PETUNJUK TEKNIS

ANALISIS *TIMELINE LOG* MENGGUNAKAN PLATFORM SOF ELK

Daftar Isi

Kata Pengantar ..... **Error! Bookmark not defined.**
I. Pendahuluan 3
II. Spesifikasi komputer pengguna 3
III. Fitur-Fitur Platform SOF ELK 4
A. Discover 4
B. Visualize and Dashboard 4
C. Canvas 4
D. Maps 4
E. Machine Learning 4
F. Metrics 4
G. *Log*s 4
H. APM 4
I. Uptime 4
J. Dev Tools 4
K. Stack Monitoring 4
L. Management 4
IV. Penggunaan Platform SOF ELK 5
A. Instalasi 5
B. Input *log* data 7
C. Analisis menggunakan SOF ELK 10

Petunjuk Teknis Analisis *Timeline Log* Menggunakan SOF ELK (Draf)

I. Pendahuluan

Dalam menjalankan salah satu tugasnya, Direktorat Operasi Keamanan Siber yang merupakan salah satu Direktorat di Badan Siber dan Sandi Negara (BSSN) melakukan pengelolaan tanggap insiden siber nasional dan sektor pemerintah, kontak siber nasional, serta pengelolaan krisis siber nasional. Di dalam Direktorat tersebut terdapat *job role* yang memiliki tugas sebagai tim pendukung dalam pelaksanaan kegiatan operasional untuk melakukan analisis *log*, yaitu Tim Tanggap Insiden. Dalam melakukan analisis *log*, Tim Tanggap Insiden menggunakan platform bantuan untuk analisis, salah satunya bernama SOF ELK.

SOF ELK merupakan singkatan dari *Security Operations and Forensics Elasticsearch, Logstash, Kibana*. SOF ELK adalah sebuah platform visualisasi untuk analisis "*big data*" untuk keperluan forensik komputer bagi penyidik forensik dan personil operasi keamanan informasi. SOF ELK merupakan sebuah platform yang bersifat *open source* yaitu gratis atau bebas untuk digunakan oleh masyarakat umum.

II. Spesifikasi komputer pengguna

Spesifikasi komputer yang digunakan untuk menjalankan platform tersebut juga memiliki persyaratan minimalnya. Berikut syarat untuk komputer tersebut :

1. Processor komputer 64-bit
2. RAM komputer : minimal 8 GB
3. *Hard Disk* : minimal 500 GB untuk menjalankan

Kemudian platform SOF ELK berbentuk sebuah file berekstensi .vmdk didalamnya dan dapat langsung digunakan, dengan syarat :

1. VMware Workstation Pro/Player : versi minimal v11.5.3
2. RAM *Virtual Machine* : minimal 4 GB (Menyesuaikan RAM yang disanggupi komputer)
3. *Hard Disk* : minimal 500 GB

III. Fitur-Fitur Platform SOF ELK

A. Discover
Fitur ini digunakan untuk menelusuri dan melakukan penyaringan data untuk mendapatkan informasi tentang strukutr dari data yang dimasukkan.

B. Visualize and Dashboard
Fitur ini merupakan sebuah tampilan visual dari data yang sudah dimasukkan ke dalam SOF ELK. Tampilan visual ini digunakan untuk membantu pengguna dalam melakukan analisis, dengan tampilan data-data dalam bentuk diagram, grafik, dan sebagainya.

C. Canvas
Fitur ini menampilkan data-data dalam bentuk visualisasi dan dapat menggabungkan data-data tersebut menjadi sebuah tampilan yang menarik bagi pengguna dengan warna, gambar, dan teks sesuai kebutuhan pengguna.

D. Maps
Fitur ini menampilkan data-data yang telah dimasukkan dalam SOF ELK dalam bentuk peta.

E. Machine Learning
Fitur ini memberikan kemudahan deteksi anomali pada aktivitas yang mencurigakan dari data yang telah dimasukkan dengan bantuan fungsi di SOF ELK dan meminimalisir kegiatan yang dilakukan oleh pengguna.

F. Metrics
Fitur ini digunakan untuk mencari sebuah item data pada index *elastic* yang berhubungan dalam bentuk sebuah metriks.

G. *Log*s
Fitur ini digunakan untuk mencari dan memfilter semua *log* yang telah dimasukkan dalam *Elasticsearch*.

H. APM
Fitur APM ini berguna untuk melakukan pemantauan layanan perangkat lunak dan aplikasi secara *real-time* atau langsung.

I. Uptime
Fitur ini digunakan untuk memantau ketersediaan dan waktu respon dari aplikasi dan layanan secara *real-time* atau langsung, serta mendeteksi masalah sebelum sampai ke titik pengguna melalui protokol HTTP/S, TCP, dan ICMP.

J. Dev Tools
Fitur ini merupakan sebuah alat yang dapat digunakan untuk berinteraksi dengan data yang telah dimasukkan.

K. Stack Monitoring
Fitur ini digunakan untuk melakukan pemantauan kesehatan data dan performa data yang ada pada *Elasticsearch* dan *Kibana*.

L. Management
Fitur ini merupakan sebuah tampilan awal pengguna untuk mengatur semua hal

yang berhubungan dengan *Elastic Stack* seperti *indices, clusters,* lisensi, pengaturan antarmuka, *index patterns*, dan lain sebagainya.

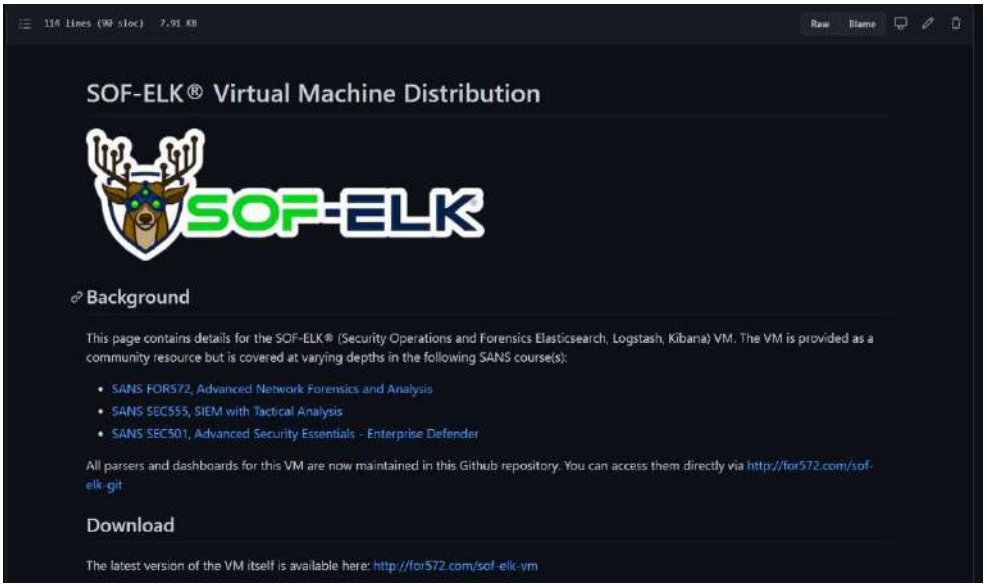
IV. Penggunaan Platform SOF ELK

A. Instalasi

1. Pada aplikasi SOF ELK, sebelum menggunakannya lakukan unduh pada website Github dengan link sebagai berikut :

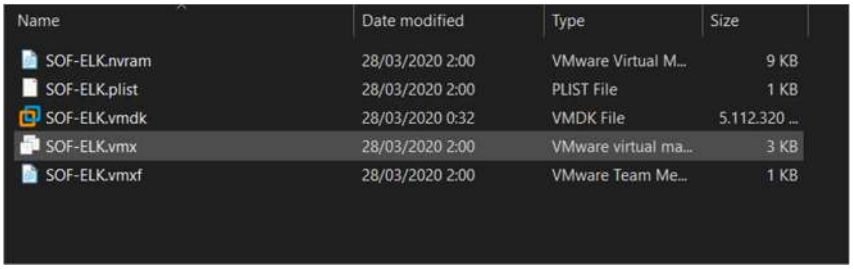
```
https://github.com/philhagen/sof-elk/blob/main/VM_README.md
```

