Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
5 (1) 2025, Page 530-539

Sistem Monitoring Keamanan Pada Data Center Berbasis Security Information And Event Management (Siem) Dengan Wazuh dan IDS

Iik Muhamad Malik Matin[1], Fadhilrahman[2], Asep Kurniawan[3], Ayu Rosyida Zain[4], Maria Agustin[5]
[1,2,3,4,5]Teknik Informatika dan Komputer, Politeknik Negeri Jakarta
Corresponding Author: Iik Muhamad Malik Matin, e-mail: iik.muhamad.malik.matin@tik.pnj.ac.id

Published: January, 2025

ABSTRAK

Pusat data adalah pusat untuk mengelola, menyimpan, dan memproses data penting yang mencakup informasi sensitif, aplikasi bisnis, dan infrastruktur teknologi. Karena pentingnya pusat data dalam mendukung operasi organisasi, kerentanannya terhadap ancaman keamanan informasi seperti serangan siber, akses tidak sah memiliki dampak serius pada operasi sehari-hari. Implementasi IDS saat ini belum optimal karena analisis mendalam sulit dilakukan dan memerlukan tenaga ahli untuk mengamatinya. Untuk itu, diperlukan sistem pemantauan keamanan yang efektif pada Intrusion Detection System (IDS) berbasis Security Information and Event Management (SIEM) menggunakan platform Wazuh. IDS berperan penting dalam mendeteksi ancaman keamanan jaringan, sementara SIEM menyediakan kemampuan untuk mengintegrasikan dan menganalisis data keamanan dari berbagai sumber. Penelitian ini merancang dan mengimplementasikan integrasi Wazuh dengan SIEM untuk memperkuat kemampuan deteksi dan respons terhadap ancaman keamanan. Metodologi eksperimental digunakan untuk mengevaluasi kinerja sistem yang dikembangkan, dengan fokus pada deteksi intrusi, analisis log, dan manajemen peristiwa keamanan. Hasil penelitian menunjukkan bahwa integrasi Wazuh dengan SIEM memberikan peningkatan signifikan dalam kemampuan pemantauan dan respons terhadap ancaman keamanan, yang akan menjadi kontribusi berharga dalam menjamin keamanan jaringan dan data sensitif.

Kata kunci: : id, Wazuh, SIEM, Sistem Pemantauan

ABSTRACT

A data center is a center for managing, storing and processing important data which includes sensitive information, business applications and technology infrastructure. Due to the importance of data centers in supporting organizational operations, their vulnerability to information security threats such as cyber attacks, unauthorized access has a serious impact on daily operations. The implementation of IDS is currently not optimal because in-depth analysis is difficult and requires experts to observe it. For this reason, an effective security monitoring system is needed on an Intrusion Detection System (IDS) based on Security Information and Event Management (SIEM) using the Wazuh platform. IDS plays an important role in detecting network security threats, while SIEM provides the ability to integrate and analyze security data from various sources. This research designs and implements Wazuh integration with SIEM to strengthen detection and response capabilities against security threats. Experimental methodology is used to evaluate the performance of the developed system, with a focus on intrusion detection, log analysis and security event management. The research results show that the integration of Wazuh with SIEM provides significant improvements in monitoring capabilities and response to security threats, which will be a valuable contribution in ensuring the security of networks and sensitive data.

Keywords: : id, Wazuh, SIEM, Monitoring System

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Keamanan *data center* melibatkan upaya melindungi integritas, kerahasiaan, dan ketersediaan data yang disimpan. Ancaman siber semakin kompleks, mencakup serangan siber yang terus berkembang, pencurian data, serangan malware, serangan DDoS, dan berbagai insiden lain yang dapat mengganggu

operasi organisasi. Dengan tingginya risiko yang dihadapi *data center*, diperlukan upaya untuk melindunginya.

