JURNAL RISET TEKNIK KOMPUTER
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jurtikom
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/ee1r1q05

IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DALAM MENINGKATKAN KEAMANAN JARINGAN

Muh. Al amin [a*], Rakhmadi Rahman [b]
[a] Sistem Informasi, alaminamin8745@gmail.com , Institut Teknologi Bacharuddin Jususf Habibie, Parepare Sulawesi Selatan
[b] Information System Departement, rakhmadi.rahman@ith.ac.id , Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
*Korespondensi

ABSTRACT

In the rapidly evolving digital era, threats to information security have become increasingly complex and diverse. Security Information and Event Management (SIEM) offers a comprehensive solution through the collection, correlation, and analysis of log data from various sources to detect and respond to threats in real-time. This research analyzes the implementation of SIEM in a large organization, highlighting its functionalities, benefits, and challenges, and conducts simulations to test its effectiveness. The results indicate that SIEM can enhance threat detection and response, ensure regulatory compliance, and improve operational efficiency. However, SIEM implementation requires careful planning, competent human resources, and strong management support.

Keywords: *SIEM, Information Security, Implementation, Threat Detection, Regulatory Compliance*

Abstrak

Di era digital yang berkembang pesat, ancaman terhadap keamanan informasi menjadi semakin kompleks dan beragam. Security Information and Event Management (SIEM) menawarkan solusi komprehensif melalui pengumpulan, korelasi, dan analisis data log dari berbagai sumber untuk mendeteksi dan menanggapi ancaman secara real-time. Penelitian ini menganalisis penerapan SIEM dalam organisasi besar, menyoroti fungsionalitas, manfaat, dan tantangannya, serta melakukan simulasi untuk menguji efektivitasnya. Hasilnya menunjukkan bahwa SIEM dapat meningkatkan deteksi dan respons ancaman, memastikan kepatuhan terhadap peraturan, dan meningkatkan efisiensi operasional. Namun, penerapan SIEM memerlukan perencanaan yang cermat, sumber daya manusia yang kompeten, dan dukungan manajemen yang kuat.

Kata Kunci: SIEM, Keamanan Informasi, Implementasi, Deteksi Ancaman, Kepatuhan Regulasi.

1. PENDAHULUAN

Keamanan informasi menjadi salah satu aspek yang sangat penting dalam era digital saat ini. Ancaman siber yang semakin kompleks menuntut organisasi untuk mengadopsi teknologi yang mampu mendeteksi dan merespons ancaman secara cepat dan efisien. Security Information and Event Management (SIEM) merupakan salah satu solusi yang menawarkan kemampuan ini melalui pengumpulan, korelasi, dan analisis data log dari berbagai sumber.

SIEM adalah teknologi yang mengintegrasikan pengumpulan, analisis, dan pelaporan data keamanan dari berbagai sumber dalam satu platform terpusat. Dengan menggabungkan kemampuan log management dan event correlation, SIEM membantu organisasi untuk memantau aktivitas sistem, mendeteksi ancaman, dan merespons insiden keamanan secara real-time.

Received Juni 2, 2024; Revised Juni 11, 2024; Accepted Juli 24, 2024; Online Available Juli 27, 2024

Sistem SIEM mengumpulkan data log dari berbagai komponen infrastruktur TI, termasuk server, perangkat jaringan, aplikasi, dan perangkat keamanan seperti firewall dan antivirus. Data ini kemudian dianalisis menggunakan algoritma canggih untuk mengidentifikasi pola atau aktivitas yang mencurigakan. Hasil analisis ini dapat memberikan wawasan berharga tentang potensi ancaman atau pelanggaran keamanan, memungkinkan tim keamanan untuk mengambil tindakan yang diperlukan [1].

Kemampuan untuk menganalisis informasi secara cepat dan efektif adalah kunci untuk kesuksesan bisnis. Salah satu alat yang telah mengubah cara organisasi memanfaatkan data mereka adalah Splunk. Dikenal sebagai platform analitik data terkemuka, Splunk memungkinkan perusahaan untuk mengumpulkan, mencari, dan menganalisis data dari berbagai sumber secara real-time, memberikan wawasan yang mendalam dan mendukung pengambilan keputusan yang lebih baik.

Splunk adalah perangkat lunak yang dirancang untuk mengelola dan menganalisis data log dan data terstruktur lainnya. Platform ini mengumpulkan data dari berbagai sumber, termasuk server, perangkat jaringan, aplikasi, dan perangkat IoT, dan kemudian mengindeks data tersebut untuk memungkinkan pencarian dan analisis yang efisien. Dengan antarmuka yang intuitif, Splunk mempermudah pengguna dalam melakukan query, visualisasi, dan pelaporan, tanpa memerlukan keterampilan pemrograman yang mendalam [2].

