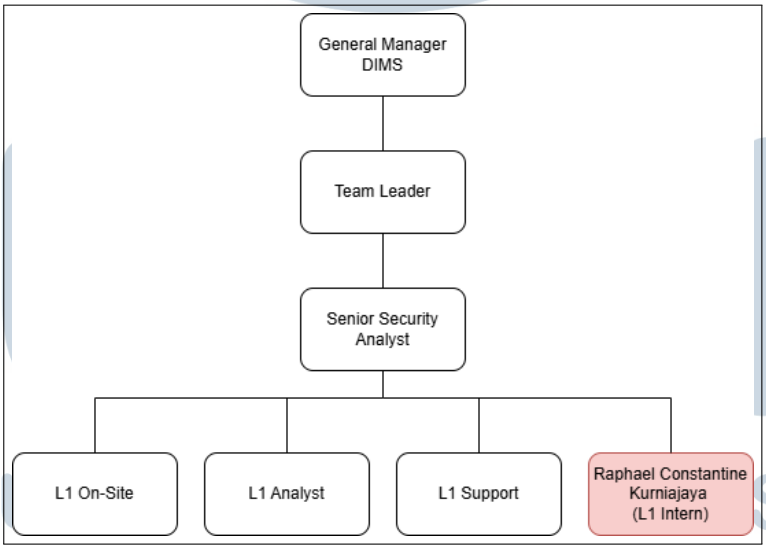
BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Kegiatan magang dilaksanakan pada unit operasional SOC di bawah pilar DIMS. Pilar ini bertanggung jawab atas layanan keamanan informasi yang mencakup aktivitas pemantauan, analisis, dan penanganan insiden siber untuk berbagai pelanggan dari sektor pemerintahan, militer, maupun swasta.

Posisi *Security Analyst Intern* ditempatkan langsung dalam tim operasional SOC, dengan tingkat koordinasi yang disetarakan dengan Level-1 (L1). Tugas utamanya meliputi validasi *alert*, korelasi log, investigasi awal *case*, serta penyusunan laporan yang dikomunikasikan kepada pelanggan. Aktivitas ini dilaksanakan sebagai bagian dari siklus kerja harian SOC di bawah supervisi berjenjang, yaitu Level-2 (L2) dan Level-3 (L3).

Struktur koordinasi internal dalam SOC dapat dilihat pada Gambar 3.1 berikut:



Gambar 3.1. Struktur koordinasi tim SOC *DIMS*
Sumber: Data Internal Pribadi [8]

Level-1 (L1) terdiri dari beberapa peran teknis utama, yaitu:

1. **L1 On-Site** — Analis yang ditempatkan di lokasi pelanggan secara fisik, bertanggung jawab atas pemantauan sistem dan komunikasi insiden di sisi pelanggan.

2. **L1 Analyst** — Fokus pada validasi, klarifikasi, investigasi, dan penutupan kasus insiden berdasarkan notifikasi dari perangkat keamanan.
3. **L1 Support** — Berperan dalam pengelolaan tiket permintaan non-insiden dari pelanggan, seperti request task, pelaporan, dan eskalasi administratif.
4. **L1 Intern** — Posisi magang yang menjalankan peran teknis setara L1 Analyst, dengan supervisi penuh dalam tugas analisis awal dan penyusunan laporan insiden.

Level-2 (L2) diisi oleh peran **Senior Security Analyst (SSA)**. SSA bertindak sebagai *threat hunter* yang bertanggung jawab atas analisis insiden tingkat lanjut, pengembangan *use case*, serta pemanfaatan *threat intelligence* untuk memahami konteks serangan. SSA juga menangani proses eskalasi pertama dari L1 dan melakukan komunikasi langsung dengan pelanggan dalam konteks insiden serta pelaporan bulanan.

Level-3 (L3) diisi oleh **Team Leader (TL)**. TL berperan sebagai *incident manager*, mengoordinasikan investigasi forensik, pengambilan keputusan dalam manajemen insiden, dan tindakan remediasi. TL juga mengatur rotasi *shift*, memantau kinerja tim, dan berkoordinasi dengan divisi lain maupun pelanggan terkait insiden kritikal.

Di atas TL, struktur dipimpin oleh **General Manager DIMS**, yang bertanggung jawab penuh atas keseluruhan operasional layanan keamanan terkelola. GM DIMS memastikan seluruh aktivitas SOC berjalan sesuai prosedur, target layanan tercapai, dan mendukung kebijakan strategis perusahaan dalam layanan keamanan informasi.

Koordinasi lintas tim juga melibatkan dua unit pendukung dari luar SOC, yaitu:

1. **System Administrator (Sysadmin)** — Bertanggung jawab atas stabilitas sistem SOC, termasuk integrasi log, troubleshooting perangkat, validasi sensor, serta pengelolaan sistem pendukung lainnya.
2. **Security Device Management (SDM)** — Menangani konfigurasi perangkat keamanan pelanggan, seperti *firewall tuning*, pemblokiran IP, serta *file blocking* berdasarkan *hash*. Permintaan ini dikelola melalui sistem tiket.

Struktur dan koordinasi ini memungkinkan proses penanganan insiden berjalan cepat, terstruktur, dan terdokumentasi dengan baik sesuai standar layanan keamanan informasi profesional.

3.2 Tugas yang Dilakukan

Selama pelaksanaan magang pada unit operasional SOC, tugas utama yang dijalankan berada dalam cakupan peran L1, yaitu bertanggung jawab terhadap proses monitoring dan analisis insiden siber berdasarkan *alert* yang dihasilkan oleh berbagai perangkat keamanan. Tujuan utama dari aktivitas ini adalah memastikan bahwa setiap potensi ancaman dapat dideteksi, dikonfirmasi, dan ditindaklanjuti secara tepat waktu, sehingga membantu pelanggan dalam menjaga ketersediaan dan integritas sistem informasinya.

