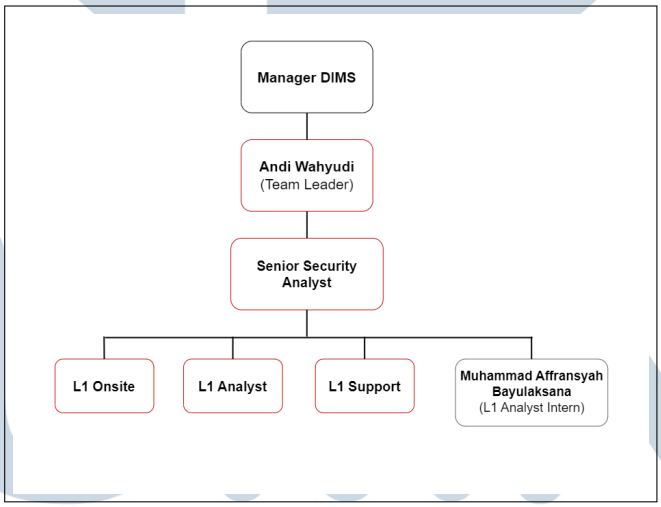
BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Dalam pelaksanaan magang di Defenxor, kedudukan setara dengan L1 Security Analyst yang bekerja *fulltime*. Tanggung jawab yang dimiliki adalah menjadi *L1 Security Analyst* yang membantu operasional SOC dalam melakukan *security monitoring* dan *incident handling*. Rangkaian magang dipandu oleh *buddy*, yang menjabat sebagai *senior security analyst*, dalam kesehariannya. Selain *buddy*, *analyst* lain yang berada dalam *shift* yang sama juga membantu agar dapat menyesuaikan dan mengoptimalkan operasional SOC. Selain *analyst*, tim juga terdiri dari SDM dan *sysadmin*. Keseluruhan tim ini disebut DIMS, Defenxor Intelligence Managed Security, yang dipimpin oleh Andi Wahyudi. Gambar 3.1 adalah struktur dari DIMS secara detail yang berfokus ke *analyst*.



Gambar 3.1. Struktur DIMS
Sumber: Data Internal Pribadi [10]

Kedudukan dari intern dapat dilihat dari struktur di gambar 3.1. Kedudukan teratas pada DIMS adalah *Manager* DIMS, bertanggung jawab untuk memimpin berjalannya SOC dalam operasional secara keseluruhan. Di bawahnya, *team leader* menjadi pemimpin yang aktif dalam keseharian operasional untuk memastikan bahwa *security monitoring* berjalan dengan baik. Untuk membagi tanggung jawab ke setiap kliennya, *senior security analyst* ditugaskan untuk menjadi penghubung antara Defenxor dan klien, serta bertanggung jawab untuk *standby* menangani

apabila terdapat eskalasi. Terdapat juga *senior security analyst* yang ditugaskan sebagai *buddy* untuk membimbing intern dalam kesehariannya. Dalam operasional SOC, posisi terbagi menjadi tiga, yaitu L1 *onsite* yang menangani SOC langsung *on-premise* di klien, L1 *analyst* yang melakukan *monitoring* dari Defenxor, dan L1 *support* yang menjadi perantara komunikasi dari tim SOC dan klien.

Dalam koordinasi tim, alur bermula dari tim yang sedang melakukan *security monitoring*. *Analyst* yang memiliki *shift* yang sama bekerja bersama dalam *monitoring* dan berdiskusi jika ada kendala dalam masing-masing analisisnya. Jika terdapat kebutuhan sistem internal atau kendala dari sistem, *analyst* perlu menghubungi *sysadmin*. Jika ada kebutuhan tindak lanjut respon kepada sistem klien, *analyst* perlu menghubungi SDM. Dalam menganalisis, apabila tim dalam ruangan operasi tidak dapat menyelesaikan, melakukan eskalasi ke L2, yaitu *senior security analyst*. Jika *case* masih tidak dapat diselesaikan, berlanjut ke L3, yaitu *team leader*, dan terakhir menuju *manager* DIMS.

3.2 Tugas yang Dilakukan

Pelaksanaan program magang melibatkan serangkaian tanggung jawab dalam aktivitas *security monitoring* dan *incident handling* terhadap sistem milik klien yang berada dalam pengawasan operasional SOC Defenxor. Aktivitas ini bertujuan untuk menjaga keamanan sistem informasi dari potensi ancaman atau serangan.

Sebelum terlibat secara langsung dalam operasional SOC, tahap awal dimulai dengan pelatihan internal yang membahas konsep dasar keamanan informasi, alur kerja operasional, serta penggunaan perangkat dan sistem *monitoring* yang digunakan. Pelatihan ini menjadi langkah persiapan untuk memastikan pemahaman terhadap standar kerja yang berlaku di lingkungan SOC.

Setelah tahap pelatihan, tanggung jawab operasional difokuskan pada kegiatan *security monitoring*, yaitu *monitoring* sistem klien secara *real time* melalui *appliance system* yang menampilkan *data log* dan *alert* dari berbagai sumber yang diaplikasikan pada sistem. *Monitoring* dilakukan untuk mendeteksi aktivitas mencurigakan atau anomali yang mengindikasikan potensi insiden keamanan.

Setiap *alert* yang muncul menjadi prioritas untuk dianalisis. Proses *incident handling* dimulai dengan mengenali jenis dan penyebab munculnya *alert*, serta dampak yang mungkin ditimbulkan terhadap sistem. Hasil dari analisis ini kemudian dituangkan dalam bentuk notifikasi insiden yang dikirimkan kepada

pihak klien sebagai bentuk pelaporan dan koordinasi.

Notifikasi berisi informasi mengenai insiden yang terdeteksi, sistem yang terdampak, serta saran tindakan mitigasi. Dalam beberapa situasi, permintaan konfirmasi juga disertakan untuk memastikan apakah aktivitas yang terpantau merupakan tindakan yang sah (*authorized*) atau tidak.

Seluruh aktivitas tersebut dilaksanakan di dalam ruangan SOC, yaitu ruang kerja terkontrol dengan akses terbatas. Ruangan ini dirancang untuk mendukung *monitoring* sistem secara 24/7 dan menerapkan ketentuan pengamanan yang mengacu pada standar ISO27001, seperti larangan penggunaan perangkat pribadi, pengawasan aktivitas kerja, dan pengaturan hak akses personel. Tabel 3.1 adalah pekerjaan yang dilakukan setiap minggunya selama pelaksanaan kerja magang berlangsung.

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

Minggu Ke -	Pekerjaan yang dilakukan
1	Onboarding dan self-learning materi Security+
2	Diskusi dan pembahasan materi Security+
3	Mempelajari sistem yang digunakan saat operasional SOC
4	*Training case analysis*
5	Review semua yang telah dipelajari dan *setup user* untuk operasional di ruangan SOC
6	Menjalankan operasional *night shift*. Menemukan alert dari alarm yang berhubungan dengan akses pada administrative port di luar jam kerja pada sistem klien. Rule dari alert ini muncul untuk pertama kalinya, sehingga dibuat draft notifikasi terkait case dengan *template* baru.
	Lanjut pada halaman berikutnya

UNIVERSITAS MULTIMEDIA NUSANTARA

Tabel 3.2. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)

Minggu Ke -	Pekerjaan yang dilakukan
7	Menjalankan operasional *night shift*. Pada week ini, terjadi initial incident, di mana terdapat powershell activity dengan upaya pengunduhan dan eksekusi skrip mencurigakan menggunakan CMD dan PowerShell untuk mengakses file php dan ps1 melalui protokol HTTP.
8	Menjalankan operasional *mid shift*. Menemukan adanya aktivitas yang mengindikasikan proses instalasi menggunakan *Alternate Data Stream* untuk menyembunyikan data di dalam sebuah file.
9	Menjalankan operasional *early shift*. Shift dijalankan pada hari libur Idul Fitri. Pada pekan ini, terdapat catatan dari klien bahwa tidak boleh ada penggantian konfigurasi pada sistem klien, sehingga jika terdeteksi aktivitas tersebut, bisa secepatnya dinotifikasi. Pada beberapa hari tersebut, terjadi beberapa konfigurasi yang dilakukan akun admin klien, sehingga perlu langsung dinotifikasi untuk mengkonfirmasi.
10	Menjalankan operasional *mid shift*. Ditemukan beberapa aktivitas terkait email security, di mana klien mendapatkan email dari sumber yang mencurigakan. Terdeteksi file yang tergolong malicious berdasarkan reputasi hash yang diperiksa melalui online tools VirusTotal.
11	Menjalankan operasional *early shift*. Pada pekan ini ditemukan banyak aktivitas bruteforce, di mana terdapat user yang mencoba masuk atau log in dan mendapatkan *failure logon* dalam jumlah banyak di waktu yang singkat.
	Lanjut pada halaman berikutnya

