BAB I PENDAHULUAN

A. Latar Belakang

Serangan siber tidak lagi menjadi ancaman yang bersifat potensial, melainkan telah menjadi realitas yang dihadapi hampir setiap institusi. Berbagai organisasi, mulai dari instansi pemerintahan, lembaga pendidikan, hingga pelaku usaha kecil dan menengah (UKM), kini bergantung pada sistem digital dalam menjalankan operasionalnya. Kondisi ini secara tidak langsung memperluas permukaan serangan *(attack surface)* yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengeksploitasi kerentanan sistem[1].

Dalam perspektif keilmuan teknologi informasi, khususnya pada bidang keamanan siber, peningkatan intensitas dan kompleksitas serangan ini menuntut adanya mekanisme pertahanan yang tidak hanya bersifat reaktif, tetapi juga proaktif. Serangan siber modern cenderung dilakukan secara terorganisasi, menggunakan teknik yang semakin canggih, serta memiliki tujuan yang beragam, mulai dari pencurian data hingga gangguan layanan. Oleh karena itu, diperlukan suatu pendekatan yang mampu mengintegrasikan proses deteksi, analisis, dan respons ancaman secara efektif dan berkelanjutan[2].

Kerugian akibat ancaman siber tidak hanya terbatas pada kerusakan infrastruktur teknologi, tetapi juga dapat melumpuhkan operasional, merusak reputasi organisasi, bahkan bisa menimbulkan kerugian ekonomi. Hal ini diperkuat dengan laporan *IBM Cost of a Data Breach Report* tahun 2024, yang menunjukkan rata-rata kerugian yang dialami oleh organisasi akibat satu insiden kebocoran data mencapai 4,9 juta USD, jumlah ini meningkat sebesar 10% dari tahun sebelumnya dan menjadikan angka tertinggi yang tercatat[3]. Data ini menegaskan bahwa ancaman siber bukan hanya isu teknis, melainkan juga risiko strategis yang dapat memengaruhi keberlangsungan organisasi.

Dalam menghadapi ancaman siber yang semakin kompleks dan sulit diprediksi, keberadaan *Security Operations Center* (SOC) menjadi kebutuhan yang tidak dapat diabaikan, karena berfungsi sebagai pusat terintegrasi yang mampu melakukan pemantauan, deteksi, analisis, hingga respons terhadap insiden keamanan secara berkelanjutan, sehingga organisasi dapat mengidentifikasi ancaman lebih cepat sebelum berkembang menjadi serangan yang merugikan. Namun di sisi lain, penerapan SOC secara konvensional masih menjadi tantangan besar, terutama karena tingginya biaya investasi yang harus dikeluarkan, mulai dari pengadaan infrastruktur perangkat keras, lisensi perangkat lunak, hingga kebutuhan sumber daya manusia yang memiliki keahlian khusus di bidang keamanan siber[4].

Kondisi ini menimbulkan kesenjangan yang cukup signifikan, di mana institusi dengan keterbatasan anggaran seperti sekolah, perguruan tinggi, dan organisasi publik berskala kecil tetap berada dalam posisi rentan terhadap serangan siber, tetapi belum memiliki kemampuan yang memadai untuk membangun sistem pertahanan yang optimal.

Tingginya biaya investasi justru membuka ruang bagi lahirnya solusi yang lebih inovatif. Kemajuan teknologi serta dukungan komunitas *open source* memungkinkan pengembangan sistem SOC yang andal melalui pendekatan integrasi *software* berbasis *open source*. Saat ini, tersedia beragam *software open source* yang terbukti mampu menjalankan fungsi utama SOC secara efektif dan fleksibel [5], [6]. Pemanfaatan ekosistem teknologi *open source* menjadi faktor penting dalam mewujudkan keamanan siber yang lebih terjangkau, sehingga organisasi yang sebelumnya terkendala biaya dapat menerapkan sistem keamanan yang memadai.

Oleh karena itu, penulis mengambil topik penelitian "PROTOTIPE *SECURITY OPERATIONS CENTER* BERBASIS INTEGRASI *SOFTWARE OPEN SOURCE* UNTUK OPTIMASI DETEKSI DAN RESPONS ANCAMAN SIBER" sebagai tugas akhir. Penelitian ini difokuskan pada evaluasi prototipe *Security Operations Center (SOC)* berbasis integrasi perangkat lunak *open source* untuk deteksi dan respons ancaman siber secara terpusat. Pendekatan ini bertujuan untuk membangun SOC yang tidak hanya mampu melakukan deteksi dan notifikasi ancaman secara *real-time*, tetapi juga memberikan arsitektur yang modular, skalabel, dan lebih hemat biaya dibandingkan SOC berbasis lisensi komersial.

