berulang kali.

DAFTAR PUSTAKA

- Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bohg, J., Bosselut, A., Brunskill, E., Brynjolfsson, E., Buch, S., Card, D., Castellon, R., Chatterji, N., Chen, A., Creel, K., Davis, J. Q., Demszky, D., ... Liang, P. (2022). *On the Opportunities and Risks of Foundation Models*. <http://arxiv.org/abs/2108.07258>
- Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, 23(4), 2911–2938. <https://doi.org/10.1007/s10207-024-00868-2>
- Mialon, G., Dessì, R., Lomeli, M., Nalmpantis, C., Pasunuru, R., Raileanu, R., Rozière, B., Schick, T., Dwivedi-Yu, J., Celikyilmaz, A., Grave, E., LeCun, Y., & Scialom, T. (2023). *Augmented Language Models: a Survey*. <http://arxiv.org/abs/2302.07842>
- What is the Model Context Protocol (MCP)? - Model Context Protocol.* (n.d.). Retrieved October 24, 2025, from <https://modelcontextprotocol.io/docs/getting-started/intro>
- home - Solusi247.* (n.d.). Retrieved January 16, 2026, from <https://solusi247.com/>

LAMPIRAN

1. Transkrip/Penilaian dari tempat magang



24 hours 7 days integrated ICT solution

TRANSKRIP PROGRAM MBKM MAGANG MANDIRI

PT Dua Empat Tujuh

NIM : 225510014
Nama : Johan Maulana
Program Studi : Teknik Komputer
Semester : 7
Asal Perguruan Tinggi : Universitas Teknologi Digital Indonesia
Pembimbing Lapangan : Adriyansyah MF
Dosen Pembimbing : Ir. M. Guntara, M.T.
Waktu Pelaksanaan : 15 September 2025 s.d 14 Januari 2026

No.	Nama Materi	Nilai Angka
1.	Fundamental Cyber Security	90
2.	System Security	87
3.	Application & Web Security	83
4.	Tools & Hands-on Security Practice	90
5.	Incident Response & SOC Basic	85
6.	Capstone / Final Project	90

Yogyakarta, 17 Desember 2025

A handwritten signature in black ink, appearing to read "Adriyansyah MF", placed over the SOLUSI247 logo.

(Adriyansyah MF)

2. Sertifikat magang



3. Dokumentasi/foto kegiatan





4. Log Activity Kegiatan Magang program MBKM *)

Log Activity Program MBKM Magang Mandiri UTDI

Minggu ke-1				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
15/09/2025	Onboarding	Menandatangani perjanjian kebijakan, mendapatkan pengenalan perusahaan, penjelasan tata tertib, dan eksplorasi awal SIEM Wazuh.	Adriyansyah MF	
16/09/2025	Penyampaian Materi	Mengikuti penyampaian materi mengenai cybersecurity dan SIEM Wazuh oleh mentor.	Adriyansyah MF	
17/09/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
18/09/2025	Analisis Log	Menganalisis log yang diberikan mentor menggunakan ruleset test. Jika belum tersedia rules atau decoder, maka dibuat baru.	Adriyansyah MF	
19/09/2025	Penambahan Rules	Mengembangkan dan menambahkan rules yang telah dibuat sebelumnya.	Adriyansyah MF	

Minggu ke-2				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
22/09/2025	Analisis Log	Menganalisis log yang diberikan mentor dan mengembangkan rules yang relevan.	Adriyansyah MF	
23/09/2025	SOC Monitoring	Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh.	Adriyansyah MF	
24/09/2025	SOC Monitoring	Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh.	Adriyansyah MF	
25/09/2025	SOC Monitoring & Meeting	Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh dan mengikuti meeting divisi cyber security.	Adriyansyah MF	

26/09/2025	Setup Lab Ubuntu	Git clone repositori ELK Stack dan website vulnerable dari mentor untuk kebutuhan pengujian.	Adriyansyah MF	
------------	------------------	--	----------------	--

