3. Analisis dan Desain Sistem

Pada bab ini akan dibahas mengenai monitoring keamanan siber yang sedang berjalan, permasalahan yang dihadapi, analisis kebutuhan perusahaan, serta desain sistem berupa *flowchart*. Analisa dan desain sistem pada bab ini bertujuan untuk memberikan gambaran mengenai permasalahan yang ada, kebutuhan untuk menyelesaikan masalah, serta implementasi yang akan dilakukan.

3.1 Analisis Monitoring Keamanan Siber yang Sedang Berjalan

Saat ini, tim keamanan siber UK Petra melakukan *monitoring* dengan menggunakan bantuan SIEM (*Security Information and Event Management*) *open-source* yaitu Wazuh. Selain Wazuh, tim keamanan siber UK Petra juga menggunakan sebuah *firewall* yaitu Sangfor NGAF yang bertugas untuk memblokir serangan – serangan siber yang masuk. Sangfor NGAF memiliki pusat operasi keamanan atau SOC yang memungkinkan tim keamanan siber untuk mengontrol, memantau, dan menganalisis keamanan jaringan. Baru – baru ini tim keamanan siber UK Petra melakukan percobaan untuk memvisualisasi data *log* dengan menggunakan bantuan *tools* Grafana yang bersifat *open source*. Data *log* diambil dari *firewall* Sangfor NGAF milik UK Petra, kemudian dimasukkan kedalam Grafana agar *log* tersebut dapat dikelola.

3.2 Analisis Permasalahan

Permasalahan yang terjadi adalah Wazuh yang digunakan di UK Petra hanya untuk memonitoring *end point* saja. Untuk mengamankan dan memantau keamanan jaringan, UK Petra menggunakan *firewall* Sangfor NGAF. Namun SOC yang dimiliki oleh Sangfor NGAF kurang *detail* dalam memvisualisasikan hasil *log* keamanan, sehingga tim keamanan siber UK Petra mencoba alternatif lain dengan cara menggunakan bantuan *tools* Grafana yang berguna sebagai visualisasi. Namun, tim keamanan siber UK Petra hanya baru melakukan uji coba untuk membaca hasil *log firewall* di Grafana dalam bentuk *text* saja. Adanya visualisasi tambahan seperti *time series, stat, table, donut chart, bar chart, logs panel dan juga alert list* pada *dashboard* Grafana tentunya akan lebih membantu tim keamanan siber dalam memantau kondisi keamanan jaringan terkini.

3.3 Analisis Kebutuhan

Dari permasalahan diatas, maka dapat disimpulkan bahwa visualisasi *monitoring* keamanan siber yang dilakukan dengan menggunakan Grafana masih kurang *detail* dalam memantau keamanan jaringan yang berasal dari *log firewall* Sangfor NGAF. Sehingga dibutuhkannya implementasi Grafana sebagai berikut :

