LAPORAN

PRAKTIK KERJA LAPANGAN

ANALISIS DAN DESKRIPSI KERENTANAN COMMON VULNERABILITIES AND EXPOSURES UNTUK MEMPERKUAT KINERJA SECURITY OPERATION CENTER MENGGUNAKAN AI ASSISTANT.

(PT Tirta Nawasena Teknologi)

IKHSAN FADILLAH

2207421013

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

DEPOK

2025

HALAMAN PENGESAHAN

LAPORAN PRAKTIK KERJA LAPANGAN

a. Judul :ANALISI DAN DESKRIPSI KERENTANAN COMMON VULNERABILITIES AND EXPOSURES UNTUK MEMPERKUAT KINERAJA OPERATION CENTER MENGGUNAKAN AI ASSISTANT

b. Penyusun

1) Nama : Ikhsan Fadillah
2) NIM : 2207421013

c. Program Studi : Teknik Multimedia dan Jaringan

d. Jurusan : Teknik Informatika dan Komputer

e. Waktu Pelaksanaan : 21 Juli 2025 - 30 Desember 2025

f. Tempat Pelaksanaan : PT Tirta Nawasena Teknologi

g. Alamat Pelaksaaan : Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec. Serpong Utara, Kota Tangerang Selatan, Banten 15323

Depok, 2025

Pembimbing PNJ

Asep Kurniawan, S.Pd., M.Kom

NIP. 199109262019031012

Pembimbing Perusahaan

Nasrulloh

Mengesahkan,

KPS Teknik Multimedia dan Jaringan

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

NIP. 198703132019031012

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat-Nya, sehingga penulis dapat menyelesaikan laporan Praktik Kerja Lapangan (PKL) berjudul **"Implementasi CVE Assistant untuk Otomasi Analisis dan Deskripsi CVE pada Security Operation Center"** tepat waktu. Laporan ini disusun sebagai syarat kelulusan mata kuliah PKL di Program Studi Teknik Multimedia dan Jaringan, Politeknik Negeri Jakarta.

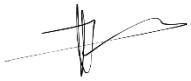
Kegiatan magang di PT Tirta Nawasena Teknologi memberikan wawasan berharga mengenai operasional *Security Operation Center* (SOC) dan penerapan teknologi otomasi dalam analisis keamanan siber. Meskipun menghadapi tantangan dalam memahami kompleksitas sistem keamanan perusahaan, penulis berhasil mengatasinya berkat bimbingan mentor dan kerja sama tim yang solid.

Penyusunan laporan ini terlaksana berkat dukungan berbagai pihak. Penulis mengucapkan terima kasih yang tulus kepada:

1. Bapak Nasrulloh, pembimbing industri yang telah memberikan bimbingan teknis selama magang.
2. Bapak Asep Kurniawan, S.Pd., M.Kom., dosen pembimbing atas arahan dalam penyusunan laporan.
3. Pimpinan dan staf Divisi SOC PT Tirta Nawasena Teknologi atas penerimaan dan ilmu yang dibagikan.
4. Orang tua dan keluarga atas doa dan dukungan moril maupun materiil yang tak terhingga.

Penulis menyadari laporan ini masih memiliki kekurangan. Kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa mendatang.

Tangerang, Desember 2025



Ikhsan Fadillah

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I
PENDAHULUAN

1.1 Latar Belakang Kegiatan

Kegiatan magang merupakan salah satu bentuk implementasi ilmu yang telah diperoleh selama perkuliahan ke dalam dunia kerja secara nyata. Melalui kegiatan magang, mahasiswa dapat memahami bagaimana teori yang dipelajari di kampus diterapkan dalam praktik, serta memperoleh pengalaman langsung terkait proses kerja di lingkungan profesional.

Dalam dunia teknologi informasi, keamanan siber (*cyber security*) menjadi aspek penting yang harus diperhatikan oleh setiap perusahaan. Ancaman siber yang semakin kompleks menuntut adanya sistem pemantauan dan penanganan insiden keamanan yang efektif. Salah satu bagian penting dalam menjaga keamanan sistem informasi adalah *Security Operation Center* (SOC), yaitu tim atau unit yang bertanggung jawab memantau, menganalisis, serta menanggapi insiden keamanan secara *real-time*.

PT Tirta Nawasena merupakan perusahaan yang bergerak di bidang penyediaan layanan dan solusi teknologi, termasuk dalam pengelolaan keamanan sistem informasi. Melalui program magang di PT Tirta Nawasena, penulis berkesempatan untuk terlibat langsung dalam aktivitas SOC (*Security Operation Center*) dan memahami proses kerja yang berkaitan dengan *monitoring*, analisis insiden, serta pelaporan keamanan siber.

Kegiatan ini diharapkan dapat memberikan pengalaman praktis dalam dunia keamanan informasi sekaligus memperkuat pemahaman terhadap konsep dan implementasi sistem pertahanan digital di lingkungan industri.

1.2 Ruang Lingkup Kegiatan

Kegiatan yang dilakukan selama magang di PT Tirta Nawesena meliputi beberapa aktivitas utama yang berkaitan dengan keamanan siber, antara lain:

a. Melakukan *monitoring* keamanan jaringan dan *endpoint* melalui sistem *Security Operation Center* (SOC).

b. Menganalisis indikator serangan siber (*Indicators of Compromise*/IoC) berdasarkan data dari sistem XDR (*Extended Detection and Response*) seperti Tehtris XDR.

c. Membantu melakukan deteksi otomatis ancaman dengan memanfaatkan sumber *Cyber Threat Intelligence* (CTI) seperti IP Abuse atau IP Criminal.

d. Membuat laporan hasil pemantauan dan analisis insiden keamanan.

e. Berpartisipasi dalam pengembangan otomasi deteksi ancaman untuk meningkatkan efisiensi SOC.

1.3 Waktu dan Tempat Pelaksanaan

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

a. Tempat dan Pelaksanaan : Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec. Serpong Utara, Kota Tangerang Selatan, Banten 15323

b. Penempatan : Security Operation Center (SOC)

c. Waktu pelaksanaan : 23 Juni – 19 Desember 2025

d. Lama PKL : 6 Bulan

1.4 Tujuan

Tujuan utama dari kegiatan magang ini adalah untuk memberikan pengalaman langsung dalam pengelolaan keamanan siber di lingkungan profesional. Secara lebih rinci, tujuan dari magang ini meliputi:

a. Mengimplementasikan kerentanan common vulnerabilities and exposures untuk memperkuat kinerja security operation center menggunakan ai assistant.

b. Menganalisis kerentanan common vulnerabilities and exposures untuk memperkuat kinerja security operation center menggunakan ai assistant.

1.5 Kegunaan

Kegunaan dari implementasi sistem otomatisasi deskripsi CVE menggunakan API NVD dan kecerdasan buatan (AI) pada Divisi Security Operation Center (SOC) PT Tirta Nawesena dapat dilihat dari beberapa aspek, antara lain:

1.5.1 Efisiensi dalam Analisis Kerentanan

Sistem ini membantu tim SOC mempercepat proses identifikasi dan pemahaman terhadap kerentanan (CVE) tanpa harus membaca laporan teknis yang panjang secara manual. Dengan deskripsi otomatis, proses triase ancaman menjadi lebih cepat dan efisien.

1.5.2 Peningkatan Akurasi dalam Penilaian Risiko

Sistem ini membantu tim SOC mempercepat proses identifikasi dan pemahaman terhadap kerentanan (CVE) tanpa harus membaca laporan teknis yang panjang secara manual. Dengan deskripsi otomatis, proses triase ancaman menjadi lebih cepat dan efisien.

1.5.3 Penyederhanaan Proses Dokomentasi Keamanan

Hasil deskripsi otomatis dari setiap CVE dapat langsung dijadikan laporan internal atau dasar dokumentasi keamanan, sehingga membantu standarisasi pelaporan kerentanan dalam sistem keamanan perusahaan.

1.5.4 Peningkatan Kapasitas Operasional

Dengan adanya sistem otomatisasi ini, beban kerja analis keamanan dapat berkurang, karena tugas deskripsi dan kategorisasi kerentanan dapat dilakukan secara otomatis oleh sistem. Hal ini meningkatkan produktivitas dan memungkinkan tim fokus pada penanganan insiden yang lebih kritikal.

1.5.5 Pengembangan Kompetensi dan Inovasi Teknologi

Proyek ini menjadi sarana pengembangan pengetahuan dan penerapan teknologi AI dalam bidang keamanan siber, serta menunjukkan kemampuan inovatif Divisi SOC PT Tirta Nawesena dalam memanfaatkan kecerdasan buatan untuk meningkatkan efektivitas operasional.

BAB II
LANDASAN TEORI

2.1 Keamanan Siber (*Cyber Security*)

Keamanan siber adalah sebuah praktik yang mencakup teknologi, proses, dan kontrol untuk melindungi sistem, jaringan, program, dan data dari serangan, kerusakan, atau akses digital yang tidak sah. Menurut Stallings & Brown (2018), keamanan siber didefinisikan sebagai upaya perlindungan aset komputer dan informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Tujuan utamanya adalah menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Chuvakin et al. (2013) menambahkan bahwa dalam konteks modern, keamanan siber juga mencakup deteksi ancaman secara *real-time* dan respons insiden, bukan hanya pencegahan pasif.

2.2 Security Operation Center (SOC)

Security Operation Center (SOC) adalah unit terpusat dalam organisasi yang bertanggung jawab untuk memantau, mendeteksi, menganalisis, dan menanggapi insiden keamanan siber. Menurut Ali & P. (2021), SOC berfungsi sebagai fasilitas tempat aset informasi dipantau dan dipertahankan dari ancaman keamanan. Muniz & McIntyre (2021) menjelaskan bahwa efektivitas SOC sangat bergantung pada kombinasi tiga elemen: orang (*people*), proses (*process*), dan teknologi (*technology*). Dalam operasionalnya, SOC sering menggunakan alat bantu otomasi untuk menangani volume peringatan (*alerts*) yang besar guna mencegah kelelahan analis atau *alert fatigue*.

