

**IMPLEMENTASI *SECURITY 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 *SECURITY 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 *SECURITY 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 *SECURITY 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

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

M. Rudyanto Arief, S.T, M.T
NIK. 190302098

Senie Destya, M.Kom
NIK. 190302312

Tanda Tangan



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.

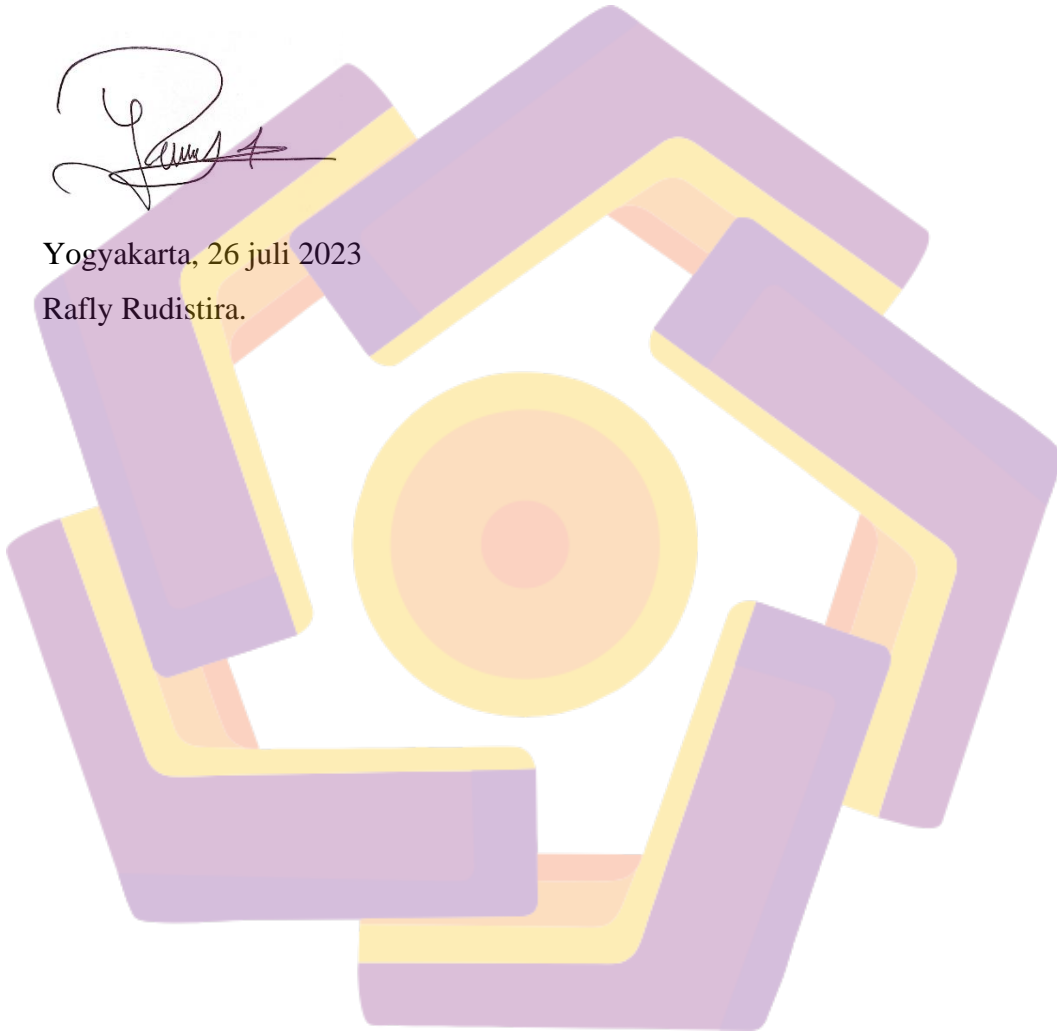
Sekali lagi, terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan skripsi ini. Semoga segala jerih payah yang telah kami persembahkan dapat bermanfaat dan bernilai bagi kita semua.

