BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Organisasi

Pelaksanaan kerja magang yang dilakukan yaitu sebagai *Technical Consultant* yang berada dalam divisi *Technical Consultant* dan dibawahi manajemen *VP Operation* dan *Project Manager* yang dilaksanakan di PT Global Innovation Technology. Pelaksanaan kerja magang disertai dengan *training* atau pelatihan Splunk yang dipandu oleh Bapak Munir selaku pengajar dan Bapak Rizki selaku *VP Operation* serta Bapak Fajar, Bapak Robi dan Bapak Wahyu selaku *Project Manager*. Untuk implementasi *project*, terdapat penugasan ke Tokio Marine selaku klien PT GIT yang memakai Splunk dan *service maintenance* dari PT GIT. *Training* yang dilakukan oleh tim magang *Technical Consultant* dilakukan secara luring di kantor dan mempelajari tentang platform Splunk yang merupakan salah satu jajaran produk yang ditawarkan PT GIT kepada klien. Tujuan dari *training* ini adalah agar para tim magang dapat melakukan promosi awal kepada klien ataupun*maintenance service* yang diminta oleh klien. Adapun beberapa perangkat atau komponen yang dibutuhkan untuk mendukung proses pelaksanaan magang yaitu sebagai berikut.

1. MyGit yang merupakan aplikasi miliki PT GIT yang di-*develop* oleh tim *Development* PT GIT. Aplikasi ini digunakan untuk absensi dan juga pembagian tugas *project* bagi tim karyawan maupun tim magang.
2. VPN FortiClient dengan akses yang disediakan oleh Tokio Marine untuk *Technical Consultant* dapat mengakses server Splunk milik Tokio Marine.
3. MobaXTerm yang digunakan untuk mengakses server dari jarak jauh (*remote*) menggunakan protokol jaringan tertentu. Contohnya seperti SSH, Telnet dan sebagainya.
4. PuTTY merupakan aplikasi yang kegunaannya sama seperti MobaXTerm, hanya saja terdapat beberapa perbedaan pada antarmuka aplikasi ini dengan aplikasi MobaXTerm.

3.2 Tugas yang Dilakukan

Tugas yang dilakukan saat pelaksanaan magang biasa diberikan oleh *Project Manager* tergantung dengan *project* yang dialokasikan kepada tiap pemagang di PT GIT. Pada konteks ini, penulis ditugaskan di *maintenance service* untuk klien Tokio Marine. Tugas *maintenance service* mencakup poin-poin berikut.

1. ***Corrective Maintenance*** adalah jenis perbaikan yang dilakukan sebagai respons terhadap masalah yang telah dilaporkan oleh klien atau pelanggan. Ini bisa berupa masalah yang ditemui secara langsung oleh pengguna atau permintaan untuk meningkatkan atau memperbaiki fungsionalitas yang ada. Salah satu contohnya adalah ketika klien mengalami masalah dengan versi lama Splunk yang mereka gunakan dan meminta untuk ditingkatkan ke versi terbaru. Prosesnya melibatkan pembaruan perangkat lunak dari versi lama ke versi yang lebih baru, memastikan kompatibilitas dengan sistem yang ada, serta menjamin bahwa semua data yang ada berhasil ditransfer dengan benar ke versi baru. Langkah-langkah pengerjaannya termasuk:

   (a) Evaluasi kebutuhan dan kesiapan sistem untuk upgrade.

   (b) Persiapan backup data dan konfigurasi yang tepat sebelum upgrade.

   (c) Pembaruan perangkat lunak secara sistematis dan pengujian setelah pembaruan.

   (d) Pelaporan dan dokumentasi hasil upgrade serta penyelesaian masalah yang mungkin muncul selama proses tersebut.

2. ***Explorative Maintenance*** melibatkan perbaikan yang membutuhkan lebih banyak eksplorasi atau penelitian untuk menemukan dan memperbaiki masalah yang muncul di lingkungan Splunk klien. Perbaikan ini mungkin melibatkan masalah yang belum pernah terjadi sebelumnya atau belum memiliki solusi yang jelas. Contohnya adalah ketika klien mengalami masalah yang kompleks atau unik dalam penggunaan Splunk mereka, seperti kesalahan dalam pembuatan dashboard atau kinerja sistem yang tidak diharapkan. Proses Explorative Maintenance dapat mencakup langkah-langkah seperti:

   (a) Analisis mendalam terhadap masalah yang terjadi, termasuk penelusuran log dan pengumpulan informasi yang relevan.

(b) Eksperimen dengan konfigurasi dan pengaturan Splunk untuk mengidentifikasi penyebab masalah.

(c) Pengembangan dan implementasi solusi yang sesuai, seperti pembuatan atau penyesuaian dashboard menggunakan Dashboard Studio Splunk.

(d) Pengujian solusi yang diusulkan untuk memastikan bahwa masalah telah diperbaiki dan tidak menyebabkan dampak negatif lainnya pada sistem.

(e) Dokumentasi seluruh proses dan solusi yang diterapkan untuk referensi masa depan dan transparansi.

Untuk melakukan tugas-tugas yang disebutkan di atas, diberikan kesempatan untuk mempelajari langkah pengerjaan dan ketentuan yang perlu diperhatikan dengan menggunakan dokumentasi yang disediakan oleh Splunk dan juga memerlukan diskusi agar perbaikan sesuai dengan kebutuhan dan permintaan klien.

3.3 Uraian Pelaksanaan Magang

Pelaksanaan kerja magang dimulai pada bulan Januari 2024 hingga Mei 2024 dan diuraikan seperti pada Tabel 3.1.

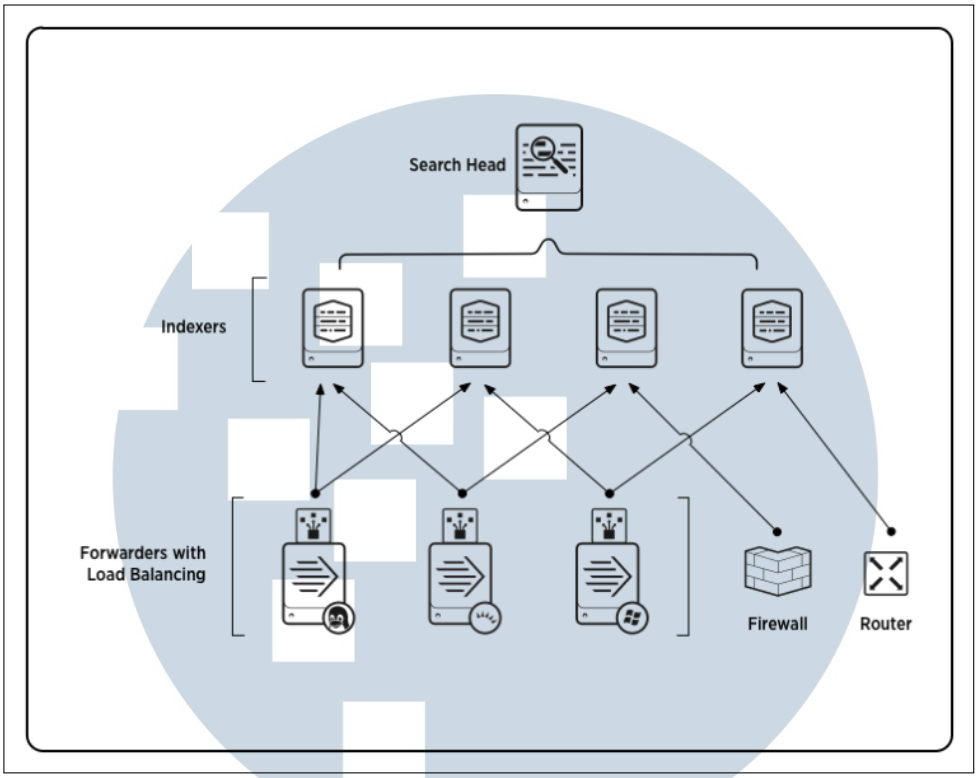
Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

Minggu Ke -	Pekerjaan yang dilakukan
1	Menyelesaikan modul Splunk untuk keperluan sertifikasi awal
2	Praktik instalasi SPLUNK (*Search Head, Indexer* dan *Agent*) di server dipandu Mas Arya dan Mas Akmal dan melakukan *custom classic dashboard* dari data yang ada di server kantor.
3	*Training* Splunk dengan materi SIEM dan pengerjaan 3 sertifikasi *School of Splunk*
4	*Training* Splunk dengan materi Splunk *Security Essential* dengan pengenalan *Proof of Concept* dokumen dan produk-produk *security*
5	*Training* Splunk dengan materi *Lightweight Directory Access Protocol*
6	*Training* Splunk dengan materi Splunk *Enterprise Security* membahas spesifik tentang *Asset* dan *Identity*.
7	*Training* Splunk dengan materi Splunk *Enterprise Security* membahas spesifik tentang *Correlation Search*
8	Penyelesaian modul sertifikasi *School of Splunk: Sales Rep II*
9	Eksplorasi pembuatan *dashboard Report Availability server local* instruksi dari Mas Akmal untuk memonitor *uptime* dan *downtime* Tokio Marine bersama Steven, Aura, Naufal.
10	*Training* Splunk dengan topik utama menentukan *Correlation Search* berdasarkan *Sequence Template*.
11	Implementasi awal *Dashboard Studio* yang termasuk dalam pelaksanaan *Corrective Maintenance* untuk Tokio Marine di server lokal GIT, kemudian diintegrasikan ke server Tokio Marine dengan *Dashboard* yang masih bersifat *private*.
12	Eksplorasi solusi dari implementasi background TM yang terkendala saat pengerjaan *dashboard* di *server* TMI dan pengerjaan *dashboard studio* Fortigate (Salwa) serta Sangfor (Aura) Performance di server Tokio Marine.
13	Kunjungan *Corrective Maintenance* ke Tokio Marine bersama Pak Rizki, Pak Wahyu, Mas Akmal dan Aura terkait *upgrade* Splunk 9.0 ke 9.2.1 (*upgrade* Search Head done)