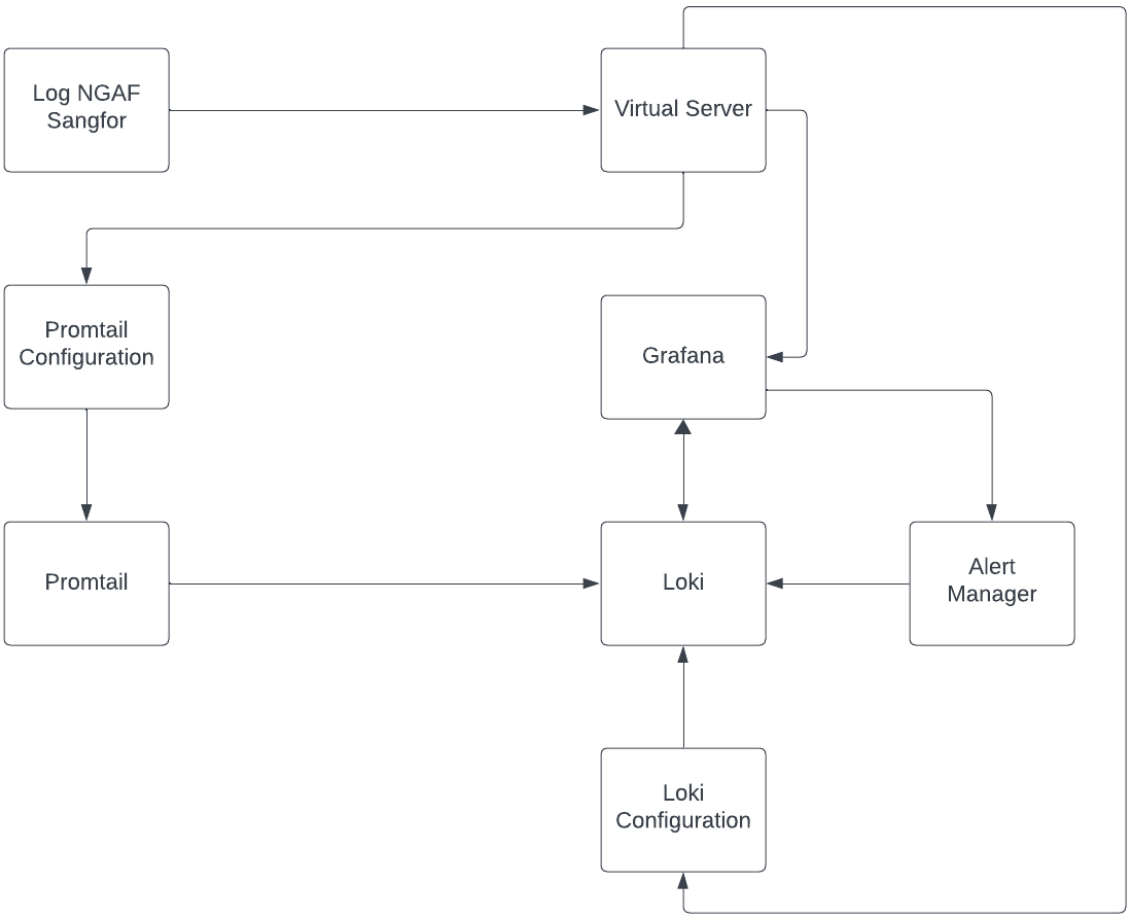
- Grafana mengelolah hasil *log* dari *firewall* Sangfor NGAF dengan bantuan loki dan promtail
- Grafana menampilkan visualisasi *time series*, *stat*, *table*, *donut chart*, *bar chart, logs panel* dan juga *alert list* ke dalam satu halaman
- Grafana dapat mengirimkan notifikasi peringatan melalui email

3.4 Desain Sistem

Pada bagian ini akan dibahas mengenai desain perancangan sistem yang akan diimplementasikan. Desain ini bertujuan untuk memberikan gambaran bagaimana sistem yang diimplementasikan berjalan.