Wassalamu'alaikum Wr. Wb.



Yogyakarta, 26 juli 2023

Rafly Rudistira.

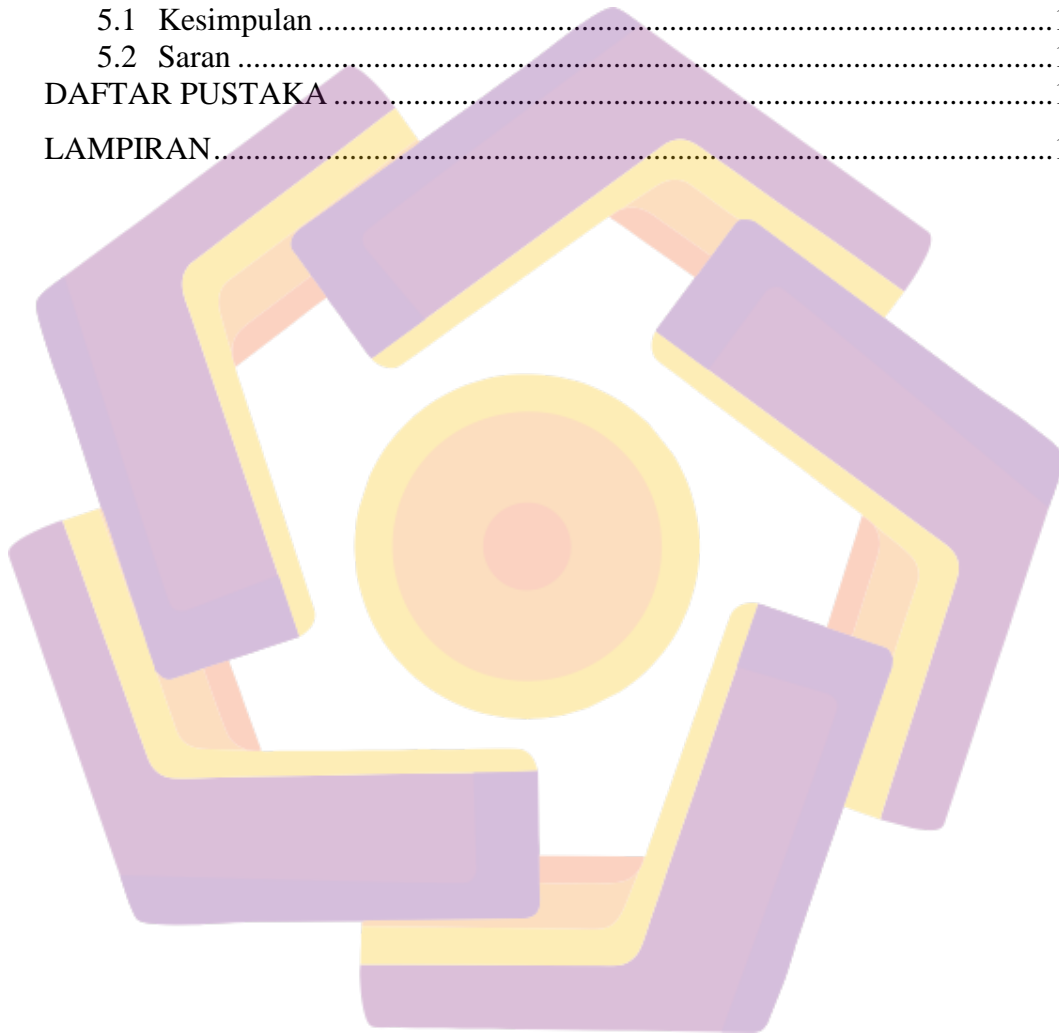


DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN.....	xvi
DAFTAR LAMBANG DAN SINGKATAN	xvii
DAFTAR ISTILAH.....	xviii
INTISARI	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan	7
BAB II TINJAUAN PUSTAKA	8
2.1 Studi Literatur	8
2.2 Dasar Teori	15
2.2.1 Security Information Management (SIM).....	15
2.2.2 Security Event Management (SEM).....	15
2.2.3 Security Information and Event Management (SIEM).....	16
2.2.4 Confidentiality, Integrity, and Availability(CIA).....	17
2.2.5 Wazuh.....	17

