BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai penerapan dan analisis kinerja *File Integrity Monitoring* (FIM) berbasis Wazuh SIEM pada server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur, maka dapat disimpulkan sebagai berikut:

1. Penerapan File Integrity Monitoring (FIM) berbasis Wazuh SIEM berhasil diimplementasikan pada tiga server Fakultas Ilmu Komputer, yaitu Server Sarpras, Server Satu, dan Server Utama. Implementasi dilakukan melalui instalasi Wazuh Server sebagai pusat monitoring, pemasangan Wazuh Agent pada masing-masing server target, konfigurasi modul File Integrity Monitoring, serta integrasi komunikasi agent-server menggunakan authentication key. Hasil implementasi menunjukkan bahwa seluruh agent berhasil terhubung secara aktif pada Wazuh Dashboard dan sistem mampu melakukan pemantauan perubahan file kritikal secara terpusat sesuai dengan rancangan penelitian.

2. Kinerja FIM berbasis Wazuh menunjukkan hasil yang efektif dalam mendeteksi perubahan file tanpa otorisasi ditinjau dari aspek waktu deteksi, akurasi, dan efisiensi sistem. Berdasarkan hasil pengujian berulang sebanyak 10 kali pada masing-masing skenario pengujian di tiga server, sistem mampu mendeteksi aktivitas penambahan, modifikasi, dan penghapusan file secara real-time dengan rata-rata waktu deteksi 1,2 hingga 1,9 detik serta tingkat akurasi deteksi sebesar 100%. Selain itu, proses monitoring berjalan tanpa memberikan beban signifikan terhadap performa server sehingga sistem dinilai efisien dan layak diterapkan sebagai mekanisme monitoring integritas file pada lingkungan server institusi. Penerapan metode PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) juga membantu proses implementasi dan evaluasi sistem berjalan secara terstruktur mulai dari tahap perencanaan hingga optimasi keamanan server.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk pengembangan sistem maupun penelitian selanjutnya, yaitu sebagai berikut:

1. Sistem File Integrity Monitoring berbasis Wazuh yang telah diimplementasikan perlu dikembangkan menjadi arsitektur keamanan berlapis (layered defense) agar perlindungan server tidak hanya berfokus pada integritas file, tetapi juga mencakup deteksi aktivitas jaringan, analisis log keamanan, serta respons otomatis terhadap ancaman.
2. Integrasi Wazuh dengan layanan proteksi eksternal seperti Cloudflare perlu dipertahankan dan dioptimalkan, karena kombinasi antara monitoring internal server dan filtering trafik eksternal dapat memberikan mekanisme pertahanan yang lebih menyeluruh terhadap serangan siber, baik dari sisi host maupun sisi jaringan web.
3. Penelitian selanjutnya disarankan untuk melakukan pengembangan pada aspek evaluasi performa keamanan secara lebih luas, seperti pengujian korelasi alert multi-serangan, analisis beban sistem saat monitoring berjalan, serta penerapan active response agar sistem tidak hanya mampu mendeteksi, tetapi juga memberikan tindakan mitigasi secara otomatis.