2. Landasan Teori

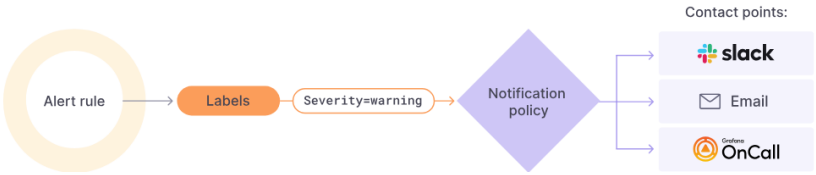
2.1 Tinjauan Pustaka

2.1.1 SIEM

"SIEM atau *Security Information and Event Management* adalah alat yang digunakan untuk memonitor dan menganalisa trafik jaringan secara *real time*. Data yang dianalisis berupa *log* yang dihasilkan oleh perangkat atau aplikasi. Selain itu, *tools* SIEM berfungsi sebagai alat deteksi potensi serangan serta melacak jalur penyusupan." (Huda, 2022). Dengan SIEM, suatu perusahaan maupun institusi akan lebih mudah dalam memantau aktivitas yang tidak biasa dan mencurigakan yang terjadi pada jaringan mereka.

2.1.2 Grafana

"Grafana adalah perangkat lunak open source yang memungkinkan untuk dapat membuat query, memvisualisasikan, memperingatkan, dan menjelajahi metrik, log, dan pelacakan dimanapun data di simpan. Grafana memiliki tools untuk mengubah data time-series database (TSDB) menjadi sebuah grafik dengan visualisasi yang menarik." (Grafana Labs, 2023). Framework plugin yang tersedia pada Grafana juga memungkinkan untuk menghubungkan ke sumber data lain. Pada Grafana terdapat fitur playlist yang berguna untuk menampilkan hasil pada dashboard secara bergilirian. Fitur lain yang dimiliki Grafana adalah Alerting yang berguna untuk memunculkan peringatan pada metrics dan logs. Notifikasi peringatan dengan menggunakan Grafana Alerting dapat dikirimkan melalui sejumlah pemberi peringatan yang berbeda, termasuk PagerDuty, SMS, Email, VictorOps, OpsGenie, atau Slack. Berikut ini adalah contoh struktur Alerting dan dashboard pada Grafana :



Gambar 2.1 Grafana Alerting

Gambar 2.2 Grafana Dashboard

2.1.3 Sangfor NGAF

"Sangfor NGAF adalah solusi keamanan gabungan yang mudah digunakan dan dirancang untuk melindungi organisasi dari ancaman internal, eksternal, saat ini, maupun masa depan." (SANGFOR TECHNOLOGIES, 2023). Sangfor NGAF ini memanfaatkan kecerdasan buatan, machine-learning, dan kecerdasan ancaman realtime dalam memberikan tingkat deteksi malware sebesar 99.76% dan juga mempertahankan ancaman di luar parimeter jaringan. Sangfor NGAF juga sudah terintegrasi dengan NGWAF. Selain itu, Sangfor NGAF juga memiliki SOC (Pusat Operasi Keamanan) Lite yang berguna untuk administrator keamanan perusahaan dalam menentukan tingkat ancaman pengguna dan server. Sangfor NGAF terintegrasi secara mulus dengan endpoint dan produk keamanan jaringan untuk menciptakan solusi yang holistik. Sangfor NGAF memiliki beberapa fitur seperti deteksi malware, threat intelligence, web application firewall (WAF), SOC Lite, anti-ransomware, dan penahanan aplikasi. Pada saat security device sedang berjalan, banyak system yang berjalan, logs akan dibuat. Kegunaan logs adalah untuk merekam keamanan dan aktivitas, kemudian system logs akan dibuat oleh perangkat untuk melihat dan menganalisis hasil logs. Pada sangfor terdapat tiga cara untuk menyimpan log files, secara local, Cyber Command (CCOM) system, dan Syslog. Berikut ini adalah contoh syslog yang dihasilkan oleh sangfor firewall :

```
Jul 28 12:31:01 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:13100553, Src IP:185.191.171.26, Src port:14478,
Jul 28 12:31:02 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:13121382, Src IP:42.200.231.120, Src port:49202,
Jul 28 12:31:03 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:13100553, Src IP:185.191.171.26, Src port:22594,
Jul 28 12:31:04 localhost fwlog: Log type: IPS, policy name:ServerProtection, vulnerability ID:10010282, vulnerability name: Microsoft
Jul 28 12:31:06 localhost fwlog: Log type: APT detection, policy name:InternetProtection, rule ID:0, src IP: 203.189.122.11, src port:
Jul 28 12:31:06 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:0, Src IP:192.53.117.16, Src port:56388, Dst IP:
Jul 28 12:31:06 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:0, Src IP:192.53.117.16, Src port:48866, Dst IP:
Jul 28 12:31:09 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:13100553, Src IP:185.191.171.4, Src port:62872,
Jul 28 12:31:10 localhost fwlog: Log type: APT detection, policy name:InternetProtection, rule ID:0, src IP: 203.189.122.11, src port:
Jul 28 12:31:10 localhost fwlog: Log type: WAF, policy name:ServerProtection, rule ID:13100553, Src IP:185.191.171.4, Src port:7566, D
```