B. Rumusan Masalah

Berdasarkan latar belakang, maka didapatkan perumusan masalah sebagai berikut:

1. Bagaimana melakukan perancangan arsitektur dan alur kerja prototipe SOC berbasis integrasi *software open source* supaya memenuhi fungsi inti keamanan siber?
2. Bagaimana melakukan implementasi dan interpretasi hasil pengujian rancangan arsitektur SOC untuk optimasi deteksi dan respons ancaman siber?

C. Batasan Masalah

Adapun batasan masalah dari penelitian yang akan dilakukan adalah sebagai berikut:

1. Software *open source* yang digunakan dalam pengembangan prototipe *Security Operations Center (SOC)* terbatas pada Wazuh versi 4.14 sebagai

Security Information and Event Management (SIEM), Graylog versi 7.0.3 sebagai *log management,* serta MISP versi 2.5 sebagai platform *threat intelligence*, yang seluruhnya berjalan pada sistem operasi Linux Ubuntu Server versi 24.04 LTS.

2. Penelitian difokuskan pada tiga fungsi utama SOC, yaitu pemantauan, deteksi ancaman, dan respons insiden. Fitur yang diimplementasikan pada prototipe meliputi:
    - Pemantauan, meliputi *File Integrity Monitoring (FIM),* pemantauan direktori sensitif dan aktivitas pengguna *root*, aktivitas Docker *(start, stop, restart, dan exec)*, penggunaan sumber daya sistem *(CPU, memori, dan disk),* serta *log* dan trafik jaringan.
    - Deteksi ancaman, meliputi deteksi perubahan file, aktivitas mencurigakan pada Docker, serangan terhadap aplikasi berbasis *container,* deteksi anomali penggunaan sumber daya dan aktivitas sistem, deteksi serangan jaringan menggunakan NIDS, deteksi *malware*, serta korelasi *Indicators of Compromise (IoC)* yang berasal dari MISP.
    - Respons insiden, terbatas pada mekanisme *active response* berupa pemblokiran alamat IP berbahaya, penghapusan *malware*, eksekusi tindakan otomatis yang telah dikonfigurasi, serta pembuatan *alert* pada *dashboard* SOC.
3. Penelitian ini tidak membahas aspek keamanan fisik, kebijakan dan tata kelola organisasi, sertifikasi keamanan, maupun audit dan kepatuhan terhadap standar atau regulasi tertentu.
4. Pengujian prototipe SOC dilaksanakan melalui penerapan skenario serangan yang mengacu pada kerangka kerja MITRE ATT&CK dan OWASP Top 10 sebagai dasar evaluasi fungsionalitas sistem, tanpa mencakup seluruh kemungkinan teknik serangan yang ada.
5. Pengujian prototipe SOC dibatasi pada pengujian fungsional, dengan setiap skenario serangan diulang sebanyak tiga kali untuk memperoleh nilai *Mean Time to Detect (MTTD)* dan *Mean Time to Respond (MTTR)* yang representatif serta memverifikasi konsistensi fungsi sistem.

D. Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan sebagai berikut:

1. Merancang arsitektur dan alur kerja prototipe *Security Operations Center (SOC)* berbasis integrasi perangkat lunak sumber terbuka yang mampu memenuhi fungsi inti keamanan siber, meliputi pemantauan, deteksi ancaman, dan respons insiden.

2. Mengimplementasikan serta mengevaluasi prototipe SOC yang telah dirancang melalui pengujian untuk menganalisis efektivitasnya dalam mengoptimalkan deteksi dan respons terhadap ancaman siber.

E. Manfaat Penelitian

Terdapat berbagai manfaat yang dapat diperoleh melalui penelitian ini. Berikut beberapa manfaat penelitian ini:

1. Menyediakan prototipe *Security Operations Center (SOC)* berbasis integrasi perangkat lunak sumber terbuka yang mampu mendukung proses deteksi dan respons ancaman siber secara *real-time.*
2. Memberikan alternatif solusi yang efisien dan terjangkau bagi organisasi dalam meningkatkan kemampuan deteksi dini dan respons terhadap ancaman siber tanpa bergantung pada solusi komersial berbiaya tinggi.
3. Mendukung upaya peningkatan ketahanan siber nasional, khususnya pada sektor-sektor yang rentan terhadap serangan siber namun memiliki keterbatasan sumber daya.