Pada bulan pertama masa magang, dilakukan pelatihan intensif untuk membekali pemahaman dasar terkait konsep keamanan informasi. Materi pelatihan mengacu pada silabus *CompTIA Security+*, mencakup antara lain: konsep *threats, vulnerabilities, and attacks*, pengenalan perangkat keamanan yang digunakan oleh pelanggan Defenxor, serta pemahaman tentang prosedur *incident response*. Selain itu, pelatihan juga mencakup alur operasional SOC, struktur tim, serta pengenalan terhadap perangkat lunak dan perangkat keras yang digunakan dalam kegiatan operasional harian.

Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

Minggu Ke -	Pekerjaan yang dilakukan
1	Pemberitahuan Silabus mengenai keamanan informasi dan juga *Self-Learning* mengenai materi *CompTia Security+*. Mempersiapkan materi untuk mempresentasikan materi *CompTia Security+*.
2	Diskusi dan presentasi mengenai materi *CompTia Security+* yang sudah dipersiapkan.
3	Melanjutkan pembelajaran mengenai *CompTia Security+* dan juga mulai mempelajari perangkat yang akan digunakan di dalam SOC.
4	Latihan bersama SSA dan rekan *intern* lainnya untuk melakukan *case analysis* dan juga mempresentasikan hasilnya di depan SSA dan rekan *intern* lain.
5	Memulai *case analysis* kedua dan mulai *set-up* perangkat di dalam SOC.
	Lanjutan pada halaman berikutnya

Tabel 3.1 Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)

Minggu Ke -	Pekerjaan yang dilakukan
6	Operasional *night shift*. Memulai minggu pertama operasional di dalam SOC. Mendapatkan mayoritas *alarm* dan *case* mengenai *web attack/web scanning*. Melaksanakan *case analysis*, dan *system availability monitoring* di dalam SOC dan juga menanggapi permintaan dari pelanggan.
7	Operasional *mid shift*. Melaksanakan *case analysis*, *system availability monitoring*, serta penanganan *malware detection*.
8	Operasional *early shift*. Melaksanakan *case analysis* terkait *credential leaks* dan *web scanning* dan juga melakukan *system availability monitoring*.
9	Operasional *night shift*. Melaksanakan *case analysis*, *system availability monitoring*, serta melakukan notifikasi pada pelanggan mengenai *malware infection* dan *logon outside office hours*.
10	Operasional *mid shift*. Melaksanakan *case analysis* terkait *brute force* dan *web scanning* dan *system availability monitoring*.
11	Operasional *early shift*. Menangani *case* terkait *email attack* dan melaksanakan *system availability monitoring*.
12	Operasional *night shift*. Melaksanakan monitoring *case* dan *system availability* dan mulai membantu penyusunan *monthly report*. Mengirimkan notifikasi ke pelanggan terkait *credential leaks* dan melakukan eskalasi *Wazuh agent disconnect*.
13	Operasional *early shift*. Melaksanakan *case analysis* mengenai ATT&CK T1178: Addition of SID History to Active Directory Object, dan *system availability monitoring*.
14	Operasional *mid shift*. Melaksanakan *case analysis* terkait *web scanning*. Menangani permintaan pelanggan untuk penarikan *log*, dan pembuatan *daily report*.
15	Operasional *night shift*. Melaksanakan *case analysis*, *system availability monitoring*, dan melakukan eskalasi status *Wazuh agent disconnect*.

Lanjutan pada halaman berikutnya

Tabel 3.1 Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)

Minggu Ke -	Pekerjaan yang dilakukan
16	Operasional *early shift*. Melakukan *case analysis* untuk case *web scanning, malware infection*, dan *email attack* dan melakukan *system availability monitoring*. Melanjutkan pembuatan *monthly report*.

Dalam operasionalnya, proses *monitoring* dilakukan secara real-time melalui beberapa perangkat keamanan *(appliance)* yang terintegrasi dalam infrastruktur pelanggan. Analyst memantau status notifikasi melalui *dashboard PWA*, serta perangkat keamanan lain yang diintegrasikan ke dalam Kibana untuk mendeteksi aktivitas mencurigakan atau anomali pada jaringan dan endpoint pelanggan.

Ketika sebuah *alert* muncul, L1 melakukan analisis terhadap *log* yang tersedia. Analisis ini bertujuan untuk menentukan validitas dari insiden, memahami vektor serangan, serta mengevaluasi tingkat dampaknya. Prioritas *alert* dikelompokkan ke dalam tiga level: **Low**, **Medium**, dan **High**. Penentuan prioritas didasarkan pada faktor seperti jenis ancaman, cakupan sistem yang terdampak, serta kemungkinan eksfiltrasi atau kerusakan yang dapat ditimbulkan.

Kemunculan *alert* umumnya berasal dari deteksi perilaku anomali, komunikasi tidak sah, *malware signature*, atau aktivitas eksploitasi. Dampak potensial dari insiden tersebut antara lain akses tidak sah ke sistem, penyebaran *malware*, kebocoran data, maupun gangguan terhadap layanan digital pelanggan.

Hasil akhir dari proses analisis insiden adalah pembuatan sebuah notifikasi yang dikirimkan kepada pelanggan. Notifikasi ini disusun melalui sistem *Case Management*, berisi informasi kronologis insiden, ringkasan analisis, dan rekomendasi tindakan yang dapat diambil oleh pelanggan. Terdapat tiga jenis notifikasi yang digunakan dalam operasional SOC:

1. **Konfirmasi** — Digunakan dalam kasus *request for validation*, yaitu ketika dibutuhkan klarifikasi tambahan dari pihak pelanggan terhadap aktivitas tertentu, misalnya aktivitas *login RDP* di luar jam kerja yang perlu dikonfirmasi sebagai aktivitas sah/tidak sah.

