

**IMPLEMENTASI ACTIVE RESPONSE PADA SIEM WAZUH
UNTUK MITIGASI SERANGAN BRUTE FORCE PADA
FIREWALL PFSENSE BERBASIS CLOUD VPS**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

MUHAMMAD WINARIS SUBIAKTO

22.11.5102

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

**IMPLEMENTASI ACTIVE RESPONSE PADA SIEM WAZUH
UNTUK MITIGASI SERANGAN BRUTE FORCE PADA
FIREWALL PFSENSE BERBASIS CLOUD VPS**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Informatika



disusun oleh

MUHAMMAD WINARIS SUBIAKTO

22.11.5102

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI ACTIVE RESPONSE PADA SIEM WAZUH UNTUK
MITIGASI SERANGAN BRUTE FORCE PADA FIREWALL PFSENSE
BERBASIS CLOUD VPS**

yang disusun dan diajukan oleh

Muhammad Winaris Subiakto

22.11.5102

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 April 2026

Dosen Pembimbing,



Ade Pujianto, M.Kom
NIK. 190302494

HALAMAN PENGESAHAN

SKRIPSI

**Implementasi Active Response pada SIEM Wazuh untuk Mitigasi Serangan
Brute Force pada Firewall pfSense Berbasis Cloud**

yang disusun dan diajukan oleh

Muhammad Winaris Subiakto

22.11.5102

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 April 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Akhmad Dahlan, S.Kom., M.Kom.
NIK. 190302174



Bambang Pulu Hartato, S.Kom., M.Eng.
NIK. 190302707



Eli Pujastuti, S.Kom., M.Kom.
NIK. 190302227



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 April 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Winaris Subiakto
NIM : 22.11.5102

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Active Response pada SIEM Wazuh untuk Mitigasi Serangan Brute Force pada Firewall pfSense Berbasis Cloud

Dosen Pembimbing : Ade Pujiyanto, M.Kom.

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, 22 April 2026

Yang Menyatakan,



Muhammad Winaris Subiakto

HALAMAN PERSEMBAHAN

Pertama saya ucapkan puji syukur kehadirat Allah SWT atas segala nikmat berupa kesehatan, kekuatan dan inspirasi yang sangat banyak dalam proses penyelesaian skripsi ini. Shalawat serta salam selalu terlimpahkan pada Nabi Muhammad SAW. Tiada lembar skripsi yang indah dalam laporan skripsi ini kecuali lembar persembahan.

Untuk karya yang sederhana ini, maka penulis persembahkan untuk :

1. Cinta pertama dan pintu surgaku, Ayahanda Budiyo dan Ibunda Nur Khayatun selaku kedua orang tua saya. Terimakasih atas segala doa dan dukungan yang tidak pernah putus. Memberikan cinta, kasih sayang, doa dan pengorbanan yang mengiringi dalam setiap langkahku untuk menyelesaikan pendidikan ini. Terima kasih sudah berjuang untukku, membesarkanku dan mendidikku sampai mendapat gelar sarjanaku. Semoga Allah SWT senantiasa menjaga kalian sampai melihatku berhasil dengan keputusanku sendiri. Hiduplah lebih lama.
2. Teruntuk diriku sendiri, yang telah bertahan dan berjuang sejauh ini. Terima kasih sudah tetap melangkah meski sering merasa lelah, ragu, bahkan ingin menyerah. Terima kasih telah mempercayai proses dan tetap menjaga mimpi – mimpi itu tetap hidup. Perjalanan ini menjadi bukti bahwa diriku mampu menghadapi segala rintangan yang datang. Teruslah kuat, teruslah tumbuh dan teruslah menjadi versi terbaik untuk dari dirimu.