Dalam upaya untuk menjaga keamanan *data center*, organisasi seringkali mengandalkan *Intrusion Detection System* (IDS). IDS adalah alat yang digunakan untuk mendeteksi aktivitas mencurigakan dalam jaringan komputer atau sistem dan memberikan peringatan jika terdeteksi ancaman keamanan (Widodo & Aji, 2022). IDS adalah salah satu komponen utama dalam perlindungan *data center* dari serangan siber. Namun, *monitoring* jaringan IDS pada *data center* cederung lebih kompleks akibat banyaknya sistem IDS yang diterapkan pada *data center*. Hal ini menyebabkan tim *monitoring* jaringan kesulitan dalam menganalisis data. Selain itu, tampilan IDS yang kurang interaktif menjadi masalah yang sangat merepotkan. Analisis data yang dihasilkan oleh IDS juga dapat menjadi tugas yang sangat sulit. Tim *monitoring* keamanan harus mampu membedakan peringatan yang valid dari false positif, dan ini memerlukan keahlian dan pengalaman yang tinggi. Dalam skala *data center*, di mana volume data dan lalu lintas jaringan sangat besar, hal ini semakin sulit dan memakan waktu.

Untuk meningkatkan efisiensi analisis, dan memahami ancaman keamanan dengan lebih baik dapat menggunakan *Security Information and Event Management* (SIEM). SIEM adalah sistem yang dapat mengelola *log* serangan siber yang dihasilkan oleh beberapa sumber data (Muhammad et al., 2022). SIEM dapat menganalisis, mengaudit, menemukan dan mengantisipasi perangkat keras, jaringan dan semua acara aplikasi secara real time dari aplikasi jaringan. SIEM mengumpulkan data dari perangkat lunak, peralatan atau layanan *hosting*, menganalisis dan memanipulasi data *log* dan catatan keamanan, serta melaporkan keamanan (Hussein & Hamza, 2022). SIEM memungkinkan integrasi berbagai sumber data keamanan, termasuk data yang dihasilkan oleh beberapa IDS (Cinque et al., 2018). Selain itu SIEM dapat menyediakan laporan yang lebih terstruktur dan relevan. Hal ini dapat membantu tim *monitoring* keamanan dalam mengidentifikasi ancaman dengan lebih cepat dan efisien.

Salah satu platform SIEM yang telah menjadi sangat populer adalah Wazuh. Wazuh adalah platform keamanan dengan memberikan perlindungan berupa XDR (*eXtended Detection and Response*) dan *Security Information and Event Management* (SIEM) untuk *endpoint* dan *cloud workloads* (Wazuh, 2023). Wazuh merupakan perangkat berbasis *open-source* dengan fungsi untuk melakukan deteksi terhadap intrusi yang berbasis *host*. Wazuh bekerja dengan cara melakukan analisis terhadap *log*, melakukan pemeriksaan terhadap integritas, melakukan pemantauan kepada registri Windows, memberikan peringatan berbasis waktu, dan respons yang aktif (Pratama et al., 2022). Integrasi Wazuh dengan IDS dan penggunaan SIEM dapat menghasilkan alat yang komprehensif untuk pemantauan dan analisis keamanan di *data center*.

Beberapa penelitian telah dilakukan diantaranya oleh Muhammad Rijal Kamal (Kamal, 2022) yang mengimplementasikan SIEM dengan aplikasi Splunk untuk menganalisis tren ancaman siber di jaringan UII. Penelitian oleh Husnul Khotimah dkk (Khotimah et al., 2022) mengimplementasikan SIEM pada aplikasi SMS Center pada pemerintahan daerah provinsi NTB. Penelitian oleh Aldi Alpauji (Alpauji, 2021) menerapkan SIEM *elastic stack*.

Untuk itu, dikembangkan suatu *Security Information And Event Management (SIEM)* untuk *monitoring* kemanan pada IDS dalam lingkungan *data center*. SIEM yang digunakan adalah Wazuh sedangkan IDS sebagai *monitoring* keamanan yang digunakan adalah suricata. Pada penelitian ini dilakukan simulasi menggunakan tiga jenis pengujian yang meliputi *port scanning, bruteforce, dan denial of service*.