2. **Eskalasi** — Digunakan ketika ditemukan anomali atau potensi insiden yang melibatkan sisi pelanggan, seperti pemutusan koneksi *Wazuh agent* atau

sensor yang mati. Eskalasi dilakukan agar pelanggan dapat melakukan tindakan segera.

3. **Pemberitahuan Serangan** — Digunakan jika sebuah insiden dikonfirmasi valid sebagai bentuk serangan yang berpotensi mengancam sistem, seperti *malware infection*, *brute force attack*, atau *web attack*. Notifikasi ini mencakup analisis lengkap serta rekomendasi teknis mitigasi.

Tugas-tugas tersebut dilaksanakan secara kolaboratif bersama tim SOC, dengan supervisi dari L2 dan L3, serta koordinasi aktif dengan tim teknis lain seperti Sysadmin dan SDM jika dibutuhkan tindakan teknis lebih lanjut.

3.3 Uraian Pelaksanaan Magang

Bagian ini menguraikan secara teknis pelaksanaan kegiatan magang yang difokuskan pada kegiatan monitoring, analisis, serta eskalasi insiden keamanan informasi dalam lingkup operasional SOC. Penjabaran dilakukan melalui beberapa aspek penting yang mencerminkan proses kerja dan sistem pendukung yang digunakan selama masa magang.

3.3.1 Perangkat Lunak yang Digunakan

SOC Defenxor menggunakan berbagai sistem dan perangkat lunak untuk menunjang kegiatan operasionalnya, yang secara umum terbagi menjadi:

a) Sistem pemantauan dan analisis log: Wazuh, DSIEM, Kibana, Moloch, dan Thruk, yang digunakan untuk *log management, endpoint monitoring*, serta sistem deteksi anomali dan pemantauan ketersediaan layanan (*service availability*).

b) Security devices: perangkat keamanan seperti *firewall*, IDS/IPS, WAF, *email security gateway* (Proofpoint, Cisco Ironport), EDR (Crowdstrike), serta pengelolaan jaringan dan perangkat melalui SD-WAN Fortinet dan Forescout.

c) *Threat intelligence tools*: digunakan untuk melakukan verifikasi, enrichment, dan validasi terhadap indikator ancaman, seperti VirusTotal, AbuseIPDB, APIVoid, MXToolbox, Kaspersky OpenTIP, AlienVault OTX, dan ThreatBook CTI.

d) Tools manajemen operasional: SOC Playbook dan Case Management System yang digunakan untuk dokumentasi, triase insiden, serta pengelolaan siklus respons.

e) Kanal komunikasi: terdiri dari media internal dan eksternal yang digunakan untuk koordinasi operasional, yaitu WhatsApp, Signal, Lark, dan e-mail.