KATA PENGANTAR

Puji Syukur saya panjatkan kepada tuhan Yang Maha Esa, karena atas berkat dan Rahmat-Nya saya dapat menyelesaikan skripsi ini dengan judul **“IMPLEMENTASI ACTIVE RESPONSE PADA SIEM WAZUH UNTUK MITIGASI SERANGAN BRUTE FORCE PADA FIREWALL PFSENSE BERBASIS CLOUD VPS”**. Penelitian ini disusun untuk memenuhi salah satu persyaratan guna memperoleh gelar sarjana di Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

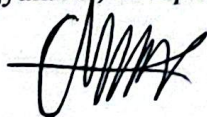
Pada kesempatan ini saya mengucapkan banyak terima kasih kepada:

1. Ade Pujiyanto, M.Kom., selaku dosen pembimbing yang telah memberikan bimbingan dan arahan sekaligus motivasi yang telah diberikan selama proses penyusunan skripsi.
2. Tim Dosen penguji, yang telah memberikan saran, kritik, dan masukan berharga dalam penyempurnaan skripsi ini.
3. Semua pihak yang telah membantu dalam penyelesaian skripsi ini, baik secara langsung maupun tidak langsung
4. Orang tua, keluarga, dan saudari Eva Kurniawati, yang telah memberikan dukungan moral dan doa selama saya menempuh pendidikan dan penyelesaian skripsi, serta memberikan semangat.

Saya menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang konstruktif sangat saya harapkan demi penyempurnaan di masa yang akan datang.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi perkembangan ilmu pengetahuan.

Yogyakarta, 22 April 2026



Muhammad Winairs Subiakto

DAFTAR ISI

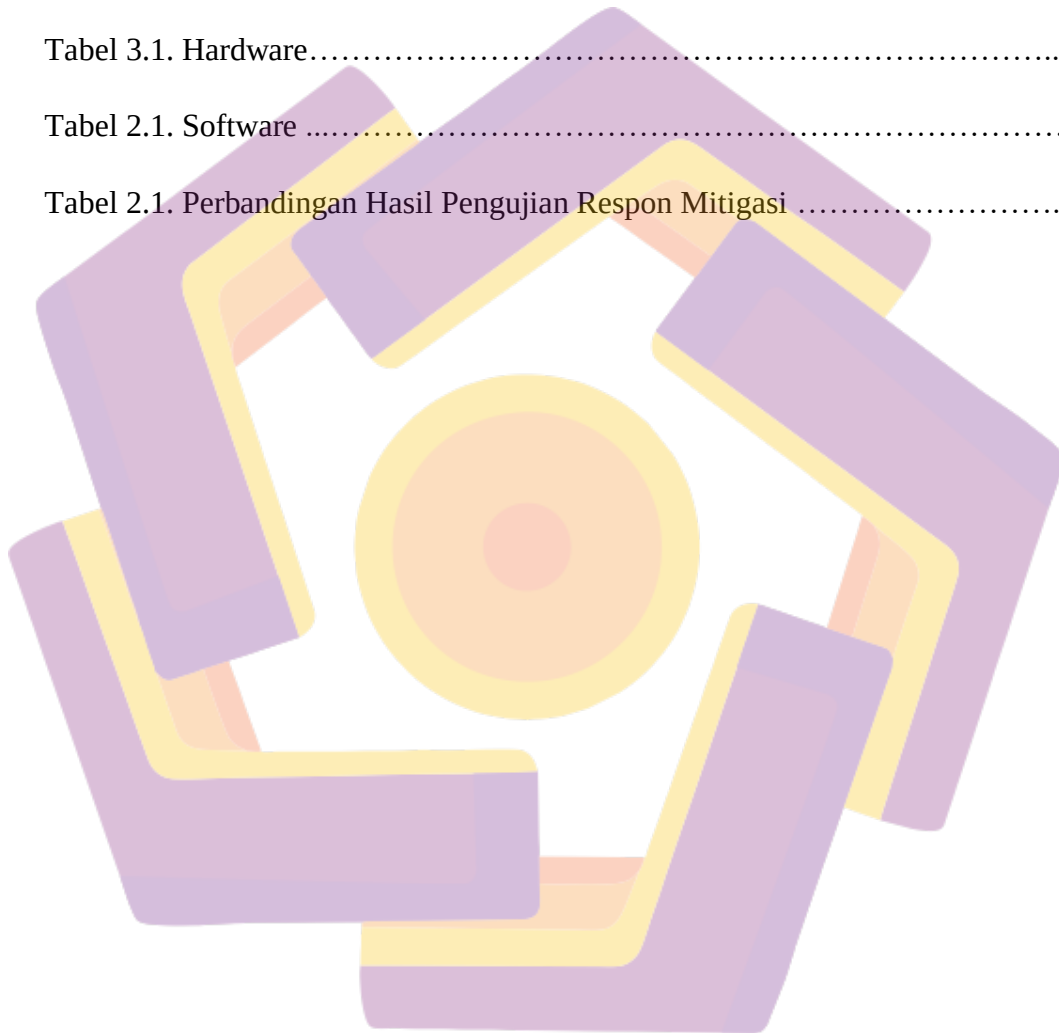
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMBANG DAN SINGKATAN	xiii
DAFTAR ISTILAH	xiv
INTISARI	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	6

