BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama kegiatan magang, posisi yang dijalani adalah sebagai SOC Analyst Level 1 (SOC L1) di bawah divisi Security Operation Center pada PT. Sembilan Pilar Semesta. Seluruh aktivitas magang berada di bawah arahan langsung dari Ibu Julia selaku SOC L2, serta berkoordinasi dengan tim keamanan siber lainnya.

Koordinasi rutin dilakukan melalui briefing pada awal shift, yang berfungsi sebagai proses *handover* antara tim shift sebelumnya dengan shift yang bertugas. Pada sesi ini, informasi mengenai *alert* yang belum terselesaikan, aktivitas yang masih perlu dipantau, serta potensi ancaman yang memerlukan perhatian khusus disampaikan secara terstruktur agar kesinambungan *monitoring* tetap terjaga. Sementara itu, pada akhir shift, dilakukan pembuatan rekapitulasi harian berupa daftar *alert* yang telah dianalisis, status tindak lanjut, dan rekomendasi tindakan. Rekap ini kemudian dikirimkan melalui grup WhatsApp internal sebagai dokumentasi serta media pelaporan kondisi keamanan harian kepada pihak terkait.

Dalam pelaksanaan tugasnya, SOC L1 juga melakukan komunikasi eksternal dan internal yang bersifat operasional. Komunikasi internal dilakukan melalui diskusi aktif dengan sesama analis L1 untuk melakukan validasi dan konfirmasi terhadap alert yang ditemukan, terutama jika terdapat indikasi anomali yang memerlukan perspektif tambahan. Jika hasil analisis awal menunjukkan adanya ancaman dengan tingkat risiko yang lebih tinggi atau memerlukan investigasi teknis lebih mendalam, *alert* tersebut diekskalasikan kepada SOC Level 2 (L2) untuk dilakukan analisis lanjutan dan penentuan tindakan respons yang sesuai.

Selain koordinasi internal, SOC L1 juga bertanggung jawab menyusun laporan insiden untuk pihak client, yang berisi ringkasan *alert* mereka, serta rekomendasi awal untuk mitigasi risiko. Laporan ini menjadi bagian penting dari komunikasi profesional antara perusahaan dan client, sekaligus memastikan bahwa setiap ancaman yang teridentifikasi tercatat dan dipahami oleh pihak terkait.

3.2 Tugas yang Dilakukan

Selama menjalani kegiatan magang, tanggung jawab yang diberikan berfokus pada proses monitoring, analisis, dan pelaporan aktivitas keamanan siber menggunakan platform *Stellar Cyber*. Sebagai SOC Analyst Level 1, tugas utama adalah melakukan pemantauan awal terhadap *alert* yang terdeteksi pada sistem, mengidentifikasi potensi ancaman, serta memastikan eskalasi dilakukan sesuai prosedur apabila ditemukan indikasi insiden yang memerlukan penanganan lebih lanjut. Adapun tugas-tugas yang dilakukan antara lain sebagai berikut:

1. Memantau *alert* keamanan secara real-time pada platform Stellar.
2. Menganalisis tingkat keparahan alert untuk menentukan validitas ancaman.
3. Melakukan eskalasi alert ke SOC Level 2 bila diperlukan.
4. Membuat rekap dan laporan harian alert untuk dokumentasi operasional.
5. Melaksanakan handover pada awal dan akhir shift untuk penyampaian status alert.
6. Menyusun laporan insiden untuk client terkait ancaman yang terdeteksi.
7. Mendokumentasikan seluruh aktivitas analisis sebagai arsip dan referensi.

3.3 Uraian Pelaksanaan Magang

Selama masa kerja magang yang berlangsung dari tanggal 26 Agustus 2025 hingga Feburari 2026, penugasan difokuskan pada peran sebagai SOC Analyst Level 1. Kegiatan utama yang dilakukan meliputi proses monitoring, analisis awal, dan pelaporan alert keamanan yang terdeteksi melalui platform Stellar Cyber. Tugas-tugas tersebut mencakup identifikasi aktivitas mencurigakan, validasi tingkat ancaman, serta eskalasi insiden apabila ditemukan potensi serangan yang memerlukan penanganan lanjutan oleh tim SOC Level 2. Selain itu, dilakukan pula penyusunan laporan harian dan laporan insiden untuk memastikan setiap temuan keamanan terdokumentasi dengan baik dan dapat ditindaklanjuti sesuai prosedur. Pelaksanaan kerja magang dirinci dalam tabel di bawah ini

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

Minggu Ke -	Pekerjaan yang dilakukan
1	Melakukan pengenalan lingkungan kerja SOC, memahami alur operasi keamanan siber, mempelajari penggunaan Stellar Cyber sebagai platform monitoring, serta memahami kebijakan, prosedur, dan aturan keamanan masing-masing *tenant/client*.
2 - 16	Melakukan monitoring alert keamanan menggunakan Stellar Cyber, menganalisis tingkat risiko setiap *alert* yang muncul, melakukan eskalasi ke L2 apabila diperlukan, serta menyusun laporan dan ticketing sebagai dokumentasi hasil pemantauan.

Selama pelaksanaan kegiatan magang, terdapat serangkaian aktivitas operasional yang dijalankan secara konsisten dalam kurun waktu enam belas minggu di lingkungan *Security Operation Center (SOC)*. Aktivitas tersebut berfokus pada proses pemantauan keamanan siber *(security monitoring)*, analisis alert yang terdeteksi pada sistem, eskalasi insiden kepada tim Level 2 apabila ditemukan potensi ancaman yang membutuhkan penanganan lanjutan, serta pembuatan laporan sebagai dokumentasi dan pelacakan insiden keamanan. Seluruh kegiatan operasional menggunakan platform Stellar Cyber, yang berfungsi sebagai sistem deteksi dan respons ancaman berbasis *Open Extended Detection and Response (Open XDR)*.

Pada minggu pertama, kegiatan difokuskan pada proses pengenalan lingkungan kerja SOC, pemahaman alur operasional keamanan informasi, serta pengenalan fitur-fitur dasar pada Stellar Cyber. Selain itu, dilakukan pembelajaran terkait prosedur kerja, kebijakan keamanan, aturan penanganan insiden, serta karakteristik dan kebutuhan keamanan masing-masing tenant atau client yang menjadi objek pemantauan.

Memasuki minggu kedua hingga minggu keenam belas, kegiatan magang berfokus pada operasional inti SOC Level 1. Aktivitas yang dilakukan meliputi pemantauan *alert* keamanan secara real-time melalui Stellar Cyber, melakukan analisis awal terhadap setiap *alert* yang muncul untuk menentukan tingkat urgensi dan klasifikasinya, serta memastikan apakah alert tersebut merupakan *false positive* atau mengindikasikan ancaman nyata *(true positive)*. Apabila ditemukan indikator serangan atau aktivitas mencurigakan yang berada di luar kewenangan SOC Level

1, maka dilakukan proses eskalasi kepada tim SOC Level 2 untuk dilakukan investigasi lebih lanjut. Selain itu, dilakukan pembuatan laporan insiden dan ticketing sebagai dokumentasi formal yang dilaporkan kepada pihak terkait, baik secara internal maupun kepada *client*, guna memastikan setiap insiden tercatat, dapat ditindaklanjuti, dan dipantau perkembangannya.

Selama periode tersebut, kegiatan monitoring, analisis, eskalasi, dan pelaporan dilakukan secara berulang dan berkesinambungan sesuai dengan *Standard Operating Procedure* yang berlaku. Meskipun tugas yang dilakukan relatif sama setiap minggunya, variasi terdapat pada jenis *alert*, tingkat risiko, frekuensi insiden, serta pola ancaman yang muncul pada masing-masing tenant. Pola kerja yang konsisten ini merupakan karakteristik utama operasional SOC L1, di mana kontinuitas pemantauan menjadi faktor penting dalam menjaga keamanan aset digital dan mencegah potensi serangan siber yang dapat merugikan perusahaan maupun *client* yang diawasi.