Tabel 3.3. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)

Minggu Ke -	Pekerjaan yang dilakukan
12	Menjalankan operasional *night shift*. Pada pekan ini, ditemukan aktivitas yang mengubah atribut-atribut dan *user member* dalam suatu *security group*. Aktivitas ini dilakukan oleh user administrator dan telah dikonfirmasi oleh klien bahwa aktivitas ini *legitimate* karena memang dilakukan aktivitas update data pada sistem.
13	Menjalankan operasional *mid shift*. Pada pekan ini ditemukan beberapa aktivitas terkait pengubahan pada *security group* suatu user. Aktivitas ini terdeteksi sebagai mencurigakan karena termasuk sebagai *high-privileged activity* yang di mana dilakukan oleh user admin.
14	Menjalankan operasional *early shift*. Pada pekan ini, ditemukan aktivitas dari IP luar yang mencoba mengakses sistem internal. Terdapat aktivitas di mana adanya akses port RDP (*Remote Desktop Protocol*) dan mencoba mengakses *setup environment* dan *configuration*.
15	Menjalankan operasional *night shift*. Pada pekan ini, ditemukan banyak aktivitas terkait *object changes* dari aset dan sistem klien. Aktivitas ini meliputi pembuatan dan modifikasi *object attributes*, serta pembuatan dan modifikasi *rule* pada sistem.
16	Menjalankan operasional *mid shift*. Pada pekan ini, ditemukan beberapa aktivitas oleh user dalam sistem klien yang mengakses *malicious website*. Aktivitas berupa mengakses dan terdeteksinya request yang dilakukan kepada *website* terkait.

3.3 Uraian Pelaksanaan Magang

Implementasi aktivitas dalam lingkungan *Security Operations Center* (SOC) mencakup proses *monitoring* sistem secara berkelanjutan dan *incident handling* keamanan melalui tahapan yang sistematis. Fokus dari kegiatan yang dilakukan

berada pada fase *detection and analysis*, yaitu tahap awal dalam siklus *incident response* yang bertujuan untuk mengidentifikasi dan memvalidasi potensi ancaman berdasarkan *alarm* dan *data log* yang terekam dalam sistem keamanan.

Monitoring dilakukan dengan pendekatan berbasis log, yang mencakup berbagai jenis sumber data dari perangkat dan sistem yang tersebar di seluruh jaringan klien. Berdasarkan model referensi OSI (*Open Systems Interconnection*), sebagian besar proses *monitoring* dan analisis dalam SOC dilakukan pada lapisan ke-3 (*Network Layer*), lapisan ke-4 (*Transport Layer*), dan lapisan ke-7 (*Application Layer*). Lapisan-lapisan tersebut mencakup data seperti alamat IP dan *routing* (*network layer*), informasi port dan koneksi (*transport layer*), serta aktivitas HTTP, DNS, email, dan protokol lainnya (*application layer*), yang semuanya menjadi indikator penting dalam mendeteksi dan menganalisis serangan.

3.3.1 Implementasi *Security Monitoring* dalam *Workflow* Operasional SOC

Pelaksanaan kegiatan *security monitoring* dan *incident handling* dalam lingkungan Security Operations Center (SOC) mengikuti standar prosedur yang telah ditetapkan oleh perusahaan. Fokus utama kegiatan ini adalah menjaga keamanan sistem informasi milik klien dari potensi serangan siber dengan cara memantau aktivitas sistem secara *real-time*, mendeteksi adanya anomali, dan menganalisis kemungkinan terjadinya insiden. Pemantauan dilakukan dengan dukungan sistem *Security Information and Event Management* (SIEM) yang terintegrasi dengan berbagai sumber *log* dari infrastruktur klien.

Dalam operasional SOC, setiap aktivitas penanganan insiden dikategorikan berdasarkan fase dalam siklus *incident response*, yang umumnya mengacu pada standar dari NIST SP 800-61. Tahapan yang dijalankan dalam kegiatan ini berfokus pada fase pertama dan kedua, yaitu *monitoring* log sistem dan *detection and analysis*. Fase ini mencakup proses identifikasi awal dari insiden, validasi terhadap alarm yang muncul, serta pencarian bukti pendukung yang relevan dari *data log*. Setiap alarm yang terdeteksi menjadi titik awal dilakukannya analisis lanjutan terhadap aktivitas mencurigakan yang terekam di dalam sistem.

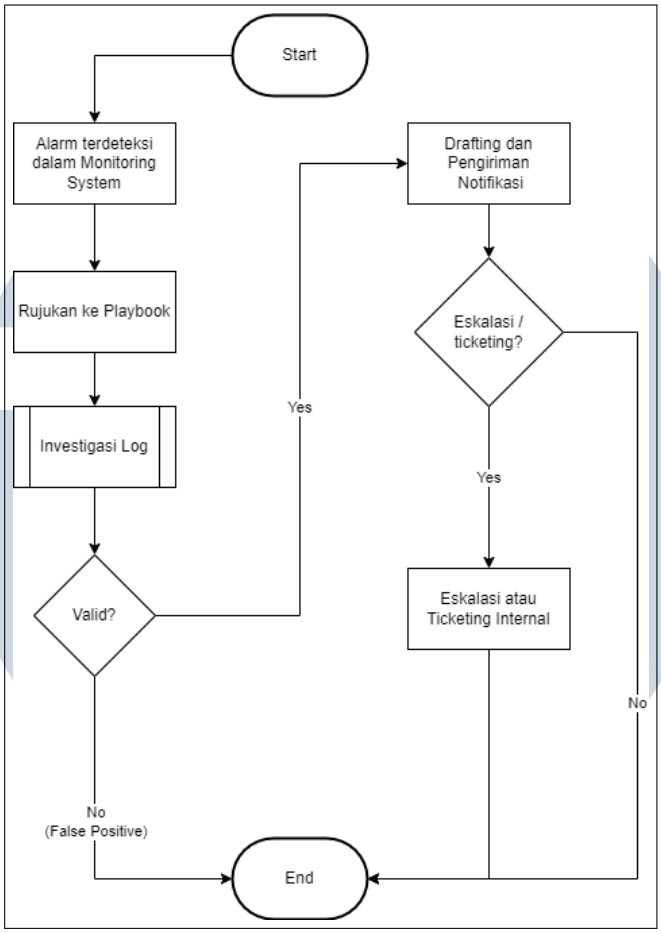
Dalam pelaksanaan analisis, berbagai sumber *log* digunakan secara bersamaan, baik dari *endpoint, firewall, IDS/NIDS, mail security*, hingga *web application firewall*. Semua log yang masuk dikonsolidasikan ke dalam sistem SIEM, memungkinkan dilakukannya korelasi dan pencarian pola serangan yang kompleks. Korelasi log memegang peranan penting dalam tahap deteksi, karena

banyak ancaman modern tidak dapat dikenali hanya dari satu sumber log saja, melainkan membutuhkan konfirmasi silang dari beberapa perangkat keamanan.

Setiap langkah yang dilakukan dalam proses pemantauan dan analisis mengikuti panduan prosedural yang terdokumentasi dalam *playbook*. *Playbook* berfungsi sebagai acuan standar untuk penanganan insiden berdasarkan jenis ancaman, jenis sistem, dan kebijakan keamanan masing-masing klien. Panduan ini membantu menentukan langkah teknis yang tepat sejak awal analisis, termasuk perangkat mana yang harus diperiksa terlebih dahulu, indikator serangan yang umum, hingga format penulisan laporan dan metode eskalasi insiden yang sesuai.

