1. Pendahuluan

Latar Belakang

Serangan DDoS merupakan ancaman signifikan yang menargetkan kinerja *Central Processing Unit* (CPU) dan memori *server* dengan mendistribusikan *Denial of Service* (DoS) yang terkoordinasi [18]. Serangan semacam ini dapat mengganggu lalu lintas jaringan yang sah, yang pada gilirannya mempengaruhi ketersediaan layanan [19]. Meskipun alat keamanan tradisional seperti IDS dan IPS [8] telah digunakan dalam organisasi, mereka cenderung hanya memberikan peringatan [6], dan sering kali memerlukan intervensi manual, yang dapat menyebabkan potensi kesalahan dan penundaan.

Topik dan Batasannya

Pendekatan untuk mengatasi tantangan ini melalui *Security Orchestration, Automation, and Response* (SOAR) telah menjadi fokus perhatian. SOAR memungkinkan otomatisasi proses melalui panduan yang telah ditetapkan sebelumnya, mengurangi upaya manual, dan meningkatkan waktu respons [14]. Pendekatan ini melibatkan integrasi antara alat seperti IDS dan SIEM, di mana SIEM mengelola log serangan siber, terutama yang berasal dari IDS [12]. Menerapkan sistem multi-agen dengan *agent* SIEM dan IDS di setiap server dianggap sebagai langkah yang komprehensif dalam pertahanan [15] terhadap serangan DDoS. Mengingat potensi volume peringatan yang cukup besar yang dihasilkan oleh IDS [13] dan kemungkinan memicu peringatan meskipun tanpa adanya aktivitas berbahaya [2], verifikasi peringatan otomatis menjadi penting untuk meminimalkan *false positive* [13].

Tujuan

Tujuan dari penelitian ini adalah untuk mengembangkan sistem *multi-agent* secara *real-time* menggunakan alat keamanan *open-source*, yang mengintegrasikan IDS, SIEM, dan SOAR. Sistem ini akan bertugas untuk mendeteksi, memverifikasi, mencegah, dan memberikan notifikasi terhadap serangan DDoS. Evaluasi kinerja sistem akan dilakukan dengan mempertimbangkan presisi dan performa, dengan tujuan mengoptimalkan akurasi pemblokiran IP dan efisiensi sistem secara keseluruhan.

Organisasi Tulisan

Jurnal ini terdiri dari lima bagian utama. Bagian pertama adalah pendahuluan, di mana akan dibahas latar belakang dari masalah yang dihadapi, topik dan batasannya, serta tujuan penelitian. Bagian studi terkait akan mengulas beberapa penelitian dari jurnal-jurnal yang relevan, yang menjadi dasar untuk memilih sistem yang akan dikembangkan dalam jurnal ini. Sisem yang dibangun akan dijelaskan secara rinci, diikuti dengan bagain evaluasi yang mencakup skenario pengujian serta analisis hasilnya. Bagian terakhir, yaitu kesimpulan, akan merangkum temuan dari evaluasi dan menawarkan pandangan tentang pengembangan masa depan.