3.3.1 Stellar Cyber

A Pengertian Stellar Cyber

Stellar Cyber merupakan platform yang dirancang khusus untuk memberikan pendekatan yang mudah digunakan untuk mempertahankan seluruh serangan yang terjadi. Stellar juga dirancang untuk menggabungkan analisis keamanan, deteksi ancaman, dan tindakan respon keamanan di dalam satu platform. Hal ini memungkinkan tim SOC dapat segera mendapatkan nilai skor berdasarkan tingkatan ancaman di setiap insiden anomali yang terdeteksi oleh Stellar. Platform ini dirancang untuk memudahkan penggunaan keamanan data dari berbagai jaringan, *endpoint*, dan *log* dalam satu tempat penyimpanan dan juga Stellar Cyber menggunakan mesin pendeteksi ancaman berbasis machine learning untuk mendeteksi dan memberikan alert secara otomatis, sehingga meningkatkan efisiensi dan akurasi dalam deteksi ancaman.[3]

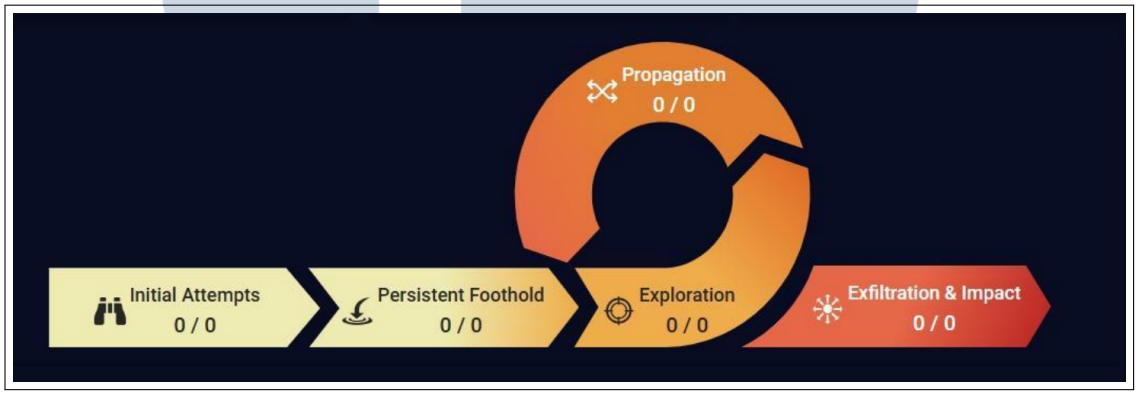
B Open XDR Sebagai Arsitektur dalam Stellar Cyber

Open XDR (Extended Detection and Response) adalah sebuah solusi keamanan siber yang dikembangkan untuk mendeteksi, menyelidiki, dan merespon serangan siber dengan cara mengintegrasikan data dari berbagai sumber keamanan yang berbeda. XDR bekerja dengan memperluas cakupan sistem threat detection

dan incident response yang mencakup lebih dari satu jenis perangkat atau sistem. Tujuan utama dari konsep ini adalah membantu organisasi memperoleh pemahaman yang lebih mendalam terkait ancaman yang ada serta meningkatkan efektivitas dalam menangani serangan siber yang kompleks.

C Peran XDR Kill Chain dalam Sistem Analisis Stellar Cyber

XDR Kill Chain mengidentifikasi lima tahap pada serangan siber yang terjadi dengan masing masing taktik dan teknik terkaitnya yang diambil berdasarkan pada *MITRE ATTCK* di mana setiap aktivitas anomali yang terdeteksi oleh Stellar telah difilter berdasarkan tahapan yang dimiliki *XDR Kill Chain*.



Gambar 3.1. XDR Kill Chain
Sumber:[4]

Menurut *Stellar Documentation* pada tools Stellar Cyber, *XDR Kill Chain* tersebut terdapat beberapa tahapan, seperti :

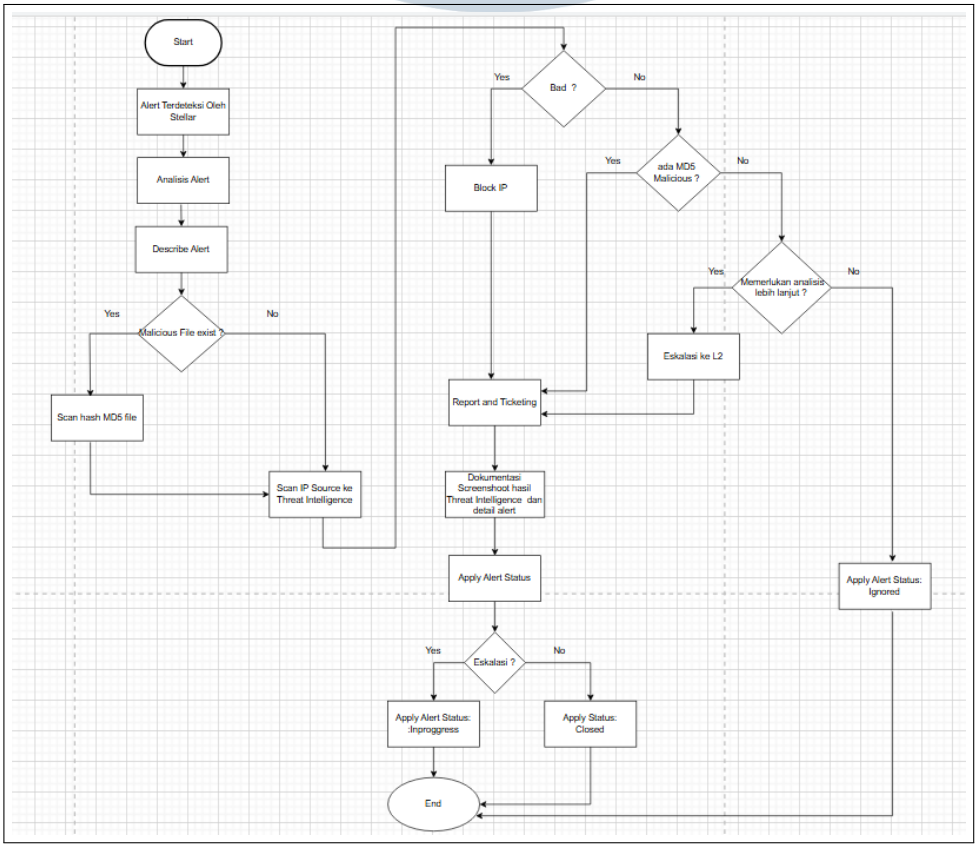
1. *Initial Attempts* merupakan tahapan awal di mana penyerang mulai mencoba masuk ke dalam sistem target.
2. *Persistent Foothold* merupakan tahapan di mana penyerang berhasil memperoleh akses, dan berusaha mempertahankannya agar tetap masuk ke sistem.
3. *Exploration* merupakan tahapan di mana penyerang sedang mempelajari, menelusuri dan memeriksa data sensitif yang tersimpan pada sistem maupun area yang rentan.
4. *Propagation* merupakan tahapan di mana penyerang berusaha meningkatkan hak akses *(Privilege Escalation)* agar dapat memperluas kendali atas sistem.

5. *Exfiltration and Impact* merupakan tahapan akhir di mana penyerang mencoba mengambil data sensitif bahkan merusak sistem.

Adanya loop antara tahap *Exploration* dan *Propagation* menggambarkan bahwa ketika penyerang tidak menemukan data ataupun akses yang diinginkan pada tahap *Propagation*, mereka dapat kembali ke tahap *Exploration* untuk mencari data sensitif lain ataupun titik rentan sebelum ke tahap terakhir yaitu *Exfiltration and Impact*.

