BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Bedasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan bahwa telah terjadi peningkatan efektifitas pengelolaan keaamaanan informasi khusunya di bidang digital pada Universitas Komputer Indonesia. Sistem SIEM mampu membuat, mengumpulkan, menyimpan, menganalisis, serta memberikan respon terhadap security event yang terjadi di lingkungan UNIKOM. Salah satu security event yang berhasil dibuat, dikumpulkan, disimpan, dianalisis, dan diberikan reponnse adalah security event yang berkaitan dengan bruteforce.

Kemampuan sistem SIEM dalam mengumpulkan, menyimpan, manganalisis, serta memberikan respon terhadap security event yang terjadi sudah memenuhi operasi-operasi apa saja yang harus ada pada sebuah SOC. Oleh karena itu dapat dikatakan juga bahwa dengan mengimplementasikan sistem SIEM menggunakan tools Wazuh, UNIKOM saat ini memiliki sebuah SOC. Hal ini juga didukung dengan intergrasi dengan sistem DFIR menggunakan toos IRIS yang memudahkan kolaborasi antara personel yang berkerja mempertahankan keamanan di UNIKOM.

5.2 Saran

Bedasasrkan hasil kesimpulan diatas, penulis memberikan saran untuk perbaikan dan pengembangan lebih lanjut terkait implementasi SIEM di lingkungan UNIKOM yaitu dengan mengintergrasikannya dengan sistem SOAR (Security Orcrhestration, Automatioin, and Response) untuk meningkatkan kemampuan incident response dan threat management. Setelah diintergrasikan oleh sistem SOAR, sistem SIEM dapat juga di intergrasikan dengan sistem Threat Sharing agar UNIKOM tidak kentinggalan tentang informasi mengenai cybersecurity yang terjadi disekitar. Dengan mengintergrasikan sistem Thrert Sharing, diharapkan nantinya UNIKOM akan berkerja dengan organisasi lain baik swasta atupun pemerintah dalah membagikan informasi mengenai cybersecurity.

Selain kedua hal tersebut, penulis juga menyarankan untuk melatih pegawai-pegawai yang telah termasuk kedalam tim CSIRT UNIKOM agar tim CSIRT UNIKOM dapat berjalan sehingga tercipta kolaborasi antara teknologi, manusia, dan proses.