Dengan keberadaan sistem SIEM yang telah diintegrasikan secara menyeluruh, serta prosedur yang terdokumentasi dalam *playbook*, proses *monitoring* dan analisis insiden dapat dijalankan secara sistematis, berulang, dan terukur. Hal ini memastikan bahwa setiap insiden yang terdeteksi diproses secara konsisten dengan standar yang telah ditentukan, serta memberikan hasil yang akurat dan dapat dipertanggungjawabkan. Gambaran dari proses tersebut dapat dilihat dalam *flowchart* pada Gambar 3.2 mengenai alur analisis dan penanganan insiden di lingkungan SOC.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA



Gambar 3.2. *Flowchart* alur analisis dan penanganan insiden SOC

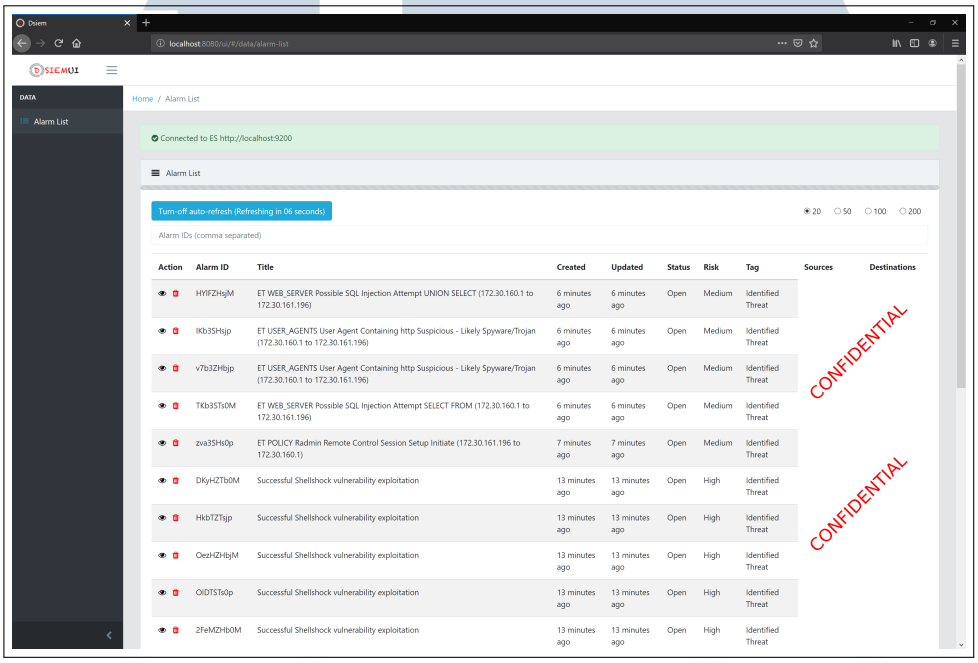
Sumber: Data Internal Pribadi [10]

A Alarm Terdeteksi dalam Sistem Monitoring

Proses penanganan insiden dimulai ketika sistem *monitoring* mendeteksi adanya aktivitas mencurigakan yang sesuai dengan *rule* atau pola yang telah ditentukan. Deteksi ini dilakukan secara otomatis oleh sistem *Security Information and Event Management* (SIEM) yang memantau *log* dari berbagai perangkat dan sistem. Salah satu platform yang digunakan dalam *monitoring* adalah DSIEM, yang menampilkan daftar alarm berdasarkan korelasi log dan rule yang telah diatur sebelumnya. DSIEM sendiri adalah SIEM yang dirancang oleh Defenxor untuk melakukan *monitoring* dan sudah bersifat open-source sehingga dapat digunakan secara bebas.

Pada DSIEM, alarm yang muncul ditampilkan dalam bentuk tabel berisi informasi seperti waktu kejadian, tingkat risiko, nama rule yang terpicu, serta sistem atau perangkat yang terdampak. Tingkat risiko digunakan sebagai acuan awal untuk

menentukan prioritas penanganan. Selain DSIEM, sistem monitoring lain seperti Wazuh yang terintegrasi dengan Opensearch atau Elasticsearch juga digunakan, di mana alarm ditampilkan melalui *security dashboard* dengan informasi yang serupa. Gambar 3.3 adalah bagaimana alarm yang muncul pada DSIEM ditampilkan dalam *list* tabel. Masing-masing dari alarm yang muncul memiliki detail sekilas dari *rule*, *source IP*, *destination IP*, waktu kejadian, status, dan *risk*.



Gambar 3.3. Tampilan *Alarm List*

Sumber: Data Internal Pribadi [10]

Alarm yang muncul tidak selalu menandakan adanya insiden yang valid. Oleh karena itu, setiap alarm perlu dianalisis lebih lanjut untuk memastikan apakah benar terjadi ancaman atau hanya *false positive*. Proses ini menjadi titik awal dalam tahapan *detection and analysis* pada siklus *incident response*.

B Rujukan ke *Playbook*

Setelah alarm terdeteksi, langkah selanjutnya adalah melakukan rujukan terhadap *playbook* yang relevan. *Playbook* menjadi dokumen prosedural yang berisi panduan teknis dan strategis dalam menangani insiden berdasarkan kategori ancaman, perangkat yang terlibat, serta karakteristik sistem milik klien. Panduan ini disusun untuk memastikan bahwa setiap alarm ditangani secara konsisten dan sesuai standar operasional yang berlaku di SOC.

Selain memuat langkah-langkah respons, *playbook* juga dilengkapi dengan informasi penting terkait sistem klien, seperti daftar aset yang terhubung ke sistem, segmentasi jaringan berdasarkan fungsi dan sensitivitas, topologi, serta daftar *whitelist* IP, *domain*, dan informasi lainnya yang telah divalidasi sebelumnya. Informasi ini digunakan sebagai referensi awal untuk membantu menganalisis apakah sebuah alarm mengindikasikan ancaman nyata, atau berasal dari aktivitas yang sudah diketahui dan diizinkan.

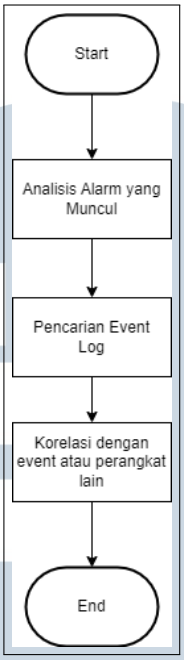
Sebagai contoh, ketika sebuah IP eksternal muncul dalam *log* koneksi masuk, *playbook* dapat digunakan untuk memeriksa apakah IP tersebut termasuk dalam daftar *whitelist* atau bagian dari sistem yang sah. Begitu pula dengan segmentasi jaringan, yang membantu mengidentifikasi apakah trafik yang terlihat antar perangkat melintasi batas zona yang tidak seharusnya berkomunikasi.

Dengan merujuk pada *playbook* sebelum analisis dilakukan, proses investigasi dapat dilaksanakan secara lebih efisien dan akurat. Hal ini juga meminimalkan risiko kesalahan interpretasi, mempercepat proses validasi insiden, dan memastikan penanganan yang konsisten antar shift dan tim yang terlibat.

C Investigasi *Log*

Setelah referensi awal terhadap *playbook* dilakukan, langkah berikutnya adalah investigasi *log* berdasarkan *alarm* yang terdeteksi. Proses ini bertujuan untuk mengonfirmasi validitas alarm dengan cara menelusuri lebih lanjut informasi *log* yang berkaitan dengan aktivitas yang dianggap mencurigakan. Tahapan ini dibagi menjadi tiga tahap, yang dapat dilihat dalam *flowchart* pada gambar 3.4.

UNIVERSITAS MULTIMEDIA NUSANTARA



Gambar 3.4. *Flowchart* Investigasi Log

Sumber: Data Internal Pribadi [10]

Data log yang sebelumnya dikonsolidasikan ke dalam platform monitoring seperti Opensearch atau Elasticsearch digunakan sebagai dasar untuk mengidentifikasi asal muasal kejadian. Investigasi dilakukan dengan membuka detail alarm seperti IP sumber dan tujuan, *event ID*, jenis *log*, sistem terdampak, serta waktu kejadian. Informasi-informasi tersebut menjadi acuan untuk pencarian lanjutan dan analisis lebih mendalam terhadap potensi ancaman yang terjadi.