Minggu Ke -	Pekerjaan yang dilakukan
14	Eksekusi solusi yang sudah dieksplorasi, yaitu memperbarui SSL Certificate Splunk di SH dan Indexer Tokio Marine dan penyelesaian dokumen *User Guide* Splunk *Dashboard Studio*, merapikan dokumen dan menambahkan daftar isi.
15	Implementasi *Classic Dashboard* untuk *Server Performance* Tokio Marine dengan menambahkan *dropdown* halaman baru di laman *apps* Splunk
16	*Corrective Maintenance Upgrade* Splunk 9.2.1 di server Indexer Splunk Tokio Marine dan pembuatan dokumen dokumentasi *step upgrade* Splunk *Search Head* dan *Indexer* di Tokio Marine
17	Eksplorasi dan instalasi *Wazuh Central Component (Indexer, Server,* dan *Dashboard)* serta instalasi Wazuh Agent untuk proses *collect data* Wazuh.
18	Eksplorasi cara penggunaan Wazuh dan lanjut *collect data* dari VirusTotal, Mikrotik, dan LDAP.

3.3.1 Splunk

Seperti yang sudah dijelaskan pada Bab 1 Latar Belakang, secara garis besar Splunk adalah perangkat untuk *monitoring* yang didalamnya terdapat banyak fitur fungsional yang dapat sangat bermanfaat bagi sisi pengguna. Splunk komponen utama yang di dalamnya wajib terdiri dari ***Search Head, Indexer*** dan *Target System* serta ***Forwarder*** sebagai perantara untuk proses *Data Collect*. Komponen penting tersebut jelas memiliki definisi dan fungsi masing-masing, Gambarr 3.1 adalah gambaran komponen Splunk yang bersumber dari dokumentasi Splunk.



Gambar 3.1. Komponen Splunk
Sumber: [6]

1. ***Search Head*** merupakan antarmuka pengguna platform Splunk di mana pengguna melakukan pencarian, analisis, dan visualisasi data. *Search Head* menangani permintaan pengguna, mengirimkannya ke *indexer* untuk mendapatkan data yang relevan, dan menampilkan hasilnya kepada pengguna melalui antarmuka web Splunk.

2. ***Indexer*** merupakan komponen yang bertanggung jawab untuk mengindeks dan menyimpan data yang dikumpulkan oleh Splunk. Indexer menerima data dari *forwarder*, mengindeksnya untuk pencarian yang efisien, dan menyimpannya dalam format yang dapat diakses oleh *Search Head*. *Indexer* juga dapat melakukan replikasi data untuk menjaga redundansi dan ketersediaan data.

3. ***Forwarder*** adalah agen yang diinstal pada sumber data untuk mengirimkan data ke *Indexer. Forwarder* dapat mengumpulkan data dari berbagai sumber, termasuk *log file*, perangkat jaringan, aplikasi, dan sensor. *Forwarder* mengirim data yang dikumpulkan ke *Indexer* untuk pengindeksan dan penyimpanan. *Forwarder* dapat dikonfigurasi untuk melakukan pra-

pemrosesan data sebelum dikirim, seperti penghapusan informasi sensitif atau pengayaan data dengan metadata tambahan.

4. ***Target System*** berfungsi sebagai sumber data yang ingin dimasukkan ke Splunk untuk dimonitor, komponen ini sangat penting karena Splunk hanya akan bisa berfungsi dengan baik dan berguna karena sumber data yang baik. *Target System* bisa berupa sistem atau aplikasi apa pun yang menghasilkan data yang relevan untuk analisis keamanan, operasional, atau bisnis. Contohnya meliputi server aplikasi, perangkat jaringan, *database, log file,* dan banyak lagi.

Dengan uraian pengantar di atas, dapat disimpulkan Splunk memiliki komponen yang saling mengikat satu sama lain untuk mencapai keberhasilan fungsionalnya. Dalam sub bab ini, penulis akan menguraikan beberapa fitur dan kegunaan Splunk yang terlibat dalam proses pelaksanaan magang. Berikut penguraiannya.

A. SIEM

Salah satu metode yang digunakan oleh organisasi untuk mengelola keamanan informasi mereka adalah *Security Information and Event Management* (SIEM). Ini mencakup pengumpulan, analisis, dan respons terhadap data keamanan dari berbagai sumber dalam lingkungan IT. *Security Information Management* (SIM) berkonsentrasi pada pengumpulan dan analisis data keamanan, termasuk log keamanan dan informasi terkait, sementara *Security Event Management* (SEM) berkonsentrasi pada deteksi dan respons terhadap peristiwa keamanan. SIEM, yang berasal dari kombinasi SIM dan SEM, membantu organisasi memahami keamanan mereka dengan lebih baik.

Splunk SIEM adalah *platform* yang populer yang memungkinkan pengguna mengumpulkan, mengindeks, dan menganalisis data dari berbagai sumber, seperti aplikasi, log keamanan, dan infrastruktur TI lainnya. Kemampuan pengumpulan data yang luas, kemampuan menggunakan bahasa pencarian yang kuat untuk mendapatkan data yang relevan, pengembangan dan penyesuaian dashboard dan laporan, deteksi ancaman yang canggih melalui analisis perilaku dan *machine learning*, dan integrasi yang kuat dengan berbagai aplikasi dan perangkat keamanan. [7]

Dengan kemampuan pengumpulan, analisis, dan respons data keamanan yang canggih dari Splunk SIEM, organisasi dapat mengoptimalkan pengelolaan keamanan informasi mereka, melawan ancaman dengan lebih baik, dan memastikan integritas sistem mereka. [4]

B. Splunk Core

Splunk *Core* adalah produk utama dari platform Splunk, yang menawarkan kemampuan untuk mengumpulkan, mengindeks, dan menganalisis data dari berbagai sumber dalam lingkup Teknologi Informasi. Berikut adalah beberapa poin penting tentang Splunk *Core*.

1. Splunk Core memungkinkan organisasi untuk mengumpulkan data dari berbagai sumber termasuk log, file teks, basis data, aplikasi, perangkat jaringan, sensor IoT, dan lebih banyak lagi. Ini berarti Anda dapat mengintegrasikan hampir semua jenis data ke dalam *platform* Splunk.

2. Salah satu fitur utama Splunk *Core* adalah kemampuannya untuk melakukan pencarian cepat dan efisien melalui data yang terkumpul. Ini memungkinkan pengguna untuk menemukan informasi yang relevan dalam data yang sangat besar dengan cepat. Selain itu, Splunk juga dapat digunakan untuk memantau data secara real-time, memberikan wawasan langsung tentang apa yang terjadi di lingkungan IT atau bisnis.

3. Splunk *Core* menyediakan berbagai alat analisis dan visualisasi untuk membantu pengguna memahami data mereka dengan lebih baik. Ini termasuk kemampuan untuk membuat laporan, *dashboard*, dan grafik interaktif yang memungkinkan pengguna untuk menganalisis data dengan lebih mendalam.

C. Splunk *Dashboard*

Gambar 3.2. Contoh *Dashboard Studio* Splunk
Sumber: [8]

Splunk *Dashboard* merupakan antarmuka visual yang memungkinkan pengguna untuk memantau, menganalisis, dan memvisualisasikan data yang dikumpulkan dan diindeks oleh I Splunk. Dashboard ini menyajikan informasi yang relevan dan terkini dalam bentuk grafik, diagram, tabel, dan metrik lainnya, yang membantu pengguna untuk memahami kondisi dan tren dalam lingkungan IT atau bisnis mereka. Pengguna dapat membuat *dashboard* yang disesuaikan sesuai dengan kebutuhan mereka dengan menambahkan panel visualisasi dari berbagai jenis data, termasuk data keamanan, operasional, infrastruktur, dan bisnis. *Dashboard* Splunk dapat digunakan untuk memantau kinerja sistem, mendeteksi ancaman keamanan, menganalisis tren operasional, dan melacak metrik bisnis kunci, seperti penjualan atau kepuasan pelanggan. [9]

Selain itu, *dashboard* dapat diatur untuk memberikan pembaruan secara *real-time* atau berdasarkan interval waktu tertentu, memastikan bahwa pengguna mendapatkan informasi yang akurat dan relevan sepanjang waktu. Dengan fitur-fitur yang fleksibel dan dapat disesuaikan, *dashboard* Splunk memberikan pengguna kemampuan untuk menggali wawasan yang mendalam dari data mereka dan membuat keputusan yang lebih baik berdasarkan pemahaman yang lebih baik tentang lingkungan mereka.

3.4 Hasil Implementasi

3.4.1 *Corrective Maintenance* Splunk Tokio Marine

Salah satu tindakan pemeliharaan yang dilakukan terhadap Tokio Marine disebut *Corrective Maintenance*. Pihak klien yaitu Tokio Marine memberikan permintaan (*request)* untuk kasus tertentu biasanya melalui *Weekly Report Meeting* antara PT GIT dan Tokio Marine yang diadakan setiap hari Jumat. Berikut uraian beberapa isu yang pernah ditangani.