METODE PENELITIAN

Kebutuhan Sistem

Analisis kebutuhan adalah proses mengidentifikasi, memahami, dan mendokumentasikan kebutuhan atau persyaratan yang harus dipenuhi oleh suatu sistem atau proyek. Tujuan dari analisis kebutuhan adalah untuk memastikan bahwa sistem yang akan dibangun atau proyek yang akan dilaksanakan akan memenuhi kebutuhan penelitian. Pada penelitian ini dibutuhkan perangkat sebagai berikut:

1. Perangkat lunak

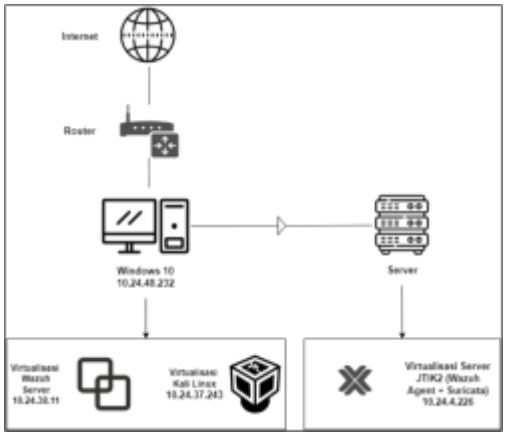
   Oracle VirtualBox : Virtualisasi untuk serangan
   Proxmox : Cloud pada data center
   Kali Linux : Sistem operasi untuk pengujian
   Wazuh : Platform SIEM
   Suricata : Intrusion Detection System

2. Perangkat keras

   Sistem operasi : Windows 10Pro
   Prosesor : Intel Core Intel® Core™ i7-8700U CPU @ 3.20GHz
   RAM : 16 Gb
   Storage : 1 TB

Perancangan Sistem

Rancangan sistem merupakan proses merencanakan dan menggambarkan struktur, fungsi, dan komponen suatu sistem yang akan dibangun. Berikut ini rancangan topo*log*i jaringan yang ditunjukan pada gambar 1



Gambar 1. Desain Sistem

Dari Gambar 1 dapat dijelaskan skenario desain sebagai berikut:

a. Satu buah PC dengan OS Windows 10 (10.24.48.232) digunakan untuk memjalankan virtualisasi Kali Linux, virtualisasi Wazuh server dan menjalankan *tools port scanning*. Serta melakukan remot pada *data center* dan mengakses *dashboard* Wazuh untuk melakukan monitoring.
b. Kali linux (10.24.37.243) sebagai OS untuk melakukan serangan bruteforce dan DoS.
c. Data Center (10.24.4.226) sebagai perangkat yang akan diserang. Server ini telah dipasang Wazuh agent dan Suricata

Pengujian

Pengujian dilakukan dengan mensimulasikan serangan siber terhadap data center yang telah dilengkapi Wazuh agent dan Suricata. Tujuan dari pengujian ini untuk mengevaluasi kemampuan sistem dalam mendeteksi dan mencatat aktivitas mencurigakan pada *log*ging dan *dashboard*. Jenis serangan yang digunakan mencakup *port scanning*, brute force, dan *Denial of Service (DoS)*. Adapun skenario pengujian secara rinci dijelaskan sebagai berikut:

a. Melakukan serangan *port scanning*

   Simulasi serangan *port scanning* dilakukan dari perangkat klien berbasis Windows 10 ke server target di data center yang telah terpasang Wazuh agent dan Suricata. Serangan ini bertujuan untuk mengidentifikasi *port* yang terbuka serta layanan yang berjalan pada server target. *Tools* yang digunakan dalam proses scanning ini adalah Zenmap dan NetScanTools demo, yang masing-masing melakukan pemindaian terhadap *port* dan protokol layanan menggunakan metode TCP SYN, service version detection, dan enumeration lainnya.

b. Monitoring dan Analisis *Log Port scanning*

   Setelah serangan *port scanning* dilakukan, sistem keamanan yang terdiri dari Suricata dan Wazuh bertugas mendeteksi aktivitas tersebut. Suricata akan menangkap signature-based intrusion dari aktivitas scanning, yang kemudian dikirimkan melalui Wazuh agent ke server Wazuh untuk dianalisis lebih lanjut. Hasil dari analisis *log* ini akan divisualisasikan melalui Wazuh *dashboard*, termasuk informasi terkait sumber serangan, jenis protokol, serta rule ID yang sesuai dengan pola serangan..

c. Melakukan serangan bruteforce

   Serangan brute force disimulasikan dari perangkat berbasis Kali Linux yang ditujukan ke *data center*. Serangan ini bertujuan untuk menguji kekuatan autentikasi dengan mencoba kombinasi *username* dan *password* secara berulang-ulang menggunakan *tools* Hydra dan Metasploit Framework. Modul-modul yang digunakan mencakup *auxiliary/scanner/ssh/ssh_login* dan ftp_*log*in, dengan target layanan SSH atau FTP yang tersedia di *data center*.