3.3.2 Flowchart SOC Analyst

Flowchart berikut menggambarkan alur kerja (workflow) operasional seorang SOC Level 1 (L1) dalam menangani alert keamanan yang muncul pada platform Stellar Cyber. Flowchart ini berfungsi untuk memperjelas proses bisnis yang dilakukan mulai dari tahap deteksi *alert*, analisis awal, hingga penentuan langkah lanjut berupa ignorasi, eskalasi, ataupun pembuatan tiket insiden. Melalui alur ini, setiap aktivitas L1 terdokumentasi secara terstruktur sehingga mudah dipahami bagaimana sebuah *alert* diproses dari awal hingga selesai.



Gambar 3.2. Flowchart Alur Kerja SOC L1

Gambar 3.2 merupakan gambar *flowchart* yang menunjukkan *workflow* SOC L1. Pada tahap awal, sistem Stellar mendeteksi adanya aktivitas mencurigakan yang mengindikasikan potensi ancaman keamanan. Setelah *alert* tersebut muncul, SOC L1 melakukan analisis awal (*alert analysis*) untuk memahami konteks kejadian, kemudian dilanjutkan dengan proses *describe alert* guna mengidentifikasi detail teknis insiden.

Pada tahap ini, SOC L1 melakukan pengecekan apakah terdapat file yang terindikasi berbahaya (*malicious file exist*). Jika file terdeteksi, maka SOC L1 melakukan pemindaian hash *MD5* file tersebut menggunakan sumber *threat intelligence* seperti *VirusTotal*. Sebaliknya, jika tidak ditemukan file berbahaya, maka SOC L1 melakukan analisis terhadap *IP* sumber dengan mencocokkannya ke *threat intelligence* untuk mengetahui reputasi *IP* tersebut.

Setelah proses validasi awal selesai, SOC L1 melakukan penilaian apakah aktivitas yang terdeteksi tergolong berbahaya (*Bad?*). Jika aktivitas dinyatakan berbahaya, maka SOC L1 segera melakukan tindakan mitigasi berupa pemblokiran *IP* sumber (*Block IP*). Jika aktivitas tidak langsung dikategorikan berbahaya, SOC L1 akan mengecek apakah hash *MD5* yang terdeteksi memiliki status *malicious*. Apabila *MD5* terkonfirmasi berbahaya, maka proses dilanjutkan ke tahap pelaporan dan pembuatan tiket.

Namun, apabila hasil pengecekan *MD5* belum memberikan kesimpulan yang jelas, SOC L1 akan menentukan apakah insiden tersebut memerlukan analisis lebih lanjut. Jika ya, maka insiden akan dieskalasikan ke tim SOC L2 untuk investigasi lanjutan. Jika tidak, maka *alert* dapat diabaikan (*ignored*) dan status *alert* diperbarui sesuai kebijakan.

Selanjutnya, untuk insiden yang terbukti valid, SOC L1 melakukan proses *report and ticketing* sebagai bentuk dokumentasi resmi. SOC L1 juga melakukan dokumentasi berupa pengambilan *screenshot* hasil *threat intelligence* serta mencatat detail *alert* sebagai bukti pendukung investigasi. Setelah itu, status *alert* pada sistem Stellar diperbarui (*apply alert status*).

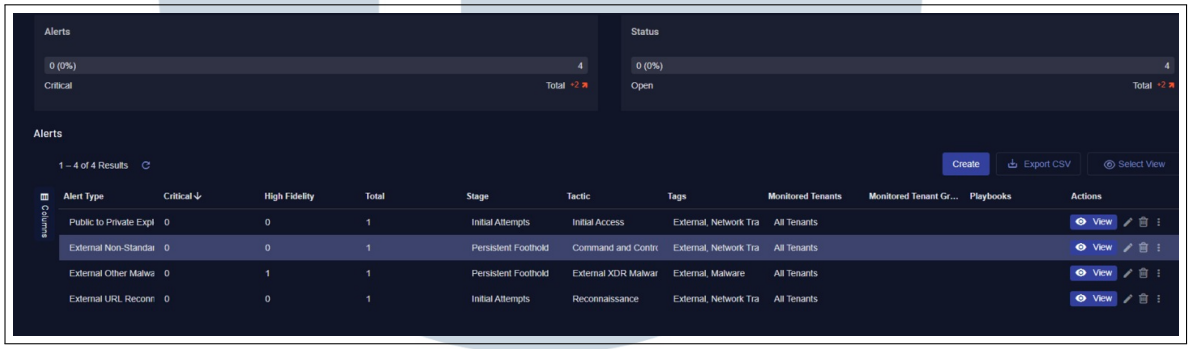
Pada tahap akhir, SOC L1 menentukan apakah insiden perlu dilakukan eskalasi lanjutan. Jika eskalasi diperlukan, maka status *alert* diubah menjadi *In Progress* sebagai penanda bahwa insiden masih dalam proses penanganan. Jika tidak diperlukan eskalasi lanjutan, maka status *alert* diubah menjadi *Closed*. Semua tindakan ini dilakukan secara terstruktur agar insiden tercatat dengan baik dan dapat dievaluasi atau diekskalasi ke tim L2 atau L3 apabila diperlukan.

3.4 Proses Monitoring dan Analisis Ancaman

3.4.1 Analysis Alert

A Dashboard Alert

Berikut merupakan tampilan dashboard Alerts pada platform Stellar Cyber yang digunakan untuk memantau setiap aktivitas mencurigakan yang terdeteksi pada lingkungan tenant. *Dashboard* ini menjadi titik awal bagi analis untuk mengidentifikasi jenis ancaman, tingkat keparahan, serta tahapan serangan dalam kill chain sebelum dilakukan analisis lebih lanjut.



Gambar 3.3. Dashboard Alert

Gambar 3.3 menunjukkan tampilan *dashboard alert* stellar. Pada *dashboard* tersebut, sistem menampilkan rangkuman seluruh *alert* yang muncul dalam periode waktu yang telah ditentukan. Di bagian atas terlihat ringkasan jumlah *alert* berdasarkan tingkat keparahan *(severity)* dan status penanganannya.

Di bawah ringkasan tersebut, ada tabel utama yang berisi daftar *alert* lengkap beserta detail informasi yang menjadi dasar investigasi awal. Setiap *alert* dilengkapi dengan jenis aktivitas yang terdeteksi, tingkat kritikalitas, serta *High Fidelity* yang menggambarkan tingkat keyakinan sistem terhadap kebenaran temuan tersebut. Kolom Stage menunjukkan tahapan ancaman dalam attack chain, seperti *Initial Attempts* atau *Persistent Foothold*, sementara Tactic mengindikasikan taktik serangan berdasarkan *MITRE ATTCK*, misalnya *Initial Access, Command and Control, atau Reconnaissance, dll.*

Informasi tambahan seperti Tags membantu mengidentifikasi kategori ancamannya, dan Monitored Tenants menunjukkan tenant mana yang terdampak. Melalui tampilan ini, analis dapat dengan cepat menilai prioritas penanganan, mengakses detail *alert*, menentukan apakah sebuah event merupakan *true positive* atau *false positive*, serta melanjutkan proses investigasi sesuai prosedur SOC.