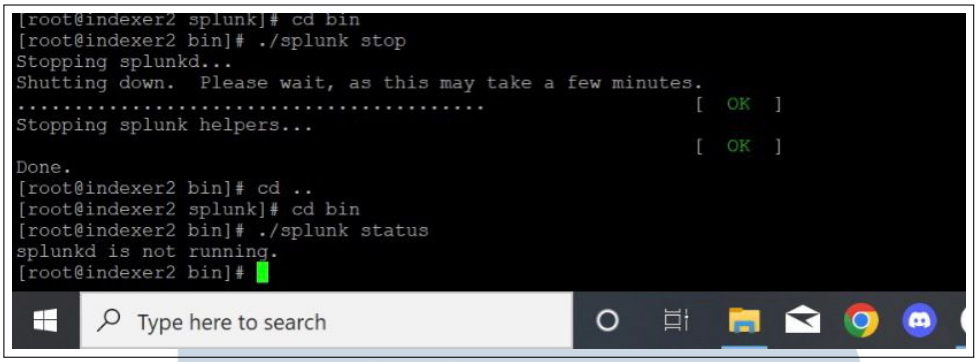
A. *Upgrade* Versi Indexer Splunk 9.0.2 ke Splunk 9.2.1

1. ***Issue***: Pihak klien meminta untuk dibuatkan *Dashboard Studio* agar tampilan *Dashboard* mereka tidak monoton, namun ada isu dimana Splunk Tokio Marine tidak bisa meng-*upload* gambar *background* untuk keperluan desainnya.

2. ***Root Cause***: Karena desain awal dilakukan di server lokal PT GIT yang memiliki versi Splunk 9.2 dan bisa melakukan *upload background*, maka asumsi isunya berasal dari versi Splunk Tokio Marine yang belum ter-*update*.

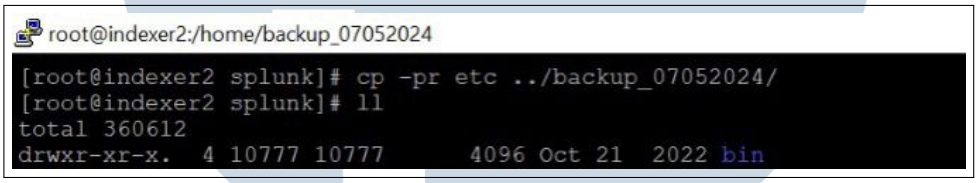
3. ***Solution***: Pada saat *Weekly Report Meeting*, PT GIT memberikan *update* tentang isu ini dan memberi informasi bahwa PT GIT akan melakukan *upgrade* versi Splunk Tokio Marine di *Search Head* maupun pada *Indexer*. Untuk pengerjaan *upgrade Search Head* dilakukan langsung di lokasi Tokio Marine. Sedangkan untuk *upgrade Indexer* dilakukan secara *remote* di PT GIT. Berikut diuraikan proses *upgrade Indexer* pada Splunk Tokio Marine.

   (a) Gambar 3.3 merupakan **proses menonaktifkan *Service* Splunk**. Proses ini bersifat wajib dilakukan untuk mengurangi resiko *crash* karena pengolahan data yang dilakukan Splunk terus berlangsung pada saat proses instalasi *upgrade* versi berlangsung.



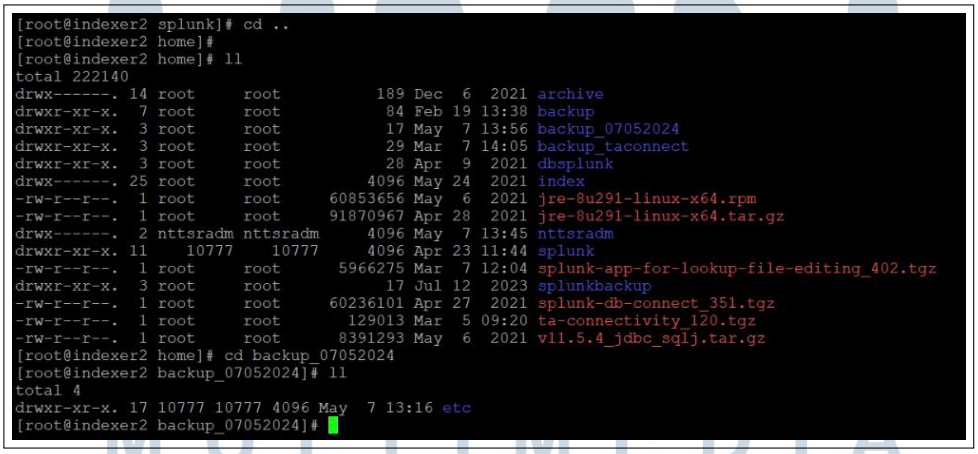
Gambar 3.3. Menonaktifkan Splunk *Service*

(b) Gambar 3.4 adalah **proses *Backup*** untuk mengurangi resiko data hilang jika ada *error* saat melakukan *upgrade.*



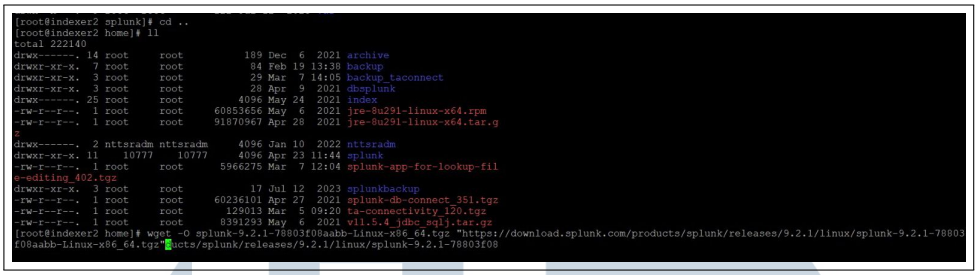
Gambar 3.4. *Command* untuk *backup* data

Setelah dijalankan, file yang sudah di-*backup* akan muncul seperti di gambar 3.5. Terlihat bahwa *file "backup-07052024"* sudah ada di direktori.



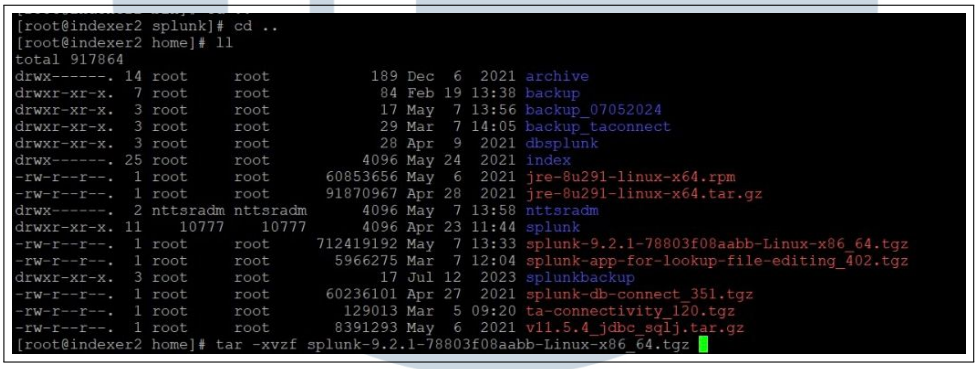
Gambar 3.5. *Backup* telah berhasil dilakukan

(c) Gambar 3.6 merupakan **proses mengunduh *Installer* untuk Versi Splunk yang baru**. *Command* di gambar 3.6 didapatkan dari *website* Splunk yang menyediakan unduhan aplikasi Splunk.



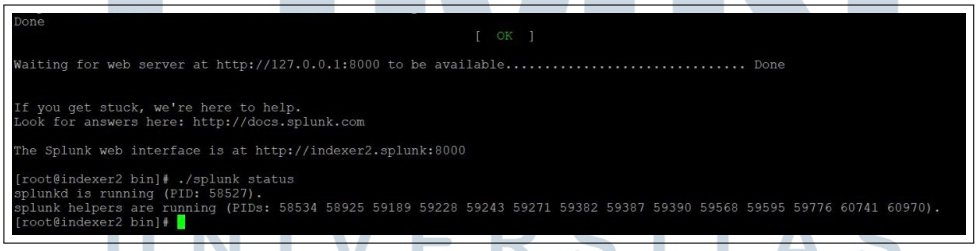
Gambar 3.6. *Command* untuk mengunduh *Installer* Splunk 9.2.1

Setelahnya, akan dilakukan ekstrak *installer* versi Splunk 9.2.1 sekaligus proses instalasi *upgrade*.