HASIL DAN PEMBAHASAN

Pengujian *Port scanning*

Pengujian *port scanning* dilakukan untuk mengidentifikasi *port* terbuka serta layanan yang berjalan pada server di lingkungan data center. Pengujian ini menggunakan dua perangkat lunak, yaitu Zenmap dan NetScanTools demo, yang dijalankan dari sistem operasi Windows 10 sebagai sumber serangan. Target pengujian adalah data center yang telah terpasang Wazuh agent dan Suricata. Tabel 1 menunjukan hasil serangan *port scanning* pada Zenmap dan NetScanTools.

Table 1. Hasl serangan *Port scanning*

Tools	**Hasil deteksi**	**Deskripsi**
Netscan	*Alert - ET SCAN Suspicious inbound to MSSQL port 1433*	adanya *request* lalu lintas mencurigakan yang masuk pada *port* 1433 MSSQL.
	Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306	adanya *request* lalu lintas mencurigakan yang masuk pada *port* 3306 mySQL.
	Suricata: Alert - Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	*Alert* ini mendeteksi adanya *request* lalu lintas mencurigakan yang masuk pada *port* 5432 PostgreSQL.
Zenmap	*Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)*	adanya *scan* yang dilakukan oleh *Nmap Scripting Engine* pada *port* 80 dan 3128.
	Alert - ET SCAN Suspicious inbound to mySQL port 3306	adanya *request* lalu lintas mencurigakan pada *port* 3306 mySQL.
	Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	adanya *request* lalu lintas mencurigakan pada *port* 5432 PostgreSQL.
	Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521	adanya *request* lalu lintas mencurigakan pada *port* 1521 Oracle SQL.
	Alert-ETSCAN Suspicious inbound to MSSQL port 1433	adanya *request* lalu lintas mencurigakan yang masuk pada *port* 1433 MSSQL.
	Suricata: Alert - ET SCAN Potential VNC Scan 5900-5920	adanya kemungkinan *scan* yang dilakukan pada VNC yang masuk pada *port* 5915.
	Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820	*Alert* ini mendeteksi adanya kemungkinan *scan* yang dilakukan pada VNC pada *port* 5801.
	Suricata: Alert ET SCAN Potential SSH Scan	adanya kemungkinan scan yang dilakukan pada SSH yang masuk pada *port* 22.
	Suricata: Alert - GPL RPC portmap listing TCP 111	*Alert* ini mendeteksi adanya proses *mapping* yang dilakukan pada RPC (*Remote Procedure Call*) dengan menggunakan *port* 111.

Pengujian Bruteforce

Pengujian serangan bruteforce dilakukan dengan tujuan untuk memperoleh kredensial autentikasi yang valid (username dan password) pada data center, sekaligus menguji efektivitas sistem Wazuh agent dan Suricata. Serangan dilakukan dari perangkat berbasis Kali Linux dengan memanfaatkan dua *tools* Hydra dan Metasploit Framework.

Pada tahap pengujian, Hydra digunakan untuk melakukan serangan terhadap layanan SSH yang berjalan pada data center dengan *dictionary attack*, menggunakan daftar kombinasi username dan password dari file wordlist. Selain itu, modul auxiliary/scanner/ssh/ssh_*log*in dari Metasploit digunakan sebagai alternatif metode serangan yang memiliki kemampuan enumerasi serta *log*ging percobaan autentikasi secara terstruktur Tabel 2 menunjukan hasil serangan bruteforce

