

ABSTRAK

Vicenzo Artan

Skripsi

Implementasi Monitoring Keamanan Siber dengan Grafana di UK Petra

Tim keamanan siber UK Petra memiliki sebuah *firewall* yang memiliki *Security Operation Center*. Pada SOC, tim dapat melihat aktivitas *firewall* yang sedang terjadi. Namun *dashboard* yang dimiliki oleh SOC Sangfor kurang efisien dikarenakan jika ingin melihat tipe *log* yang berbeda harus berpindah ke halaman lain terlebih dahulu. Selain itu, tampilan *dashboard* SOC Sangfor kurang menarik untuk dilihat. Tim keamanan siber UK Petra sudah mencoba *tools* visualisasi yang bernama Grafana, namun tim hanya baru melakukan pemindahan log, pengelolaan *log*, dan pembuatan *alerting* saja, tanpa adanya satupun grafik.

Untuk mengatasi permasalahan diatas, pada skripsi ini akan diimplementasikan *tools* Grafana. Grafana ini nantinya akan digunakan untuk menampilkan visualisasi dari *log* yang telah di export dari *firewall* NGAF Sangfor. Pada skripsi ini juga akan dilakukan *log rotate* pada *syslog*, dan juga penggunaan Loki Promtail yang berguna untuk mengelola data *log* dari server ke Grafana.

Hasil penelitian menunjukkan bahwa Grafana memang dapat memberikan tampilan visualisasi *dashboard* yang menarik dari sumber data *log firewall* NGAF Sangfor. Tampilan *dashboard* pada Grafana lebih bervariasi daripada *dashboard* yang dimiliki oleh SOC NGAF Sangfor. Namun Grafana masih memiliki kekurangan yaitu tidak memiliki fungsi deduplikasi dan juga Loki kurang mampu untuk menampilkan data dalam jumlah yang besar. Hal itu membuat proses monitoring menjadi kurang bagus, karena tidak bisa melihat hasil data dalam jangka waktu harian, mingguan, bahkan bulanan. Penelitian ini masih jauh dari sempurna dan perlu untuk dilakukan peningkatan lebih lanjut.

Kata Kunci : Pemantauan, Keamanan siber, Grafana, Loki, Promtail

ABSTRACT

Vicenzo Artan

Undergraduate Thesis

Implementation of Cyber Security Monitoring using Grafana at PCU

PCU's cyber security team have a firewall that has a Security Operation Center. Inside the SOC, they can monitoring firewall activities in real time. But, the Sangfor SOC's dashboard is inefficient because if the team want to monitoring different type of log, they must go to another page. Besides that, Sangfor SOC's dashboard is not interesting to see. PCU's cyber security team already try a visualization tools named Grafana, but they just only do log transfer, log query, and creating an alert, without any graphs.

To solve the problem above, in this thesis we will do an implementation of Grafana tools. This Grafana will be used to create a visualization from exported NGAF Sangfor Firewall logs. Also, in this thesis we will do a log rotate to the logs, and using Loki Promtail for querying logs and pushing the logs from server to Grafana.

The results of this research show that Grafana can provide an attractive dashboard visualization display from NGAF Sangfor firewall log data source. The dashboard on Grafana is more varied than NGAF Sangfor SOC's dashboard. However Grafana still has shortcomings, it does not have a deduplication function for syslog and also Loki is less capable of querying large amounts of data. This makes the monitoring process less good because it cannot process and shows the data results over a daily, weekly, or even monthly period. This research still far away from perfect and further improvement is needed

Keyword : Monitoring, Cyber security, Grafana, Loki, Promtail

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	iii
KATA PENGANTAR	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
1. PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan Skripsi.....	2
1.4 Ruang Lingkup.....	2
1.5 Metodologi Penelitian.....	3
1.6 Manfaat Penelitian.....	3
1.7 Sistematika Penulisan.....	4
2. LANDASAN TEORI	5
2.1 Tinjauan Pustaka	5
2.1.1 SIEM.....	5
2.1.2 Grafana.....	5
2.1.3 Sangfor NGAF.....	6
2.1.4 Security Operations Center.....	7
2.1.5 Loki.....	8

2.1.6 Promtail.....	10
2.2 Tinjauan Studi	10
3. ANALISIS DAN DESAIN SISTEM	12
3.1 Analisis Monitoring Keamanan Siber yang Sedang Berjalan	12
3.2 Analisis Permasalahan	12
3.3 Analisis Kebutuhan	12
3.4 Desain Sistem	13
3.4.1 Desain Flowchart Implementasi Sistem	13
3.4.2 Desain Flowchart Implementasi Dashboard Grafana	14
3.4.3 Desain Dashboard Grafana	15
3.4.4 Desain Alerting Grafana	16
4. IMPLEMENTASI SISTEM	17
4.1 Instalasi Grafana	17
4.2 Instalasi Loki dan Promtail	17
4.3 Konfigurasi Rsyslog	18
4.4 Konfigurasi Promtail	19
4.5 Konfigurasi Loki	20
4.6 Konfigurasi Logrotate	21
4.7 Penambahan Data Source Loki	21
4.8 Pembuatan Dashboard Grafana	22
4.8.1 Pembuatan Visualisasi Donut Chart	22
4.8.2 Pembuatan Visualisasi Stat	24
4.8.3 Pembuatan Visualisasi Time Series	25
4.8.4 Pembuatan Visualisasi Bar Chart	26

