BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan sudah menjadi hal yang perlu diperhatikan seiring dengan berkembangnya teknologi yang pesat. Melakukan pemantauan melalui catatan-catatan log jaringan sudah seharusnya dilakukan. Berdasarkan prediksi *owaps.org* (2021) ancaman *Security Logging* masuk ke dalam salah satu 10 besar ancaman security pada tahun 2021, dan berdasarkan data dari BSSN (2023), mengungkapkan bahwa prediksi serangan *cyber* yang terjadi dapat mengancam sebuah data dan server sebuah perusahaan, diantaranya *data breach, ransomware, bruteforce distributed denial of service, pishing.* Berdasarkan dengan data tersebut sudah semestinya memerlukan sebuah teknologi untuk manajemen log jaringan serta penanganan pada ancaman yang terjadi di jaringan secara cepat dan realtime.

Security Information and Event Management (SIEM). Menurut Granadillo, Zarzosa, & Diaz (2021), SIEM merupakan sebuah sistem yang telah digunakan secara luas sebagai salah satu alat yang ampuh untuk mencegah, mendeteksi, memberikan respon terhadap ancaman siber yang terjadi. Salah satu perusahaan teknologi keamanan ternama yang memperkenalkan SIEM secara luas diperkenalkan oleh *'Gartner'*. Menurut Gartner Fungsi kegunaan dari SIEM secara luas merupakan sebuah teknologi yang dapat memanajemen informasi dan peristiwa keamanan mendukung pada deteksi ancaman yang terjadi, dan respon terhadap peristiwa keamanan data secara *realtime* dari berbagai sumber data pada log jaringan. Maka teknologi SIEM dapat digunakan untuk membantu mendeteksi dan merespon ancaman yang terjadi pada log jaringan secara *realtime*.

Menurut IBM (2023), IBM QRADAR merupakan *Security Intelegence Platform* yang menyediakan arsitektur terpadu untuk mengintegrasikan SIEM, memanajemen log, deteksi anomali, insiden forensik serta manajemen konfigurasi dan kerentanan. IBM adalah sebuah perusahaan ternama yang mengembangkan produk Qradar sebagai teknologi SIEM, salah satu produk nya adalah IBM QRadar Community Edition. Dengan Community Edition ini adalah versi gratis Qradar berfitur lengkap dengan penggunaan memori rendah, EPS rendah, dan sebuah lisensi abadi.

Berdasarkan data dari InfiniteLearning.id. Infinite Learning Indonesia merupakan anak perusahaan dari PT Kinema Systrans Multimedia, berfokus pada pengembangan pelatihan kejuruan yang terbuka secara umum yang dilaksanakan melalui kerja sama dengan lembaga pendidikan lokal dan internasional. Salah satu perusahaan international ternama yang sudah bekerja sama dengan Infinite Learning Indonesia yaitu IBM Academy. Dengan alur bisnis perusahaan yang memberikan pelatihan gratis dan umum secara luas, maka peningkatan keamanan juga perlu diperhatikan khususnya dalam sektor jaringan. Karena semakin tinggi tingkat akses maka *traffic* jaringan yang masuk akan semakin banyak, permasalahan yang dihadapi berfokus pada peningkatan dalam segi pemantauan lalu-lintas jaringan yang terjadi. Karena sangat dipastikan banyak nya orang yang dapat mengakses infinite learning baik masuk atau keluar secara mudah, dan dengan sistem kelancaran di bisnis ini adalah semakin banyaknya orang yang akses untuk mengetahui infinite learning maka bisnis akan semakin meningkat.

Dengan adanya data yang didapat, bahwa serangan siber di indonesia meningkat terutama dalam sebuah jaringan yang dapat mengakibatkan dampak buruk bagi sebuah perusahaan. Maka dibutuhkan lah sebuah sistem yang dapat memonitoring semua *traffic* yang masuk apakah akses yang benar atau sebuah serangan. IBM Qradar menjadi jawaban atas permasalahan keamanan jaringan yang terjadi khususnya disebuah perusahaan, karena IBM Qradar temasuk ke dalam teknologi SIEM yang dimana dapat memantau aktivitas log jaringan yang masuk secara *real-time*. Teknologi ini dibutuhkan untuk mengatasi permasalah di perusahaan infinite learning indonesia dimana bisnis perusahaan yang mengharuskan banyaknya akses public sehingga harus dilakukan sebuah pemantauan *traffic log* yang terjadi secara *real-time* dan dilakukan penanganan keamanan secara cepat.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah dan identifikasi masalah diatas, rumusan masalah dalam penelitian ini adalah “Bagaimana penerapan IBM Qradar SIEM dalam mendeteksi ancaman keamanan jaringan serta analisis hasil”.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk memberikan pandangan secara luas tentang implementasi QRadar SIEM di Infinite Learning Indonesia serta menganalisis dan mengidentifikasi jenis - jenis permasalahan ancaman keamanan jaringan yang terjadi

pada infinite learning yang telah terdeteksi oleh IBM Qradaar SIEM. Serta mengukur sejauh mana IBM Qradar dapat memenuhi tujuan dan harapan dalam keamanan jaringan.