BAB II TINJAUAN PUSTAKA	8
2.1 Studi Literatur	8
2.2 Dasar Teori.....	13
BAB III METODE PENELITIAN	15
3.1 Objek Penelitian.....	15
3.2 Alur Penelitian	16
3.3 Alat dan Bahan.....	18
BAB IV HASIL DAN PEMBAHASAN	22
4.1 Hasil Implementasi Sistem	22
4.1.1 Konfigurasi Cloud VPS	22
4.1.2 Konfigurasi pfSense Lokal	24
4.1.3 Konektivitas Hybrid (Remote Logging)	25
4.1.4 Konfigurasi <i>Ruleset</i> dan <i>Active Response</i>	27
4.2 Pengujian dan Analisis Serangan.....	32
4.2.1 Skenario Pengujian A (Tanpa Active Response).....	32
4.2.2 Skenario Pengujian B (Dengan Active Response).....	34
4.2.3 Analisis Kecepatan Respon Mitigasi (Data 2,2 Detik)	35
4.3 Analisis Efektivitas <i>Active Response</i>	40
4.3.1 Reduksi Jendela Waktu Serangan (<i>Attack Window</i>)	40
4.3.2 Akurasi Identifikasi dan Klasifikasi Bahaya.....	41
4.3.3 Analisis Kendala Infrastruktur dan Resiliensi Sistem.....	41
4.4 Pembahasan Temuan Berdasarkan Rumusan Masalah.....	42

4.4.1 Jawaban Rumusan Masalah 1: Integrasi Arsitektur Hybrid.....	42
4.4.2 Jawaban Rumusan Masalah 2: Konfigurasi dan Otomasi Active Response	42
4.4.3 Jawaban Rumusan Masalah 3: Efektivitas Kecepatan Respon dan Akurasi Mitigasi.....	43
4.4.4 Jawaban Rumusan Masalah 4: Stabilitas Performa Cloud VPS RAM 4GB	43
BAB V PENUTUP	45
5.1 Kesimpulan	45
5.2 Saran	46
REFERENSI	47
LAMPIRAN.....	49