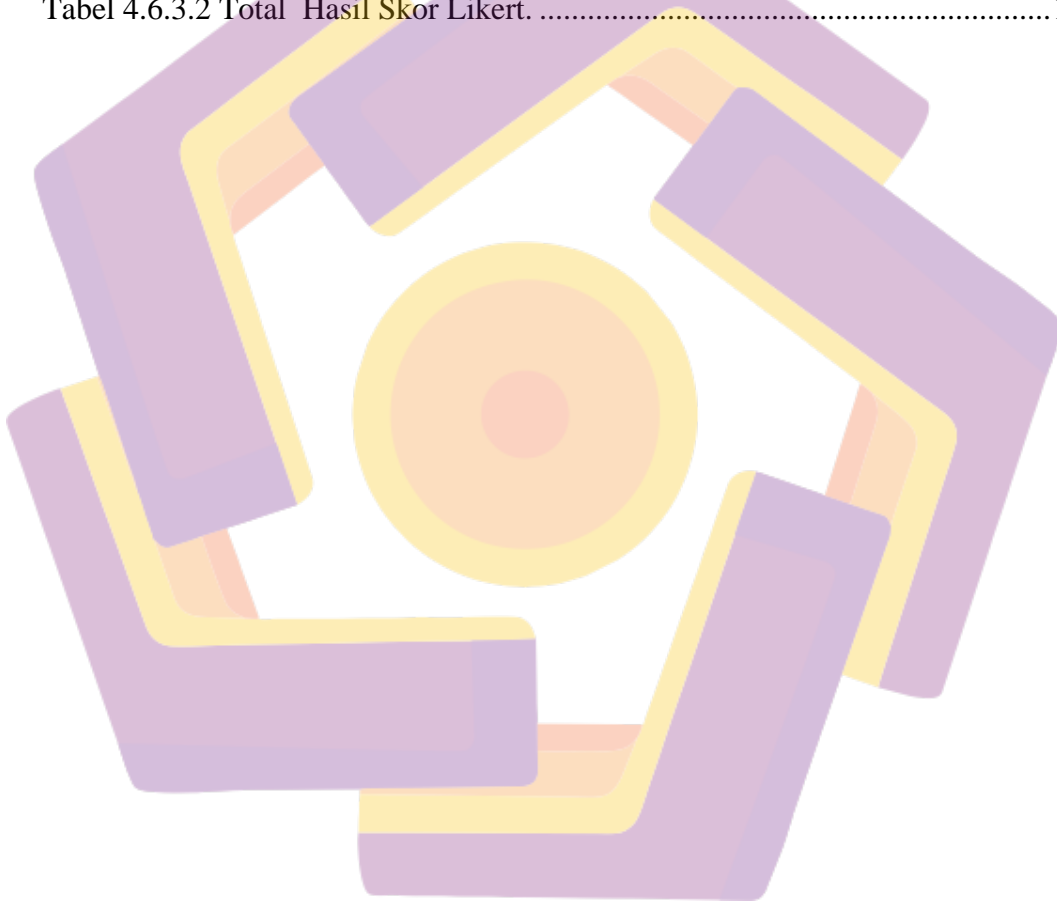
2.2.6 Prepare, Plan, Design, Implement, Operate, and Optimize(PPDIOO).	26
2.2.7 Vulnerable Pentesting Lab Environment(VPLE).....	29
2.2.8 Kali Linux.....	29
2.2.9 Cyber Attack.....	30
2.2.10 DDoS.....	30
2.2.11 SQL Injection.....	31
2.2.12 Brute Force.....	32
2.2.13 Telegram.....	32
2.2.14 Kuesioner.....	33
2.2.15 Menentukan Jumlah Responden.....	33
2.2.16 Teknik Skala Likert.....	34
BAB III METODE PENELITIAN	36
3.1 Objek Penelitian.....	36
3.2 Alur Penelitian	36
3.3 Alat dan Bahan.....	40
3.4 Observasi	41
BAB IV HASIL DAN PEMBAHASAN	42
4.1 Prepare (Persiapan).....	42
4.2 Plan (Perencanaan)	42
4.3 Design (Desain)	42
4.3.1 Topologi Perusahaan.....	43
4.3.2 Topologi VPLE.....	44
4.4 Implement (Implementasi)	45
4.4.1 Instalasi dan Konfigurasi Sistem Operasi.....	45
4.4.2 Instalasi Wazuh	48
4.4.3 Instalasi Wazuh Agent	66
4.4.4 Instalasi Bot Telegram	68
4.5 Operate (Operasional)	77
4.5.1 Implementasi SIEM	77
4.5.2 Pengujian Sistem.....	82

