UNIVERSITAS
GADJAH MADA
Enrichment dan Monitoring Log DNS Server Berbasis Elasticsearch Logstash Kibana (ELK Stack)
HILYA QOTHRUN N, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

PROYEK AKHIR

ENRICHMENT DAN *MONITORING* LOG *SERVER* DNS BERBASIS ELASTICSEARCH LOGSTASH KIBANA (ELK STACK)

DNS merupakan bagian yang penting dalam internet, sehingga masalah keamanan DNS menjadi sangat penting untuk diperhatikan. Serangan DNS dapat diantisipasi dengan melakukan analisis data log. Log merupakan *file* yang berisi catatan kejadian yang terjadi pada sebuah sistem, maka dengan memanfaatkan data log dapat mencegah dan mengidentifikasi aktivitas berbahaya yang mungkin terjadi pada sebuah sistem. Memperkaya data dengan menggunakan informasi relevan dapat menjadikan sebuah data lebih bernilai. Pada penelitian ini, mekanisme *enrichment* akan dilakukan untuk membangun sebuah sistem *monitoring* terhadap data log DNS. Sistem dirancang agar mampu mengolah data log dan menganalisis log dalam bentuk visual. Perancangan sistem dilakukan dengan menggunakan ELK Stack sebagai komponen pengelola log *service* dan *IP Profile database* sebagai *third-party data sources*. *Enriching* dan *monitoring* terhadap data log dilakukan untuk memudahkan admin dalam mengetahui kemungkinan adanya aktivitas berbahaya, sehingga dapat mengatisipasi terjadinya serangan atau aktivitas merugikan lainnya.

Kata Kunci: Log, DNS *Server*, *Data Log Enrichment, Monitoring Server*, ELK Stack.

UNIVERSITAS
GADJAH MADA
Enrichment dan Monitoring Log DNS Server Berbasis Elasticsearch Logstash Kibana (ELK Stack)
HILYA QOTHRUN N, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

ENRICHMENT AND MONITORING DNS SERVER LOG BASED ON ELASTICSEARCH LOGSTASH KIBANA (ELK STACK)

DNS is an important part of the internet; therefore, DNS security is crucial issues that must be considered. DNS attacks can be carried out by performing log data analysis. Logs are file which contain records of events that occurred on a system, therefore by utilizing log data can prevent and identify dangerous activities that may occur on a system. Enriching data by using relevant information can make data more proper. In this study, an enrichment mechanism will be used to build a monitoring system for DNS log data. The system is designed to be able processing log data and analyzing logs in a visual appearance. The system design is carried out using the ELK Stack as a service log management component and the IP Profile database as a third-party data source. Enrichment and monitoring of log data are used to make it easier for admins to find out the possibility of malicious activity, therefore they can anticipate attacks or other dangers on the system.

Keyword: Log, DNS Server, Data Log Enrichment, Monitoring Server, ELK Stack.