3.4.1 Desain *Flowchart* Implementasi Sistem

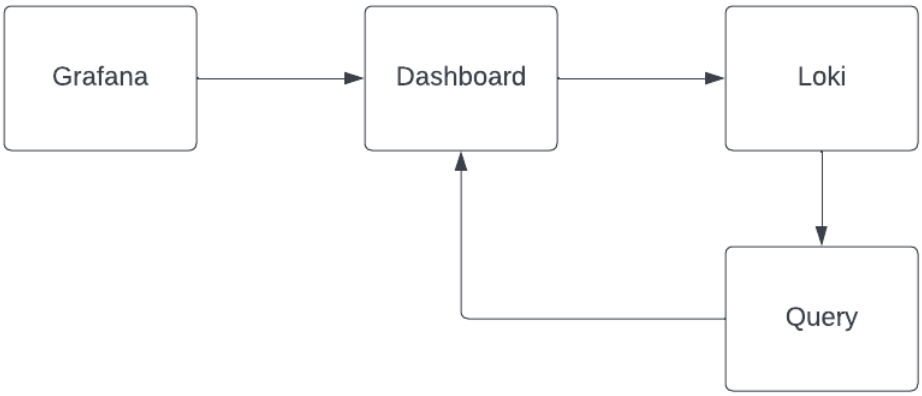
Flowchart pada bagian ini menggambarkan keseluruhan sistem yang akan di implementasikan. Log Sangfor NGAF akan di export menuju sebuah virtual server yang menggunakan sistem operasi Linux. Kemudian pada virtual server akan di *install* tiga *tools* yang diperlukan yaitu Grafana, Loki, dan Promtail. Setelah itu, admin dapat mengkonfigurasi promtail dan loki melalui *file config* yang ada pada server. Setelah semuanya selesai dikonfigurasi maka Grafana dapat dijalankan. Admin bisa mengakses Grafana melalui *port* 3000, kemudian *login* dengan menggunakan *username* dan *password* admin agar dapat mengedit, mengelola, dan menggunakan Grafana. Loki harus ditambahkan dulu melalui halaman *data source* yang terdapat di *navigation bar* milik Grafana. Promtail memiliki tugas untuk mengirimkan semua *log* yang terpilih ke Loki. Kemudian, *alert manager* dapat dipasang pada Loki untuk mendapatkan notifikasi peringatan. *Alert manager* dapat ditemukan di *navigation bar* milik Grafana.



Gambar 3.1 Desain Flowchart Implementasi Sistem

3.4.2 Desain Flowchart Implementasi Dashboard Grafana

Flowchart pada bagian ini menggambarkan proses untuk mengelola data *log* agar dapat divisualisasikan pada Grafana. Halaman *dashboard* dapat diakses melalui melalui Grafana, kemudian pengguna dapat menambahkan panel baru. Pada halaman panel, pengguna dapat menentukan *data source* yang ingin digunakan, kemudian melakukan *Query* untuk mengelola data tersebut.



