IMPLEMENTASI S*ECURITY INFORMATION and EVENT MANAGEMENT*(SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 - Informatika

disusun oleh

RAFLY RUDISTIRA

19.11.3016

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

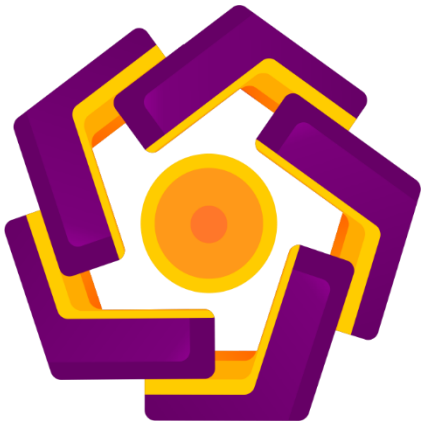
2023

IMPLEMENTASI S*ECURITY INFORMATION and EVENT MANAGEMENT*(SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 - Informatika



disusun oleh

RAFLY RUDISTIRA

19.11.3016

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI S*ECURITY INFORMATION and EVENT MANAGEMENT*(SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM

yang disusun dan diajukan oleh

Nama Mahasiswa
RAFLY RUDISTIRA

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 juli 2023

Dosen Pembimbing,

Majid Rahardi, S.Kom., M.Eng
NIK. 190302393

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI S*ECURITY INFORMATION and EVENT MANAGEMENT*(SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM

yang disusun dan diajukan oleh

RAFLY RUDISTIRA

19.11.3016

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 juli 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Majid Rahardi, S.Kom., M.Eng **NIK. 190302393**	
M. Rudyanto Arief, S.T, M.T **NIK. 190302098**	
Senie Destya, M.Kom **NIK. 190302312**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 juli 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Nama mahasiswa : RAFLY RUDISTIRA
NIM : 19.11.3016

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI *SECURITY INFORMATION and EVENT MANAGEMENT* (SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM.

Dosen Pembimbing : Majid Rahardi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 26 juli 2023

Yang Menyatakan,

Rafly Rudistira

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur, kesyukuran, dan keikhlasan, saya ingin mengabdikan halaman ini sebagai ungkapan penghormatan dan persembahan kepada mereka yang telah memberikan dukungan, cinta, dan inspirasi sepanjang perjalanan penulisan skripsi ini.

Terima kasih yang tak terhingga kepada Allah SWT, Tuhan Yang Maha Esa, atas rahmat, hidayah, dan keberkahan-Nya yang melimpah selama perjalanan hidup dan penulisan skripsi ini. Semoga segala usaha dan karya yang saya hasilkan menjadi amal jariyah yang bermanfaat dan diridhai-Nya.

Terima kasih kepada keluarga tercinta, terutama kepada orangtua saya, yang telah memberikan cinta, doa, dan dukungan tanpa henti sepanjang hidup saya. Terima kasih atas kesabaran, pengertian, dan semangat yang selalu kalian tanamkan dalam diri saya. Kalian adalah sumber inspirasi dan motivasi sejati bagi saya.

Saya juga ingin mengucapkan terima kasih kepada Majid Rahardi selaku dosen pembimbing saya yang luar biasa. Terima kasih atas kesediaan beliau untuk membimbing, mendukung, dan memberikan arahan yang berharga dalam penulisan skripsi ini. Bimbingan dan masukan beliau telah membantu saya dalam mengembangkan pemahaman dan keterampilan penelitian saya.

Tidak lupa, terima kasih kepada teman-teman terbaik saya, yang selalu hadir di setiap langkah dan perjuangan saya. Terima kasih atas dukungan, semangat, dan kebersamaan yang tak tergantikan. Persahabatan kita adalah anugerah yang tidak ternilai bagi saya.

Terima kasih juga kepada seluruh dosen dan staf akademik di Universitas Amikom Yogyakarta yang telah memberikan pengetahuan, wawasan, dan pengalaman berharga selama masa studi saya. Saya juga berterima kasih kepada subjek penelitian dan partisipan yang telah memberikan waktunya untuk menjadi bagian dari penelitian ini. Saya tidak akan melupakan dedikasi dan perjuangan para ilmuwan, peneliti, dan penulis sebelum saya yang telah berkontribusi dalam bidang

penelitian ini. Terima kasih atas upaya dan karya mereka yang menjadi sumber referensi dan inspirasi dalam penulisan skripsi ini.

Akhir kata, terima kasih kepada semua individu dan pihak yang telah memberikan sumbangsih dan dukungan dalam perjalanan penulisan skripsi ini. Semoga karya ini dapat memberikan manfaat, mendorong pengetahuan, dan memperkaya bidang penelitian yang saya teliti.

Terima kasih.

KATA PENGANTAR

Puji syukur saya ucapkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya yang tiada terhingga, sehingga kami dapat menyelesaikan penyusunan skripsi ini dengan judul "IMPLEMENTASI SECURITY INFORMATION and EVENT MANAGEMENT(SIEM) MENGGUNAKAN WAZUH DENGAN NOTIFIKASI TELEGRAM". Penyusunan skripsi ini merupakan bagian dari syarat akademik dalam menyelesaikan studi kami di Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Proses penulisan skripsi ini tidaklah mudah, namun dengan dukungan dan bantuan dari berbagai pihak, saya berhasil menyelesaikannya. Saya berterima kasih sebesar-besarnya kepada Pak Majid Rahardi sebagai dosen pembimbing saya yang memberikan bimbingan, pengarahan, dan dukungan tak ternilai selama penyusunan skripsi ini. Bantuan beliau telah membantu mengembangkan pemahaman dan keterampilan penelitian saya.