2. Unduh dengan klik tautan pada sub judul “Download”.

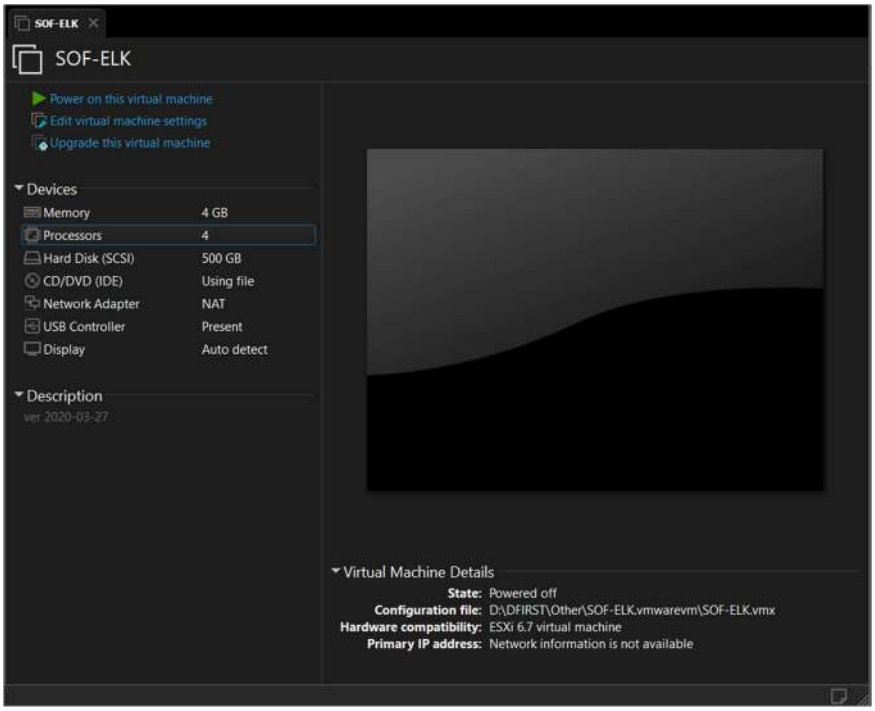


Gambar 1. Unduh SOF ELK

3. Ekstrak file SOF ELK yang telah diunduh, kemudian klik dua kali file yang memiliki ekstensi .vmx, atau klik kanan file tersebut kemudian arahkan pada tab “Open with” dan selanjutnya pilih “VMware Workstation” atau “VMware Player”.



4. Setelah diklik, maka akan muncul tampilan *virtual machine* SOF ELK pada aplikasi VMware. Setelah muncul selanjutnya klik “Power on this virtual machine” untuk memulai menjalankan platform tersebut.



5. Proses *login* dimana diminta memasukkan sebuah user dan *password* untuk masuk menggunakan platform tersebut, dengan user dan *password* sebagai berikut.

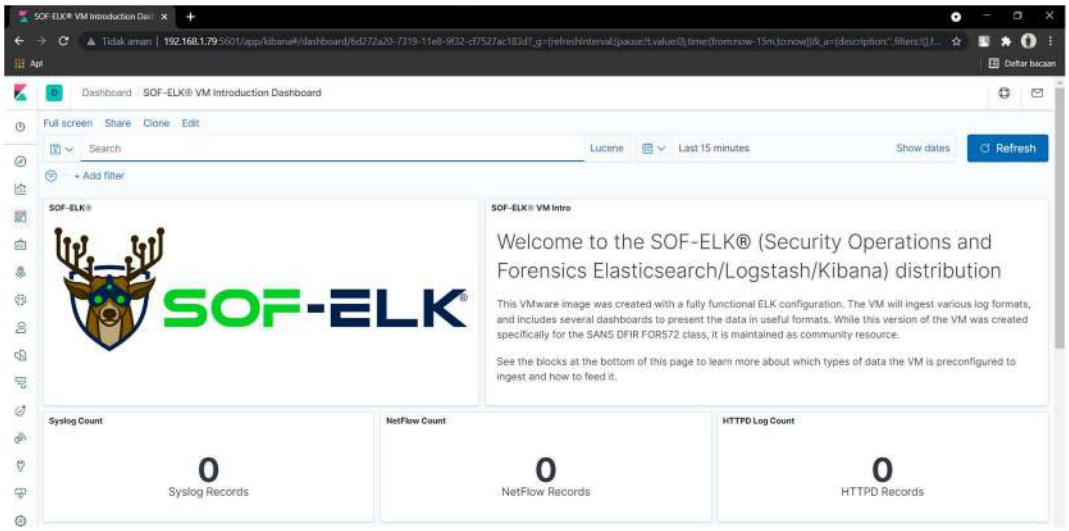
```
sof-elk login : elk_user
Password : forensics
```

6. Setelah berhasil masuk, selanjutnya lakukan pengecekan alamat IP yang digunakan oleh platform SOF ELK.

```
[elk_user@sof-elk ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:82:9e:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.79/24 brd 192.168.1.255 scope global noprefixroute dynamic ens33
       valid_lft 85749sec preferred_lft 85749sec
    inet6 fe80::b612:9a9b:6478:466a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[elk_user@sof-elk ~]$ _
```

7. Lakukan pengecekan apakah platform SOF ELK tersebut telah berjalan atau belum, dengan memasukkan alamat IP dan port dari SOF ELK tersebut pada

browser yang sedang digunakan. **Perlu diingat juga bahwa paltform tersebut menggunakan port 5601**.



8. Jika belum muncul tampilan dari paltform SOF ELK di browser, maka lakukan *restart service* pada *virtual machine* SOF ELK. Hal ini bertujuan untuk melakukan pengulangan layanan kembali.

```
[elk_user@sof-elk ~]$ sudo systemctl restart kibana.service
```

9. Kemudian lakukan pembaruan file konfigurasi SOF ELK.

```
[elk_user@sof-elk ~]$ sudo /usr/local/sbin/sof_elk_update.sh
```

B. Input *log* data

Proses memasukkan *log* data ini bertujuan untuk sumber data yang selanjutnya dilakukan proses analisis aktivitas apa saja yang terjadi di dalam rekaman *log* tersebut.

1. *Log* pada SOF ELK

   Dalam proses analisis, terdapat masukkan data yang dapat diproses oleh platform SOF ELK. Data tersebut antara lain adalah *log syslog*, *nfarch* (*NetFlow*), HTTP, *PassiveDNS*, KAPE (JSON *format*), dan plaso.

   a. *Log* Sys*log*

      Sys*log* merupakan protokol yang digunakan sistem komputer untuk mengirimkan *log-log* sistem data ke penyimpanan. Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index

"**logstash**".

b. *Log* NetFlow

Log ini berisi data rekaman jaringan pada perangkat, seperti alamat dan port IP sumber, alamat dan port IP tujuan, layanan yang digunakan komunikasi, serta informasi lain yang dapat diberikan oleh *log* tersebut. Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index "**netflow**".

c. *Log* HTTP

Log ini berisi tentang rekaman aktivitas komunikasi dari protokol HTTP/S. Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index "**httpdlog**".

d. *Log* Passivedns

Log ini merupakan rekaman dari data yang berisi seperti nama server, alamat IP server, dan domain dari server. Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index "**logstash**".

e. *Log* KAPE

Log ini memiliki format JSON yang harus dilakukan *generate* dan *parsing* dahulu pada data yang akan dimasukkan supaya data tersebut dapat terbaca pada platform SOF ELK dengan menggunakan alat bernama KAPE (*the Kroll Artifact Parser and Extractor*). Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index "**evtxlogs**".

f. *Log* Plaso

Log ini dapat dimasukkan data berformat CSV, dan harus dilakukan *generate* menggunakan alat bernama Plaso. Plaso merupakan sebuah alat untuk membuat *timeline* secara terstruktur sesuai format, dan dapat dibaca pada platform SOF ELK. Log ini ketika sudah dimasukkan ke dalam platform SOF ELK akan masuk dalam kategori index "**plaso**".