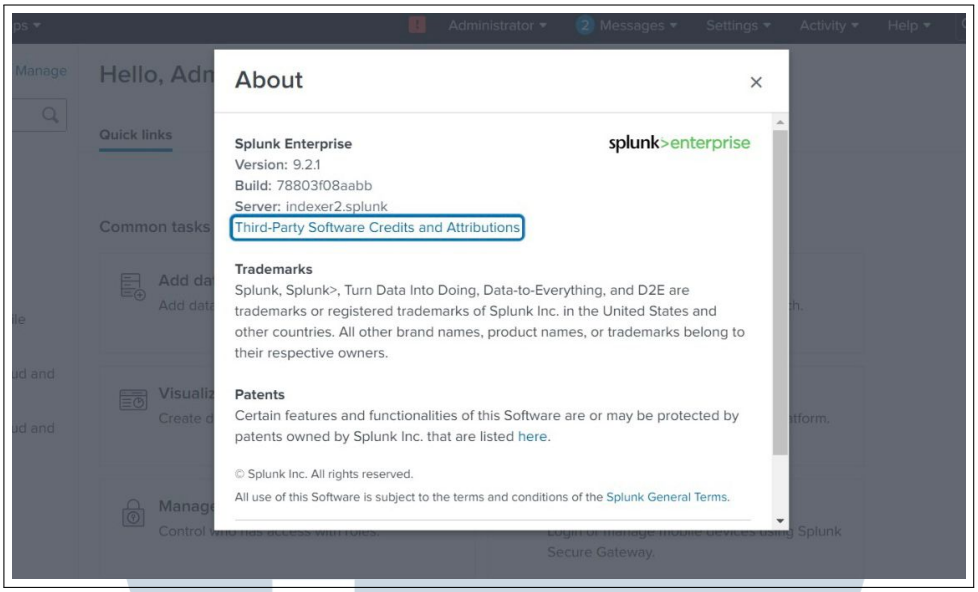
Gambar 3.7. *Command* untuk ekstrak *Installer* Splunk 9.2.1

(d) Gambar 3.8 merupakan **proses mengaktifkan kembali *Service Splunk*** setelah dilakukan *upgrade*. Terlihat bahwa status sudah berubah menjadi **"splunkd is running"**.



Gambar 3.8. Status Splunk sudah aktif kembali

(e) Gambar 3.9 merupakan **pengecekan status versi *Splunk*** sebagai bukti bahwa proses *upgrade* Splunk 9.2.1 telah selesai.



Gambar 3.9. Splunk sudah ter-*upgrade*

B. *Upgrade SSL Certificate User Splunk*

1. ***Issue***: Setelah dilakukan *upgrade* versi Splunk, isu tidak bisa *upload* gambar dan beberapa fitur yang bersifat media masih tidak bisa digunakan.

2. ***Root Cause***: Setelah dilakukan pengecekan kode *error* diasumsikan penyebab isunya adalah kesalahan pada KV Store Splunk yang inti masalahnya berada di SSL *User* admin sudah kedaluwarsa, ini terjadi pada keduanya (*Search Head* dan Indexer).

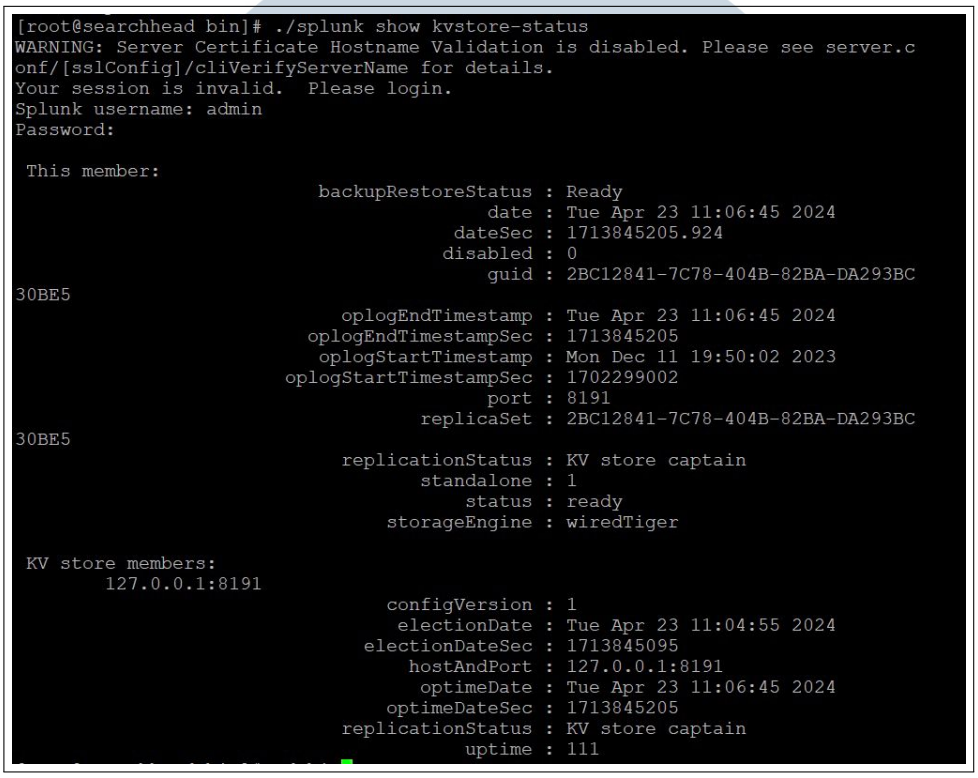
3. ***Solution***: Menelusuri kode *error* di Internet dan mengumpulkan beberapa kemungkinan solusinya, solusi kemudian dipilah dan diputuskan untuk memperbaharui SSL Certificate Splunk User Tokio Marine secara *remote* menggunakan SSH Linux. Berikut adalah langkahnya.

   (a) Gambar 3.10 adalah **proses menonaktifkan *Service* Splunk dan menjalankan *command* Linux** untuk memperbaharui tanggal status SSL *Certificate User* Splunk Tokio Marine.

```
[root@searchhead auth]# openssl x509 -enddate -noout -in /home/splunk/etc/auth/s
erver.pem
notAfter=Apr 23 04:04:34 2027 GMT
[root@searchhead auth]# cd ../..
[root@searchhead splunk]# cd bin
[root@searchhead bin]# splunk show kvstore-status
-bash: splunk: command not found
```

Gambar 3.10. *Command* untuk memperbaharui SSL

(b) Gambar 3.11 adalah **proses pengecekan status KV *Store* setelah dilakukan pembaharuan** terlihat bahwa statusnya sudah menjadi ”*Ready*” kembali yang artinya KV*Store* sudah aktif.



Gambar 3.11. *Output* hasil setelah SSL diperbaharui

C. Pembuatan *User Guide Dashboard Studio* Tokio Marine

1. ***Issue***: Setelah pihak Tokio Marine menyetujui desain *Dashboard Studio* yang dibuat khusus oleh PT GIT, Tokio Marine meminta untuk dibuatkan *User Guide Dashboard Studio*.

2. ***Root Cause***: *User Guide Dashboard Studio* digunakan untuk panduan Tokio Marine jika ingin memodifikasi *Dashboard* mereka sendiri.

3. ***Solution***: Dengan permintaan itu, disusunlah *User Guide Dashboard Studio* khusus untuk Tokio Marine yang berisikan langkah-langkah dan tips pembuatan *Dashboard Studio*. Gambar 3.12 adalah tampilan halaman judul *User Guide*.

Gambar 3.12. *Cover User Guide Dashboard Studio* Tokio Marine

3.4.2 *Explorative Maintenance* Splunk Tokio Marine

A. Permintaan *Upgrade Classic Dashboard* ke versi *Dashboard Studio*

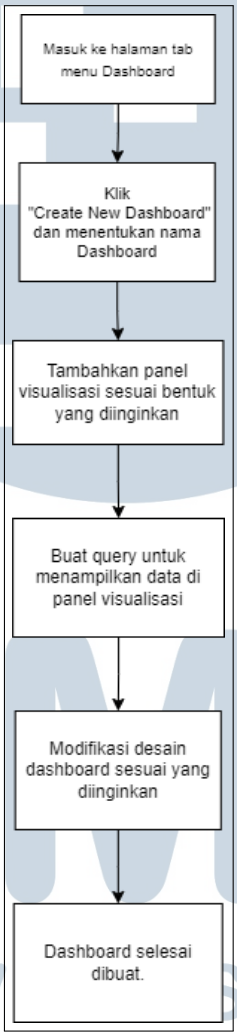
1. ***Issue***: Pihak Tokio Marine menginginkan tampilan *dashboard* mereka lebih menarik karena yang digunakan sebelumnya adalah *Classic Dashboard* yang memiliki tampilan monoton.

2. ***Root Cause***: *Dashboard Studio* memiliki fitur yang lebih banyak dibandingkan fitur *Classic Dashboard* sehingga dapat dimodifikasi

sedemikian rupa sesuai keinginan *User*.

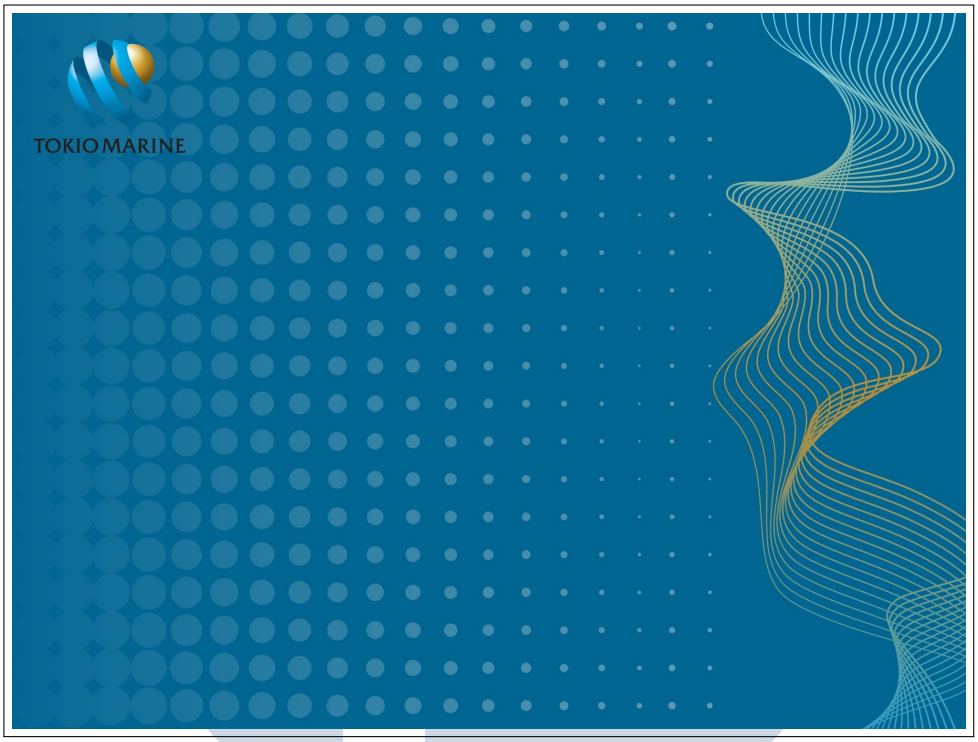
3. ***Solution***: Karena baru pertama kali melakukan implementasi nyata terhadap *Dashboard Studio* dan banyak yang perlu didalami, selama pengerjaan perlu dilakukan eksplorasi terhadap kegunaan fiturnya.

