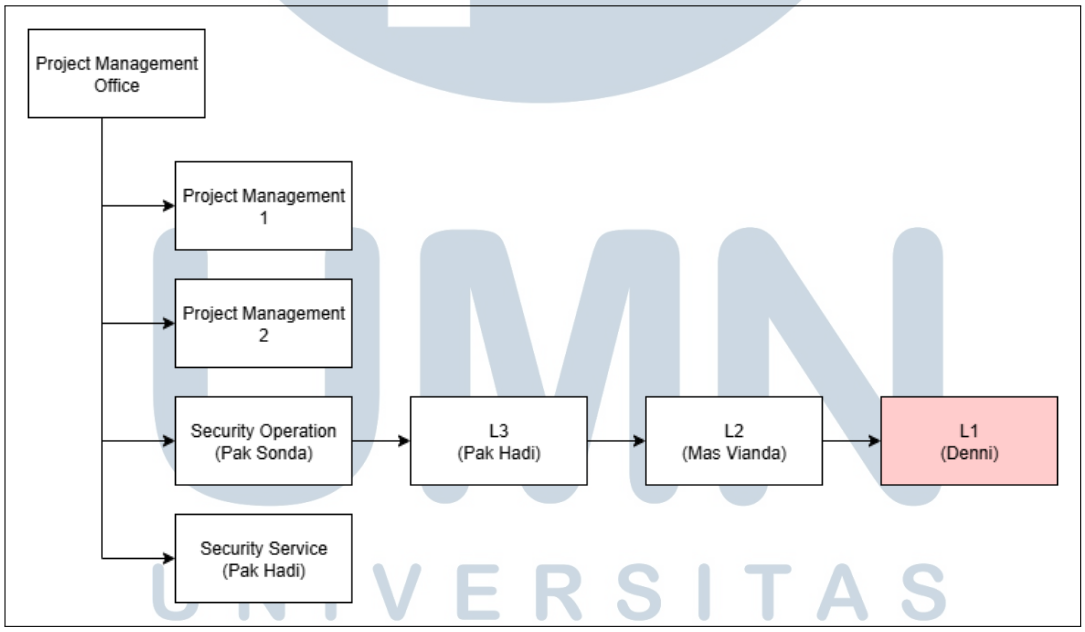
BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Pelaksanaan program magang di PT Visionet Data Internasional dilakukan pada divisi *Security Operation Center* (SOC) Level 1, di bawah supervisi Bapak Hadi Ismanto selaku Kepala Departemen *Security Services*. Divisi SOC memiliki tanggung jawab utama untuk melakukan pengawasan, analisis, dan pelaporan terhadap *alert* yang muncul dari sistem SIEM dan EDR kepada PIC klien yang bersangkutan. Untuk meningkatkan koordinasi antar anggota SOC dilakukan *weekly meeting via Microsoft Teams* setiap hari Senin pukul 14.00 dimana satu atau dua anggota SOC melakukan *sharing session* berupa presentasi hal yang menarik bagi mereka atau bermanfaat untuk anggota SOC yang lain. Gambar 3.1 merupakan struktur subdivisi dari divisi *Project Management Office*.



Gambar 3.1. Struktur Divisi *Project Management Office*

SOC L1 memiliki beberapa tugas rutin yang perlu dilakukan setiap hari, salah satunya adalah melaporkan agen Visionet dan Lippo-Karawaci yang terputus dari *server* Wazuh maupun SentinelOne setiap pukul 10.00 ke grup WhatsApp masing-masing. Selain itu, pada pukul 14.00, dilakukan pelaporan khusus untuk agen Cinepolis yang terputus dari *server* Wazuh kepada PIC Cinepolis.

Untuk tugas mingguan, SOC L1 bertanggung jawab menyusun dan mengirimkan laporan yang berisi rekap *alert*, penambahan agen baru, dan penghapusan agen yang sudah tidak dipakai yang terdeteksi di SentinelOne selama 7 hari terakhir. Laporan ini disampaikan setiap hari Jumat sebelum pukul 12.00 kepada Bapak Hadi Ismanto selaku Kepala Departemen *Security Services*.

3.2 Tugas yang Dilakukan

Tugas yang dikerjakan adalah sebagai berikut.

1. Melakukan pengawasan terhadap sistem SIEM (Wazuh dan SOCFortress) dan EDR (SentinelOne) untuk memantau adanya *alert* yang menunjukkan aktivitas mencurigakan pada *endpoint*.
2. Menganalisis *alert* yang muncul, serta melaporkannya kepada PIC terkait apabila hasil analisis menunjukkan potensi ancaman atau aktivitas berbahaya.
3. Melaporkan secara harian status agen yang terputus dari SIEM maupun SentinelOne kepada PIC terkait.
4. Menyusun laporan mingguan yang berisi rekapitulasi *alert* yang muncul di SentinelOne sebagai bahan evaluasi dan dokumentasi.

3.3 Uraian Pelaksanaan Magang

Berikut adalah uraian semua kegiatan selama enam bulan yang dilakukan dalam pelaksanaan Magang di PT Visionet Data Internasional sebagai SOC L1 Engineer dalam tabel 3.1.

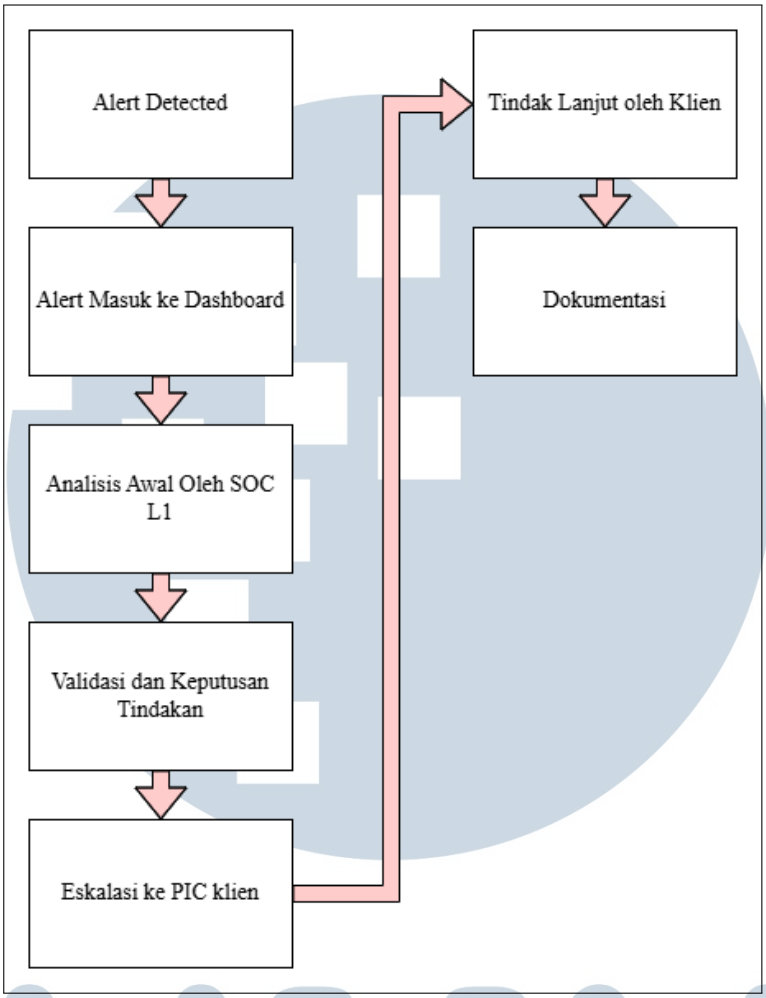
Pelaksanaan kerja magang diuraikan seperti pada Tabel 3.1.

