Implementasi SIEM Wazuh pada Server Rumah Sakit Islam Madinah Ngunut

Mohammad Rosed Firmansyah[1]*, Iin Kurniasari[2], Harso Kurniadi [3]

Universitas Islam Kadiri Kediri
Jl. Sersan Suharmaji No.38, Manisrenggo, Kec. Kota, Kota Kediri, Indonesia
rosid.firmansah39@gmail.com[1], iin.kurniasari@uniska-kediri.ac.id[2], harsokurniadi@uniska-kediri.ac.id[3]

Intisari— **Globalisasi telah membawa perubahan mendalam dalam era teknologi informasi, yang memainkan peran kunci dalam kemajuan dan perkembangan negara-negara di seluruh dunia. Namun, kemajuan teknologi juga membawa risiko ancaman siber yang dapat merusak keamanan dan integritas sistem komputer, jaringan, dan data. Serangan siber merupakan ancaman serius yang dapat merugikan individu, organisasi, dan bahkan negara secara keseluruhan. Rumah Sakit Islam Madinah Ngunut sebagai lembaga kesehatan menghadapi potensi risiko serius terhadap keamanan data pasien, gangguan layanan medis, dan penurunan kepercayaan pasien akibat serangan siber. Untuk mengatasi ancaman tersebut, penting untuk menerapkan strategi keamanan yang efektif. Penelitian ini memfokuskan pada implementasi SIEM (Security Information and Event Management) Wazuh pada Server Rumah Sakit Islam Madinah Ngunut. Wazuh dipilih karena kemampuannya dalam mengelola data dalam skala besar, perkembangan yang cepat, dan kemudahan pemeliharaan. Selain itu, integrasi dengan platform pesan instan seperti Telegram juga dilakukan untuk meningkatkan efisiensi dan efektivitas tim keamanan dalam merespons ancaman siber. Diharapkan bahwa implementasi SIEM Wazuh ini akan memperkuat pertahanan keamanan informasi Rumah Sakit Islam Madinah Ngunut, melindungi data pasien, dan menjaga kelancaran operasional sehari-hari dari potensi ancaman siber. Penelitian ini juga diharapkan dapat memberikan panduan bagi rumah sakit lain dalam meningkatkan ketahanan mereka terhadap ancaman siber yang terus berkembang.**
Kata kunci— Monitoring, Siber, SIEM, Wazuh, Telegram.

Abstract— Globalization has brought profound changes in the era of information technology, playing a key role in the advancement and development of countries worldwide. However, technological advancements also bring the risk of cyber threats that can compromise the security and integrity of computer systems, networks, and data. Cyber attacks are a serious threat that can harm individuals, organizations, and even countries as a whole. Madinah Ngunut Islamic Hospital, as a healthcare institution, faces potential serious risks to patient data security, medical service disruptions, and a decline in patient trust due to cyber attacks. To address these threats, it is important to implement effective security strategies. This research focuses on the implementation of Wazuh Security Information and Event Management (SIEM) on the Servers of Madinah Ngunut Islamic Hospital. Wazuh is chosen for its capabilities in managing large-scale data, rapid development, and ease of maintenance. Additionally, integration with instant messaging platforms like Telegram is also carried out to enhance the efficiency and effectiveness of the security team in responding to cyber threats. It is hoped that the implementation of Wazuh SIEM will strengthen the information security defense of Madinah Ngunut Islamic Hospital, protect patient data, and ensure the smooth daily operations from potential cyber threats. This research is also expected to provide guidelines for other hospitals in improving their resilience against ever-evolving cyber threats.
Keywords— Monitoring, Cyber, SIEM, Wazuh, Telegram

I. PENDAHULUAN

Globalisasi telah menjadi pendorong terciptanya era kemajuan teknologi informasi. Teknologi informasi memiliki kedudukan atau peran sangat penting dalam suatu negara, sehingga perkembangan teknologi mendapat tempat yang penting bagi kemajuan dan perkembangan negara yang bersangkutan [1]. Akses internet yang berkembang cukup luas memberikan kemudahan dalam melakukan komunikasi ke berbagai tujuan dengan jangkauan yang sangat luas.

Kemajuan teknologi informasi telah memberikan dampak positif yang signifikan pada berbagai aspek kehidupan manusia [2]. Namun, di sisi lain, kemajuan ini juga membawa risiko, terutama dalam bentuk serangan siber. Serangan siber merupakan ancaman serius terhadap keamanan dan integritas sistem komputer, jaringan, dan data.