   Pembuatan *Dashboard Studio* memiliki tahap-tahap seperti pada bagan di gambar 3.13.



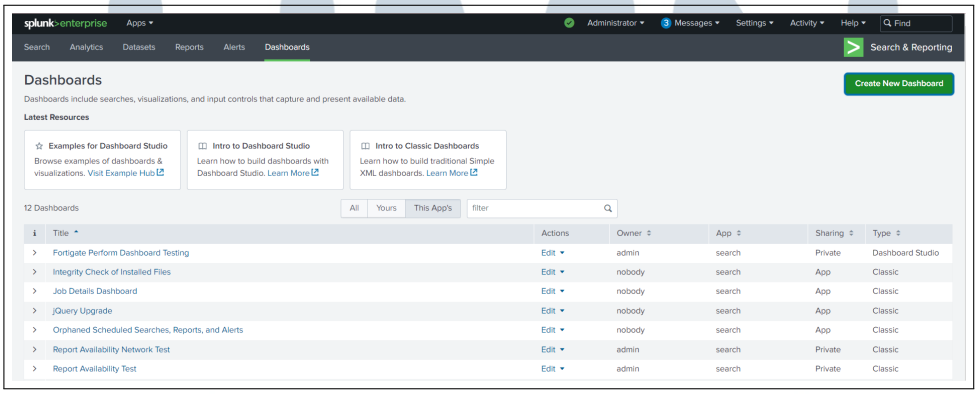
Gambar 3.13. Bagan tahap pembuatan *Dashboard*

Yang pertama dilakukan adalah pembuatan desain *dashboard background* dengan menggunakan Canva sebagai wadah untuk membuat desainnya. Gambar 3.14 adalah desain *background* yang dibuat khusus untuk Tokio Marine.



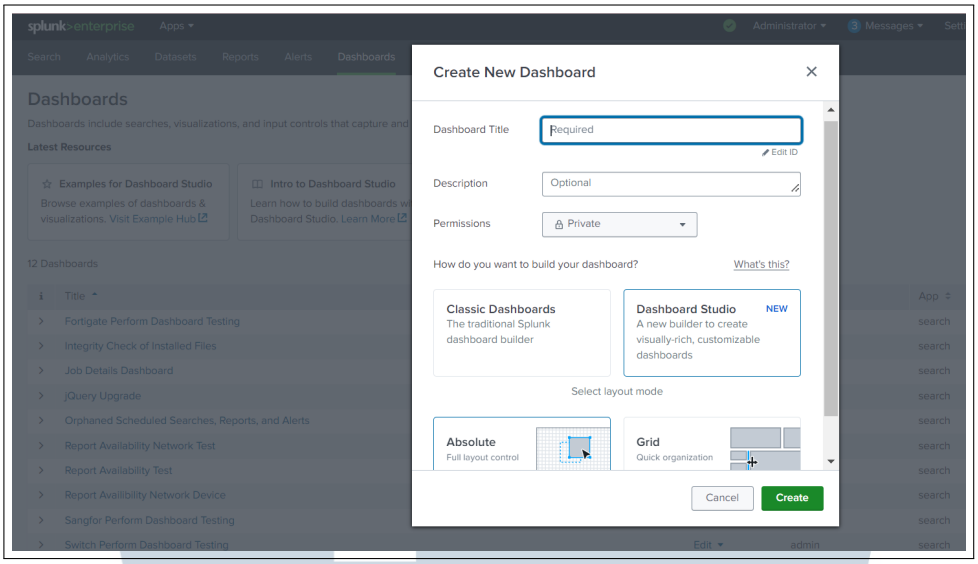
Gambar 3.14. Desain *background dashboard* TMI

Setelah melakukan desain *background Dashboard* di aplikasi Canva, pembuatan *Dashboard* dimulai dengan memasuki *page* untuk *"Create New Dashboard"* seperti yang ada di gambar 3.15 berikut.



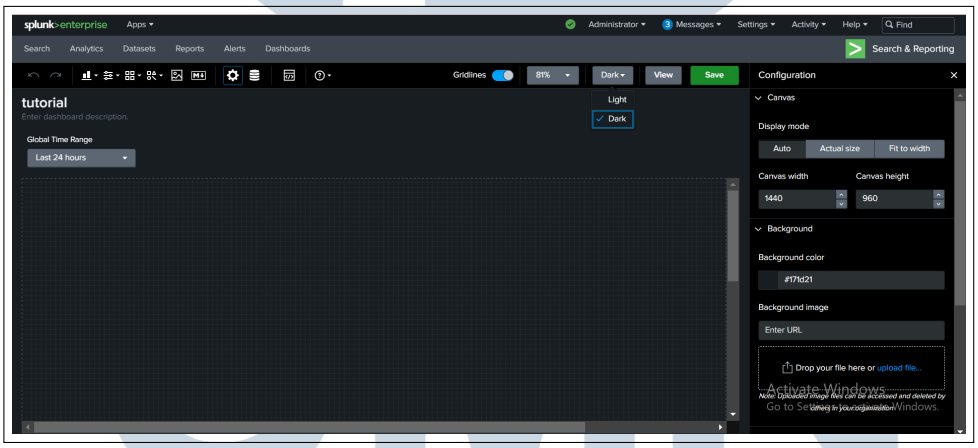
Gambar 3.15. Halaman untuk memulai pembuatan *Dashboard*

Selanjutnya setelah menekan tombol *"Create New Dashboard"*, maka akan muncul panel seperti di gambar 3.16 untuk memasukkan nama *Dashboard* dan menentukan jenis *Dashboard* yang akan dibuat, karena PT Tokio Marine meminta dibuatkan *Dashboard Studio* maka yang dipilih adalah *Dashboard Studio*.



Gambar 3.16. Panel membuat *Dashboard*

Setelah klik tombol ”*Create*”, maka halaman akan beralih ke *Dashboard* baru yang memiliki tampilan *default* seperti di gambar 3.17.