2. Langkah *input log*

a. Pertama supaya data *log* tidak tercampur dengan data lain yang ada, lakukan *list* data.

```
[elk_user@sof-elk ~]$ sudo /usr/local/sbin/sof_elk_clear.sh -i
list
```

```
[elk_user@sof-elk logstash]$
[elk_user@sof-elk logstash]$ sudo /usr/local/sbin/sof-elk_clear.py -i list
There are no active data indices in Elasticsearch
[elk_user@sof-elk logstash]$
```

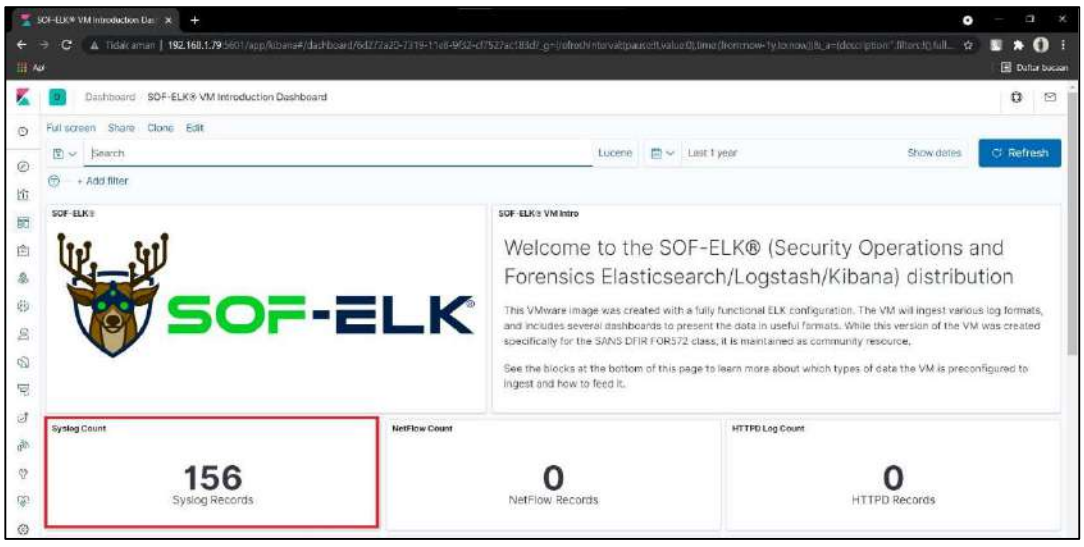
b. Jika terdapat *log* sebelumnya, lakukan penghapusan *log* untuk nantinya akan dimasukkan *log* baru dalam proses analisis.

```
[elk_user@sof-elk ~]$ sudo /usr/local/sbin/sof_elk_clear.sh -i
[folder log yang akan dihapus]
```

c. Selanjutnya masukkan data yang dibutuhkan dalam direktori sesuai file *log* yang dimiliki atau akan dilakukan proses analisis. Sebagai contoh akan diambil data Sys*log* dari operasi sistem Windows.

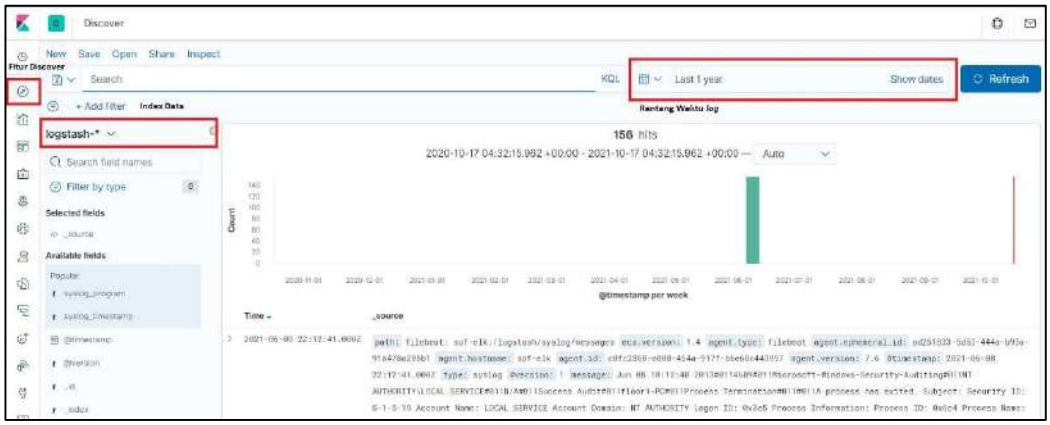
```
[elk_user@sof-elk floor1-PC]$ cd /logstash/syslog/
[elk_user@sof-elk syslog]$ ls
messages
[elk_user@sof-elk syslog]$ _
```

d. Buka platform SOF ELK pada browser dengan memasukkan alamat IP dan port sesuai akses yang diberikan pada SOF ELK. Setelah muncul tampilan platform SOF ELK, data *log* sudah masuk pada platform tersebut menandakan bahwa pemrosesan data berhasil dan sesuai format.



e. Jika isi *log* data yang dimasukkan belum muncul, kemungkinan data sedang mengalami pemrosesan *input data*. Solusi lain ketika data tersebut memang belum muncul, maka buka fitur “Discover” dan atur index masukkan sesuai data *log* yang dimasukkan. Selain itu atur rentang waktu data yang

dimaksud, supaya data tersebut muncul sesuai hasil nyata waktu aktivitas dalam *log* tersebut.



C. Analisis menggunakan SOF ELK

1. Proses analisis dengan pemilahan data

   Dalam proses analisis, pada fitur “Discover” terdapat beberapa bantuan yang dapat membantu pengguna dalam melakukan analisis sebuah *log*, seperti *filtering text*, rentang waktu *log*, sumber *log* yang ditampilkan, dan tampilan umum isi dari *log* yang akan dianalisis.

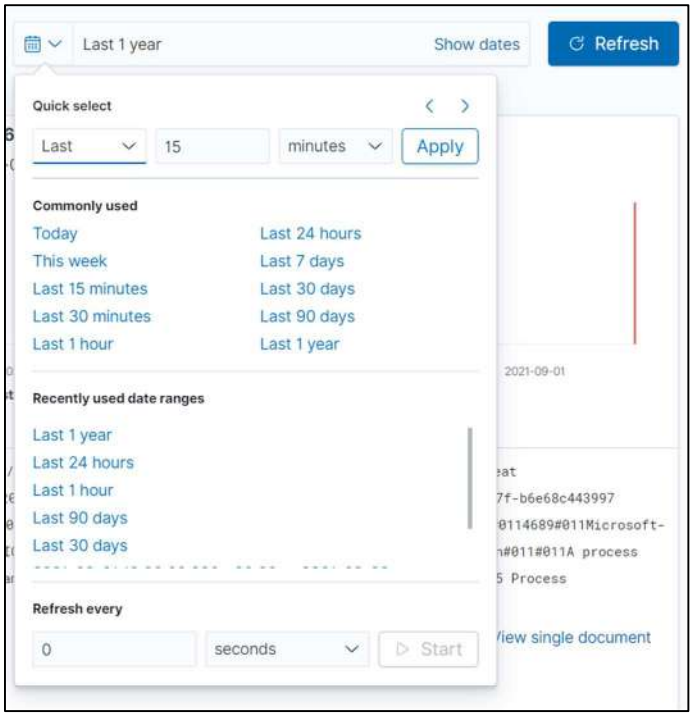
   a. Pencarian menggunakan *filter*

      Pencarian ini digunakan untuk mencari secara spesifik hal apa saja yang akan dicari pengguna. Pencarian ini menggunakan sebuah *field* sebagai bahannya. *Field* disini adalah sebuah format spesifik yang dimiliki oleh sebuah *log*, seperti *timestamp* dari *log* tersebut, alamat IP tujuan maupun sumber, nama host, dan sebagainya sesuai format pada *log*. Pencarian ini juga mengikuti sesuai bahasa yang disediakan oleh platform SOF ELK untuk

melakukan pencarian sesuai *field*.

b. Pengaturan rentang waktu *log*

Dalam menganalisis sebuah *log*, fitur ini dapat bermanfaat untuk fokus dalam proses analisis sebuah data dengan melakukan analisis spesifik data sesuai *timeline* kejadian muncul. Isi dari pengaturan ini meliputi tanggal dan jam sesuai kebutuhan pengguna.



c. Pencarian menggunakan *field*

Pencarian ini digunakan untuk pencarian secara cepat dan ditampilkan secara umum data apa saja yang ada pada *field* yang dipilih. Untuk

menambahkan dapat klik tombol ‘add’ yang ada pada sebelah masing-masing *field*.