Dalam era digital ini, individu, organisasi, bahkan negara secara keseluruhan rentan terhadap dampak merugikan yang dapat dihasilkan oleh serangan siber. Serangan siber dapat mengambil berbagai bentuk, mulai dari serangan sederhana seperti virus komputer hingga serangan canggih yang dilakukan oleh kelompok atau negara dengan tujuan merusak, mencuri informasi rahasia, atau menghancurkan infrastruktur digital.

Dalam konteks Rumah Sakit Islam Madinah Ngunut, serangan siber membawa potensi risiko serius yang mencakup pencurian data pasien, gangguan layanan medis, dan penurunan kepercayaan pasien. Sebagai lembaga kesehatan yang berkomitmen tinggi terhadap standar pelayanan dan etika profesi, Rumah Sakit Islam Madinah Ngunut tidak dapat mengabaikan ancaman terhadap keamanan data pasien dan integritas operasionalnya.

Pentingnya melindungi informasi pasien dan menjaga kelancaran layanan medis menjadi fokus utama dalam merancang strategi keamanan. Dengan meningkatnya penggunaan teknologi informasi dalam industri kesehatan,

Rumah Sakit Islam Madinah Ngunut perlu memastikan bahwa sistem informasi kesehatan mereka memiliki lapisan keamanan yang kuat.

II. BACKGROUND/LATAR BELAKANG

A. Implementasi

Menurut Kamus Besar Bahasa Indonesia, implementasi merujuk pada pelaksanaan dan penerapan suatu konsep atau rencana yang telah disepakati sebelumnya. Implementasi ini melibatkan langkah-langkah untuk mengubah ide menjadi kenyataan [3].

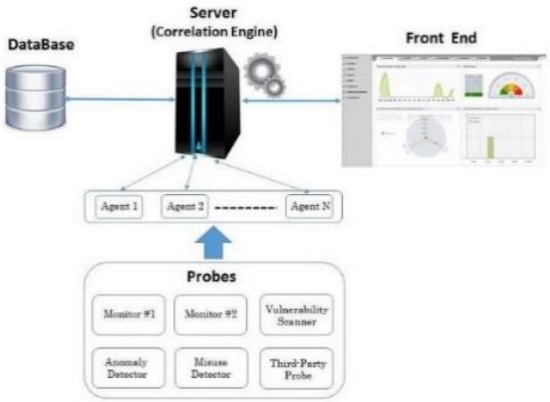
B. Ancaman Kemanan Siber

Ancaman keamanan siber adalah setiap potensi risiko yang dapat mengganggu, merusak, atau mengakses sistem komputer, jaringan, atau data tanpa izin [4]. Dua jenis ancaman yang sering dihadapi adalah *Suspicious Detection from Malware* dan *Possible Brute Force SSH Activity:*

1. *Suspicious Detection from Malware* merupakan proses identifikasi aktivitas atau file yang dapat mengindikasikan adanya malware dalam sistem. Malware adalah perangkat lunak berbahaya yang dirancang untuk menyusup dan merusak sistem komputer, dapat masuk melalui email phishing, situs web terinfeksi, atau perangkat eksternal terinfeksi[5].
2. *Possible Brute Force SSH Activity* adalah upaya penyerang untuk mendapatkan akses tidak sah ke server dengan mencoba berbagai kombinasi username dan password [6].

C. *Security Information and Event Management* (SIEM)

Salah satu komponen penting dalam strategi keamanan siber saat ini adalah SIEM. (Security Information and Event Management) SIEM adalah Sistem monitoring yang dapat mendeteksi serangan dan respon suatu sistem keamanan terhadap serangan melalui analisis log dari berbagai event-log yang berasal dari berbagai sumber data seperti (IPS, IDS, UTM, Router, Server) [7]. Teknologi SIEM berfokus pada pengumpulan, pengelolaan, dan analisis data keamanan dari berbagai sumber di dalam sebuah organisasi. Data tersebut dapat mencakup log keamanan, informasi kejadian jaringan, aktivitas pengguna, dan banyak lagi.