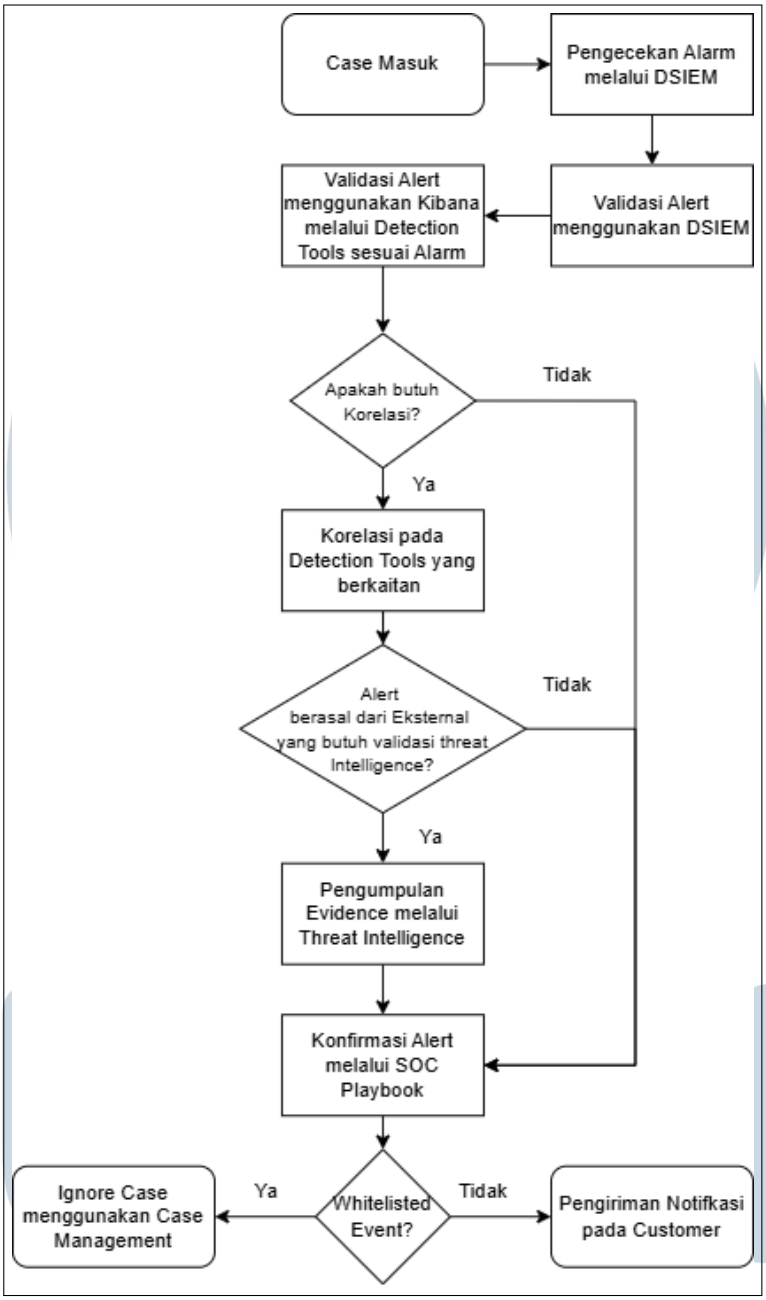
3.3.2 Perangkat Keras yang Digunakan

Kegiatan operasional SOC juga ditunjang oleh perangkat keras yang tersedia secara lokal di SOC, termasuk penggunaan *workstation* tipe **Lenovo ThinkCentre M720q** yang dilengkapi prosesor **Intel Core i5-14500T**, memori **32 GB RAM**, serta penyimpanan internal **512 GB SSD**. Spesifikasi ini dirancang untuk mendukung kebutuhan multitasking intensif selama proses analisis insiden dan pemantauan log. Selain itu, tersedia juga *monitoring display* berupa **TV Wall** yang digunakan untuk menampilkan status layanan dan sistem pelanggan secara real-time. Infrastruktur jaringan internal perusahaan telah tersegmentasi dan dienkripsi guna memastikan keamanan data selama proses analisis berjalan.

3.3.3 Alur Analisis Case

Sebagai bagian dari tim operasional, peran L1 Analyst difokuskan pada proses analisis awal terhadap setiap *Case* yang muncul dari sistem keamanan pelanggan. Setiap *Case* yang terpicu akan melalui serangkaian tahapan: validasi, investigasi, konfirmasi, dan notifikasi.

Analisis dilakukan dengan mengacu pada perangkat yang telah terintegrasi, kemudian dianalisis lebih lanjut menggunakan sumber *Detection Tools* dan *Threat Intelligence* untuk validasi ancaman.



Gambar 3.2. Alur proses analisis *Case*

Sumber: Data Internal Pribadi [8]

Flowchart di atas menggambarkan alur proses analisis insiden pada operasional SOC Defenxor, khususnya pada peran L1 *Analyst*. Alur ini terdiri dari beberapa tahap utama:

1. *Case* masuk ke sistem sebagai hasil dari *alarm* yang terpicu oleh *rule* pada DSIEM. Setiap *alarm* akan dinaikkan statusnya menjadi *case* melalui *Case Collector*.

2. Dilakukan pengecekan awal terhadap alarm menggunakan platform DSIEM untuk memperoleh informasi dasar, seperti jenis alarm, perangkat pemicu, serta waktu dan sumber kejadian.

3. Validasi lanjutan terhadap *alert* dilakukan dengan menelusuri informasi *log* pada *Kibana*, berdasarkan perangkat *detection tools* yang tercantum pada *alarm*. Sebagai contoh, apabila *alarm* berasal dari Wazuh atau EDR, maka data yang dihasilkan oleh perangkat tersebut akan ditelusuri untuk memperoleh informasi yang diperlukan. Sementara itu, apabila *alarm* berasal dari perangkat NIDS, maka *log* dari *Suricata* akan diperiksa secara mendetail. Selain itu, dilakukan juga analisis korelasi waktu guna membangun konteks yang utuh terhadap *case* yang ditangani.

4. Setelah mendapatkan informasi tersebut, dilakukan penilaian terhadap kebutuhan proses korelasi, Misal, seperti adanya aktivitas berulang atau membutuhkan pengecekan apakah aktivitas tersebut diijinkan oleh perangkat lain. Jika tidak terdapat indikasi korelatif, maka *alert* dapat langsung dikonfirmasi melalui *SOC Playbook*.

5. Jika korelasi diperlukan, dilakukan pencarian informasi yang berkaitan pada *detection tools* lainnya. Informasi yang dikumpulkan dapat berupa *hostname*, *username*, nama proses, dan keterkaitan antar *event*. Korelasi ini penting untuk memperkuat validitas *alert* dan mencegah kesalahan notifikasi.

6. Selanjutnya, ditentukan apakah *alert* berasal dari eksternal dan membutuhkan validasi tambahan melalui sumber *threat intelligence*. Hal ini umum terjadi jika perangkat *customer* mendeteksi adanya perangkat yang mengakses alamat IP asing, file mencurigakan, atau URL yang belum dikenal. Jika tidak dibutuhkan, maka analisis langsung berlanjut ke konfirmasi melalui *SOC Playbook*.

7. Jika ya, maka dilakukan pengumpulan bukti atau *evidence* tambahan dari layanan *threat intelligence* publik seperti VirusTotal, AbuseIPDB, atau ThreatBook. Proses ini dilakukan untuk memverifikasi reputasi *file hash*, alamat IP, domain, atau URL yang terlibat dalam insiden.

8. Setelah bukti teknis terkumpul dan dianalisis, dilakukan konfirmasi terhadap *alert* menggunakan referensi yang tercantum dalam *SOC Playbook*. Playbook

menyediakan panduan analisis berdasarkan jenis insiden dan prosedur komunikasi yang telah disepakati dengan pelanggan.

9. Tahap akhir adalah pengecekan terhadap *whitelisted event*. Jika aktivitas tersebut telah dinyatakan aman dan tercatat dalam daftar *whitelist*, maka *case* akan ditutup dengan status *"ignored-by-soc"* pada sistem *Case Management*.