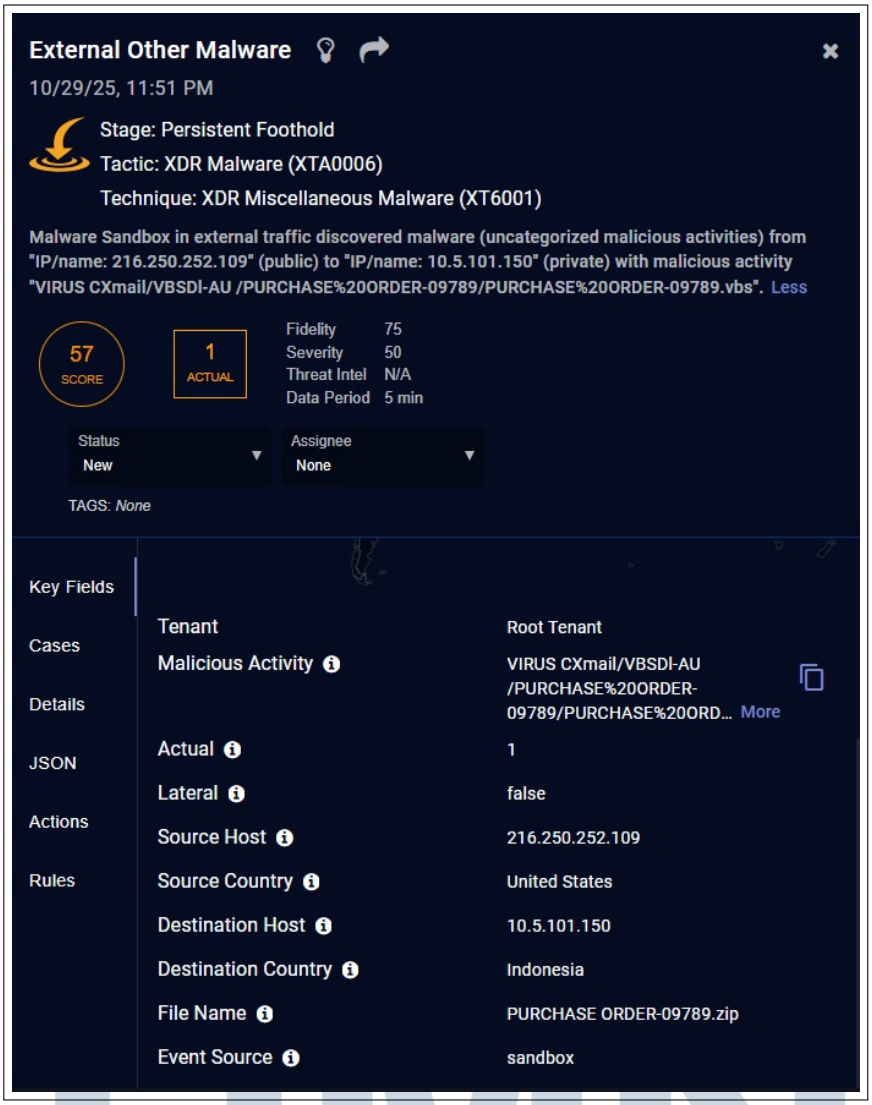
B Alert Details

Setelah memilih salah satu *alert* pada daftar utama, sistem akan menampilkan halaman detail *alert* seperti pada gambar berikut. Tampilan ini menyajikan informasi lengkap mengenai insiden yang terdeteksi—mulai dari tahap serangan, taktik yang digunakan, skor ancaman, hingga atribut teknis seperti alamat IP sumber dan tujuan, negara asal trafik, file yang terlibat, serta metadata pendukung lainnya. Halaman inilah yang menjadi dasar bagi analis SOC dalam melakukan investigasi lebih dalam terhadap setiap aktivitas yang terindikasi berbahaya.

Gambar 3.4. Alert Detail

Gambar 3.5. Alert Detail

Gambar 3.4 dan Gambar 3.5 menunjukkan rincian teknis dari *alert* yang terdeteksi. Informasi yang ditampilkan mencakup waktu kejadian, tingkat keparahan (alert score), reputasi sumber dan tujuan, *port* yang digunakan, aplikasi yang terlibat (dalam hal ini SMTP), hingga status sesi koneksi. Dari data tersebut, analis dapat memahami karakteristik awal serangan, memvalidasi potensi ancaman, serta menentukan langkah tindak lanjut.



Gambar 3.6. Alert Info

Gambar 3.6 merupakan tampilan More Info dari *alert* yang dianalisis. *Alert* ini termasuk kategori *External Other Malware*. Alert ini terjadi karena Stellar Cyber mendeteksi adanya aktivitas mencurigakan berupa pengiriman file yang berpotensi berbahaya melalui protokol SMTP (port 25), yang umumnya digunakan untuk proses pengiriman email. Aktivitas tersebut berasal dari alamat IP publik 216.250.252.109 yang berlokasi di Amerika Serikat, dan ditujukan menuju salah satu host internal.

Stellar juga mengidentifikasi bahwa paket data yang dikirim membawa lampiran bernama PURCHASE ORDER-09789.zip. Penamaan file yang menyerupai dokumen transaksi bisnis seperti *purchase order* merupakan teknik sosial yang sering digunakan dalam kampanye *phishing*, di mana pelaku

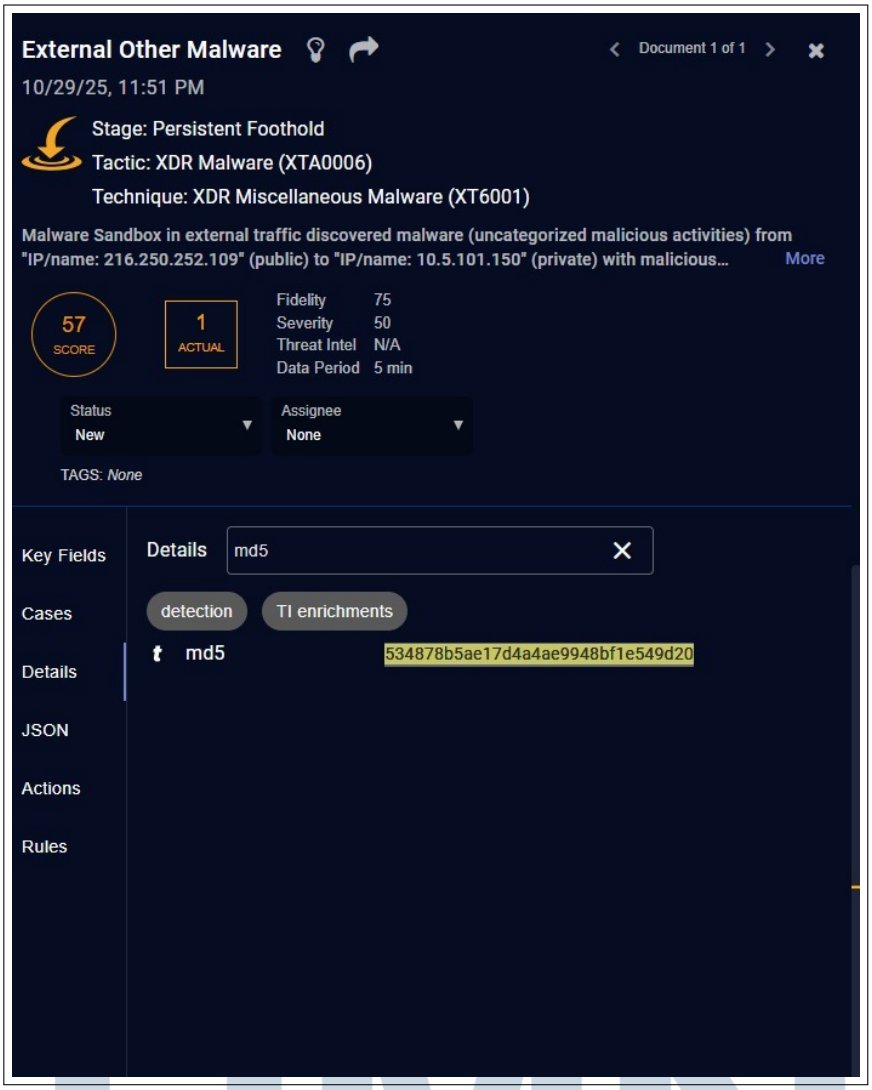
memanfaatkan istilah yang familiar agar korban terdorong untuk membuka file tersebut tanpa kecurigaan.

Setelah file diekstraksi dan dianalisis oleh modul *maltrace-cloud sandbox*, ditemukan bahwa ZIP tersebut berisi skrip *Visual Basic Script (.vbs)* bernama PURCHASE ORDER-09789.vbs. Sandbox kemudian memberikan *verdict* "VIRUS CXmail/VBSDl-AU", yang menunjukkan bahwa skrip ini termasuk dalam jenis *malware* berbasis email yang dirancang untuk menjalankan instruksi secara otomatis ketika dieksekusi pengguna. Format *.vbs* sendiri bukan sekadar *script* biasa, namun merupakan komponen *native* Windows yang mampu menjalankan perintah sistem, memanggil *PowerShell*, membuat koneksi jaringan, ataupun men-download *payload* tambahan. Karakteristik inilah yang menjadikan *.vbs* sebagai salah satu bentuk *malware loader* yang sering dipakai dalam tahap awal kompromi jaringan modern.