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

Minggu Ke -	Pekerjaan yang dilakukan
1-2	Mempelajari cara melakukan *monitoring* sistem SIEM untuk klien Cinepolis, BPD DIY, dan untuk internal VDI, serta memahami prosedur eskalasi yang sesuai
3-4	Mempelajari cara melakukan *monitoring* sistem EDR SentinelOne untuk klien Lippo-Karawaci, dan internal VDI, serta memahami prosedur eskalasi yang sesuai
5-14	Melakukan *monitoring* terhadap kedua sistem, serta melakukan eskalasi ke PIC terkait
15	Melakukan transisi ke SOC L2 dengan cara mempelajari *threat intelligence* Recorded Future
16-19	Mencari *vulnerability* yang dapat dimasukkan kedalam *playbook* dan mencari adanya *credential leak* yang dapat dilaporkan menggunakan Recorded Future
20-23	Kembali ke SOC L1 dan melanjutkan tugas sebagai L1

3.3.1 Pipeline Standard Operating Procedure di divisi SOC PT Visionet Data Internasional

Pada hari pertama masuk ke kantor diberikan penjelasan mengenai tugas dari tim SOC PT Visionet Data Internasional (VDI). Tim SOC bertanggung jawab untuk melakukan pengawasan terhadap sistem SIEM yang digunakan oleh klien Cinepolis, BPD DIY, lingkungan internal VDI, dan Lippo-Karawaci serta sistem EDR yang digunakan untuk lingkungan internal VDI dan klien Lippo Karawaci. Gambar 3.2 menunjukkan *standard operating procedure* divisi SOC VDI.



Gambar 3.2. Pipeline *Standard Operating Procedure* SOC VDI

Berikut penjelasan lebih mendalam mengenai gambar 3.2:

1. *Alert Detected*

   Sistem SIEM atau EDR akan mendeteksi adanya aktivitas yang mencurigakan, seperti percobaan *login* yang gagal berulang-ulang kali, adanya *file* yang ditandai sebagai sebuah malware, URL/IP yang mencurigakan, atau aktivitas diluar jam kerja.

2. *Alert* Masuk ke *Dashboard*

   Aktivitas mencurigakan tersebut akan masuk ke *dashboard* monitoring sebagai sebuah *alert* sesuai dengan klien (Wazuh untuk Cinepolis/BPD DIY dan SOCFortress/SentinelOne untuk Internal VDI/Lippo-Karawaci).

3. Analisis Awal Oleh SOC L1

Akan dilakukan verifikasi awal terhadap *alert* yang muncul dengan cara mengidentifikasi *severity* dari *alert* sesuai dengan *playbook* yang telah dibuat (*Critical, High, Medium, Low*). Setelah itu akan diecek detail dari *alert* (Waktu terdeteksi, *source* IP, Hash *file*, *hostname*, nama *user*). Kemudian melakukan cek terhadap reputasi dari *file/IP/URL* menggunakan *threat intelligence* seperti VirusTotal, AbuseIPDB, URLVoid, dan Recorded Future.

4. Validasi dan Keputusan Tindakan

   Setelah dilakukan cek terhadap *alert* akan diketahui apakah *alert* tersebut merupakan sebuah *false positive* atau *true positive*. Jika *alert* tersebut *false positive* didokumentasikan tetapi tidak dieskalasi, tapi apabila *true positive* maka akan dilanjutkan dengan proses eskalasi.

5. Eskalasi ke PIC Klien

   Eskalasi *alert* digunakan menggunakan email *Office Outlook*, grup Whatsapp, atau platform SDP VDI (khusus untuk *alert* internal). Eskalasi pertama dilakukan dengan waktu yang tidak melebihi 30 menit sejak *alert* muncul dan akan dilakukan *follow up* secara berkala sesuai dengan *severity* dari *alert* apabila tidak mendapat respon dari PIC klien. (*Critical*: tiap 2 jam, *High*: tiap 4 jam, *Medium*: tiap 8 jam, *Low*: tiap 24 jam)

6. Tindak Lanjut Oleh Klien

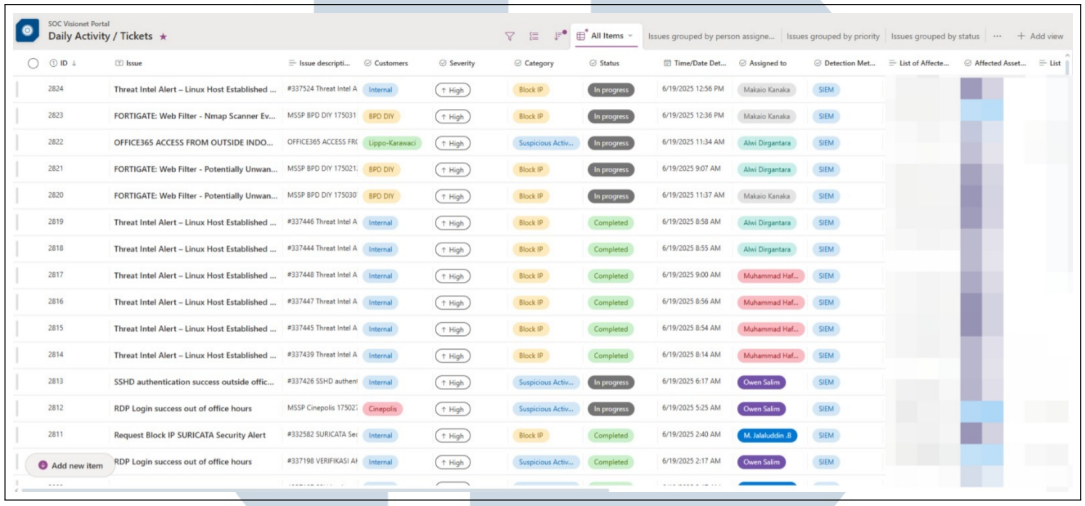
   Klien akan melakukan respon seperti mengisolasi *endpoint*, melakukan *restart* pada agen, menghapus *file*, dll. Khusus untuk *alert* dari SentinelOne apabila perlu tim SOC L1 dapat melakukan *remote shell* ke *endpoint* untuk menghapus *file* yang tertandai sebagai *malware/virus*.