4.6 Optimize (Optimalisasi)	92
4.6.1 Hasil Deteksi.....	92
4.6.2 Hasil Analisis.....	102
4.6.3 Uji Validasi.....	103
BAB V PENUTUP	108
5.1 Kesimpulan	108
5.2 Saran	108
DAFTAR PUSTAKA	109
LAMPIRAN.....	113



DAFTAR TABEL

Tabel 2.1 Studi Literatur.	8
Tabel 3.1 Kebutuhan perangkat lunak	35
Tabel 4.6.2 Daftar serangan yang terdeteksi.....	96
Tabel 4.6.3.1 Hasil kuesioner responden.....	99
Tabel 4.6.3.3 Persentase interval.....	100
Tabel 4.6.3.2 Total Hasil Skor Likert.....	101



DAFTAR GAMBAR

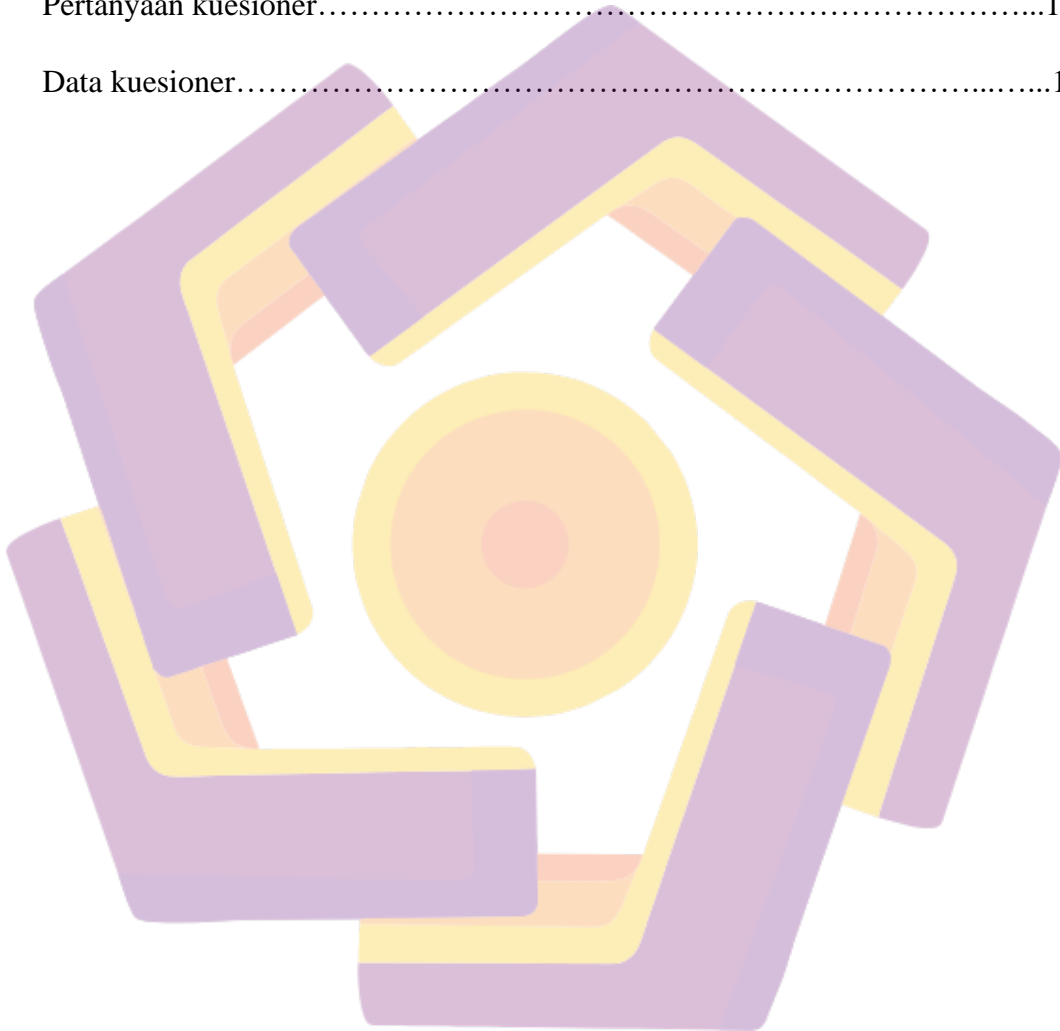
Gambar 1.1 Sebaran kasus per sektor pada Agustus 2022	1
Gambar 1.2 Top 5 Malware hasil monitoring keamanan siber Agustus 2022.....	2
Gambar 1.3 Sebaran kasus per sektor pada Agustus 2022.	3
Gambar 2.1 Struktur Wazuh.	13
Gambar 2.2 Struktur dari Wazuh Indexer.....	15
Gambar 2.3 Struktur Wazuh Server.....	17
Gambar 2.4 Dashboard Wazuh.	18
Gambar 2.5 Struktur Wazuh Agent.	20
Gambar 3.1 Alur Penelitian.	31
Gambar 3.2 Alur Penelitian Menggunakan Metode PPDIOO.....	32
Gambar 4.3.1 Topologi PT. Elforza.....	38
Gambar 4.3.2 Topologi.	39
Gambar 4.4.1.1 Importing Ubuntu Server.	40