Minggu ke-3				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
29/09/2025	Latihan Offensive dan Defensive	Melakukan latihan strategi <i>offensive</i> dan <i>defensive</i> pada sistem yang telah disiapkan.	Adriyansyah MF	
30/09/2025	Latihan Offensive dan Defensive	Melakukan latihan strategi <i>offensive</i> dan <i>defensive</i> pada sistem yang telah disiapkan.	Adriyansyah MF	
1/10/2025	Install Rocky Linux	Melakukan instalasi dan konfigurasi dasar Rocky Linux (update, SSH, firewall) pada VM.	Adriyansyah MF	
2/10/2025	SOC Monitoring	Melakukan monitoring insiden keamanan siber menggunakan SIEM Wazuh.	Adriyansyah MF	
3/10/2025	Analisis File	Melakukan analisis file .pcap dan .eml yang diberikan oleh mentor.	Adriyansyah MF	

Minggu ke-4				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
6/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
7/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
8/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	

9/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
10/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	

Minggu ke-5				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
13/10/2025	Membuat Proyek	Membuat Proyek “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
14/10/2025	Membuat detector anomali	Mempelajari dan membuat detector di anomaly detection pada Wazuh.	Adriyansyah MF	
15/10/2025	Analisis File Malware	Melakukan analisis statis terhadap file malware yang diberikan untuk memeriksa struktur file dan metadata.	Adriyansyah MF	
16/10/2025	Analisis File Malware	Melakukan analisis statis terhadap file malware yang diberikan untuk memeriksa struktur file dan metadata.	Adriyansyah MF	
17/10/2025	Memmbuat Laporan Hasil Analisis File Malware	Membuat laporan hasil analisis statis.	Adriyansyah MF	

Minggu ke-6				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
20/10/2025	Analisis File Malware	Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan sandbox.	Adriyansyah MF	
21/10/2025	Analisis File Malware	Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan	Adriyansyah MF	

		<i>sandbox.</i>		
22/10/2025	Analisis File Malware	Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan <i>sandbox</i> .	Adriyansyah MF	
23/10/2025	Analisis File Malware	Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan <i>sandbox</i> .	Adriyansyah MF	
24/10/2025	Analisis File Malware	Melakukan analisis dinamis terhadap file malware yang diberikan di lingkungan <i>sandbox</i> .	Adriyansyah MF	

Minggu ke-7				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
27/10/2025	Memmbuat Laporan Hasil Analisis File Malware	Membuat laporan hasil analisis dinamis terkait perilaku sistem, aktivitas jaringan, dan IoC.	Adriyansyah MF	
28/10/2025	Analisis File Malware	Menganalisis File Malware menggunakan IT Hygiene Wazuh berdasarkan prosesnya.	Adriyansyah MF	
29/10/2025	Analisis File Malware	Menganalisis File Malware menggunakan IT Hygiene Wazuh berdasarkan prosesnya.	Adriyansyah MF	
30/10/2025	Analisis File Malware	Menganalisis File Malware menggunakan IT Hygiene Wazuh berdasarkan prosesnya.	Adriyansyah MF	
31/10/2025	Memmbuat Laporan Hasil Analisis File Malware	Membuat laporan analisis Malware berdasarkan proses IT Hygiene yang ditemukan.	Adriyansyah MF	

Minggu ke-8				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
03/11/2025	Membuat script	Membuat script untuk integrasi Wazuh dengan MISP	Adriyansyah MF	
04/11/2025	Membuat script	Membuat script untuk integrasi Wazuh dengan MISP	Adriyansyah MF	

05/11/2025	Membuat script	Membuat script untuk integrasi Wazuh dengan MISP	Adriyansyah MF	
06/11/2025	Membuat script	Membuat script untuk integrasi Wazuh dengan MISP	Adriyansyah MF	
07/11/2025	Membuat script	Membuat script untuk integrasi Wazuh dengan MISP	Adriyansyah MF	

Minggu ke-9				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
10/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
11/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
12/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
13/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
14/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	

Minggu ke-10				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
17/11/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	

18/11/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
19/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
20/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
21/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	

Minggu ke-11				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
24/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
25/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
26/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
27/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
28/11/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam	Adriyansyah MF	

	Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)"	
--	---	--

Minggu ke-12				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
1/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Reconnaissance: Berhasil mengumpulkan informasi awal, pemetaan subdomain, dan identifikasi infrastruktur dasar pada target.	Adriyansyah MF	
2/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Service Enumeration: Melakukan pemindaian port dan identifikasi versi layanan (<i>banner grabbing</i>) untuk memetakan titik masuk potensial.	Adriyansyah MF	
3/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Vulnerability Assessment: Melakukan analisis celah keamanan secara manual pada aplikasi web dan layanan jaringan yang aktif.	Adriyansyah MF	
4/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Exploitation & Validation: Melakukan validasi temuan untuk memastikan kerentanan benar-benar dapat dieksplorasi (<i>Proof of Concept</i>).	Adriyansyah MF	
5/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Post-Exploitation & Evidence: Mengumpulkan bukti-bukti pengujian, log aktivitas, dan screenshot temuan sebagai data pendukung utama.	Adriyansyah MF	

Minggu ke-13				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
08/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Risk Analysis: Melakukan penilaian dampak dari setiap temuan dan menentukan skor tingkat keparahan berdasarkan standar CVSS.	Adriyansyah MF	

09/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Mitigation Planning: Menyusun langkah-langkah remediasi dan saran perbaikan teknis untuk setiap celah keamanan yang ditemukan.	Adriyansyah MF	
10/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Drafting Report: Menyusun draft laporan teknis yang mencakup metodologi pengujian, detail temuan, dan bukti-bukti pendukung.	Adriyansyah MF	
11/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Final Review: Melakukan pengecekan ulang terhadap laporan untuk memastikan akurasi data dan kerapihan format dokumen.	Adriyansyah MF	
12/12/2025	Melakukan <i>Penetration Testing</i> terhadap target dari mentor.	Reporting & Submission: Menyerahkan laporan akhir kepada mentor dan melakukan diskusi terkait hasil evaluasi keamanan target.	Adriyansyah MF	

Minggu ke-14				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
15/12/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
16/12/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
17/12/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
18/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
19/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	

Minggu ke-15				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
22/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
23/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
24/12/2025	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
25/12/2025	Libur Nasional		Adriyansyah MF	
26/12/2025	Libur Nasional		Adriyansyah MF	

Minggu ke-16				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
29/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
30/12/2025	Menyusun Tugas Akhir	Menyusun Tugas Akhir “Implementasi Model Context Protocol (MCP) dalam Integrasi Multi-Tools OSINT untuk Analisis Threat Intelligence Berbasis Large Language Model (LLM)”	Adriyansyah MF	
31/12/2025	Libur Nasional		Adriyansyah MF	
1/1/2026	Libur Nasional		Adriyansyah MF	
2/1/2026	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	

Minggu ke-17				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
5/1/2026	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
6/1/2026	SOC Monitoring	Melakukan monitoring insiden menggunakan SIEM Wazuh.	Adriyansyah MF	
7/1/2026	Menyusun Laporan Akhir Magang	Menyusun bagian awal laporan seperti cover, lembar pengesahan, kata pengantar, dan daftar isi.	Adriyansyah MF	
8/1/2026	Menyusun Laporan Akhir Magang	Menyusun Bab I (Pendahuluan) yang meliputi latar belakang, tujuan magang, dan batasan masalah.	Adriyansyah MF	
9/1/2026	Menyusun Laporan Akhir Magang	Menyusun Bab II yang berisi profil instansi serta deskripsi proyek Tugas Akhir yang dikerjakan di tempat magang.	Adriyansyah MF	

Minggu ke-18				
Tanggal	Kegiatan	Hasil	Nama Mentor	Tandatangan Mentor
12/1/2026	Menyusun Laporan Akhir Magang	Menyusun Bab III yang mendeskripsikan persoalan topik proyek serta merincikan seluruh proses pelaksanaan magang.	Adriyansyah MF	
13/1/2026	Menyusun Laporan Akhir Magang	Menyusun Bab III menyusun detail pencapaian hasil magang, baik dari sisi kompetensi teknis maupun pengetahuan yang didapat.	Adriyansyah MF	
14/1/2026	Menyusun Laporan Akhir Magang	Menyusun Bab IV membuat kesimpulan, saran, serta melakukan finalisasi seluruh dokumen dan lampiran laporan.	Adriyansyah MF	