2.3 *Common Vulnerabilities and Exposures* (CVE)

Common Vulnerabilities and Exposures (CVE) adalah standar industri untuk pengidentifikasian kerentanan keamanan yang diketahui publik. MITRE

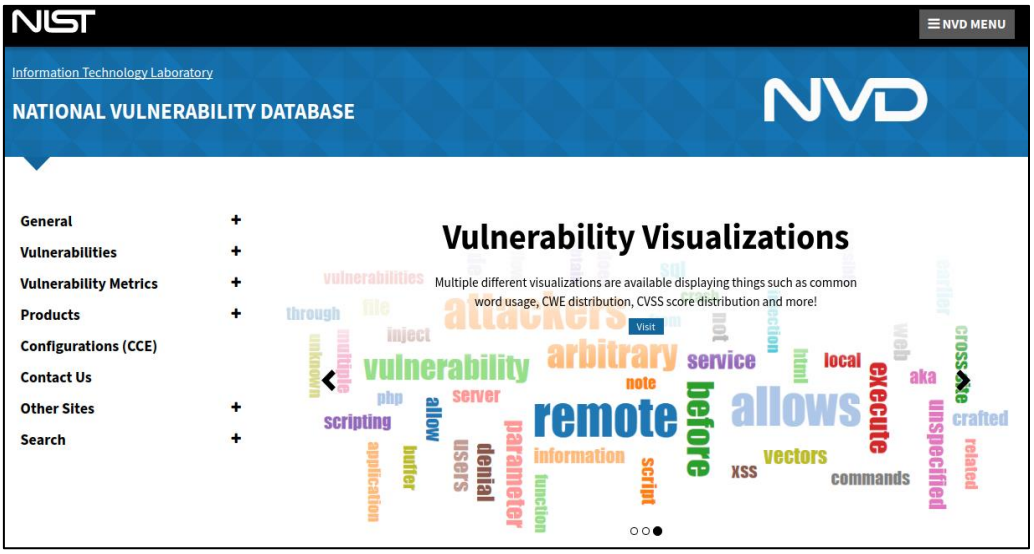
Corporation (2024) mendefinisikan CVE sebagai daftar referensi kerentanan keamanan informasi yang diidentifikasi secara unik. Setiap entri CVE memiliki nomor identifikasi (ID), deskripsi, dan setidaknya satu referensi publik. Martin (2001), salah satu pencetus konsep ini, menyatakan bahwa tujuan CVE adalah memungkinkan interoperabilitas data antara berbagai alat keamanan dan layanan basis data kerentanan.

2.4 *Common Vulnerability Scoring System* (CVSS)

Selain identifikasi, penilaian tingkat keparahan kerentanan sangat penting. CVSS adalah kerangka kerja terbuka untuk mengomunikasikan karakteristik dan tingkat keparahan kerentanan perangkat lunak. Menurut FIRST (2019), CVSS menyediakan skor numerik (0.0 hingga 10.0) yang mencerminkan tingkat keparahan, yang kemudian dapat diterjemahkan ke dalam representasi kualitatif (seperti Rendah, Sedang, Tinggi, dan Kritis). Skor ini membantu tim SOC memprioritaskan proses manajemen kerentanan berdasarkan dampaknya terhadap sistem.

2.5 *National Vulnerability Database* (NVD)

National Vulnerability Database (NVD) adalah repositori data manajemen kerentanan pemerintah AS yang berbasis standar. NIST (2024) menjelaskan bahwa NVD melakukan analisis terhadap setiap CVE yang diterbitkan dan melengkapinya dengan skor CVSS, tipe kelemahan (*Common Weakness Enumeration* - CWE), dan data platform yang terpengaruh (*Common Platform Enumeration* - CPE). NVD menyediakan API publik yang memungkinkan pengembang untuk mengintegrasikan data kerentanan yang kaya ini ke dalam aplikasi mereka secara otomatis (Booth et al., 2013).



Gambar 2.1 National Vulnerability Database
(Sumber: https://avleonov.com/wp-content/uploads/2017/09/NVD_new.png)

2.6 Kecerdasan Buatan dan *Large Language Models* (LLM)

Kecerdasan Buatan (AI) adalah studi tentang agen cerdas yang dapat memahami lingkungan dan mengambil tindakan untuk mencapai tujuan (Russell & Norvig, 2020). Salah satu perkembangan terkini dalam AI adalah *Large Language Models* (LLM). Vaswani et al. (2017) memperkenalkan arsitektur *Transformer* yang menjadi dasar bagi LLM modern seperti GPT dan Gemini. Zhao et al. (2023) menjelaskan bahwa LLM dilatih pada korpus teks yang sangat besar, memungkinkannya untuk melakukan berbagai tugas pemrosesan bahasa alami (*Natural Language Processing*) seperti peringkasan, penerjemahan, dan pembuatan teks dengan kualitas yang mendekati kemampuan manusia.

2.7 Promt Engineering

Untuk memanfaatkan LLM secara efektif, diperlukan teknik yang disebut *Prompt Engineering*. White et al. (2023) mendefinisikan *prompt engineering* sebagai teknik merancang input (instruksi) untuk model AI generatif guna menghasilkan *output* yang optimal dan spesifik. Dalam konteks analisis keamanan, teknik ini digunakan untuk mengarahkan model agar menghasilkan deskripsi kerentanan yang teknis namun mudah dipahami, serta menghindari halusinasi atau informasi yang tidak akurat.

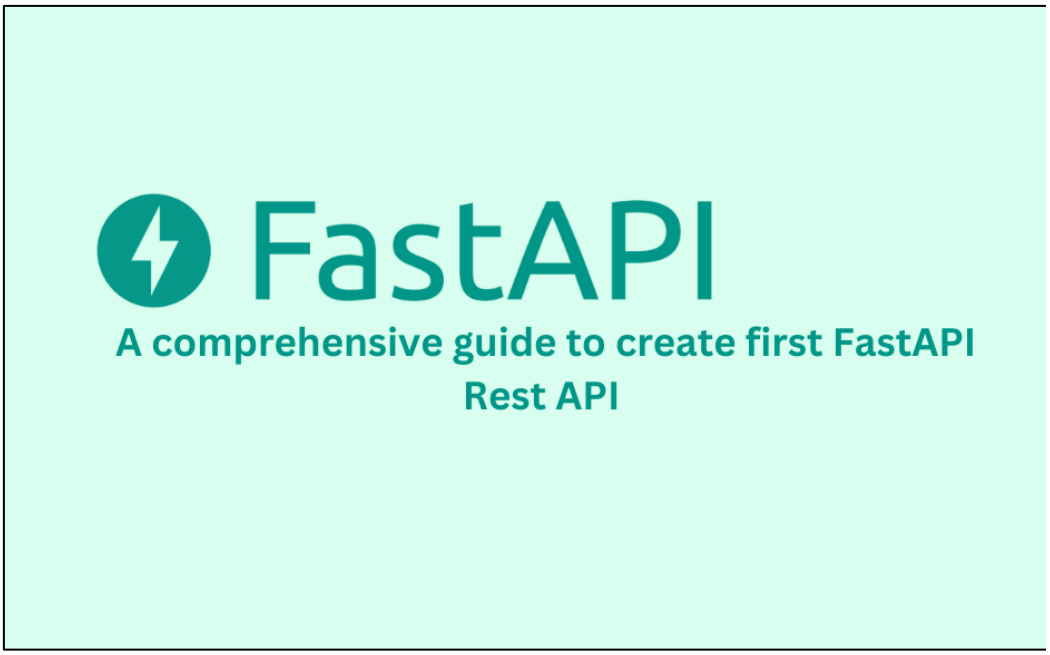
2.8 Bahasa Pemograman Python

Python adalah bahasa pemrograman tingkat tinggi yang ditafsirkan (*interpreted*) dan berorientasi objek. Van Rossum & Drake (2009) menciptakan Python dengan filosofi desain yang menekankan keterbacaan kode. Python menjadi sangat populer di bidang keamanan siber dan pengembangan AI karena ekosistem pustaka (*library*) yang luas. Dalam proyek ini, Python digunakan sebagai bahasa utama untuk logika *backend* karena dukungannya yang kuat terhadap manipulasi data JSON dan permintaan HTTP.

Gambar 2.2 Bahasa Pemograman Python
(Sumber:
https://cdn.computerhoy.com/sites/navi.axelspringer.es/public/media/image/2023/04/raspberry-lanza-editor-codigo-aprender-python-lenguaje-ia-3008158.jpg)

2.9 FastAPI Framework

FastAPI adalah kerangka kerja web modern untuk membangun API dengan Python. Ramirez (2024), pengembang FastAPI, merancang *framework* ini agar memiliki kinerja tinggi (setara dengan NodeJS dan Go) dan mudah digunakan. FastAPI memanfaatkan fitur *type hints* standar Python untuk validasi data otomatis dan dokumentasi interaktif. Penggunaan FastAPI dalam sistem ini memungkinkan pembuatan layanan mikro (*microservice*) yang ringan namun cepat untuk menangani permintaan analisis CVE.



Gambar 2.3 FastAPI
(Sumber: https://miro.medium.com/v2/resize:fit:1358/1*MBUCZSXY0eX-JZGrxvVk6A.png)

2.10 *Representational State Transfer* (REST) API

REST adalah gaya arsitektur perangkat lunak yang mendefinisikan seperangkat batasan yang digunakan untuk membuat layanan web. Fielding (2000) memperkenalkan REST sebagai pendekatan komunikasi *stateless* antara klien dan server. Dalam arsitektur REST, sumber daya dimanipulasi menggunakan metode HTTP standar (GET, POST, PUT, DELETE). Sistem *AI Assistant* ini menerapkan prinsip REST API untuk komunikasi antara antarmuka pengguna (*frontend*) dan logika server (*backend*), menggunakan format pertukaran data JSON.

