ABSTRAK

Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis efektivitas implementasi *Security Information and Event Management* (SIEM) *open-source* menggunakan Elastic Security dalam mendeteksi ancaman siber yang semakin kompleks. Fokus utama penelitian ini adalah pada pengintegrasian *Threat Intelligence* dan *Threat Behavior* untuk meningkatkan kapabilitas deteksi ancaman pada SIEM. Elastic Security digunakan dalam penelitian ini untuk mengelola dan menganalisis data log yang dihasilkan oleh sistem dan aplikasi yang terhubung ke jaringan organisasi.

Penelitian ini dilakukan melalui serangkaian eksperimen yang melibatkan berbagai jenis serangan siber, termasuk *port scanning*, *brute force*, dan *Distributed Denial of Service* (DDoS). Eksperimen dilakukan dalam lingkungan virtual yang telah dikonfigurasi dengan menggunakan VMware untuk mensimulasikan *server* target (CentOS) dan mesin penyerang (Kali Linux). Dalam setiap eksperimen, metode yang digunakan melibatkan analisis terhadap *log* yang dihasilkan oleh Elastic Security untuk mengevaluasi efektivitas deteksi dan respon terhadap serangan.

Hasil penelitian menunjukkan bahwa Elastic Security mampu mendeteksi sebagian besar jenis serangan dengan akurasi tinggi, terutama pada serangan *port scanning* dan *brute force*, dengan waktu respons yang bervariasi.Serangan Nmap - Zenmap GUI (Intense Scan, All TCP) terdeteksi paling cepat dalam 15 detik, sementara serangan Nmap - Zenmap GUI (Intense Scan plus UDP) terdeteksi paling lambat dalam 9 menit 41 detik. Namun, terdapat kelemahan dalam mendeteksi serangan DDoS dan serangan brute force yang dilakukan dengan alat Medusa, yang tidak terdeteksi sama sekali, menunjukkan kebutuhan akan peningkatan dalam konfigurasi dan aturan deteksi. Selain itu, metrik *risk* menunjukkan bahwa *Nping Process Activity* yang digunakan untuk mendeteksi *DDoS Attack* dan *Potential Internal Linux SSH Brute Force* yang digunakan untuk mendeteksi *Brute Forece Attack* memiliki skor risiko tertinggi sebesar 47 dengan tingkat *severity medium*, sementara potensi deteksi port scanning memiliki skor risiko 21 dengan tingkat *severity low*.

Elastic Security efektif dalam mendeteksi serangan *port scanning* dan *brute force*, namun menunjukkan kelemahan dalam mendeteksi serangan DDoS dan *brute force* menggunakan Medusa. Skor risiko tertinggi ditemukan pada *Nping Process Activity* dan *Potential Internal Linux SSH Brute Force*. Untuk meningkatkan efektivitas, perlu dilakukan peningkatan konfigurasi, aturan deteksi, serta integrasi yang lebih baik dengan *Threat Intelligence* dan *Behavior Profiling*.
Kata kunci **— Elastic Security, SIEM, Threat Intelligence, Behavior Profiling, Deteksi Ancaman.**