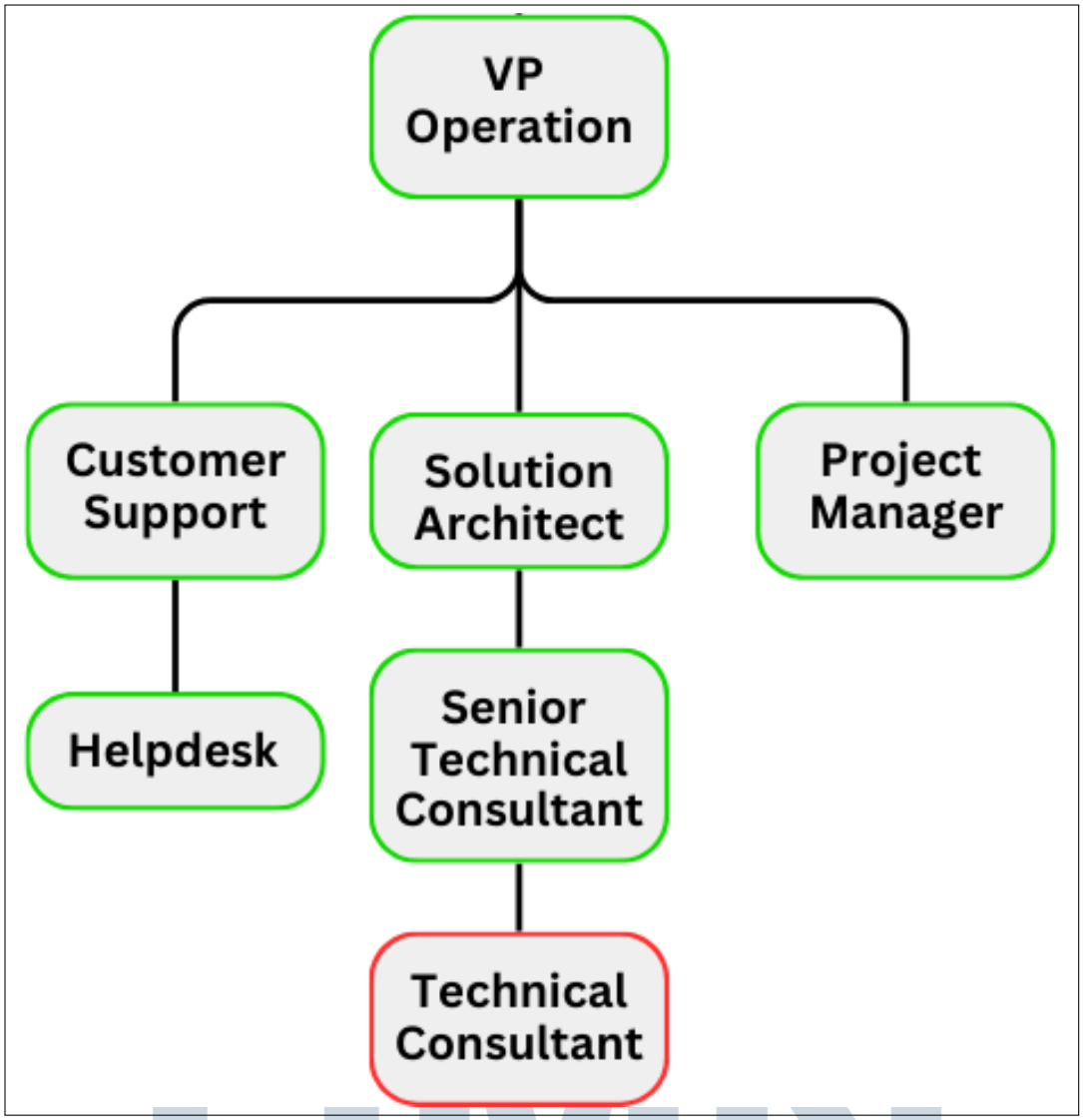
BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Organisasi

Sesungguhnya kedudukan dan orginisasi dapat dibagi menjadi dua kategori, yakni internal yang berarti perusahaan tempat pelaksanaan magang berlangsung yaitu di PT. Global Innovation Technology (GIT) dan organisasi proyek bersama dengan klien. Berikut adalah penjelasan lengkapnya:

3.1.1 Internal PT. GIT

Menurut struktur organisasi GIT, posisi *Technical Consultant* (TC) berada pada departemen Operasional. Adapun departemen ini dipimpin oleh Bapak Ahmad Rizki selaku *Vice President* (VP) dan juga sebagai *supervisor* peserta magang. Walaupun apa yang terjadi dilapangan, tugas-tugas tetap diberikan melalui *Project Manager* (PM). Bapak Wahyu Erlangga merupakan PM yang mengurus proyek pada PT. Bursa Efek Indonesia (BEI). Selain itu, terdapat tim pendukung seperti *Solution Architect* (SA) dan Senior TC yang mengidentifikasi dan menganalisis kebutuhan klien yaitu, Bapak Akmal Faudzan dan Bapak Arya sena. Sederhananya VP memiliki tanggung jawab untuk mengawasi divisi secara keseluruhan, PM bertugas untuk mengelola suatu proyek dan koordinasi tim, serta SA/TC berperan sebagai *implememtor*. Adapun struktur organisasi pada dapartemen *operational* terlihat sebagaimana pada Gambar 3.1.



Gambar 3.1. Struktur Dapartemen Operasional

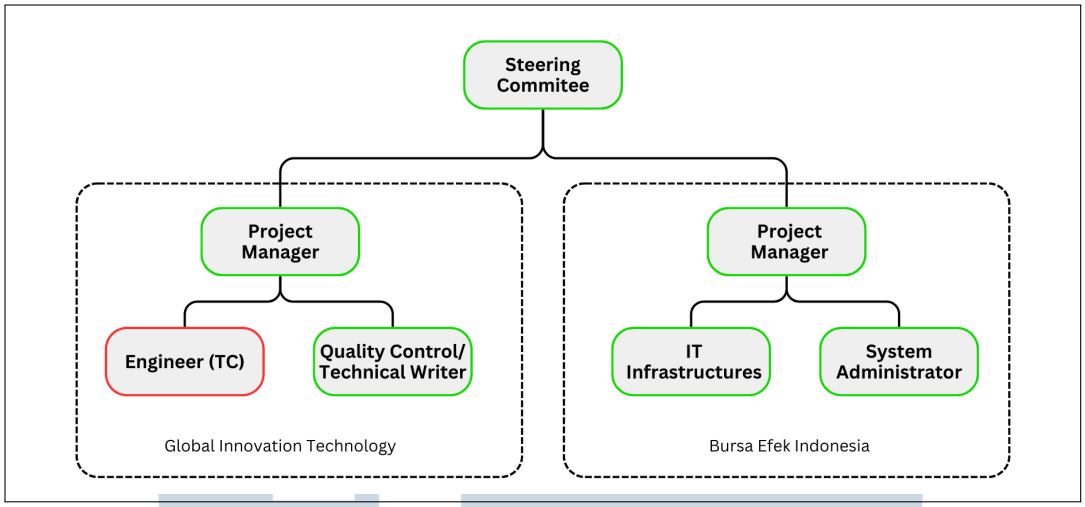
Proses berjalannya suatu proyek pada GIT memiliki alur kerja yang dinamis. Dimana seluruh divisi dapat berkerja sama untuk mendapatkan hasil yang terbaik sesuai dengan kebutuhan klien. Alur kerja proyek (khususnya yang sedang berjalan/berlangsung) dimulai dari permintaan klien kepada PM, ini biasanya terkait permasalahan, penambahan *use case*, dan *fallback*. Kemudian PM akan membuat keputusan untuk mengatur waktu pengerjaan, koordinasi dengan VP, dan pemberian tugas. TC akan menerima tugas yang telah diberikan PM serta bertanggung jawab untuk memberikan solusi kepada klien. Segala bentuk penyampaian rencana kerja *(mock)* baru atau permintaan oleh klien dapat dikoordinasikan melalui platform G Meet, E-mail dan Whatsapp. Proses implementasi dilakukan baik pada *Graphical User Interface* (GUI) Splunk dan *terminal* OS klien secara *onsite*. Hal ini biasanya

diminta oleh klien karena kebijakan yang berlaku untuk menjamin keamanan *IT services* perusahaan.

Sementara untuk alur kerja ketika GIT ingin mengajukan proyek kepada klien baru, biasanya dibagi menjadi dua fase yakni *pre-sales* dan *post-sales*. *Pre-sales* merupakan proses kegiatan menjelang penjualan sebenarnya seperti memahami kebutuhan pelanggan, mengusulkan solusi melalui *Prof of Concept* (PoC), dan menegosiasikan persyaratan kesepakatan. Sedangkan untuk *post-sales* adalah kegiatan setelah penjualan selesai dan berfokus pada implementasi solusi yang telah diajukan dan disepakati bersama sebelumnya. Pada proses *pre-sales*, VP akan melakukan pertemuan rapat internal baik itu oleh PM maupun SA dan TC. Rapat membahas kebutuhan klien hingga perencanaan pembagian tugas tim terhadap keterlibatan dalam menyusun PoC. Peran SA dan TC disini diperlukan untuk merancang topologi Splunk, penilaian sumber data, dan penentuan *technical deployment* seperti konfigurasi pada *server*. Sementara fase *post-sales*, SA dan TC bertanggung jawab untuk melakukan implementasi apa yang telah dirancangkan sebelumnya. Fase *post-sales* ini berlanjut hingga pemberikan dukungan pengembangan dan pemeliharaan.

3.1.2 Berdasarkan Proyek

Pelaksanaan magang berlangsung dengan turut serta membantu implementasi pengembangan dan pemeliharaan platform Splunk pada klien terkhususnya pada BEI. Sebagai *implentator*, TC bertanggung jawab dalam memenuhi kebutuhan klien dalam mengelola data mentah menjadi hal yang dapat dimonitor untuk mendapatkan wawasan. Namun dalam proses pelaksanaannya, proyek kerja sama antara GIT dengan BEI memiliki struktur organisasi proyek agar dapat berjalan secara lancar dan terorganisir. Gambar 3.2 menunjukan struktur organisasi proyek GIT dengan BEI. Dengan adanya struktur organisasi ini pekerjaan akan terstruktur dan profesional. TC hanya dapat arahan untuk melakukan implementasi satu pintu dari PM GIT yakni Bapak Wahyu. Oleh karena itu, pihak BEI jika ingin melakukan tambahan *Scope of Work* (SoW) atau *mock* baru perlu dikordinasikan ke Bapak Wahyu selaku PM terlebih dahulu.



Gambar 3.2. Struktur Proyek Dengan Klien

3.2 Tugas yang Dilakukan

Selama pelakasanaan magang berlangsung, TC *intern* diberikan kepercayaan untuk bertanggung jawab melakukan implementasi dan pemeliharaan platform *big data monitoring* Splunk pada PT. Bursa Efek Indonesia (BEI). Skenario atau rencana implementasi dan pemeliharaan di BEI disebut dengan *mock* dan ini perlu persetujuan kedua belah pihak. Kemudian untuk jadwal pelaksanakan kegiatan *mock* tersebut telah ditetapkan BEI dihari Jumat dan Sabtu di gedung Cyber-1. Hari tersebut ditentukan BEI untuk menghindari serta tidak mengganggu operasional perdagangan. Umumnya kegiatan *mock* dapat dijabarkan sebagai berikut:

1. Implementasi

   Tahap implementasi melibatkan pelaksanaan *mock* atau simulasi dari proses yang akan diimplementasikan. Pada tahap ini, klien biasanya memperkenalkan *use case* atau protokol baru yang memerlukan konfigurasi khusus. Sebagai TC, tanggung jawab utama adalah memastikan bahwa sistem Splunk dapat mengumpulkan dan memonitor data yang terkait dengan protokol baru ini. Ini melibatkan penyesuaian konfigurasi dan pengujian untuk memastikan data dapat diakses dan dianalisis dengan baik dalam platform Splunk agar dapat divisualisasikan.

2. *Fallback*

   Setelah tahap implementasi, tahap berikutnya adalah *fallback*, yang biasanya dilakukan pada hari berikutnya. Pada tahap ini, klien melakukan pengecekan

menyeluruh untuk memastikan bahwa semua data tersedia dan sesuai dengan kebutuhan operasional mereka. Jika klien telah mengonfirmasi bahwa implementasi berjalan sesuai rencana, TC bertanggung jawab untuk mengembalikan sistem ke kondisi semula. Ini penting untuk mencegah gangguan pada protokol yang sudah ada atau proses bisnis yang sedang berjalan. Proses *fallback* juga memastikan bahwa perubahan sementara yang dilakukan selama implementasi tidak berdampak negatif pada stabilitas sistem.

3. *Pre-live*

   Tahap terakhir dalam proses ini adalah *prelive*. Pada tahap ini, setelah beberapa kali pelaksanaan *mock*, dan jika klien merasa bahwa protokol baru memenuhi kebutuhan operasionalnya, maka solusi tersebut siap untuk di-*deploy* secara penuh. Tahap *prelive* bertujuan untuk melakukan pengujian akhir dan memastikan bahwa setiap perubahan telah dievaluasi dengan hati-hati untuk memastikan kesuksesan implementasi dalam lingkungan produksi. TC berperan dalam memverifikasi kesiapan sistem dan mengidentifikasi potensi masalah sebelum implementasi penuh dilakukan. Dengan demikian, tahap *prelive* adalah langkah penting untuk menjamin transisi yang lancar ke implementasi produksi tanpa mengganggu operasi yang ada.

3.3 Uraian Pelaksanaan Magang

Pelaksanaan kerja magang diuraikan seperti pada Tabel 3.1, yang mencakup serangkaian kegiatan bertujuan untuk memberikan pengalaman praktis dalam lingkungan kerja nyata. Tabel 3.1 di bawah merangkum aktivitas dan tugas yang dilaksanakan selama periode magang. Maka dari itu, penjelasan lebih rinci diperlukan untuk memberikan gambaran yang lebih komprehensif tentang bagaimana pelaksanaan magang dirancang dan diimplementasikan, serta untuk memberikan wawasan tentang kontribusi peserta magang kepada perusahaan. Dalam bagian ini, isi tabel akan diuraikan dalam beberapa sub-bab untuk memberikan pemahaman yang lebih mendalam mengenai peran dan tanggung jawab yang diemban selama magang berlangsung. Lebih lanjut, rincian ini juga akan mencakup pembelajaran dan tantangan yang dihadapi selama periode magang, serta bagaimana pengalaman ini berkontribusi pada pengembangan profesional dan akademis peserta magang.

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

No.	Minggu Ke -	Pekerjaan yang dilakukan
1.	1	*Introduction*: Pengenalan lingkungan kerja, penjelasan tugas, penempatan tim proyek.
2.	2 - 3	*Training*: Mempelajari dan mengerjakan kursus khusus *official* dari Splunk.
3.	4 - 6	*Training*: Pelatihan insentif oleh Splunk *Expert* mengenai security dan IT *Architecture* perusahaan.
4.	6 - 8	*Training*: Pelatian insentif oleh Splunk *Expert* mengenai Splunk Core.
5.	8 - 10	*Training*: Mempelajari dan mengerjakan *best practice* Splunk topology untuk perusahaan.
6.	10 - 12	*Implement*: Pembuatan Visualisasi *Server* dan *Network Device Availbility* untuk klien.
7.	12 - 15	*Implement*: Implementasi dan *fallback* fitur *services* pada klien.
8.	16 - 19	*Implement*: Imlementasi dan *fallback* untuk aktivasi server protokol baru klien.
9.	18 - 19	*Preventive Maintenance* untuk periode Februari dan Mei 2024 untuk klien.

3.3.1 Minggu 1: Pengenalan dan *Onboarding*

Minggu pertama magang di GIT, dimulai pada tanggal 2 Januari 2024 yang berfokus pada perkenalan dan *onboarding*. Tahap ini sangat penting untuk membangun fondasi bagi peserta magang dalam memahami lingkungan kerja dan struktur perusahaan. Proses *onboarding* dipimpin oleh salah satu HR GIT dan melibatkan beberapa kegiatan yang dirancang untuk membantu peserta magang merasa diterima dan siap bekerja. Tahap pertama dalam proses ini adalah pengenalan kepada tim operasional secara keseluruhan. Peserta magang diberi kesempatan untuk bertemu dengan rekan kerja satu divisi. Interaksi ini membantu peserta magang untuk mengenal dinamika tim dan membangun hubungan awal antar sesama karyawan.

Peserta magang diberi pemahaman tentang lini bisnis perusahaan. GIT memiliki fokus pada solusi teknologi informasi, dan peserta magang diberi

wawasan tentang berbagai layanan dan produk yang ditawarkan perusahaan. Penjelasan ini membantu peserta magang memahami konteks bisnis di mana mereka akan bekerja, serta memberi gambaran tentang sektor industri yang dilayani oleh GIT. Salah satu aspek penting dari *onboarding* ini adalah penjelasan singkat mengenai platform Splunk, yang menjadi layanan dan produk unggulan perusahaan. Splunk adalah platform analitik data yang digunakan oleh GIT dalam berbagai proyek dengan berbagai klien. Pengenalan ini mencakup dasar-dasar penggunaan Splunk, serta bagaimana platform ini digunakan dalam konteks proyek yang sedang berjalan.

Gambar 3.3. Logo Splunk

Selain itu, peserta magang juga diberi informasi tentang klien-klien yang saat ini bekerja dengan GIT. Supervisi dari perusahaan memberikan gambaran tentang proyek-proyek yang sedang berlangsung, memberikan peserta magang kesempatan untuk memahami kebutuhan klien dan ekspektasi yang harus dipenuhi selama magang. Untuk mendukung komunikasi internal, peserta magang juga diberikan akses seperti pembuatan alamat *email* kantor. Hal ini bertujuan untuk berkomunikasi secara profesional dengan rekan kerja dan klien, serta mengakses sumber daya perusahaan yang dibutuhkan untuk menyelesaikan tugas.

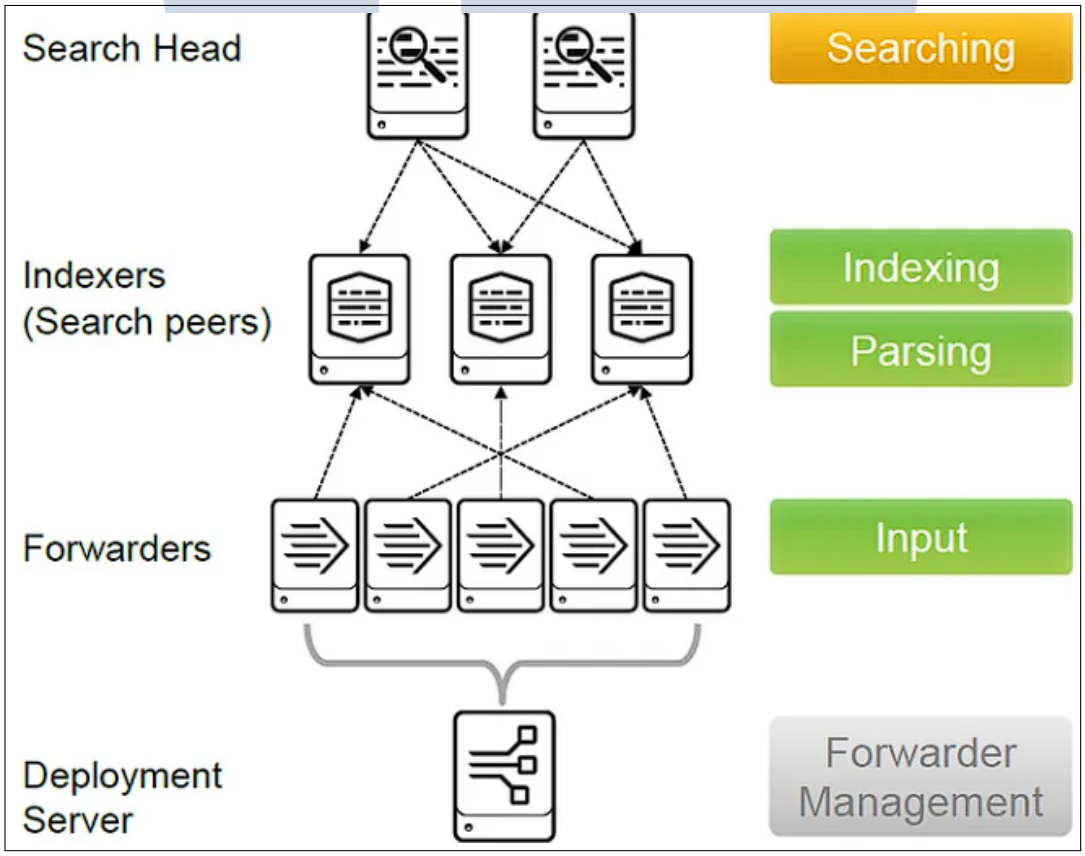
Secara keseluruhan, minggu pertama yang berfokus pada perkenalan dan *onboarding* adalah langkah awal yang penting dalam memastikan peserta magang merasa terhubung dengan tim dan memiliki pemahaman yang baik tentang perusahaan serta tugas-tugas yang akan menjadi tanggung jawab. Dengan dasar yang kuat ini, peserta magang siap melanjutkan ke tahap berikutnya dalam pengalaman magang di GIT.

Untuk peserta magang pada divisi TC ada beberapa *software tools* penting yang digunakan untuk mendukung berbagai tugas dan kegiatan. GIT memberikan kesempatan pelatihan guna meningkatkan kompetensi terhadap penggunaan *tools* untuk peserta magang sebelum siap melakukan tugas di klien. Berikut adalah

penjelasan mengenai beberapa *tools* tersebut dan fungsinya dalam konteks penggunaannya di klien yakni BEI:

A. Splunk

Splunk adalah platform analitik data yang dirancang untuk menangani *big data*, khususnya data yang dihasilkan oleh mesin (*machine-generated data*), seperti *logs*, *metrics*, dan *traces* yang berasal dari infrastruktur IT dan sistem keamanan. Splunk memungkinkan pengguna untuk mengumpulkan, menganalisis, dan memvisualisasikan data dalam berbagai bentuk, membantu perusahaan untuk memantau dan mengambil keputusan berdasarkan data yang akurat.

