BAB V KESIMPULAN

A. Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan pembahasan yang telah dilakukan pada bab sebelumnya, dapat disimpulkan sebagai berikut:

1. Prototipe *Security Operations Center* dirancang dan dibangun melalui integrasi berbagai perangkat lunak *open source*, yang mencakup Wazuh sebagai *Intrusion Detection System (IDS), Endpoint Detection and Response (EDR),* serta *Intrusion Prevention System (IPS),* Suricata sebagai *Network Intrusion Detection System (NIDS),* VirusTotal sebagai *Extended Detection and Response (XDR),* MISP sebagai sumber *threat intelligence*, Graylog sebagai *centralized log management*, serta Telegram dan *email* sebagai media notifikasi. Seluruh komponen tersebut diintegrasikan untuk mendukung fungsi utama SOC, yaitu *monitoring*, pengumpulan *log*, deteksi ancaman, *threat intelligence*, dan respons insiden secara terpusat, sehingga prototipe tersebut dapat dikatakan berhasil dikembangkan.
2. Implementasi dan pengujian prototipe SOC dilakukan melalui berbagai skenario, meliputi *File Integrity Monitoring (FIM)*, *Directory Monitoring*, Docker *Monitoring*, *Active Response, Block Malicious Actor, Monitoring Resource Usage, Anomaly Detection*, Anti *Malware*, *Threat Intelligence*, serta skenario serangan berdasarkan OWASP Top 10 dan MITRE ATT&CK. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi berbagai aktivitas dan ancaman keamanan dengan tingkat akurasi yang tinggi serta menjalankan respons otomatis melalui mekanisme *active response,* sehingga prototipe tersebut dapat dinyatakan berhasil dalam mendukung proses deteksi dan respons ancaman siber secara efektif.

B. Saran/Rekomendasi

Mengingat proses penanganan insiden keamanan pada penelitian ini masih memiliki keterbatasan dalam hal otomatisasi yang belum berjalan secara *end-to-end,* sehingga pada beberapa tahapan kritis masih diperlukan intervensi manual, maka disarankan pengembangan penelitian lebih lanjut sebagai berikut:

1. Mengimplementasikan platform *Security Orchestration, Automation, and Response (SOAR)* dan DFIR-IRIS untuk meningkatkan kemampuan otomatisasi dalam proses investigasi serta respons insiden keamanan.