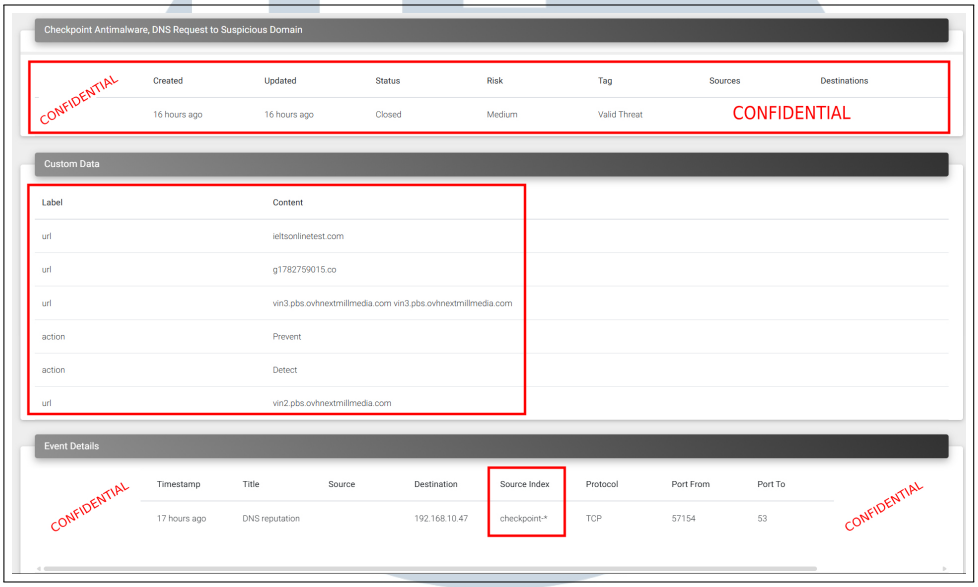
Analisis *log* tidak hanya terbatas pada satu perangkat, tetapi juga mempertimbangkan struktur jaringan klien secara menyeluruh. Proses ini sangat krusial karena kesalahan interpretasi dapat mengakibatkan salah klasifikasi insiden. Oleh karena itu, setiap tahapan investigasi dirancang untuk terintegrasi dan selaras dengan alur yang telah didefinisikan secara sistematis dalam flowchart sebagai bagian dari prosedur operasional standar SOC.

C.1 Analisis Alarm yang Muncul

Setelah alarm terdeteksi dan dilakukan referensi terhadap *playbook*, langkah selanjutnya adalah menganalisis alarm secara detail untuk memahami konteks dan validitas ancaman yang dilaporkan. Informasi alarm ditampilkan dalam sistem SIEM seperti Wazuh atau DSIEM, dengan detail yang mencakup timestamp,

kategori ancaman, severity, IP sumber dan tujuan, serta perangkat yang terlibat.

Gambar 3.4 menunjukkan *flowchart* dari proses investigasi yang mengarahkan proses menuju pemeriksaan detail alarm dan pencarian lanjutan berdasarkan informasi yang tersedia. Proses ini penting untuk menilai apakah alarm tersebut valid dan perlu ditindaklanjuti, atau merupakan *false positive*.



Gambar 3.5. Tampilan detail suatu *alarm*

Sumber: Data Internal Pribadi [10]

Sebagai contoh, gambar 3.5 memperlihatkan salah satu tampilan alarm detail dari dashboard SIEM. Alarm ini berjudul ”Checkpoint Antimalware, DNS Request to Suspicious Domain”, di mana terdapat aktivitas DNS request ke beberapa domain mencurigakan yang berhasil ditandai oleh *rule* dalam *monitoring system*. Informasi yang disajikan mencakup *risk level (medium)*, nama *rule*, serta domain yang menjadi objek dari aktivitas tersebut. Selain itu, *alarm* juga menampilkan IP sumber, IP tujuan, serta pesan *log* yang menjadi dasar *alarm* muncul.

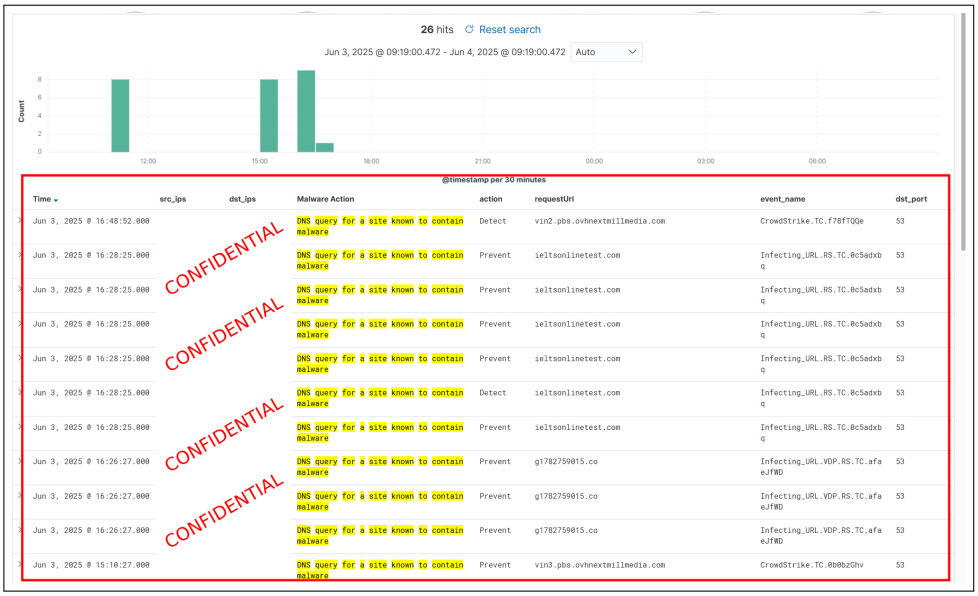
Melalui informasi ini, aktivitas perlu dinilai apakah domain yang dimaksud adalah bagian dari aktivitas sah atau merupakan bagian dari aktivitas anomali yang memerlukan investigasi lebih lanjut. Langkah lanjutan dari alarm ini melibatkan pencarian *log* terkait aktivitas DNS, validasi reputasi domain, serta korelasi dengan aktivitas *user* atau proses yang berlangsung di *endpoint*.

C.2 Pencarian *Event Log* Terkait

Setelah dilakukan analisis awal terhadap *alarm*, langkah selanjutnya adalah melakukan pencarian *log* yang relevan untuk mendukung atau membantah adanya insiden. Pencarian ini dilakukan menggunakan *dashboard log management* Opensearch atau Elasticsearch yang telah terintegrasi dengan *pipeline log* dari berbagai perangkat keamanan.

Melalui fitur *Discover* atau *Search Query Builder*, pencarian dilakukan dengan menggunakan parameter yang didapat dari *alarm* sebelumnya, seperti IP sumber atau tujuan, nama perangkat, *event ID*, *path log*, atau *keyword* yang muncul dalam pesan *log*. Proses ini memungkinkan identifikasi rangkaian aktivitas yang terjadi sebelum dan sesudah waktu *alarm*, guna membangun *timeline* awal serta mencari pola serangan seperti koneksi bertahap, autentikasi berulang, atau perubahan konfigurasi sistem.

Informasi ini kemudian digunakan dalam *query* pencarian untuk menemukan *event log* terkait aktivitas aktivitas yang dicurigai, baik sebelum maupun sesudah waktu alarm. Dalam kasus pada gambar 3.6, pencarian difokuskan pada permintaan DNS dari IP tertentu ke domain yang mencurigakan berdasarkan isi *alarm* sebelumnya. Dengan informasi berdasarkan *alarm*, ditemukan 26 *event log* terkait aktivitas yang sesuai.



Gambar 3.6. Tampilan *Event Log*

Sumber: Data Internal Pribadi [10]

Gambar 3.6 menunjukkan log dari aktivitas ke suspicious domain yang

berdasarkan alarm yang muncul sebelumnya. Kolom dari setiap log ditampilkan sesuai dengan data-data yang relevan sebagai bentuk informasi yang dilampirkan sebagai bukti aktivitas kepada klien. Dalam pencarian log tersebut, digunakan field informasi yang menjadi signature setiap alarm, yaitu *source IP*, *destination IP*, nama *rule*, dan domain yang dikses.