2. TINJAUAN PUSTAKA

2.1. Security Information and Event Management (SIEM)

SIEM merupakan solusi teknologi yang krusial dalam manajemen keamanan informasi modern. SIEM mengintegrasikan pengumpulan, analisis, dan pelaporan data log dari berbagai sumber untuk mendeteksi dan merespons ancaman secara real-time. Sebagai teknologi yang menggabungkan log management dan event correlation, SIEM menawarkan kemampuan untuk memantau aktivitas sistem, mendeteksi ancaman, dan merespons insiden dengan cepat. Menurut Allen (2020), SIEM berfungsi dengan mengumpulkan log dari berbagai sumber, menganalisis data untuk mengidentifikasi pola atau anomali, dan menyediakan laporan untuk mendukung keputusan keamanan.

2.1.1. Fungsi dan Manfaat SIEM

Menurut Brown & Smith (2019), SIEM memiliki beberapa fungsi utama, termasuk pengumpulan log terpusat, korelasi data untuk mendeteksi ancaman, serta pelaporan yang mendukung kepatuhan regulasi. Dengan mengintegrasikan data dari berbagai sumber, SIEM membantu organisasi dalam mendeteksi ancaman yang mungkin tersembunyi dalam volume data yang besar. Chuvakin, Schmidt, & Phillips (2013) menekankan pentingnya log management sebagai komponen kunci dalam SIEM, karena log menyediakan jejak audit yang diperlukan untuk investigasi insiden keamanan.

2.1.2. Splunk sebagai Platform SIEM

Splunk merupakan salah satu platform SIEM yang banyak digunakan di berbagai organisasi. Menurut SANS Institute (2021), Splunk menyediakan berbagai fitur seperti pencarian data, analisis real-time, dan visualisasi yang mendukung deteksi ancaman dan kepatuhan regulasi. Proses instalasi Splunk, seperti yang dijelaskan dalam panduan pengguna Splunk, melibatkan pengunduhan file dari situs resmi dan instalasi perangkat lunak pada sistem operasi yang sesuai. Splunk juga memungkinkan integrasi data dari berbagai sumber dan konfigurasi yang mendukung kebutuhan spesifik organisasi.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode Studi literatur digunakan untuk mengumpulkan data tentang berbagai jenis yang melibatkan pengumpulan, evaluasi, dan sintesis informasi dari berbagai sumber yang telah dipublikasikan sebelumnya.

4. HASIL DAN PEMBAHASAN

4.1 Implementasi SIEM di organisasi besar

a. Pengumpulan Log Terpusat: Organisasi mengumpulkan log dari berbagai perangkat keamanan dan aplikasi, mengintegrasikan data ke dalam sistem SIEM.

b. Korelasi Data dan Pemantauan Real-time: SIEM menggunakan algoritma korelasi untuk mengidentifikasi ancaman yang kompleks. Pemantauan real-time memungkinkan tim keamanan merespons ancaman dengan cepat.
c. Pelaporan dan Kepatuhan: SIEM menyediakan laporan yang membantu organisasi memenuhi berbagai persyaratan regulasi, memastikan audit trail yang lengkap dan komprehensif.

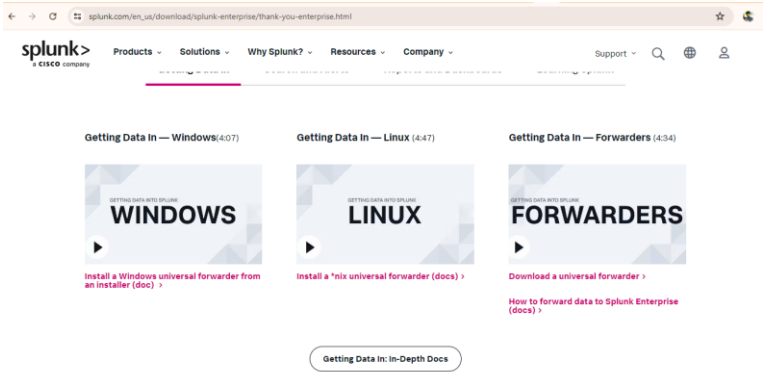
4.2 Tantangan Implementasi

a. Kompleksitas Teknis: Integrasi SIEM dengan berbagai sistem yang ada di organisasi memerlukan penyesuaian khusus dan sering kali menimbulkan tantangan teknis yang signifikan.
b. Kebutuhan Sumber Daya: Implementasi dan pemeliharaan SIEM membutuhkan sumber daya manusia yang terlatih dan anggaran yang cukup, termasuk biaya untuk perangkat keras, perangkat lunak, dan pelatihan.
c. Dukungan Manajemen: Keberhasilan implementasi SIEM sangat tergantung pada dukungan manajemen puncak, termasuk komitmen untuk menyediakan sumber daya yang diperlukan dan memahami pentingnya keamanan informasi.