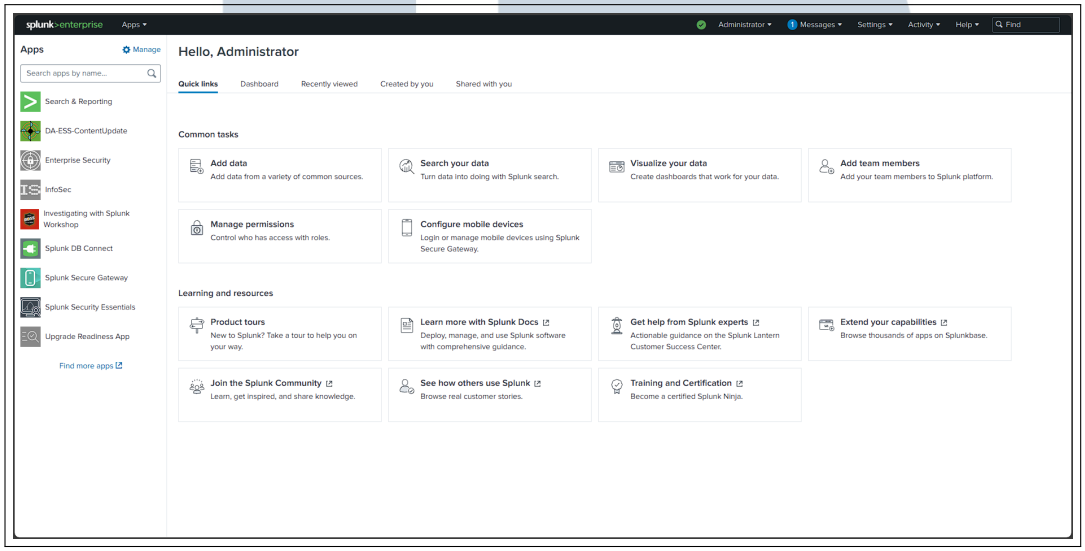


Gambar 3.4. Topologi Aristektur Splunk

Sumber: [4]

Splunk memiliki tiga komponen utama yakni *Forwarder*, *Indexer*, dan *Search Head*. *Forwarder* bertugas mengirimkan data dari sumber eksternal ke sistem Splunk. *Indexer* bertanggung jawab untuk menyimpan dan mengindeks data yang diterima, sehingga data dapat diakses dengan cepat untuk analisis. *Search*

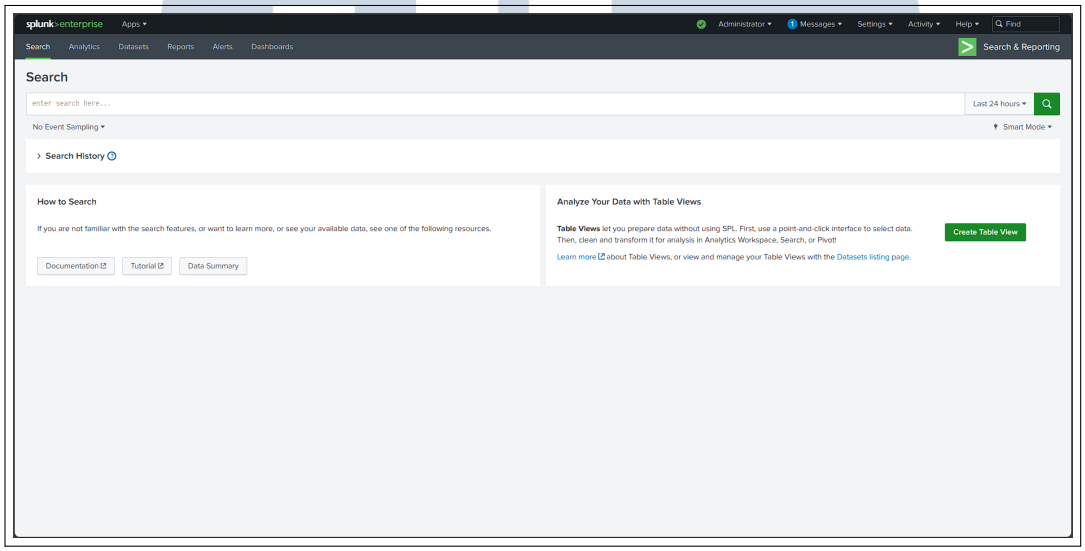
Head adalah antarmuka yang memungkinkan pengguna melakukan pencarian dan visualisasi data, termasuk pembuatan *dashboard* dan laporan. Adapun fungsi dan kegunaan ketiga komponen tersebut dapat diilustrasikan seperti pada Gambar 3.4. Selain itu, Splunk menawarkan berbagai *add-on* dan aplikasi untuk memperluas fungsinya. Salah satu *add-on* yang populer adalah Splunk *Machine Learning Toolkit*, yang menyediakan fitur untuk menjalankan analisis dan model *machine learning* pada data yang dikumpulkan [3].



Gambar 3.5. Halaman Utama Splunk

Gambar 3.5 diatas menunjukkan tampilan halaman utama Splunk, memberikan gambaran umum tentang antarmuka pengguna dan opsi navigasi yang tersedia. Antarmuka atau GUI Splunk secara *default* dapat diakses melalui IP dan port bawaan yakni 8000. Dari halaman utama ini, pengguna dapat mengakses berbagai fitur Splunk, seperti pencarian data, pembuatan dashboard, dan pelaporan. Sedangkan gambar 3.6 merupakan gambar yang menunjukkan fitur ”Search and Reporting” dalam Splunk. Bagian ini adalah tempat di mana pengguna dapat melakukan analisis data menggunakan Splunk *Search Processing Language* (SPL). SPL adalah bahasa yang digunakan untuk mengatur dan memanipulasi data dalam Splunk. Bahasa ini mencakup berbagai perintah pencarian serta fungsinya, argumen, dan klausa. Perintah pencarian dalam SPL menentukan tindakan yang dilakukan Splunk terhadap data yang diambil dari indeks. Misalnya, perintah pencarian dapat digunakan untuk memfilter informasi yang tidak diinginkan, mengekstraksi lebih banyak informasi, mengevaluasi *field* baru, menghitung statistik, mengatur ulang hasil, atau membuat grafik.

Query SPL juga memiliki fungsi dan argumen terkait yang memungkinkan pengguna untuk memperinci tindakan yang dilakukan pada hasil pencarian. Pengguna dapat menggunakan fungsi untuk memformat data dalam grafik, menentukan jenis statistik yang akan dihitung, dan menetapkan *field* mana yang perlu dievaluasi. Beberapa perintah juga memiliki klausa yang dapat digunakan untuk mengelompokkan hasil pencarian. Hal ini memungkinkan pengguna untuk mengelompokkan hasil berdasarkan *field* tertentu, yang berguna saat membuat laporan atau grafik yang tersegmentasi.

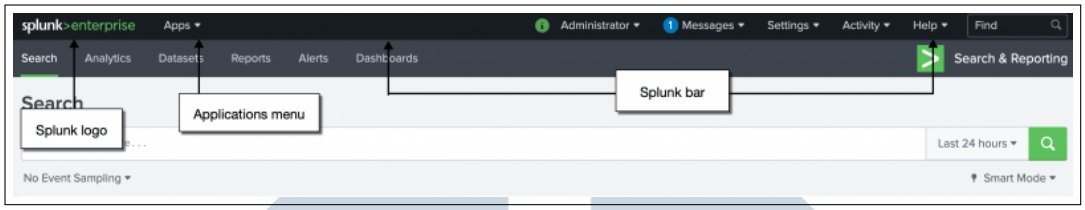


Gambar 3.6. Menu *Search* dan *Reporting* Splunk

Terdapat beberapa fitur kunci pada Splunk yang mendukung kebutuhan pengguna dalam menganalisis dan visualisasi data selain menu *Search and Reporting*, antara lain:

A.1 Splunk Bar

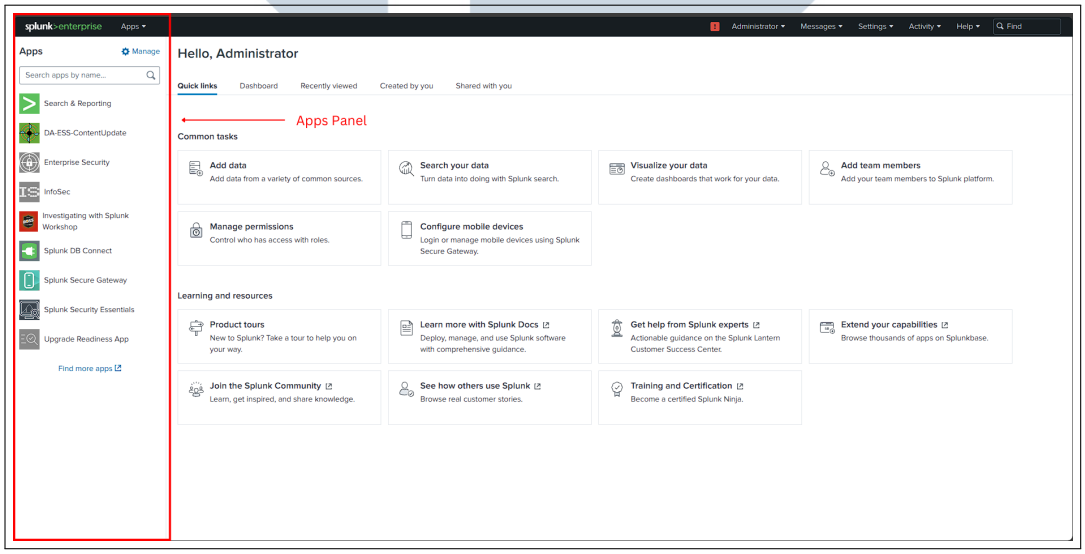
Splunk *Bar* merupakan bagian yang muncul pada setiap halaman dalam Splunk. Fungsinya adalah untuk beralih antara aplikasi (*apps*), mengkonfigurasi implementasi Splunk pada pengaturan, melihat pesan-pesan tingkat sistem, dan memantau kemajuan pekerjaan pencarian *(search jobs*). Dengan Splunk *Bar*, pengguna dapat dengan cepat mengakses berbagai fitur dan fungsi Splunk tanpa harus memerlukan navigasi yang rumit. Ini memberikan pengalaman pengguna yang terpusat dan efisien dalam menjalankan tugas-tugas yang berbeda di dalam platform Splunk.



Gambar 3.7. Splunk Bar

A.2 *Apps*

Fitur *Apps* pada Splunk memungkinkan pengguna untuk mengakses dan menginstal aplikasi tambahan yang menyediakan fungsionalitas tambahan dan integrasi dengan sistem dan sumber data lainnya. *Apps* ini dapat berupa aplikasi bawaan Splunk atau aplikasi yang dikembangkan oleh pihak ketiga. Pengguna dapat menemukan dan menginstal *apps/add-on* yang sesuai dengan kebutuhan analisis dan pemantauan, memperluas kemampuan Splunk sesuai dengan lingkungan dan kebutuhan spesifik pengguna.

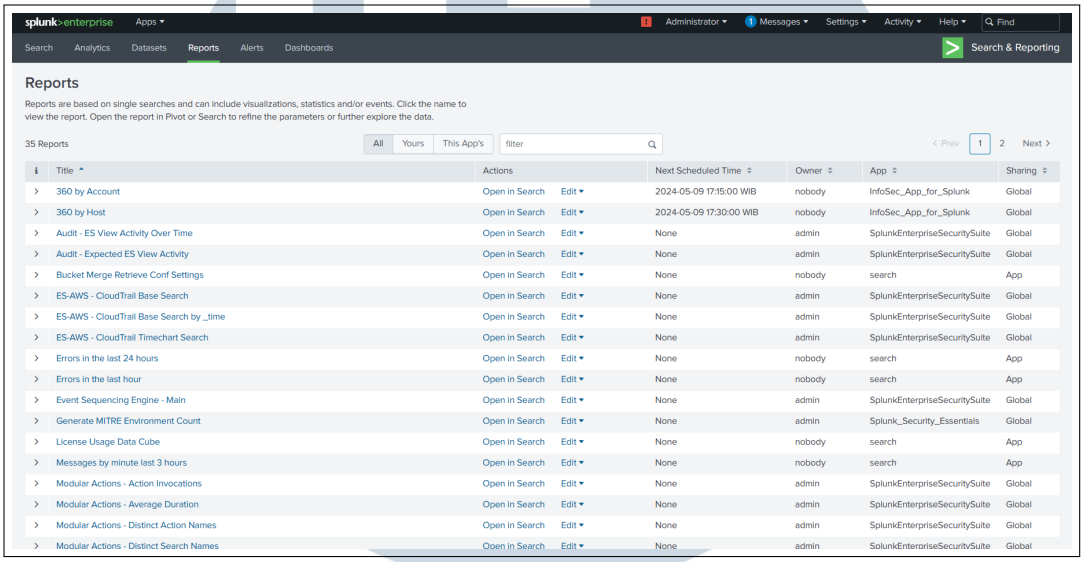


Gambar 3.8. *App Panel* Splunk

A.3 *Report*

Fitur *Report* memungkinkan pengguna untuk membuat laporan berdasarkan hasil pencarian data. Laporan ini dapat mencakup berbagai metrik dan dimensi yang relevan sesuai dengan kebutuhan analisis. Pengguna dapat menyesuaikan format dan tampilan laporan sesuai preferensi, termasuk grafik, tabel, atau format lainnya. Selain itu, report memungkinkan pengguna untuk menyimpan hasil pencarian

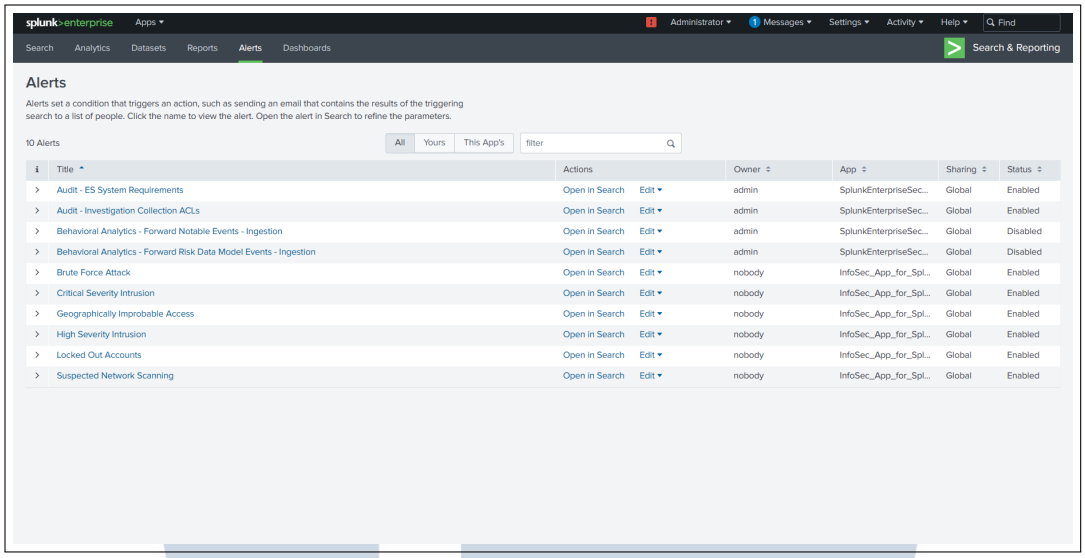
(*search*) dari *query* SPL yang telah dibuat. Dengan menyimpan hasil pencarian tersebut dalam bentuk laporan, pengguna dapat dengan mudah mengakses dan menganalisis data tanpa perlu melakukan *query* ulang. Hal ini memungkinkan pengguna untuk membuat *snapshot* dari data tertentu pada waktu tertentu, serta mempermudah dalam membagikan informasi atau hasil analisis kepada orang lain.



Gambar 3.9. Halaman Splunk *Reports*

A.4 *Alert*

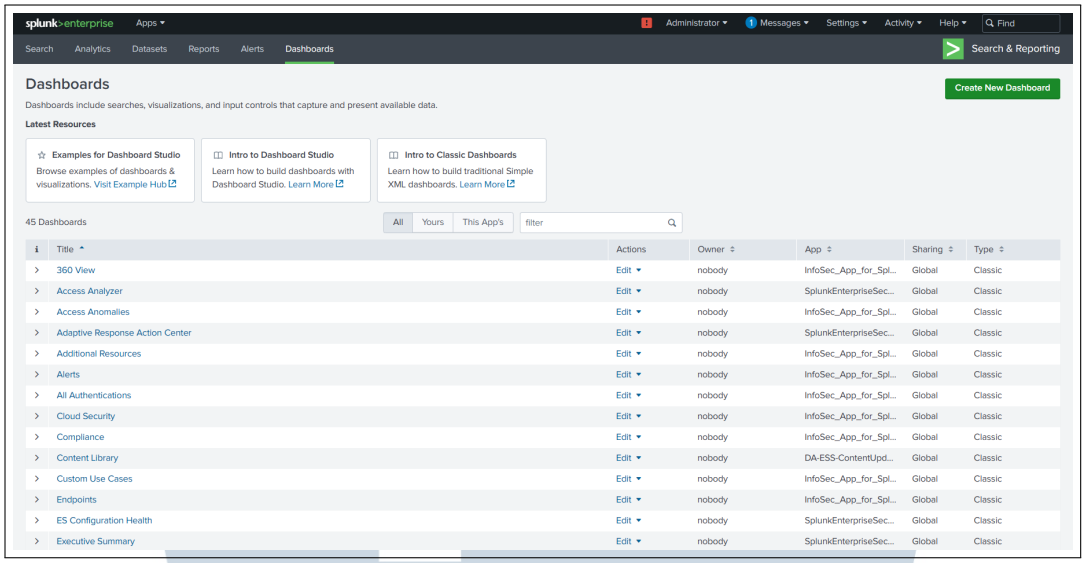
Alert memungkinkan pengguna untuk mengatur pemberitahuan atau notifikasi otomatis berdasarkan kondisi atau pola tertentu dalam data. Ketika kondisi yang ditentukan terpenuhi, Splunk akan secara otomatis mengirimkan pemberitahuan kepada pengguna, memungkinkan mereka untuk segera merespons perubahan atau insiden yang mungkin terjadi dalam lingkungan mereka. Ini membantu dalam mendeteksi dan menanggapi perubahan atau kejadian penting secara *real-time*, memastikan ketersediaan dan keamanan sistem.



Gambar 3.10. Halaman Splunk Alert

A.5 Dashboards

Dashboards merupakan halaman yang mengumpulkan semua *dashboard* yang telah dibuat oleh pengunna. *Dashboard* berisikan tampilan visual yang menyajikan informasi dan metrik penting dari data secara terkompilasi dalam satu layar. Suatu *dashboard* data berupa kumpulan dari beberapa laporan atau visualisasi data yang disusun dalam tata letak yang terstruktur. Pengguna dapat membuat dan menyesuaikan *dashboard* sesuai dengan kebutuhan, memilih metrik dan visualisasi yang paling relevan untuk dipantau secara langsung. *Dashboard* menyediakan gambaran holistik tentang kinerja sistem, tren, dan kejadian penting lainnya, memungkinkan pengguna untuk dengan cepat memahami situasi dan membuat keputusan berdasarkan data *real-time*. Dengan menggunakan *dashboard*, pengguna dapat memahami informasi secara visual dan langsung, memudahkan dalam pengambilan keputusan yang berbasis data.



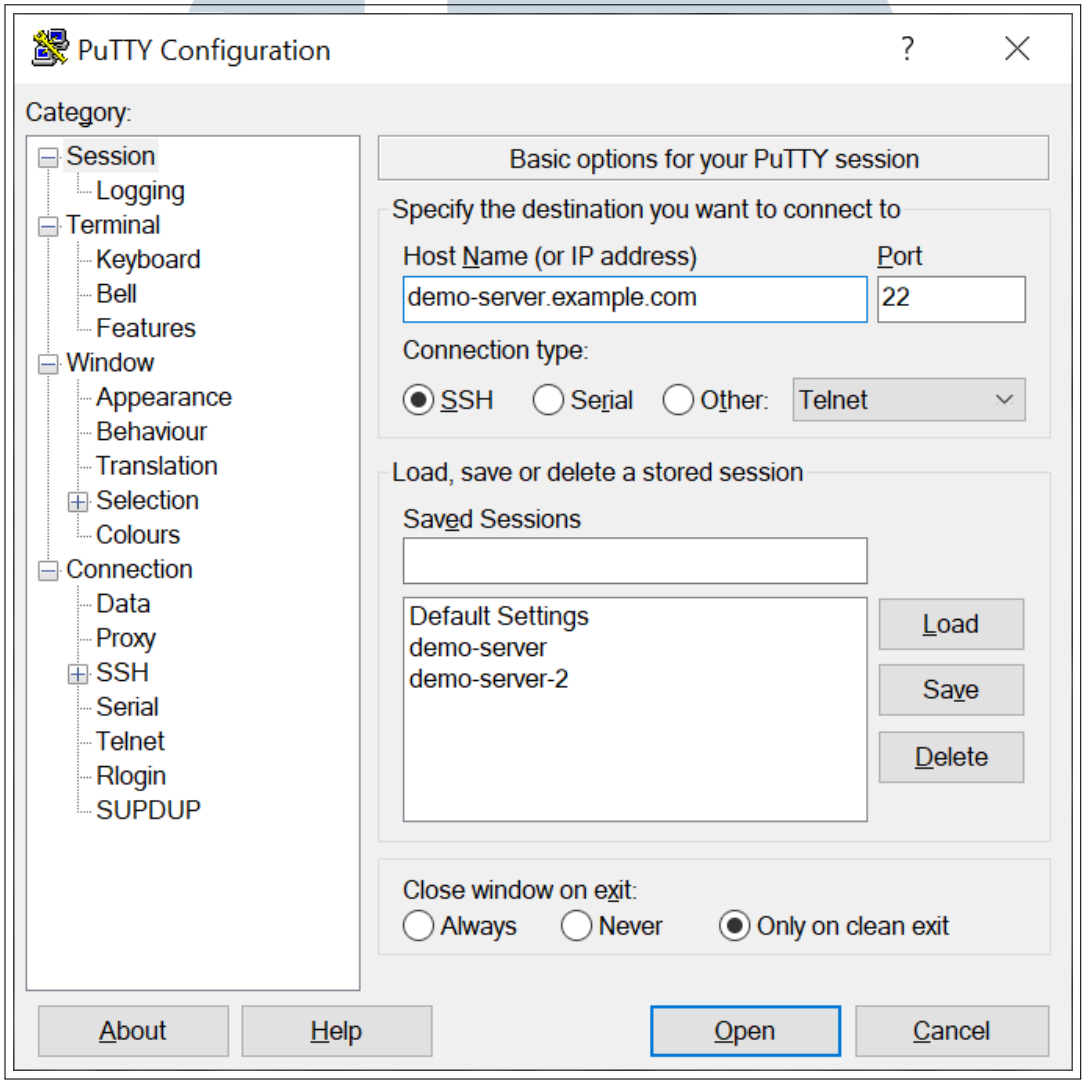
Gambar 3.11. Halaman Splunk *Dashboards*

B. PuTTY

PuTTY merupakan aplikasi *terminal* dan klien SSH (Secure Shell) yang digunakan untuk mengakses sistem komputer secara jarak jauh [5]. Aplikasi ini sangat berguna bagi teknisi dan administrator sistem yang perlu terhubung dengan *server* berbasis Unix atau Linux. Dengan PuTTY, pengguna dapat melakukan koneksi aman ke *server* melalui protokol SSH, memungkinkan mereka untuk menjalankan perintah, mengelola *file*, dan melakukan tugas-tugas administratif lainnya. PuTTY juga mendukung berbagai protokol lain, seperti Telnet dan rlogin, sehingga pengguna memiliki fleksibilitas dalam mengakses berbagai jenis sistem. Penggunaan PuTTY sangat krusial karena TC perlu mengakses SSH untuk dilakukannya konfigurasi dan pemeliharaan di *server*. SSH memungkinkan koneksi yang aman dan terenkripsi, sehingga TC dapat bekerja dengan sistem tanpa risiko keamanan. Dengan akses SSH, TC dapat melakukan tugas-tugas seperti instalasi perangkat lunak, konfigurasi, dan pemecahan masalah. Ini memungkinkan mereka untuk bekerja dengan efisien dan responsif, tanpa harus berada di tempat yang sama dengan *server*.

