BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era yang semakin berkembang ini, pemanfaatan teknologi dan informasi di berbagai bidang menjadi sangat penting dalam mendukung produktivitas dan kemajuan bisnis serta organisasi. Namun, meskipun pentingnya keamanan informasi dalam pemanfaatan teknologi dan informasi, masih banyak organisasi yang kurang memperhatikan keamanan informasi mereka. Tidak jarang, keamanan informasi menjadi hal yang terlupakan dan kurang diperhatikan, padahal kerentanan pada sistem dan kehilangan data bisa mengakibatkan kerugian yang signifikan seperti kehilangan informasi rahasia, penyalahgunaan informasi pribadi, kerusakan pada sistem, dan bahkan kehilangan reputasi. Keamanan informasi menjadi faktor yang sangat penting untuk melindungi kerahasiaan data (*confidentiality*), integritas data (*integrity*) dan ketersediaan data maupun layanan (*availability*) bagi pengguna dan penyedia sebuah layanan yang memanfaatkan teknologi informasi. CIA *triad* adalah model standar dalam keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana sebuah organisasi atau perusahaan ketika data disimpan, dikirim, atau diproses (Hermawan[1] et al., 2022). Sebuah organisasi, perusahaan maupun individu yang memanfaatkan teknologi informasi harus dapat melindungi sistem mereka dari berbagai ancaman yang beresiko dapat merusak sistem. Sehingga membutuhkan solusi untuk memantau dan mengatasi ancaman tersebut secara efektif.

Banyak sekali ancaman dan serangan siber yang menyerang keamanan jaringan dan system. Ancaman dan serangan yang dilakukan oleh pihak yang tidak bertanggung jawab tidak dapat dideteksi secara keseluruhan (Parulian et al., 2021). Ancaman dan serangan ini memberikan dampak negatif seperti kebocoran dan kehilangan data penting, kerusakan pada *server* dan sistem komputer yang merugikan perusahaan atau organisasi terkait yang dapat menjadi resiko terhadap keamanan sebuah sistem jaringan (Raharjo & Ekawati, 2022). Oleh karena itu dibutuhkan suatu teknologi keamanan yang dapat membantu dalam membaca dan menganalisa serangan yang masuk ke dalam sebuah *server*.

Salah satu cara untuk meningkatkan keamanan sistem informasi dan teknologi adalah dengan menggunakan teknologi SIEM (*Security Information and Event Management*). SIEM adalah solusi teknologi keamanan yang digunakan untuk mengumpulkan, analisis, dan respon terhadap serangan dan ancaman keamanan dalam jaringan (González-granadillo et al., 2021). SIEM menggabungkan data log dan *alert* dari berbagai sumber, seperti *firewall*, *intrusion detection systems* (IDS) dan aplikasi lain, untuk membuat laporan dan memantau aktivitas sistem secara *real-time*. Tujuannya adalah untuk membantu organisasi mengatasi dan mengatasi ancaman keamanan secara efektif dan cepat.

Manfaat utama dari penggunaan sistem SIEM adalah memantau *log* aktivitas sistem dan jaringan secara *real-time*, sehingga memungkinkan deteksi ancaman lebih cepat dan tepat. SIEM memungkinkan untuk melakukan analisis dan investigasi keamanan yang lebih efektif dan efisien, sehingga mempermudah identifikasi dan penanganan ancaman keamanan (Khotimah et al., 2022). SIEM memungkinkan untuk memantau seluruh aktivitas sistem dan jaringan, termasuk

log aplikasi *firewall* dan perangkat jaringan, sehingga memberikan gambaran keseluruhan situasi keamanan. SIEM dapat berintegrasi dengan sistem dan aplikasi lain seperti IDS/IPS, *firewall* dan sistem manajemen jaringan, sehingga memberikan solusi keamanan yang lebih komprehensif. SIEM membantu memenuhi kebutuhan regulasi dan standar keamanan yang berlaku, seperti PCI DSS, HIPAA dan NIST (Williams, 2016). Dengan memakai sistem SIEM, organisasi dapat lebih efektif dalam mengelola dan mengatasi ancaman keamanan, sehingga dapat menjaga integritas dan keamanan informasi yang dimilikinya.