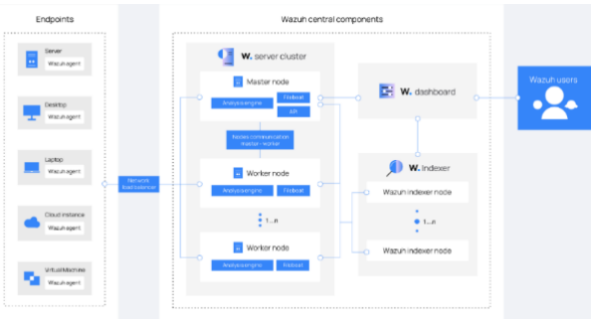
Gambar 1. Arsitektur SIEM

D. Wazuh

Dalam rangka meningkatkan keamanan terhadap ancaman siber di Rumah Sakit Islam Madinah Ngunut, penelitian ini memutuskan untuk menerapkan Wazuh sebagai solusi SIEM. Wazuh adalah platform keamanan terbuka dan gratis yang dipilih karena kemampuannya yang mumpuni dalam mengelola data dalam skala besar, perkembangannya yang cepat, dan kemudahan dalam pemeliharaan [8]. Wazuh merupakan perangkat yang memberikan visibilitas keamanan yang lebih mendalam ke infrastruktur dengan memantau host pada tingkat sistem operasi dan aplikasi, Adapun komponen dan arsitektur Wazuh sebagai berikut:

1. Komponen Wazuh:
   a. Wazuh Indexer memiliki kemampuan pencarian teks yang tinggi dan dilengkapi dengan mesin analisis. Fungsi utamanya adalah untuk melakukan indeks dan menyimpan alarm yang dihasilkan dari Wazuh Server.
   b. Wazuh Server berfungsi untuk menganalisis data yang diterima dari agen, kemudian melakukan dekoder dan penyesuaian dengan aturan keamanan standar.
   c. Wazuh Dashboard adalah antarmuka pengguna web yang digunakan untuk visualisasi dan analisis data.
   d. Wazuh Agent diinstal pada berbagai endpoint seperti laptop, desktop, server, cloud, atau virtual. Mereka memberikan kemampuan pencegahan, deteksi, dan respons terhadap ancaman.
2. Arsitektur Wazuh:

   Arsitektur Wazuh berbasis pada agent yang dijalankan pada endpoint yang akan dimonitor, yang kemudian mengirimkan data keamanan ke server pusat. Server pusat menerjemahkan dan menganalisis informasi yang diterima, dan kemudian meneruskan hasilnya ke Wazuh Indexer untuk diindeks dan disimpan.



Gambar 2. Arsitektur Wazuh

Salah satu keunggulan utama Wazuh adalah kemampuannya dalam mengelola data dalam skala besar. Antarmuka pengguna Wazuh juga menjadi pertimbangan penting, terutama karena tampilannya yang intuitif dan berbentuk grafis. Hal ini diharapkan dapat mempermudah para Administrator jaringan di Rumah Sakit Islam Madinah Ngunut

dalam melakukan pemantauan dan merespons potensi ancaman siber.

E. Telegram

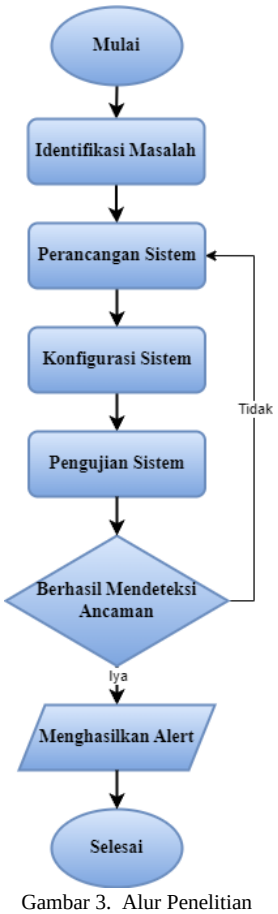
Integrasi Wazuh dengan platform pesan instan seperti Telegram juga merupakan langkah proaktif yang strategis. Dengan menerima Notifikasi realtime melalui Bot Telegram, para Administrator jaringan Rumah Sakit Islam Madinah Ngunut dapat merespons dengan cepat setiap kali terjadi ancaman siber. Selain itu Telegram diklaim sebagai aplikasi yang aman dimana menyediakan pilihan pesan end-to-end yang akan di enskripsi [9]. Hal ini merupakan langkah proaktif yang strategis untuk menjaga keamanan dan kelangsungan operasional Rumah Sakit Islam Madinah Ngunut.