DAFTAR TABEL

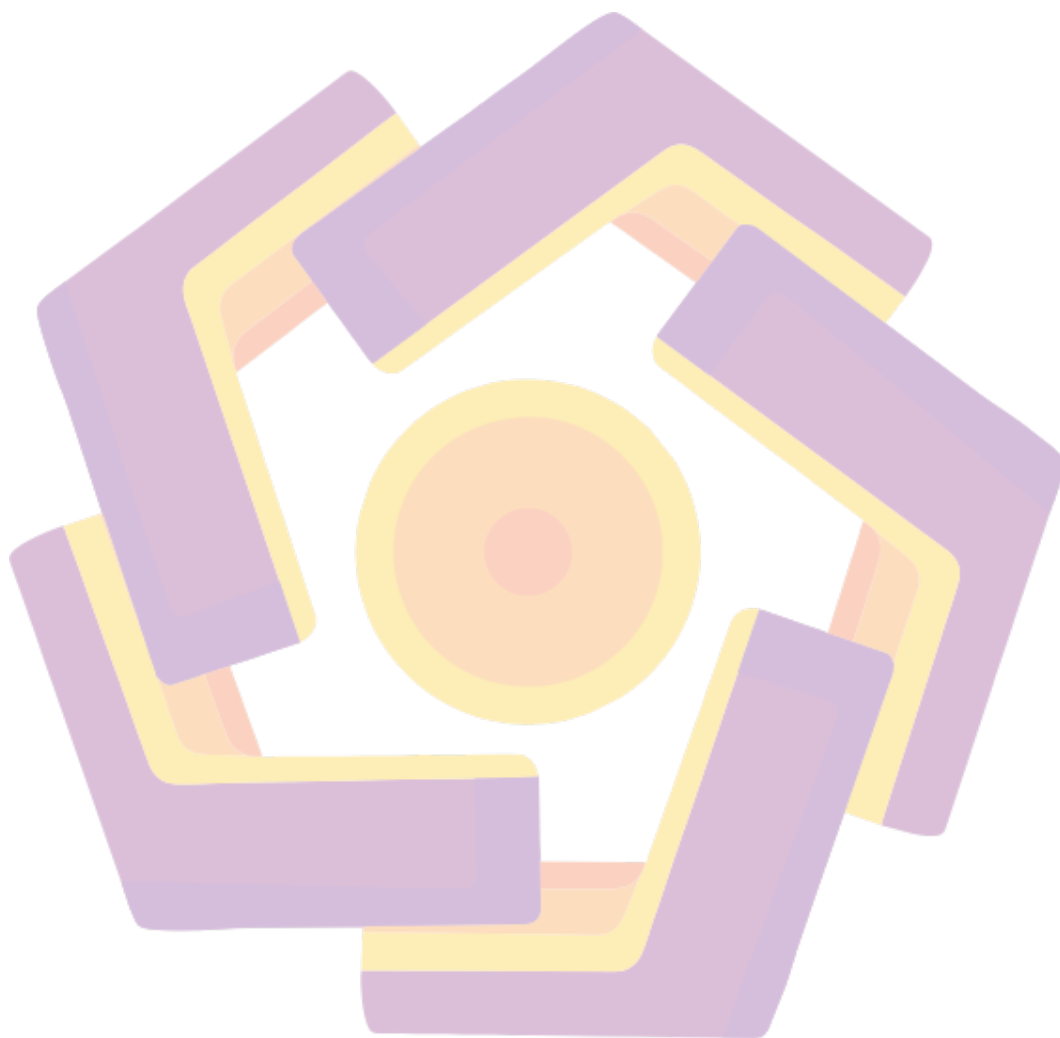
Tabel 2.1. Keaslian Penelitian	8
Tabel 2.1. Keaslian Penelitian	9
Tabel 3.1. Hardware.....	16
Tabel 2.1. Software	17
Tabel 2.1. Perbandingan Hasil Pengujian Respon Mitigasi	32