Terima kasih juga kepada keluarga, teman-teman, serta seluruh dosen dan staf pengajar di Program Studi Informatika atas dukungan dan ilmu berharga yang telah diberikan selama masa studi. Semua kontribusi ini membentuk saya menjadi pribadi yang lebih kompeten.

Skripsi ini merupakan hasil penelitian dan pengembangan yang saya lakukan selama beberapa bulan. Tujuan utama dari penelitian ini adalah Meningkatkan keamanan jaringan menggunakan SIEM yang terintegrasi telegram. Saya berharap temuan dan analisis yang disajikan dalam skripsi ini dapat memberikan kontribusi yang berarti dalam bidang keamanan siber dan jaringan serta memperluas pemahaman kita tentang keamanan siber.

Akhir kata, semoga skripsi ini dapat memberikan kontribusi dan manfaat bagi perkembangan ilmu pengetahuan dan bermanfaat bagi pembaca yang berminat untuk mengkaji lebih lanjut tentang topik yang kami bahas.

Sekali lagi, terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan skripsi ini. Semoga segala jerih payah yang telah kami persembahkan dapat bermanfaat dan bernilai bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 26 juli 2023

Rafly Rudistira.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

SIEM	Security Information dan Event Management
PPDIOO	Prepare, Plan, Design, Implement, Operate, dan Optimize
SQL	Structured Query Language
DDoS	Distributed Denial of Service
BSSN	Badan Siber dan Sandi Negara
HIDS	Host-Based Intrusion Detection System
NTB	Nusa Tenggara Barat
SEM	Security Event Management
SIM	Security Information Management
FIM	File Integrity Monitoring
IDS	Intruction Detection Sistem
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
CIS	Center for Internet Security
NIST	National Institute of Standards and Technology
API	Application Programming Interface
RBAC	Role-Based Access Control
SSO	Single Sign-On
VPLE	Vulnerable Pentesting Lab Environment
NAT	Network Address Translation
IP	Internet Protocol
SMB	Server Message Block
SSH	Secure Shell
SMS	Short Message Service
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge

DAFTAR ISTILAH

Cyber security	kamanan siber
Ubuntu linux	sistem operasi linux
Kali linux	sistem operasi linux yang digunakan menyerang
Oracle Virtualbox	aplikasi mesin virtual
vulnerabillity testing	pengetesan kerentangan
Security testing	pengetesan keamanan
Cyber crime	kejahatan siber
Cyber attack	serangan siber
Anomali traffic	lalu lintas kejanggalan
Alert	peringatan
Realtime	secara langsung
Confidentiality	kerahasiaan
Integrity	integritas
Availability	ketersediaan
Monitoring	pengamatan

INTISARI

Perusahaan yang bergerak dibidang jaringan seperti infrastruktur jaringan, konsultasi jaringan, pemeliharaan jaringan dan menjual produk jaringan. Seharusnya perusahaan yang bergerak dibidang tersebut sudah memilki atau meningkatkan keamanan jaringannya dari serangan-serangan dari luar. Dengan adanya Security Information dan Event Management(SIEM) diharapkan bisa meningkatkan keamanan Perusahaan. Menggunakan wazuh yang terintegrasi dengan telegram membuat pemantauan terhadap informasi dan peristiwa secara realtime dapat mempermudah pekerjaan pekerja dalam mengamankan jaringan perusahaan.

Penelitian ini menggunakan metode Prepare, Plan, Design, Implement, Operate, dan Optimize(PPDIOO) yang dimana metode ini merupakan metode yang cukup populer dibidang jaringan. Dengan menggunakan kuesioner yang sebagai alat pengambilan data dari perusahaan yang dimana menggunakan teknik populasi dan sampling jenuh. Dikarenakan perusahaan memiliki jumlah pekerja yang terbilang sedikit maka jumlah populasi digunakan sebagai sampel. Setelah data didapatkan maka data diolah menggunakan metode skala likert yang bertujuan mengetahui pendapat kemajuan dari keamanan jaringan, berupa kuesioner yang ditujukan untuk pekerja atau karyawan yang bekerja di perusahaan.

Hasil dari penelitian ini 81,5% menurut hasil akhir skala likert responden memberikan respon yang sangat baik dengan adanya SIEM wazuh yang terintegrasi telegram. Wazuh bisa mendeteksi serangan SQL injection, Brute forece, dan Ddos dan mengirimkan notifikasi alert secara realtime.

Kata kunci: SIEM, Wazuh, Bot, Telegram, PPDIOO.

ABSTRACT

The Company engaged in networking such as network infrastructure, network consulting, network maintenance, and network product sales. Ideally, companies operating in this field should have or improve the security of their networks from external attacks. The presence of Security Information and Event Management (SIEM) is expected to enhance the security of company. By using Wazuh integrated with Telegram, real-time monitoring of information and events can facilitate the work of employees in securing the company's network.

This research uses the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) method, which is a popular method in the field of networking. A questionnaire is used as a data collection tool by the company, employing a population and saturation sampling technique. Due to the small number of employees in the company, the population size is used as the sample. After obtaining the data, the data is processed using the Likert scale method to determine the opinions on the progress of network security. The questionnaire is targeted at employees working in the company.

The results of this research show that 81.5% of the respondents, based on the final results of the Likert scale, provided a very positive response to the integration of Wazuh SIEM with Telegram. Wazuh can detect SQL injection, brute force, and DDoS attacks and send real-time alert notifications.

Keyword: SIEM, Wazuh, Bot, Telegram, PPDIOO.