Dengan demikian, peneliti memutuskan untuk mengimplementasikan SIEM Wazuh pada Server Rumah Sakit Islam Madinah Ngunut, yang diharapkan dapat memperkuat pertahanan keamanan informasi Rumah Sakit Islam Madinah Ngunut. Hal ini tidak hanya menciptakan lingkungan yang lebih aman, tetapi juga melindungi data pasien dan kelancaran operasional sehari-hari dari potensi ancaman siber yang dapat merugikan.

III. METODOLOGI PENELITIAN

A. Alur Penelitian

Alur Penelitian yang berisi proses yang dilakukan pada penelitian ini, berupa diagram alur berikut:



Gambar 3. Alur Penelitian

Beberapa tahapan yang ada didalam alur penelitian yaitu:

1. Identifikasi masalah adalah proses awal dalam proyek atau penelitian untuk memahami situasi yang ada, mengumpulkan informasi, dan menentukan masalah utama yang perlu diatasi.
2. Perancangan Sistem adalah proses penggambaran dan perencanaan monitoring keamanan jaringan menggunakan SIEM Wazuh pada Server Rumah Sakit Islam Madinah Ngunut. Dalam penelitian ini, sistem Wazuh akan diinstal untuk melakukan monitoring terhadap ancaman keamanan, dengan Bot Telegram yang terintegrasi untuk memberikan notifikasi alert.
3. Konfigurasi sistem pada penelitian ini adalah peneliti akan menginstall Ubuntu Server 20.04.3 sistem operasi pada Wazuh. Setelah itu, peneliti akan mengkonfigurasi Wazuh Server, Wazuh Indexer, dan Wazuh Dashboard sebagai sistem monitoring. Langkah berikutnya adalah memasang Wazuh Agent pada Server Rumah Sakit Islam Madinah Ngunut untuk mengirimkan log ke Wazuh Server guna analisis lebih lanjut. Terakhir menghubungkan sistem ini dengan Bot Telegram sebagai notifikasi alert.
4. Pengujian Sistem dilakukan untuk dapat mengetahui apakah sistem yang telah dibuat dapat berjalan dengan baik sesuai dengan rencana yang telah dibuat. Pengujian sistem tersebut, nantinya dilakukan dengan menggunakan ancaman berupa *Suspicious Detection from Malware* dan *Possible Brute Force SSH Activity* pada Wazuh Agent yaitu Server Rumah Sakit Islam Madinah Ngunut
5. Menghasilkan alert ketika Wazuh berhasil mendeteksi ancaman, sistem akan mengirimkan notification alert melalui Bot Telegram yang telah diintegrasikan kepada para Administrator jaringan Rumah Sakit Islam Madinah Ngunut.

B. Metode Pengumpulan Data

Peneliti mengumpulkan data yang diperlukan dalam penelitian ini melalui beberapa metode:

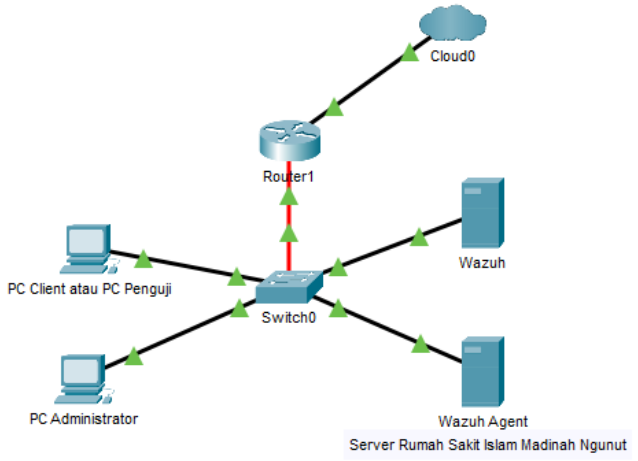
1. Studi Lapangan / Observasi, metode ini melibatkan pengamatan langsung terhadap objek atau fenomena yang diteliti di lingkungan aslinya. Penelitian dilakukan di Rumah Sakit Islam Madinah Ngunut, Kabupaten Tulungagung, karena fasilitas yang tersedia mendukung proses penelitian. Peneliti mengamati perilaku, situasi, atau kondisi yang menjadi fokus penelitian secara langsung.
2. Studi Pustaka / Literatur, metode ini dilakukan dengan memanfaatkan teori-teori yang ada di website terkait, jurnal-jurnal teknologi yang dapat diakses melalui Google Scholar, dan berbagai penelitian lainnya yang relevan dengan topik penelitian ini.