Hasil pencarian log umumnya menampilkan data seperti permintaan DNS berulang, resolusi domain ke IP tertentu, atau adanya koneksi lanjutan setelah resolusi DNS berhasil. Jika ditemukan pola bahwa sistem melakukan permintaan ke beberapa domain mencurigakan dalam rentang waktu singkat, maka dugaan adanya *malware beaconing* atau penggunaan *domain command and control* (C2) semakin kuat. Seperti pada gambar 3.6, aktivitas yang terjadi sesuai dengan IP asal, IP tujuan, dan domain yang terdapat pada detail *alarm*.

Selain *log* dari DNS *resolver* atau *endpoint*, pencarian juga dapat diperluas ke sumber *log* lainnya, seperti *log proxy*, *firewall*, atau WAF (*Web Application Firewall*), untuk mengidentifikasi apakah ada koneksi aktif atau transfer data setelah domain tersebut diakses. Pendekatan ini dilakukan guna memastikan bahwa aktivitas yang terdeteksi bukan hanya anomaly isolated, tetapi memiliki kaitan dengan pola serangan tertentu.

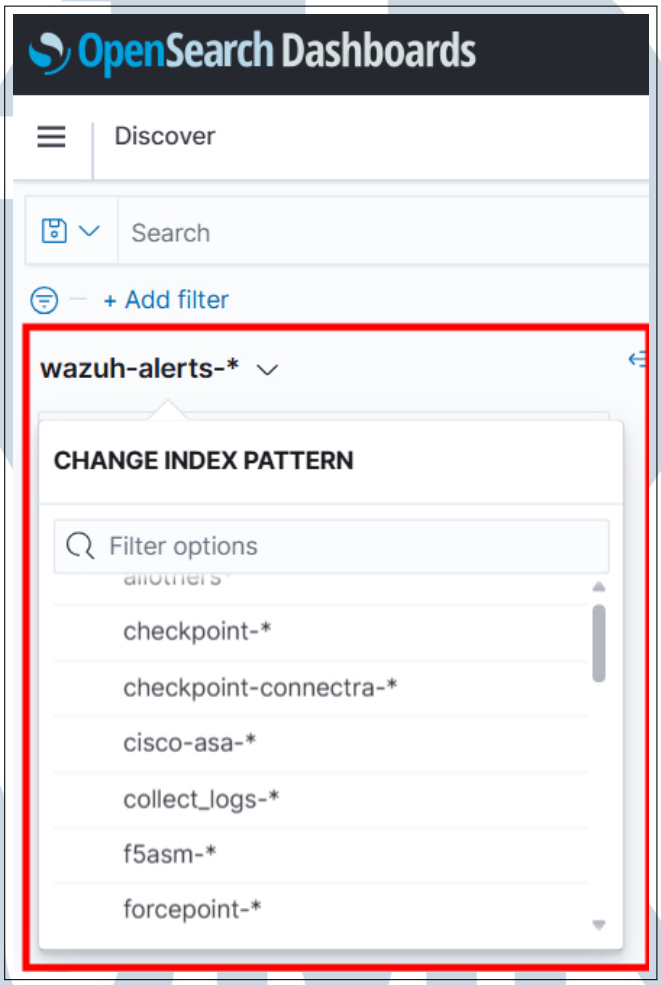
Pencarian *event log* yang relevan merupakan tahapan penting untuk memperkuat analisis, memberikan bukti tambahan terhadap validitas insiden, serta sebagai bahan pertimbangan dalam penyusunan notifikasi dan rekomendasi tindak lanjut.

C.3 Korelasi Data dari *Event* atau Perangkat Lain

Setelah *log* yang relevan ditemukan, proses dilanjutkan dengan melakukan korelasi antar log dari berbagai sumber perangkat keamanan. Tujuan dari tahap ini adalah untuk memperoleh gambaran menyeluruh dari aktivitas yang terjadi serta memastikan apakah alarm yang terpicu merupakan bagian dari insiden nyata atau hanya aktivitas yang sah namun mencurigakan secara parsial.

Korelasi dilakukan dengan membandingkan *log* dari sumber yang berbeda, seperti *log* dari *firewall*, *endpoint*, *intrusion detection system (IDS/NIDS),* serta *mail* atau *proxy server*. Misalnya, jika alarm menunjukkan adanya koneksi dari IP eksternal ke salah satu server, maka *log* dari *firewall* diperiksa untuk melihat apakah koneksi tersebut benar terjadi dan apakah diarahkan ke port terbuka. Selanjutnya, *log* dari *endpoint* dicek untuk melihat apakah terjadi eksekusi perintah, login, atau

perubahan sistem pasca koneksi tersebut. *Log* perangkat keamanan yang terhubung dapat dibuka melalui *data view* yang terdapat pada *dashboard Discover*. Gambar 3.6 adalah *menu* bagaimana perangkat lain dapat diakses, seperti dari *firewall*, WAF, *endpoint*, dan perangkat lainnya yang terhubung



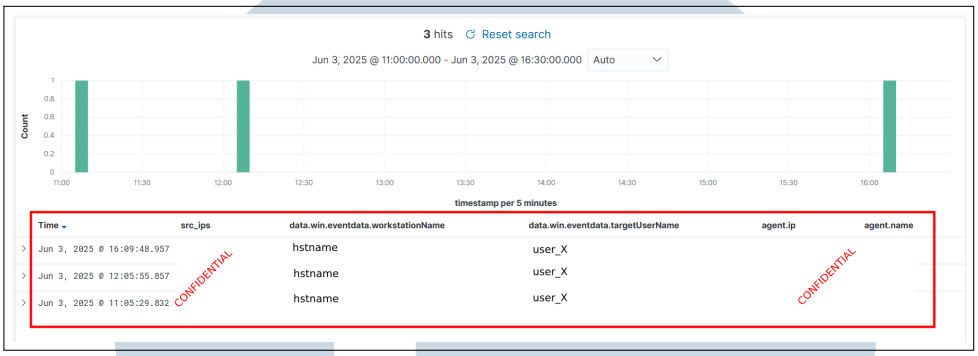
Gambar 3.7. Tampilan Pemilihan *Data View* atau *Index* Perangkat

Sumber: Data Internal Pribadi [10]

Proses korelasi juga memperhatikan aspek waktu (*timestamp*), jalur komunikasi (*source–destination*), dan *user* atau *service* yang digunakan. Dengan mengaitkan elemen-elemen ini dari berbagai perangkat, pola serangan seperti *lateral movement*, *privilege escalation*, hingga *malware beaconing* dapat dikenali lebih dini. Jika semua elemen mendukung asumsi adanya aktivitas mencurigakan yang saling berkaitan, maka insiden dikategorikan sebagai valid dan siap untuk ditindaklanjuti lebih lanjut.

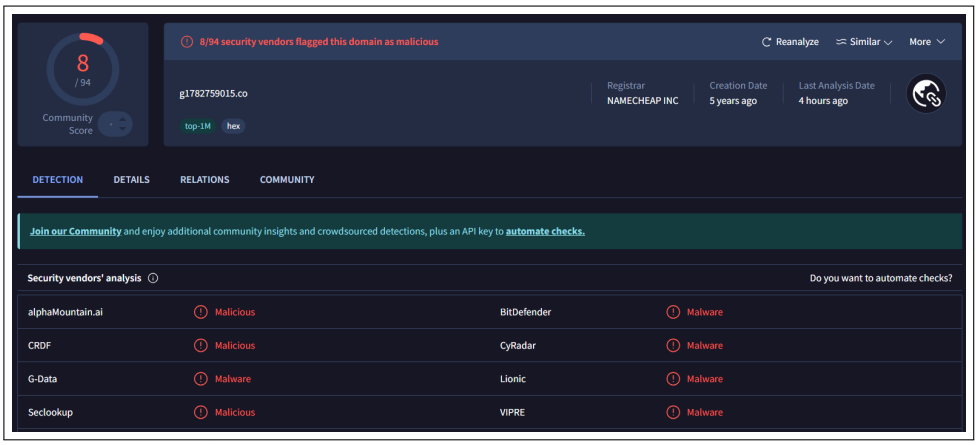
Korelasi *log* merupakan bagian krusial dalam proses analisis, karena serangan modern sering kali terdistribusi dan tidak tampak mencurigakan jika

hanya dilihat dari satu jenis *log*. Oleh karena itu, keberhasilan tahap ini sangat bergantung pada kemampuan sistem *monitoring* dalam mengkonsolidasikan *log* serta kompetensi dalam mengaitkan informasi yang tersedia.