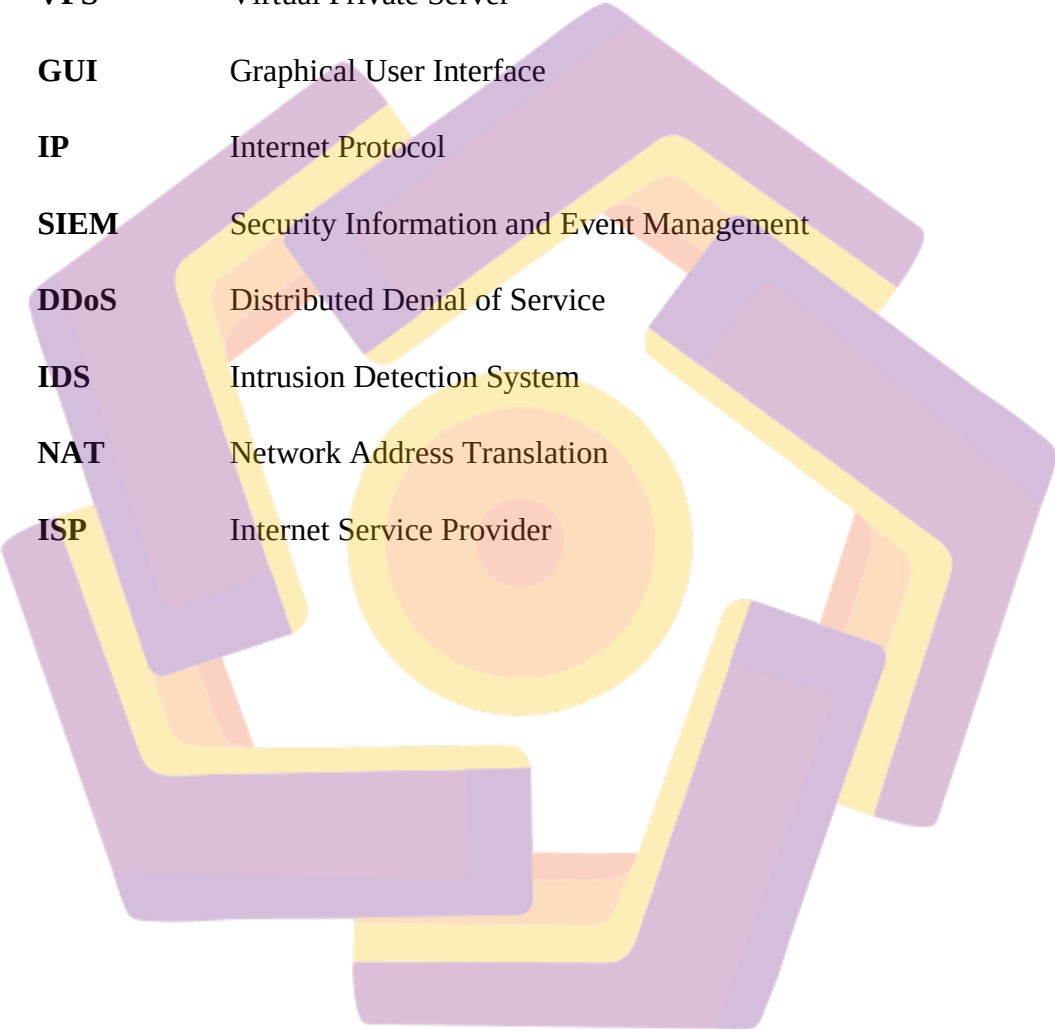
DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian	14
Gambar 3.2 Topologi Jaringan	17
Gambar 4.1 Konfigurasi Cloud Vps	18
Gambar 4.2 Konfigurasi Pfsense Lokal	20
Gambar 4.3 Konektivitas Hybrid	22
Gambar 4.4 Konfigurasi Logika Deteksi.....	24
Gambar 4.5 Skenario Pengujian A	29
Gambar 4.6 Skenario Pengujian B.....	30
Gambar 4.7 Active Response.....	31
Gambar 4.8 Diagram Akumulasi Total Waktu Responce	34

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN



PC	Personal Computer
VPS	Virtual Private Server
GUI	Graphical User Interface
IP	Internet Protocol
SIEM	Security Information and Event Management
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
NAT	Network Address Translation
ISP	Internet Service Provider