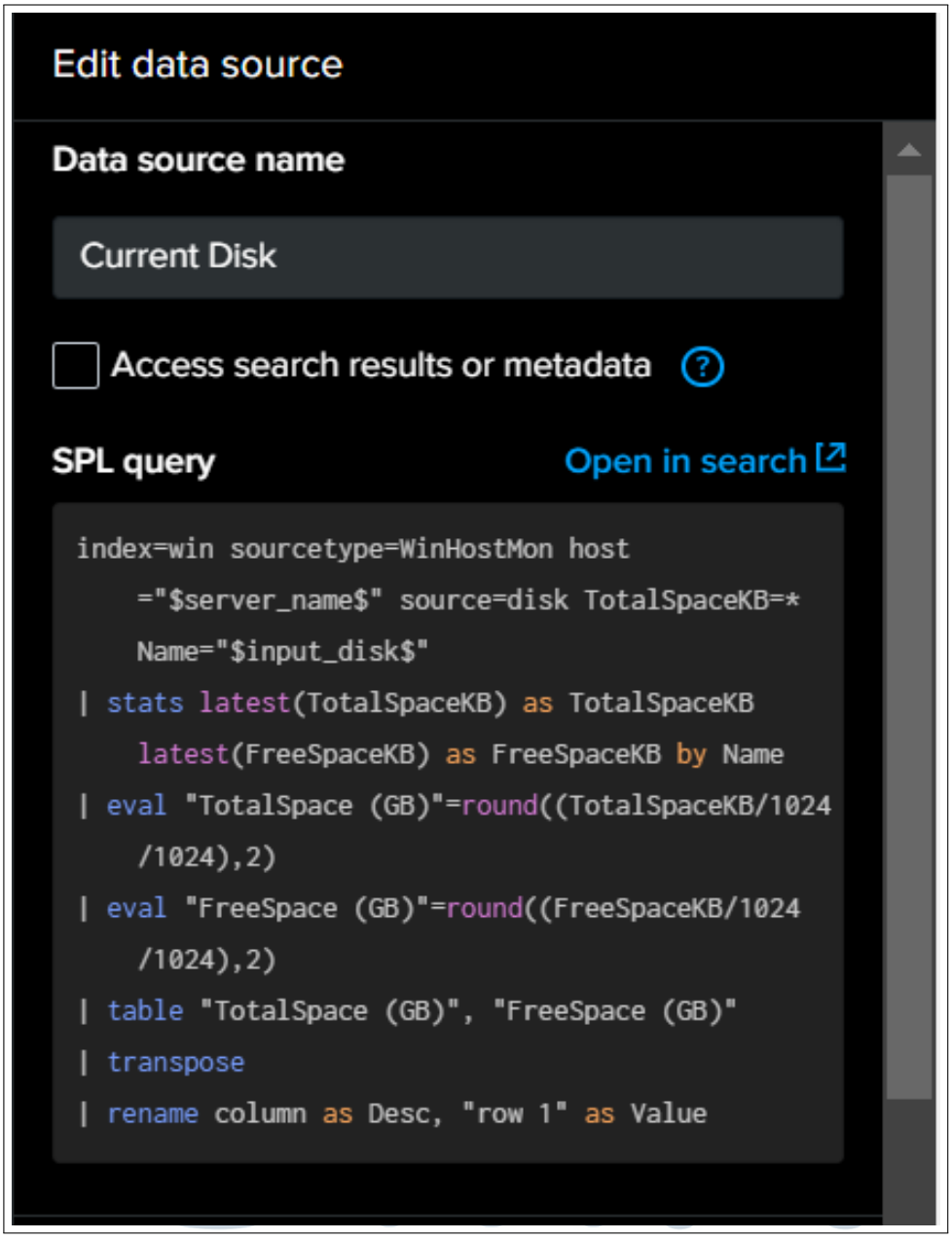


Gambar 3.17. Tampilan *default Dashboard*

Untuk menambahkan visualisasi data, pengguna dapat memilih bentuk visualisasi yang diinginkan dengan pilihan seperti di gambar 3.18.

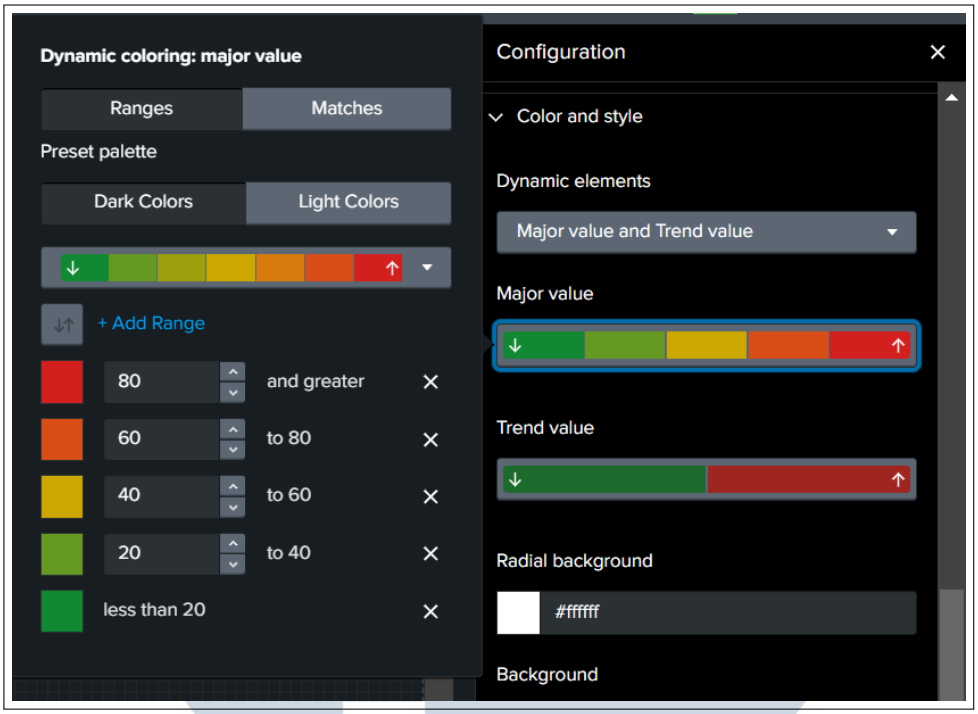
Gambar 3.18. *Toolbar* pilihan bentuk visualisasi data

Untuk menampilkan data dalam panel visualisasi, dibutuhkan *query* yang dinamakan Splunk *Query Language*, *query* ini menyesuaikan kebutuhan pengguna ingin menampilkan data seperti apa, dalam konteks gambar 3.19, *query* ini mengambil dan menampilkan data kalkulasi penggunaan *Disk*.



Gambar 3.19. *Query* untuk visualisasi

Selanjutnya untuk memodifikasi panel visualisasi data agar terlihat lebih menarik, Splunk menyediakan fitur pewarnaan dinamis yang dapat disesuaikan dengan kebutuhan pengguna. Contoh penggunaannya yaitu seperti di gambar 3.20 berikut, dimana disini terdapat *range* angka yang akan menentukan kapan dia akan berwarna Hijau, Kuning, ataupun Merah.



Gambar 3.20. Fitur pewarnaan dinamis pada Splunk *Dashboard*

Penggunaan dan mengatur panel visualisasi juga bisa dilakukan tanpa batas sesuai keinginan dan kebutuhan pengguna, hanya perlu membuat *query* di panel menu *"Data Source"* seperti pada gambar 3.21, dimana disini terkumpul semua daftar *query* untuk pemanggilan dan menampilkan data di tiap panel visualisasi.

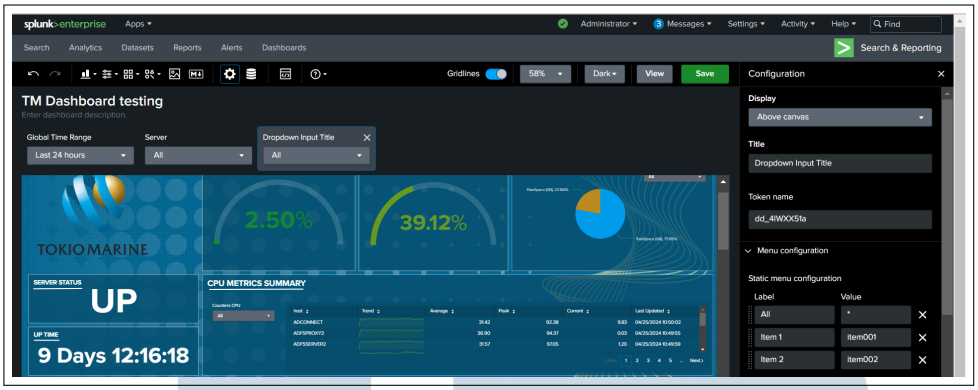
Gambar 3.21. *Toolbar* untuk membuat kumpulan *query* sumber data visualisasi

Setelah membuat dan mengatur panel visualisasi data di *Dashboard*, selanjutnya merupakan penambahan *dropdown* untuk mengelompokkan

visualisasi data sesuai dengan kategori yang ingin dipilih, dalam gambar 3.22 merupakan cara menambahkan *dropdown*.

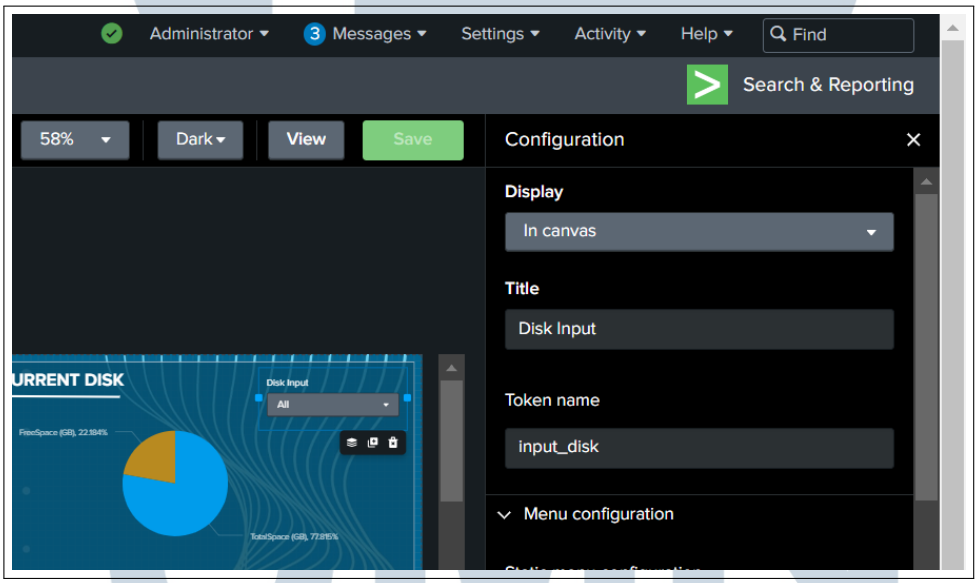
Gambar 3.22. *Toolbar* pilihan untuk *Inputs*

Selanjutnya setelah memilih ”*Dropdown*”, akan muncul *default dropdown* seperti di gambar 3.23.



Gambar 3.23. *Default dropdown*

Dropdown kemudian dimasukkan ke dalam *canvas Dashboard* agar terlihat lebih spesifik dan rapi seperti di gambar 3.24.