10. Namun, jika *event* tidak termasuk dalam daftar whitelist dan valid sebagai insiden, maka notifikasi akan disusun dan dikirimkan kepada pelanggan. Notifikasi ini memuat ringkasan insiden, hasil analisis, serta rekomendasi teknis atau tindakan mitigasi yang dapat diambil oleh pihak pelanggan.

Alur ini dirancang untuk meminimalkan false positive, meningkatkan efektivitas deteksi, serta memastikan bahwa setiap insiden ditangani secara cepat dan terstandarisasi. Jika ditemukan kesulitan teknis atau eskalasi lebih lanjut diperlukan, alur akan mengikuti jalur **escalation matrix** dengan urutan: **L1** $\rightarrow$ **L2 (SSA)** $\rightarrow$ **L3 (Team Leader)** $\rightarrow$ **General Manager**.

3.3.4 Pemantauan System Availability

Selain bertanggung jawab terhadap insiden keamanan, L1 analyst juga melakukan pemantauan terhadap ketersediaan sistem pelanggan menggunakan *Dashboard Grafana* dan *Thruk*. Aktivitas ini bertujuan untuk memastikan bahwa seluruh perangkat dan layanan keamanan pelanggan berjalan sebagaimana mestinya dalam mendukung deteksi dini dan respons insiden secara efektif.

Parameter yang diawasi mencakup:

1. Status konektivitas perangkat keamanan (seperti *firewall*, *endpoint*, dan sensor lainnya)
2. *Service uptime* dari aplikasi dan layanan utama milik pelanggan.
3. *Status Wazuh agent* yang terpasang pada endpoint pelanggan.
4. Ketersediaan *Defenxor Security Appliance* (DSA).
5. Gangguan akses atau kegagalan integrasi log dari sistem eksternal.

Setiap perubahan status akan dianalisis berdasarkan jenis dan tingkat urgensinya, serta ditangani sesuai alur eskalasi berikut:

1. *Device unreachable*, *service down*, dan *sensor offline* akan terlebih dahulu ditangani oleh tim Sysadmin atau SSA. Jika ditemukan bahwa gangguan berasal dari sisi pelanggan, maka akan dilakukan notifikasi dan eskalasi ke pihak pelanggan.
2. *Wazuh agent disconnected* akan langsung dieskalasikan ke pelanggan karena berdampak langsung terhadap pengiriman log dan visibilitas endpoint.
3. *DSA unreachable* akan langsung dieskalasikan ke pelanggan karena DSA merupakan perangkat kritikal yang dipasang di sisi pelanggan dan tidak dapat dikendalikan langsung oleh tim internal.

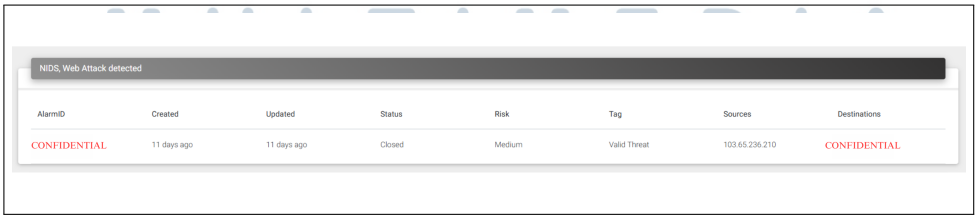
Prosedur pemantauan ini mendukung ketahanan layanan secara menyeluruh dan memastikan bahwa sistem pelanggan tetap aktif, aman, serta dapat direspons secara cepat apabila terjadi anomali atau gangguan.

3.4 Case Analysis

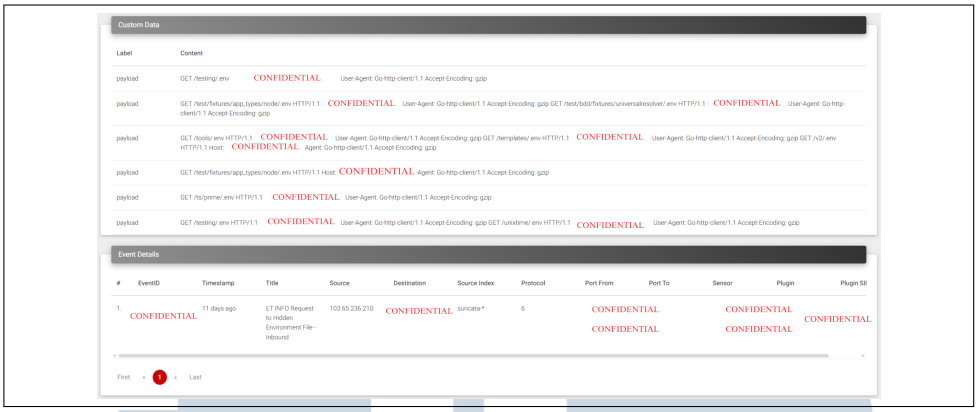
Pada bagian ini diuraikan proses analisis terhadap salah satu insiden serangan web yang terdeteksi oleh *Network Intrusion Detection System* (NIDS). Kasus ini dipilih karena mencerminkan alur kerja L1 *Analyst* secara menyeluruh, mulai dari deteksi awal, validasi teknis, korelasi lintas perangkat, hingga konfirmasi melalui sumber *threat intelligence*.

3.4.1 Latar Belakang Kasus

Pada tanggal 7 Juni 2025 pukul 04:33:14 (Asia/Jakarta), SOC menerima sebuah *case* dengan judul *NIDS, Web Attack Detected* yang berasal dari *alarm* yang terpicu pada DSIEM. *Alarm* ini menunjukkan adanya upaya scanning terhadap file `.env` pada berbagai direktori umum milik pelanggan, yang sering kali berisi parameter sensitif seperti kredensial basis data, *API key*, serta *secret tokens*.