Pada Gambar 3.12 di bawah merupakan contoh tampilan jendela *pop-up* dari *software* PuTTY, yang merupakan aplikasi untuk mengakses sistem melalui protokol Secure Shell (SSH). Jendela *pop-up* ini adalah tempat di mana pengguna dapat mengonfigurasi koneksi dengan memasukkan alamat IP dari *server* yang ingin diakses. Untuk masuk ke *server*, pengguna perlu menyediakan informasi

autentikasi, yaitu alamat IP, *username*, dan *password*. Jendela konfigurasi ini juga memiliki opsi untuk mengatur parameter koneksi tambahan, seperti jenis enkripsi, port yang digunakan (biasanya port 22 untuk SSH), dan pengaturan lainnya yang terkait dengan keamanan dan performa koneksi. *Pop-up* ini adalah langkah awal yang diperlukan sebelum pengguna dapat terhubung ke *server* dan mulai bekerja dengan sistem yang ingin diakses.

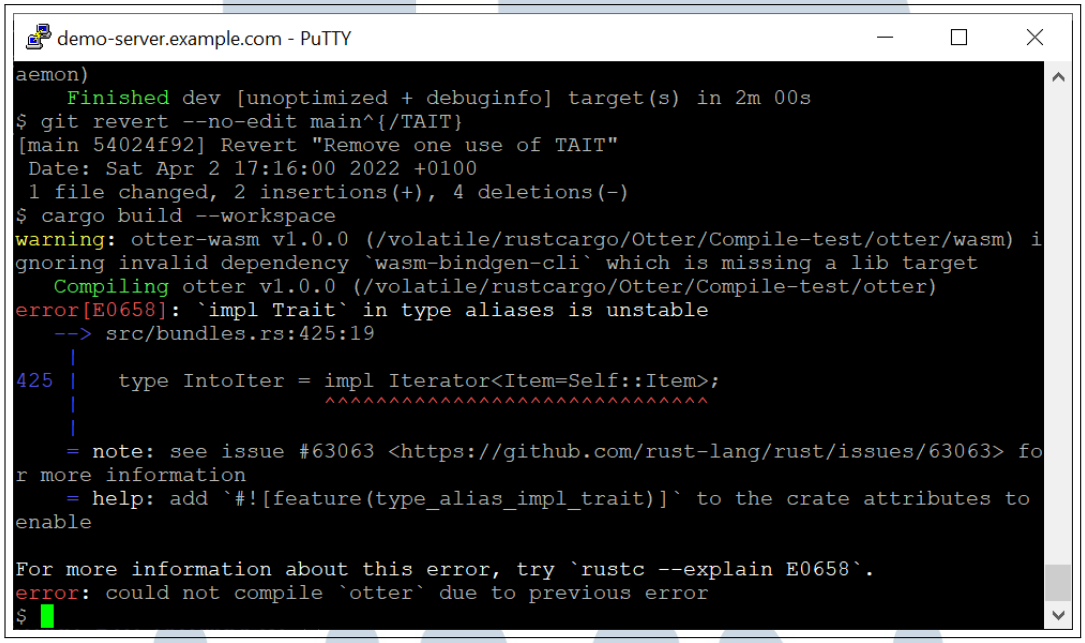


Gambar 3.12. Konfigurasi Koneksi di PuTTY

Sumber: [6]

Seperti Gambar 3.13 di bawah menunjukkan contoh *terminal* PuTTY, yang muncul setelah pengguna berhasil masuk ke *server* dengan menggunakan *credentials* yang tepat. *Terminal* ini adalah antarmuka berbasis teks yang memungkinkan pengguna untuk berinteraksi langsung dengan sistem operasi pada

server. Di dalam *terminal*, pengguna dapat menjalankan berbagai perintah, seperti menavigasi *directory*, mengedit *file*, menjalankan program, dan melakukan tugas-tugas administratif. *Terminal* PuTTY memberikan akses yang fleksibel kepada pengguna untuk mengelola *server* dari jarak jauh, dan menjadi alat yang sangat penting bagi TC yang bekerja dengan infrastruktur IT. Munculnya *terminal* ini menandakan bahwa koneksi SSH telah berhasil, dan pengguna sekarang dapat melakukan tugas-tugas mereka didalam lingkungan *server* yang diakses.

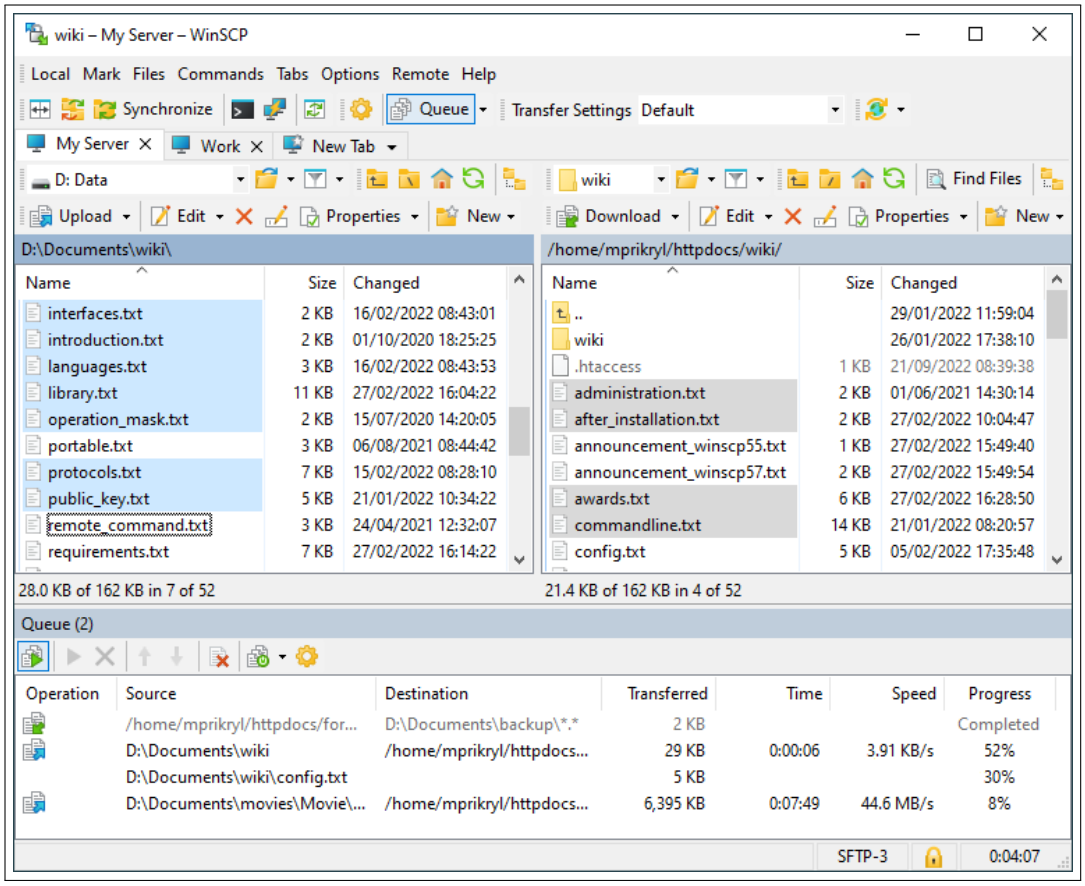


Gambar 3.13. PuTTY Terminal Interface

Sumber: [6]

C. WinSCP

WinSCP adalah perangkat lunak yang digunakan untuk mentransfer *file* antara sistem Windows dan *server* Linux [7]. Alat ini memungkinkan pengguna untuk memindahkan *file* dengan mudah dan aman melalui protokol SSH, SFTP, atau SCP. WinSCP sangat berguna bagi teknisi yang perlu memindahkan *file* antara platform yang berbeda, misalnya dari komputer Windows ke *server* Linux. Antarmuka pengguna WinSCP mirip dengan Windows Explorer, membuatnya mudah digunakan oleh mereka yang terbiasa dengan sistem operasi Windows. Dengan WinSCP, pengguna dapat melakukan operasi *file* dasar seperti menyalin, memindahkan, dan menghapus *file* di *server* jarak jauh.



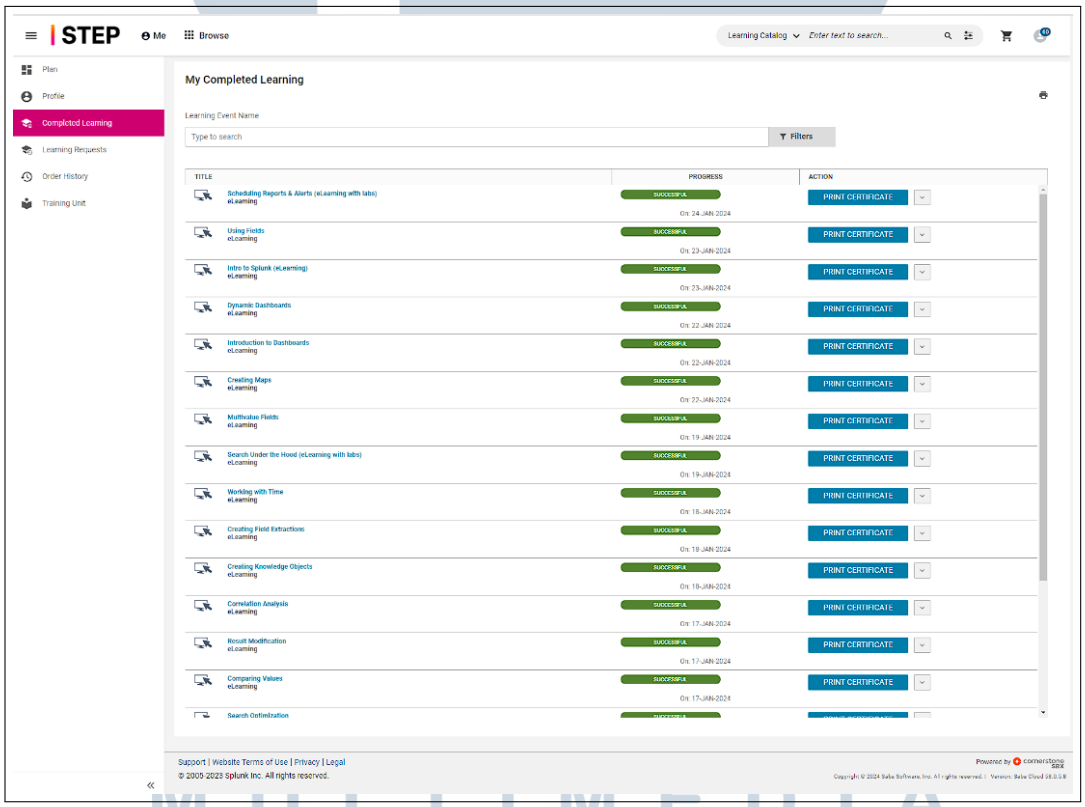
Gambar 3.14. *Interface* WinSCP

Sumber: [8]

Gambar 3.14 merupakan contoh antarmuka dari WinSCP, sebuah perangkat lunak yang dirancang untuk memindahkan *file* antara komputer lokal dan *server*. Antarmuka WinSCP biasanya terdiri dari dua kolom utama yakni kolom di sebelah kiri mewakili *directory* di komputer lokal, sedangkan kolom di sebelah kanan mewakili *directory* pada *server* atau sistem operasi yang dituju. Dengan desain ini, pengguna dapat dengan mudah menyeret dan melepaskan *file* antara dua kolom untuk memindahkan *file* dari komputer mereka ke *server*, atau sebaliknya. WinSCP mendukung beberapa protokol transfer *file*, seperti SSH dan FTP, yang membuat proses pemindahan *file* menjadi cepat dan aman. Alat ini sangat berguna bagi TC ketika ingin mengunggah skrip atau konfigurasi ke *server*, serta mengunduh data atau *file* untuk analisis atau cadangan. WinSCP memberikan kemudahan dan fleksibilitas dalam mengelola *file* dalam lingkungan IT yang kompleks.

3.3.2 Minggu 2 - 3: Mengerjakan Kursus *Official* dari Splunk

Sebagai bagian dari persiapan untuk magang di PT. GIT, peserta magang diwajibkan untuk mengikuti serangkaian kursus bersertifikat resmi dari *website* Splunk. Kursus berisi serangkaian video pembelajaran yang dapat diakses secara online, memungkinkan peserta magang untuk mempelajari materi kapan saja dan dari mana saja. Kursus tersebut hanya tersedia secara eksklusif bagi perusahaan yang telah menjalin kemitraan dengan Splunk, dan memberikan akses kepada peserta magang untuk mendapatkan pengetahuan yang mendalam tentang penggunaan dan konfigurasi Splunk. Untuk mencapai kompetensi yang diharapkan, peserta magang perlu menyelesaikan sekitar 16 kursus (seperti pada Gambar 3.15) yang mencakup berbagai aspek penting dalam mengoperasikan Splunk, dari tingkat fundamental hingga tingkat menengah dan mahir.

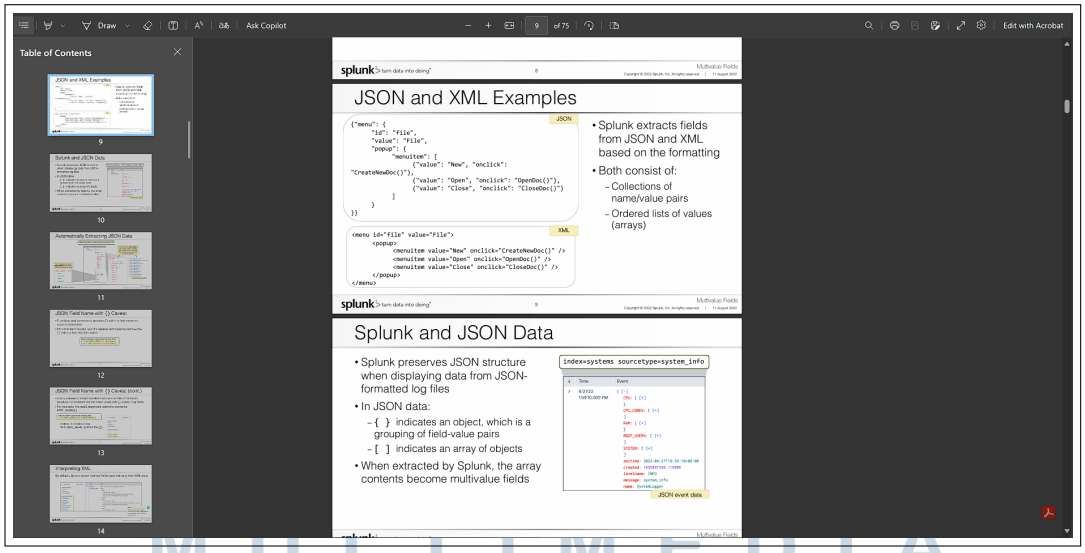


Gambar 3.15. Daftar Kursus yang Telah Selesai Dikerjakan

Kursus-kursus ini dirancang untuk memberikan pemahaman komprehensif mengenai fitur-fitur utama Splunk dan bagaimana menggunakannya secara efektif dalam konteks bisnis. Materi yang dipelajari meliputi konsep dasar tentang ingest data ke Splunk, penggunaan *Splunk Processing Language* (SPL), pembuatan

dashboard untuk *monitoring*, hingga konfigurasi fungsi-fungsi lanjutan dalam Splunk. Kursus-kursus ini disusun sedemikian rupa sehingga peserta magang dapat mengikuti *path* pembelajaran yang sistematis, dengan peningkatan tingkat kesulitan secara bertahap.

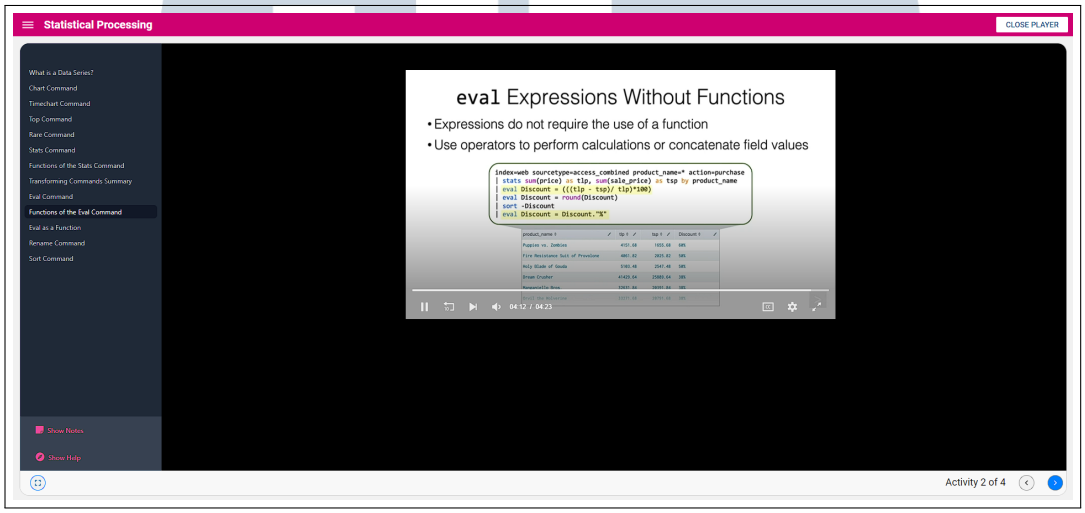
Splunk memberikan *training* dalam tiga bentuk utama yakni modul dalam format *slide* materi, video pembelajaran, dan laboratorium praktis (lab). Seperti terlihat pada Gambar 3.16, materi pembelajaran telah disusun menjadi *slide* presentasi, yang dijelaskan dalam video pembelajaran yang menyertainya. Video ini memudahkan peserta magang untuk memahami konsep secara visual dan mendengarkan penjelasan detail. Jika merujuk pada Gambar 3.17, video pembelajaran juga menjelaskan modul secara lebih rinci secara materi dipandu oleh tim Splunk yang berpengalaman. Selain itu, kursus ini tidak hanya memberikan teori, tetapi juga menawarkan kesempatan bagi peserta magang untuk mengaplikasikan pengetahuan dalam tugas-tugas praktis. Latihan-latihan dalam bentuk lab seperti pada Gambar 3.18 memungkinkan peserta magang untuk menerapkan keterampilan yang telah dipelajari secara langsung. Kursus ini sangat membantu peserta magang dalam mengembangkan pemahaman praktis tentang cara mengoperasionalkan Splunk dalam lingkungan kerja yang sesungguhnya.



Gambar 3.16. *Preview* Modul Pembelajaran

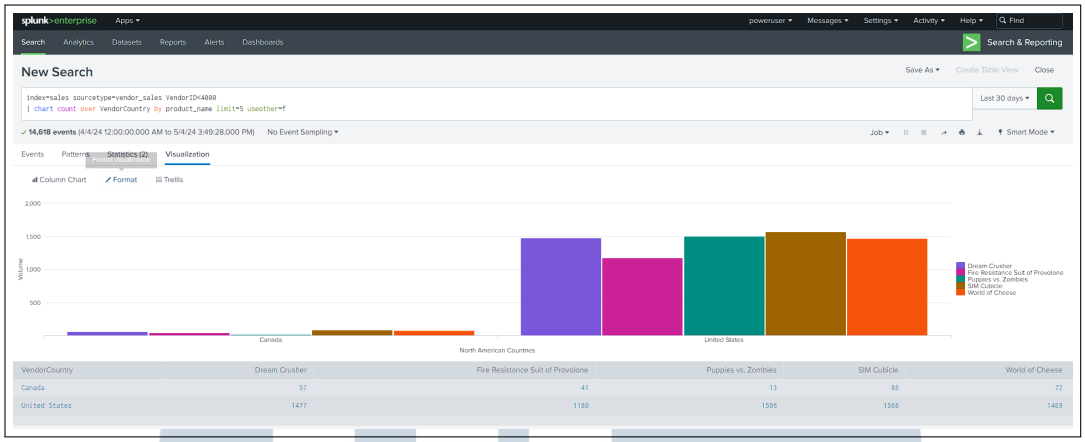
Gambar 3.16 adalah *preview* dari modul pembelajaran yang mencakup materi tentang *multivalue fields* dalam Splunk. *Multivalue fields* adalah jenis *fields* yang dapat menyimpan lebih dari satu nilai dalam satu kolom data. Modul ini memberikan pemahaman mendasar tentang konsep *multivalue fields* dan

menjelaskan bagaimana Splunk dapat mengidentifikasi dan mengekstraksi data dalam berbagai format, termasuk XML dan JSON. Ketika Splunk mengekstraksi data dari format ini, konten yang berbentuk *array* akan diubah menjadi *multivalue fields*, memungkinkan pengguna untuk menganalisis data tersebut secara lebih detail dan fleksibel. Penjelasan ini penting bagi pengguna Splunk Splunk yang berurusan dengan data kompleks, di mana satu *field* dapat berisi beberapa nilai. Materi ini memberikan wawasan tentang bagaimana menangani dan memanipulasi data tersebut dalam lingkungan Splunk.