C. Rancangan Sistem

Penelitian ini bertujuan membangun sistem monitoring keamanan jaringan menggunakan SIEM (*Security Information and Event Management*) Wazuh dan Bot Telegram sebagai alat

notification alert. Sistem monitoring tersebut nantinya akan dikonfigurasi sehingga sistem ini dapat melakukan monitoring terhadap ancamanan kemanan siber. Pengujian akan dilakukan untuk memastikan sistem dapat mendeteksi ancaman keamanan. Pendeteksian ancaman kemanan ini nantinya akan dilakukan oleh *tools* SIEM yaitu Wazuh, kemudian informasi bahwasanya telah terjadi ancaman akan ditampilkan di Wazuh Dashboard serta dikirimkan melalui Bot Telegram. Integrasi dengan Bot Telegram memungkinkan para Administrator jaringan Rumah Sakit Islam Madinah Ngunut merespons dan mengambil tindakan pencegahan dengan cepat, guna mengamankan infrastruktur IT Rumah Sakit Islam Madinah Ngunut.

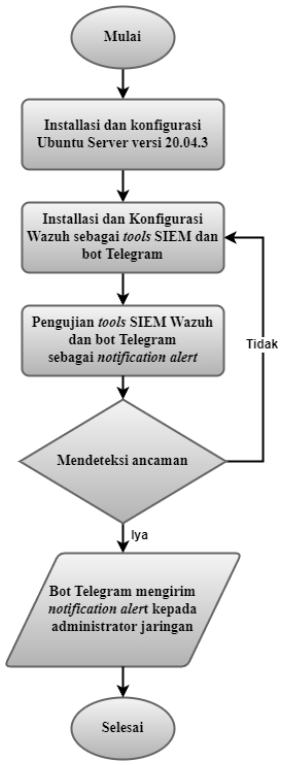
Topologi Sistem Monitoring Keamanan Jaringan yang akan dibangun seperti dibawah ini:



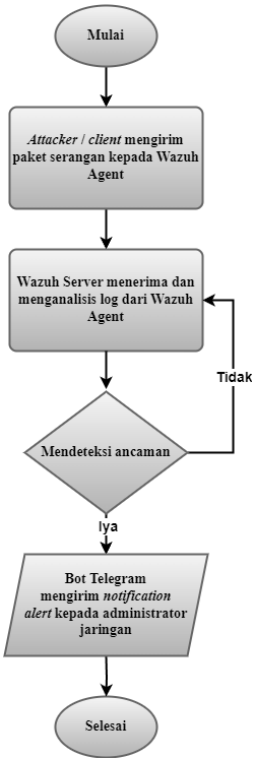
Gambar 3. Topologi Jaringan

Perancangan topologi jaringan sistem Intrussion SIEM (Security Information And Event Management) diatas dapat menjelaskan bahwa dalam jaringan yang akan dibuat nantinya akan terdapat sebuah server yang akan terinstall tools Wazuh sebagai SIEM (Security Information And Event Management) dan juga terdapat target monitoring yaitu Server Rumah Sakit Islam Madinah Ngunut yang telah diinstall Wazuh Agent, Server Rumah Sakit Islam Madinah Ngunut nantinya akan diuji oleh PC client atau PC Penguji dengan melakukan beberapa ancaman keamanan berupa *Suspicious Detection from Malware* dan *Possible Brute Force SSH Activity* untuk mengetahui apakah ancaman keamanan tersebut dapat terdeteksi oleh sistem monitoring, lalu Bot telegram yang nantinya dihubungkan dengan Wazuh akan memberitahu para Administrator jaringan Rumah Sakit Islam Madinah Ngunut jika telah terjadi ancaman terdahap Wazuh Agent sehingga Bot Telegram dapat berfungsi sebagai *notification alert*.