7. Dokumentasi

   Setelah dilakukan langkah-langkah diatas, *alert* dimasukkan kedalam formulir *daily activity* untuk kemudahan L2 membuat *weekly report* tentang aktivitas keamanan siber dari klien yang nantinya akan disampaikan melalui *meeting* dengan klien.

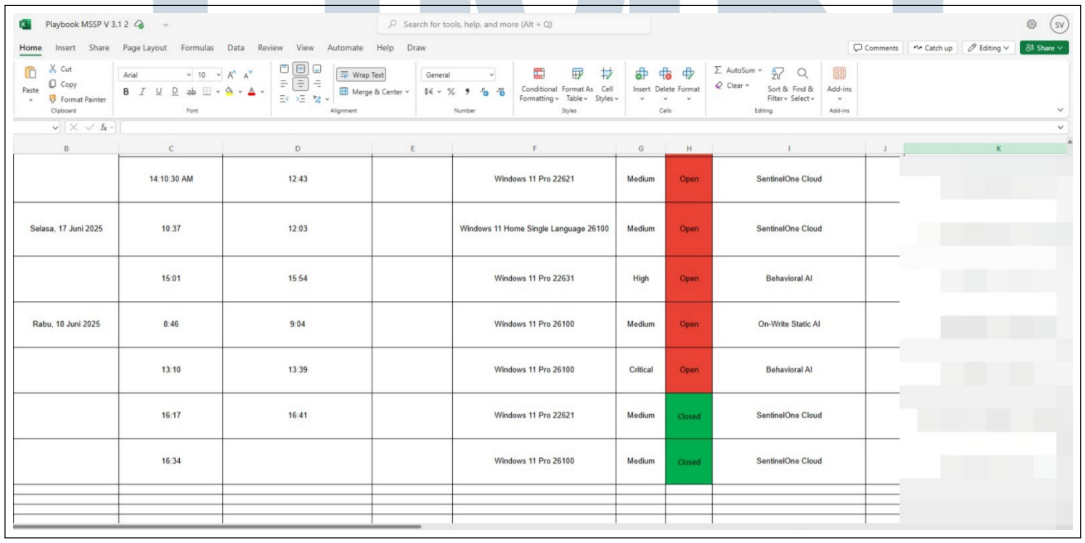
   Gambar 3.3 berikut merupakan tampilan formulir *daily activity* untuk Cinepolis, Bank Pembangunan Daerah Daerah Istimewa Yogyakarta (Bank BPD DIY), dan Visionet. Dalam formulir ini perlu diberikan informasi

mengenai Nama *alert* yang muncul, ID dari *alert* untuk memudahkan identifikasi lebih lanjut, *Severity* dari *alert*, Nama klien, Nama petugas L1 yang melakukan eskalasi, Status eskalasi dari *alert*, Waktu *alert* muncul dan Waktu eskalasi *alert* dilakukan.



Gambar 3.3. Formulir *Daily Activity* Cinepolis, BPD DIY, dan VDI

Gambar 3.4 merupakan tampilan formulir *daily activity* untuk Lippo-Karawaci. Formulir ini berisi Waktu *alert* muncul, Sistem operasi dari *endpoint*, *Severity* dari *alert*, Status eskalasi dari *alert*, Nama petugas L1 yang melakukan eskalasi, Nama *endpoint* dan pengguna *endpoint* tersebut.



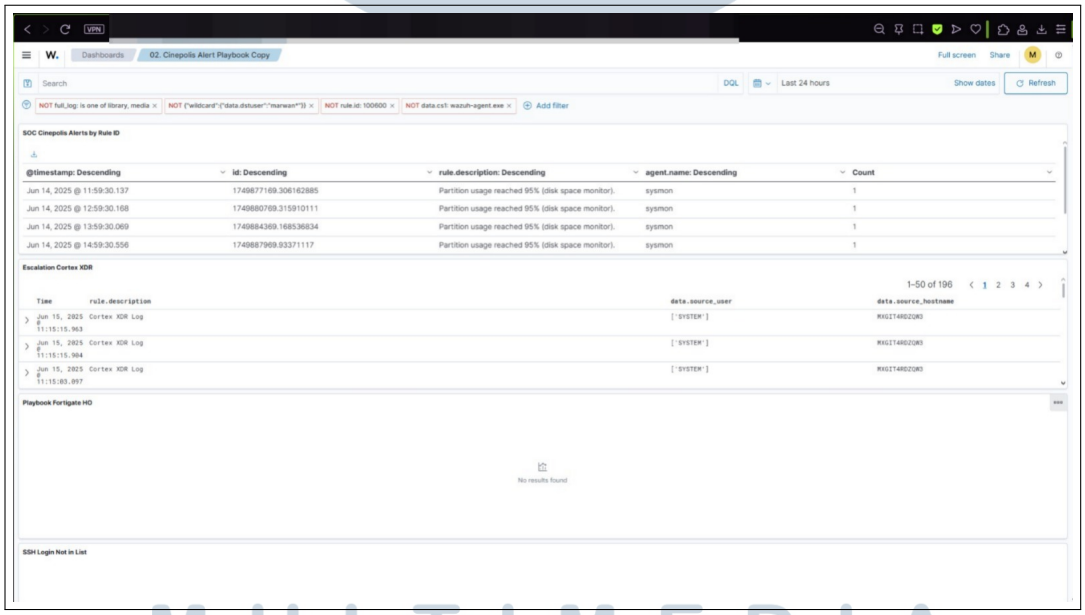
Gambar 3.4. Formulir *Daily Activity* Lippo-Karawaci