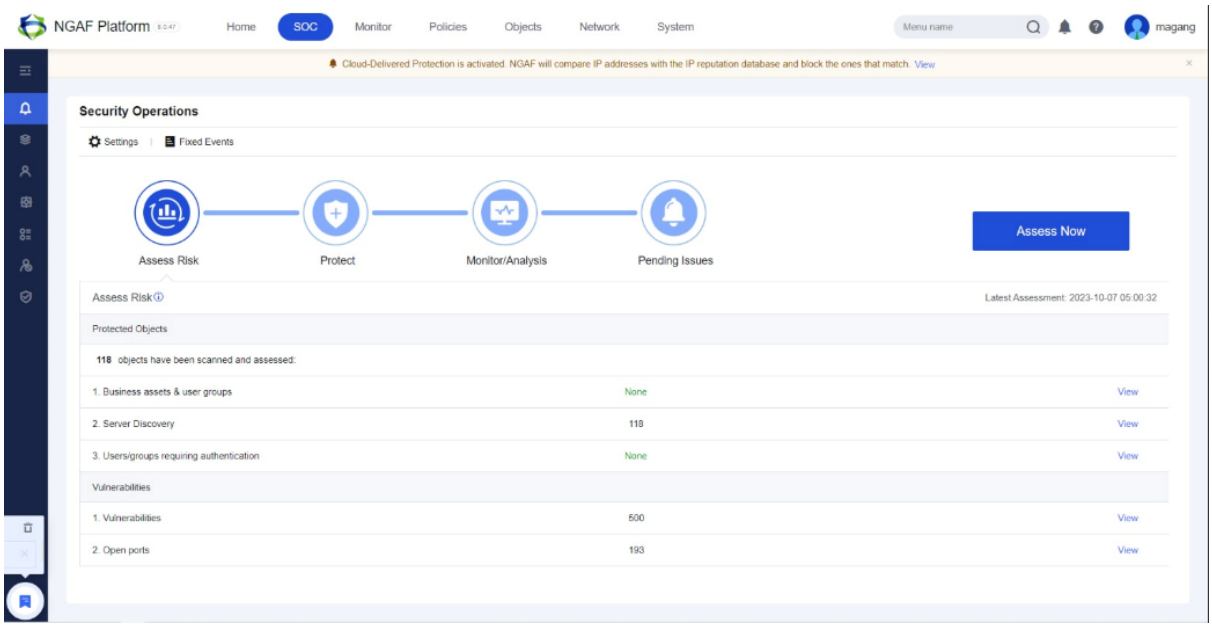
Gambar 2.3 Log Sangfor NGAF (1)

```
Dst IP:203.189.120.52, Dst port:443, attack type:Website scan, threat level:Medium, action:Denied, URL:recruitment.petra.ac.id/dev/type/eyJpdiI6Ii9vZ
Dst IP:203.189.120.27, Dst port:80, attack type:Web site vulnerabilities, threat level:High, action:Denied, URL:cice.petra.ac.id/wordpress/xmlrpc.php
Dst IP:203.189.120.52, Dst port:443, attack type:Website scan, threat level:Medium, action:Denied, URL:recruitment.petra.ac.id/dev/type/eyJpdiI6Ii9vZ
Windows SMB Server Remote Code Execution Vulnerability(CVE-2017-0144), Src IP:14.163.77.244, Src port:52780, dst IP:203.189.123.209, Dst port:445, pr
47363, dst IP: 0.0.0.0, dst port: 53, attack type: Botnet, threat level:High, action:Denied, URL:rtvwerjyuver.com
203.189.120.38, Dst port:80, attack type:Access by hacker IP, threat level:High, action:Denied, URL:cop.petra.ac.id/web/vendor/phpunit/phpunit/src/Uti
203.189.120.38, Dst port:443, attack type:Access by hacker IP, threat level:High, action:Denied, URL:cop.petra.ac.id/v2/vendor/phpunit/phpunit/src/Uti
Dst IP:203.189.120.179, Dst port:80, attack type:Website scan, threat level:Medium, action:Denied, URL:icesti.org/estinnovation/index.php?Itemid=1&cat
43488, dst IP: 0.0.0.0, dst port: 53, attack type: Botnet, threat level:High, action:Denied, URL:rtvwerjyuver.com
st IP:203.189.120.179, Dst port:80, attack type:Website scan, threat level:Medium, action:Denied, URL:icesti.org/estinnovation/index.php?Itemid=1&cati
```