Gambar 3.8. Korelasi dengan aktivitas atau perangkat lain
Sumber: Data Internal Pribadi [10]

Gambar 3.8 menggambarkan korelasi dari event sebelumnya. Korelasi yang digunakan adalah pencarian aktivitas pada IP terkait, di mana ditemukan user yang mengakses tiga kali sesuai dengan jumlah domain yang diakses. User tersebut melakukan aktivitas pada IP tujuan yang di mana merupakan IP server. Sebagai informasi lanjutan, *hostname* dari IP menjadi lokasi segmen yang dinotifikasi ke klien.



Gambar 3.9. Hasil pengecekan reputasi domain menggunakan VirusTotal
Sumber: Data Internal Pribadi [10]

Online tools biasa digunakan untuk membantu pengecekan reputasi dari informasi yang dimiliki. Informasi yang umum dapat dicek reputasinya meliputi *IP address*, *domain*, email, dan *hash* pada file. *Online tools* yang digunakan pada gambar 3.9 adalah *VirusTotal*, di mana dilakukan pengecekan apakah domain

tersebut telah dimasukkan ke *blocklist* oleh vendor yang terdapat pada *list* di bawahnya. Berdasarkan hasil VirusTotal tersebut, domain telah dimasukkan *blocklist* oleh 8 vendor. Dengan hasil informasi reputasi tersebut, ditarik kesimpulan bahwa domain tersebut adalah *malicious domain*.

D Drafting dan Pengiriman Notifikasi

Setelah seluruh *data log* dan bukti pendukung terkumpul, termasuk hasil korelasi dan pemeriksaan reputasi, tahap selanjutnya adalah menyusun notifikasi insiden yang dikirimkan kepada pihak klien terkait.

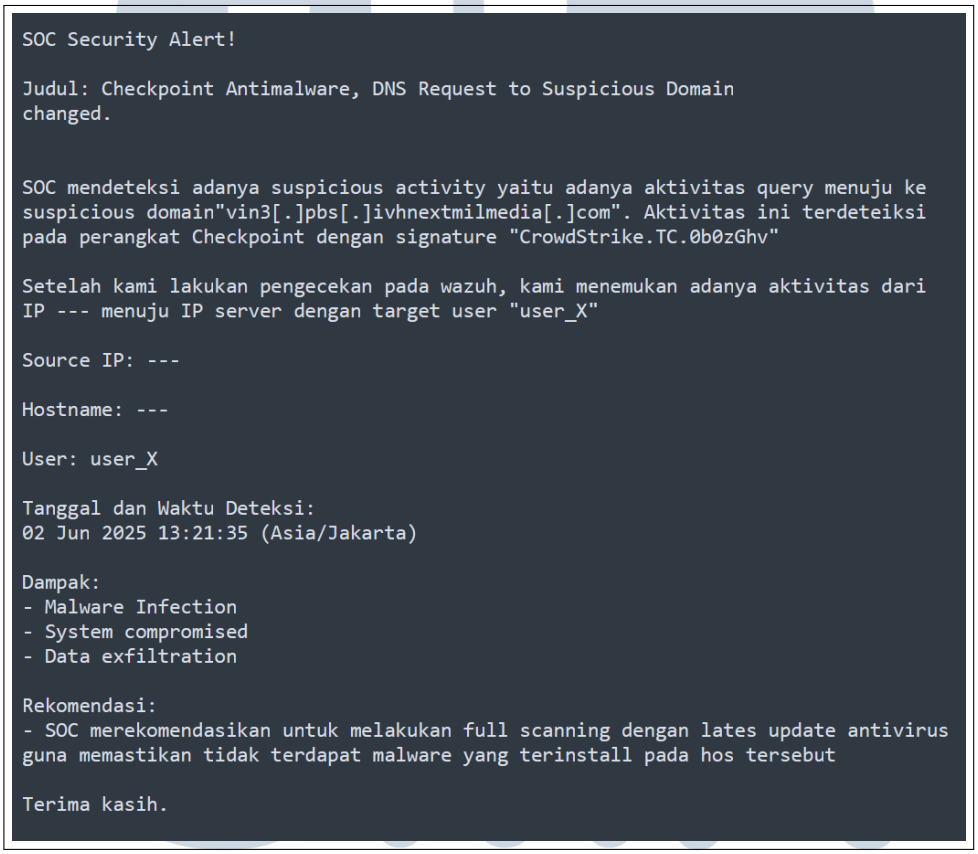
Notifikasi disusun berdasarkan format standar yang telah ditentukan. Format tersebut umumnya mencakup elemen-elemen berikut.

1. Judul Insiden
2. *Severity Level*
3. Waktu Kejadian
4. Kronologi Singkat
5. Analisis Singkat
6. Indikator Ancaman (IP, *domain*, *hash*, dan lainnya)
7. Sistem yang Terpengaruh
8. Rekomendasi Tindakan

Penyusunan notifikasi harus disesuaikan dengan karakteristik klien, terutama dari sisi sistem yang digunakan dan level pemahaman teknis tim klien. Notifikasi ditulis dalam gaya yang profesional dan objektif, serta tidak menggunakan istilah teknis yang terlalu rumit apabila tidak diperlukan. Notifikasi juga mencantumkan lampiran berupa *log* atau hasil tangkapan layar sebagai bukti pendukung tambahan.

Selain menyusun isi notifikasi, perlu dipastikan bahwa informasi yang disampaikan telah diverifikasi dan tidak menimbulkan alarm yang tidak perlu. Oleh karena itu, sebelum dikirimkan, notifikasi dapat melalui proses review internal atau persetujuan dari rekan satu tim yang bertugas di *shift* yang sama.

Setelah notifikasi insiden selesai disusun, proses selanjutnya adalah pengiriman notifikasi tersebut kepada klien menggunakan sistem yang telah terintegrasi dengan kanal komunikasi resmi. Di lingkungan operasional, proses pengiriman ini dilakukan melalui platform internal, yang dirancang khusus untuk mengelola *drafting*, dokumentasi, serta pengiriman insiden secara terstandarisasi dan efisien. Gambar 3.10 berikut adalah contoh dari kasus serupa yang pernah dinotifikasikan, di mana mencakup elemen-elemen pada draf yang telah disebutkan sebelumnya.



Gambar 3.10. Notifikasi Case
Sumber: Data Internal Pribadi [10]

Draf notifikasi pada gambar 3.10 mencakup informasi hasil dari investigasi dan analisis sebelumnya. Notifikasi memberikan judul sesuai dengan rule dari alarm yang terdeteksi. Deskripsi singkat diberikan untuk menjelaskan yang terjadi berdasarkan aktivitas pada log. Setelah deskripsi diberikan, dicantumkan informasi terkait deteksi yang terjadi, di antaranya *source IP*, *hostname*, *user*, dan kapan terdeteksinya aktivitas tersebut. Sebagai bagian akhir dari draf, dampak terkait aktivitas tersebut dicantumkan beserta dengan rekomendasi yang dapat dilakukan

untuk menangani kemungkinan terjadinya dampak yang disebutkan.

Notifikasi yang telah didraf secara otomatis dikirimkan melalui kanal komunikasi yang telah ditentukan untuk setiap klien. Umumnya, pengiriman dilakukan ke email dan aplikasi Signal secara bersamaan. Namun, terdapat juga klien yang hanya menerima notifikasi melalui satu kanal tertentu, atau memiliki preferensi kanal lain sesuai dengan kebijakan masing-masing. Konfigurasi pengiriman ini telah diatur sebelumnya dalam sistem, sehingga ketika notifikasi dikirim, sistem secara otomatis menyesuaikan tujuan pengiriman tanpa perlu dilakukan manual oleh SOC.