Meskipun status koneksi tercatat "Aborted", yang berarti tidak ada bukti kesinambungan proses atau eksekusi lanjutan pada *endpoint*, keberadaan file berbahaya yang telah terverifikasi oleh *sandbox* menjadikan *alert* ini sebagai *True Positive*. *Alert* ini telah memasuki tahap *Persistent Foothold* bukan hanya sekadar *Delivery*. Tahap ini menunjukkan bahwa aktor ancaman sudah berhasil memasukkan *script* awal berupa file *.vbs* ke dalam lingkungan target. File *.vbs* tersebut berperan sebagai pijakan awal yang dapat digunakan untuk mempertahankan akses, karena apabila dieksekusi oleh korban, *script* tersebut mampu mengunduh dan menjalankan *payload* tambahan, membuka koneksi *Command-and-Control (C2)*, atau melakukan modifikasi sistem yang memungkinkan penyerang tetap memiliki kendali walaupun sistem direstart atau dilakukan perubahan konfigurasi keamanan.

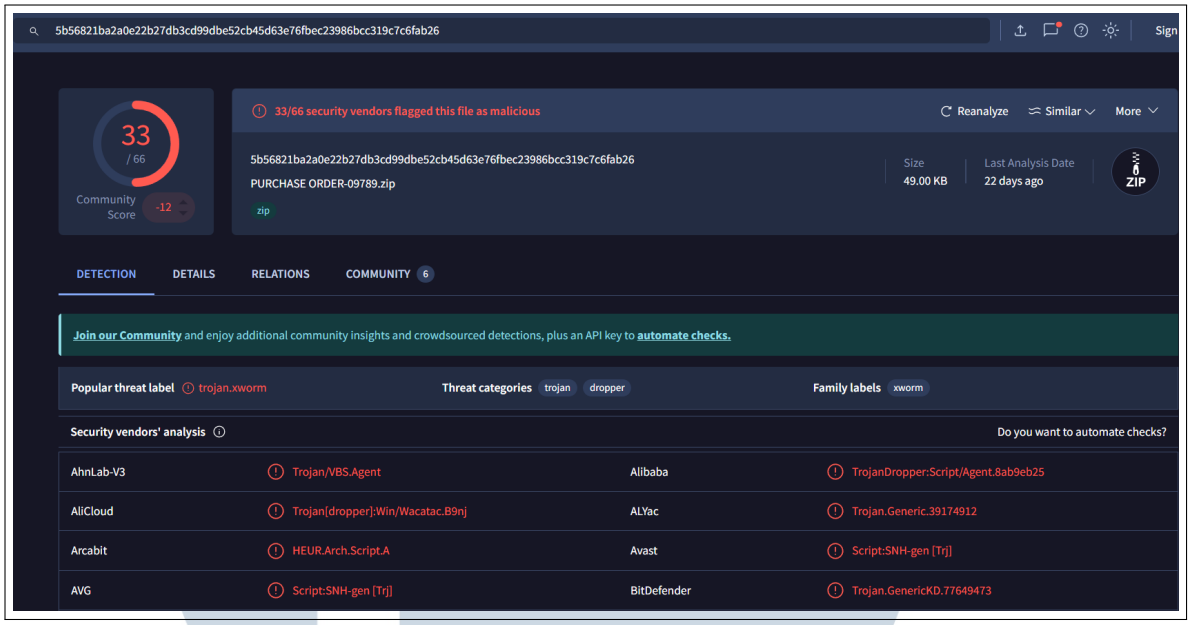
C Threat Intelligence Analysis

Selain melakukan analisis awal melalui menu Alert Details pada Stellar Cyber, proses investigasi juga dilengkapi dengan pengecekan menggunakan berbagai sumber *threat intelligence* eksternal. Langkah ini dilakukan untuk memvalidasi tingkat bahaya artefak atau alamat IP yang terlibat, memastikan apakah komponen tersebut telah teridentifikasi sebagai ancaman oleh komunitas keamanan global. Analisis tambahan ini meliputi pemeriksaan hash file, reputasi alamat IP, serta indikasi aktivitas berbahaya lainnya melalui layanan seperti VirusTotal dan AbuseIPDB.



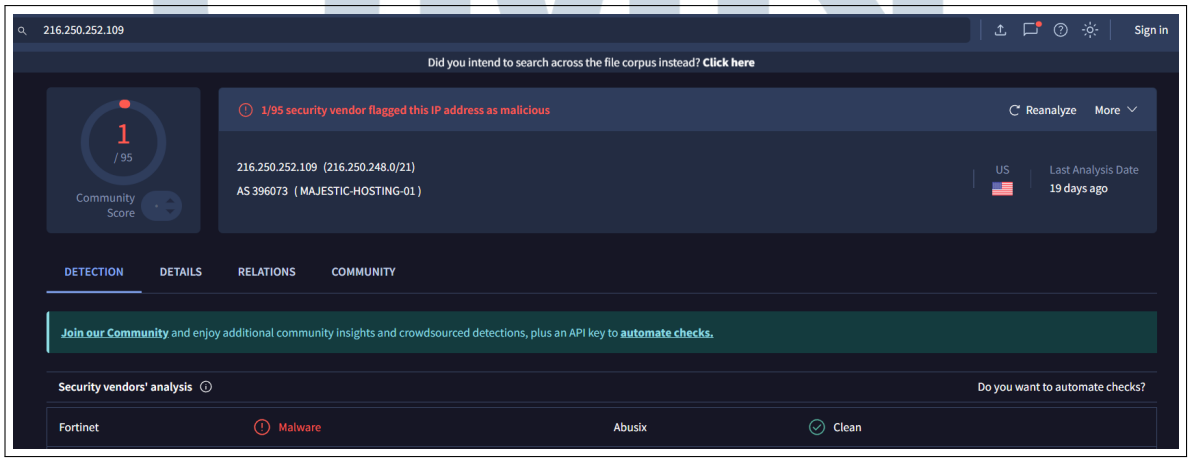
Gambar 3.7. Hash MD5

Pada gambar 3.7 terlihat bahwa sistem menampilkan *hash value* dari file yang terdeteksi, yaitu nilai MD5. *Hash* ini merupakan identifikasi unik dari file yang diduga berbahaya. Dengan adanya *hash* tersebut, analis dapat melakukan pemeriksaan lanjutan melalui layanan *Threat Intelligence* eksternal (seperti VirusTotal, AbuseIPDB, dan lainnya) untuk mengetahui apakah file tersebut sudah pernah dilaporkan sebagai *malware*, tingkat bahaya, serta reputasinya di berbagai vendor keamanan.