3.3.2 Sistem SIEM

Security Information and Event Management (SIEM) adalah sistem yang digunakan untuk mengumpulkan, menganalisis, dan memantau log serta data keamanan dari berbagai perangkat dan sistem dalam suatu infrastruktur TI. SIEM menggabungkan dua fungsi utama, yaitu *Security Information Management* (pengelolaan informasi keamanan) dan *Security Event Management* (manajemen kejadian keamanan), untuk memberikan visibilitas secara *real-time* terhadap aktivitas jaringan dan mendeteksi potensi ancaman atau insiden keamanan. Dengan SIEM, tim keamanan dapat melakukan korelasi antar log dari berbagai sumber seperti *firewall, endpoint, server*, dan aplikasi, sehingga mempermudah dalam mengidentifikasi pola serangan, melakukan investigasi, dan menyusun respons yang cepat serta tepat terhadap insiden yang terjadi [6].

A Wazuh Cinepolis

Gambar 3.5 merupakan tampilan dari Wazuh Cinepolis.



Gambar 3.5. Dashboard Wazuh Cinepolis

Untuk klien Cinepolis beberapa *alert* yang perlu dilaporkan sebagai berikut:

(a) *Windows Failed Login 5 Times in a Row*

Alert ini muncul ketika terdapat percobaan *login* yang gagal sebanyak lima kali berturut-turut pada suatu *endpoint*, yang dapat mengindikasikan

upaya brute force atau akses tidak sah. Proses eskalasi dilakukan dengan menyertakan bukti *alert* kepada PIC klien dan menanyakan apakah aktivitas tersebut merupakan tindakan yang valid (sah) atau mencurigakan, guna memastikan apakah perlu dilakukan tindak lanjut lebih lanjut.

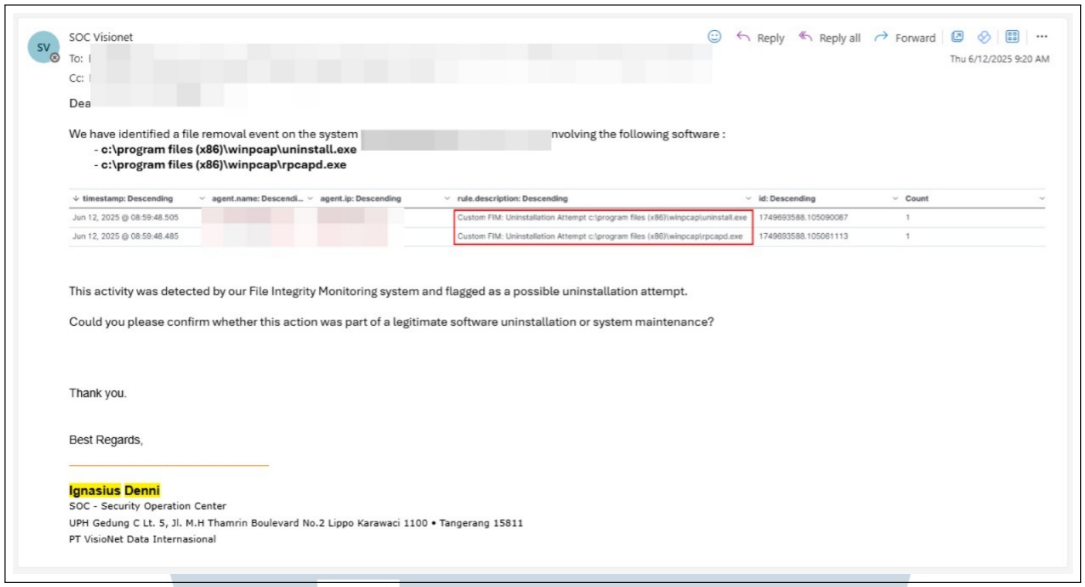
(b) *Cortex XDR terminated unexpectedly*

Alert ini muncul apabila Cortex XDR agen pada suatu *endpoint* terdeteksi sedang dalam kondisi tidak aktif, yang berpotensi menyebabkan *endpoint* kehilangan perlindungan dari ancaman. Sebelum dilakukan eskalasi, tim terlebih dahulu memastikan bahwa proses Cortex XDR benar-benar tidak aktif pada *endpoint* tersebut. Setelah validasi dilakukan, eskalasi dilanjutkan dengan pelaporan kepada PIC klien untuk meminta agar Cortex XDR diaktifkan kembali.

(c) *Cortex XDR Wildfire Malware Event*

Alert ini muncul ketika terdapat aplikasi pada *endpoint* yang terdeteksi oleh Cortex XDR sebagai malware. Sebelum dilakukan eskalasi, dilakukan verifikasi terlebih dahulu terhadap *hash* file aplikasi tersebut menggunakan platform *threat intelligence*. Jika hasil pengecekan menunjukkan bahwa file tersebut memang berbahaya, maka eskalasi dilakukan dengan melaporkan temuan tersebut kepada PIC klien untuk menghapus file tersebut.

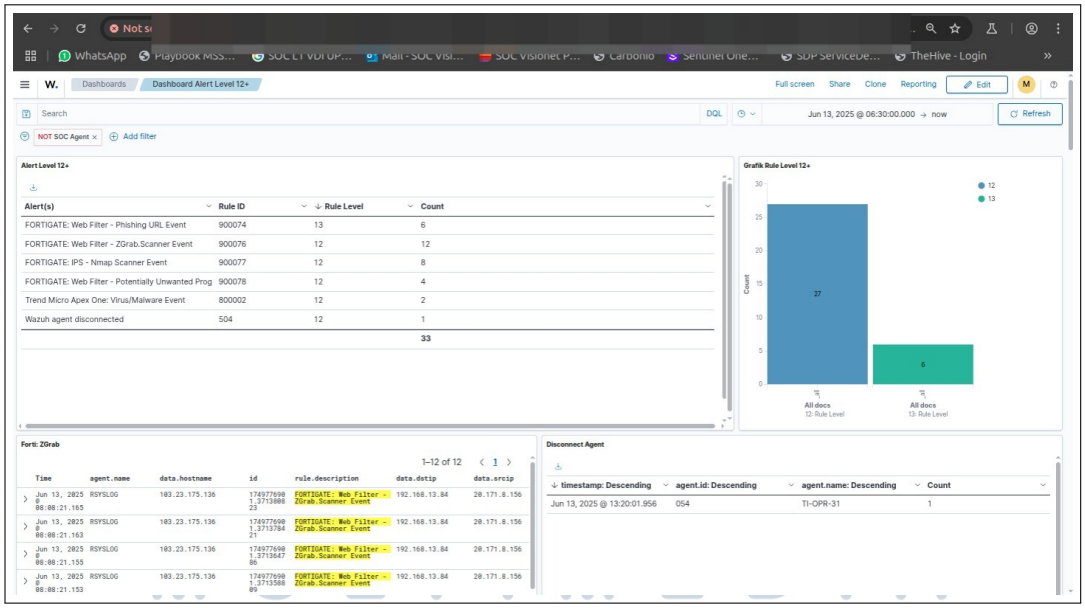
Gambar 3.6 merupakan eskalasi salah satu *alert* yang muncul pada Wazuh Cinepolis.