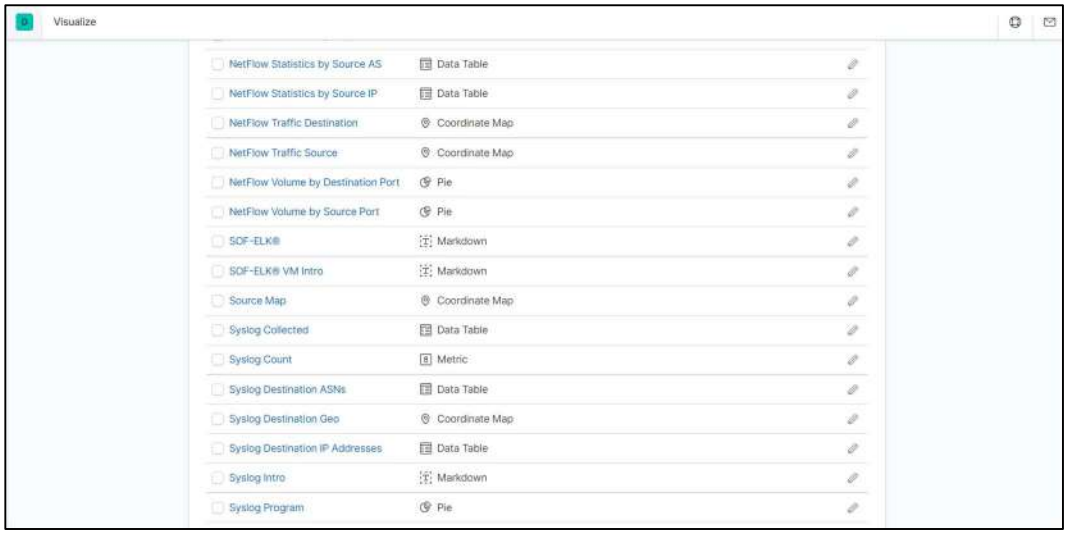
d. Tampilan umum *log* data

Tampilan ini berisi mengenai *timeline* grafik balok beserta keterangan isi masing-masing data di bawah grafik tersebut.

2. Analisis dengan Dashboard

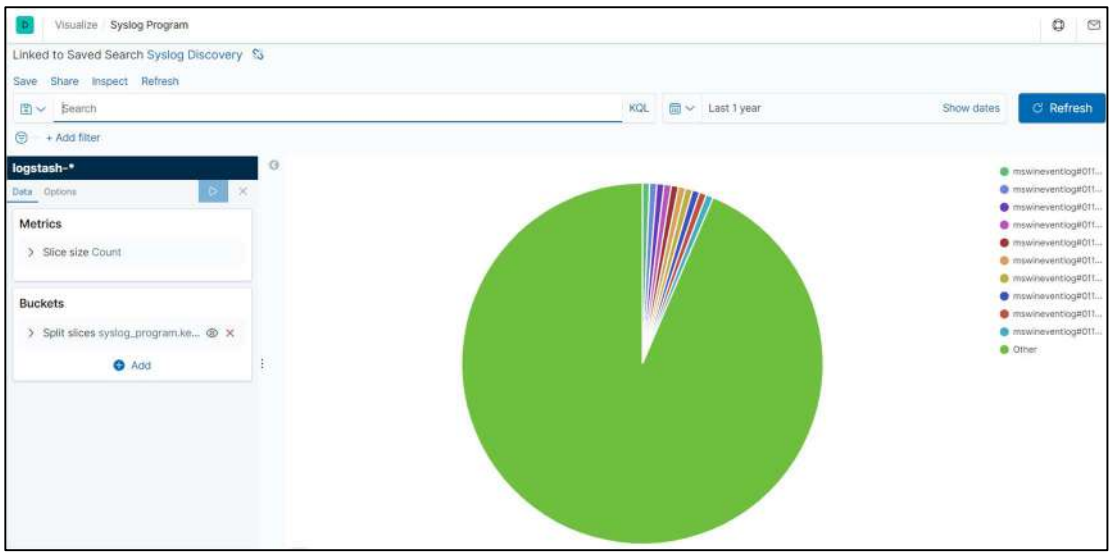
Dalam proses analisis sebuah *log* data, supaya mempermudah proses analisis dapat dibuat sebuah representasi data dalam bentuk sebuah gambar. Pada SOF ELK, hal ini dapat diatur dalam fitur ‘Dashboard’. Dalam proses analisis, SOF ELK juga sudah menyediakan *menu Dashboards* untuk masing-masing *log*.

a. Untuk melihat dan melakukan analisis menggunakan menu bawaan dari SOF ELK, klik fitur menu Dashboard, maka akan muncul beberapa pilihan tampilan data dashboard. Dari *menu* tersebut, pilih yang sesuai dengan data yang sudah dimasukkan ke dalam SOF ELK.



b. Dari *menu* bawaan yang ada, terdapat beberapa kategori yang telah disediakan seperti IP yang ada pada *log* tersebut, program yang berjalan pada *log* tersebut, jumlah data yang masuk pada *log* tersebut, dan sebagainya.

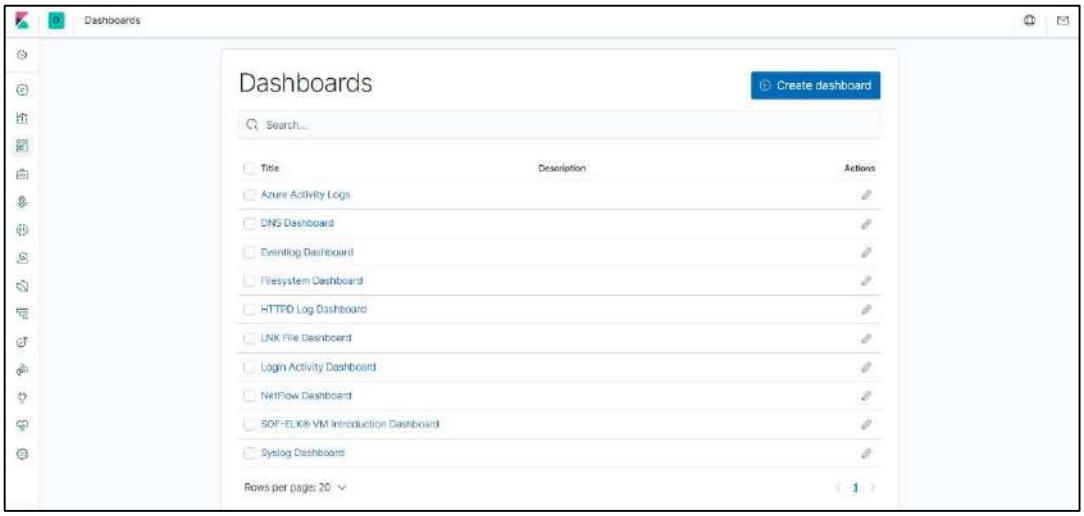
c. Setelah menentukan hal apa yang akan dibutuhkan, selanjutnya pilih *menu dashboard* yang ada. Pada contoh, dipilih *menu* "Sys*log* Program", dimana *menu* ini menampilkan program yang menjalankan sebuah proses yang telah direkam dalam *log*.