2.11 *JavaScript Object Notation* (JSON)

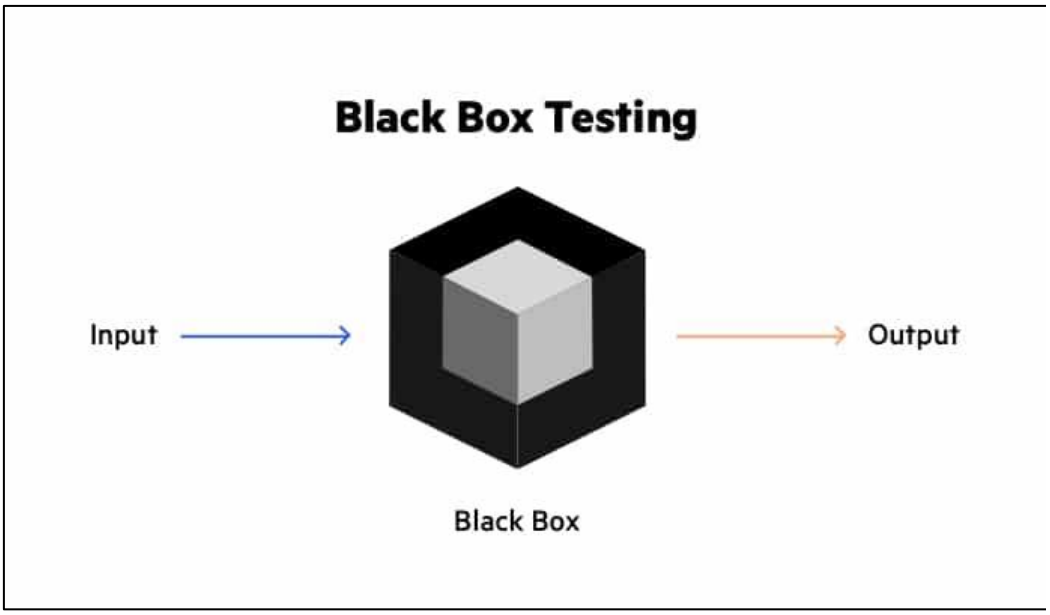
JSON adalah format pertukaran data yang ringan, mudah dibaca oleh manusia, dan mudah diurai oleh mesin. Crockford (2006) mendefinisikan JSON sebagai format teks yang tidak bergantung pada bahasa pemrograman tertentu, meskipun menggunakan konvensi yang familiar bagi pemrogram keluarga bahasa C. Dalam

sistem ini, JSON digunakan sebagai format utama untuk mengirimkan daftar CVE dari klien ke server dan mengembalikan hasil analisis laporan.

Gambar 2.4 JSON
(Sumber: https://blog.madrzejewski.com/wp-content/uploads/2018/07/json-logo.png)

2.12 Pengujian *Black Box*

Untuk memanfaatkan LLM secara efektif, diperlukan teknik yang disebut *Prompt Engineering*. White et al. (2023) mendefinisikan *prompt engineering* sebagai teknik merancang input (instruksi) untuk model AI generatif guna menghasilkan *output* yang optimal dan spesifik. Dalam konteks analisis keamanan, teknik ini digunakan untuk mengarahkan model agar menghasilkan deskripsi kerentanan yang teknis namun mudah dipahami, serta menghindari halusinasi atau informasi yang tidak akurat.

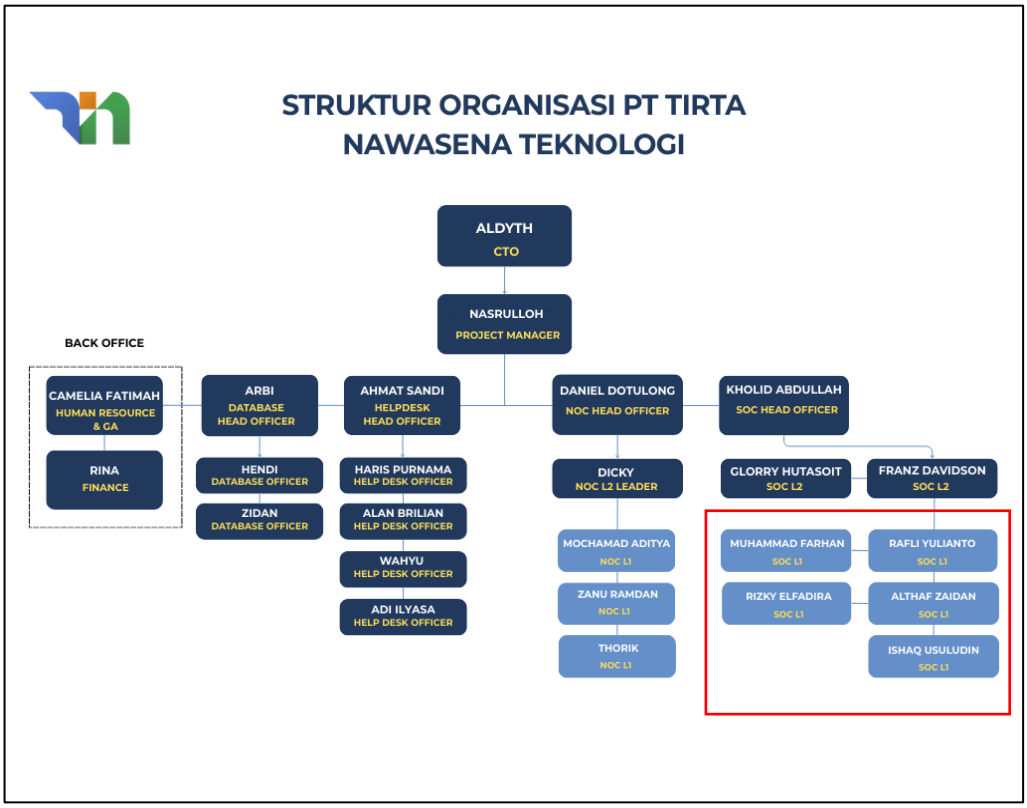


Gambar 2.4 Black Box Testing
(Sumber;https://www.imperva.com/learn/wp-content/uploads/sites/13/2020/03/thumbnail_Black-box.jpg)

BAB III
HASIL KEGIATAN MAGANG

3.1 Profil DUDI

PT Tirta Nawasena Teknologi adalah perusahaan yang bergerak di bidang penyediaan layanan teknologi informasi dan solusi digital terintegrasi. Perusahaan ini berfokus pada pemberian layanan *Managed Services*, konsultasi infrastruktur jaringan, dan keamanan siber untuk membantu berbagai instansi dan korporasi dalam mengelola aset digital mereka secara efisien dan aman.



Gambar 3.1 Struktur Organisasi

Dalam struktur operasionalnya, perusahaan ini memiliki unit kerja khusus yang bertanggung jawab atas keamanan informasi, yaitu:

Divisi *Security Operation Center* (SOC) Divisi ini merupakan tempat penulis melaksanakan kegiatan Praktik Kerja Lapangan (PKL). Sebagai garda terdepan

pertahanan siber perusahaan, SOC beroperasi selama 24/7 untuk memantau, mendeteksi, dan menanggapi ancaman keamanan secara *real-time*.

Tugas dan tanggung jawab utama divisi SOC meliputi:

a. **Pemantauan Keamanan (*Monitoring*):** Mengawasi lalu lintas jaringan dan aktivitas *endpoint* secara terus-menerus untuk mendeteksi anomali atau perilaku mencurigakan.
b. **Analisis Ancaman (*Threat Analysis*):** Menganalisis indikator serangan siber (*Indicators of Compromise*) menggunakan berbagai sumber intelijen ancaman (*Cyber Threat Intelligence*).
c. **Penanganan Insiden (*Incident Response*):** Melakukan respons cepat terhadap insiden keamanan yang terdeteksi untuk meminimalkan dampak kerusakan.
d. **Manajemen Kerentanan (*Vulnerability Management*):** Mengidentifikasi, mengklasifikasikan, dan memberikan rekomendasi perbaikan terhadap celah keamanan pada sistem.

Tim SOC bekerja secara kolaboratif menggunakan berbagai teknologi mutakhir seperti SIEM (*Security Information and Event Management*), EDR (*Endpoint Detection and Response*), dan alat otomasi untuk memastikan integritas dan ketersediaan data klien terjaga.

3.2 Uraian Kegiatan Magang

Selama periode magang berlangsung dari tanggal 21 Juli 2025 hingga akhir Desember 2025 di PT Tirta Nawasena Teknologi, penulis ditempatkan pada divisi *Security Operation Center* (SOC). Kegiatan magang difokuskan pada pemantauan keamanan siber, analisis insiden, dan penerapan alat bantu untuk efisiensi operasional. Berdasarkan catatan kegiatan mingguan, kegiatan dapat dikelompokkan menjadi tiga tahapan utama:

3.2.1 Tahap Pengenalan dan Pelatihan (*Onboarding*)

Pada tahap awal (Minggu 1-2), penulis mendapatkan pengenalan mendalam mengenai lingkungan perusahaan dan mitra kerja (PT Semen Indonesia Group). Penulis mempelajari berbagai *tools* yang digunakan di SOC, seperti SIEM Crowdstrike, serta alat-alat *Cyber Threat Intelligence* (CTI) meliputi OTX, CTX, Cyfirma, IBM X-Force Exchange, dan VirusTotal. Penulis juga mendapatkan pelatihan dasar *cybersecurity* melalui materi Fortinet Training Institute (NSE 1) dan memahami dokumen *Playbook* SOC sebagai pedoman penanganan insiden.

3.2.2 Tahap Operasional Harian (*Dily Operations*)

Memasuki minggu ke-3 hingga seterusnya, penulis aktif melakukan *monitoring* keamanan siber secara *shifting* (24/7). Tugas utama meliputi pemantauan deteksi *endpoint* menggunakan Crowdstrike dan XDR Tehtris, serta manajemen IOC (*Indicators of Compromise*). Rutinitas harian mencakup **monitoring EDR & SIEM serta pembuatan Flash Report** untuk insiden yang terdeteksi. Penulis juga rutin menyusun laporan mingguan, seperti laporan data karantina (*quarantine report*), laporan bukti *blocking hash* (Dokumen SOC 7 Layer), dan laporan kebocoran data (*databreach*) dari Cyfirma. Penulis juga terlibat dalam proses penarikan data log (*data pulling*) dari perangkat Firewall Palo Alto pada minggu ke-16 dan ke-19.

3.2.3 Tahap Implementasi dan Pengembangan CVE Assistant

Mulai minggu ke-5, penulis mulai mengimplementasikan alat bantu bernama **"CVE Assistant"** untuk meningkatkan efisiensi tim dalam menganalisis kerentanan. Penulis mempelajari cara kerja *tools* tersebut, melakukan konfigurasi penyesuaian (*tuning*), dan memanfaatkannya untuk mempercepat pembuatan laporan data karantina. Pada minggu ke-8 dan ke-19, penulis melakukan perbaikan kode (*debugging*) dan peningkatan antarmuka (*UI/UX*) pada CVE Assistant agar lebih mudah digunakan oleh tim SOC untuk mendeskripsikan dan menganalisis CVE secara otomatis.