Gambar 3.3. *Alarm* yang diterima pada DSIEM *Case* (bagian 1)
Sumber: Data Internal Pribadi [8]



Gambar 3.4. *Alarm* yang diterima pada DSIEM *Case* (bagian 2)

Sumber: Data Internal Pribadi [8]

3.4.2 Proses Analisis dan Investigasi

Proses investigasi dilakukan sesuai dengan alur analisis insiden yang berlaku di SOC.

A Pengecekan Awal pada DSIEM

Informasi awal diperoleh dari tampilan DSIEM (Gambar 3.3 dan Gambar 3.4). Ringkasan informasi:

1. **Alarm Name**: *NIDS, Web Attack Detected*
2. **Source IP**: 103.65.236.210 (Indonesia)
3. **Risk Level**: Medium
4. **Tag**: Valid Threat
5. **Payload**: Serangkaian permintaan GET untuk file `.env` di berbagai path, contoh:
   (a) GET /testing/.env
   (b) GET /unixtime/.env
   (c) GET /theme/.env

B Validasi pada Log Suricata

Pemeriksaan lanjutan dilakukan melalui Kibana terhadap perangkat NIDS Suricata. Signature **ET SCAN Request to Hidden Environment File - .Env** terdeteksi, yang mengindikasikan proses *automated scanning* oleh pelaku terhadap file konfigurasi `.env`. Signature ini merupakan bagian dari *Emerging Threats (ET)* dan dirancang untuk mengidentifikasi aktivitas probing yang secara spesifik menargetkan kelemahan umum pada sistem web berbasis file environment.

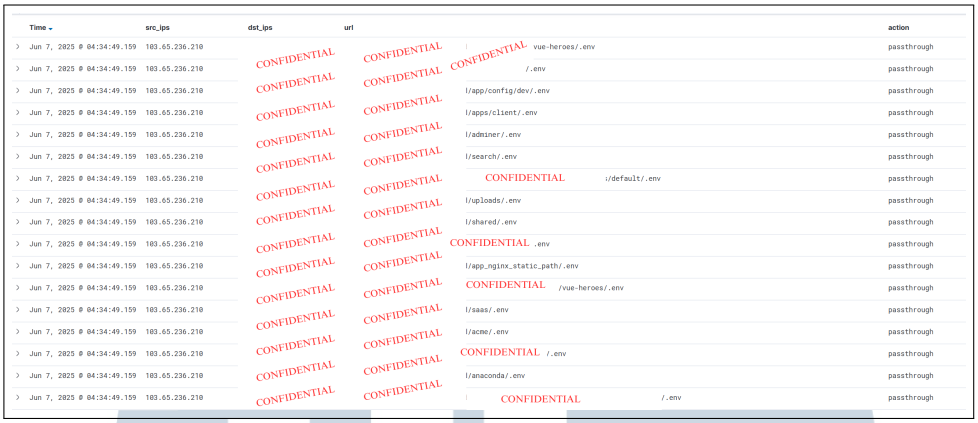
Gambar 3.5. Validasi signature pada perangkat NIDS Suricata
Sumber: Data Internal Pribadi [8]

Log yang terpantau menunjukkan bahwa serangkaian permintaan HTTP seperti `GET /app/.env`, `GET /auth/.env`, dan `GET /assets/.env` mendapatkan *action* berupa **allow** dari Suricata, yang berarti lalu lintas tidak diblokir namun tetap dicatat sebagai aktivitas mencurigakan untuk analisis lebih lanjut.

C Korelasi dengan Perangkat Keamanan Lain

1. **Fortigate**

   Berdasarkan log Fortigate (Gambar 3.6), terlihat bahwa traffic dari IP `103.65.236.210` diberi status *passthrough*. Ini berarti koneksi diteruskan menuju perangkat WAF untuk dianalisis lebih lanjut.



Time	src_ips	dst_ips	url	action
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL vue-heroes/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/app/config/dev/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/apps/client/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/adminer/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/search/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL :/default/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/uploads/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/shared/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL .env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/app_nginx_static_path/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL /vue-heroes/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/saas/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/acme/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL /.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	l/anaconda/.env	passthrough
Jun 7, 2025 @ 04:34:49.159	103.65.236.210	CONFIDENTIAL	CONFIDENTIAL /.env	passthrough

Gambar 3.6. Log lalu lintas pada perangkat Fortigate
Sumber: Data Internal Pribadi [8]

Log menunjukkan bahwa lalu lintas HTTP dari IP penyerang tidak diblokir oleh Fortigate dan diteruskan ke layer aplikasi. Hal ini sesuai dengan fungsi Fortigate sebagai firewall perimeter yang mengizinkan traffic HTTP/HTTPS masuk sebelum dianalisis lebih lanjut oleh sistem WAF.

2. **WAF F5-ASM**

   Berdasarkan data dari perangkat WAF (Gambar 3.7), seluruh permintaan GET yang diarahkan ke file `.env` menerima kode respons HTTP `404 Not Found`, yang mengindikasikan file tidak ditemukan pada target direktori. Meskipun status aksi adalah *passed*, hasil validasi membuktikan bahwa tidak ada informasi sensitif yang terekspos.