Adapun flowchart rancangan sistem dan rancangan security SIEM Wazuh sebagai berikut:



Gambar 3. Rancangan Sistem



Gambar 5. rancangan security SIEM Wazuh

IV. HASIL DAN PEMBAHASAN/DISKUSI

A. Pengujian Sistem Monitoring SIEM Wazuh

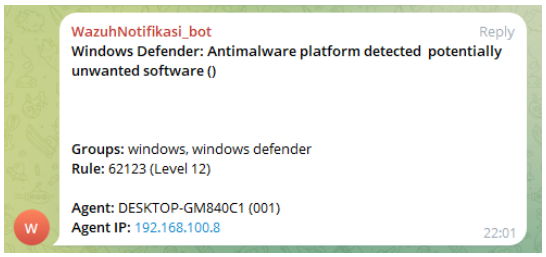
Pengujian sistem monitoring ini bertujuan untuk memastikan bahwa SIEM Wazuh yang telah dikonfigurasi mampu mendeteksi ancaman yang terjadi pada target monitoring. Pengujian ini dilakukan dengan mensimulasikan ancaman keamanan yaitu *suspicious detection from malware* dan *possible bruteforce ssh activity*.

1. *Suspicious detection from malware*

Dalam pengujian ini, penguji dengan sengaja mengunduh dan menjalankan file eicar sebagai malware di Server Rumah Sakit Islam Madinah Ngunut untuk menguji respon dan kemampuan deteksi ancaman pada SIEM Wazuh.

Gambar 4. Eicar file

Hasil pengujian *suspicious detection from malware* menunjukkan bahwa SIEM Wazuh berhasil mendeteksi adanya malware pada server tersebut dan notifikasi terkait ancaman berhasil dikirimkan melalui Bot Telegram.



Gambar 5. Notifikasi Telegram Suspicious Detection from Malware

2. Possible Bruteforce SSH Activity

Pengujian menggunakan *possible Bruteforce ssh activity* dilakukan dari PC client atau PC Penguji. Penguji menggunakan Nmap sebagai tools Bruteforce untuk mencoba login SSH ke Server Rumah Sakit Islam Madinah Ngunut dengan berbagai kombinasi username dan password.

Gambar 6. Ancaman Possible Brute Force SSH Activity

Hasil pengujian *possible Bruteforce SSH activity*, dapat dilihat bahwa sistem monitoring SIEM Wazuh berhasil mendeteksi adanya upaya Bruteforce pada target monitoring yaitu Server Rumah Sakit Islam Madinah Ngunut, Notifikasi terkait ancaman tersebut juga berhasil dikirimkan melalui Bot Telegram.

Gambar 7. Notifikasi Telegram Possible Bruteforce SSH Activity

B. Hasil Pengujian Sistem Monitoring SIEM Wazuh

Hasil pengujian menunjukkan bahwa SIEM Wazuh dapat mendeteksi dan memberikan notifikasi yang berisi informasi tentang ancaman keamanan.

1. Hasil Deteksi Ancaman

Pada tabel 1. Hasil Pengujian Ancaman menunjukkan bahwa SIEM Wazuh dapat mendeteksi ancaman dengan akurasi yang tinggi.

Tabel 1. Hasil Pengujian Ancaman

No	Jenis Ancaman	Hasil yang didapat	Level Alert	Kesimpulan
1	*Suspicious detection from malware*	Terdeteksi	12	Berhasil
2	*Possible Bruteforce SSH activity*	Terdeteksi	5	Berhasil

2. Waktu Deteksi Ancaman

Pada tabel 2. Hasil Deteksi Pengujian Berdasarkan Waktu menunjukkan bahwa waktu pendeteksian ancaman sangat cepat, dengan rata-rata waktu yang dibutuhkan untuk mendeteksi ancaman dari saat ancaman dimulai hingga terdeteksi oleh SIEM Wazuh adalah kurang dari 1 menit.

Tabel 2. Hasil Deteksi Pengujian Berdasarkan Waktu

No	Jenis Ancaman	Hasil deteksi pengujian (waktu)		
		Awal Ancaman	Terdeteksi	Notifikasi Terkirim
1	*Suspicious detection from malware*	22:01	22:01	22:01
2	*Possible Bruteforce ssh activity*	22:24	22:24	22:24

3. Hasil Keseluruhan

Implementasi SIEM Wazuh di Rumah Sakit Islam Madinah Ngunut terbukti efektif dalam mendeteksi dan memberikan peringatan tentang ancaman keamanan. Sistem ini memungkinkan administrator jaringan

merespons cepat dan mengambil tindakan untuk melindungi sistem dan data. Penerapan SIEM Wazuh meningkatkan keamanan jaringan dan memberikan perlindungan tambahan yang sangat penting di lingkungan rumah sakit.