Gambar 3.8. Hasil Virustotal

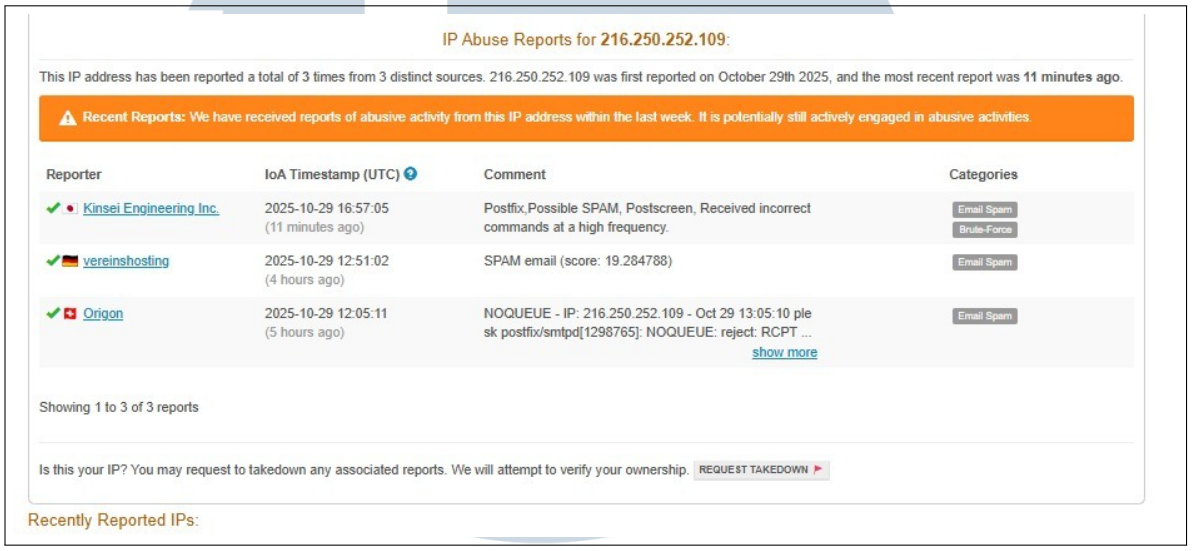
Gambar 3.8 menunjukkan hasil analisis hash file pada VirusTotal, di mana 33 dari 66 vendor keamanan mendeteksi file tersebut sebagai berbahaya. Mayoritas label deteksi mengindikasikan bahwa file tersebut merupakan *trojan* dengan kemampuan dropper, serta termasuk dalam keluarga *xWorm* yang dikenal sebagai *malware* berbasis *remote access*. Tingginya jumlah deteksi ini menegaskan bahwa file tersebut tidak aman dan berpotensi mengeksekusi kode berbahaya atau menurunkan *payload* tambahan. Oleh karena itu, file ini dikategorikan sebagai ancaman dan tidak boleh dijalankan pada lingkungan produksi maupun perangkat utama.



Gambar 3.9. Hasil Virustotal ip

Gambar 3.9 menampilkan hasil pemindaian alamat IP pada VirusTotal, di

mana hanya satu dari 95 vendor keamanan yang menandai IP tersebut sebagai berpotensi berbahaya. Meskipun tingkat deteksi sangat rendah, adanya satu vendor yang mengklasifikasikannya sebagai *malware* menunjukkan bahwa IP tersebut pernah terlibat dalam aktivitas mencurigakan atau memiliki reputasi yang tidak sepenuhnya bersih. Namun, sebagian besar vendor lainnya menilai IP tersebut aman, sehingga temuan ini perlu dikonfirmasi dengan sumber lain.



Gambar 3.10. Hasil AbuseIP

Gambar 3.10 kemudian mendukung temuan tersebut melalui laporan dari AbuseIPDB yang menunjukkan bahwa IP ini telah menerima beberapa laporan aktivitas penyalahgunaan. Jenis aktivitas yang dilaporkan meliputi *possible spam, postscreen errors*, dan *upaya brute-force*, yang menandakan bahwa IP tersebut pernah digunakan untuk mengirim spam atau melakukan percobaan akses yang tidak sah. Riwayat laporan yang masih baru menunjukkan bahwa IP ini kemungkinan masih digunakan dalam aktivitas yang tidak diinginkan. Secara keseluruhan, kedua platform memberikan indikasi bahwa meskipun tidak semua sistem keamanan mendeteksi ancaman, IP tersebut memiliki reputasi buruk dan perlu diwaspadai.

D Bloking IP

Gambar 3.11. Blocking IP

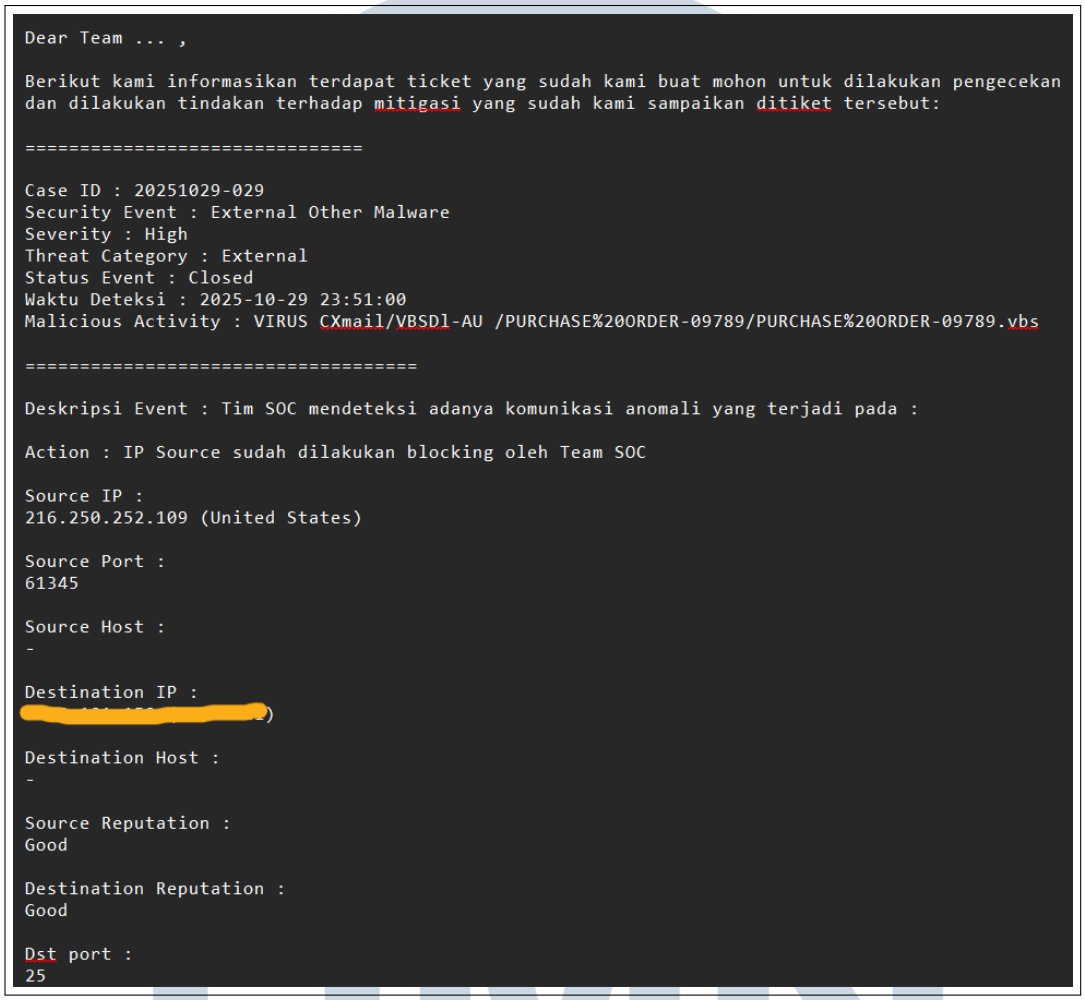
Gambar 3.11 memperlihatkan proses pemblokiran terhadap alamat IP yang telah terkonfirmasi sebagai sumber aktivitas *malware* berdasarkan hasil pemeriksaan pada berbagai platform *threat intelligence*. Setelah dilakukan korelasi dan verifikasi reputasi, IP tersebut diidentifikasi sebagai berbahaya sehingga perlu dilakukan tindakan pencegahan.

Pemblokiran diterapkan pada arah *incoming*, yang berarti seluruh koneksi masuk dari IP tersebut menuju jaringan internal akan dihentikan secara permanen. Langkah ini bertujuan untuk mencegah upaya komunikasi lebih lanjut, menghindari eksploitasi ulang, serta memutus potensi alur serangan yang dapat membahayakan aset internal organisasi. Dengan demikian, tindakan blocking ini menjadi salah satu bagian penting dari strategi mitigasi untuk menghentikan serangan sebelum menimbulkan dampak yang lebih luas.