Salah satu contoh dari SIEM yang digunakan untuk mengelola, menganalisis, dan melindungi sistem dari serangan siber adalah *Splunk* dan *Elastic Stack*. *Splunk* adalah platform SIEM yang menggunakan teknologi analisis data untuk memberikan visibilitas *real-time* dan pemahaman tentang data keamanan yang masuk (Abidian, 2021). *Splunk* dapat digunakan untuk menganalisis data dari berbagai sumber, termasuk *log*, aplikasi, sistem, dan infrastruktur. Dalam konteks serangan siber, *Splunk* dapat membantu mengidentifikasi ancaman, menganalisis *log* aktivitas jaringan, dan memberikan laporan tentang serangan siber yang terjadi. *Elastic Stack*, sebelumnya dikenal sebagai ELK *Stack*, adalah *platform* SIEM *open source* yang terdiri dari tiga komponen utama: *Elasticsearch*, *Logstash* dan *Kibana*. *Elasticsearch* digunakan sebagai mesin pencari dan penyimpan data, *Logstash* digunakan untuk mengumpulkan dan memproses data *log* dari berbagai sumber, dan *Kibana* digunakan untuk visualisasi data (Affandi, 2022). Dalam konteks serangan siber, *Elastic Stack* dapat membantu mengidentifikasi ancaman, menganalisis data *log* dan memberikan laporan tentang serangan siber yang terjadi.

Oleh karena itu berdasarkan permasalahan diatas, penulis bertujuan untuk melakukan penelitian dengan judul "Analisa Perbandingan Kinerja Monitoring *Security Information and Event Management* (SIEM) menggunakan *Splunk* dan *Elastic Stack* dari Serangan Siber" untuk mengevaluasi manfaat dan efektivitas penggunaan SIEM dalam meningkatkan keamanan sistem informasi dan teknologi perusahaan dari serangan siber. Tujuan dari penelitian ini untuk mendeteksi *alert* serangan, menghitung kecepatan *ingest log*, menghitung kecepatan waktu notifikasi *email* dan penggunaan *resource* komputer. Parameter tersebut diharapkan dapat membantu untuk menentukan kelebihan dan kekurangan dari SIEM *Splunk* dan *Elastic Stack*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan masalah pada penelitian ini sebagai berikut:

1. Bagaimana implementasi Monitoring *Security Information and Event Management* (SIEM) menggunakan *Splunk* dan *Elastic Stack* dalam mendeteksi beberapa macam serangan siber?
2. Bagaimana perbandingan kinerja *Monitoring* pada *Security Information and Event Management* (SIEM) menggunakan *Splunk* dan *Elastic Stack* sehingga dapat disimpulkan kelebihan dan kekurangan masing-masing SIEM untuk mendeteksi serangan siber?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas batasan masalah pada penelitian ini sebagai berikut:

1. SIEM yang digunakan adalah *Splunk* dan *Elastic Stack*.
2. Parameter pengujian kinerja adalah kecepatan *ingest log*, deteksi *alert* serangan, waktu notifikasi *alert* dan penggunaan *resource* komputer.
3. Serangan yang dilakukan untuk pengujian kinerja SIEM adalah *Denial of Service* (DoS) *Attack, Port Scanning* dan *Bruteforce Attack*.
4. *Source code* pemrograman yang dibuat hanya untuk membantu dalam penelitian.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Melakukan implementasi *Splunk* dan *Elastic Stack* sebagai SIEM dalam mendeteksi beberapa macam serangan siber.
2. Membandingkan kinerja *Splunk* dan *Elastic Stack* untuk menentukan kelebihan dan kekurangan masing-masing SIEM dalam mendeteksi serangan siber.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

a. Bagi Perusahaan
    1. Dapat menentukan SIEM mana yang lebih baik dan cocok diantara *Splunk* dan *Elastic Stack* untuk diterapkan pada perusahaan.
    2. SIEM membantu *Security Operation Center* pada perusahaan atau organisasi untuk meningkatkan keamanan sistem, menganalisis dan mendeteksi serangan siber secara cepat dan akurat.

3. Perusahaan dapat memperoleh wawasan yang lebih baik tentang kelemahan dan celah dalam sistem mereka.
4. Perusahaan dapat meningkatkan efektivitas bisnis mereka dan memperkuat reputasi mereka di mata pelanggan dan mitra bisnis.

b. Bagi Bidang Keilmuan

1. Dapat menambah wawasan baru terkait analisis kinerja *Splunk* dan *Elastic Stack* dalam mendeteksi serangan siber dengan efektif.
2. Dapat mengembangkan atau memperbaiki metodologi yang digunakan dalam evaluasi dan pengujian sistem keamanan.
3. Sebagai referensi bagi penelitian berikutnya.

c. Bagi Kampus

1. Meningkatkan kurikulum keamanan informasi dan serangan siber di kampus.
2. Memastikan mahasiswa memperoleh pengetahuan dan keterampilan yang lebih baik tentang pentingnya analisis kinerja SIEM.
3. Membuka peluang kolaborasi dengan fakultas atau peneliti lain di kampus yang tertarik dengan bidang keamanan informasi.

a. Bagi Penulis

1. Melalui penelitian ini penulis dapat mengembangkan keterampilan analisis data, pemecahan masalah, dan penelitian ilmiah.

2. Menjadi kebanggaan bagi penulis dalam menyumbangkan pengetahuan baru dan memecahkan masalah yang relevan dalam bidang keamanan informasi.