Gambar 4.4.1.2 Network Konfigurasi.....	41
Gambar 4.4.1.3 Importing Ubuntu Agent.	41
Gambar 4.4.1.4 Konfigurasi Network Ubuntu Agent.....	42
Gambar 4.4.1.5 Importing Kali Linux.	42
Gambar 4.4.2.2 Mengunduh file sertifikat.....	43
Gambar 4.4.2.3 Config.yml	44
Gambar 4.4.2.4 Tampilan setelah memasukkan perintah.	45
Gambar 4.4.2.5 Tampilan setelah install debconf.....	46
Gambar 4.4.2.6 Tampilan setelah install gnupg.....	46
Gambar 4.4.2.7 Tampilan setelah mengunduh GPG key.....	46
Gambar 4.4.2.8 Tampilan setelah update repository,	47
Gambar 4.4.2.9 Tampilan setelah install wazuh-indexer.....	48
Gambar 4.4.2.10 Tampilan opensearch.yml.	48
Gambar 4.4.2.11 Tampilan setelah memasukkan command wazuh indexer.	49
Gambar 4.4.2.14 Tampilan menjalankan indexer-security-init.sh.....	50
Gambar 4.4.2.15 inialisasi cluster berhasil.....	51
Gambar 4.4.2.16 Memasukkan repository wazuh manager.....	52
Gambar 4.4.2.17 Intalisasi wazuh manager.	53
Gambar 4.4.2.18 memulai layanan wazuh manager.	53
Gambar 4.4.2.19 Pengecekan status wazuh manager.	53
Gambar 4.4.2.20 Instalasi filebeat.	54
Gambar 4.4.2.21 mengunduh file filebeat.yml	54