Proses ini tidak hanya mempercepat pengiriman, tetapi juga memastikan bahwa isi notifikasi tetap konsisten antar kanal. Setiap notifikasi yang dikirim memuat kronologi insiden, bukti analisis yang relevan, dan rekomendasi tindakan yang perlu dilakukan. Dengan mekanisme otomatis ini, distribusi informasi ke klien dapat dilakukan secara cepat, akurat, dan terdokumentasi.

E Eskalasi atau *Ticketing* Internal

Jika dari hasil investigasi ditemukan bahwa insiden membutuhkan tindakan teknis lebih lanjut, seperti pemblokiran IP, isolasi perangkat, atau pengecekan langsung pada sisi infrastruktur, maka insiden diteruskan melalui proses eskalasi internal. Eskalasi ini dilakukan dengan membuat tiket pada sistem *ticketing* internal perusahaan, yang ditujukan kepada tim teknis terkait seperti *sysadmin*, *network engineer*, atau tim keamanan internal klien.

Proses pembuatan tiket mencakup pengisian informasi insiden secara ringkas namun jelas, seperti referensi notifikasi yang telah dikirimkan, kronologi singkat, hasil analisis, dan tindakan teknis yang direkomendasikan atau dibutuhkan. Tiket juga mencantumkan informasi perangkat terdampak serta urgensi penanganan berdasarkan severity insiden.

Setelah tiket dibuat, sistem akan mengarahkan tiket insiden tersebut kepada tim yang berwenang. Dalam beberapa kasus, *update* dari tim teknis juga ditambahkan ke tiket yang sama, sehingga dokumentasi proses dapat dilakukan secara terpusat dan transparan antar divisi.

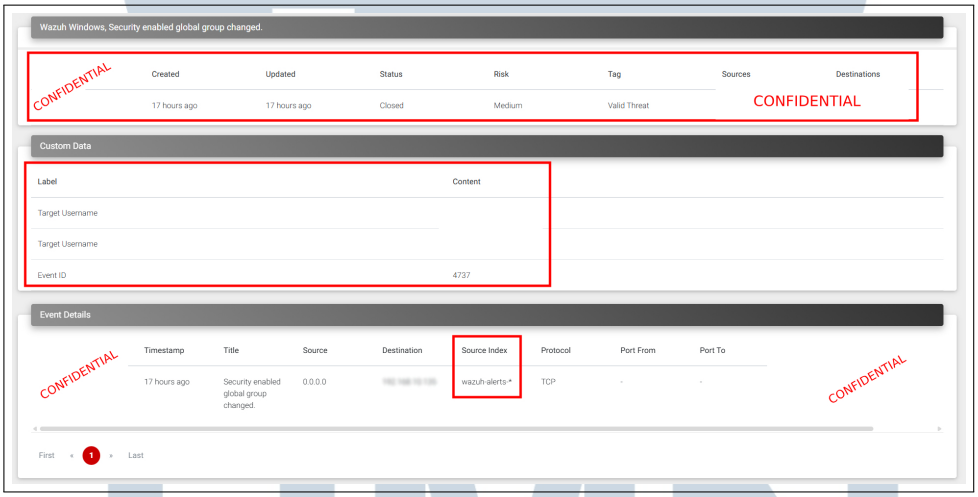
Dalam implementasi security monitoring ini, pemahaman mendalam terhadap baseline normal dari aktivitas sistem sangat krusial untuk secara efektif membedakan anomali dari noise biasa. Pengamatan berkelanjutan terhadap perilaku *log* dan *alert/alarm* membantu membangun intuisi yang tajam, memungkinkan

identifikasi dini terhadap potensi ancaman di tengah volume data yang besar, sehingga menjaga efektivitas operasional SOC.

3.3.2 Implementasi *Case Incident Handling*

Pada bagian ini, dijabarkan bagaimana contoh *case handling* yang dilakukan dalam operasional SOC. Kasus yang dianalisis adalah terkait *alarm* ”Wazuh Windows, Security enabled global group changed”. Secara singkat, *alarm* ini terkait adanya pengubahan group security pada *user* sistem klien terkait.

A *Alarm Details*



Gambar 3.11. *Alarm Detail* dari *Case* yang dianalisis

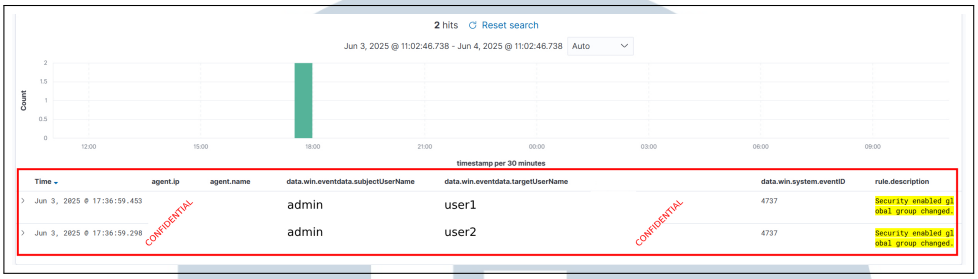
Sumber: Data Internal Pribadi [10]

Insiden pertama kali terdeteksi melalui sistem SIEM Wazuh, yang menampilkan *alarm* dengan indikator perubahan grup keamanan global. Seperti ditunjukkan pada gambar 3.11, aktivitas tersebut menunjukkan adanya perubahan yang dilakukan dari IP internal (0.0.0.0) ke IP tujuan yang telah diketahui sebagai IP server berdasarkan referensi *playbook*. *Alarm* ini mencatat adanya aktivitas terhadap dua akun pengguna yang berbeda, dan seluruh data muncul dalam perangkat *wazuh-alerts*.

B *Analysis Details*

Langkah awal analisis dilakukan dengan memanfaatkan detail *alarm* sebagai *filter* dalam pencarian *log* tambahan pada *monitoing system*. Ditemukan dua event

log yang sesuai, masing-masing dengan *event ID* 4737, yang dalam dokumentasi merujuk pada perubahan atribut keamanan dalam grup pengguna.



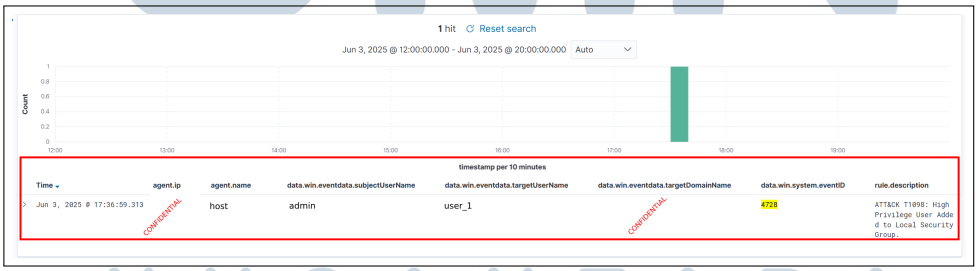
Gambar 3.12. *Event Log* dari aktivitas yang terdeteksi

Sumber: Data Internal Pribadi [10]

Dalam gambar 3.12, adalah bukti ditemukannya log aktivitas dari *event ID* 4737. Aktivitas dari log tersebut dilakukan oleh *user* admin ke dua *user*, yaitu user1 dan user2. Selanjutnya, dilakukan korelasi terhadap log lain yang mungkin relevan. Terdapat beberapa *event ID* yang sering dikaitkan dengan aktivitas ini, antara lain.

1. 4728, *A member was added to a security-enabled global group*
2. 4725, *A user account was disabled*
3. 4738, *A user account was changed*

Dalam proses ini, ditemukan log tambahan dengan *Event ID* 4728, yang dapat dilihat pada gambar 3.13. Aktivitas yang terjadi adalah user1 dimasukkan sebagai *high privileged user* yang memliki hak akses luas dalam *security group* tersebut. Hal ini sangatlah penting untuk dilihat, karena keberadaan *high privileged user* perlu diperhatikan aktivitasnya.



Gambar 3.13. Korelasi dengan aktivitas yang berhubungan sesuai konteks alarm

Sumber: Data Internal Pribadi [10]

Keberadaan kombinasi aktivitas ini dalam rentang waktu yang berdekatan dan dilakukan oleh user yang sama, mengindikasikan kemungkinan adanya aktivitas

mencurigakan (*suspicious activity*). Gambar 3.12 dan 3.13 memperlihatkan hasil korelasi *log* antara perubahan grup, user yang melakukan aksi, serta target akun yang terdampak.

