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

DAFTAR GAMBAR