Time	src_ips	dst_ips	event_name	requestMethod	request	response_code	action
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.docker/.env	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/assets/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env.production	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env.local	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env.old	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env.backup	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	404	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210	CONFIDENTIAL	Successful Request	GET	/.env	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	CONFIDENTIAL /.env	0	passed
Jun 7, 2025 @ 04:32:09.000	103.65.236.210		Successful Request	GET	/.env	404	passed

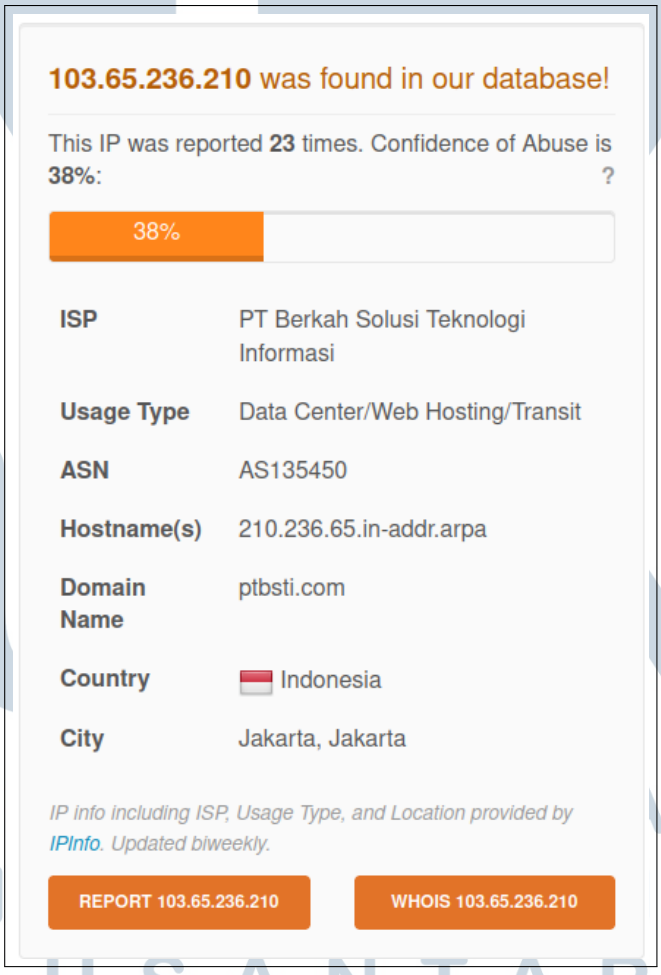
Gambar 3.7. Hasil inspeksi dari WAF F5-ASM
Sumber: Data Internal Pribadi [8]

Berdasarkan log WAF, setiap request seperti `GET /app/.env`, `GET /auth/.env`, dan `GET /assets/.env` mendapatkan respons 404,

menandakan bahwa file yang diminta tidak tersedia. Hal ini menjadi indikasi bahwa tidak terdapat file sensitif yang terekspos secara publik pada direktori web pelanggan.

D Validasi dengan *Threat Intelligence*

IP **103.65.236.210** divalidasi menggunakan sumber *threat intelligence* AbuseIPDB. Hasil pengecekan menunjukkan reputasi berisiko dengan *Confidence of Abuse* sebesar 38% dan dilaporkan sebanyak 23 kali. Hal ini memperkuat dugaan bahwa aktivitas yang dilakukan merupakan bagian dari *scanning* otomatis oleh pelaku atau *botnet*.



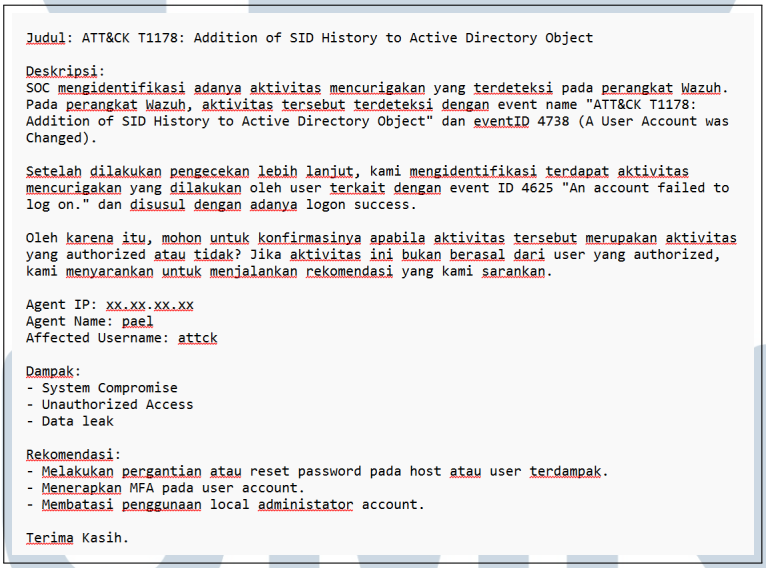
Gambar 3.8. Reputasi IP 103.65.236.210 pada AbuseIPDB

Sumber: Data Internal Pribadi [8]

Tampilan AbuseIPDB pada Gambar 3.8 menunjukkan identitas jaringan dari IP sumber, termasuk lokasi geografis, ASN, dan klasifikasi laporan oleh pengguna lain. Selain itu, platform ini menyajikan histori waktu pelaporan dan kategori aktivitas yang mendasari penilaian reputasi. Informasi tersebut membantu *analyst* dalam mengevaluasi konteks serangan secara eksternal, serta memperkuat justifikasi saat menyusun notifikasi insiden kepada pelanggan.

3.4.3 Notifikasi kepada Pelanggan

Setelah analisis dinyatakan valid dan tidak terdapat tanda-tanda pelanggaran lanjutan, notifikasi dikirimkan kepada pelanggan. Notifikasi mencakup ringkasan insiden, kronologi, hasil analisis perangkat keamanan, serta rekomendasi tindakan lanjutan.



Judul: ATT&CK T1178: Addition of SID History to Active Directory Object

Deskripsi:
SOC mengidentifikasi adanya aktivitas mencurigakan yang terdeteksi pada perangkat Wazuh. Pada perangkat Wazuh, aktivitas tersebut terdeteksi dengan event name "ATT&CK T1178: Addition of SID History to Active Directory Object" dan eventID 4738 (A User Account was Changed).