3.4.2 Report dan Ticketing

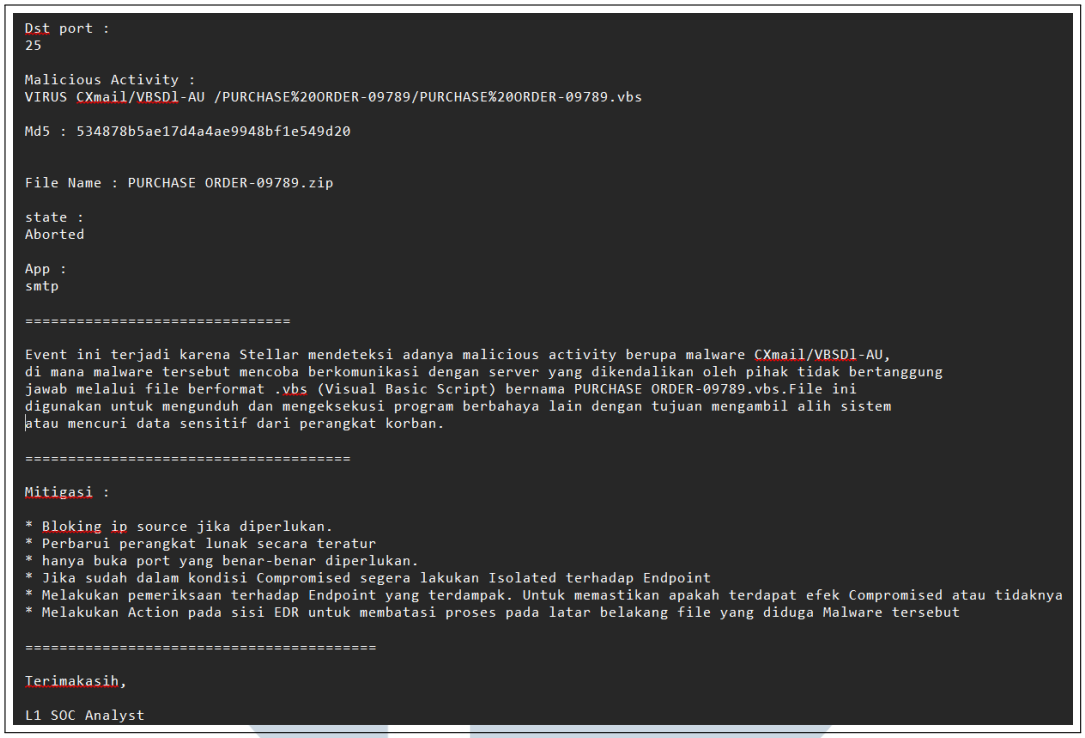
Tahapan ini merupakan langkah penting dalam alur kerja operasional SOC, karena setiap temuan harus didokumentasikan secara sistematis, dan diteruskan kepada tim yang bertanggung jawab untuk penanganan lebih lanjut. Melalui mekanisme pelaporan dan pembuatan tiket, seluruh informasi terkait insiden mulai dari kronologi, indikator ancaman, bukti teknis, hingga penjelasan alert dan

rekomendasi mitigasi dicatat secara lengkap agar proses respon insiden dapat berjalan secara detail dan terstruktur.



```
Dear Team ... ,

Berikut kami informasikan terdapat ticket yang sudah kami buat mohon untuk dilakukan pengecekan
dan dilakukan tindakan terhadap mitigasi yang sudah kami sampaikan ditiket tersebut:

================================

Case ID : 20251029-029
Security Event : External Other Malware
Severity : High
Threat Category : External
Status Event : Closed
Waktu Deteksi : 2025-10-29 23:51:00
Malicious Activity : VIRUS CXmail/VBSDl-AU /PURCHASE%20ORDER-09789/PURCHASE%20ORDER-09789.vbs

==================================

Deskripsi Event : Tim SOC mendeteksi adanya komunikasi anomali yang terjadi pada :

Action : IP Source sudah dilakukan blocking oleh Team SOC

Source IP :
216.250.252.109 (United States)

Source Port :
61345

Source Host :
-

Destination IP :
[redacted])

Destination Host :
-

Source Reputation :
Good

Destination Reputation :
Good

Dst port :
25
```

Gambar 3.12. Template Report Bagian 1



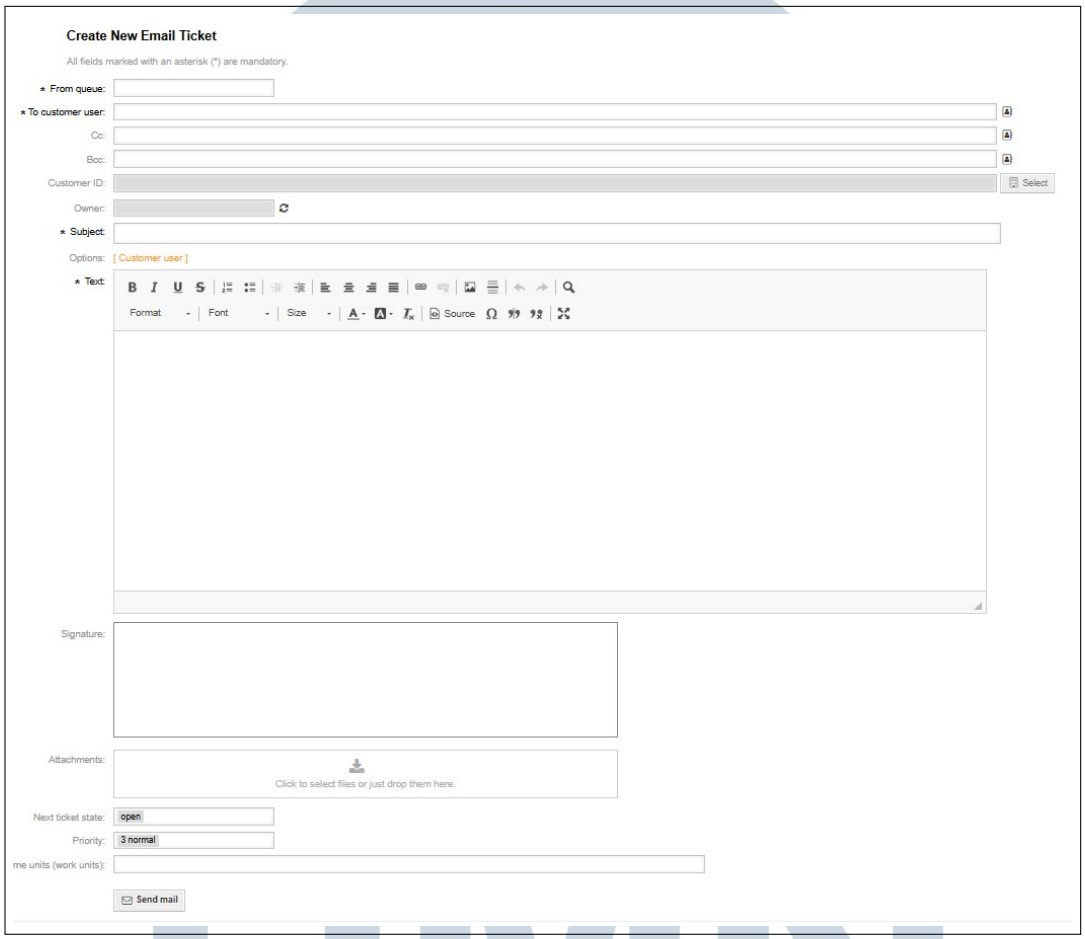
```
Dst port :
25

Malicious Activity :
VIRUS CXmail/VBSDl-AU /PURCHASE%20ORDER-09789/PURCHASE%20ORDER-09789.vbs

Md5 : 534878b5ae17d4a4ae9948bf1e549d20


File Name : PURCHASE ORDER-09789.zip

state :
Aborted

App :
smtp

==============================

Event ini terjadi karena Stellar mendeteksi adanya malicious activity berupa malware CXmail/VBSDl-AU,
di mana malware tersebut mencoba berkomunikasi dengan server yang dikendalikan oleh pihak tidak bertanggung
jawab melalui file berformat .vbs (Visual Basic Script) bernama PURCHASE ORDER-09789.vbs.File ini
digunakan untuk mengunduh dan mengeksekusi program berbahaya lain dengan tujuan mengambil alih sistem
atau mencuri data sensitif dari perangkat korban.

====================================

Mitigasi :

* Bloking ip source jika diperlukan.
* Perbarui perangkat lunak secara teratur
* hanya buka port yang benar-benar diperlukan.
* Jika sudah dalam kondisi Compromised segera lakukan Isolated terhadap Endpoint
* Melakukan pemeriksaan terhadap Endpoint yang terdampak. Untuk memastikan apakah terdapat efek Compromised atau tidaknya
* Melakukan Action pada sisi EDR untuk membatasi proses pada latar belakang file yang diduga Malware tersebut

========================================

Terimakasih,

L1 SOC Analyst
```