Table 3.1 Logbook harian

Hari ke-	Hari / Tanggal	Kegiatan / Aktivitas	Output / Hasil
1	Senin, 21 Juli 2025	Pengenalan perusahaan Tirta Nawasena Teknologi sebagai Mitra dari PT Semen Indonesia Group.	Memahami profil perusahaan & klien.
2	Selasa, 22 Juli 2025	Pengenalan lingkungan kerja dan divisi SOC.	Mengenal tim & workflow SOC.
3	Rabu, 23 Juli 2025	Pengenalan Tools SIEM Crowdstrike.	Memahami dashboard Crowdstrike.
4	Kamis, 24 Juli 2025	Pengenalan CTI Tools (OTX, CTX, Cyfirma, IBM X-change dan VirusTotal).	Mengetahui fungsi tools CTI.
5	Jumat, 25 Juli 2025	Pengenalan flash reporting.	Memahami format laporan cepat.
6	Senin, 28 Juli 2025	Melaksanakan Training dasar-dasar cybersecurity (Fortinet Training Institute NSE 1).	Sertifikat/Modul NSE 1 selesai.
7	Selasa, 29 Juli 2025	Lanjutan Training Fortinet NSE 1 & Diskusi materi.	Pemahaman threat landscape.
8	Rabu, 30 Juli 2025	Memahami Playbook SOC.	Mengerti SOP penanganan insiden.
9	Kamis, 31 Juli 2025	Melakukan monitoring endpoint detection Crowdstrike (Observasi).	Log monitoring awal.
10	Jumat, 01 Agustus 2025	Evaluasi materi training & monitoring minggu ke-2.	Review pemahaman.
11	Senin, 04 Agustus 2025	Pengenalan tools XDR Tehtris & Monitoring rutin.	Memahami dashboard Tehtris.
12	Selasa, 05 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian & Flash Report.

13	Rabu, 06 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Draft laporan Harian.
14	Kamis, 07 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	Log harian & IOC terupdate.
15	Jumat, 08 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Analisis log Tehtris.	Laporan analisis log.
16	Senin, 11 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
17	Selasa, 12 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine mingguan.	Laporan Harianselesai.
18	Rabu, 13 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Pengenalan CTI Tools baru Cisco Talos.	Memahami fitur Cisco Talos.
19	Kamis, 14 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	Database IOC diperbarui.
20	Jumat, 15 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Eskalasi tiket insiden.	Tiket insiden terkirim.
21	Senin, 18 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
22	Selasa, 19 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
23	Rabu, 20 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Perancangan penggunaan tools CVE Assistant.	Konsep implementasi tools.
24	Kamis, 21 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Analisis fitur pada CVE Assistant.	Pemahaman fitur tools.
25	Jumat, 22 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Evaluasi mingguan.	Catatan evaluasi.
26	Senin, 25 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
27	Selasa, 26 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Uji coba CVE Assistant untuk scan data CVE.	Hasil scan otomatis.
28	Rabu, 27 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Testing akurasi output CVE Assistant.	Hasil testing akurasi.

29	Kamis, 28 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Implementasi CVE Assistant untuk laporan Harian.	Laporan harian cepat.
30	Jumat, 29 Agustus 2025	Monitoring EDR/SIEM, Flash Report, & Cek kesehatan agen Tehtris.	Status agen endpoint.
31	Senin, 01 September 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
32	Selasa, 02 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
33	Rabu, 03 September 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
34	Kamis, 04 September 2025	Monitoring EDR/SIEM, Flash Report, & Analisis anomali trafik jaringan.	Laporan analisis trafik.
35	Jumat, 05 September 2025	Monitoring EDR/SIEM, Flash Report, & Evaluasi performa tools CVE Assistant.	Feedback tools.
36	Senin, 08 September 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
37	Selasa, 09 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
38	Rabu, 10 September 2025	Monitoring EDR/SIEM, Flash Report, & Memperbaiki kode CVE Assistant (Bug fixing).	Kode program diperbarui.
39	Kamis, 11 September 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
40	Jumat, 12 September 2025	Monitoring EDR/SIEM, Flash Report, & Rekap aktivitas mingguan.	Laporan mingguan.
41	Senin, 15 September 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
42	Selasa, 16 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
43	Rabu, 17 September 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
44	Kamis, 18 September 2025	Monitoring EDR/SIEM, Flash Report, & Cek status antivirus server kritis.	Status keamanan server.

45	Jumat, 19 September 2025	Monitoring EDR/SIEM, Flash Report, & Diskusi tim mengenai ancaman terbaru.	Notulensi diskusi.
46	Senin, 22 September 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
47	Selasa, 23 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
48	Rabu, 24 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen SOC 7 Layer.
49	Kamis, 25 September 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
50	Jumat, 26 September 2025	Monitoring EDR/SIEM, Flash Report, & Analisis trafik outbound mencurigakan.	Hasil investigasi IP.
51	Senin, 29 September 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
52	Selasa, 30 September 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
53	Rabu, 01 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
54	Kamis, 02 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
55	Jumat, 03 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Evaluasi bulanan kinerja.	Hasil evaluasi.
56	Senin, 06 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
57	Selasa, 07 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
58	Rabu, 08 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
59	Kamis, 09 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Melakukan konfigurasi EDR Tehtris.	Policy EDR baru.
60	Jumat, 10 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Cek log firewall terkait EDR.	Log koneksi.

61	Senin, 13 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
62	Selasa, 14 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
63	Rabu, 15 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
64	Kamis, 16 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Melakukan konfigurasi EDR Tehtris.	Konfigurasi EDR.
65	Jumat, 17 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Persiapan handover shift.	Catatan handover.
66	Senin, 20 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
67	Selasa, 21 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
68	Rabu, 22 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan Databreach dari Cyfirma.	Laporan Databreach.
69	Kamis, 23 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
70	Jumat, 24 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
71	Senin, 27 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.
72	Selasa, 28 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
73	Rabu, 29 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan Databreach dari Cyfirma.	Laporan Databreach.
74	Kamis, 30 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
75	Jumat, 31 Oktober 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
76	Senin, 03 November 2025	Monitoring EDR/SIEM, Flash Report, & Monitoring Crowdstrike/Tehtris 24/7 shifting.	Log harian.

77	Selasa, 04 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
78	Rabu, 05 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
79	Kamis, 06 November 2025	Monitoring EDR/SIEM, Flash Report, & Konfigurasi Crowdstrike IOC management.	IOC list updated.
80	Jumat, 07 November 2025	Monitoring EDR/SIEM, Flash Report, & Mengerjakan tarikan data dari Palo Alto.	Data Log Palo Alto.
81	Senin, 10 November 2025	Monitoring Endpoint detection SIEM EDR & EPP (P1, P2, P3) Tehtris 24/7 shifting.	Log harian & Matriks eskalasi.
82	Selasa, 11 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
83	Rabu, 12 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan Databreach dari Cyfirma.	Laporan Databreach.
84	Kamis, 13 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
85	Jumat, 14 November 2025	Monitoring EDR/SIEM, Flash Report, & Melakukan konfigurasi EDR Tehtris.	Konfigurasi EDR.
86	Senin, 17 November 2025	Monitoring Endpoint detection EDR & EPP (P1, P2, P3) Tehtris 24/7 shifting.	Log harian.
87	Selasa, 18 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.
88	Rabu, 19 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan Databreach dari Cyfirma.	Laporan Databreach.
89	Kamis, 20 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
90	Jumat, 21 November 2025	Monitoring EDR/SIEM, Flash Report, & Melakukan konfigurasi EDR Tehtris.	Konfigurasi EDR.
91	Senin, 24 November 2025	Monitoring Endpoint detection EDR, EPP (P1, P2, P3), & SIEM Tehtris 24/7 shifting.	Log harian.
92	Selasa, 25 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat laporan data quarentine.	Laporan Harian.

93	Rabu, 26 November 2025	Monitoring EDR/SIEM, Flash Report, & Membuat Laporan bukti blocking hash (SOC 7 Layer).	Dokumen bukti blocking.
94	Kamis, 27 November 2025	Monitoring EDR/SIEM, Flash Report, & Mengerjakan tarikan data dari Palo Alto.	Data Log Palo Alto.
95	Jumat, 28 November 2025	Monitoring EDR/SIEM, Flash Report, & Memperbaiki kode CVE Assistant (UI/UX).	Tampilan UI baru.
96	Senin, 01 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Finalisasi fitur CVE Assistant.	Fitur bulk aktif.
97	Selasa, 02 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Analisis insiden akhir tahun.	Laporan insiden.
98	Rabu, 03 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Dokumentasi teknis CVE Assistant.	User Guide.
99	Kamis, 04 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Handover kode program ke supervisor.	Source code handover.
100	Jumat, 05 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Backup data kerja pribadi.	Data backup.
101	Senin, 08 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Penyusunan draf Laporan Magang (Bab 1-2).	Draf Laporan.
102	Selasa, 09 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Penyusunan draf Laporan (Bab 3).	Draf Bab 3.
103	Rabu, 10 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Membantu operasional tim SOC.	Log harian.
104	Kamis, 11 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Revisi laporan magang.	Revisi laporan.
105	Jumat, 12 Desember 2025	Monitoring EDR/SIEM, Flash Report, & Verifikasi akses tools sebelum pamit.	Checklist akses.
106	Senin, 15 Desember 2025	Monitoring EDR/SIEM, Flash Report, terakhir dan perpisahan tim shift.	Log harian terakhir.
107	Selasa, 16 Desember 2025	Presentasi hasil proyek CVE Assistant di depan manajer SOC.	Slide presentasi.
108	Rabu, 17 Desember 2025	Penyelesaian administrasi magang & Tanda tangan logbook.	Logbook lengkap.

109	Kamis, 18 Desember 2025	Pengembalian inventaris perusahaan (ID Card, Akses).	Berita acara kembali.
110	Jumat, 19 Desember 2025	Penutupan kegiatan magang secara resmi di PT Tirta Nawasena.	Surat keterangan selesai.

3.3 Pembahasan Hasil Magang

Selama pelaksanaan Praktik Kerja Lapangan di PT Tirta Nawasena Teknologi, penulis ditempatkan pada divisi *Security Operation Center* (SOC). Tugas utama yang dilakukan meliputi pemantauan lalu lintas jaringan, analisis peringatan keamanan (*security alerts*), dan pelaporan insiden.

Salah satu tantangan utama yang ditemukan dalam operasional harian SOC adalah proses analisis kerentanan (*vulnerability analysis*) yang memakan waktu. Analis harus mencari informasi CVE (*Common Vulnerabilities and Exposures*) secara manual dari *National Vulnerability Database* (NVD), menerjemahkan deskripsi teknis, dan menyusunnya menjadi laporan berbahasa Indonesia yang mudah dipahami oleh klien atau pemangku kepentingan. Volume CVE yang tinggi seringkali menyebabkan keterlambatan dalam pelaporan (*bottleneck*).