Setelah dilakukan pengecekan lebih lanjut, kami mengidentifikasi terdapat aktivitas mencurigakan yang dilakukan oleh user terkait dengan event ID 4625 "An account failed to log on." dan disusul dengan adanya logon success.

Oleh karena itu, mohon untuk konfirmasinya apabila aktivitas tersebut merupakan aktivitas yang authorized atau tidak? Jika aktivitas ini bukan berasal dari user yang authorized, kami menyarankan untuk menjalankan rekomendasi yang kami sarankan.

Agent IP: xx.xx.xx.xx
Agent Name: pael
Affected Username: attck

Dampak:
- System Compromise
- Unauthorized Access
- Data leak

Rekomendasi:
- Melakukan pergantian atau reset password pada host atau user terdampak.
- Menerapkan MFA pada user account.
- Membatasi penggunaan local administator account.

Terima Kasih.

Gambar 3.9. Contoh notifikasi yang dikirimkan kepada pelanggan

Sumber: Data Internal Pribadi [8]

Gambar 3.9 memperlihatkan format notifikasi standar yang digunakan dalam lingkungan operasional SOC. Setiap elemen dalam notifikasi disusun secara sistematis, mencakup identifikasi kasus, atribut teknis (*source IP, alarm ID, risk level*), deskripsi aktivitas, serta dampak dan rekomendasi. Penyusunan ini mengacu pada template internal dan bertujuan untuk memastikan pelanggan memperoleh informasi yang relevan, mudah dipahami, dan siap ditindaklanjuti.

3.4.4 Temuan

1. *Alert* dikategorikan sebagai **True Positive**.
2. Serangan termasuk dalam kategori *web vulnerability scanning*.
3. IP penyerang memiliki riwayat aktivitas mencurigakan dan reputasi buruk.

3.4.5 Rekomendasi dan Tindak Lanjut

Berikut adalah rekomendasi yang disampaikan kepada pelanggan:

1. Memastikan service yang terdapat pada target host sudah di *hardening*.
2. Melakukan *review* dan *fine tuning* Firewall.
3. *Temporary blocking IP address attacker* jika diperlukan, untuk menghindari aktivitas *web scanning/attack* lanjutan.

3.5 Kendala dan Solusi yang Ditemukan

Bagian ini membahas berbagai kendala yang dihadapi selama pelaksanaan program magang, baik dari sisi teknis, operasional, maupun komunikasi dalam lingkungan kerja SOC. Setiap tantangan yang muncul menjadi bagian dari proses pembelajaran untuk memahami kompleksitas peran sebagai *Security Analyst Intern*. Selain itu, dijelaskan pula sejumlah solusi yang diterapkan untuk mengatasi kendala tersebut, termasuk strategi adaptasi, kolaborasi tim, dan peningkatan kapasitas individu selama proses magang berlangsung.

3.5.1 Kendala

Pada pelaksanaan kegiatan magang di lingkungan operasional SOC, ditemukan sejumlah tantangan yang memengaruhi efektivitas dalam menjalankan tugas sebagai *Security Analyst Intern*. Kendala-kendala tersebut muncul baik dari sisi teknis, komunikasi, maupun adaptasi terhadap sistem kerja yang kompleks dan dinamis. Berikut merupakan beberapa permasalahan utama yang dihadapi selama masa magang:

1. Kurangnya latar belakang teknis dan pemahaman dasar mengenai konsep-konsep *cybersecurity* pada awal masa magang, yang menyebabkan adaptasi terhadap alur kerja SOC menjadi agak sulit.
2. Keterbatasan komunikasi antar L1 selama *shift*, sehingga terkadang menghambat koordinasi dan komunikasi secara efektif.
3. Ditemukannya beberapa *case* baru yang belum memiliki riwayat penanganan sebelumnya, sehingga diperlukan analisis lanjutan dan diskusi teknis dengan L1 lain maupun *Level-2 (L2)* untuk validasi dan klasifikasi insiden.
4. Permintaan klarifikasi dari pelanggan terhadap *case* yang telah dinotifikasi, terutama ketika pelanggan tidak memiliki latar belakang teknis yang kuat, sehingga dibutuhkan komunikasi yang lebih kontekstual dan mudah dipahami.

3.5.2 Solusi

Sebagai bentuk respons terhadap kendala yang ditemui, dilakukan berbagai upaya penyesuaian dan perbaikan guna meningkatkan kinerja serta kemampuan analisis selama kegiatan magang. Solusi-solusi berikut dirancang untuk mendukung proses pembelajaran, memperkuat koordinasi, serta mengoptimalkan proses analisis insiden dalam lingkungan SOC:

1. Melakukan pembelajaran mandiri secara aktif melalui kanal daring, *training* internal, dan diskusi dengan analis senior untuk mempercepat pemahaman mengenai topik-topik penting dalam SOC.
2. Meningkatkan intensitas komunikasi antar-analis melalui diskusi informal maupun formal, serta mencatat temuan penting dalam dokumentasi harian untuk mempermudah kolaborasi lintas shift.
3. Berkoordinasi dengan rekan satu shift dalam menghadapi kasus baru, serta menggunakan referensi dari *SOC Playbook* dan hasil investigasi sebelumnya sebagai acuan dalam proses analisis, dan melakukan eskalasi pada L2 jika diperlukan,
4. Menyusun notifikasi insiden dengan penjelasan tambahan dalam bahasa yang lebih umum dan disertai dengan rekomendasi, agar lebih mudah dipahami oleh pihak pelanggan tanpa latar belakang teknis mendalam.