4.3 Implementasi Splunk

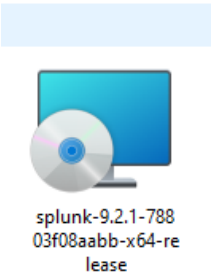
a. Instalasi Splunk

Masuk pada browser dan cari splunk.com hingga muncul gambar seperti di bawah dan pilih sesuai sistem perasi yang digunakan perangkat masing-masing.



Gambar 1 Instalasi Splunk

b. Bentuk file Splunk setelah di download

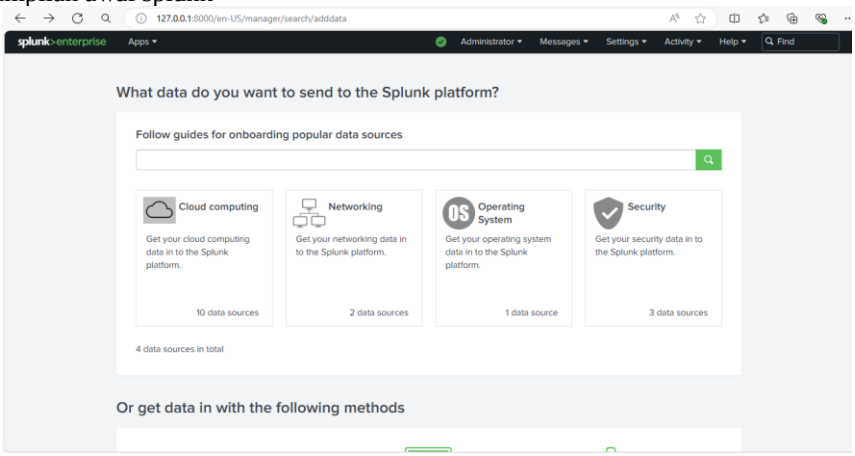


Gambar 2 File Splunk

c. Setelah di download maka silahkan lakukan penginstalan hingga selesai seperti pada gambar berikut