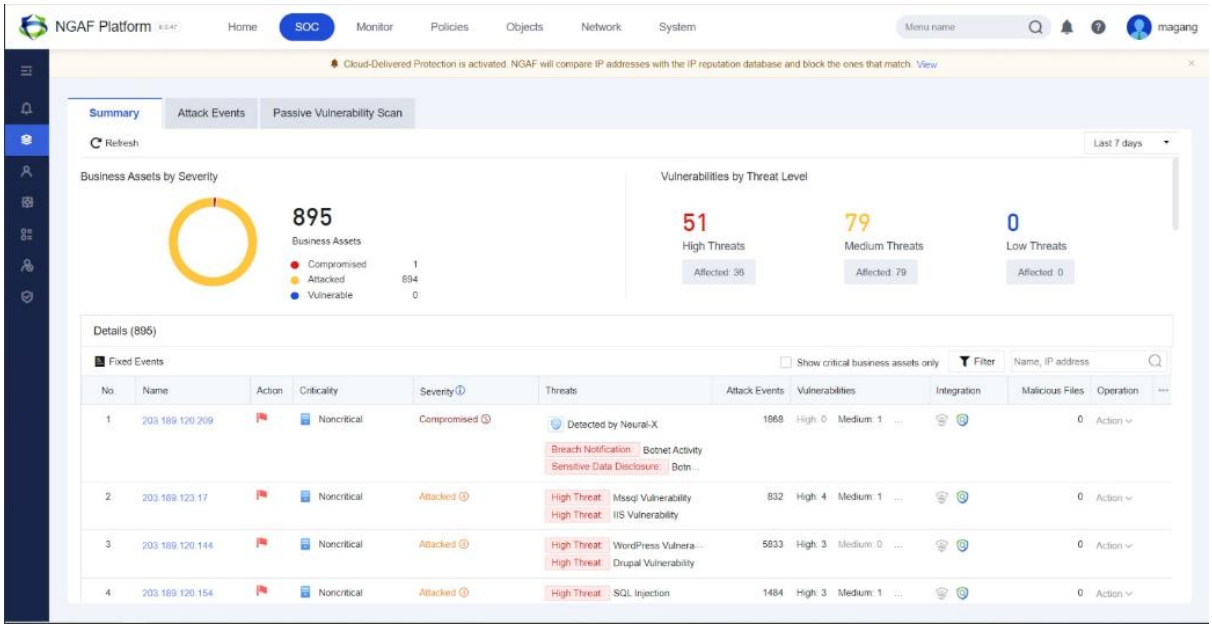
Gambar 2.4 Log Sangfor NGAF (2)

2.1.4 Security Operations Center

"*Security Operations Center* atau SOC adalah pusat dunia maya dari organisasi manapun. Tim ahli yang mengontrol, memantau, dan menganalisis semua data yang mengalir melalui jaringan perusahaan." (SANGFOR TECHNOLOGIES, 2023). Fungsi utama dari SOC ini adalah proteksi dan keamanan dari sebuah organisasi. Dengan menggunakan SOC, tim keamanan siber dapat terbantu untuk menjaga keamanan jaringan. Beberapa fitur pada SOC adalah *security operations, monitoring, log maintenance, alert ranking, incident response, dan recovery and remediation*.



