BAB V
PENUTUP

5.1.KESIMPULAN

Setelah dilakukan penelitian mengenai pendeteksian data eksfiltasi menggunakan *Security Information and Event Management* (SIEM) dengan menggunakan *log* sistem pada dua buah sistem operasi, dapat disimpulkan bahwa.

1. Cara mengetahui sistem yang mengalami data eksfiltrasi adalah dengan melakukan pemantauan pada sistem tersebut secara berkala dan memperhatikan ciri-ciri terjadinya data eksfiltrasi.
2. Melalui penelitian ini SIEM yang digunakan hanya dapat mendeteksi ciri-ciri dari data eksfiltrasi seperti perubahan data, terjadinya *control and command*, melalui eksekusi virus, dan pemasangan perangkat keras. Terbukti dari penelitian ini bahwa dari 3 percobaan hanya ada 1 yang dapat memastikan terjadinya eksfiltrasi data. Kegiatan menganalisa dilakukan oleh penulis dikarenakan SIEM hanya dapat menangkap ciri-ciri dari data eksfiltrasi.
3. SIEM dapat membantu organisasi termasuk Organisasi Kecil untuk mengatasi kejahatan siber dengan melakukan pemantauan secara berkala pada melalui SIEM yang sudah terkonfigurasi sesuai dengan kebutuhan, mendalami pengetahuan seputar data eksfiltrasi dan system operasi. SIEM yang digunakan penulis dalam penelitian merupakan SIEM yang *open-source* dan tetap memiliki kemampuan dalam pengawasan termasuk pada organisasi dengan investasi infrastruktur jaringan dengan biaya yang rendah. Jika dibandingkan dengan SIEM lain Wazuh memiliki kapabilitas untuk melakukan pemantauan bukan hanya untuk eksfiltrasi data melainkan hal lain.

5.2.SARAN

Berdasarkan penelitian solusi untuk mengatasi data eksfiltrasi adalah melakukan pemantauan kepada sistem secara berkala, memperhatikan ciri-ciri dari eksfiltrasi data pada proses monitoring, memberi konfigurasi kepada SIEM sesuai dengan studi kasus yaitu eksfiltrasi data, dan meningkatkan pengetahuan mengenai data eksfiltrasi.

Saran penulis untuk penelitian selanjutnya adalah memaksimalkan penggunaan tools SIEM yang digunakan, berikan konfigurasi tambahan untuk meghilangkan false positif sehingga proses pemantauan menjadi maksimal.