Gambar 3.17. *Preview* Video Kursus Pembelajaran Online Splunk

Seperti yang ditunjukan pada Gambar 3.17 diatas yang merupakan *preview* video pembelajaran dari Splunk, video tersebut membahas salah satu *command search* pada Splunk yakni *Eval*. *Eval* adalah salah satu perintah yang paling umum digunakan dalam Splunk, dengan fungsi utama untuk menghitung ekspresi dan menyimpan hasilnya dalam *field* baru atau menggantikan nilai dari *field* yang sudah ada. Video pembelajaran ini menjelaskan berbagai cara *Eval* dapat digunakan, mulai dari operasi matematika sederhana hingga manipulasi teks yang kompleks. Dengan memahami *Eval*, pengguna Splunk dapat melakukan analisis data yang lebih kompleks dan canggih. Penjelasan dalam video ini dilengkapi dengan contoh praktis, memberikan ilustrasi yang jelas tentang cara *Eval* bekerja dalam skenario nyata. Hal ini membantu peserta magang mengembangkan keterampilan penting dalam melakukan analisis data dan memungkinkan untuk mengeksplorasi berbagai fungsi *Eval* dalam tugas-tugas yang berhubungan dengan data.



Gambar 3.18. *Preview Hands-On* Langsung pada Splunk

Gambar 3.18 diatas memberikan gambaran tentang pendekatan *hands-on* dalam kursus Splunk. Tidak hanya berfokus pada teori, kursus ini juga mendorong peserta untuk melakukan praktik lab sebagai bagian dari pembelajaran. Praktik ini memberikan kesempatan bagi peserta untuk menerapkan pengetahuan yang telah dipelajari melalui modul dan video pembelajaran ke dalam skenario praktis. Dengan pendekatan ini, peserta magang dapat menguji pemahaman mereka dan mendapatkan pengalaman langsung dalam mengoperasionalkan Splunk. Lab ini biasanya mencakup serangkaian tugas atau proyek yang dirancang untuk mensimulasikan situasi dunia nyata, sehingga peserta magang dapat mempraktikkan keterampilan mereka dan mengembangkan kepercayaan diri dalam menggunakan Splunk. *Hands-on* lab juga berfungsi sebagai sarana evaluasi, memungkinkan peserta magang untuk menerima umpan balik dan memperbaiki keterampilan mengoperasikan Splunk sebelum melanjutkan ke tugas yang lebih kompleks di tempat kerja atau di klien.

3.3.3 Minggu 4 - 6: Mempelajari *Security* dan *IT Architecture* bersama Splunk Expert

Sebagai bagian dari pelaksanan magang di GIT, para peserta magang memiliki kesempatan untuk belajar langsung dari seorang ahli Splunk yang berpengalaman, Bapak Munir. Perusahaan menyediakan fasilitas khusus untuk menyelenggarakan sesi pengajaran yang intensif dan interaktif bersama praktiksi Splunk langsung. Program pelatihan terdiri dari 12 sesi yang mencakup berbagai topik mulai dari konsep dasar hingga fitur lanjutan dalam keamanan informasi (*security*) dan arsitektur IT, seperti terlihat pada Gambar 3.19 yang

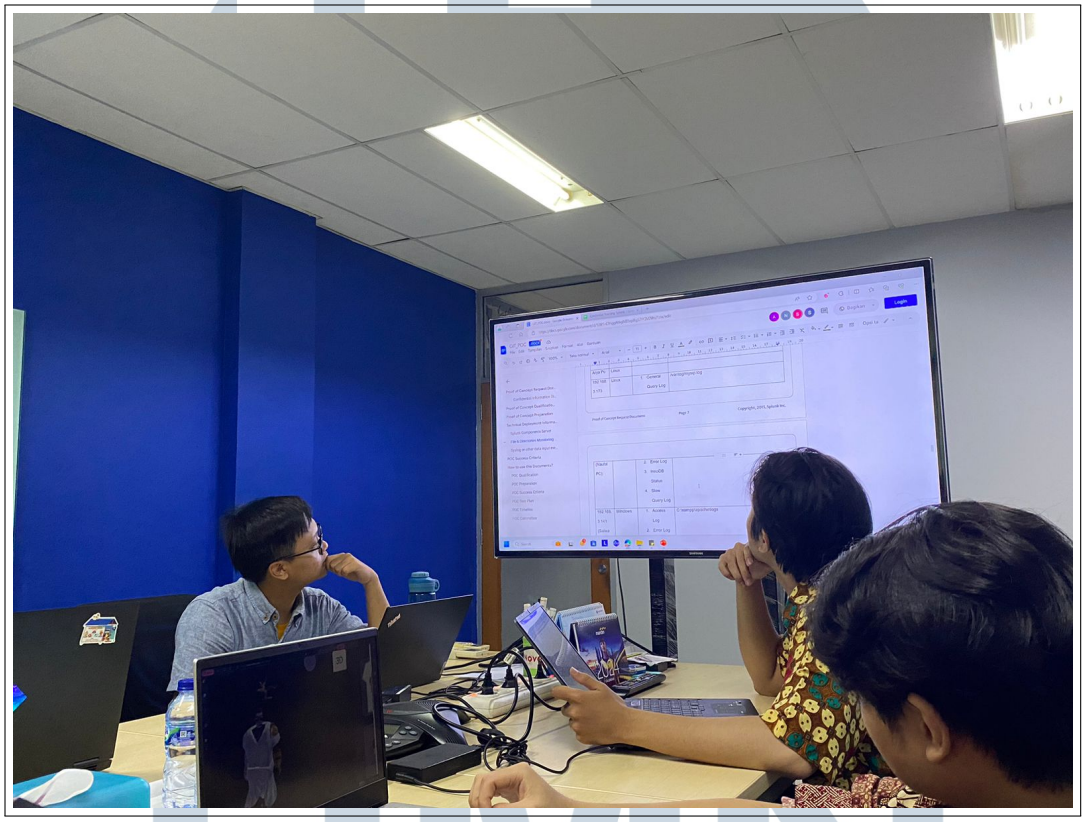
merupakan daftar materi per pertemuannya. Setiap sesi dirancang untuk memberikan pemahaman mendalam serta peluang diskusi tentang penggunaan Splunk dalam berbagai skenario keamanan. Sesi pertama memberikan *Overview* SIEM/SOC, membahas konsep *Security Information and Event Management* (SIEM) dan *Security Operations Center* (SOC). Pada sesi ini, peserta magang dikenalkan dengan prinsip kerja infrastruktur IT dalam sebuah perusahaan dan peran Splunk dalam memantau serta menganalisis aspek keamanan. Sesi ini memberikan gambaran umum mengenai cara kerja SIEM/SOC dalam mendeteksi dan menanggapi ancaman keamanan.

Pertemuan Ke	Materi Training
1	*Overview SIEM/SOC*
2	*Splunk Security Essential*
3	*Overview Splunk Enterprise Security*
4	*Asset and Identity*
5	*Correlation Search*
6	*Data Model*
7	*Common Information Model*
8	*Installation/Configuration Practice*
9	*Splunk Stream*
10	*Risk Base Alerting*
11	*Threat Intelligence*
12	*Use Case*

Gambar 3.19. Daftar Materi *Training* Pada Setiap Pertemuan

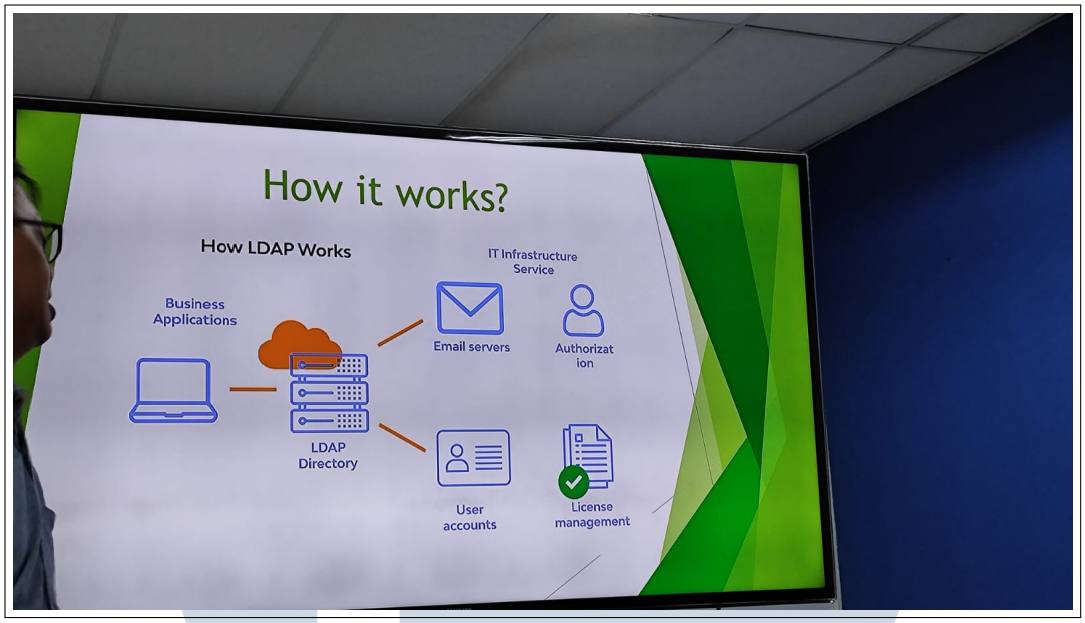
Sesi berikutnya, yang mencakup Splunk *Security Essential*, mengajarkan tentang komponen kunci dalam keamanan Splunk, termasuk Splunk *Enterprise Security platform* khusus untuk mendukung operasi keamanan perusahaan. Dalam sesi ini, dijelaskan bagaimana Splunk dapat digunakan untuk meningkatkan strategi keamanan perusahaan. Sesi-sesi lainnya mencakup topik-topik seperti *Asset* dan *Identity*, *Correlation Search*, *Data Model*, dan *Common Information Model* (CIM), yang menunjukkan cara Splunk dapat mendukung pengelolaan aset, identitas pengguna, serta pencarian korelasi untuk mendeteksi aktivitas yang mencurigakan. Ada juga sesi yang membahas instalasi dan konfigurasi Splunk serta fitur Splunk *Stream* untuk analisis jaringan. Sesi-sesi *Risk Based Alerting* dan *Threat Intelligence* mengajarkan teknik untuk mendeteksi dan menanggapi ancaman keamanan berdasarkan data yang dikumpulkan Splunk. Peserta magang

diajarkan cara Splunk dapat digunakan untuk memberikan peringatan berdasarkan tingkat risiko, serta bagaimana intelijen ancaman dapat membantu mencegah serangan yang lebih besar. Sesi terakhir, *Use Case*, memberikan contoh penerapan praktis dari konsep-konsep yang telah dipelajari, dengan berbagai skenario yang menunjukkan penggunaan Splunk dalam konteks dunia nyata.



Gambar 3.20. Situasi *Training* Saat Membahas PoC

Gambar 3.12 diatas menunjukkan situasi saat pelatihan sedang berlangsung. Dalam gambar ini, terlihat suasana kelas di mana peserta magang mengikuti pelatihan dengan serius. Bapak Munir, sebagai instruktur utama, memberikan penjelasan materi menggunakan layar proyektor untuk memperlihatkan proses pembuatan *Proof of Concept* (PoC). Pada saat itu, pelatihan sedang membahas cara membuat PoC, termasuk bagaimana menyelesaikan masalah klien dengan menggunakan Splunk, perhitungan komponen yang digunakan untuk menjalankan Splunk, hingga kriteria sukses untuk memenuhi kebutuhan klien.



Gambar 3.21. Situasi *Training* Saat Pembahasan *Asset* dan *Identity*

Selain itu, situasi lain yang digambarkan pada Gambar 3.13 diatas menunjukkan interaksi pembelajaran mengenai cara kerja *Lightweight Directory Access Protocol* (LDAP), yang merupakan salah satu alat untuk mengelola identitas dan autentikasi dalam sistem keamanan. Fasilitas pelatihan dilengkapi dengan peralatan yang diperlukan untuk mendukung proses belajar, termasuk ruang diskusi dengan akses internet yang memadai. Interaksi antara peserta magang dan instruktur terlihat dinamis, dengan banyak pertanyaan dan diskusi yang terjadi sepanjang sesi. Atmosfer dalam gambar ini menunjukkan suasana yang kondusif untuk belajar, menegaskan pentingnya pelatihan langsung dalam membangun keterampilan dan pemahaman tentang Splunk serta keamanan IT.

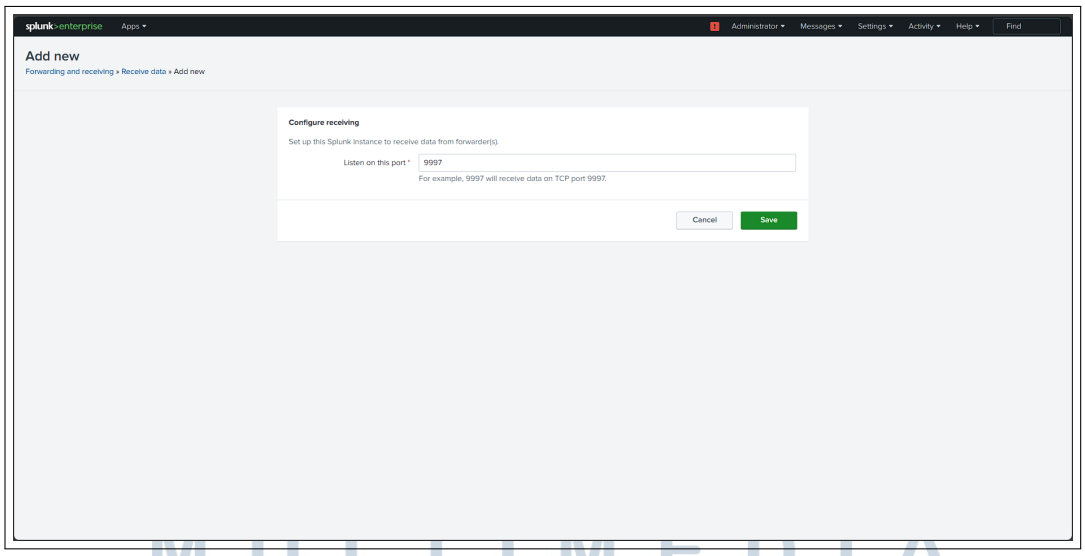
3.3.4 Minggu 6 - 8: Pelatihan Lanjutan oleh Splunk *Expert* Mengenai Splunk Core

Setelah memahami struktur keamanan (*security*) dan arsitektur IT dalam perusahaan, pelatihan lanjutan yang juga dibawakan oleh Bapak Munir adalah tentang Splunk Core. Pelatihan ini ditujukan untuk membahas aspek-aspek lebih lanjut dari Splunk, memastikan bahwa penggunaan platform ini sesuai dengan kebutuhan klien dan fokus pada area di mana perusahaan mungkin mengalami *pain point*. Pelatihan ini mencakup berbagai topik penting yang mendukung operasi Splunk secara optimal dalam skop perusahaan besar. Meteri dibagi menjadi enam pertemuan seperti terlihat pada Gambar 3.22.

Pertemuan Ke	Materi Training
1	*Ingest Data*
2	*Splunk Licensing*
3	*Clustering Architecture*
4	*Advanced SPL Query*
5	*Alerting*
6	*Data Retention*

Gambar 3.22. Daftar Materi Pertemuan Splunk Core

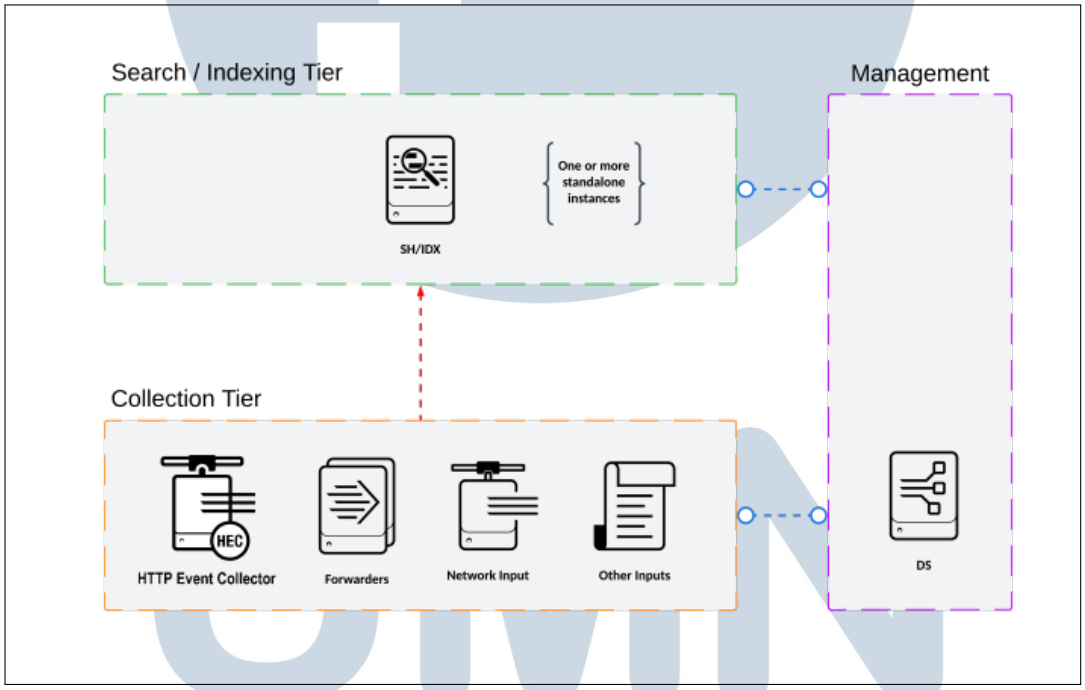
Topik pertama yang dibahas dalam pelatihan ini adalah bagaimana melakukan *forwarding data* dari alamat IP tertentu. Ini mencakup penggunaan *agent* dan *forwarder* pada setiap perangkat yang ingin diambil datanya. Dengan pendekatan ini, Splunk dapat mengumpulkan data dari berbagai sumber dalam infrastruktur klien, memastikan bahwa seluruh informasi yang relevan tersedia untuk analisis. Penerapan *agent* dan *forwarder* menjadi penting untuk memastikan konsistensi dan keandalan data yang diambil dari berbagai sistem dalam perusahaan. Umumnya Splunk akan menerima data melalui port 9997 yang dapat dibuka melalui pengaturan di GUI atau lewat terminal seperti pada Gambar 3.23.



Gambar 3.23. Mengonfigurasi Penerimaan Data dari *Forwarder* lewat GUI Splunk

Pelatihan juga mencakup penerapan arsitektur *clustering*, yang sangat relevan bagi klien dengan infrastruktur besar. Bapak Munir menunjukkan contoh-contoh arsitektur Splunk yang berbeda, membandingkan *single-site deployment* dengan *distributed clustered deployment*. Diskusi tentang arsitektur ini membantu

peserta magang memahami bagaimana memilih dan menerapkan struktur yang tepat sesuai dengan skala dan kebutuhan klien. Pada Gambar 3.24 dibawah menampilkan arsitektur Splunk yang cukup sederhana, cocok untuk perusahaan dengan infrastruktur yang relatif kecil atau tidak terlalu kompleks. Dalam arsitektur ini, seluruh komponen Splunk, termasuk *indexer* dan *search head*, berada dalam satu lokasi fisik atau site. Konfigurasi ini biasanya digunakan ketika volume data yang harus diolah tidak terlalu besar dan perangkat yang digunakan untuk *forward* data relatif sedikit. Dalam *Single Site Deployment*, pengelolaan data dan koordinasi antar-komponen lebih mudah karena semua sistem berada dalam satu tempat. Namun, arsitektur ini mungkin kurang cocok untuk perusahaan yang memiliki volume data yang besar atau yang memerlukan skalabilitas tinggi.