1.4 Batasan Masalah

Batasan ruang lingkup diperlukan agar menjadi parameter untuk menentukan cakupan suatu masalah dalam penelitian ini agar tindakan yang dilakukan tidak menyimpang dari maksud yang sebenarnya. Selain itu membantu mengarahkan fokus pada hal-hal yang relevan dan memperoleh pemahaman yang lebih dalam tentang masalah tersebut. Berdasarkan latar belakang dan batasan masalah maka penerapan QRadar SIEM sebagai sistem monitoring jaringan di infinite learning indonesia adalah sebagai berikut:

1. QRadar di implementasi untuk mengetahui traffic log yang masuk ke dalam sistem jaringan.
2. Berfokus pada penggunaan IBM QRadar Community Edition yang digunakan sebagai tools monitoring.
3. Jenis serangan yang terjadi berupa lingkup jaringan seperti *bruteforce attack*, *distributed denial of service* (ddos).
4. Lingkup penelitian hanya mencakup jaringan server web Infinite Learning bukan keseluruhan jaringan pada Infinite Learning.
5. Penelitian ini hanya fokus pada sudut pandang pemantauan keamanan jaringan tidak mencakup yang lainnya.
6. Penelitian ini dibatasi oleh penerapan sistem dalam *local system* satu jaringan yang sama.
7. Penelitian ini akan dibatasi oleh ketersediaan data dan log yang relevan.

1.5 State of the Art

Judul Jurnal	Pembahasan
Secured Access Control in Security Information and Event Management Systems **Penulis :** - Leila Rikhtechi - Vahid Rafe - Afshin Rezakhani **Lokasi :** Iran, Arak **Tahun :** 2020	**Hasil Penelitian :** Jurnal ini membahas metode yang disarankan untuk kontrol akses yang aman dan terintgrasi dalam SIEM. dan menerapkan tiga tahap analisis yaitu persyaratan untuk pembentukan sistem SIEM yang aman, desain arsitektur yang aman, dan pengkodean yang aman. **Alasan Menjadi Tinjauan Penelitian :** Jurnal ini memberikan pendalaman lebih tentang SIEM dimana menjelaskan model kerja SIEM, perancangan sistem nya. Pada jurnal ini didapatkannya pemahaman tentang component SIEM
Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII **Penulis :** - Muhammad Rijal Kamal - Mukhamad Andri Setiawan **Lokasi :** Universitas Islam Indonesia Yogyakarta, Indonesia **Tahun :** 2021	**Hasil Penelitian :** Jurnal ini membahas penerapan SIEM menggunakan Splunk menggunakan studi kasus penerapan Sistem Informasi Event Management untuk membantu meningkatkan sistem keamanan jaringan pada perubahan teknologi informasi pada Universitas Islam Indonesia sehingga hasil penelitiannya dapat memantau log jaringan yang terjadi dan dapat di visualisasi kan dengan hasil akhir dapat membantu meningkatkan keamanan jaringan menggunakan SIEM splunk.

	Alasan Menjadi Tinjauan Penelitian : Pada metode penelitian penerapan SIEM splunk dapat digunakan sebagai masukan dalam penerapan SIEM Qradar di Infinite Learning
Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server **Penulis :** - Huelilik Dyan Heluka - Wiwin Sulistyo **Lokasi :** STMIK Banjarbaru Banjarbaru, Indonesia **Tahun :** 2023	**Hasil Penelitian :** Jurnal ini membahas tentang implementasi SIEM wazuh dengan menggunakan penerapan *virtual private server* (VPS) dengan tinjauan Hasil utamanya untuk memantau log jaringan yang terjadi dan tervisualisasikan pada SIEM Wazuh Hasil dan pembahasan dari implementasi SIEM wazuh untuk mendeteksi adanya serangan pada VPS web aplikasi. **Alasan Menjadi Tinjauan Penelitian :** Pada bagian perancanga menjelaskan diagram alir SIEM bekerja dan toppologi yang digunakan, sehingga dapat menjadi masukan dalam penelitian ini dengan cara yang berbeda.
Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos **Penulis :** - Oky Dwi Prasetyo - Primantara Hari Trisnawan - Adhitya Bhawiyuga	**Hasil Penelitian :** Jurnal ini membahas tentang pengujian sistem dan uji kinerja SIEM Wazuh dengan menggunakan HIDS (Host Intrusion Detection System) dalam mendeteksi berbagai jenis serangan diantaranya *bruteforce attack* dan *denial of service* dengan menggunakan berbagai metode pengujian sehingga

Lokasi : Universitas Brawijaya Malang, Indonesia **Tahun :** 2023	mendapatkan hasil yang dianalisis tiap skenario pengujiannya. **Alasan Menjadi Tinjauan Penelitian :** Jurnal ini memberikan gambaran dalam melakukan pengujian sistem SIEM untuk mendapatkan log hasil yang sesuai dan beberapa metode serta jenis serangan yang digunakan.

1.6 Sistematika Penulisan

Sistematika penulisan ini bertujuan untuk mengorganisir dan menyusun informasi dalam sebuah tulisan dan memudahkan untuk memahami isi tulisan dengan baik dan logis. Sistem penulisan laporan penelitian terdiri dari:

BAB I : PENDAHULUAN

Bab ini berisi tentang pengenalan terhadap topik yang akan dibahas seperti latar belakang, tujuan penelitian, batasan masalah, *state of the art* dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini mencakup teori-teori serta studi literatur penelitian sejenis yang digunakan sebagai rujukan atau acuan dalam penyusunan laporan penelitian implementasi *IBM Qradar SIEM*.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini berfokus pada penjelasan tentang analisis permasalahan, perancangan dan kebutuhan pada sistem yang digunakan dalam melakukan penelitian, termasuk langkah-langkah dalam pengujian, menganalisa data dan mendapatkan hasil yang relevan.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil implementasi program berdasarkan alur sistem yang dibuat, hasil pengujian dan penerapan rules pada program yang dibuat.

BAB V : PENUTUP

Bab ini berisi tentang rangkuman keseluruhan tulisan, kesimpulan yang diperoleh serta saran dan rekomendasi untuk penelitian selanjutnya.