Gambar 4.4.2.22 Mengedit file filebeat.yml.....	54
Gambar 2.2.4.23 Pembuatan keystore, username dan password.	55
Gambar 2.2.4.24 Mengunduh alert.	55
Gambar 2.2.4.25 Mengunduh alert filebeat.	55
Gambar 4.4.2.26 Tampilan setelah memasukkan perintah.	57
Gambar 4.4.2.27 Tampilan pengunduhan repository wazuh dashboard.....	58
Gambar 4.4.2.28 Tampilan penyerbaran sertifikat wazuh dashboard.....	59
Gambar 4.4.2.29 Status wazuh dashboard.	60
Gambar 4.4.2.30 Tampilan antarmuka wazuh dashboard.....	60
Gambar 4.4.3.1 menambahkan agen.	61
Gambar 4.4.3.2 menambahkan agent.....	61
Gambar 4.4.3.3 Tampilan status wazuh agen	62
Gambar 4.4.4.1 BotFather.....	63
Gambar 4.4.4.2 Memulai BotFather	63
Gambar 4.4.4.3 Membuat bot alerts.....	64
Gambar 4.4.4.4 Memulai bot.	64
Gambar 4.4.4.5 Membangkitkan chat id.....	65
Gambar 4.4.4.6 Pencarian chat id	65
Gambar 4.4.4.7 Mengimput isi file ke file custom-telegram.	67
Gambar 4.4.4.8 Memasukkan chat id pada file custom-telegram.py.....	69
Gambar 4.4.4.9 Memasukkan karyawan perusahaan ke grub bot.	71
Gambar 4.5.1.1 Tampilan agen kontrol.	71
Gambar 4.5.1.2 Tampilan agen kontrol pada agen.	72
Gambar 4.5.1.3 Tampilan agen pada dashboard.....	72
Gambar 4.5.1.4 Tampilan dashboard integrity monitoring.....	73
Gambar 4.5.1.5 Tampilan event integrity monitoring.	73
Gambar 4.5.1.6 Tampilan Event security events.	74
Gambar 4.5.1.7 Tampilan dashboard security events.	74
Gambar 4.5.1.8 Tampilan dashboard system auditing.....	74
Gambar 4.5.1.9 Tampilan events system auditing.....	75
Gambar 4.5.1.10 Tampilan inventory vunerabilities.	75
Gambar 4.5.1.11 Tampilan event vunerabilities.....	76
Gambar 4.5.2.1.1 Tampilan rules pada agen.....	77
Gambar 4.5.2.1.2 Penyerangan sql injection menggunakan kali linux.....	78
Gambar 4.5.2.1.3 Hasil deteksi sql injection 1.	78
Gambar 4.5.2.1.4 Hasil deteksi sql injection 2.	78
Gambar 4.5.2.1.5 Hasil deteksi sql injection 3.	79
Gambar 4.5.2.2.6 Notifikasi grub bot alert telegram.	79