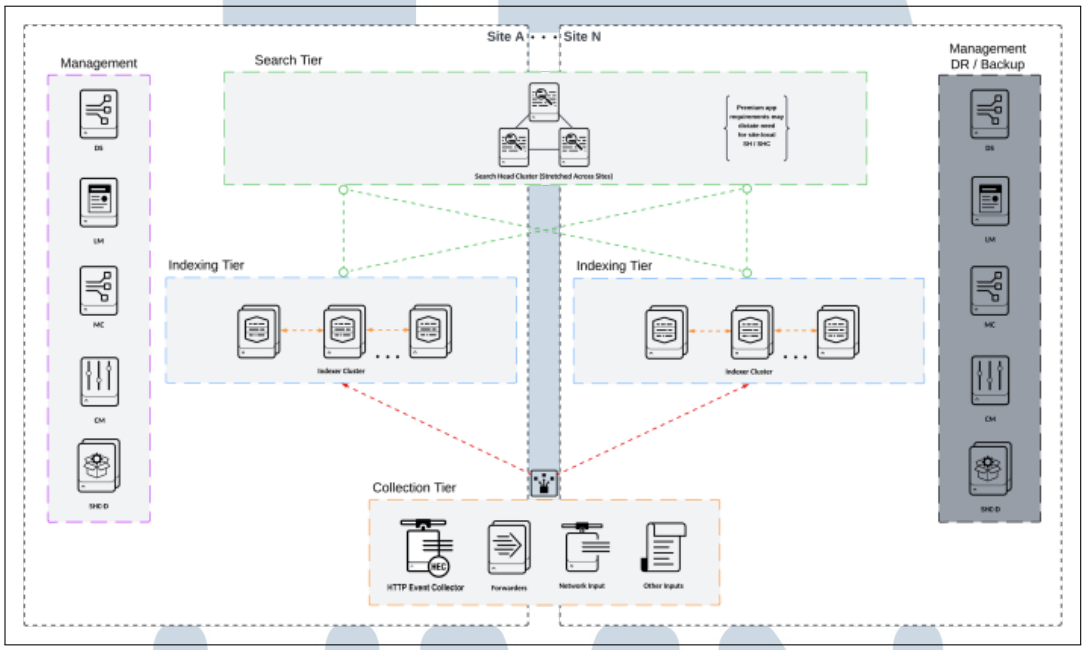


Gambar 3.24. Ilustrasi Arsitektur *Single-Site Deployment*

Sumber: [9]

Sedangkan seperti yang ditunjukan Gambar 3.25 menampilkan arsitektur yang lebih kompleks dan skalabel, dikenal sebagai Distributed Clustered Deployment with SHC (*Search Head Cluster*) *Multi-Site*. Arsitektur ini dirancang untuk perusahaan yang memiliki infrastruktur besar, dengan banyak perangkat yang mengirim data ke Splunk dan volume data yang sangat tinggi setiap harinya. Dalam arsitektur ini, komponen Splunk tersebar di berbagai lokasi atau *site*, memungkinkan distribusi beban kerja dan redundansi. *Search Head Cluster*

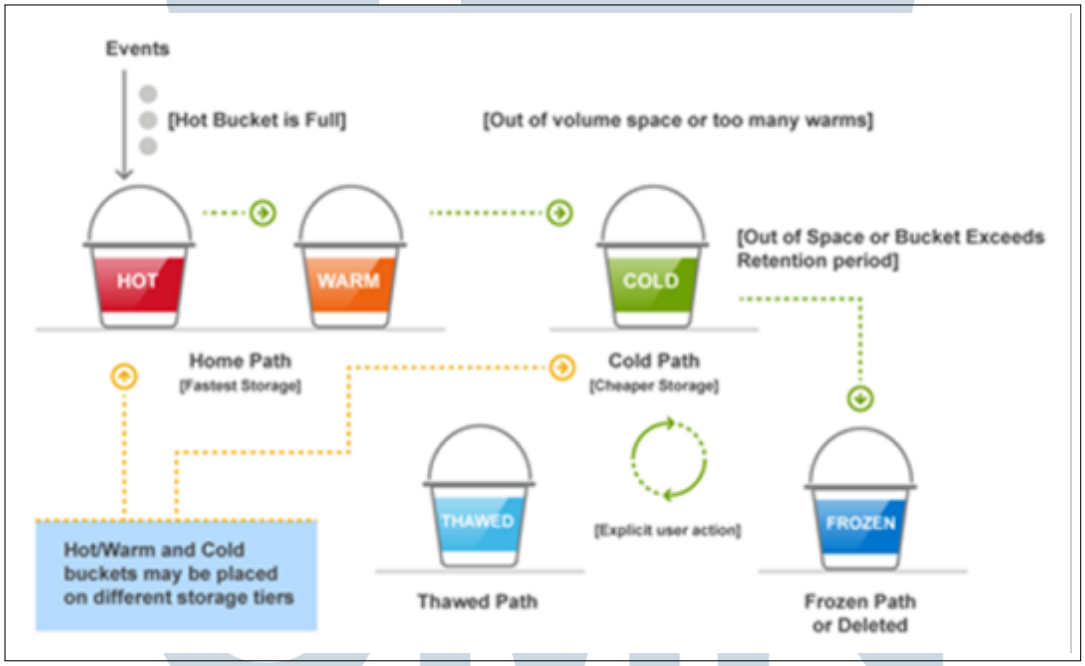
memungkinkan pencarian data secara lebih efisien dan memastikan ketersediaan layanan jika salah satu *site* mengalami gangguan. Arsitektur ini juga mendukung pengaturan *load balancing*, yang penting untuk perusahaan dengan lingkungan IT yang sangat kompleks. Dengan memahami berbagai jenis arsitektur, klien dan TC dapat memilih konfigurasi yang sesuai dengan kebutuhan operasional, memastikan Splunk dapat berfungsi secara optimal untuk mendukung operasional perusahaan dan pengambilan keputusan berbasis data.



Gambar 3.25. Ilustrasi Arsitektur *Distributed Clustered Deployment*
Sumber: [10]

Topik selanjutnya adalah mengenai *licensing* juga menjadi topik penting dalam pelatihan ini. Bapak Munir menjelaskan cara mengatur *license master* dalam Splunk, yang diperlukan untuk mengelola dan mengontrol penggunaan Splunk sesuai dengan perjanjian lisensi. Pemahaman tentang *licensing* ini membantu memastikan bahwa perusahaan memenuhi persyaratan legal dan tidak melanggar ketentuan penggunaan Splunk. Kemudian pelatihan juga mencakup penggunaan *Splunk Processing Language* (SPL) untuk menampilkan visualisasi, membuat dashboard, serta melakukan optimalisasi *query* agar tidak membebani *runtime*. Ini adalah keterampilan penting karena SPL digunakan untuk menganalisis dan memvisualisasikan data dalam Splunk. Selain itu, bagian ini mencakup teknik optimalisasi *query* untuk menjaga kinerja sistem dan menghindari penggunaan sumber daya yang berlebihan.

Selain itu, pelatihan juga mencakup *setting alerting* untuk memungkinkan Splunk memicu notifikasi ke pengguna melalui *email* atau aplikasi pesan seperti Telegram. Fitur ini penting untuk memberikan peringatan dini jika ada masalah dalam sistem, memungkinkan perusahaan merespons dengan cepat untuk mencegah kerusakan atau gangguan yang lebih besar. Terakhir, konfigurasi retensi data dibahas dalam pelatihan ini. Splunk memiliki konsep *hot*, *warm*, *cold*, *frozen*, dan *thawed bucket* untuk mengelola retensi data. Pelatihan ini memberikan panduan tentang cara mengatur retensi data agar tidak membebani server tempat Splunk diinstal, sekaligus memastikan bahwa data yang diperlukan tetap dapat diakses untuk analisis lebih lanjut. Adapun ilustrasi cara kerja *bucket* ini ditunjukan seperti pada Gambar 3.26.



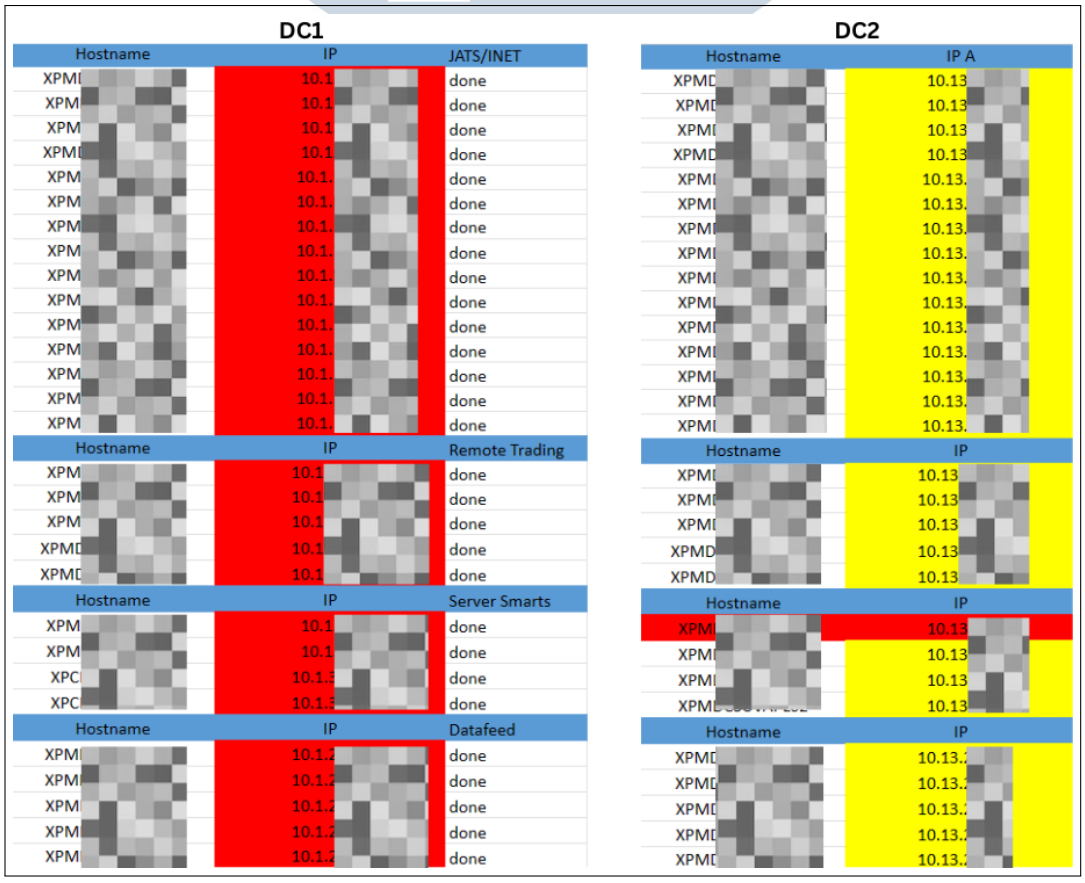
Gambar 3.26. Ilustrasi Splunk Buckets

Sumber: [11]

Melalui pelatihan yang komprehensif ini, peserta magang mendapatkan pemahaman yang lebih mendalam tentang Splunk Core dan bagaimana menerapkan *best practice* dalam lingkungan IT yang kompleks. Materi yang diajarkan oleh Bapak Munir memberikan dasar yang kuat untuk bekerja dengan Splunk dalam konteks operasional dan membantu memastikan bahwa solusi yang diterapkan sesuai dengan kebutuhan klien dan mendukung operasional perusahaan secara keseluruhan.

3.3.5 Minggu 8 - 10: Mempelajari dan Memahami Dokumen Proyek Klien

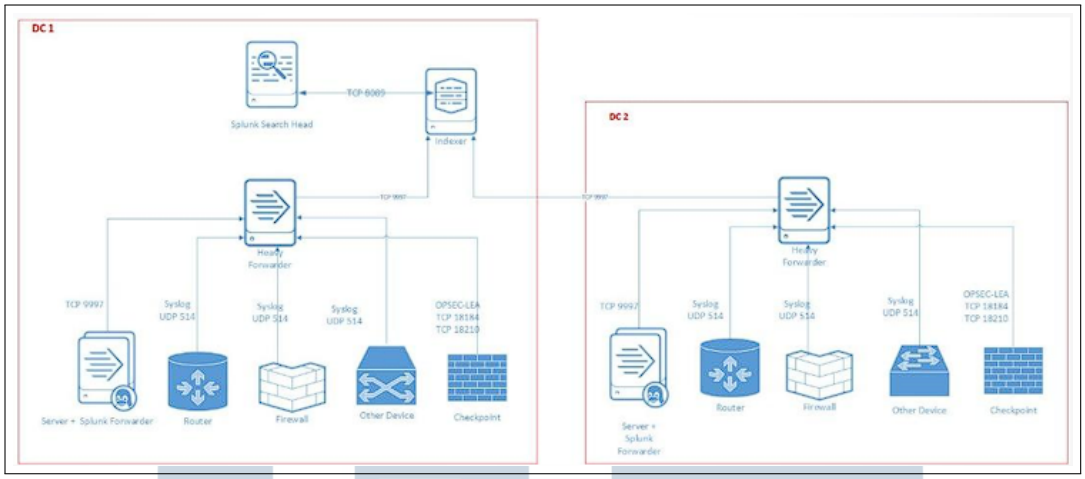
Dalam konteks implementasi Splunk, memahami arsitektur dan infrastruktur IT klien adalah langkah krusial sebelum memulai proses konfigurasi. Di proyek GIT untuk PT. Bursa Efek Indonesia (BEI), dokumen proyek memainkan peran penting dalam memberikan wawasan tentang sistem dan layanan yang ingin dimonitor oleh Splunk. Mempelajari dokumen ini membantu TC memahami struktur dan komponen yang terlibat, memastikan bahwa solusi Splunk yang diterapkan sesuai dengan kebutuhan klien. Arsitektur IT BEI melibatkan dua *data center* utama yang disebut DC1 dan DC2. Kedua *data center* ini merupakan lokasi penting di mana layanan klien berjalan dan di mana data penting dihasilkan. Setiap *data center* memiliki setidaknya 30 *hostname* dan 30 alamat IP yang digunakan untuk mendukung operasi berbagai layanan dan aplikasi seperti ditunjukan pada Gambar 3.27. Dengan adanya dua *data center* ini, BEI memastikan redundansi dan kelancaran operasional perdagangnnya, bahkan dalam situasi yang membutuhkan *failover* atau *load balancing*.



Gambar 3.27. Daftar *Server* pada DC 1 dan DC 2

Fokus utama *monitoring* Splunk di BEI adalah empat aplikasi kunci yang menjalankan layanan penting bagi klien. Aplikasi tersebut adalah JATS/INET, Remote Trading, Server Smarts, dan Datafeed. Keempat aplikasi ini memiliki peran unik dalam infrastruktur BEI, dengan JATS/INET yang berkaitan dengan sistem perdagangan, Remote Trading untuk akses jarak jauh, *Server* Smarts untuk pemantauan sistem, dan Datafeed untuk pengiriman data. Memahami bagaimana layanan ini beroperasi dalam *data center* adalah kunci untuk memastikan *monitoring* Splunk mencakup semua aspek yang relevan. Topologi arsitektur Splunk di BEI relatif sederhana tetapi efektif dan tetap mencukupi untuk kebutuhan klien. Splunk di BEI menggunakan satu *search head*, satu *indexer*, dan dua *forwarder* (satu untuk DC1 dan satu untuk DC2). *Forwarder* ini bertanggung jawab untuk mengirim data dari *data center* masing-masing ke *indexer*, yang kemudian mengelola data tersebut untuk ditampilkan oleh *search head*. Dengan konfigurasi ini, BEI dapat mengumpulkan dan menganalisis data dari berbagai sumber dengan efisien, sementara struktur yang sederhana membantu menjaga stabilitas dan kemudahan pengelolaan.

Gambar 3.28 di bawah menunjukkan topologi arsitektur Splunk di BEI, yang menggambarkan aliran data dari *forwarder* ke *indexer* dan akhirnya ke *search head*. Desain ini dipilih karena sesuai dengan kebutuhan klien dan volume data yang dihasilkan setiap harinya. BEI juga mempertimbangkan jumlah pengguna Splunk dan beban kerja pada *indexer* saat menentukan konfigurasi ini. Selain itu, perangkat-perangkat yang terhubung ke Splunk untuk *monitoring* meliputi *log server*, *router*, *firewall*, dan komponen jaringan lainnya. Komponen ini memberikan berbagai jenis data yang dapat diolah oleh Splunk untuk analisis dan *monitoring*. Memahami bagaimana data mengalir melalui sistem dan perangkat apa saja yang berperan adalah bagian penting dari proses implementasi Splunk.



Gambar 3.28. *Architecture* Splunk pada PT. Bursa Efek Indonesia

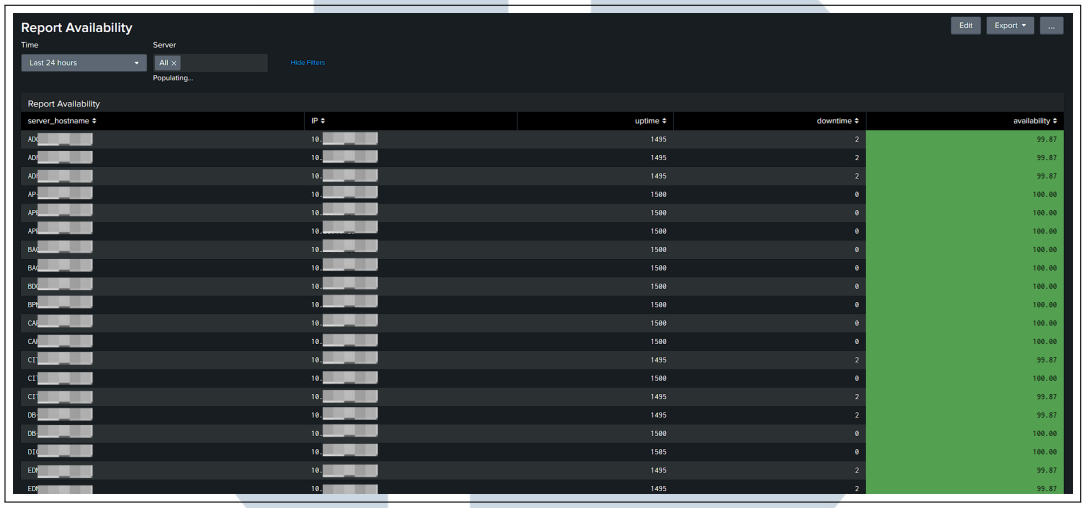
Dengan memahami dokumen proyek klien secara menyeluruh, TC dapat memastikan bahwa implementasi Splunk memenuhi kebutuhan BEI dan memberikan solusi yang sesuai dengan struktur IT yang ada. Analisis terhadap dokumen proyek juga membantu TC dalam mengantisipasi potensi tantangan dan merencanakan pendekatan yang tepat untuk implementasi dan pemantauan berkelanjutan.

3.3.6 Minggu 10 - 12: Pembuatan Visualisasi *Server and Network Device Availbility* untuk Klien

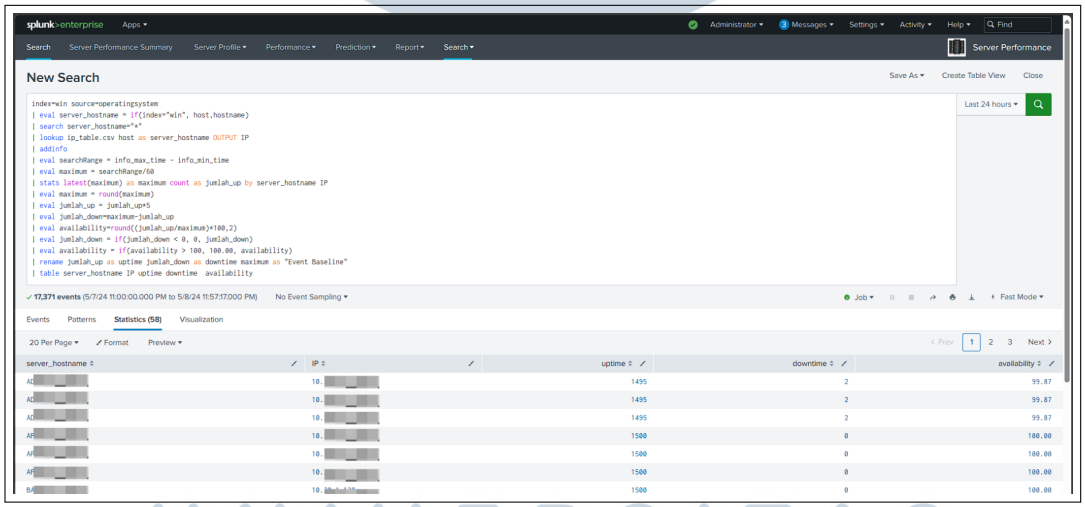
Salah satu tugas dalam program magang di GIT adalah membuat visualisasi sesuai dengan kebutuhan klien. Pada saat pelakasanan magang berlangsung, TC *Intern* diminta untuk memenuhi kebutuhan klien yang ingin memiliki visualisasi untuk memantau ketersediaan *server* dan perangkat jaringan. Visualisasi ini sangat penting karena memungkinkan klien untuk melihat *uptime* dan *downtime server*, serta *availability* perangkat jaringan, secara *real-time*. Berikut akan dibahas dua jenis visualisasi yang telah dibuat dari dari visualisasi *server performance* dan *network device availability*.

Gambar 3.29 di bawah menunjukkan visualisasi dalam bentuk tabel yang mengilustrasikan kinerja *server* klien. Tabel ini menyajikan informasi tentang *uptime* dan *downtime server*, memungkinkan klien untuk mengetahui seberapa sering server mengalami gangguan dalam periode waktu tertentu. Dengan informasi ini, klien dapat menilai ketersediaan *server* secara keseluruhan dan mengidentifikasi potensi masalah yang mungkin mempengaruhi operasi bisnis mereka. Data untuk visualisasi ini diambil menggunakan *Simple Network Management Protocol*

(SNMP), sebuah protokol yang umum digunakan untuk memonitor dan mengelola perangkat jaringan. Dengan SNMP, data tentang *uptime* dan *downtime* dapat dikumpulkan secara otomatis dan dianalisis untuk menghasilkan visualisasi yang informatif.



