# BAB I PENDAHULUAN

## I.1 Latar Belakang

*Security Information and Event Management* (SIEM) adalah solusi teknologi yang memungkinkan organisasi untuk mengumpulkan, mengelola, dan menganalisis data log dari berbagai sumber untuk mendeteksi dan menanggapi kejadian keamanan. Dengan semakin kompleksnya ancaman keamanan informasi dan serangan siber yang terjadi, SIEM telah menjadi komponen penting dalam melindungi sistem informasi dan aset digital organisasi.

Namun, SIEM sering menghadapi masalah dalam memproses dan menganalisis jumlah data yang sangat besar. Salah satu cara untuk mengoptimalkan kinerja SIEM adalah dengan menggunakan profiling SIEM untuk menganalisis atribut data *log* yang dihasilkan oleh berbagai aplikasi dan sistem yang terhubung ke jaringan organisasi.

Profiling SIEM memiliki potensi besar untuk meningkatkan kemampuan sistem untuk mendeteksi ancaman keamanan. Namun, penelitian tentang subjek ini masih terbatas dan belum dilakukan secara menyeluruh. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan pemahaman tentang profiling SIEM dan bagaimana hal itu berdampak pada keamanan data organisasi.

Dalam penelitian ini, fokus utama akan tertuju pada pemanfaatan *Security Information and Event Management (SIEM)* dengan penekanan khusus pada *threat intelligence* dan *behavior analysis*. SIEM telah terbukti sebagai komponen esensial dalam melindungi sistem informasi dan aset digital organisasi dari ancaman keamanan yang semakin kompleks. Namun, tantangan terbesar yang dihadapi oleh SIEM adalah kemampuannya dalam memproses dan menganalisis volume data yang sangat besar. Untuk mengatasi hal ini, penelitian ini akan memanfaatkan profiling SIEM untuk mengidentifikasi dan menganalisis atribut data log yang dihasilkan oleh berbagai aplikasi dan sistem yang terhubung ke jaringan organisasi.

Selain itu, penelitian ini akan memfokuskan perhatian pada *threat intelligence* yang memungkinkan organisasi untuk mengumpulkan, menganalisis, dan menginterpretasikan informasi mengenai ancaman potensial. Hal ini akan memungkinkan organisasi untuk merespons ancaman keamanan dengan lebih efektif dan tepat waktu. *Behavior analysis* juga akan menjadi fokus utama, memungkinkan deteksi pola perilaku yang mencurigakan atau abnormal, sehingga memungkinkan tindakan pencegahan yang lebih proaktif.

Dalam penelitian ini, akan dipelajari mekanisme Elastic Security sebagai platform analitik utama dalam mengelola dan menganalisis data log secara efisien. Penelitian ini akan mendalami bagaimana mekanisme tersebut dapat dioptimalkan dalam konteks SIEM untuk menangani tantangan pemrosesan data log yang dihasilkan oleh berbagai aplikasi dan sistem yang terhubung ke jaringan organisasi.

Penelitian ini bertujuan untuk memberikan wawasan mendalam tentang cara organisasi dapat meningkatkan kemampuan dalam mendeteksi dan menanggapi ancaman keamanan dengan lebih akurat dan efisien. Pendekatan ini melibatkan integrasi Security Information and Event Management (SIEM) dengan *Threat Intelligence* dan *Behavior Analysis*, serta penerapan Elastic Security sebagai platform analitik. Hasil penelitian ini diharapkan dapat memberikan panduan praktis bagi organisasi yang mengandalkan SIEM sebagai lapisan pertahanan kunci dalam menghadapi ancaman siber.

## I.2 Perumusan Masalah

Berdasarkan uraian masalah yang telah dijelaskan pada latar belakang, maka permasalahan yang akan dikaji pada penelitian ini adalah sebagai berikut:

1. Bagaimana mengenali fungsi SIEM Elastic Security sebagai kontrol keamanan?
2. Bagaimana fungsi kontrol SIEM Elastic Security memiliki rincian data?
3. Bagaimana fungsi kontrol keamanan dengan rincian data SIEM Elastic Security dapat berfungsi mendeteksi serangan pada jaringan?

## I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang ada, tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Mengenali fungsi *Threat Intelligence* pada SIEM Elastic Security yaitu berupa fungsi kontrol utama menggunakan aspek *Identification*, *Authentication*, *Authorization*, dan *Accounting log*.
2. Mengenali metrik-metrik yang merinci fungsi kontrol utama pada SIEM Elastic Security.
3. Profiling metrik fungsi kontrol Elastic Security sebagai SIEM berdasarkan variasi serangan pada jaringan.

## I.4 Batasan Penelitian

Adapun batasan dalam melakukan penelitian ini, sebagai berikut:

1. Lingkup pengenalan fungsi kontrol berupa serangan dan pendeteksian serangan dalam bentuk simulasi dan eksperimen.
2. Kategori serangan berupa *Port Scanning*, *Brute Force*, dan *DDoS* dengan 3 softtware berbeda untuk kategori *Port Scanning*, *Brute Force*, dan *DDoS*. Setiap software ini digunakan dengan perilaku yang berbeda untuk mendapatkan gambaran Profiling SIEM Elastic Security dalam mendeteksi dan merespons berbagai jenis serangan siber.
3. Eksperimen menggunakan pendekatan sistem *blackbox* dan analisa tidak membahas aspek internal *software* yang digunakan.

## I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis

a. Dapat menambah pengetahuan terkait fungsi kontrol utama pada SIEM Elastic Security menggunakan *Identification*, *Authentication*, *Authorization*, dan *Accounting*.
b. Dapat mengenali metrik-metrik dari *Threat Intelligence* dan *Threat Behavior* berdasarkan hasil eksperimen serangan.

2. Secara praktis
    a. Sistem SIEM Elastic Security pada jaringan membantu praktik keamanan dalam mengimplementasikan indikator rules sesuai dengan berbagai jenis serangan siber.
    b. Mengenali serangan yang digunakan berdasarkan pada praktik konfigurasi rules untuk *Port Scanning*, *Brute Force*, dan *DDoS*.