ANALISIS *LOG* SISTEM PADA *SECURITY INFORMATION AND EVENT MANAGEMENT* UNTUK MENDETEKSI DATA *EXFILTRATION*

Tiara Sakinah

1810511031

Abstrak

Teknologi sangat erat kaitannya dengan data. Keberadaan teknologi adalah untuk menyampaikan kumpulan informasi dengan mudah dan efisien. Setiap individu maupun organisasi bertukar informasi dengan tujuan tertentu, dan banyak dari informasi tersebut yang memiliki tingkat keamanan yang tinggi. Pentingnya pengawasan pada setiap informasi merupakan aturan yang tidak bisa dilewatkan oleh setiap individu maupun organisasi. Kurangnya *awareness* pada keamanan data memancing kejahatan dengan mencuri data tersebut atau biasa disebut *data exfiltration.* Untuk mengatasi hal tersebut diatas, penulis menggunakan *Security Information and Event Management* atau disingkat SIEM. SIEM merupakan metode untuk mengumpulkan, menganalisa, memberi *alert* memberi laporan, serta melakukan automatisasi respon pada sebuah insiden. Penelitian ini diharapkan dapat menjabarkan hasil pengujian dan analisis serta memberikan rekomendasi solusi yang dapat dilakukan untuk mengatasi *data exfiltration* pada SIEM.

Kata kunci: ***Sistem log, Security Information and Event Management, Data exfiltration***

ANALISIS *LOG* SISTEM PADA *SECURITY INFORMATION AND EVENT MANAGEMENT* UNTUK MENDETEKSI DATA *EXFILTRATION*

Tiara Sakinah

1810511031

Abstract

Technology is closely related to data. The existence of technology is to convey a collection of information easily and efficiently. Each individual or organization exchanges information for a specific purpose, and much of that information has a high level of security. The importance of monitoring every piece of information is a rule that can not be missed by every individual or organization. Lack of *awareness* on data security provokes crime by stealing such data or commonly called *xfiltration data.* To overcome the above, the author uses *Security Information and Event Management* or abbreviated siem. SIEM is a method of collecting, analyzing, alerting ports, and automating responses to an incident. This research is expected toexpand the results of testing and analysis and provide recommendations for solutions that can be done to overcome *exfiltration data* in SIEM.

Kata kunci: ***Sistem log, Security Information and Event Management, Data exfiltration***