Gambar 3.2 Desain Flowchart Implementasi Dashboard Grafana

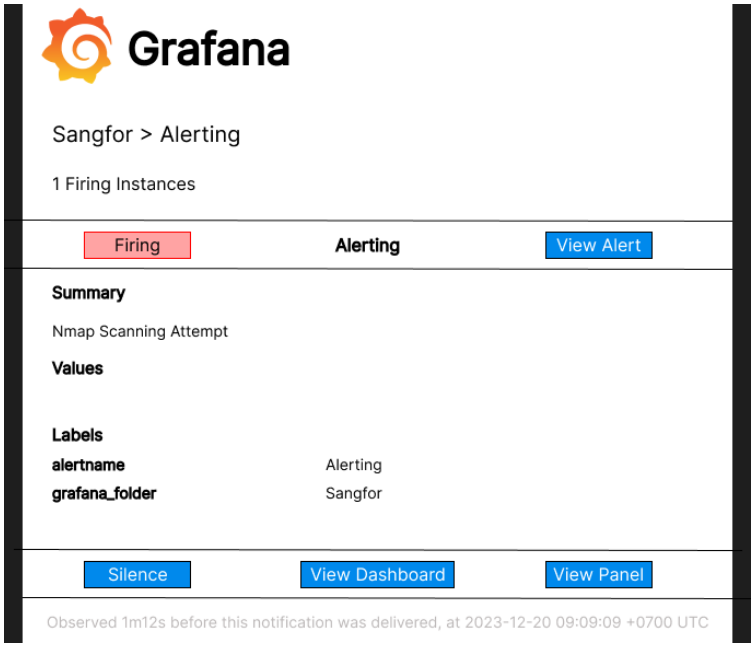
3.4.3 Desain Dashboard Grafana

Pada bagian *dashboard* akan digunakan beberapa visualisasi yaitu *time series* yang berguna untuk mencatat bagaimana kenaikan jumlah serangan pada jangka waktu tertentu. Digunakan juga visualisasi *stat* untuk mentotalkan masing-masing tingkat ancaman dan juga serangan yang dilakukan. Kemudian ada *table* yang berguna untuk menginformasikan *detail – detail* penting seperti *source ip address*, *destination ip address*, tanggal serangan, tingkat ancaman serangan, dan lainnya. Kemudian terdapat juga *pie chart* untuk mengkategorikan tingkat ancaman secara keseluruhan. Selanjutnya ada histogram dan logs yang berguna untuk melihat aktivitas log yang ada. Terakhir ada juga alert list yang berguna untuk melihat alert yang tersedia sekaligus untuk melihat alert yang sedang aktif.

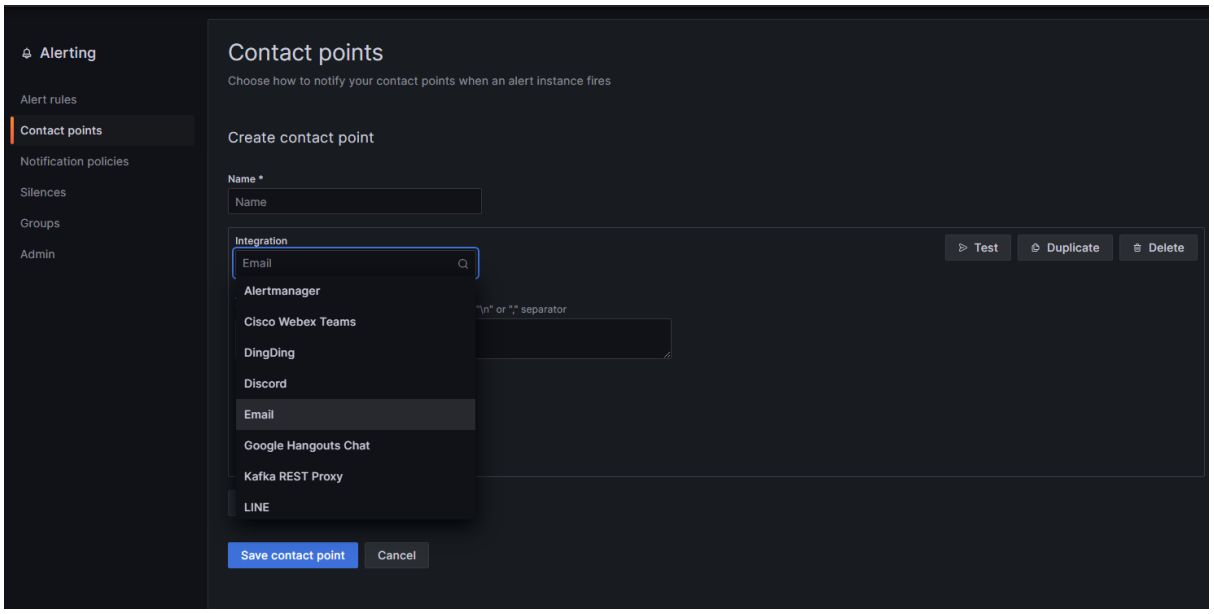
Gambar 3.3 Ilustrasi Tampilan Dashboard Grafana

3.4.4 Desain Alerting Grafana

Pada fungsi *alerting*, Grafana akan mengirimkan notifikasi peringatan jika ada masalah yang terindikasi. Notifikasi peringatan dapat dikirimkan melalui berbagai macam aplikasi, namun pada skripsi ini notifikasi peringatan akan dikirimkan melalui email. Notifikasi yang muncul adalah judul peringatan, kondisi peringatan, catatan kesimpulan dan juga *labels* peringatan yang telah dibuat. Hasil notifikasi dibuat secara *default*.



Gambar 3.4 Ilustrasi Alerting Email



Gambar 3.5 Contoh Alerting Integration