Gambar 4.5.2.2.1 Membuat file password.....	80
Gambar 4.5.2.2.2 Penyerangan menggunakan hydra.....	80
Gambar 4.5.2.2.3 Tampilan wazuh dashboard.....	81
Gambar 4.5.2.2.4 Notifikasi grub bot alert telegram.....	83
Gambar 4.5.2.3.1 Pentmenu tools.....	83
Gambar 4.5.2.3.2 scanning port menggunakan nmap.....	84
Gambar 4.5.2.3.3 Pengujian serangan ddos.....	84
Gambar 4.5.2.3.4 Wazuh dashboard deteksi ddos.....	85
Gambar 4.5.2.3.5 Notifikasi grub bot alert telegram.....	86
Gambar 4.6.1.1 Tampilan serangan sql injection.....	87
Gambar 4.6.1.2 Tampilan rincian serangan sql injection 1.....	87
Gambar 4.6.1.3 Tampilan rincian serangan sql injection 2.....	87
Gambar 4.6.1.4 Tampilan sql injection yang dianalisis wazuh.....	87
Gambar 4.6.1.5 Tampilan rincian serangan brute force 1.....	89
Gambar 4.6.1.6 Tampilan rincian serangan brute force 2.....	90
Gambar 4.6.1.7 Tampilan rincian serangan brute force 2.....	90
Gambar 4.6.1.8 Tampilan rincian serangan brute force 3.....	91
Gambar 4.6.1.9 Tampilan serangan brute force yang dianalisis wazuh.....	91
Gambar 4.6.1.10 Tampilan rincian serangan ddos 1.....	94
Gambar 4.6.1.11 Tampilan rincian serangan ddos 2.....	94
Gambar 4.6.1.12 Tampilan rincian serangan ddos 3.....	95
Gambar 4.6.1.13 Tampilan rincian serangan ddos 3.....	95
Gambar 4.6.4.1 Rumus Skala Likert.....	100
Gambar 4.6.4.2 Rumus Akhir.....	101

DAFTAR LAMPIRAN

Surat izin penelitian.....	107
Balasan surat izin penelitian.....	108
Profile perusahaan.....	109
Pertanyaan kuesioner.....	109
Data kuesioner.....	110

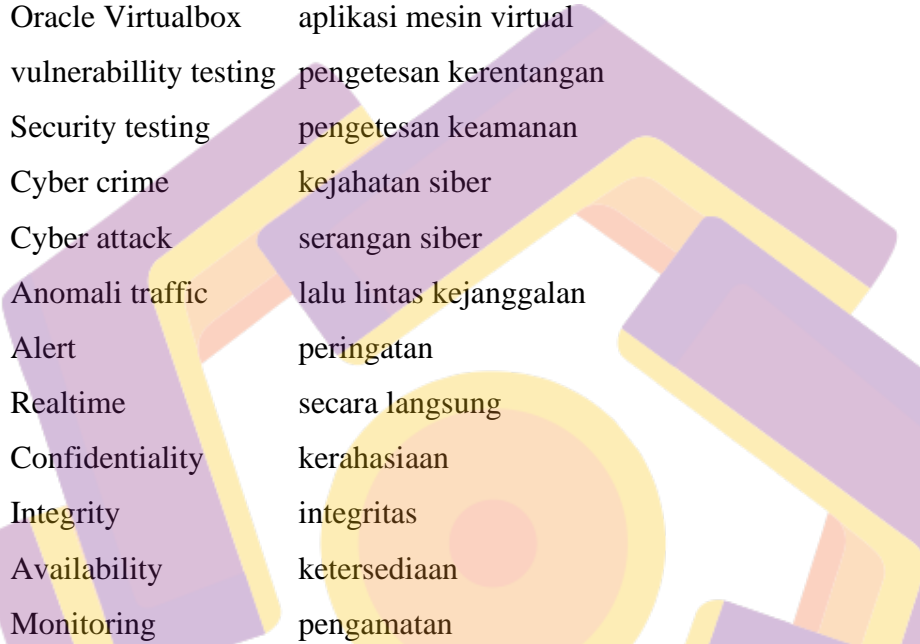


DAFTAR LAMBANG DAN SINGKATAN



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	Intrusion 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
vulnerability 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 memiliki 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 force, 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.