Gambar 3.6. Contoh Eskalasi *Alert* Cinepolis

B Wazuh BPD DIY

Gambar 3.7 merupakan tampilan dari Wazuh BPD DIY.



Gambar 3.7. Dashboard Wazuh BPD DIY

Untuk klien BPD DIY beberapa *alert* yang perlu dilaporkan sebagai berikut:

(a) FORTIGATE: *Web Filter - ZGrab.Scanner Event*

Alert ini muncul ketika terdapat *source IP* yang ditandai oleh sistem Fortinet sebagai aktivitas ZGrab, yaitu alat pemindaian port yang sering digunakan oleh pelaku ancaman untuk mengumpulkan informasi dari *server* target [7]. Sebelum dilakukan eskalasi, *source IP* tersebut diverifikasi terlebih dahulu menggunakan platform *threat intelligence*. Jika hasil verifikasi menunjukkan bahwa IP address tersebut tergolong berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

(b) FORTIGATE: *Web Filter - Phishing URL Event*

Alert ini muncul ketika terdapat URL yang ditandai oleh sistem Fortinet sebagai aktivitas phishing, yaitu upaya penipuan untuk memperoleh informasi sensitif seperti kredensial atau data pribadi melalui media digital [8]. Sebelum dilakukan eskalasi, URL tersebut diverifikasi terlebih dahulu menggunakan platform *threat intelligence*. Jika hasil verifikasi menunjukkan bahwa URL address tersebut berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

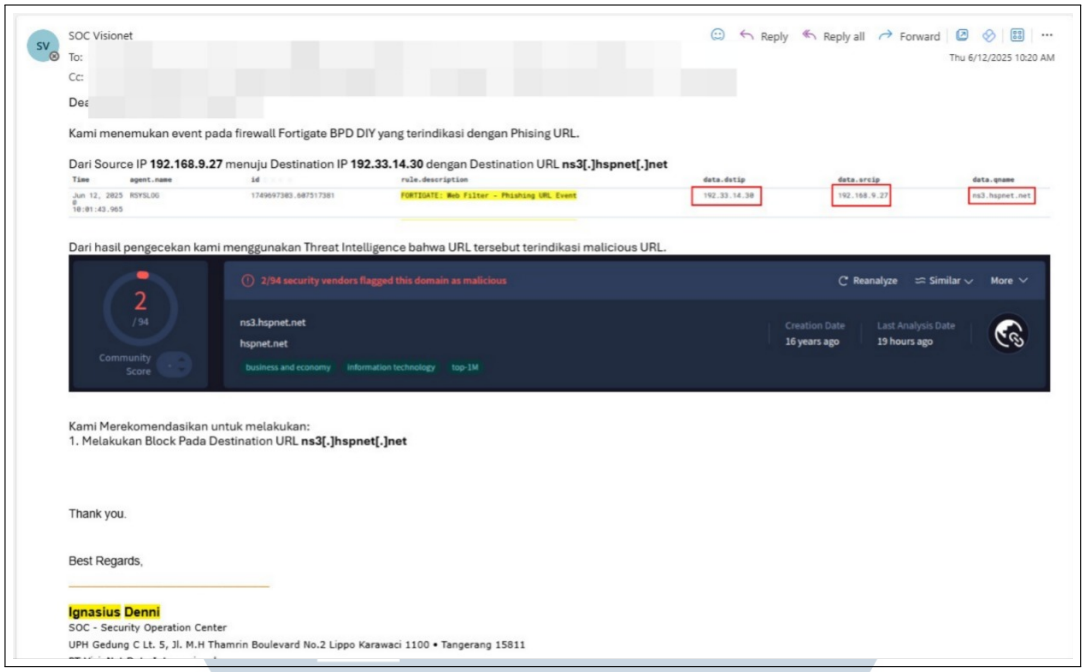
(c) FORTIGATE: *Web Filter - Nmap Scanner Event*

Alert ini muncul ketika ada *source IP* yang ditandai oleh sistem Fortinet melakukan Nmap *scanning* ke sebuah *destination IP*. Nmap adalah sebuah alat yang digunakan untuk melakukan *scanning* terhadap suatu jaringan untuk melihat *port*/layanan mana yang terbuka [9]. Sebelum dilakukan eskalasi, *source IP* tersebut diverifikasi terlebih dahulu menggunakan platform *threat intelligence*. Jika hasil verifikasi menunjukkan bahwa IP address tersebut tergolong berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

(d) Trend Micro Apex One: *Virus/Malware Event*

Alert ini muncul ketika sistem Trend Micro mendeteksi adanya virus pada suatu *endpoint*. Tindak lanjut yang dilakukan adalah menganalisis terlebih dahulu jenis dan karakteristik virus yang terdeteksi, termasuk jalur infeksi dan potensi dampaknya terhadap sistem. Setelah analisis dilakukan dan dipastikan bahwa ancaman tersebut signifikan, maka dilakukan eskalasi kepada PIC klien untuk penanganan lebih lanjut.