3. Pembuatan Dashboard dan Visualisasi

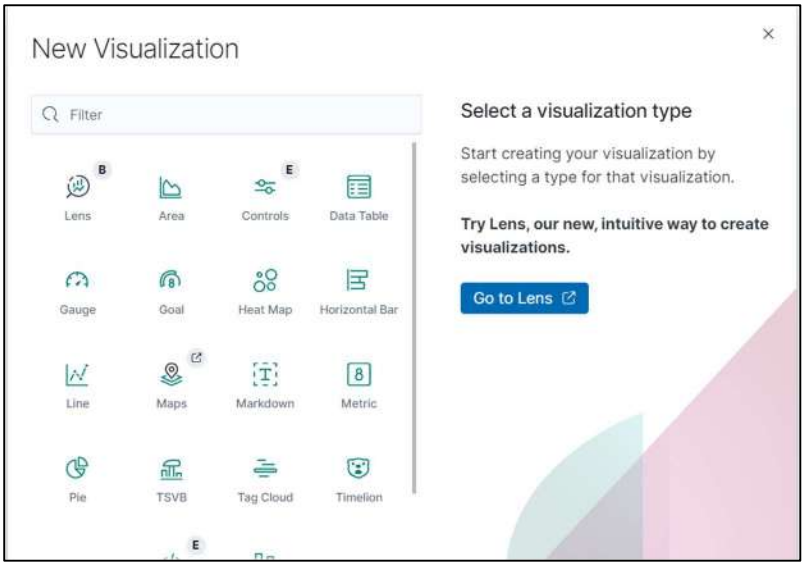
Pembuatan dashboard ini bertujuan ketika pengguna ingin mengatur visualisasi apa saja yang akan diatur dalam dashboard tersebut, maka pengguna hanya perlu menambahkan hal apa saja yang ingin dimasukkan dalam dashboard tersebut.

a. Pembuatan dashboard dapat dilakukan dengan mengklik tab “Create dashboard”.



b. Selanjutnya, buat tampilan sebuah objek baru pada dashboard yang telah dibuat dengan klik tab “Create new”.

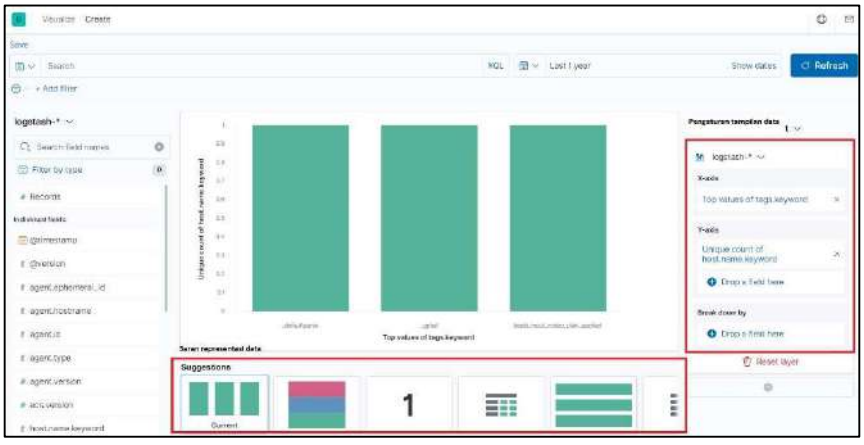
c. Pilih tampilan visualisasi data yang dibutuhkan untuk proses analisis. Pada tahap ini pengguna bebas menggunakan bentuk representasi data apa yang ingin diletakkan pada dashboard yang sedang dibuat.



Dalam pembuatan visualisasi baru, terdapat berbagai macam representasi data yang ada pada visualisasi SOF ELK.

1) Lens

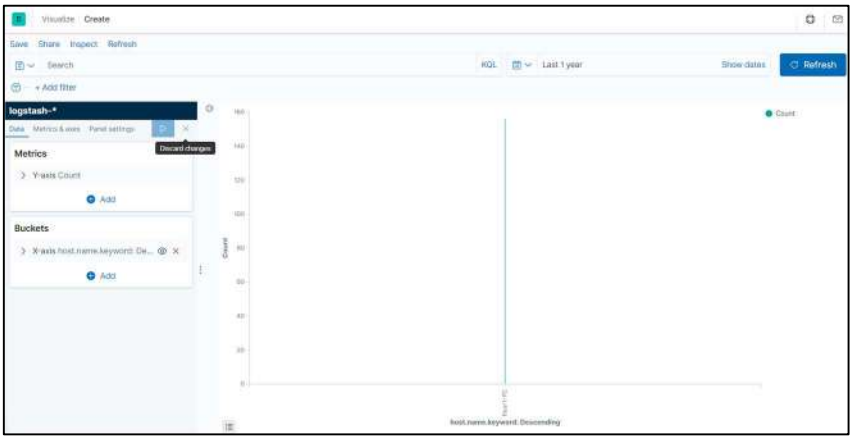
   Visualisasi ini merupakan representasi data yang berisi beberapa tampilan data di dalamnya seperti *bar*, *pie*, *table*, dan sebagainya. Untuk menggunakan visualisasi ini, pengguna dapat mengatur tampilan datanya melalui menu di sebelah kanan, dan juga dapat mengatur sumber *field data* yang ada pada *log* tersebut pada menu di sebelah kiri. Visualisasi ini juga menyediakan representasi data yang disarankan oleh SOF ELK.



2) Area

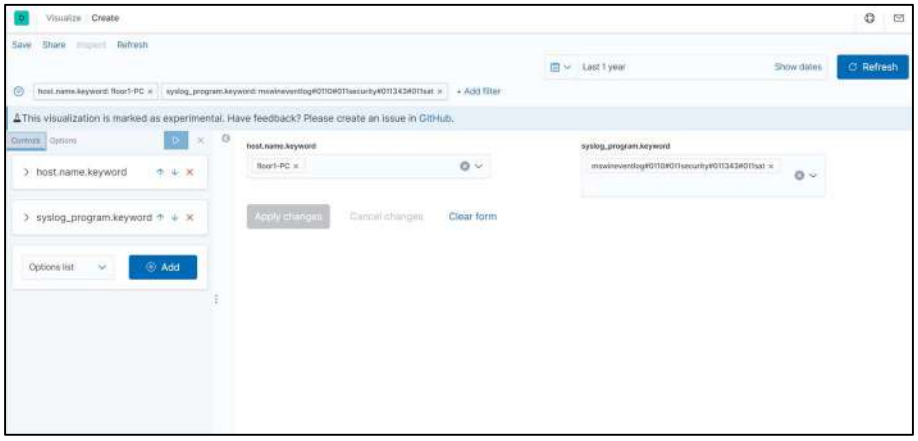
   Visualisasi ini melakukan representasi data dengan diagram garis X dan

Y. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



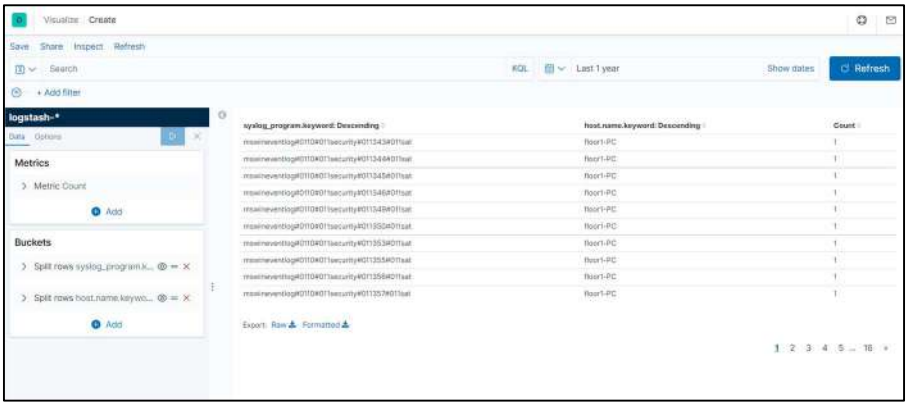
3) Controls

Visualisasi ini berguna untuk membantu pengguna dalam mengatur masukkan *field* pada isi *log* yang telah dipilih, dengan dua metode yaitu menu *dropdown* (menu daftar) dan menu geser. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