Gambar 3.13. Template Report Bagian 2

Gambar 3.12 dan 3.13 menunjukkan contoh isi report yang dikirimkan kepada client. Dokumen tersebut mencantumkan informasi penting seperti nama alert, waktu terdeteksi, tingkat keparahan, alamat IP yang terlibat, hash, serta ringkasan singkat mengenai penyebab munculnya alert dan langkah mitigasi yang perlu dilakukan untuk mencegah dampak yang lebih besar. Reason dan mitigation menjadi elemen yang sangat krusial, karena reason memberikan gambaran singkat tentang jenis serangan yang terjadi, bagaimana serangan tersebut berlangsung, serta faktor yang memungkinkan insiden tersebut muncul. Sementara itu, bagian mitigasi berisi langkah-langkah yang direkomendasikan untuk meminimalkan risiko dan mencegah insiden serupa di kemudian hari.

Pada proses penyusunan report, penting untuk memastikan bahwa seluruh informasi yang disampaikan akurat dan sesuai dengan kondisi serangan siber yang benar-benar terdeteksi.Dengan begitu, client, manajemen, maupun tim teknis dapat memahami konteks insiden serta mengetahui tindakan apa yang perlu dilakukan untuk mengurangi dampaknya. Report juga disertai dokumen pendukung seperti screenshot hasil analisis Threat Intelligence yang digunakan saat investigasi. Selain penyusunan report, SOC Analyst juga melakukan tindakan lanjutan berupa pemblokiran IP melalui Stellar Cyber, khususnya pada client tertentu yang memerlukan tindakan proteksi langsung terhadap sumber ancaman tersebut.

Setelah proses pelaporan (reporting) kepada client dilakukan, tahap selanjutnya adalah membuat tiket sebagai bentuk dokumentasi resmi dari insiden yang telah dianalisis.



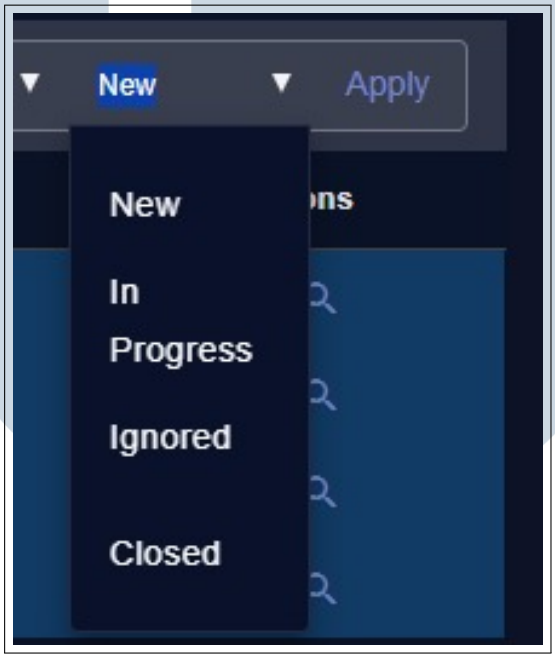
Gambar 3.14. Ticket Report

Gambar 3.14 menunjukkan tampilan formulir pembuatan tiket pada sistem ticketing. Pada tahap ini, SOC Analyst mengisi informasi penting seperti sumber antrian (queue), penerima tiket, subjek, serta penjelasan detail mengenai kejadian yang ditemukan. Bagian teks berfungsi sebagai ruang untuk merangkum jenis alert, waktu terjadinya, hasil analisis singkat, serta langkah mitigasi yang sudah atau perlu dilakukan.

Pembuatan tiket ini memastikan setiap insiden terdokumentasi dengan baik, memudahkan proses tracking, audit, dan tindak lanjut jika terjadi kejadian serupa di kemudian hari. Dengan adanya tiket, alur komunikasi antara SOC dan client menjadi lebih terstruktur dan transparan.

Setelah proses ticketing selesai dan seluruh informasi terkait insiden telah

terdokumentasi, langkah berikutnya adalah memperbarui status alert pada sistem. Pada tahap ini, status alert diubah dari “New” menjadi “Closed” sebagai penanda bahwa investigasi telah dilakukan, laporan sudah dikirimkan kepada client, dan tindak lanjut yang diperlukan telah dicatat melalui tiket. Pengubahan status ini penting untuk menjaga kerapihan monitoring, menghindari duplikasi pekerjaan, serta memastikan bahwa setiap alert ditangani hingga selesai sesuai prosedur.



Gambar 3.15. Status Apply

Gambar 3.15 menunjukkan bahwa status alert telah diubah dari “New” menjadi “Closed”. Perubahan status ini menandakan bahwa seluruh proses penanganan telah selesai dilakukan, mulai dari analisis, pembuatan report, hingga pembuatan ticket untuk client. Dengan ditutupnya alert tersebut, sistem mencatat bahwa insiden sudah ditangani secara tuntas dan tidak memerlukan tindakan lanjutan, sehingga membantu menjaga ketertiban alur kerja dan memastikan tidak ada alert yang tertinggal.

3.5 Kendala dan Solusi yang Ditemukan

A Kendala yang Ditemukan

Selama pelaksanaan kegiatan pemantauan dan analisis keamanan siber, terdapat beberapa kendala yang dihadapi dalam proses identifikasi dan penanganan insiden. Kendala-kendala ini muncul sebagai bagian dari dinamika operasional

Security Operation Center (SOC) yang menangani berbagai jenis alert dengan tingkat kompleksitas yang berbeda-beda.

1. Kompleksitas Serangan Siber. Banyak alert memiliki pola serangan yang rumit sehingga membutuhkan analisis lebih mendalam untuk memastikan jenis ancaman dan langkah mitigasinya.
2. Pemenuhan SLA. Batas waktu penanganan yang ketat menjadi tantangan, terutama saat volume alert meningkat atau analisis membutuhkan data tambahan.
3. Kinerja PC Lambat. PC yang lemot atau not responding memperlambat proses investigasi, akses dashboard, hingga pembuatan laporan.
4. Konflik VPN antar Tenant. Beberapa VPN tenant saling bertabrakan sehingga hanya satu yang dapat aktif dalam satu waktu, membuat perpindahan tenant menjadi lambat.

B Solusi yang Ditemukan

Untuk mengatasi kendala yang ditemukan selama proses pemantauan dan analisis keamanan siber, beberapa solusi diterapkan guna meningkatkan efektivitas analisis alert serta memastikan penanganan insiden dapat dilakukan secara tepat dan efisien.

1. Melakukan pemeriksaan menggunakan beberapa threat intelligence, memahami pola serangan umum, serta berkonsultasi dengan L2/L3 untuk mempercepat validasi dan memastikan akurasi analisis.
2. Mengutamakan alert berdasarkan prioritas, menggunakan template analisis/reporting agar lebih cepat, dan melakukan eskalasi lebih awal jika ditemukan indikasi ancaman tinggi.
3. Melakukan restart pada masing-masing PC setelah selesai digunakan.
4. Menggunakan tambahan device untuk mengakses beberapa tenant tertentu.