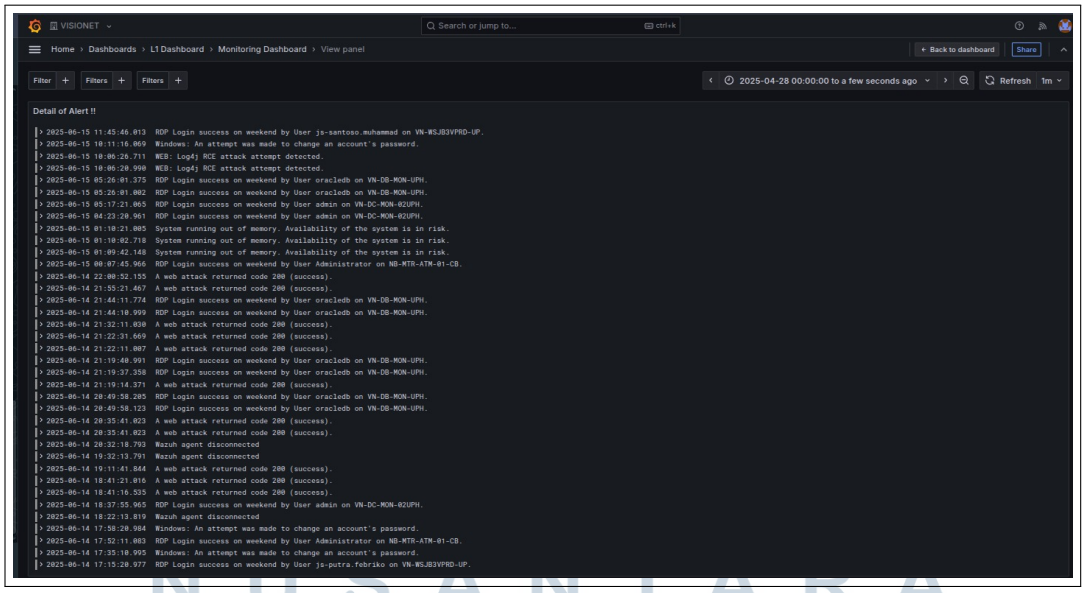
Gambar 3.8 merupakan eskalasi salah satu *alert* yang muncul pada Wazuh BPD DIY.



Gambar 3.8. Contoh Eskalasi *Alert* BPD DIY

C SOCFortress Internal VDI

Berikut merupakan tampilan dari SOCFortress Internal VDI.



Gambar 3.9. Dashboard SOCFortress Internal VDI

Hampir semua proses eskalasi untuk sistem internal VDI dilakukan melalui platform SDP VDI, yang merupakan sistem pelaporan dan manajemen insiden

internal perusahaan. Sebagian lainnya dieskalasikan menggunakan outlook atau Beberapa *alert* yang perlu dieskalasikan pada SOCFortress VDI antara lain:

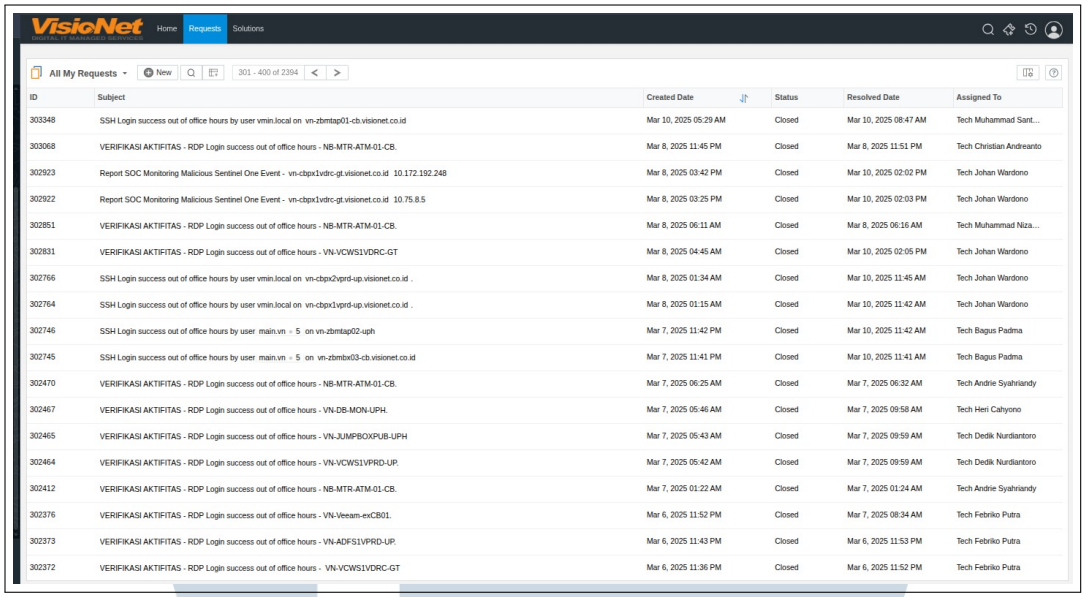
(a) *RDP Login Success out of office hour*

Remote Desktop Protocol (RDP) merupakan sebuah alat yang digunakan untuk mengakses lingkungan *desktop* dan *server* dari jarak jauh [10]. *Alert* ini muncul ketika terdapat pengguna (user) yang berhasil melakukan *login* ke *endpoint* menggunakan protokol RDP di luar jam operasional, yaitu antara pukul 17.00 hingga 07.00. Aktivitas seperti ini dianggap tidak wajar dan berpotensi mengindikasikan akses tidak sah, sehingga perlu segera dilakukan eskalasi kepada tim ITSD tanpa perlu analisis lanjutan.

(b) *Log4j RCE attack attempt detected*

Alert ini muncul ketika sistem mendeteksi adanya upaya serangan *Remote Code Execution* (RCE) yang mengeksploitasi kerentanan pada platform Log4j. Log4j adalah sebuah *library open-source* gratis yang mengimplementasikan *logging framework* [11]. RCE adalah sebuah kerentanan yang memungkinkan penyerang untuk menjalankan kode mereka dalam mesin korban [11] [12]. Sebelum dilakukan eskalasi, dilakukan pengecekan terlebih dahulu terhadap *source IP* menggunakan platform *threat intelligence*. Jika IP address tersebut teridentifikasi sebagai malicious, maka eskalasi segera dilakukan kepada tim ITSD untuk melakukan blok terhadap IP tersebut.

Berikut merupakan tampilan dari SDP Visionet.