4) Data table

Visualisasi ini menampilkan isi data sebuah *log* dalam bentuk tabel yang dapat diatur masukkan *field* datanya. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



5) Gauge

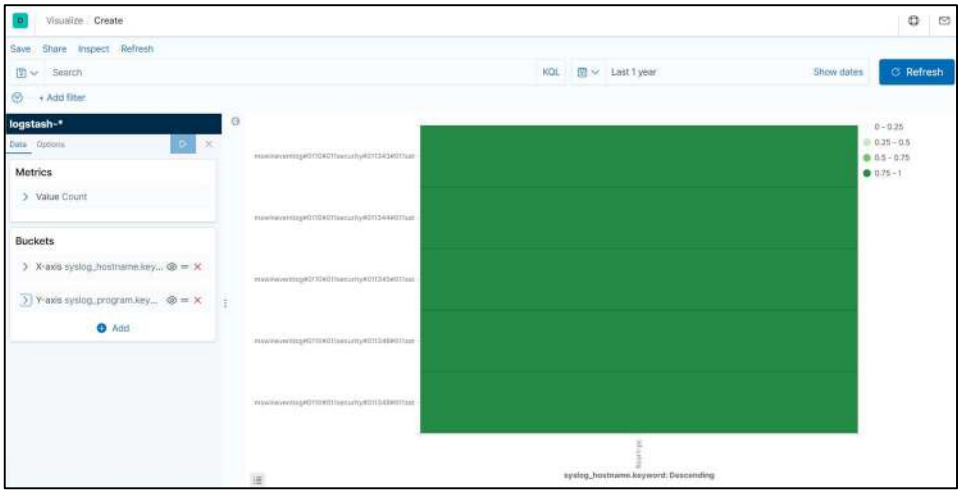
Visualisasi menampilkan status isi *field* pada *log* dalam bentuk pengukur sesuai metriks yang telah ditentukan oleh pengguna. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.

6) Goal

Visualisasi menampilkan status isi *field* pada *log* dengan bentuk capaian sesuai metriks yang telah ditentukan oleh pengguna. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.

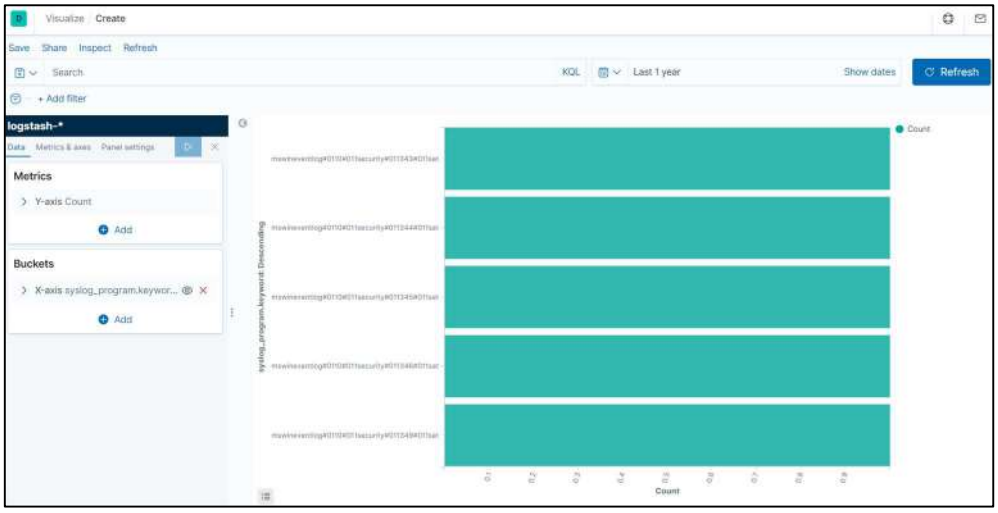
7) Heat Map

Visualisasi ini melakukan representasi data dengan tampilan data dimana nilai *field* yang telah diatur direpresentasikan dengan nilai warna yang ada. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



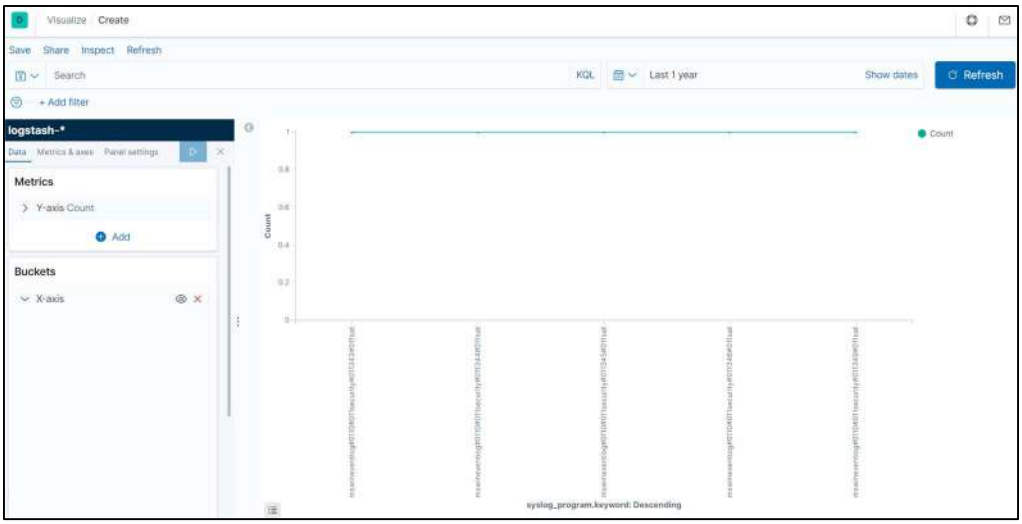
8) Horizontal Bar

Visualisasi ini melakukan representasi data dengan sebuah bentuk tampilan data bar mendatar. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



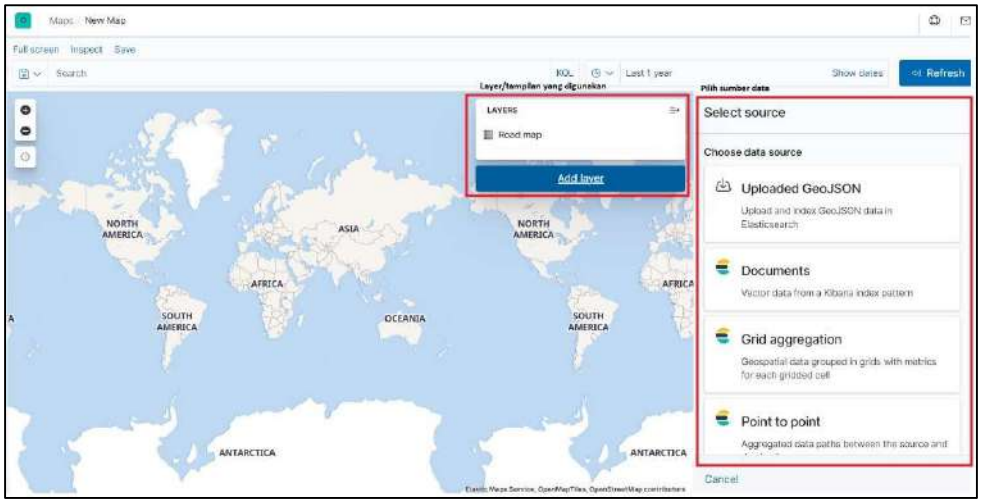
9) Line

Visualisasi ini melakukan representasi data dengan bentuk garis grafik. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