Sebagai solusi atas permasalahan tersebut, penulis mengembangkan sebuah alat bantu (*tool*) bernama "CVE Assistant". Hasil utama dari magang ini adalah sebuah aplikasi berbasis *web* yang mengotomatisasi proses pengambilan data CVE, penerjemahan, dan format laporan menggunakan teknologi *Generative AI*. Sistem ini berhasil mengintegrasikan *Application Programming Interface* (API) publik NVD dan Google Gemini untuk menghasilkan deskripsi kerentanan yang terstandarisasi, sehingga meningkatkan efisiensi waktu analisis tim SOC secara signifikan.

3.4 Deskripsi *Project/Produk*

Produk yang dihasilkan diberi nama **CVE Assistant**. Ini adalah aplikasi berbasis *web* yang dirancang khusus untuk kebutuhan internal tim SOC PT Tirta Nawasena Teknologi.

3.4.1 Gambaran Umum Sistem

CVE Assistant berfungsi sebagai *agregator* dan *generator* konten cerdas. Pengguna (analis SOC) cukup memasukkan daftar ID CVE yang terdeteksi, dan sistem akan secara otomatis:

a. Mengambil metadata teknis yang akurat dari sumber resmi (NVD NIST).

b. Mengambil metadata teknis yang akurat dari sumber resmi (NVD NIST).

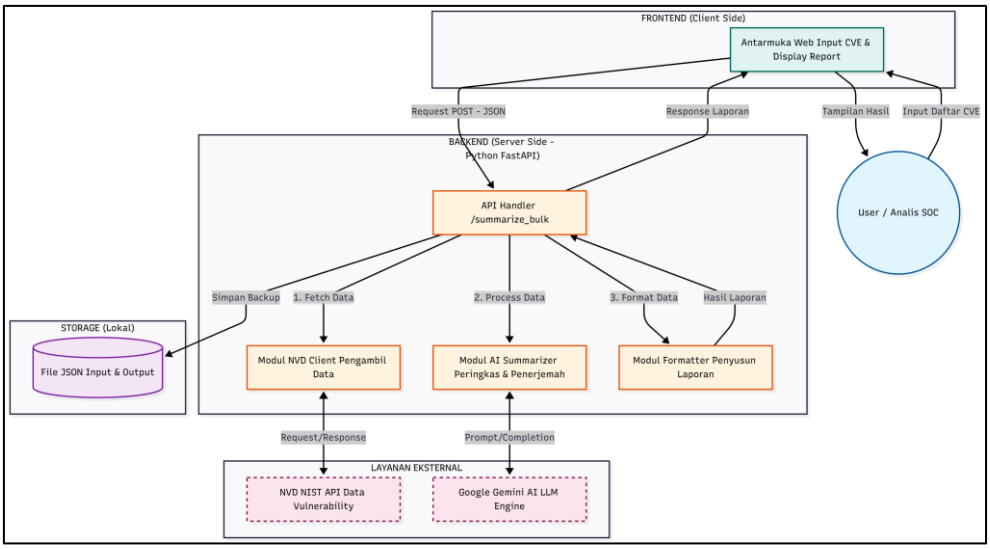
c. Menggunakan kecerdasan buatan (Google Gemini) untuk meringkas dan menerjemahkan dampak teknis ke dalam Bahasa Indonesia.

d.Menghasilkan keluaran dalam format laporan standar perusahaan.

3.4.2 Arsitektur dan Diagram Blok Sistem

Sistem *CVE Assistant* dirancang menggunakan arsitektur *Client-Server* dengan pola komunikasi *RESTful API*. Pendekatan ini memisahkan logika presentasi (*frontend*) dan logika pemrosesan bisnis (*backend*) untuk memastikan skalabilitas dan kemudahan pemeliharaan kode.

Untuk memberikan gambaran menyeluruh mengenai komponen dan aliran data dalam sistem, berikut disajikan diagram blok arsitektur sistem:



Gambar 3.2 Diagram Blok Arsitektur Sistem

a. **Frontend (Client Side)** Bagian ini merupakan antarmuka pengguna berbasis web yang dimuat pada *browser*. Komponen ini bertugas:

(1) Menyediakan formir input untuk daftar CVE.

(2) Mengirimkan permintaan (*request*) data dalam format JSON ke server.

(3) Menampilkan hasil laporan yang telah diproses kepada pengguna (*User/Analis SOC*).

b. ***Backend*** **(Server Side)** Bagian ini adalah inti pemrosesan yang dibangun menggunakan **Python FastAPI**. *Backend* berfungsi sebagai *API Handler* yang mengatur rute lalu lintas data, meliputi:

(1) Validasi data yang masuk dari *frontend*.

(2) Orkestrasi komunikasi dengan modul-modul internal (NVD Client, AI Summarizer, dan Formatter).

(3) Manajemen *input* dan *output* data.

c. ***Storage*** **(Penyimpanan Lokal)** Sistem dilengkapi dengan mekanisme penyimpanan lokal berbasis *file* JSON. Komponen ini berfungsi untuk:

(1) Menyimpan arsip data input mentah sebagai cadangan (*backup*).

(2) Menyimpan hasil laporan yang telah digeneralisasi agar dapat diunduh kembali tanpa perlu memproses ulang.

3.5 Requirement/Spesifikasi *Project/Produk*

Untuk memastikan sistem dapat berjalan dengan baik di lingkungan operasional SOC, berikut adalah spesifikasi kebutuhan sistem:

3.5.1 Kebutuhan Perangkat Lunak (*Software*)

a. **Bahasa Pemrograman**: Python 3.10 atau lebih baru (untuk performa *asynchronous* yang lebih baik).

b. **Web Framework**: FastAPI (dipilih karena kecepatan eksekusi dan kemudahan pembuatan API).

c. **Web Server**: Uvicorn (sebagai server ASGI).

d. **Generative AI SDK**: google-generativeai (untuk akses ke model Gemini).

e. **HTTP Client: Library requests (untuk komunikasi dengan NVD).**

f. **Frontend**: HTML5, CSS3, dan *Vanilla JavaScript*.

3.5.2 Kebutuhan Perangkat Keras (*Hardware*)

Aplikasi ini bersifat ringan dan dijalankan pada perangkat kerja analis atau *server* lokal pengembangan dengan spesifikasi minimum:

a. **Prosesor**: Intel Core i5 / setara

b. **RAM**: 8 GB (disarankan 16 GB untuk *multitasking*).

c. **Koneksi Internet**: Wajib dan stabil (untuk mengakses API NVD dan Google AI).

3.5.3 Kebutuhan Fungsional

a. Sistem harus dapat menerima *input* berupa satu atau lebih ID CVE sekaligus (*bulk processing*).

b. Sistem harus dapat mengambil data deskripsi, skor CVSS, dan produk terdampak dari NVD.

c. Sistem harus mampu menerjemahkan istilah teknis keamanan siber ke Bahasa Indonesia yang baku.

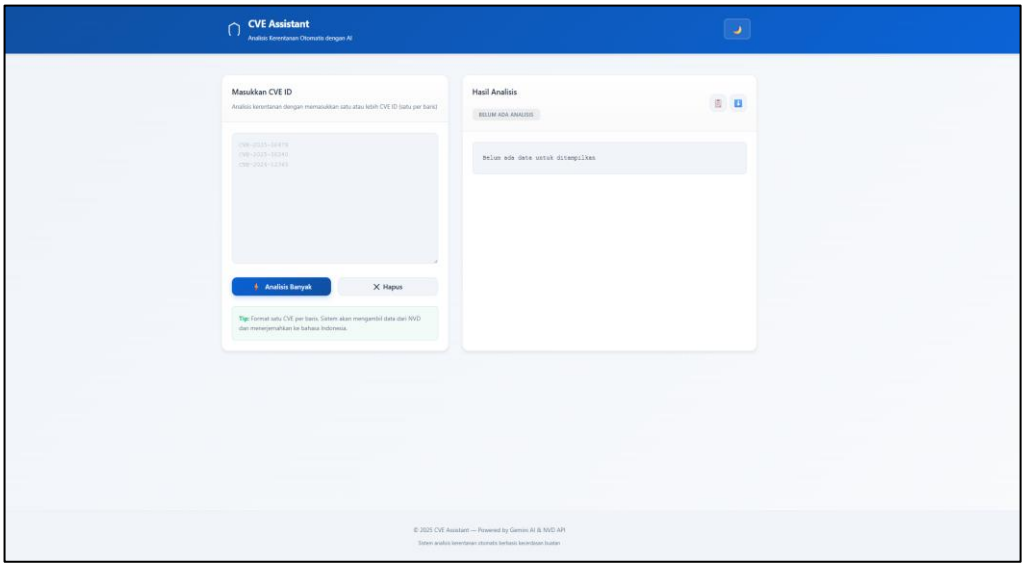
d. Sistem harus menghasilkan format laporan yang mencakup: Deskripsi, Produk Terdampak, Potensi Risiko, dan Rekomendasi.

3.6 Desain *Project/Produk*

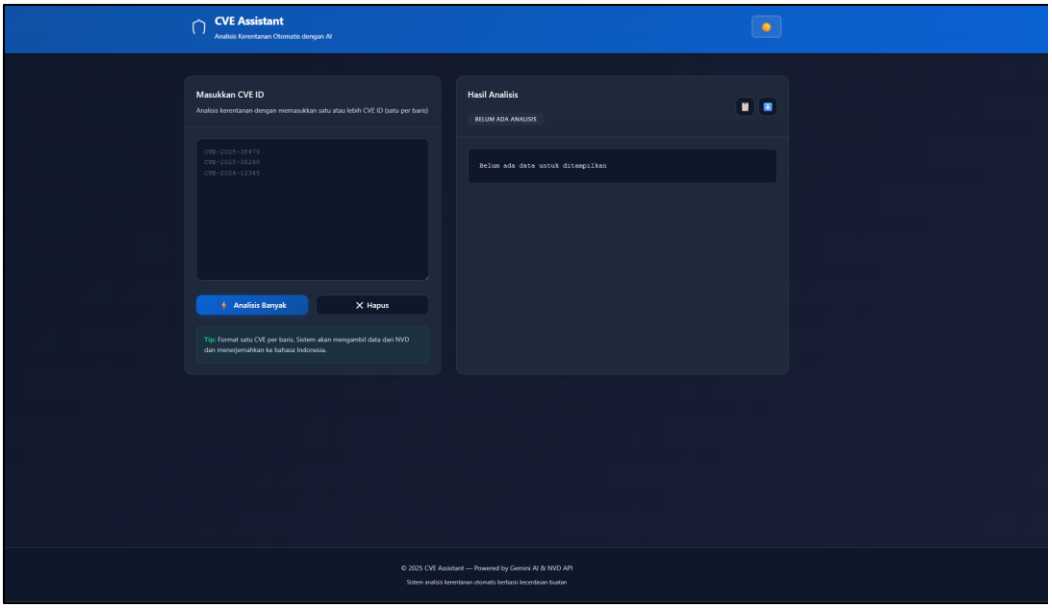
Perancangan sistem difokuskan pada kesederhanaan penggunaan (*user experience*) karena target penggunanya adalah analis teknis yang membutuhkan kecepatan.

