

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari penelitian diatas, peneliti menyimpulkan bahwa penelitian ini dapat diambil beberapa kesimpulan yaitu;

1. Wazuh SIEM dapat mempermudah monitoring karena terintegrasi dengan bot telegram secara real-time.
2. Dengan adanya wazuh SIEM dapat meningkatkan keamanan jaringan perusahaan dilihat dari jumlah akhir skor skala likert yang bernilai 81,5% (Sangat setuju) yang didapatkan dari responden.
3. Untuk serangan yang diuji mendapatkan nilai level rules yang besar, hal ini menandakan serangan SQL injection, brute force, dan DDoS adalah serangan yang berbahaya bagi keamanan jaringan.

5.2 Saran

Sebagai penutup penelitian skripsi ini, peneliti berharap semoga apa yang peneliti sajikan dapat memberikan banyak manfaat bagi pembaca dan peneliti. Peneliti menyadari bahwa skripsi ini yang berjudul Implementasi Security Information and Event Managemet (SIEM) Berbasis wazuh dengan notifikasi Telegram masih memiliki kekurangan, oleh karena itu saran yang bisa peneliti berikan diantaranya adalah;

1. Penelitian ini mengimplementasi wazuh hanya sebagai SIEM hanya untuk mendeteksi serangan SQL injection, brute force, dan DDoS dengan konfigurasi standar. Untuk penelitian selanjutnya dapat menggunakan wazuh untuk mitigasi secara langsung.
2. Penelitian ini menggunakan bot telegram untuk mengirimkan notifikasi seranagan. Untuk penelitian selanjutnya bisa mencoba dengan mengintegrasikan line, sms, email dan lain-lainya.
3. Penelitian ini hanya melakukan pengujian serangan tanpa adanya penyembuhan untuk sistem yang diujikan. Untuk penelitian berikutnya dapat melakukan upaya penyembuhan agar penelitian lebih baik.