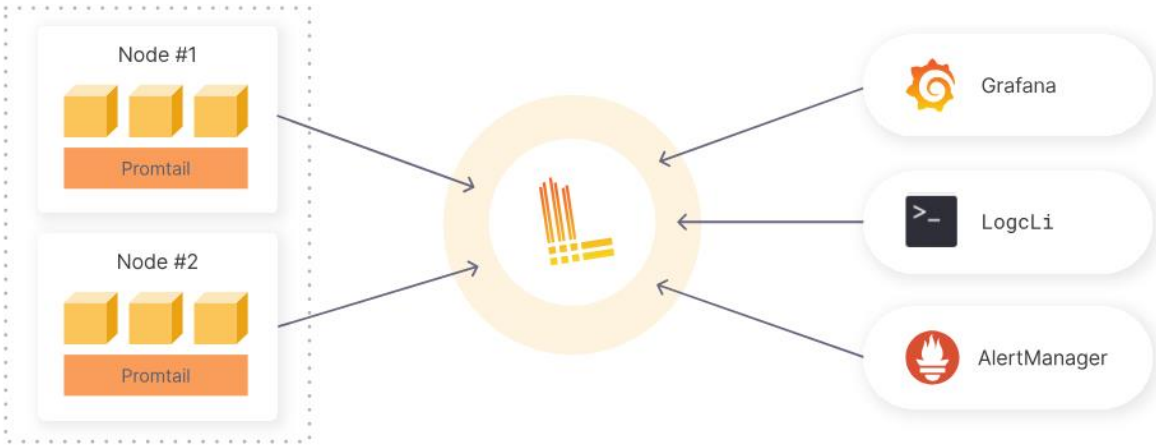
Gambar 2.5 Sangfor NGAF SOC (1)



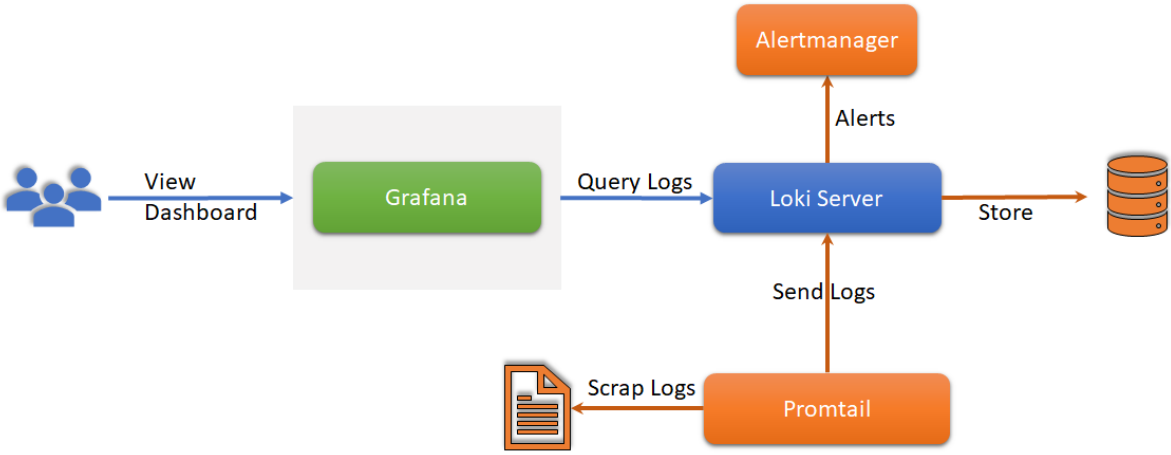
Gambar 2.6 Sangfor NGAF SOC (2)

2.1.5 Loki

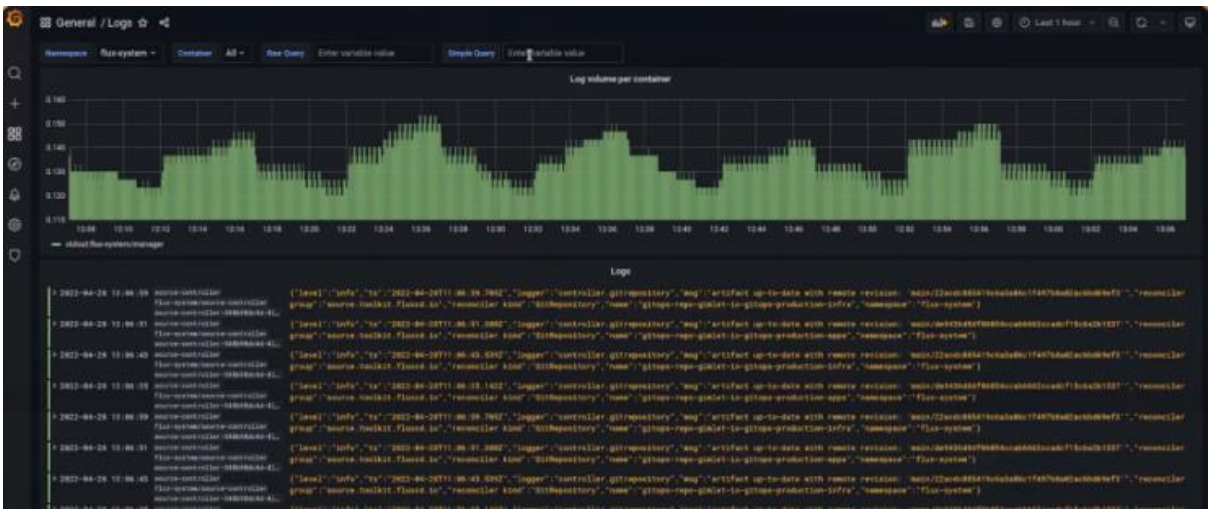
"Loki adalah sistem agregasi *log* yang didesain untuk menyimpan dan mengkueri *log* dari semua aplikasi dan infrastruktur. Loki didesain agar hemat biaya dan gampang untuk dioperasikan." (Grafana Labs, 2023). Loki dapat digunakan untuk mengatur seluruh *log* baik dari sistem *server*, *firewall*, dan lainnya. Membuat metrik dan *alerts* juga menjadi lebih gampang karena sifatnya bukan berupa indeks, melainkan kumpulan label sehingga mudah untuk digunakan. Log pada Loki dapatdipantau secara *realtime, log* di *update* setiap beberapa saat, dan juga pengguna dapat melihat *log* pada kurun waktu tertentu. Namun Loki membutuhkan agen promtail yang bertugas untuk mengirimkan konten *log* lokal ke Loki Grafana.