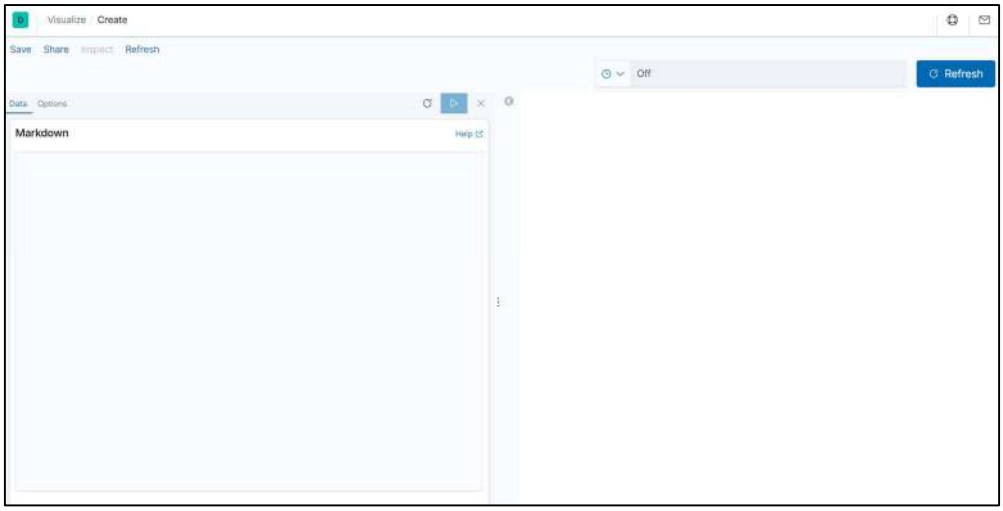
10)Maps

Visualisasi ini melakukan representasi data dengan sebuah tampilan peta. Pengaturan tampilan dan data yang masuk dapat diatur pada menu di sebelah kanan.



11)Markdown

Visualisasi ini digunakan untuk menampilkan informasi mengenai *log* atau hal apapun. Pengguna hanya perlu menuliskan hal apa yang akan disampaikan pada masukkan “Markdown”.

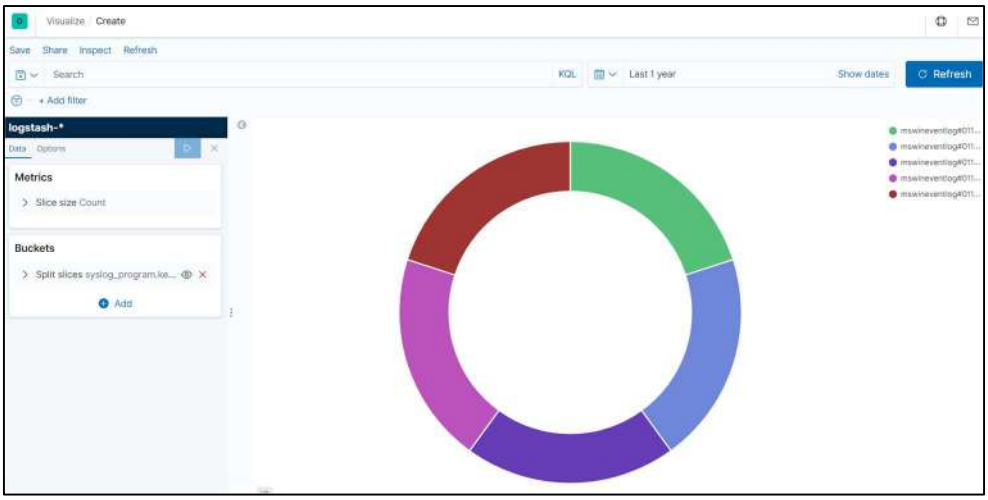


12)Metric

Visualisasi ini melakukan representasi data dengan tampilan sebuah angka dari masukkan *field* yang telah diatur oleh pengguna. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.

13)Pie

Visualisasi ini melakukan representasi data dengan tampilan bentuk *pie chart* atau diagram lingkaran. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.



14)TSVB (*Time Series Visual Builder*)

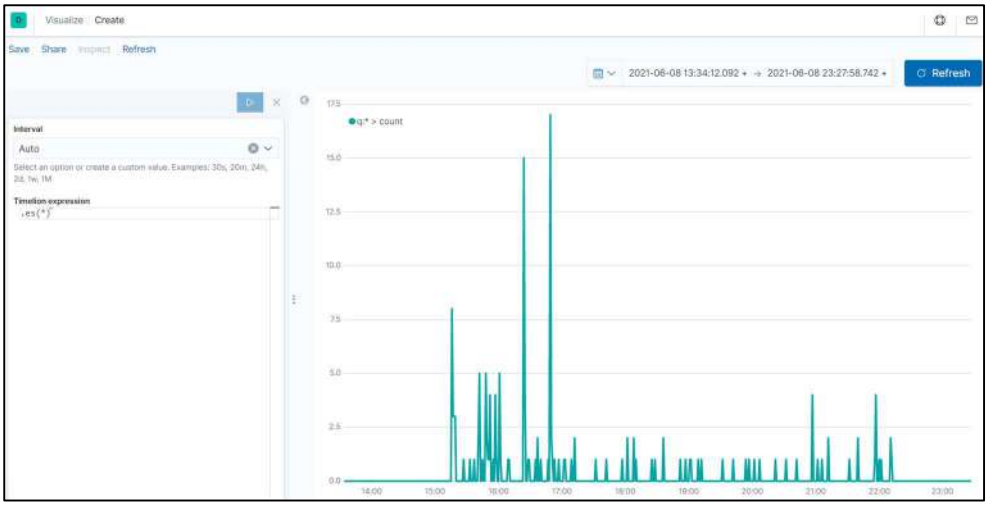
Visualisasi ini melakukan representasi data dengan beberapa gabungan visualisasi data untuk menampilkan data secara utuh kepada pengguna. Tampilan isi *field data* pada *log* yang telah diatur dapat dilihat pada tampilan di sebelah kiri, dan pengaturan data yang masuk dapat diatur pada menu di sebelah bawah tampilan data.

15)Tag Cloud

Visualisasi ini melakukan representasi data dengan tampilan teks sesuai isi dari *field data* pada *log* yang diatur. Tampilan teks ini dapat berbeda bentuknya seiring banyaknya atau pentingya *field data* yang muncul. Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.

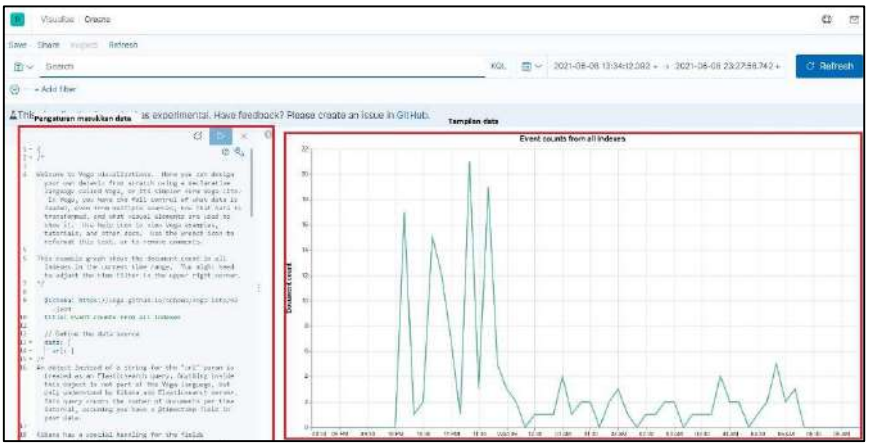
16)Timelion

Visualisasi ini melakukan representasi data dengan tampilan sebuah grafik yang dapat digabungkan dengan isi data lain untuk dibandingkan, sesuai masukkan yang telah diatur oleh pengguna. Pengaturan data dapat diatur sesuai *syntax* pada menu di sebelah kiri.