KESIMPULAN

Penelitian ini telah mengimplementasikan SIEM Wazuh sebagai solusi untuk meningkatkan keamanan informasi di Rumah Sakit Islam Madinah Ngunut. Dengan mengintegrasikan Wazuh dengan Bot Telegram, sistem ini mampu memberikan monitoring keamanan yang efektif dengan kemampuan deteksi dan respons yang cepat terhadap ancaman siber pada sebuah Server. Berdasarkan hasil pengujian, Wazuh mampu mendeteksi dan melaporkan berbagai ancaman yang ditujukan pada Server Rumah Sakit Islam Madinah Ngunut.

Implementasi SIEM Wazuh juga memberikan manfaat tambahan berupa laporan keamanan yang mendalam. Dengan demikian, Rumah Sakit Islam Madinah Ngunut dapat menjaga integritas data pasien dan kelancaran operasional, serta meningkatkan kepercayaan masyarakat terhadap layanan kesehatan yang disediakan.

SARAN

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk penelitian selanjutnya:

1. Perluasan Lingkup Penelitian: Untuk penelitian selanjutnya, disarankan untuk memperluas cakupan implementasi SIEM Wazuh ke seluruh sistem jaringan rumah sakit, tidak hanya terbatas pada satu server saja. Hal ini akan memberikan gambaran yang lebih komprehensif tentang keamanan jaringan secara keseluruhan.
2. Pengujian dengan Beragam Ancaman: Selain *Suspicious Detection from Malware* dan *Possible Brute Force SSH Activity*, penelitian berikutnya dapat menguji sistem terhadap berbagai jenis ancaman siber lainnya.
3. Evaluasi dan Pemeliharaan Berkala: Penting untuk melakukan evaluasi dan pemeliharaan sistem secara berkala. Mengadakan audit keamanan rutin dan mengupdate sistem Wazuh sesuai dengan perkembangan teknologi dan ancaman siber terbaru.
4. Penggunaan Fitur-Fitur Lanjutan: Manfaatkan fitur-fitur lanjutan dari Wazuh seperti threat hunting dan integrasi dengan lebih banyak platform monitoring untuk meningkatkan kapabilitas keamanan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Islam Kadiri Kediri atas dukungan akademik yang diberikan selama penelitian. Ucapan terima kasih juga disampaikan kepada Rumah Sakit Islam Madinah Ngunut yang telah memberikan fasilitas dan data penelitian. Penghargaan khusus kepada Ibu Iin Kurniasari, S.Kom., M.Si., M.Kom dan Bapak Harso Kurniadi, S.Kom., M.Kom atas bimbingan dan masukan berharga mereka. Terima kasih kepada rekan-rekan dan keluarga atas dukungan moril dan finansial selama proses penelitian ini.

REFERENSI

[1] H. Kurniadi and . K., "Implementasi Algoritma A Stars, Tilebase Collision Dan Fuzzy Logic Pada Game Strategy," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 9, no. 1, p. 43, 2017, doi: 10.22303/csrid.9.1.2017.43-53.

[2] I. Kurniasari, H. Al Fatta, and Kusrini, "Analisis Sentimen Opini Publik pada Instagram mengenai Covid-19 dengan SVM," *JTECS J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. Komput.*, vol. 1, no. 1, pp. 67–74, 2021.

[3] Y. B. Utomo, "Aplikasi Sistem Pakar Dalam Mendeteksi Kerusakan Ac Rumah Berbasis Android Dengan Mengimplementasikan Metode Certainty Factor," *J. Tek. Inf. dan Komput.*, vol. 4, no. 2, p. 175, 2021, doi: 10.37600/tekinkom.v4i2.290.

[4] Firda, S. Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," *Pros. SEMNAS INOTEK (Seminar Nas. Inov. Teknol.*, vol. 7, no. 1, pp. 52–59, 2023, [Online]. Available: https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/3411

[5] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017.

[6] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023, doi: 10.60076/indotech.v1i3.239.

[7] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, "Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi Analysis of Router Attack With Security Information and Event Management and Implications in Information Security Index," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 2615–8442, 2019.

[8] Fitri Nova, M. D. Pratama, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 3, no. 1, pp. 1–7, 2022, doi: 10.30630/jitsi.3.1.59.

[9] N. Setiawan and M. Agustina, "Pengembangan Perangkat Lunak Payment Remainder di Universitas Bina Darma," *J. Inf. Technol. Ampera*, vol. 1, no. 1, pp. 50–60, 2020, doi: 10.51519/journalita.volume1.isssue1.year2020.page50-60.