4.8.5 Pembuatan Visualisasi Table	29
4.8.6 Pembuatan Visualisasi Logs Panel	30
4.9 Konfigurasi Grafana.ini dan Defaults.ini	30
4.10 Pembuatan Alert	31
4.11 Pembuatan Display Dashboard	32
5. HASIL DAN PEMBAHASAN	34
5.1 Pengujian Promtail	34
5.2 Pengujian Loki	35
5.3 Pengujian Grafana	36
5.4 Pengujian Dashboard	38
5.5 Pengujian Alert	40
5.6 Pengujian Logrotate	42
5.7 Uji Komparasi Grafana dan Sangfor	42
6. KESIMPULAN DAN SARAN	46
6.1 Kesimpulan	46
6.2 Saran	46
DAFTAR REFERENSI	47

DAFTAR GAMBAR

2.1 Grafana Alerting	5
2.2 Grafana Dashboard	6
2.3 Log Sangfor NGAF (1)	6
2.4 Log Sangfor NGAF (2)	7
2.5 Sangfor NGAF SOC (1)	7
2.6 Sangfor NGAF SOC (2)	8
2.7 How Loki Works (1)	9
2.8 How Loki Works (2)	9
2.9 Loki Data Source	9
3.1 Desain Flowchart Implementasi Sistem	14
3.2 Desain Flowchart Implementasi Dashboard Grafana	15
3.3 Ilustrasi Tampilan Dashboard Grafana	15
3.4 Ilustrasi Alerting Email	16
3.5 Contoh Alerting Integration	16
4.1 Data Source Loki	21
4.2 Halaman Explore	22
4.3 Query Donut Chart	23
4.4 Transform Donut Chart	23
4.5 Donut Chart (IPS)	23
4.6 Donut Chart (WAF)	24
4.7 Query Stat	24

4.8 Color Scheme	25
4.9 Stat (IPS)	25
4.10 Stat (WAF)	25
4.11 Query Time Series	25
4.12 Time Series (IPS)	26
4.13 Time Series (WAF)	26
4.14 Query Parsing Log Bar Chart	26
4.15 Transformation Bar Chart (1)	27
4.16 Transformation Bar Chart (2)	27
4.17 Transformation Bar Chart (3)	27
4.18 Bar Chart Vulnerabilities (IPS)	28
4.19 Bar Chart Threats (IPS)	28
4.20 Bar Chart IP (IPS)	28
4.21 Bar Chart Threats (WAF)	28
4.22 Bar Chart URL (WAF)	28
4.23 Query Parsing Log Table	29
4.24 Transformation Table	29
4.25 Table (IPS)	29
4.26 Table (WAF)	30
4.27 Query Log	30
4.28 Logs Panel (IPS)	30
4.29 Logs Panel (WAF)	30
4.30 SMTP Configuration	31
4.31 Server Configuration Grafana.ini and Defaults.ini	31

4.32 Alert Rule Grafana	32
4.33 Contact Point Alert	32
4.34 Pembuatan Display Dashboard	33
5.1 Promtail 9080	34
5.2 Promtail Explore	34
5.3 Loki 3100	35
5.4 Loki Explore	35
5.5 Grafana 3000	36
5.6 Profile Grafana	36
5.7 Explore Grafana	37
5.8 Alerting Grafana	37
5.9 Connections Grafana	37
5.10 Administration Grafana	38
5.11 Dashboard Grafana IPS	38
5.12 Dashboard Grafana WAF	39
5.13 Dashboard Grafana Alert List	39
5.14 Display Dashboard Grafana	40
5.15 Alert in Normal State	40
5.16 Alert in Pending State	41
5.17 Alert in Firing State	41
5.18 Log Result when Alerting	41
5.19 Table Result when Alerting	41
5.20 Email Alert Notification	42
5.21 Hasil Logrotate	42

5.22 Grafana Dashboard (1)	43
5.23 Grafana Dashboard (2)	43
5.24 SOC Dashboard 1	43
5.25 Grafana Dashboard 1	43
5.26 Grafana Dashboard 2	44
5.27 SOC Dashboard 2	44
5.28 SOC Dashboard 3	44
5.29 Grafana Dashboard 3	44
5.30 Grafana Dashboard 4	44
5.31 SOC Dashboard 4	45
5.32 Grafana Dashboard 5	45