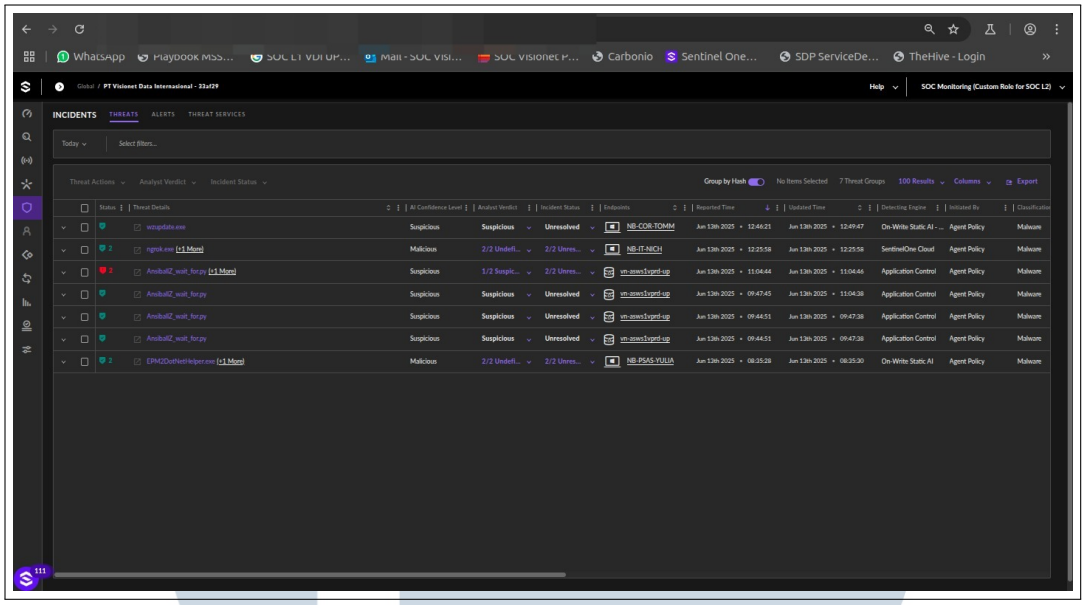


Gambar 3.10. SDP Visionet

3.3.3 Sistem EDR

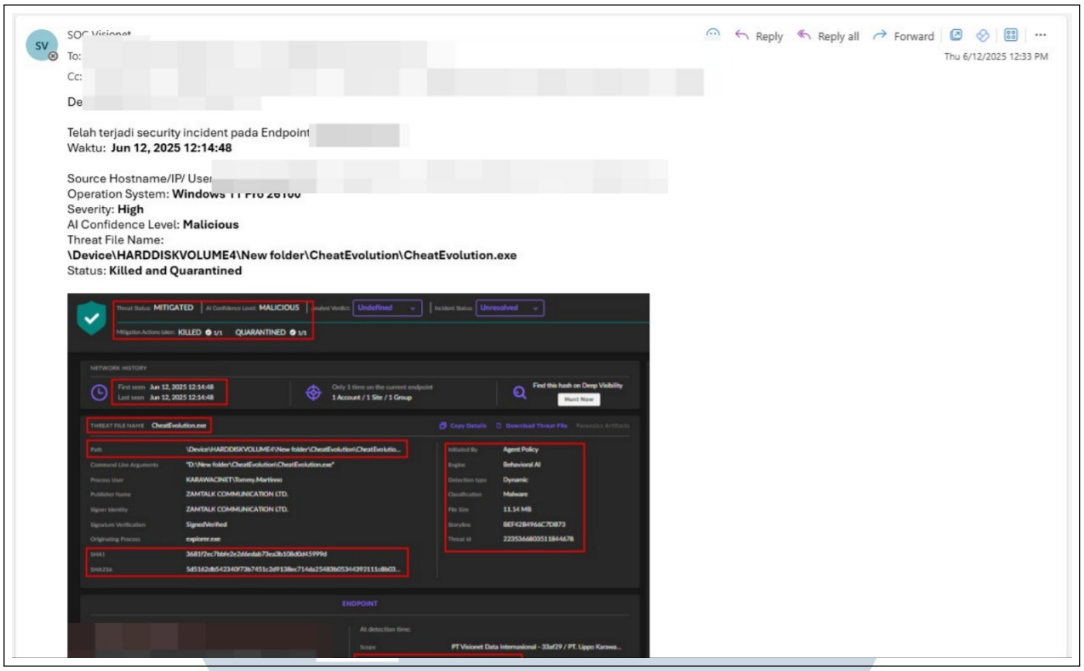
Endpoint Detection and Response (EDR) adalah teknologi keamanan siber yang secara kontinu memantau aktivitas pada *endpoint* untuk mendeteksi adanya ancaman serta melakukan tindakan otomatis guna membantu mitigasi. *Endpoint* mencakup berbagai perangkat fisik yang terhubung ke jaringan seperti desktop, laptop, ponsel, mesin virtual, dan perangkat *Internet of Things* (IoT), yang semuanya dapat menjadi titik masuk bagi penyerang. Solusi EDR mencatat perilaku *endpoint* selama 24 jam penuh dan menganalisis data tersebut untuk mengidentifikasi aktivitas mencurigakan, seperti indikasi serangan ransomware. Selain mendeteksi, EDR juga mampu melakukan isolasi otomatis terhadap ancaman serta mengirimkan notifikasi kepada tim keamanan, yang kemudian dapat menggunakan data yang tercatat untuk menyelidiki secara rinci bagaimana insiden terjadi, apa saja yang terdampak, dan langkah penanganan yang perlu dilakukan selanjutnya [13].

Berikut merupakan tampilan dari EDR SentinelOne.



Gambar 3.11. Dashboard EDR SentinelOne

Eskalasi untuk *alert* yang muncul pada SentinelOne dilakukan melalui Outlook secara langsung kepada pengguna *endpoint* yang terlibat. Nama pengguna biasanya sudah tercantum dalam *alert*, dan alamat email pengguna dapat diperoleh dari informasi tersebut. Sebelum dilakukan eskalasi, tim SOC L1 terlebih dahulu melakukan pengecekan terhadap *hash* file yang terdeteksi menggunakan platform *threat intelligence*. Jika *hash* file tersebut dikategorikan sebagai malicious, maka tim L1 akan segera mengambil tindakan dengan menggunakan fitur *remote shell* dari SentinelOne untuk menghapus file berbahaya tersebut secara langsung dari *endpoint*. Namun, apabila hasil pengecekan tidak menunjukkan bahwa file tersebut berbahaya, maka tim L1 akan menghubungi pengguna terkait untuk menanyakan legitimasi atau keabsahan file yang menjadi sumber *alert* tersebut. Berikut adalah bentuk eskalasi yang dilakukan melalui email *Office Outlook*.