3.6.1 Desain Antarmuka (*User Interface*)

Antarmuka dirancang dengan tata letak dua panel (*split-screen*):



Gambar 3.3 Desain Web Light Mode



Gambar 3.4 Desain Web Dark Mode

a. **Panel Kiri (Input)**: Area teks (*textarea*) bagi analis untuk menempelkan (*paste*) daftar CVE dari alat deteksi ancaman. Tombol aksi "Analisis Banyak" ditempatkan di bawah area ini.

b. **Panel Kanan (Output)**: Area hasil yang menampilkan laporan terstruktur. Dilengkapi dengan fitur "Salin ke *Clipboard*" dan "Unduh Laporan" untuk mempercepat pemindahan data ke dokumen laporan resmi.

c. **Tema**: Menyediakan opsi tampilan Mode Gelap (*Dark Mode*) dan Terang (*Light Mode*) yang dapat disesuaikan secara fleksibel, guna memaksimalkan kenyamanan visual analis di berbagai kondisi pencahayaan ruang kerja

3.7 Implementasi

Tahap implementasi adalah realisasi dari rancangan sistem ke dalam kode program. Struktur direktori proyek diatur secara modular untuk memudahkan pemeliharaan.

3.7.1 Modul *Backend* (app/)

Logika utama aplikasi dibangun dalam tiga modul Python terpisah:

a. main.py (*Core Application*):

Modul ini menginisialisasi aplikasi FastAPI dan memuat variabel lingkungan (seperti GEMINI_API_KEY). Fungsi utamanya adalah menangani *endpoint* POST /summarize_bulk. Saat permintaan diterima, modul ini memvalidasi *input*, memanggil fungsi pengambilan data, dan mengembalikan respons JSON.

b.nvd_client.py (*Data Fetching*):

Bertanggung jawab untuk komunikasi dengan API NIST NVD. Fungsi fetch_cve_from_nvd(cve_id) mengirimkan permintaan HTTP GET. Modul ini menangani pengecekan status respon dan mengekstrak objek kerentanan (*vulnerabilities*) dari data JSON yang kompleks yang dikembalikan oleh NVD.

c. Synnarize.py (*AI Processing*):

Modul ini adalah "otak" dari fitur kecerdasan buatan. Fungsi summarize_cve_with_gemini mengirimkan *prompt* khusus ke model Google Gemini untuk meminta ringkasan teknis. Fungsi translate_to_indonesian memastikan *output* akhir diterjemahkan ke Bahasa Indonesia tanpa menghilangkan konteks teknis. Modul ini juga memiliki fungsi format_user_template untuk menyusun *string* akhir sesuai standar laporan.

3.7.2 Modul *Frontend* (app/static/)

a. app.js: Menggunakan JavaScript murni (*Vanilla JS*) untuk menangani interaksi *Document Object Model* (DOM). Skrip ini menangkap klik tombol, mengirim data ke *backend* menggunakan *fetch API*, dan menampilkan animasi *loading* saat proses berlangsung.

b. style.css: Mengatur estetika tampilan menggunakan variabel CSS modern untuk konsistensi warna dan responsivitas tata letak.

3.8 Pengujian dan Pembahasan

Pengujian sistem dilakukan menggunakan metode **Black Box Testing**. Metode ini dipilih untuk memvalidasi fungsionalitas perangkat lunak berdasarkan spesifikasi kebutuhan, dengan cara mengamati hasil eksekusi melalui data uji dan memeriksa fungsionalitas dari antarmuka pengguna (*interface*) tanpa melihat struktur kode internalnya.

3.8.1 Skenario Pengujian

Pengujian dibagi menjadi tiga skenario utama untuk memastikan keandalan sistem:

a. **Pengujian Input Valid:** Memasukkan format CVE yang benar dan terdaftar di NVD.

b. **Pengujian Input Invalid:** Memasukkan format CVE yang salah atau tidak terdaftar.

c. **Pengujian Fungsionalitas Fitur:** Menguji tombol salin, unduh, dan hapus.

3.8.2 Hasil Penguian Black Box

Berikut adalah table hasil pengujian yang telah di lakukan terhadap sistem *CVE Assistan.*

Table 3.2 Hasil Pengujian

No	Skenario Pengujian	Input (Data Uji)	Ekspektasi Output	Hasil Pengujian (Aktual)	Status
1	**Input CVE Tunggal (Valid)**	CVE-2023-4863	Sistem menampilkan deskripsi, dampak, dan rekomendasi CVE tersebut dalam Bahasa Indonesia.	Sistem berhasil menampilkan laporan lengkap dalam Bahasa Indonesia sesuai format.	**Berhasil**

2	**Input CVE Banyak (*Bulk*)**	CVE-2023-4863, CVE-2024-21626	Sistem menggabungkan kedua CVE menjadi satu laporan terpadu.	Sistem menampilkan dua poin deskripsi dan rekomendasi yang terpisah namun dalam satu tampilan.	**Berhasil**
3	**Input CVE Tidak Ditemukan**	CVE-2099-99999 (Data Fiktif)	Sistem memberikan notifikasi bahwa data tidak ditemukan di NVD atau *skip* ke CVE berikutnya.	Sistem melewati CVE tersebut dan memberikan pesan *log* "Data tidak ditemukan".	**Berhasil**
4	**Input Format Salah**	TEST-ERROR-123 (Bukan format CVE)	Sistem menolak proses atau memberikan pesan kesalahan format.	Sistem tetap mencoba memproses namun mengembalikan pesan *error* dari API NVD karena format ID tidak valid.	**Berhasil**
5	**Fitur Tombol "Salin"**	Klik tombol "Salin Laporan"	Teks laporan tersalin ke *clipboard* komputer.	Teks berhasil disalin dan dapat di-*paste* ke Notepad/Word.	**Berhasil**
6	**Fitur Tombol "Unduh"**	Klik tombol "Unduh JSON"	*Browser* mengunduh file .json berisi hasil analisis.	File cve_report.json berhasil terunduh ke folder *Downloads*.	**Berhasil**

7	**Kualitas Terjemahan AI**	Deskripsi teknis CVE (Inggris)	Terjemahan Bahasa Indonesia yang mudah dipahami namun tetap mempertahankan istilah teknis (seperti *Buffer Overflow*).	Terjemahan cukup akurat, istilah teknis tetap dipertahankan, struktur kalimat baku.	**Berhasil**

Perhitungan Persentase Keberhasilan

Untuk mengukur tingkat keberhasilan fungsional sistem, digunakan rumus persentase kelayakan sebagai berikut:

$$\text{Persentase Keberhasilan} = \left(\frac{Jumlah\ Skenario\ Berhasil}{Jumlah\ Total\ Skenario}\right) \times 100\%$$

Berdasarkan Tabel 3.2, perhitungan keberhasilannya adalah:

$$\text{Persentase Keberhasilan} = \left(\frac{7}{7}\right) \times 100\% = 100\%$$

Hasil perhitungan menunjukkan bahwa sistem memiliki tingkat keberhasilan fungsional sebesar **100%**.

3.8.3 Pengujian Efesiensi Waktu

Pengujian ini bertujuan untuk membandingkan rata-rata waktu yang dibutuhkan untuk menganalisis dan membuat laporan CVE antara metode manual (sebelumnya) dengan menggunakan sistem *CVE Assistant*.

Table 3.3 Perbandingan Waktu Pengerjaan (Manual vs Sistem)

Sample	**ID CVE**	Manual (Menit)	Sistem (Menit)	Efisiensi
1	CVE-2024-21626	12.5	0.8	15.6x Lebih Cepat
2	CVE-2023-4863	10.0	0.5	20.0x Lebih Cepat
3	CVE-2024-3400	15.2	0.9	16.8x Lebih Cepat
4	CVE-2023-38545	11.4	0.7	16.2x Lebih Cepat
5	CVE-2024-3094	14.0	0.8	17.5X Lebih Cepat
Total		63.1	3.7	

Perhitungan Rata-Rata Waktu

Perhitungan rata-rata waktu (*Mean Time*) dilakukan menggunakan rumus:

$$\bar{X} = \frac{\sum xi}{n}$$

Dimana :

$\bar{X}$= Rata-rata waktu

$\sum xi$= Total waktu seluruh sample

n = Jumlah sample (5)

a. Rata-rata Waktu Manual

$$\bar{x}_{Manual} = \frac{63.1}{5} = 12.62\ Menit$$

b.Rata-rata Waktu Sistem (CVE Assistant)

$$\bar{x}_{sistem} = \frac{3.7}{5} = 0.74\ Menit \approx 44.4\ Detik$$

3.8.4 Analisi Hasil Pengujian

Berdasarkan hasil pengujian di atas, dapat dianalisis bahwa:

a. **Fungsionalitas Utama:**

Sistem berhasil menjalankan fungsi utamanya dengan tingkat keberhasilan 100%. Tidak ditemukan *bug* kritis saat diberikan input valid maupun invalid.

b. **Peningkatan Efisiensi:**

Implementasi *CVE Assistant* terbukti mampu memangkas waktu pengerjaan secara signifikan. Rata-rata waktu analisis berkurang dari **12,62 menit** (manual) menjadi hanya **0,74 menit** (44 detik) menggunakan sistem. Hal ini menunjukkan peningkatan efisiensi waktu sebesar kurang lebih **17 kali lipat**.

c. **Penanganan Kesalahan (Error Handling):**

Integrasi dengan Google Gemini menunjukkan hasil yang memuaskan. Model AI mampu memahami konteks keamanan siber, misalnya menerjemahkan *"Remote Code Execution"* dengan benar tanpa mengubah makna teknisnya. Namun, pada beberapa kasus CVE yang sangat baru (0-day), AI mungkin memberikan deskripsi yang terlalu umum jika data rinci belum tersedia di NVD.

d. **Akurasi AI:**

Integrasi dengan Google Gemini menunjukkan hasil terjemahan yang memuaskan dan kontekstual terhadap istilah keamanan siber, sesuai juga dengan model pelaporan yang dipakai perusahaan.