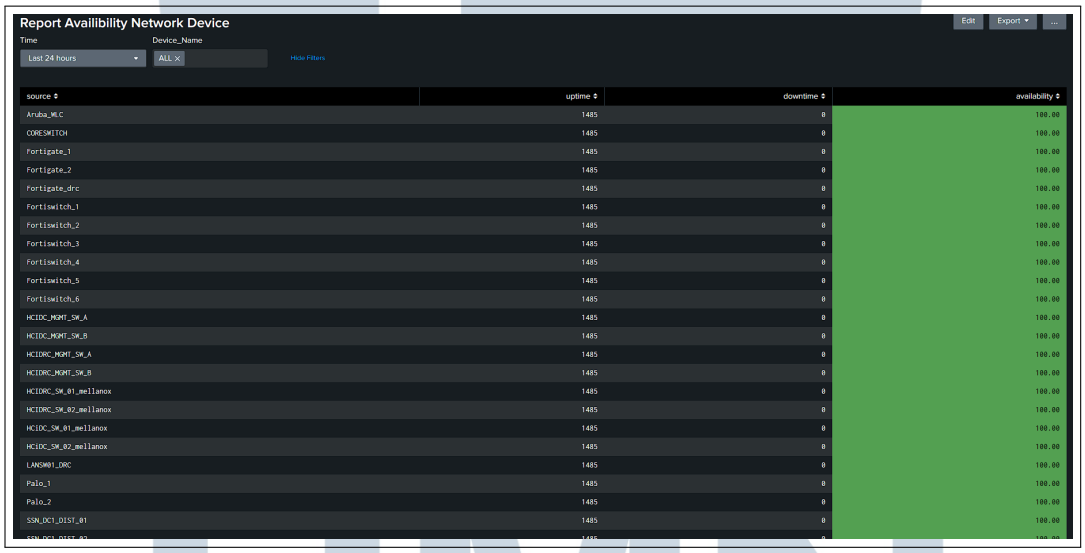
Gambar 3.29. Visualisasi *Server Performance*



Gambar 3.30. *Query* SPL untuk membuat Visualisasi *Server Performance*

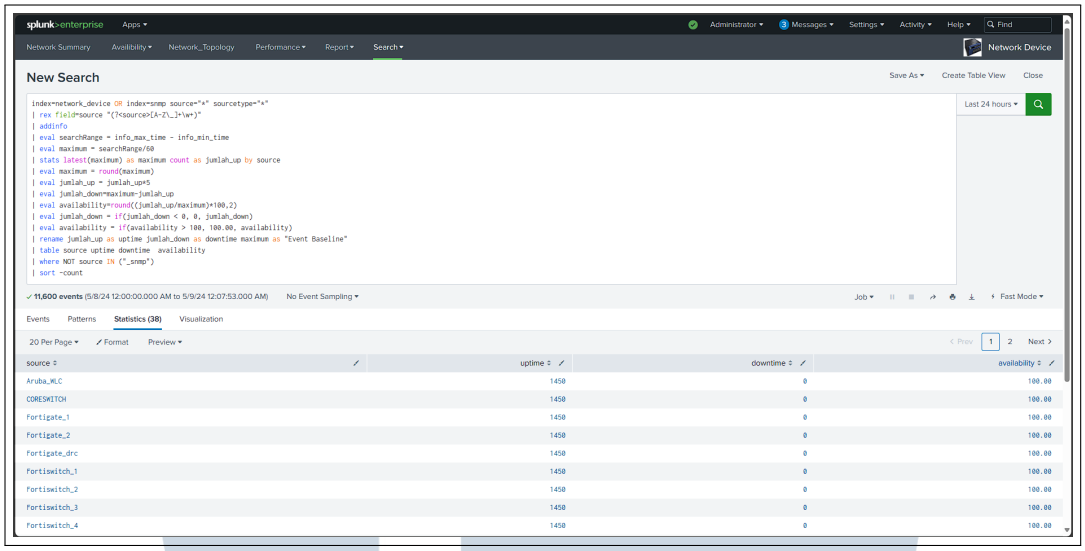
Seperti terlihat pada Gambar 3.30, data untuk visualisasi *server performance* dikumpulkan dari indeks Splunk yang terkait dengan sistem operasi Windows (index=win). Adapun *query* untuk membuat visualisasi ini dimulai dengan memilih data dari sumber yang relevan, yaitu 'operatingsystem'. Setelah itu, *field server hostname* dibuat menggunakan fungsi *eval*, yang menyimpan *hostname server* berdasarkan *field host*. Selanjutnya, data server yang relevan digabungkan dengan informasi IP menggunakan tabel lookup dari file 'ip_table.csv'. Informasi

tambahan ditambahkan dengan fungsi *addinfo*, dan rentang waktu pencarian dihitung untuk mendapatkan waktu maksimum dalam menit. Dari sini, *uptime* dihitung berdasarkan jumlah *event* dan dikalikan dengan lima untuk memperoleh jumlah menit *uptime*. *Downtime* diperoleh dengan menghitung selisih antara waktu maksimum dan *uptime*. Pada akhirnya, persentase *availability* ditentukan dengan membandingkan *uptime* dengan waktu maksimum. Setelah menghitung *uptime* dan *downtime*, hasil akhir disusun dalam bentuk tabel dengan field seperti server_hostname, IP, *uptime*, *downtime*, dan availability. Penyusunan ini memungkinkan klien untuk melihat dan memantau ketersediaan *server* dengan jelas.



Gambar 3.31. Visualisasi *Network Device Performance*

Visualisasi yang seperti ditunjukan pada 3.31 menampilkan ketersediaan perangkat jaringan yang digunakan oleh klien. Visualisasi ini dirancang untuk memberikan gambaran yang jelas tentang status operasional berbagai perangkat jaringan, seperti *router*, *switch*, dan *firewall*. Dengan melihat visualisasi ini, klien dapat dengan cepat mengetahui perangkat mana yang beroperasi dengan baik dan perangkat mana yang mungkin mengalami masalah. Sama seperti visualisasi *server performance*, data untuk visualisasi ini juga diambil melalui SNMP, memungkinkan pengambilan data secara *real-time* dan konsisten. Informasi ini sangat berharga bagi tim IT klien, karena memungkinkan mereka untuk segera menanggapi jika ada perangkat jaringan yang mengalami gangguan.



Gambar 3.32. *Query* SPL untuk membuat Visualisasi *Network Device Performance*

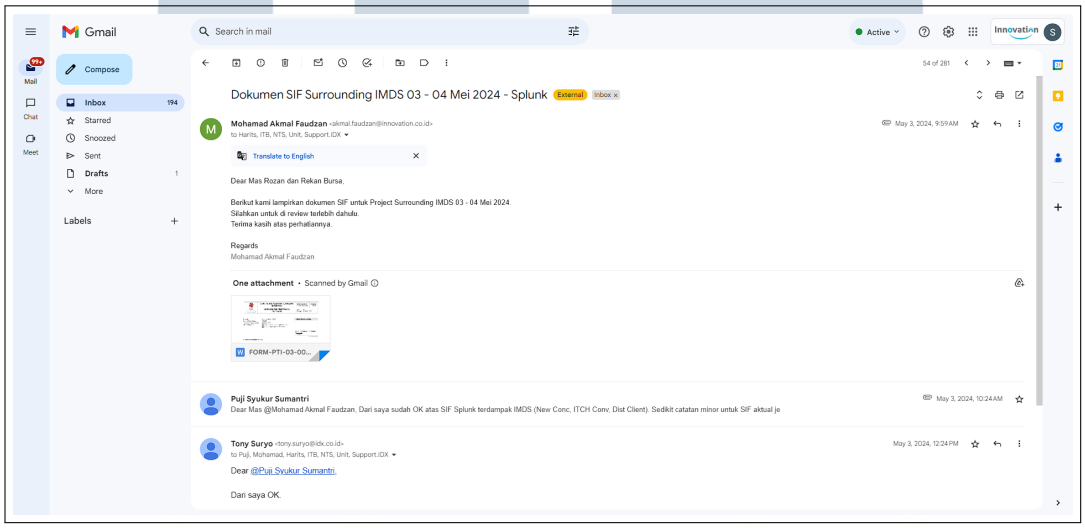
Terliahat pada Gambar 3.32, *query* dimulai dengan mengambil data dari indeks network_device dan snmp, lalu menggunakan *rex* untuk mengekstrak nama sumber dari *field source*. Seperti pada visualisasi sebelumnya, waktu pencarian dan waktu maksimum dihitung, lalu *uptime* diperoleh dari jumlah *event*. *Downtime* dihitung sebagai selisih antara waktu maksimum dan *uptime*. Query juga menggunakan fungsi *where* untuk mengecualikan sumber data yang tidak relevan. Hasil akhirnya disusun dalam bentuk tabel dengan kolom seperti *source*, *uptime*, *downtime*, dan *availability*. Penyusunan ini memberikan cara yang mudah dan intuitif bagi klien untuk memahami status perangkat jaringan yang dimiliki. Kemampuan untuk memantau dan menganalisis ketersediaan perangkat jaringan dan *server* ini membantu klien dalam mendeteksi masalah lebih awal dan memastikan kelancaran bagi operasi IT secara keseluruhan.

3.3.7 Minggu 12 - 15: Implementasi dan *Fallback* fitur *services* pada klien

Setelah mempelajari dan memahami dokumen proyek klien, selanjutnya TC diminta untuk melakukan implementasi konfigurasi secara *onsite*. Pada proyek ini, implementasi dilakukan di Gedung Cyber 1 pada hari Jumat dan Sabtu, untuk menghindari jam perdagangan dan meminimalisir risiko malfungsi di antara layanan yang dijalankan oleh BEI. Dalam proses implementasi ini, tim TC GIT harus bekerja secara hati-hati untuk memastikan bahwa perubahan konfigurasi tidak menyebabkan gangguan pada sistem yang sudah berjalan.

Implementasi dilakukan sesuai dengan dokumen SIF (Skenario

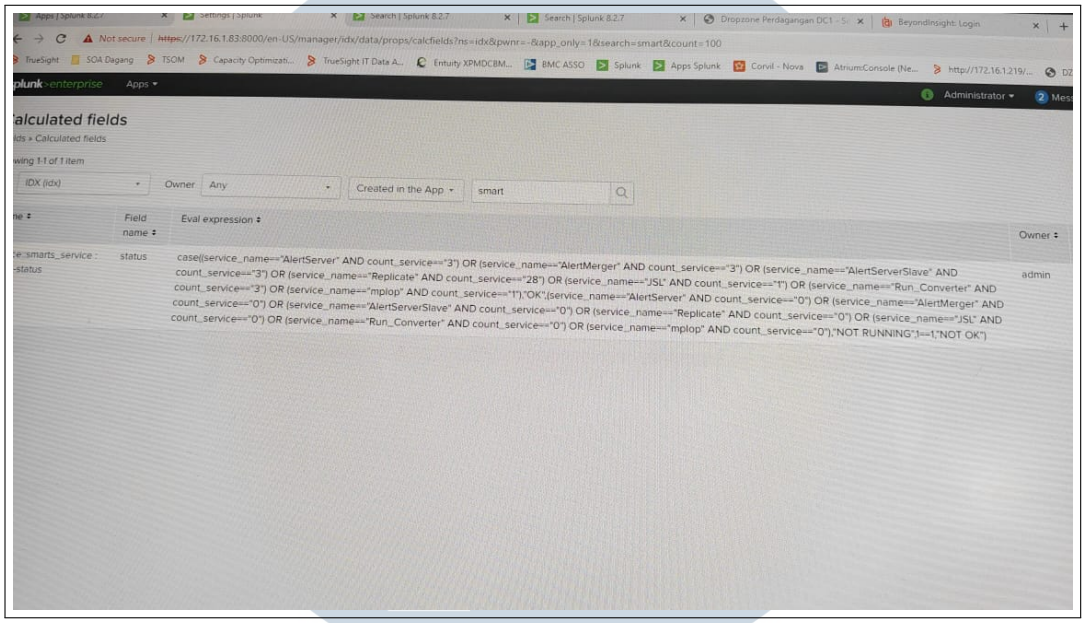
Implementasi dan Fallback) yang telah dibuat dan disetujui oleh klien sebelumnya. Dokumen SIF ini dikoordinasikan melalui email untuk memastikan semua langkah dan prosedur telah disepakati dan dipahami oleh semua pihak terkait seperti telihat pada Gambar 3.33. Implementasi ini dilakukan untuk menambahkan hostname XPMDCDFDCOC01, XPMDCDFDCOC02, XPCBDDFDDCL01, XPCBDDFDDCL02, XPCBDITCHCV01, dan XPCBDITCHCV02. Tujuan penerapannya adalah memastikan bahwa semua hostname tersebut dapat termonitor oleh Splunk, sehingga BEI dapat mengawasi dan mengelola operasional data dari server-server ini.



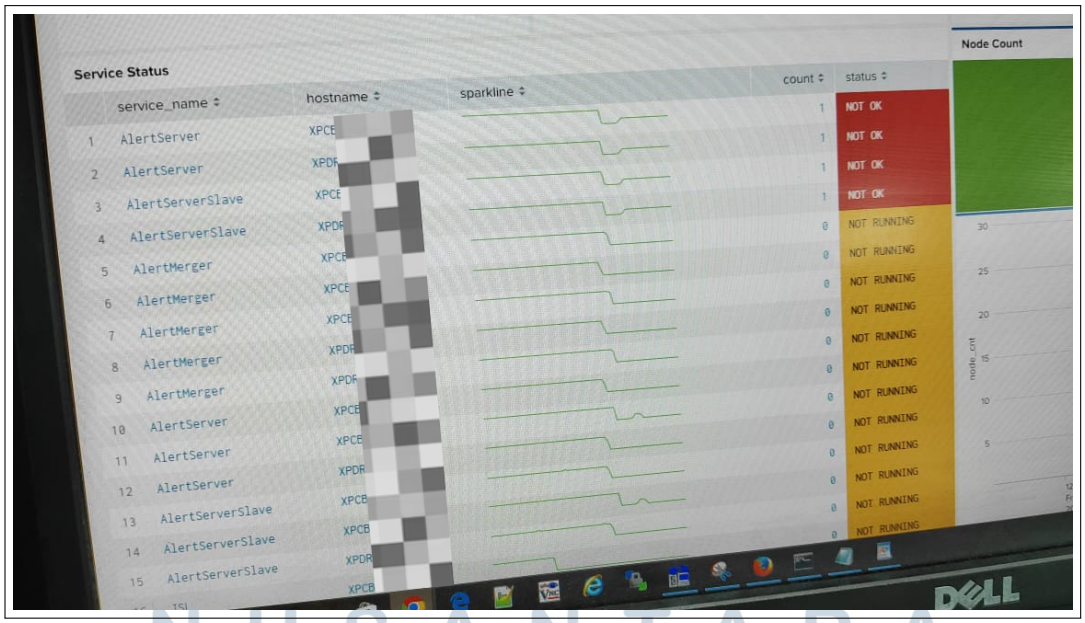
Gambar 3.33. Koordinasi Dokumen SIF yang telah Dibuat Melalui Email

Pada implementasi kali ini, TC intern bekerja di bawah bimbingan Bapak Akmal, mentor dan senior TC. Kehadiran Bapak Akmal memastikan bahwa setiap langkah implementasi dilakukan dengan benar dan sesuai dengan *best practice*. Konfigurasi yang dilakukan melibatkan beberapa aspek penting, termasuk setup Splunk untuk memonitor dan menganalisis berbagai data dari server PT. BEI. Salah satu langkah krusial dalam proses ini adalah membuat *alert* untuk mendeteksi dan memberikan peringatan jika terjadi kondisi anomali atau yang tidak diharapkan. Dengan adanya *alert* ini, tim operasional dapat mengambil tindakan preventif untuk mencegah gangguan yang lebih besar. Pembuatan *alert* dilakukan pada *calculated field* agar dapat disimpan dan dipanggil ketika dibutuhkan. Gambar 3.34 yang merupakan tangkapan foto dari *query* yang telah dibuat, terlihat contoh pembuatan *eval expression* dalam Splunk untuk menampilkan tiga status yaitu *OK* alias *running*, *Not Running*, dan *Not OK* pada *server* milik PT. BEI. *Eval expression* ini digunakan untuk mengevaluasi kondisi *server* dan menampilkan informasi yang

dapat membantu tim IT memantau operasional terhadap kinerja *service server*. Adapun visualisasi yang menampilkan status *service* yang menggunakan *alert* terlihat seperti pada Gambar 3.35.



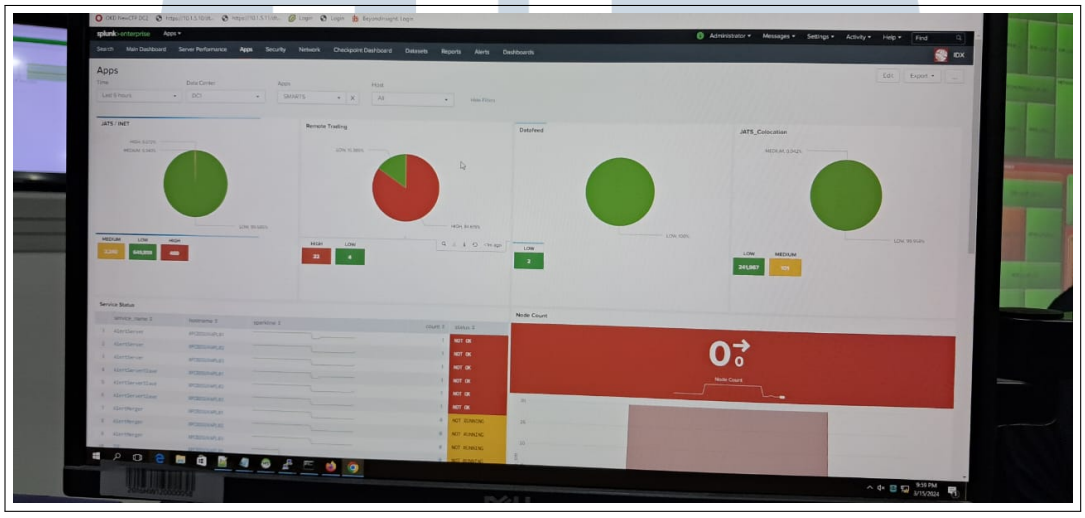
Gambar 3.34. Query Pembuatan *Alert* Status untuk *Server Services*



Gambar 3.35. Tampilan Visualisasi yang Menggunakan *Alert* Status

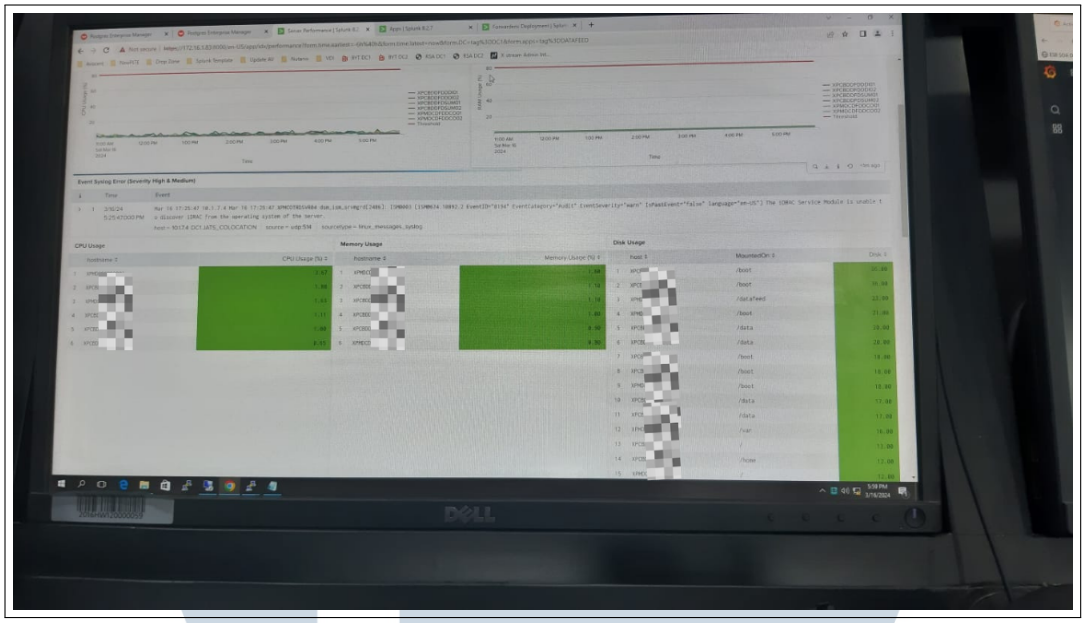
Secara keseluruhan visualisasi yang memperlihatkan status atas *services* yang berjalan pada server akan disatukan kedalam *dasboard* Apps. *Dashboard* ini dibangun dengan tujuan agar tim operational IT BEI dapat memantau layanan

aplikasi-aplikasi yang sedang berjalan. *Dasboard* dirancang untuk mempermudah pengguna dengan memberikan pilihan berbentuk *dropdown* agar dapat difilter berdasarkan *data center*, nama *apps*, ataupun nama *host*. Gambar 3.36 di bawah merupakan tampilan dari *dashboard app* yang telah dibuat. Dimana untuk melihat *traffic* pada setiap *service apps* pada *server*, dibuatlah visualisasi berbentuk *pie chart* dengan pelebelan penggunaan ditiga kategori yakni kecil (low), sedang (*medium*), dan tinggi (*high*). Penetapan kategori ini dibuat berdasarkan nilai *threshold* yang ditetapkan oleh tim IT BEI.



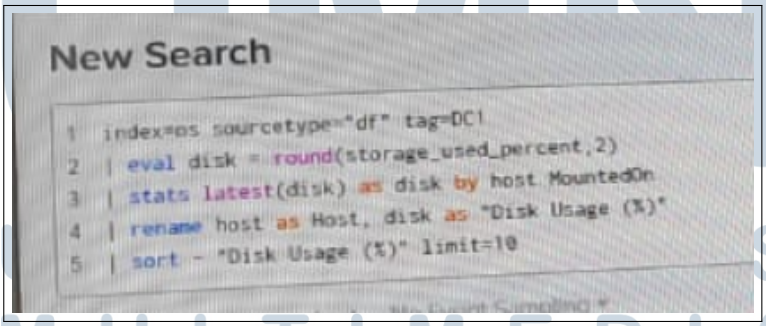
Gambar 3.36. Tampilan Visualisasi yang Menggunakan *Alert* Status

Selain itu, implementasi ini juga mencakup visualisasi yang menampilkan metrik penting seperti *CPU Usage*, *Memory Usage*, *Disk Usage*, dan *Data Usage*. Visualisasi ini memberikan gambaran tentang performa *server* dan dapat membantu mendeteksi masalah sebelum menjadi serius. Untuk perhitungan apakah suatu server kelebihan atau tidak, tim IT BEI dan TC menetapkan suatu *threshold* terhadap persentase penggunaan. Apa bila angka persentase penggunaan tidak melebihi 90 persen maka indikator berwarna hijau, sedangkan melebihi 90 persen maka indikator berubah menjadi merah. Gabungan dari berbagai visualisasi tersebut kemudian dijadikan satu *dashbord* yang dapat memantau performa *server* secara keseluruhan. Gambar 3.37 menunjukan bagaimana *dashboard* menampilkan performa *server* dalam menjalankan layanan BEI.