DAFTAR ISTILAH



Brute Force	Metode serangan dengan mencoba banyak kombinasi username/password sampai berhasil
Firewall	Sistem keamanan yang mengontrol lalu lintas jaringan masuk & keluar
Port Scanning	Teknik untuk mencari port terbuka pada suatu sistem
Server	Komputer yang menyediakan layanan ke client
Gateway	Penghubung antara dua jaringan berbeda
On-Premises	Sistem yang dijalankan di lokasi sendiri (bukan cloud)
Cloud	Layanan komputasi berbasis internet
Cloud Manager	Sistem untuk mengelola resource cloud
Virtual Machine	Mesin virtual yang berjalan di atas sistem fisik
Hybrid	Kombinasi antara cloud dan on-premises
Open-source	Software dengan kode sumber terbuka
Linux	Sistem operasi berbasis open-source
FreeBSD	Sistem operasi berbasis Unix (sering dipakai di firewall seperti pfSense)
Software	Perangkat lunak
Hardware	Perangkat keras
Bandwidth	Kapasitas maksimum transfer data
Latency	Waktu delay dalam pengiriman data
Broadcast	Pengiriman data ke semua perangkat dalam satu jaringan
Syslog	Protokol untuk mengirim log antar system
Ruleset	Kumpulan aturan untuk mendeteksi atau memfilter aktivitas
Parsing	Proses membaca dan mengolah data agar bisa dianalisis
Logging	Proses pencatatan aktivitas sistem

INTISARI

Keamanan infrastruktur jaringan lokal saat ini menghadapi ancaman serangan siber yang semakin kompleks, salah satunya adalah serangan *brute force* yang dapat mengakibatkan kelumpuhan akses pada perangkat krusial seperti *firewall*. Penelitian ini bertujuan untuk mengatasi masalah tersebut dengan mengimplementasikan sistem *Security Information and Event Management* (SIEM) menggunakan Wazuh yang dikonfigurasi pada infrastruktur *Hybrid Cloud*. Metode yang digunakan meliputi integrasi antara Wazuh Manager yang ditempatkan pada *Cloud VPS* dengan spesifikasi RAM 4GB dan pfSense sebagai *gateway* di jaringan lokal. Sistem dirancang untuk melakukan *remote logging* serta menjalankan fitur *Active Response* sebagai mekanisme mitigasi otomatis. Hasil penelitian menunjukkan bahwa sistem berhasil mendeteksi serangan *brute force* secara *real-time* dan melakukan pemblokiran alamat IP penyerang pada tabel *firewall* pfSense dengan rata-rata waktu respon sebesar 2,2 detik. Meskipun menggunakan spesifikasi memori terbatas sebesar 4GB, *Cloud VPS* terbukti stabil dan efisien dalam mengelola beban analisis *log*. Kontribusi penelitian ini memberikan solusi pengamanan jaringan yang *responsif* dan ekonomis bagi organisasi yang memiliki infrastruktur *on-premises* namun menginginkan pemantauan terpusat berbasis *cloud*. Hasil penelitian ini dapat dimanfaatkan oleh administrator jaringan dan praktisi IT keamanan untuk meningkatkan postur pertahanan jaringan dari ancaman autentikasi ilegal. Penelitian selanjutnya dapat dikembangkan dengan menambahkan integrasi notifikasi melalui platform pesan instan untuk mempercepat pelaporan insiden kepada administrator.

Kata kunci: SIEM, Wazuh, pfSense, *Active Response*, *Hybrid Cloud*.

ABSTRACT

Local network infrastructure currently faces increasingly complex cyber threats, such as brute force attacks that can lead to access paralysis on crucial devices like firewalls. This research aims to address these issues by implementing a *Security Information and Event Management (SIEM)* system using Wazuh configured on a Hybrid Cloud infrastructure. The method involves integrating a Wazuh Manager deployed on a Cloud VPS with 4GB RAM specifications and pfSense as the local network gateway. The system is designed to perform remote logging and execute the Active Response feature as an automated mitigation mechanism. The results demonstrate that the system successfully detects brute force attacks in real-time and performs IP address blocking on the pfSense firewall table with an average response time of 2.2 seconds. Despite using limited memory specifications of 4GB, the Cloud VPS proved to be stable and efficient in managing the log analysis load. This research contributes a responsive and economical network security solution for organizations with on-premises infrastructure that require centralized cloud-based monitoring. These findings can be utilized by network administrators and IT security practitioners to enhance network defense postures against illegal authentication threats. Future research could be developed by adding notification integration through instant messaging platforms to accelerate incident reporting to administrators.

Keyword: *SIEM, Wazuh, pfSense, Active Response, Hybrid Cloud.*