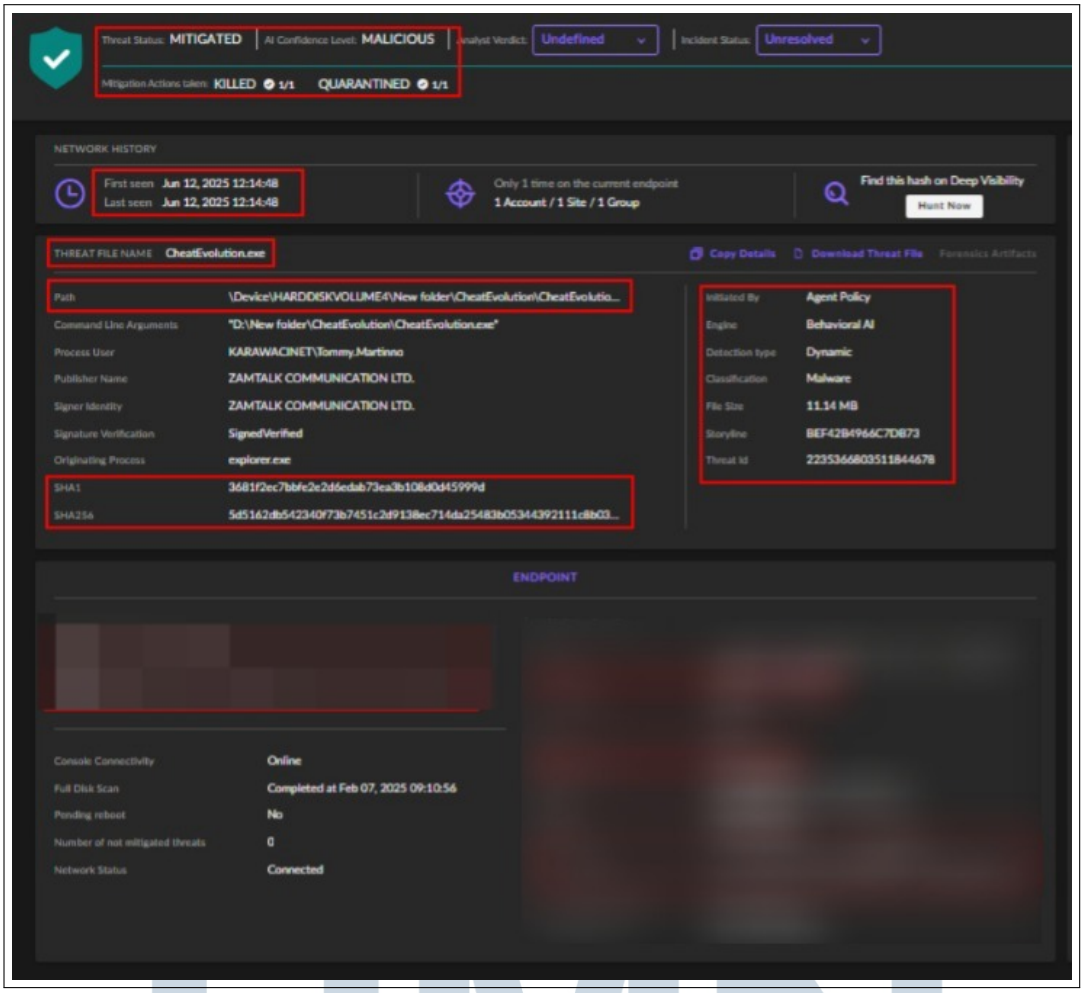


Gambar 3.12. Contoh Eskalasi EDR SentinelOne

Dalam laporan eskalasi ada beberapa hal yang perlu dicantumkan yaitu:

1. Nama *endpoint*
2. Waktu *alert* muncul di SentinelOne
3. Nama dan alamat IP pengguna
4. *Operation System* yang digunakan *endpoint*
5. Tingkat *severity* dari *alert*
6. Keputusan dari AI SentinelOne tentang seberapa berbahaya *alert*
7. Nama dan *file path* dari *file* yang terdeteksi
8. Bukti bahwa *alert* muncul berupa *screenshot*
9. *Screenshot* dari sebuah *threat intelligence* yang menunjukkan reputasi dari *file* yang terdeteksi
10. Analisa singkat mengenai *file* yang terdeteksi
11. Tindakan yang telah dilakukan oleh SOC dan saran tindakan bagi pengguna

Berikut merupakan salah satu *alert* yang muncul di SentinelOne.



Gambar 3.13. Contoh *Alert* dari SentinelOne

Gambar 3.13 merupakan *screenshot* dari alert yang menyoroti hal-hal yang penting untuk diketahui oleh penerima laporan. Hal-hal yang perlu disoroti adalah Status dari *file* berbahaya, Waktu *alert* muncul, Informasi mengenai *file* seperti nama, *file path*, dan *hash*, *Engine* yang digunakan SentinelOne untuk mendeteksi *file*, Klasifikasi yang diberikan oleh SentinelOne untuk *file*, dan Informasi mengenai *endpoint*.

3.4 Kendala dan Solusi yang Ditemukan

Selama pelaksanaan kerja magang ini ditemukan beberapa kendala ketika melaksanakan tugas. Beberapa kendala yang ditemukan adalah sebagai berikut.

1. Saat menjalani masa magang di divisi SOC L2 selama satu bulan, karena bukan merupakan pegawai tetap tidak diberikan akses untuk menggunakan VPN perusahaan.

2. Karena *alert* yang muncul di SentinelOne dilaporkan secara langsung kepada pengguna yang terkait, terkadang ditemukan *alert* dengan nama pengguna yang kurang jelas, seperti "*Administrator*". Hal ini dapat menyulitkan dalam proses identifikasi pemilik perangkat yang sebenarnya.

Dari berbagai kendala yang dialami selama kegiatan magang, berikut adalah solusi-solusi yang ditemukan untuk menangani masalah tersebut:

1. Diberikan tugas yang tidak memerlukan akses VPN, yaitu melakukan pencarian dan pemantauan berita terkait CVE serta *credential leak* menggunakan platform *threat intelligence* Recorded Future. Informasi yang diperoleh digunakan sebagai bahan analisis potensi ancaman yang mungkin berdampak pada klien maupun sistem internal perusahaan.

2. Melakukan koordinasi terlebih dahulu dengan PIC utama dari klien untuk mengidentifikasi nama pengguna dari *endpoint* terkait. Jika informasi tidak tersedia, maka dilakukan pelaporan kepada tim *IT Support* klien agar dapat ditindaklanjuti dan langsung dilaporkan ke pengguna *endpoint*.