3.8.5 Kendala yang Dihadapi

Selama pengembangan dan uji coba, terdapat beberapa kendala teknis:

a.Batasan API NVD (*Rate Limiting*):

API publik NVD memiliki batasan jumlah permintaan per menit. Jika pengguna memasukkan terlalu banyak CVE sekaligus, sistem terkadang mengalami *timeout* atau penolakan akses. *Solusi Sementara*: Menambahkan jeda waktu (*delay*) antar permintaan di kode *backend*.

b.Ketergantungan Koneksi Internet:

Sistem sepenuhnya bergantung pada koneksi internet untuk mengakses NVD dan Gemini. Jika jaringan *offline*, alat ini tidak dapat berfungsi.

c. Akurasi Terjemahan:

Pada kasus CVE yang sangat baru atau spesifik, AI terkadang memberikan terjemahan yang terlalu harfiah. Namun, hal ini diatasi dengan fitur *editing* manual pada hasil *output* di *frontend* sebelum disalin.

BAB IV
PENUTUP

4.1 Kesimpulan

Berdasarkan kegiatan magang yang telah dilakukan serta pengembangan sistem "CVE Assistant" di PT Tirta Nawasena Teknologi, dapat ditarik beberapa kesimpulan yang menjawab tujuan pelaksanaan Praktik Kerja Lapangan sebagai berikut:

a. **Keberhasilan Implementasi Sistem Otomasi** Penulis telah berhasil mengimplementasikan sistem *CVE Assistant* yang terintegrasi dengan API NVD dan teknologi *Generative AI* (Google Gemini). Sistem ini mampu memperkuat kinerja *Security Operation Center* (SOC) dengan menyediakan deskripsi kerentanan, produk terdampak, dan rekomendasi mitigasi secara otomatis. Berdasarkan pengujian fungsional (*Black Box Testing*), seluruh fitur utama sistem berjalan dengan baik dengan tingkat keberhasilan **100%** pada semua skenario pengujian.

b. **Peningkatan Efisiensi Analisis Kerentanan** Hasil analisis kinerja menunjukkan bahwa penggunaan *AI Assistant* mempercepat proses triase dan pelaporan insiden secara signifikan. Berdasarkan data pengujian efisiensi waktu: * Rata-rata waktu pengerjaan manual berkurang drastis dari **12,62 menit** per insiden menjadi hanya **0,74 menit (44,4 detik)** menggunakan sistem. * Hal ini membuktikan adanya peningkatan efisiensi waktu sebesar kurang lebih **17 kali lipat**, yang memungkinkan tim SOC untuk merespons ancaman lebih cepat dan mengurangi risiko *bottleneck* pada antrean insiden.

c. **Penguatan Kualitas Pelaporan** Sistem ini berhasil menstandarisasi *output* laporan kerentanan ke dalam Bahasa Indonesia yang baku dan sesuai format internal perusahaan. Hal ini meminimalkan inkonsistensi interpretasi teknis yang sering terjadi pada pengerjaan manual, sehingga meningkatkan akurasi komunikasi risiko kepada pemangku kepentingan.

4.2 Saran

Demi pengembangan sistem yang lebih optimal dan keberlanjutan manfaat bagi perusahaan di masa mendatang, penulis menyampaikan beberapa saran sebagai berikut:

a. **Manajemen *Rate Limiting*:** Disarankan untuk mengimplementasikan mekanisme *caching* (penyimpanan sementara) pada *database* lokal untuk data CVE yang sering diakses. Hal ini akan mengurangi ketergantungan langsung pada API NVD dan menghindari pemblokiran akibat batas permintaan (*rate limit*).

b. **Peningkatan Antarmuka:** Pengembangan antarmuka pengguna (*User Interface*) dapat ditingkatkan dengan fitur riwayat pencarian (*history*) dan manajemen akun pengguna jika alat ini akan digunakan oleh tim yang lebih besar.

c. **Validasi Manusia (*Human-in-the-loop*):** Meskipun akurasi AI sudah baik, disarankan agar analis SOC tetap melakukan tinjauan akhir (*review*) terhadap *output* yang dihasilkan, terutama untuk kerentanan yang bersifat sangat kritis (*critical severity*), guna memastikan tidak ada kesalahan interpretasi konteks.

DAFTAR PUSTAKA

Ali, S., & P., A. (2021). *Security Operations Center (SOC) - A Practical Guide*. Packt Publishing.

Booth, H., Rike, D., & Witte, G. (2013). *The National Vulnerability Database (NVD): Overview*. National Institute of Standards and Technology.

Chuvakin, A., Schmidt, K. J., & Phillips, C. (2013). *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Syngress.

Crockford, D. (2006). *The Application/JSON Media Type for JavaScript Object Notation (JSON)*. RFC 4627.

Fielding, R. T. (2000). *Architectural Styles and the Design of Network-based Software Architectures* (Doctoral dissertation). University of California, Irvine.

FIRST. (2019). *Common Vulnerability Scoring System v3.1: Specification Document*. Forum of Incident Response and Security Teams.

Martin, R. A. (2001). Managing Vulnerabilities in Networked Systems. *Computer*, 34(11), 32-38.

MITRE Corporation. (2024). *About CVE*. Diakses pada 3 November 2025.

Muniz, J., & McIntyre, G. (2021). *The Modern Security Operations Center*. Cisco Press.

National Institute of Standards and Technology (NIST). (2024). *NVD General Information*. Diakses pada 3 November 2025.

Nidhra, S., & Dondeti, J. (2012). Black Box and White Box Testing Techniques - A Literature Review. *International Journal of Embedded Systems and Applications (IJESA)*, 2(2), 29-50.

Ramirez, S. (2024). *FastAPI Documentation*. Diakses pada 5 November 2025.

Russell, S. J., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.

Van Rossum, G., & Drake, F. L. (2009). *Python 3 Reference Manual*. CreateSpace.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems (NIPS)*, 30.

White, J., Fu, Q., Hays, S., Sandborn, M., Olea, C., Gilbert, H., ... & Schmidt, D. C. (2023). A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT. *arXiv preprint arXiv:2302.11382*.

Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., ... & Wen, J. R. (2023). A Survey of Large Language Models. *arXiv preprint arXiv:2303.18223*.

LAMPIRAN

PT. Tirta Nawasena Teknologi
Jl. Villa Melati Mas Raya No. 6 Blok I9
Tangerang Selatan 15323, Banten
Ph. (+62) 888 1772 211
Email. info@tirtanawasena.com

SURAT KETERANGAN
No. 02/SK/HRD/TNT/X1I/2025

Yang betanda tangan dibawah ini, Human Resource Departemen dari PT. Tirta Nawasena Teknologi, dengan ini menerangkan bahwa :

Nama : Ikhsan Fadillah
NIM / ID : 2207421013
Instisusi Pendidikan : Teknik Multimedia dan Jaringan

Telah melakukan program Magang pada divisi **Security Operation Center (SOC)** pada PT. Tirta Nawasena Teknologi, terhitung sejak :

Periode Magang : 21 Juli – 30 Desember 2025

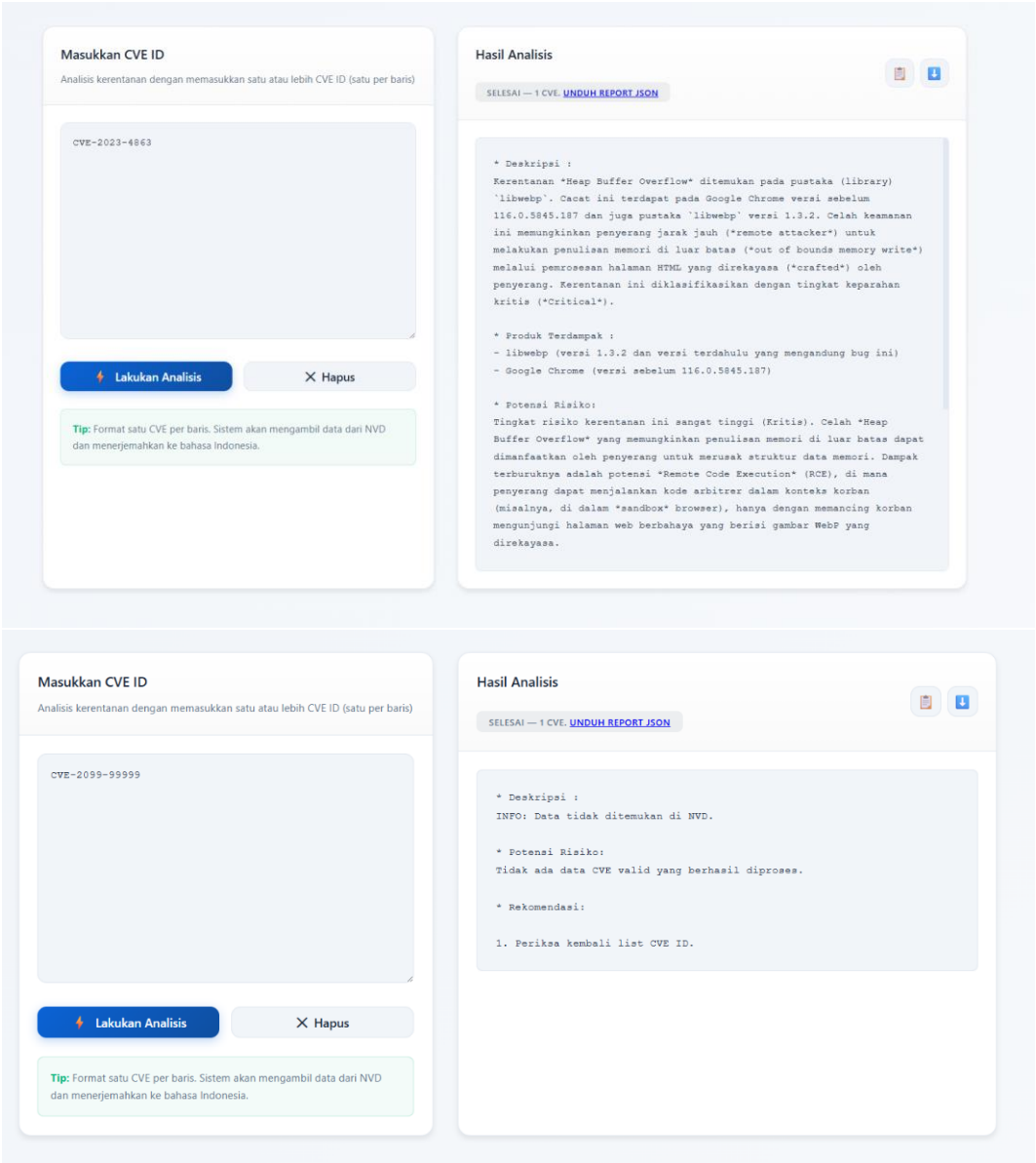
Selama masa magang, yang bersangkutan telah menjalankan tugas dan tanggung jawab dengan baik sesuai dengan standar dan ketentuan perusahaan, dengan rincian tugas sebagai berikut :