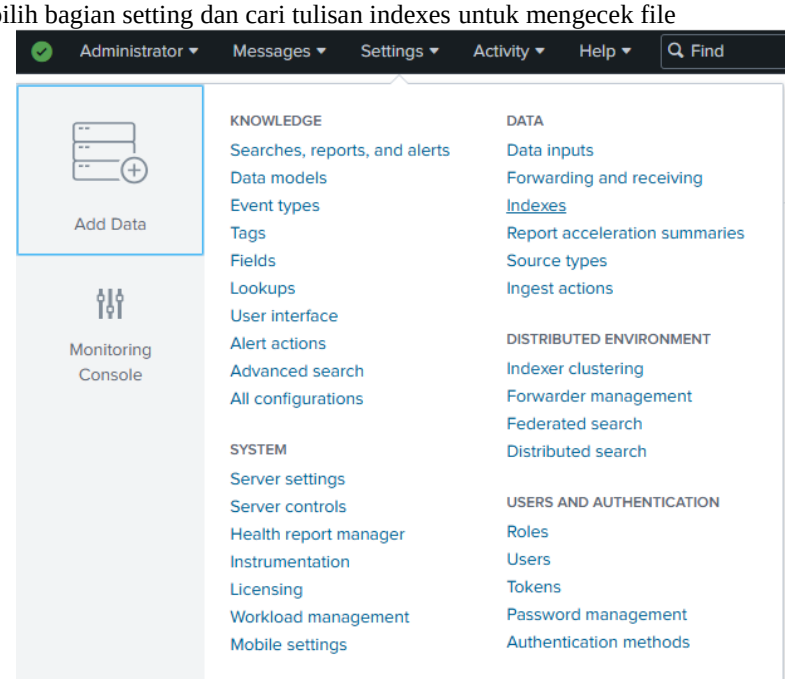
Gambar 3 Instal Splunk

d. Berikut tampilan awal splunk



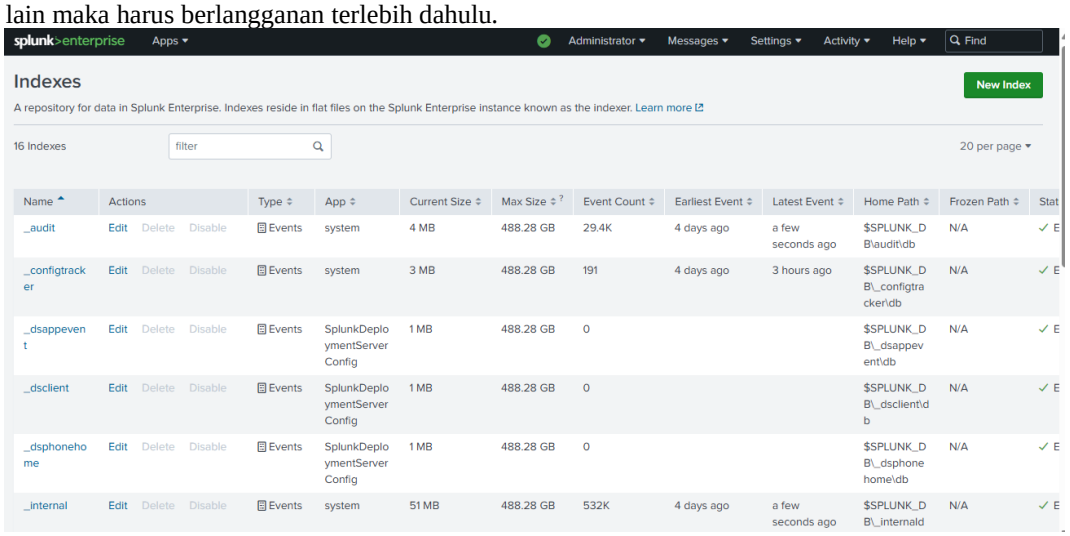
Gambar 4 Tampilan Awal Splunk

e. Kemudian pilih bagian setting dan cari tulisan indexes untuk mengecek file



Gambar 5 Bagian Setting Splunk

f. Selanjutnya akan muncul gambar seperti di bawah untuk mengecek file dan ketika ingin melihat fitur lain maka harus berlangganan terlebih dahulu.



Gambar 6 Mengecek File

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa implementasi SIEM dalam manajemen keamanan informasi dapat secara signifikan meningkatkan kemampuan deteksi dan respons terhadap ancaman, membantu memenuhi persyaratan kepatuhan regulasi, dan meningkatkan efisiensi operasional tim keamanan informasi. Meskipun terdapat tantangan dalam implementasinya, seperti kompleksitas teknis dan kebutuhan sumber daya yang tinggi, manfaat yang ditawarkan oleh SIEM menjadikannya investasi yang berharga bagi organisasi.

Perencanaan yang Matang organisasi harus melakukan perencanaan yang matang sebelum mengimplementasikan SIEM, termasuk analisis kebutuhan dan sumber daya yang diperlukan. Pelatihan dan Pengembangan memberikan pelatihan yang cukup bagi tim keamanan untuk mengoperasikan SIEM dengan efektif. Dukungan Manajemen memastikan dukungan manajemen puncak untuk keberhasilan implementasi SIEM, termasuk komitmen untuk menyediakan sumber daya yang diperlukan. Evaluasi Berkala melakukan evaluasi berkala terhadap kinerja SIEM untuk memastikan sistem berjalan dengan optimal dan melakukan penyesuaian jika diperlukan.

DAFTAR PUSTAKA

[1] Allen, J. (2020). Security Information and Event Management (SIEM) Implementation Guide. Wiley.
[2] Brown, K. & Smith, A. (2019). "Real-Time Threat Detection with SIEM". Journal of Cyber Security, 15(2), 102-115
[3] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669, 2022
[4] Chuvakin, A., Schmidt, K., & Phillips, C. (2013). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress.
[5] Johnson, R., & White, P. (2020). "The Role of SIEM in Modern Cybersecurity Strategies". Cybersecurity Today, 12(4), 234-245.
[6] Kamal and Setiawan. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. Jurnal Informatika Universitas Islam Indonesia Vol. 2 No. 2, 2021Martin, L. (2021). Advanced Threat Detection with SIEM. O'Reilly Media.
[7] NIST. (2018). "Guide to Computer Security Log Management". NIST Special Publication 800-92.
[8] Purwanto, A, & Soewito, B. Optimization problem of computer network using ppdioo. ICIC Express Lett, scholar.archive.org,z,2021
[9] SANS Institute. (2021). "SIEM Architecture and Best Practices".