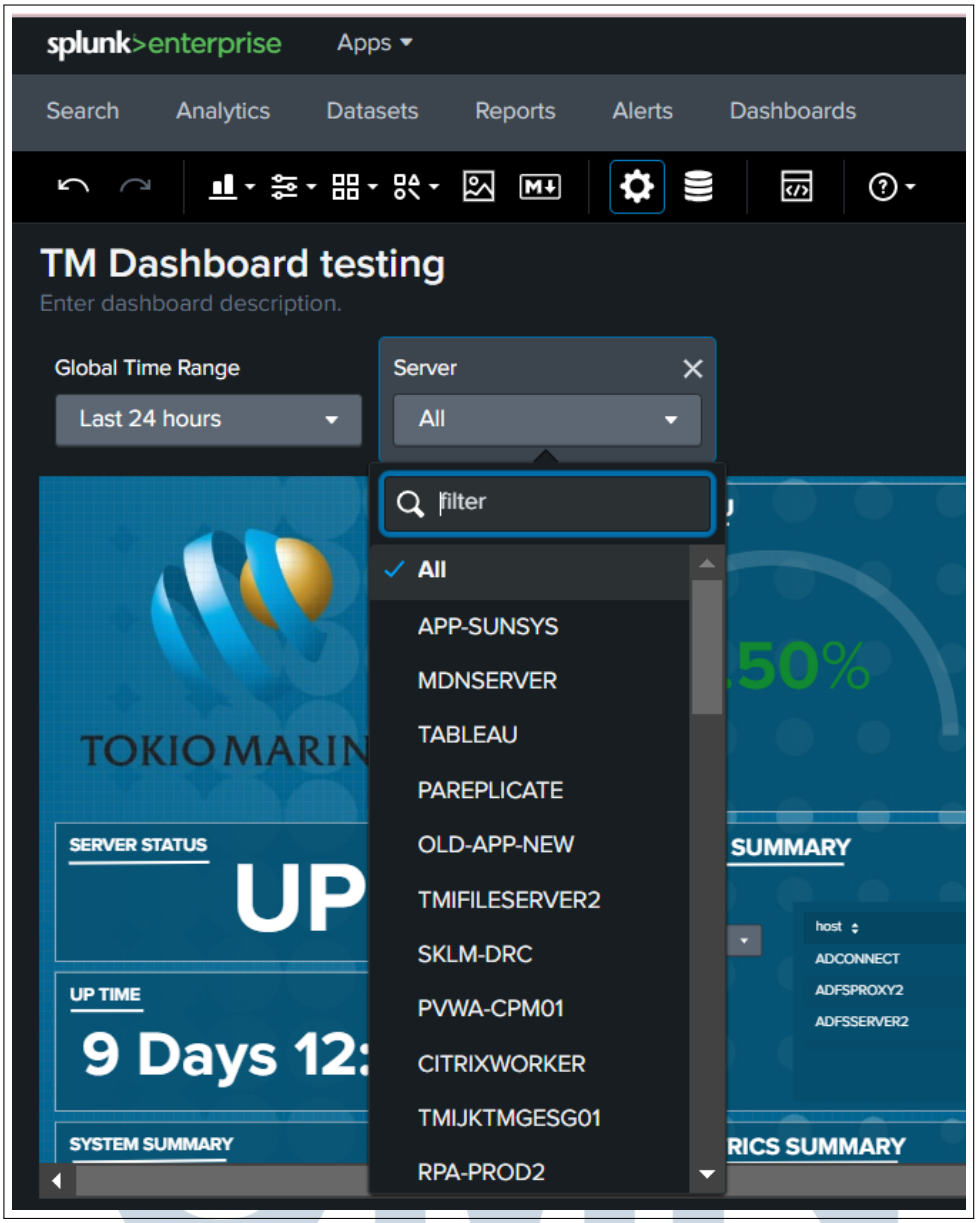


Gambar 3.24. Pengaturan *dropdown in canvas*

Dropdown juga membutuhkan *query* khusus untuk menampilkan data, salah satunya yaitu berada di gambar 3.25.

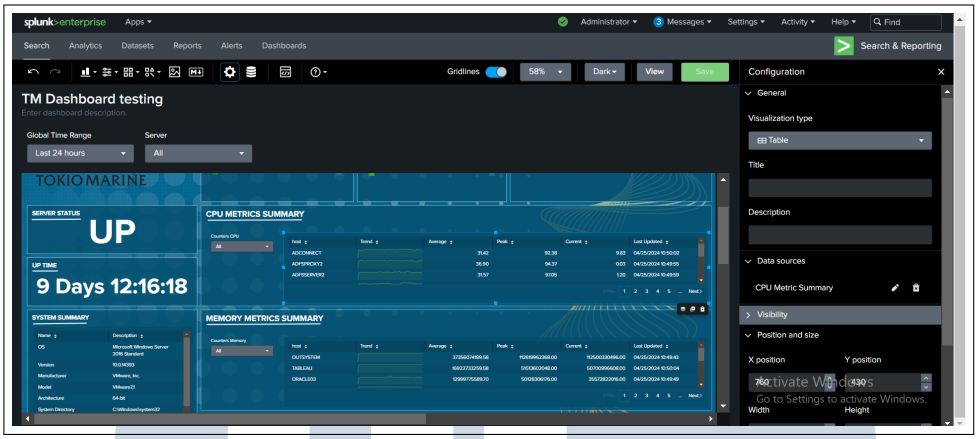
Gambar 3.25. *Query* khusus untuk data *dropdown*

Setelah token *dropdown* dibuat melalui *query*, maka *dropdown* akan memiliki daftar perangkat atau kategori yang diinginkan seperti pada gambar 3.26.

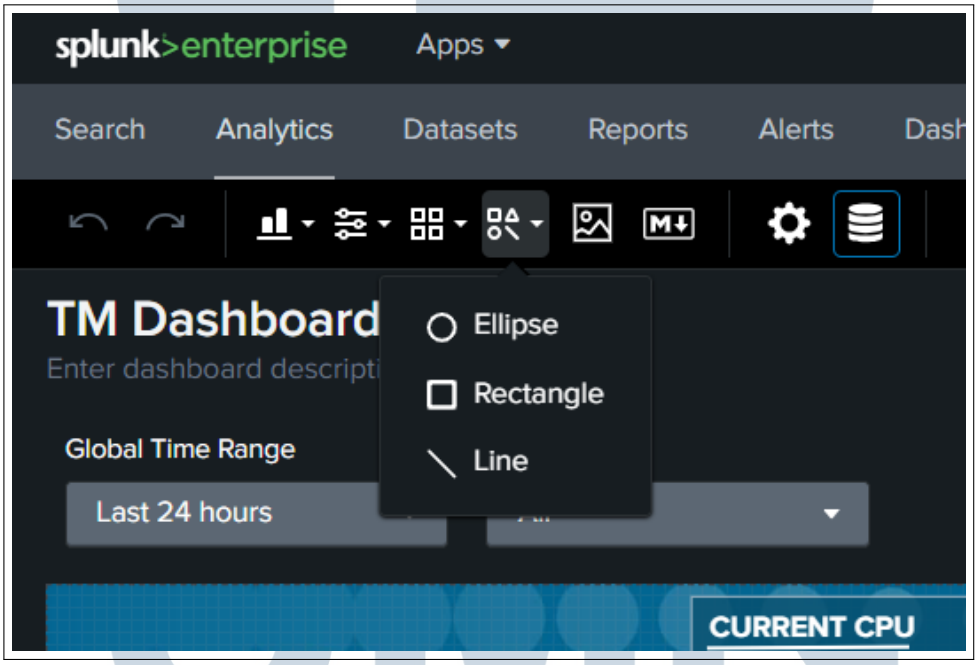


Gambar 3.26. Hasil penggunaan *query dropdown*

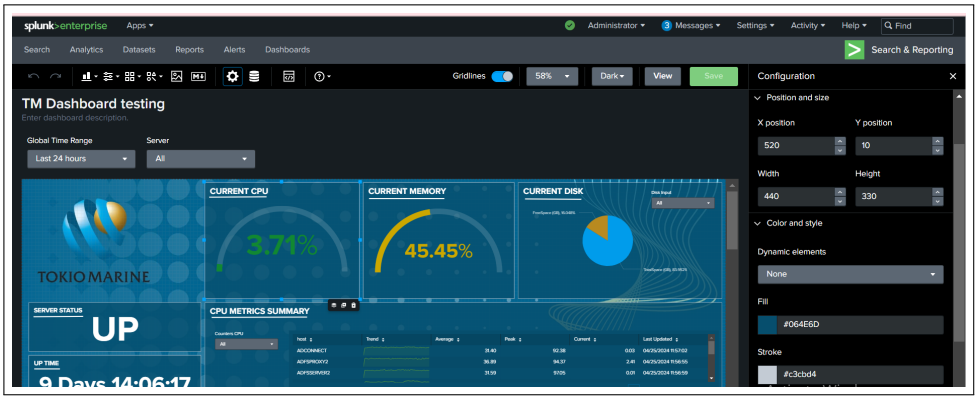
Ada beberapa visualisasi yang juga dapat digunakan menyesuaikan dengan kebutuhan dan keinginan pengguna, beberapa yang digunakan dalam *Dashboard* Tokio Marine yaitu pada gambar 3.27 yang merupakan visualisasi tabel dan gambar 3.28 yang merupakan visualisasi bentuk yang akan digunakan sebagai *background* dari setiap panel visualisasi seperti pada gambar 3.29.