1. Melaksanakan monitoring dan respons keamanan sistem menggunakan CrowdStrike EDR dan ekosistem Tehtris (EPP, EDR, XDR, SIEM), termasuk analisis alert, penanganan insiden, penyusunan Flash Report, serta penerapan kebijakan keamanan dan pemblokiran indikator ancaman.
2. Menyusun dan memperbarui laporan keamanan dan vulnerability assessment secara berkala, meliputi laporan SIEM, data breach, analisis time event, serta validasi domain berisiko.
3. Mengembangkan proyek akhir berupa aplikasi AI "CVE Assistant" untuk mengotomatisasi analisis kerentanan dan pembuatan laporan guna meningkatkan efisiensi operasional tim SOC.

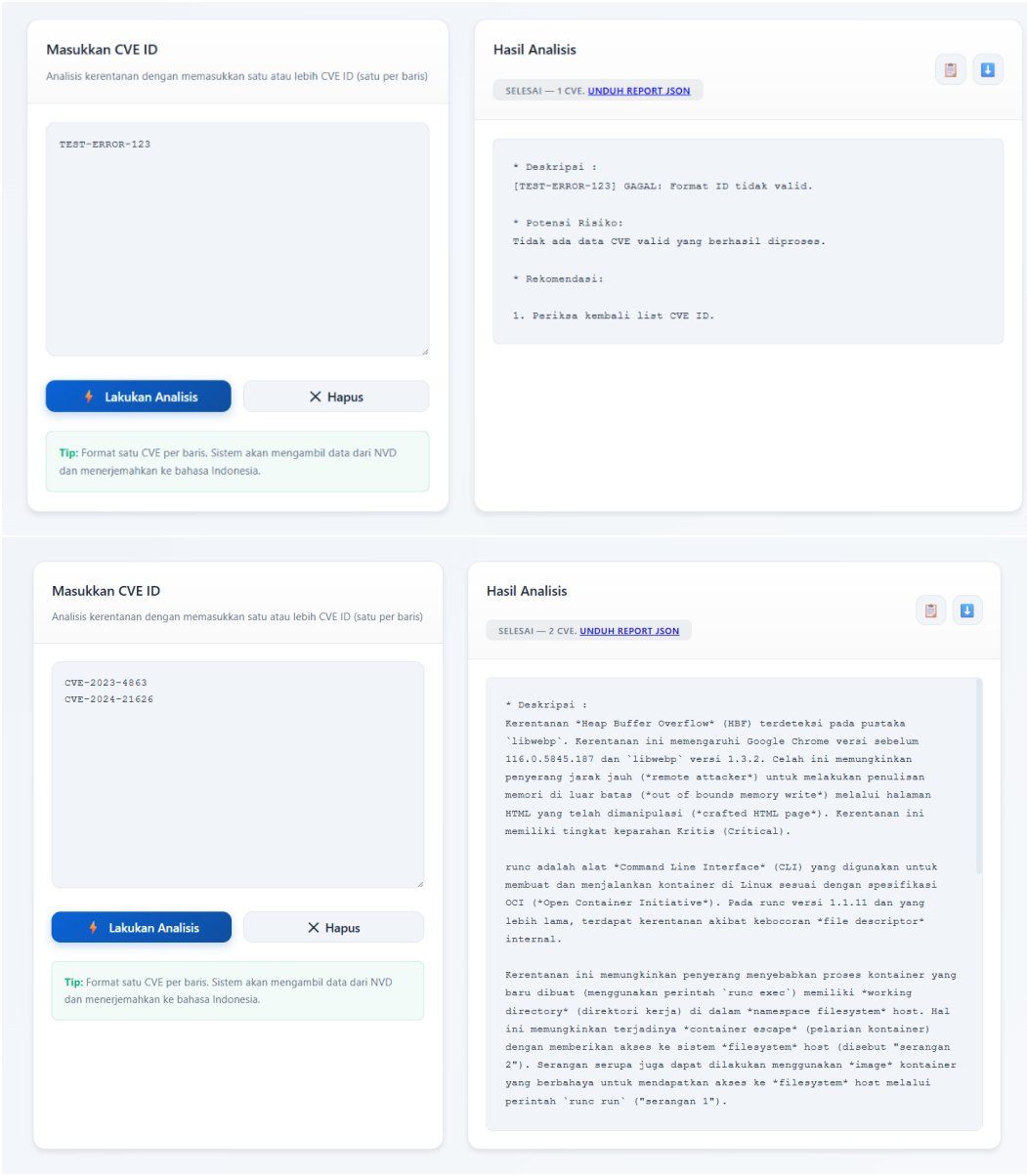
Demikian Surat Keterangan Magang dibuat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Tangerang Selatan, 22 Desember 2025

(**Camelia Fatimah**)
Human Resource


Masukkan CVE ID
Analisis kerentanan dengan memasukkan satu atau lebih CVE ID (satu per baris)
CVE-2023-4863
Lakukan Analisis
Hapus
Tip: Format satu CVE per baris. Sistem akan mengambil data dari NVD dan menerjemahkan ke bahasa Indonesia.
Hasil Analisis
SELESAI — 1 CVE. UNDUH REPORT JSON
* Deskripsi :
Kerentanan *Heap Buffer Overflow* ditemukan pada pustaka (library) `libwebp`. Cacat ini terdapat pada Google Chrome versi sebelum 116.0.5845.187 dan juga pustaka `libwebp` versi 1.3.2. Celah keamanan ini memungkinkan penyerang jarak jauh (*remote attacker*) untuk melakukan penulisan memori di luar batas (*out of bounds memory write*) melalui pemrosesan halaman HTML yang direkayasa (*crafted*) oleh penyerang. Kerentanan ini diklasifikasikan dengan tingkat keparahan kritis (*Critical*).
* Produk Terdampak :
- libwebp (versi 1.3.2 dan versi terdahulu yang mengandung bug ini)
- Google Chrome (versi sebelum 116.0.5845.187)
* Potensi Risiko:
Tingkat risiko kerentanan ini sangat tinggi (Kritis). Celah *Heap Buffer Overflow* yang memungkinkan penulisan memori di luar batas dapat dimanfaatkan oleh penyerang untuk merusak struktur data memori. Dampak terburuknya adalah potensi *Remote Code Execution* (RCE), di mana penyerang dapat menjalankan kode arbitrer dalam konteks korban (misalnya, di dalam *sandbox* browser), hanya dengan memancing korban mengunjungi halaman web berbahaya yang berisi gambar WebP yang direkayasa.

Masukkan CVE ID
Analisis kerentanan dengan memasukkan satu atau lebih CVE ID (satu per baris)
CVE-2099-99999
Lakukan Analisis
Hapus
Tip: Format satu CVE per baris. Sistem akan mengambil data dari NVD dan menerjemahkan ke bahasa Indonesia.
Hasil Analisis
SELESAI — 1 CVE. UNDUH REPORT JSON
* Deskripsi :
INFO: Data tidak ditemukan di NVD.
* Potensi Risiko:
Tidak ada data CVE valid yang berhasil diproses.
* Rekomendasi:
1. Periksa kembali list CVE ID.


Masukkan CVE ID
Analisis kerentanan dengan memasukkan satu atau lebih CVE ID (satu per baris)
TEST-ERROR-123
Lakukan Analisis
Hapus
Tip: Format satu CVE per baris. Sistem akan mengambil data dari NVD dan menerjemahkan ke bahasa Indonesia.
Hasil Analisis
SELESAI — 1 CVE. UNDUH REPORT JSON
* Deskripsi :
[TEST-ERROR-123] GAGAL: Format ID tidak valid.
* Potensi Risiko:
Tidak ada data CVE valid yang berhasil diproses.
* Rekomendasi:
1. Periksa kembali list CVE ID.
Masukkan CVE ID
Analisis kerentanan dengan memasukkan satu atau lebih CVE ID (satu per baris)
CVE-2023-4863
CVE-2024-21626
Lakukan Analisis
Hapus
Tip: Format satu CVE per baris. Sistem akan mengambil data dari NVD dan menerjemahkan ke bahasa Indonesia.
Hasil Analisis
SELESAI — 2 CVE. UNDUH REPORT JSON
* Deskripsi :
Kerentanan *Heap Buffer Overflow* (HBF) terdeteksi pada pustaka `libwebp`. Kerentanan ini memengaruhi Google Chrome versi sebelum 116.0.5845.187 dan `libwebp` versi 1.3.2. Celah ini memungkinkan penyerang jarak jauh (*remote attacker*) untuk melakukan penulisan memori di luar batas (*out of bounds memory write*) melalui halaman HTML yang telah dimanipulasi (*crafted HTML page*). Kerentanan ini memiliki tingkat keparahan Kritis (Critical).
runc adalah alat *Command Line Interface* (CLI) yang digunakan untuk membuat dan menjalankan kontainer di Linux sesuai dengan spesifikasi OCI (*Open Container Initiative*). Pada runc versi 1.1.11 dan yang lebih lama, terdapat kerentanan akibat kebocoran *file descriptor* internal.
Kerentanan ini memungkinkan penyerang menyebabkan proses kontainer yang baru dibuat (menggunakan perintah `runc exec`) memiliki *working directory* (direktori kerja) di dalam *namespace filesystem* host. Hal ini memungkinkan terjadinya *container escape* (pelarian kontainer) dengan memberikan akses ke sistem *filesystem* host (disebut "serangan 2"). Serangan serupa juga dapat dilakukan menggunakan *image* kontainer yang berbahaya untuk mendapatkan akses ke *filesystem* host melalui perintah `runc run` ("serangan 1").