Gambar 2.7 How Loki Works (1)



Gambar 2.8 How Loki Works (2)



Gambar 2.9 Loki Data Source

2.1.6 Promtail

"Promtail adalah agen yang mengirimkan konten *log* lokal ke *instance* Grafana Loki pribadi atau Grafana Cloud. Biasanya diterapkan ke setiap mesin yang menjalankan aplikasi yang perlu dipantau." (Grafana Labs, 2023). Promtail dikonfigurasi menggunakan *scrape_configs*. Promtail dapat digunakan untuk file yang telah dikompres, Promtail juga dapat dikonfigurasi untuk menerima *log* dari Promtail lainnya atau Loki dengan menggunakan Loki Push API.

2.2 Tinjauan Studi

1. Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram (Rahman, Amnur, & Rahmayuni, 2020)
   - Permasalahan yang diangkat pada penelitian ini adalah ketidakefisienan pada *monitoring* jaringan yang dilakukan oleh administrator.
   - Melakukan perancangan topologi untuk menghasilkan dan mengumpulkan metrik yang akan di visualisasi oleh grafana
   - Hasil dari penelitian ini adalah monitoring server berhasil dilakukan dengan menggunakan Prometheus dan Grafana terhadap server. Alert pada Grafana berhasil mengirin notifikasi ke telegram apabila CPU, memori, ataupun service apache dan mysql jika ada yang mati.
2. Implementasi Security Information and Event Management (SIEM) dengan Splunk untuk Analisis Tren Ancaman Siber Pada Jaringan UII (Kamal, 2022)
   - Permasalahan yang diangkat pada penelitian ini adalah ditemukannya celah keamanan pada salah satu situs web dan digunakan oleh orang yang tidak bertanggung jawab untuk menyerang web lain di luar UII sehingga domain uii.ac.id diblokir oleh vendor karena telah dilaporkan atas tindak kejahatan oleh pemilik web yang diserang dan menyebabkan beberapa layanan di UII tidak dapat berjalan dengan lancar
   - Pengumpulan data sekunder diperoleh dari pencatatan *log firewall* pada Badan Sistem Informasi Universitas Islam Indonesia
   - Hasil dari penelitian ini adalah diimplementasikannya *tools* Splunk untuk analisis tren ancaman siber, data dari *log firewall* dapat diolah dengan baik oleh Splunk. Hasil penelitian ini menunjukkan bahwa Splunk dapat membantu proses analisis ancaman serangan siber, menentukan respon dan mitigasi pada suatu kejadian baik

- ancaman maupun serangan, serta menjadi bahan evaluasi untuk setiap aturan yang diterapkan pada jaringan UII.

3. Implementasi Sistem Monitoring Menggunakan Prometheus dan Grafana (Febriana, 2020)
   - Permasalahan yang diangkat pada penelitian ini adalah dengan peningkatan ukuran dan jumlah perangkat jaringan maka akan semakin tinggi juga resiko terjadinya gangguan pada jaringan tersebut. Maka manajemen jaringan sangat dibutuhkan khususnya sistem *monitoring*.
   - Metode yang digunakan pada penelitian ini adalah System Development Life Cycle (SDLC).
   - Hasil penelitian menunjukkan bahwa penggunaan Prometheus dan Grafana dapat membantu sistem administrasi jaringan untuk mengetahui kondisi jaringan yang ada.