Melalui hasil investigasi ini, aktivitas dikategorikan sebagai *suspicious internal activity*, yang berpotensi sebagai aksi *privilege escalation* tanpa *authorization*. Oleh karena itu, aktivitas ini memerlukan konfirmasi lebih lanjut kepada pihak klien terkait.

C *Impact and Recommendation*

Berdasarkan informasi yang didapatkan, potensi dampak dari aktivitas ini meliputi hal berikut.

1. *Unauthorized Access*, pengguna yang tidak sah mendapatkan akses administratif atau khusus ke sistem.
2. *Data Exfiltration*, akses lebih dapat dimanfaatkan untuk mencuri data penting.
3. *System Compromise*, perubahan *security group* dapat membuka jalan bagi tindakan lebih lanjut yang bersifat merusak.

Berdasarkan potensi risiko yang telah diidentifikasi, terdapat beberapa rekomendasi teknis sebagai langkah mitigasi yang dapat diambil. Rekomendasi ini ditujukan untuk memastikan bahwa tidak terjadi pelanggaran hak akses lebih lanjut dan menjaga integritas sistem. Adapun rekomendasi tersebut meliputi:

1. Melakukan pengecekan lanjutan terhadap aktivitas pada server yang terindikasi.
2. Mengganti kredensial pada akun-akun yang terlibat.
3. Jika aktivitas tersebut tidak diotorisasi, melakukan pencabutan akses terhadap user yang melakukan perubahan.
4. Meninjau kembali kebijakan privilege access management pada server tersebut.

D *Notification Draft*

Berdasarkan hasil investigasi, disusun sebuah draf notifikasi insiden yang dirancang untuk dikirim kepada klien. Notifikasi ini mencakup elemen penting seperti waktu kejadian, user yang terlibat, segmentasi sistem terdampak, rekomendasi mitigasi, serta bukti pencarian *event log*. Gambar 3.14 berikut adalah isi draf notifikasi yang disusun berdasarkan hasil analisis kasus.

```
SOC Security Alert!

Judul: Wazuh Windows, Security enabled global group
changed.


SOC mendeteksi adanya aktivitas audit pada log Wazuh. Aktivitas ini terdeteksi
dengan event sebagai berikut:

- 4737 (A security-enabled global group was changed)
- 4728 (A member was added to a security-enabled global group)

Aktivitas ini menunjukkan adanya perubahan, dan penambahan/penghapusan member pada
grup yang diakui oleh Active Directory. Oleh karena itu, kami meminta konfirmasi
apakah aktivitas tersebut legitimate atau tidak? Jika tidak kami menyarankan untuk
melakukan rekomendasi yang kami berikan.

Subject Username :
- admin

Target User:
- user_1
- user_2

Affected IP: X.X.X.X
Hostname: SVR
Segment: SGMT

Tanggal & Waktu Kejadian: 03 June 2025 17:36:59 (Asia/Jakarta)


Dampak:
- Unauthorized access
- System compromised

Rekomendasi:
- Memastikan pada user terkait atau Domain Admin apakah aktivitas ini diizinkan
atau tidak.
- Melakukan remove user terkait apabila aktivitas tersebut tidak authorized.

Terima Kasih.
```

Gambar 3.14. Draf notifikasi hasil analisis kasus

Sumber: Data Internal Pribadi [10]

Gambar 3.14 adalah hasil draf dari aktivitas yang dinotifikasi ke klien. Inti dari aktivitas yang terjadi adalah pada event 4727 (*A security-enabled global group was changed*) dan 4728 (*A member was added to a security-enabled global* group). Aktivitas dilakukan oleh *user* admin ke user1 dan user2. Dengan adanya korelasi,

yaitu event ID 4728, di mana user1 dimasukkan ke suatu *security group* sebagai *high privileged user*.

Melalui penanganan insiden, didapatkan pemahaman mendalam mengenai pentingnya korelasi log dari berbagai sumber. Kasus yang melibatkan deteksi Event ID 4737 (*Security enabled global group changed*) secara spesifik menyoroti bagaimana sebuah perubahan yang tampak sederhana pada keanggotaan grup di sistem dapat menjadi indikator awal aktivitas mencurigakan yang berpotensi mengarah pada eskalasi hak akses yang tidak sah. Investigasi lebih lanjut seringkali memerlukan korelasi *log Event ID* 4737 dengan *log* aktivitas *user* (seperti logon events atau process creation) dan *log* perubahan konfigurasi sistem. Pendekatan ini memungkinkan identifikasi pola anomali atau urutan kejadian yang mengindikasikan upaya lateral movement atau privilege escalation. Oleh karena itu, case ini juga menunjukkan krusialnya dokumentasi yang akurat dan konfirmasi terhadap setiap aktivitas administratif yang melibatkan perubahan grup keamanan pada sistem, guna memvalidasi legitimasi perubahan tersebut dan meminimalisir risiko akses yang tidak sah.

3.3.3 *System Availability Monitoring*

Selain melakukan pemantauan terhadap aktivitas keamanan dan alarm yang muncul dari sistem *log*, proses *monitoring* di SOC juga mencakup pengawasan terhadap status dan ketersediaan perangkat keamanan yang terpasang di sisi klien. Aktivitas ini dikenal sebagai *system availability monitoring*, yang bertujuan untuk memastikan bahwa seluruh perangkat keamanan seperti *agent endpoint*, *firewall*, *intrusion detection system (IDS/NIDS)*, serta *log forwarder* berjalan normal dan mengirimkan data secara konsisten.

Sistem *monitoring* ketersediaan ini dilakukan melalui *platform* Thruk, yang menampilkan status konektivitas dan respons perangkat yang dimonitor secara *real-time*. Thruk menunjukkan status seperti *OK*, *Warning*, atau *Critical*, tergantung apakah perangkat aktif dan mengirimkan data log sesuai yang diharapkan. Ketika salah satu perangkat terpantau dalam kondisi tidak aktif, terputus koneksi, atau tidak mengirimkan *log* dalam rentang waktu tertentu, maka kondisi tersebut dianggap sebagai potensi insiden operasional dan perlu ditindaklanjuti.

Jika terdapat perangkat yang tidak tersedia atau berhenti berfungsi, langkah selanjutnya adalah melakukan eskalasi sesuai dengan kategori perangkat dan sistem yang terhubung. Misalnya, jika perangkat yang bermasalah adalah bagian dari *log*

forwarding endpoint, maka insiden dieskalasi ke tim *sysadmin* atau klien terkait. Namun apabila yang terdampak adalah perangkat yang kritikal atau berdampak langsung terhadap fungsionalitas SOC, maka eskalasi diteruskan kepada *senior security analyst* untuk langkah teknis lanjutan.

Aspek *system availability monitoring* menunjukkan bahwa pendekatan proaktif sangat krusial. Tidak hanya memastikan sistem berjalan, tetapi juga mendeteksi anomali kinerja yang mungkin mengindikasikan serangan *Denial of Service* atau masalah infrastruktur kritis. Pemantauan ini berfungsi sebagai lapisan pertahanan awal yang mendukung operasi keamanan secara keseluruhan.

3.4 Kendala dan Solusi yang Ditemukan

Selama program magang berlangsung, terdapat beberapa kendala yang dihadapi, baik itu besar maupun kecil. Kendala yang dihadapi selama proses kegiatan kerja magang ini adalah:

1. Penggunaan *monitoring system* sangat bervariasi berdasarkan perangkat keamanan yang terhubung pada setiap klien, sehingga *treatment* yang dilakukan berbeda pada setiap sistemnya.
2. Kurangnya *hands-on training* dalam menotifikasi, sehingga memakan banyak waktu saat awal masuk operasional

Dari berbagai kendala yang dihadapi selama proses kegiatan kerja magang, berikut adalah solusi yang ditemukan untuk menanganinya:

1. Membaca *playbook* secara menyeluruh, mempelajari sistem aset dan segmentasi klien, serta bertanya kepada tim untuk memahami konteks insiden klien terkait.
2. Komunikasi secara intensif dengan tim dan mempelajari melalui dokumentasi notifikasi sebelumnya