Gambar 3.37. Tampilan *Dashboard Server Performance*

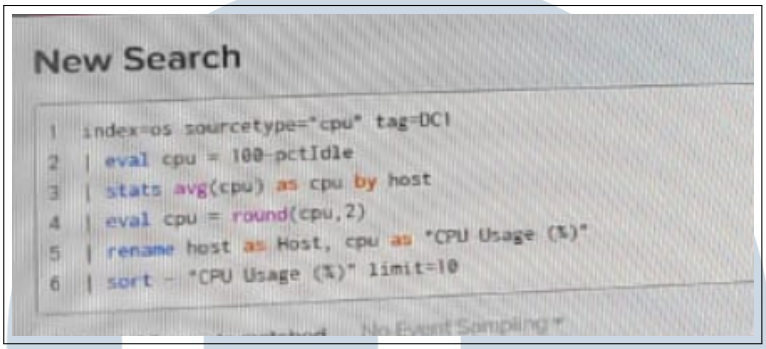
Untuk membuat dashboard, misalnya dalam membuat visualisasi kinerja penggunaan server, TC perlu melakukan query SPL pada kotak pencarian Splunk. Query ini akan mengekstrak data yang diperlukan dari metrik server dan menghasilkan visualisasi yang relevan. Dengan menggunakan query SPL, TC dapat membuat berbagai visualisasi seperti diagram lingkaran, diagram batang, dan diagram garis yang dapat dimasukkan ke dalam dashboard. Pengguna dapat menyimpan query ini sebagai laporan atau peringatan, yang kemudian dapat ditambahkan ke dalam dashboard.



Gambar 3.38. *Query* SPL untuk membuat Visualisasi *Disk Usage Server*

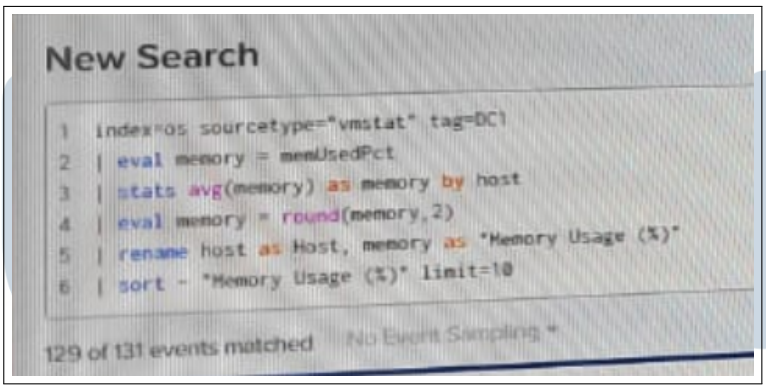
Gambar 3.38 merupakan perintah query yang dijalankan untuk membuat visualisasi penggunaan disk di mana TC menggunakan field storage_used_percentguna menampilkan penggunaan disk. Query ini akan mengumpulkan data terkait penggunaan disk pada setiap host yang dimonitor, dan menampilkan hasilnya dalam bentuk visualisasi yang mudah dipahami. Dengan

menggunakan field ini, pengguna dapat melihat seberapa banyak kapasitas disk yang telah digunakan oleh setiap host dalam jaringan.



Gambar 3.39. *Query* SPL untuk membuat Visualisasi *CPU Usage Server*

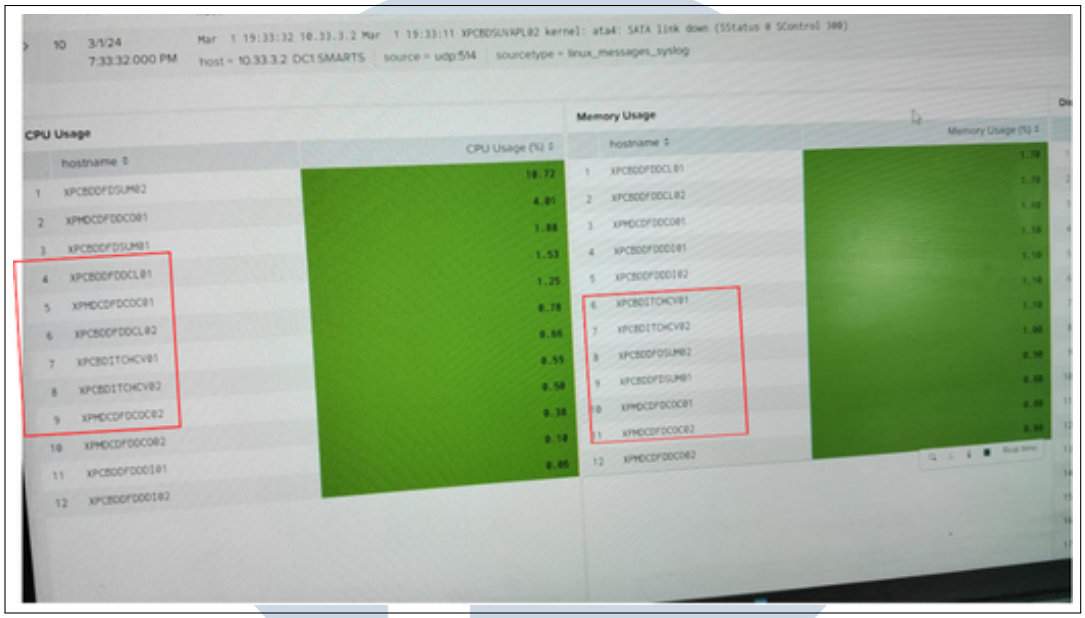
Selanjutnya Gambar 3.39 menunjukkan perintah query yang dijalankan untuk membuat visualisasi penggunaan CPU. TC menggunakan perintah evaluntuk melakukan pengurangan 100 dengan field pctIdleguna menampilkan penggunaan CPU. Evaluasi ini dilakukan untuk mendapatkan persentase penggunaan CPU dengan cara menghitung perbedaan antara total kapasitas CPU (100%) dan kapasitas yang tidak terpakai (pctIdle). Hasilnya kemudian divisualisasikan untuk memberikan gambaran yang jelas mengenai beban kerja CPU pada setiap host.



Gambar 3.40. *Query* SPL untuk membuat Visualisasi *Memory Usage Server*

Gambar 3.40 menunjukkan perintah *query* yang dijalankan untuk membuat visualisasi penggunaan memori di mana TC menggunakan *field* memUsedPctguna menampilkan penggunaan memori. *Query* ini mengumpulkan data tentang persentase memori yang digunakan pada setiap host, yang kemudian divisualisasikan untuk membantu tim operasional IT BEI dalam memantau dan mengelola pemakaian memori. Dengan visualisasi ini, pengguna dapat dengan mudah melihat mana host yang mendekati atau melebihi kapasitas memori yang

tersedia, sehingga tindakan pencegahan dapat diambil sebelum terjadi masalah kinerja.

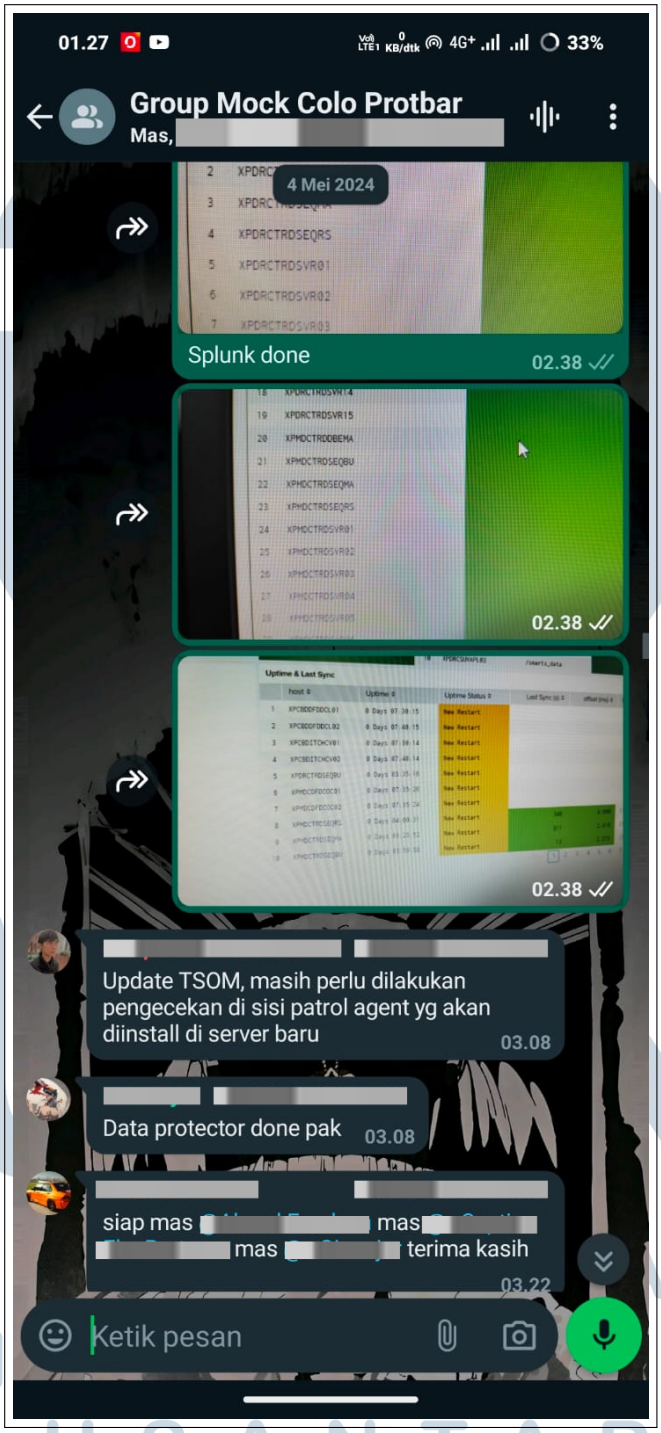


Gambar 3.41. Bukti *Hostname* Sudah Masuk ke *Dashboard* Splunk

Seperti terlihat pada Gambar 3.41, bahwa penambahan data hostname XPMDCDFDCOC01, XPMDCDFDCOC02, XPCBDDFDDCL01, XPCBDDFDDCL02, XPCBDITCHCV01, dan XPCBDITCHCV02 berhasil masuk ke dashboard Splunk. Dalam gambar ini, terlihat bahwa semua hostname baru yang ditambahkan dapat terdeteksi dan dimonitor oleh Splunk, menampilkan metrik penting seperti penggunaan CPU, penggunaan memori, dan penggunaan disk. Keberhasilan ini menunjukkan bahwa konfigurasi yang dilakukan sudah tepat dan sistem dapat memproses serta menampilkan data dari hostname-hostname baru tersebut dengan baik.

Karena aktivitas implementasi dilakukan secara *onsite*, segala bentuk dokumentasi dan pengecekan dilakukan secara manual oleh tim operasional IT BEI. Setelah selesai melakukan implementasi serta konfigurasi kemudian TC akan melakukan koordinasi dengan pihak BEI untuk memastikan segala bentuk kegiatan telah berhasil dan selesai. Selain itu, tidak lupa TC melakukan tangkapan foto atas pekerjaan yang dilakukan saat implementasi sebagai bukti pekerjaan telah berjalan dengan baik. Tangkapan foto ini kemudian dikirimkan melalui grup Whatsapp sekaligus meminta tanggapan oleh tim IT BEI secara keseluruhan. Gambar 3.42 menunjukan bagaimana koordinasi dilakukan setelah implementasi berhasil. Proses dokumentasi ini membantu memastikan transparansi dan memberikan catatan untuk

referensi di masa depan.



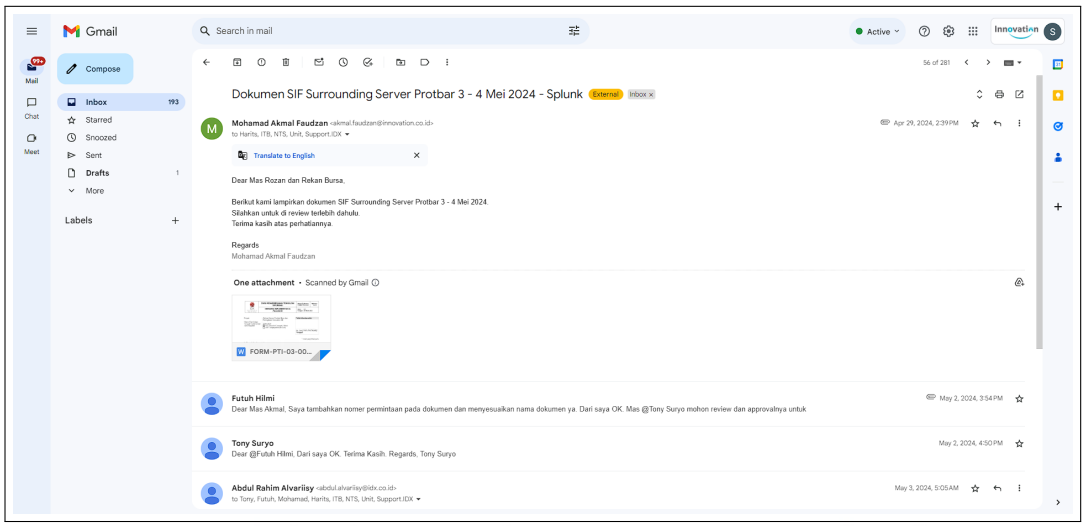
Gambar 3.42. Tampilan Koordinasi pada Grup Whatsapp

Setelah implementasi selesai, fase *fallback* juga disiapkan untuk memastikan bahwa jika terjadi masalah, sistem dapat kembali ke konfigurasi sebelumnya tanpa mengganggu operasi bisnis. *Fallback* adalah bagian penting dari

proses implementasi, karena memberikan jaminan bahwa sistem tetap stabil dan dapat dipulihkan dengan cepat jika diperlukan. Dengan demikian, implementasi dan *fallback* fitur *services* pada klien dilakukan dengan hati-hati, mengikuti prosedur yang ketat untuk memastikan kelancaran operasional BEI.

3.3.8 Minggu 16 - 19: Implementasi dan *Fallback* untuk Aktivasi *Server* Protokol Baru pada Klien

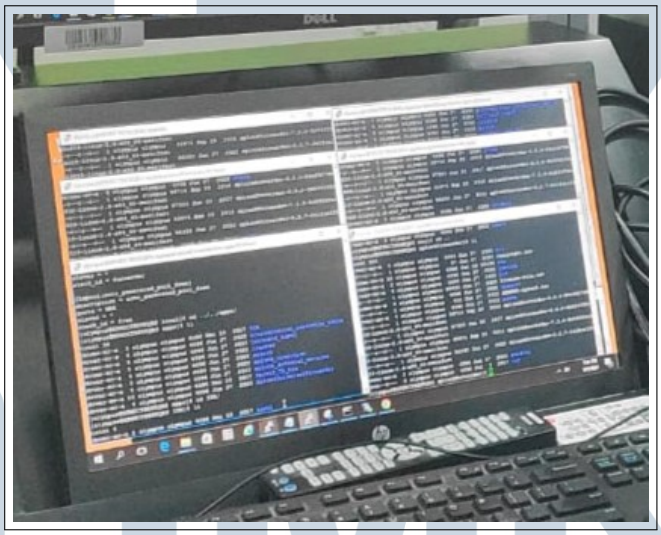
Protokol baru yang dimaksud dalam implementasi ini adalah penambahan hostname server baru XPMDCTRDSEQMA, XPMDCTRDSEQBU, dan XPMDCTRDSEQRS pada DC 1, serta XPDRCTRDSEQMA, XPDRCTRDSEQBU, dan XPDRCTRDSEQRS pada DC 2. Sebelum proses implementasi dilakukan, TC terlebih dahulu membuat dokumen SIF (Skenario Implementasi dan Fallback) yang mencakup seluruh rencana langkah-langkah teknis serta prosedur fallback jika terjadi kesalahan. Dokumen SIF ini kemudian dikirm melalui email untuk disepakati oleh kedua belah pihak, yaitu tim TC dan klien, agar memastikan bahwa semua pihak memiliki pemahaman yang jelas tentang proses dan tujuan implementasi sebagaimana terlihat pada Gambar 3.43.



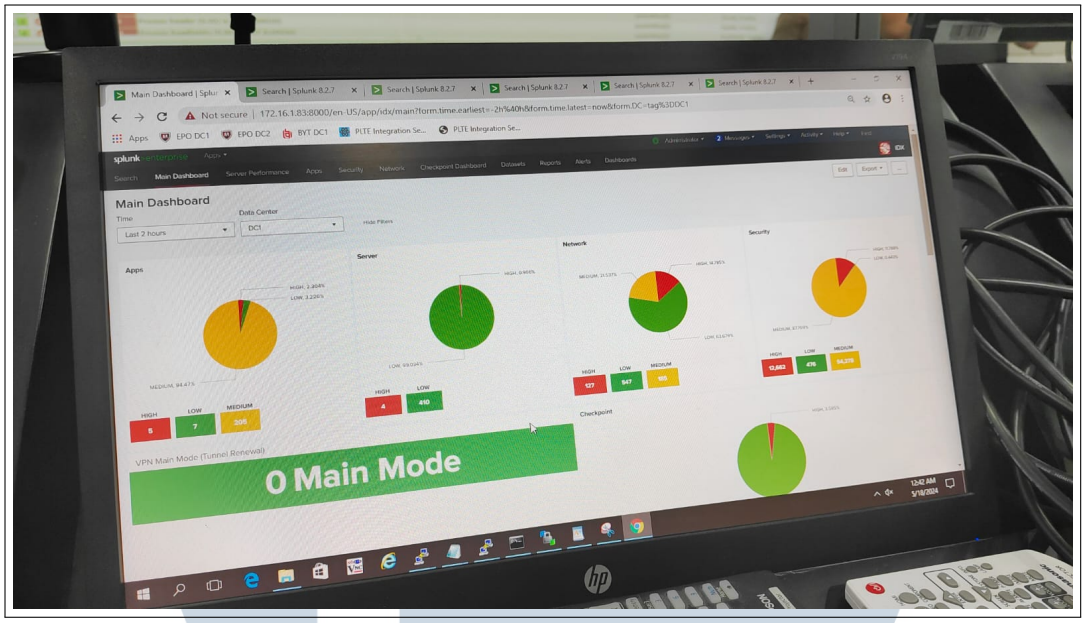
Gambar 3.43. Koordinasi Dokumen SIF Untuk Protol Baru Melalui Email

Implementasi dan *fallback* merupakan proses penting dalam mengaktifkan protokol baru pada *server* klien. Saat klien memutuskan untuk menerapkan protokol baru, divisi TC harus memberikan dukungan teknis untuk memastikan bahwa data dari protokol tersebut masuk ke dalam sistem Splunk dan memperbarui *dashboard monitoring* sesuai kebutuhan. Proses ini membutuhkan serangkaian

langkah yang rumit dan memerlukan perhatian terhadap detail untuk memastikan kesuksesan. Langkah pertama dalam implementasi adalah menghubungkan ke server klien menggunakan *Secure Shell* (SSH) melalui aplikasi PuTTY. Pada Gambar 3.44, terlihat bagaimana TC mengakses *server* untuk keenam *hostname* dengan memasukkan alamat IP, *username*, dan *password* untuk mendapatkan akses. Setelah berhasil masuk, langkah selanjutnya adalah menjalankan perintah UNIX yang diperlukan untuk melakukan konfigurasi di dalam *directory* Splunk. Konfigurasi ini mencakup penyesuaian *file-file* penting dan struktur direktori, serta memastikan bahwa Splunk siap menerima data dari protokol baru yang akan dijalankan oleh klien. Fase ini dilakukan sebelum protokol baru mulai aktif, sehingga sangat penting untuk memastikan semuanya telah diatur dengan benar untuk mencegah gangguan saat protokol baru berjalan.