Gambar 3.27. Visualisasi berbentuk tabel

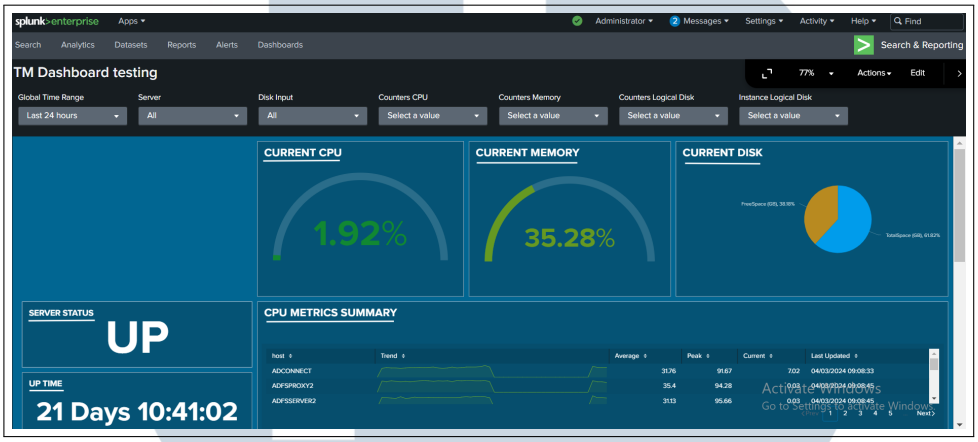


Gambar 3.28. *Toolbar* untuk menambahkan *shape*



Gambar 3.29. Penggunaan *shapes* sebagai *background* panel visualisasi

Pembuatan komponen *Dashboard* telah dilakukan, sehingga yang tersisa adalah penambahan desain *background* yang sudah dibuat di awal, gambar 3.30 merupakan desain *dashboard* sebelum dimasukkan *background* dan sedang dalam proses pembuatan *Dashboard Studio*.

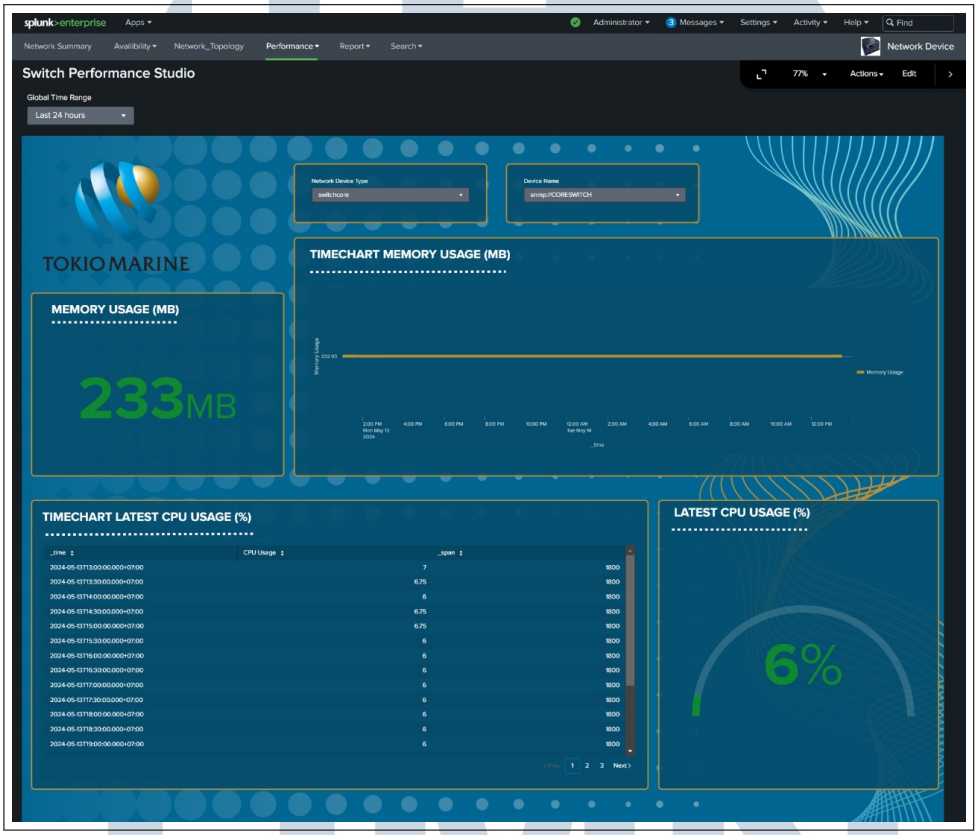


Gambar 3.30. Proses pembuatan *dashboard* TMI

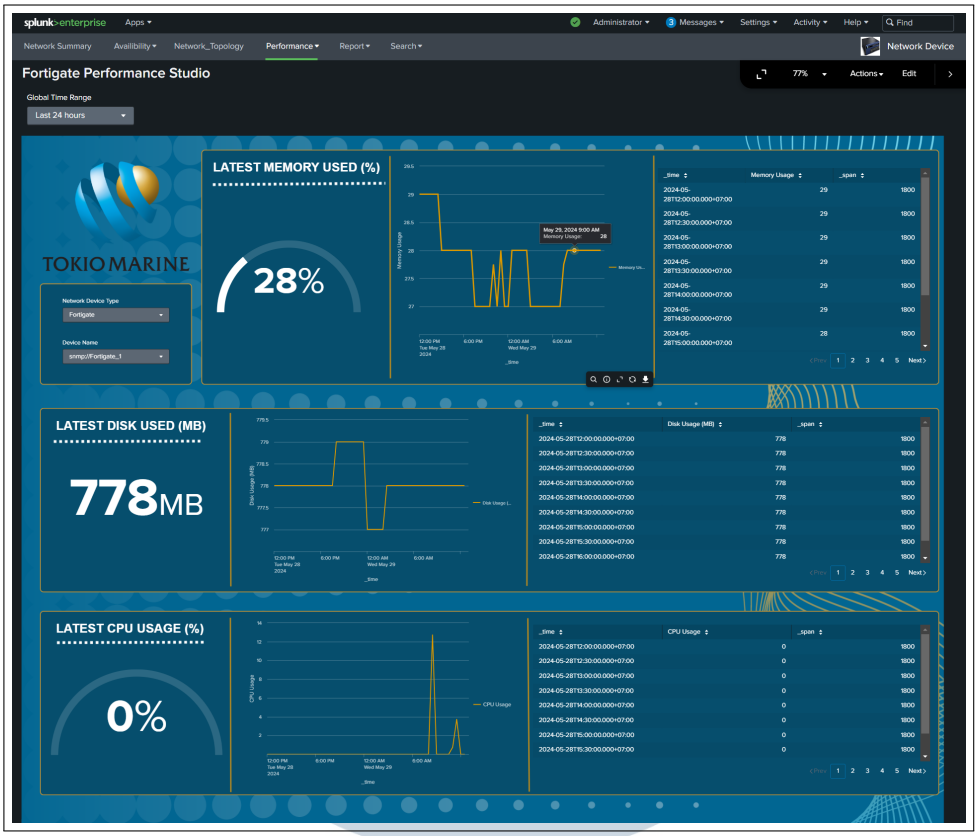
Gambar 3.31 merupakan hasil modifikasi dan perancangan dari *Dashboard Studio* milik Tokio Marine dan kemudian didemonstrasikan saat *Weekly Report Meeting* di hari Jumat bersama PT Tokio Marine.

Gambar 3.31. Hasil *Dashboard Studio* TMI

Gambar 3.32 dan gambar 3.33 merupakan beberapa modifikasi *dashboard* lainnya atas permintaan dari pihak klien, kali ini informasi yang digunakan untuk *Dashboard Studio* adalah *monitoring Network Device* milik Tokio Marine. Untuk prosedur pembuatannya juga hampir sama dengan pembuatan *Dashboard Server Profile*.



Gambar 3.32. Hasil *Dashboard Studio Network Device* TMI Switch



Gambar 3.33. *Dashboard Studio Network Device* TMI Fortigate

3.5 Kendala dan Solusi yang Ditemukan

3.5.1 Kendala

Selama pelaksanaan magang di PT Global Innovation Technology sesuai dengan tugas yang diuraikan di sub-bab 3.4 Hasil dan Implementasi, diantaranya terdapat kendala sebagai berikut.

1. Teori Splunk sudah dipelajari namun implementasi langsung baru dilakukan saat ini, sehingga diperlukan eksplorasi lanjutan terkait dengan *maintenance* Splunknya.
2. Isu yang terjadi pada Splunk Tokio Marine didapatkan dari permintaan klien yang membutuhkan beberapa waktu untuk eksplorasi dan pengerjaan karena tim yang bertugas hanya sekitar 3 orang dengan satu orang yang merupakan *Technical Lead.*
3. *Timeline Maintenance* menjadi sedikit lebih lama karena banyak isu yang secara tiba-tiba muncul selama pengerjaan.

3.5.2 Solusi

Adapun dalam sub bab ini akan diuraikan solusi dari tiap poin kendala yang sudah disebutkan sebelumnya. Berikut uraiannya.

1. Melakukan eksplorasi sesuai dengan arahan bantuan dari *Technical Lead* dan mencari di dokumentasi yang disediakan oleh Splunk untuk *Technical*.
2. Bertanya kepada *Technical Lead* selaku senior atau *Project Manager* perihal apa yang menjadi kesulitan dan dilakukan eksplorasi bersama-sama di dokumentasi Splunk saat isu yang menjadi alasan pemagang kesulitan juga belum diketahui oleh *Technical Lead* dan *Project Manager*. Meski dengan keterbatasan SDM, pelaksanaan kerja juga tetap dapat dilakukan dengan baik.
3. Urutan pengerjaan dilakukan dari yang paling mudah hingga penyelesaian pekerjaan tetap tepat waktu.