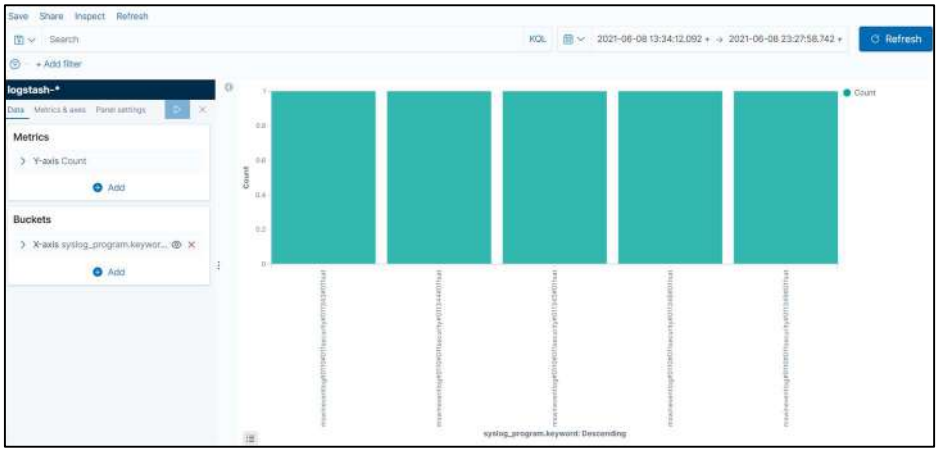
17)Vega

Visualisasi ini melakukan representasi data dengan menggunakan format *syntax* bernama Vega dan Vega-lite. Visualisasi ini menggunakan format JSON untuk menampilkan datanya. Pengaturan data dapat diatur sesuai *syntax* pada menu di sebelah kiri.



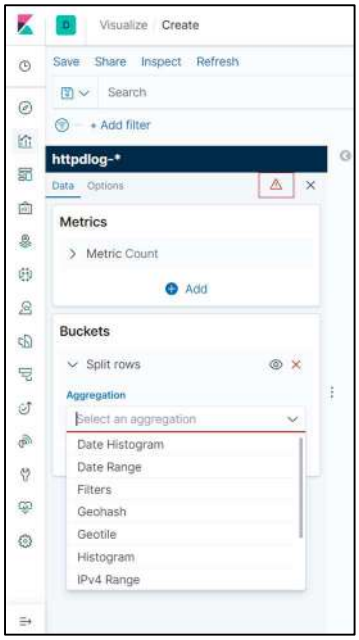
18)Vertical Bar

Visualisasi ini melakukan representasi data dengan sebuah bentuk tampilan data bar keatas (sesuai grafik garis Y). Pengaturan data yang masuk dapat diatur pada menu di sebelah kiri.

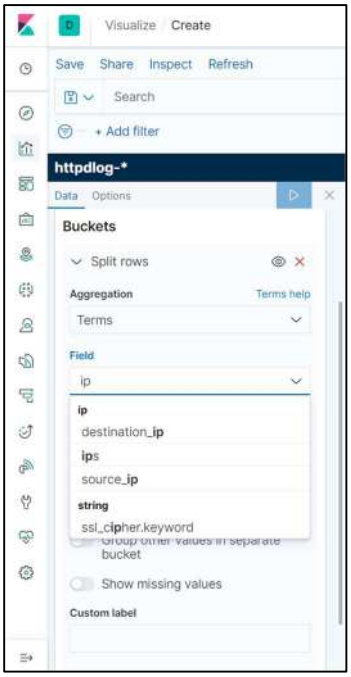


d. Setelah muncul tampilan pembuatan visualisasi data baru, buat tampilan dengan mengaturnya pada tab “Buckets” dan “Metrics” sesuai kebutuhan analisis.

1) Dalam melakukan analisis sebuah *log*, pengguna harus tahu hal apa yang akan dicari untuk dianalisis dan menemukan korelasinya antara *field data* satu dengan yang lain. Untuk membuat visualisasi, dalam hal ini digunakan *log* httpd untuk masukkan data yang akan dipakai.
2) Dalam membuat representasi *field data* pada visualisasi yang akan dibuat pada *log* httpd, pengguna harus menentukan fokus utama dalam hal analisis seperti alamat IP dari penyerang atau yang melakukan akses komunikasi jaringan, kode respon, metode permintaan, serta kapan waktu alamat IP tersebut mengakses.
3) Untuk mencari alamat IP dari sebuah *log*, dapat diatur masukkan data yang ada pada tab “Buckets”. Klik “Add” lalu pilih antara *split rows* atau *split table*. Setelah dipilih, maka tentukan agregasi data yang akan digunakan. Jika ingin memilih agregasi data tepat sesuai isi *field data* yang terdapat pada *log* tersebut, dapat menggunakan agregasi data “**Terms**”.

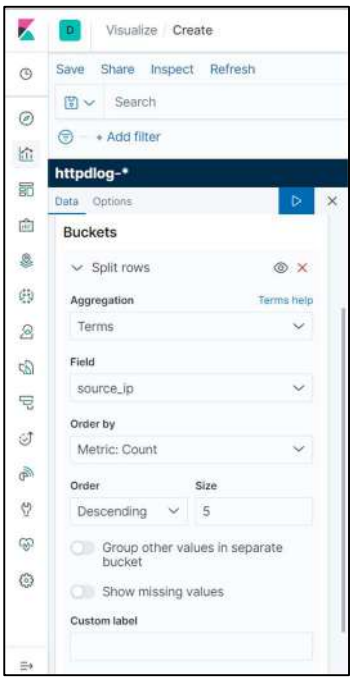


4) Selanjutnya pilih *field data* yang akan ditampilkan. Proses pemilihan *field data* harus dipilih sesuai isi *field* yang ada pada *log* tersebut. Jika ingin menampilkan alamat IP, biasanya *field data* memiliki hubungan kata dengan "ip". Gunakan *field data* sesuai kehendak pengguna dalam melakukan analisis.

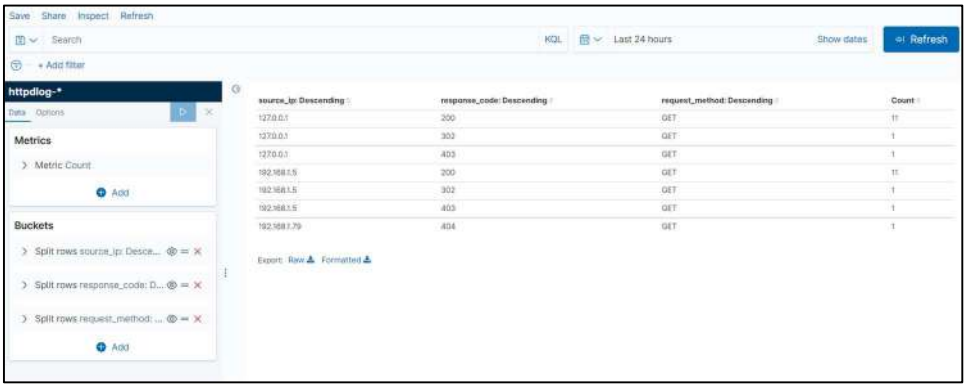


5) Kemudian terdapat pengaturan lanjutan seperti *Order* (urutan) dan *Size* (ukuran) yang akan ditampilkan, pengelompokkan data, penampilan nilai yang hilang, dan penamaan label visualisasi. Atur

sesuai kebutuhan pengguna dalam proses analisis data. Setelah itu klik gambar *icon* biru dengan bentuk segitiga untuk proses penampilan data.



6) Pengguna juga dapat melakukan penambahan “Buckets” lagi untuk mendapatkan korelasi *field data* yang akan ditampilkan di visualisasi. Hal ini bertujuan untuk mempermudah pengguna dalam fokus melakukan analisis sebuah *log*.



e. Setelah selesai membuat visualisasi, kemudian klik “Save” untuk menyimpan. Setelah disimpan, maka akan tampil sebuah visualisasi data yang telah dibuat. Pada dashboard tersebut, pengguna juga dapat menggerakan, memperbesar, dan memperkecil visualisasi data yang telah dibuat untuk mengatur tata letak yang sesuai bagi pengguna dalam

membantu proses analisis.