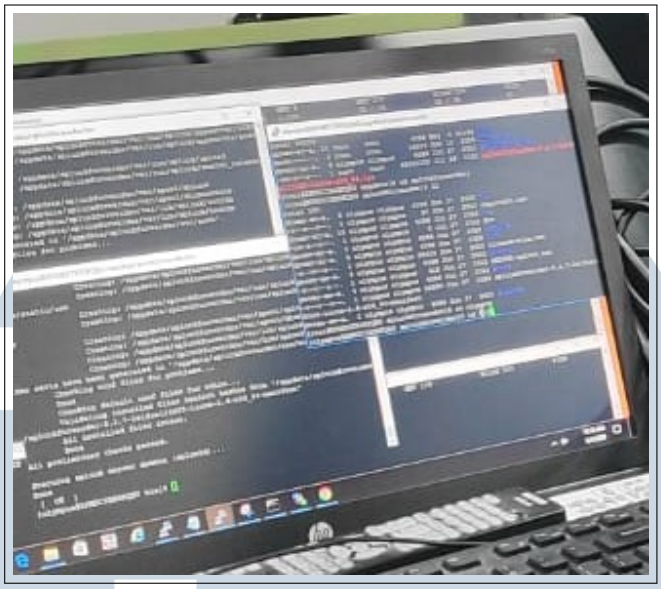


Gambar 3.44. Melakukan Konfigurasi di *Server* melalui *Terminal* PuTTY



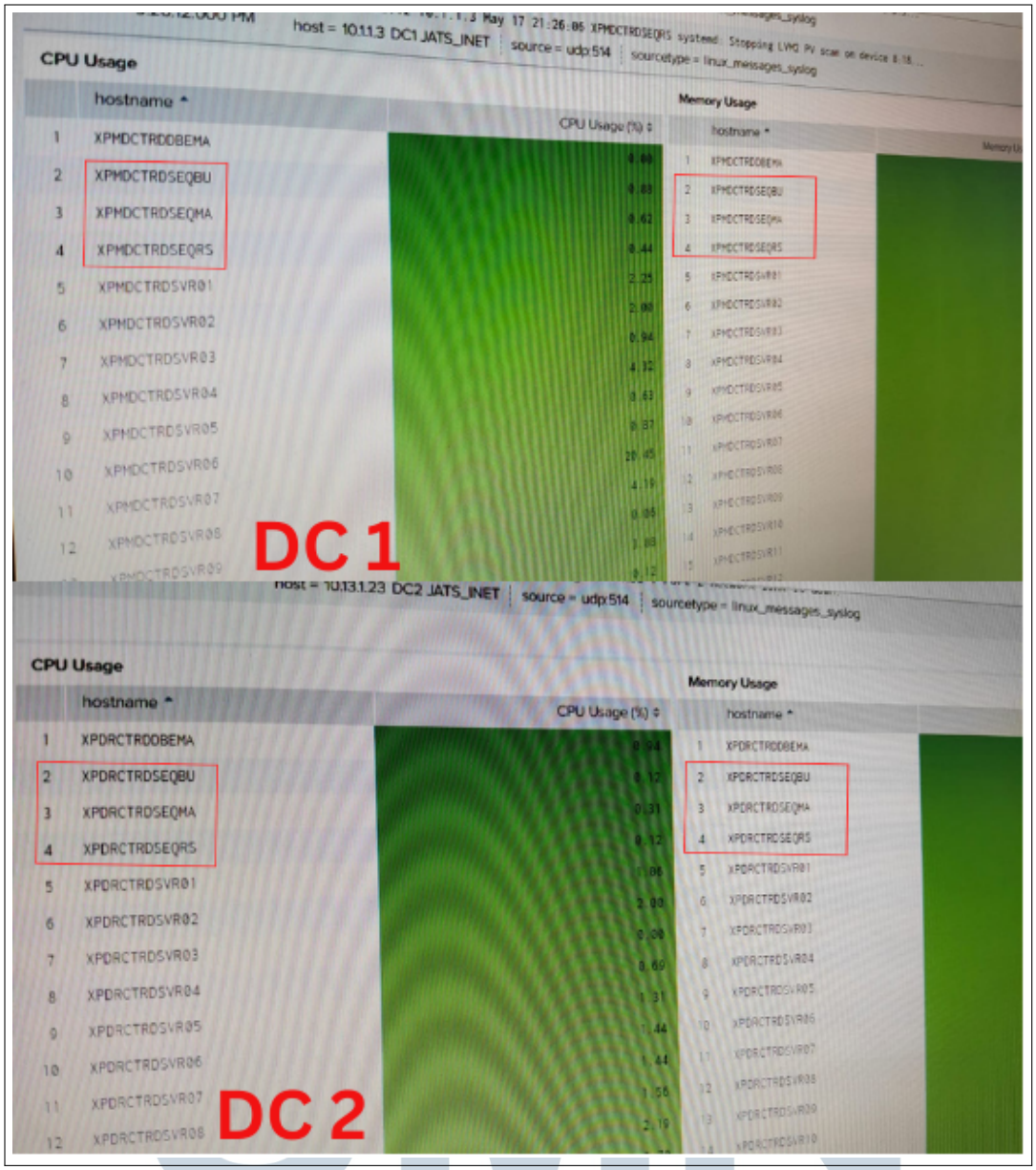
Gambar 3.45. Konfigurasi *Dashboard* untuk Memastikan Data Masuk

Sesudah melakukan konfigurasi pada *server*, langkah berikutnya adalah mengecek *Graphical User Interface* (GUI) Splunk untuk mengkonfigurasi *dashboard monitoring*. Gambar 3.45 menunjukkan proses ini, di mana sebagai TC perlu unutk memastikan bahwa *dashboard* Splunk dapat menerima dan menampilkan data dari protokol baru dengan benar. Proses ini melibatkan penyesuaian tampilan, pengaturan visualisasi data, dan penambahan komponen *monitoring* yang sesuai dengan kebutuhan klien dengan pengaturan *query* SPL. Tujuannya adalah untuk memantau secara *real-time* data yang masuk dan mendeteksi anomali atau masalah potensial saat protokol baru mulai berjalan. Setelah klien mengaktifkan protokol baru, langkah selanjutnya adalah melakukan pengecekan pada *server* melalui *terminal* untuk memastikan bahwa data baru telah mulai masuk ke dalam sistem Splunk. Gambar 3.46 menggambarkan situasi ini, di mana TC memantau aktivitas *server* melalui *terminal* dan mengonfirmasi bahwa data dari protokol baru muncul setelah server diaktifkan.



Gambar 3.46. Memastikan konfigurasi pada Protokol Baru

Untuk proses pengecekan dilakukan melalui konfirmasi dari tim IT BEI dengan cara memperlihatkan bahwa *hostname* baru telah berhasil masuk ke dalam Splunk. Setelah konfigurasi selesai, tim TC melakukan verifikasi untuk memastikan bahwa semua *hostname* baru, yaitu XPMDCTRDSEQMA, XPMDCTRDSEQBU, dan XPMDCTRDSEQRS pada DC 1, serta XPDRCTRDSEQMA, XPDRCTRDSEQBU, dan XPDRCTRDSEQRS pada DC 2, dapat terpantau dengan baik di dalam dashboard Splunk. Tim IT BEI melakukan validasi ini dengan mengakses dashboard Splunk dan mengecek apakah semua *hostname* baru sudah tercantum dan mengirimkan data yang diharapkan. Gambar 3.47 menunjukkan tampilan dashboard Splunk yang memperlihatkan hostname baru telah terdaftar dan aktif. Validasi ini memastikan bahwa data dari *server-server* baru telah berhasil diparsing dan diolah oleh Splunk, sehingga monitoring dapat dilakukan secara *real-time*. Dengan langkah ini, proses implementasi dianggap sukses sepenuhnya, dan sistem siap digunakan dalam lingkungan produksi dengan *fallback* yang telah diatur untuk mencegah gangguan operasi. Proses ini tidak hanya menunjukkan keberhasilan teknis tetapi juga koordinasi yang efektif antara tim TC dan IT BEI dalam memastikan integritas dan keandalan sistem.

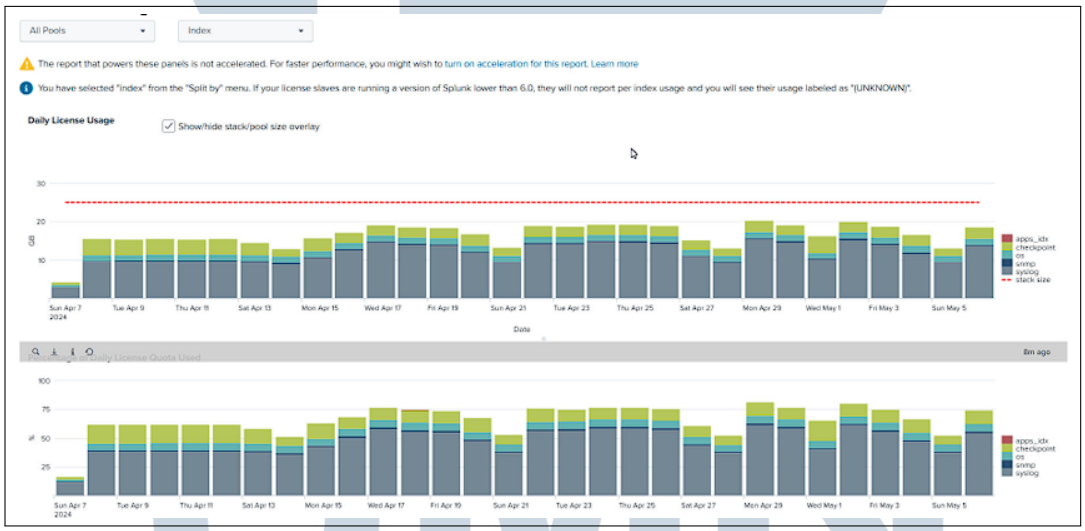


Gambar 3.47. Bukti Data Protokol Baru telah Termonitor di Dashboard

Dengan selesainya langkah-langkah ini, implementasi dianggap sukses dan *server* siap untuk digunakan dalam produksi. *Fallback* juga dipertimbangkan untuk memastikan bahwa jika terjadi masalah, sistem dapat kembali ke konfigurasi sebelumnya tanpa mengganggu operasi. Proses ini menuntut pemahaman mendalam tentang infrastruktur *server*, konfigurasi Splunk, dan pendekatan *troubleshooting* yang efektif. Sesi-sesi ini juga menjadi kesempatan bagi peserta magang untuk memahami kompleksitas implementasi protokol baru dalam konteks operasional nyata.

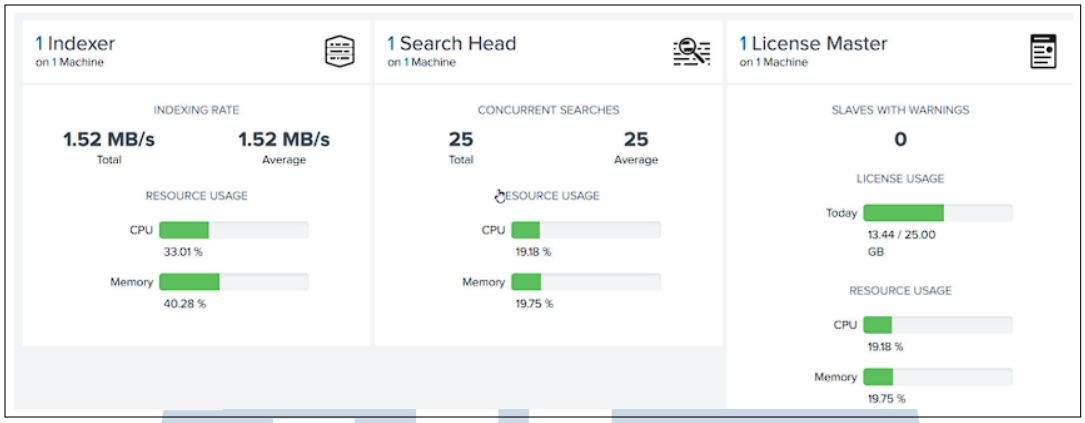
3.3.9 Minggu 18 - 19: *Preventive Maintence* Splunk Untuk Periode Februari-Mei 2024

Preventive maintenance Splunk untuk periode Februari hingga Mei 2024 dilakukan dengan mengakses IP GUI Splunk melalui VPN yang disediakan oleh pihak IT BEI. Akses ini memungkinkan tim TC untuk menjalankan serangkaian kegiatan pemeliharaan penting guna memastikan sistem Splunk beroperasi dengan optimal. Salah satu langkah utama dalam pemeliharaan ini adalah pengecekan lisensi untuk mengetahui apakah kuota lisensi pemakaian melebihi batas atau tidak, yang dilakukan untuk menjamin arus data dapat diproses di Splunk dengan lancar. Gambar 3.48 menampilkan informasi kuota lisensi terpakai harian dalam kurun waktu 30 hari terakhir berdasarkan setiap index, yang membantu dalam memantau penggunaan dan memastikan tidak ada pelanggaran terhadap batasan lisensi.



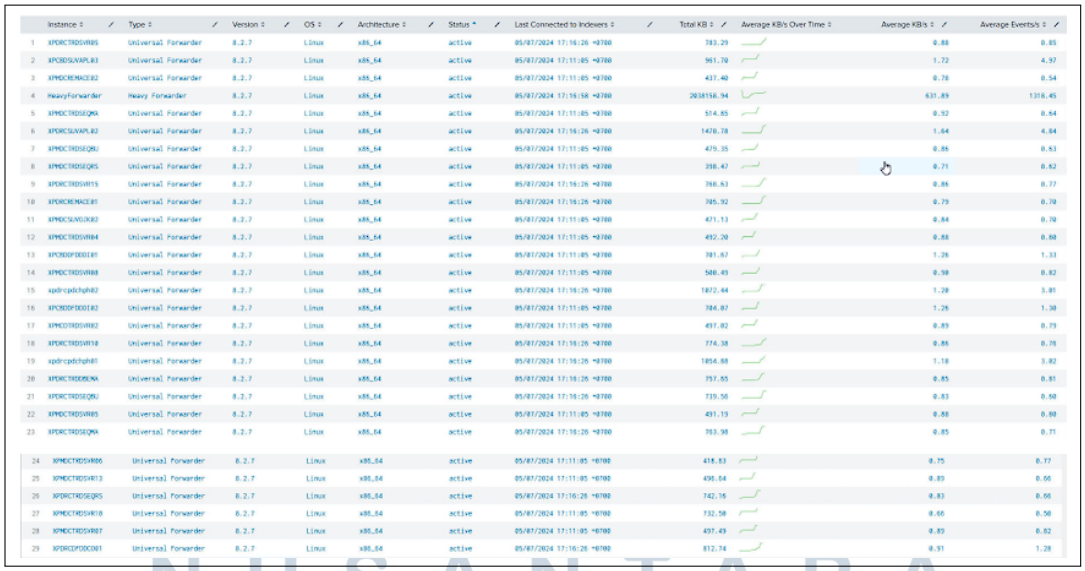
Gambar 3.48. Pengunaan Lisensi Splunk Selama 30 Hari Kebelakang

Selain lisensi, kegiatan pemeliharaan juga mencakup pengecekan penggunaan CPU dan *memory* pada topologi Splunk, khususnya pada *indexer* dan *search head*. Seperti yang ditunjukkan pada Gambar 3.49 di *Monitoring Console*, overview dari Splunk *Indexer* dan *Search Head* menunjukkan bahwa tidak ada penggunaan yang melebihi 60% dari ambang batas standar Splunk *monitoring console*. Detail penggunaan *resource* adalah sebagai berikut, *Search Head* menunjukkan penggunaan CPU sebesar 19,18% dan *memory* sebesar 19,75%, sementara *Indexer* menunjukkan penggunaan CPU sebesar 30,01% dan *memory* sebesar 40,28%. Pemantauan ini penting untuk memastikan bahwa sistem beroperasi dalam kondisi optimal tanpa *overutilization*.



Gambar 3.49. Pengunaan Lisensi oleh Splunk Selama 30 Hari Kebelakang

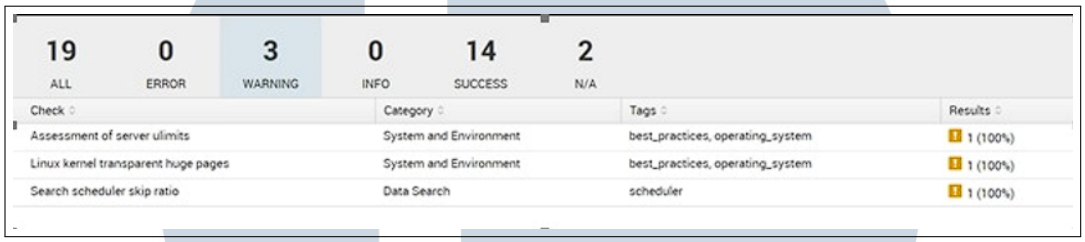
Selanjutnya, pengecekan dilakukan pada Splunk *Universal Forwarder* untuk memastikan setiap *agent-agent* mengirim data secara konsisten pada setiap hostname server. Apabila ditemukan *agent* yang tidak aktif, TC akan berkoordinasi dengan pihak IT BEI untuk memastikan apakah *hostname* tersebut masih digunakan. Jika *agent missing* dan *hostname* masih digunakan, TC akan menindaklanjuti dengan mengakses server yang bermasalah untuk melakukan perbaikan. Gambar 3.50 menunjukkan bahwa semua *agent Splunkforwarder* berstatus aktif dan tidak ada konsumsi *resource* yang besar baik di DC1 maupun DC2, menandakan bahwa data *forwarding* berjalan dengan baik.



Gambar 3.50. *Preview* Daftar *Forwarder* Dengan Status *Active*

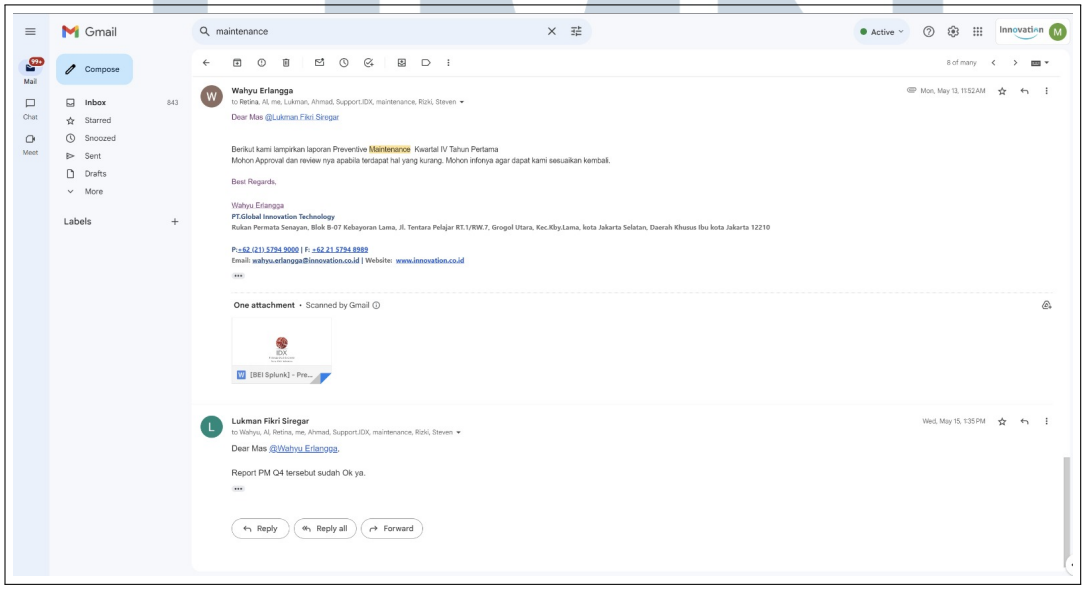
Langkah terakhir dalam *preventive maintenance* adalah melakukan *health check* pada Splunk untuk mengevaluasi keseluruhan proses yang terjadi di dalam sistem dan memberikan rekomendasi konfigurasi sesuai dengan best practice.

Gambar 3.51 menunjukkan tiga warning dalam *health check*, Linux Kernel *Transparent Hugepages*, yang direkomendasikan untuk dinonaktifkan sesuai best practice namun dapat diabaikan, *Assessment of server ulimits*, dengan rekomendasi untuk meningkatkan *Ulimit* guna meningkatkan performa yang juga dapat diabaikan, dan *Search Scheduler Skip Ratio*, yang mengukur kinerja penjadwalan pencarian, dan warning ini juga dapat diabaikan.



Gambar 3.51. *Health Check Dashboard* Splunk

Kesimpulan dari serangkaian preventive maintenance ini adalah bahwa *health check* pada lingkungan Splunk menunjukkan tiga peringatan yang bersifat rekomendasi dan tidak mendesak. Untuk penggunaan lisensi Splunk Enterprise, lisensi sudah diperbarui sebesar 25GB/day dan berlaku hingga 19 Januari 2038 dan 22 Desember 2024, memastikan bahwa sistem tetap memiliki kapasitas yang memadai untuk waktu yang panjang. Proses *preventive maintenance* ini penting untuk memastikan lingkungan Splunk tetap optimal dan mampu mendukung kebutuhan operasional IT BEI secara efektif.



Gambar 3.52. Dokumen *Maintenance* yang Diserahkan Melalui Email

Seluruh pengecekan tersebut kemudian dibungkus menjadi laporan

maintenance Splunk yang terperinci, mencakup semua temuan dan rekomendasi dari setiap tahap pengecekan. Laporan ini disusun dengan detail yang lengkap untuk memastikan transparansi dan memberikan gambaran yang jelas tentang kondisi sistem kepada pihak terkait. Laporan *maintenance* ini kemudian dikirimkan melalui email kepada pihak IT BEI sebagai bentuk dokumentasi resmi dan untuk referensi di masa depan yang terlihat sebagaimana Gambar 3.52. Dengan adanya laporan ini, pihak IT BEI dapat lebih mudah melakukan tindak lanjut serta memastikan sistem Splunk tetap dalam kondisi optimal.

3.4 Kendala yang ditemukan

Adapun secara keseluruhan pelaksanaan kegiatan magang di GIT yang berlangsung lebih dari 640 jam kerja dapat berjalan lancar. Akan tetapi, pada saat proses bekerja terdapat permasalahan atau kendala saat pengerjaan suatu tugas yang diberikan. Berikut adalah kendala yang dialami saat pelaksaaan magang berlangsung:

1. Minimnya pengetahuan pada sektor jaringan dan arsitektur IT di sebuah perusahaan dapat menyebabkan kendala dalam bekerja. Situasi ini menekankan perlunya waktu untuk belajar bidang tersebut agar dapat memahami layanan yang ditawarkan oleh GIT.
2. Adanya penggunaan *software tools* analitik data dan *monitoring* seperti Splunk yang belum pernah dipelajari sebelumnnya, sehingga harus beradaptasi dengan *tools* tersebut untuk mengerti bagaimana cara kerjanya.
3. Pemberian tugas yang tidak jelas dan kurang terstruktur dapat menyebabkan kebingungan apabila suatu tugas sudah selesai. Hal ini terjadi karena adanya miskomunikasi dalam beberapa kasus pada saat WFH terlebih karena terlalu banyak grup Whatsapp.

3.5 Solusi atas Kendala yang Dihadapi

Setiap kendala atau permasalaah yang ditemukan selama proses kerja berlangsung. Langkah intervensi selanjutnya adalah upaya penemuan solusi sebagai jalan keluar dari kendala yang dihadapi. Solusi ini dilakukan untuk mencari cara alternatif untuk mengatasi dampak dari kendala tersebut, yakni:

1. Untuk poin pertama dan kedua pada kendala yang ditemukan, perusahaan memberikan fasilitas berupa *training* diawal berupa mentor yang ekspert pada jaringan dan aristektur IT. Selain itu, para peserta magang yang terdaftar dengan *email* kantor dapat mengakses kursus online yang disediakan *official* dari Splunk karena perusahaan telah berkerja sama dengan Splunk.
2. Sedangkan kendala pada poin ketiga dapat ditanggani dengan menanyakan secara eksplisit mengenai tugas kerjaan secara mendetail terhadap PM terkait, saat pertemuan pagi dilakukan.