Table 2. Hasl serangan BruteForce

Tools	**Hasil deteksi**	**Deskripsi**
Hydra	*sshd: Attempt to login using a non-existent user*	*Alert* ini mendeteksi terjadinya proses *log*in dengan menggunakan user yang tidak terdaftar pada perangkat..
	PAM: User login failed	*Alert* ini mendeteksi terjadinya proses *login* yang gagal pada perangkat.
	PAM: Multiple failed logins in a small period of time	*Alert* ini mendeteksi terjadinya proses *log*in yang gagal pada perangkat dalam jangka waktu yang pendek.
	sshd: brute force trying to get access to the system. Non existent user.	*Alert* ini mendeteksi terjadinya serangan bruteforce dengan membaca adanya beberapa *log* percobaan *log*in yang gagal dengan menggunakan user-user yang tidak dikenal
	Suricata: Alert- SURICATA Applayer Detect protocol only one direction	*Alert* ini mendeteksi adanya protokol yang terdeteksi pada Applayer yang bersifat hanya satu arah pada *port* 50116, 50122, 50124, 50126, 50128, 50136 dengan tujuan IP adalah 10.24.37.243
	Suricata: Alert-ET SCAN Potential SSH Scan	*Alert* ini mendeteksi adanya kemungkinan scan yang dilakukan pada SSH (*Secure Shell*) yang masuk pada *port* 22
	Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	*Alert* ini mendeteksi adanya serangan bruteforce yang terjadi melalui koneksi ssh berbasis LibSSH
	sshd: authentication failed.	*Alert* ini mendeteksi terjadinya autentikasi yang gagal karena penggunaan password yang salah
	Multiple authentication failures followed by a success.	*Alert* ini mendeteksi terjadinya beberapa autentikasi yang gagal karena penggunaan password yang salah diikuti dengan berhasilnya proses *log*in dengan menggunakan password yang benar
	PAM: Login session opened	*Alert* ini mendeteksi proses autentikasi yang berhasil dengan menggunakan *user* yang benar.
	PAM: Login session closed.	Berdasarkan hasil analisis Wazuh, *alert* ini menginformasikan bahwa sesi *log*in telah berakhir
Metasploit	*sshd: Attempt to login using a non-existent user*	*Alert* ini mendeteksi terjadinya proses *log*in dengan menggunakan user yang tidak terdaftar pada perangkat
	PAM: User login failed	*Alert* ini mendeteksi terjadinya proses *log*in yang gagal pada perangkat
	sshd: brute force trying to get access to the system	*Alert* ini mendeteksi terjadinya serangan bruteforce dengan membaca adanya beberapa *log* percobaan *log*in yang gagal dengan menggunakan user-user yang tidak dikenal.

Tools	**Hasil deteksi**	**Deskripsi**
	Suricata: Alert-ET SCAN Potential SSH Scan	*Alert* ini mendeteksi adanya kemungkinan scan yang dilakukan pada SSH (Secure Shell) yang masuk pada *port* 22
	PAM: Multiple failed logins in a small period of time.	*Alert* ini mendeteksi terjadinya proses *login* yang gagal pada perangkat dalam jangka waktu yang pendek.
	sshd: authentication failed	*Alert* ini mendeteksi terjadinya autentikasi yang gagal karena penggunaan password yang salah
	Multiple authentication failures followed by a success.	*Alert* ini mendeteksi terjadinya beberapa autentikasi yang gagal karena penggunaan password yang salah diikuti dengan berhasilnya proses *log*in dengan menggunakan password yang benar
	PAM: Login session opened	*Alert* ini mendeteksi proses autentikasi yang berhasil dengan menggunakan user yang benar.

Pengujian DoS

Pengujian serangan *Denial of Service (DoS)* dilakukan untuk menguji kemampuan sistem keamanan yang telah diimplementasikan dalam mendeteksi dan merespons serangan yang bertujuan untuk mengganggu ketersediaan layanan pada server. Serangan ini bekerja dengan membebani sumber daya sistem dengan lalu lintas data secara berlebihan sehingga server menjadi lambat atau tidak dapat merespons permintaan secara normal.

Pada pengujian ini, dua *tools* digunakan, yaitu LOIC (*Low Orbit Ion Cannon*) dan Hping3. LOIC digunakan untuk menghasilkan trafik secara masif dengan metode HTTP, TCP, atau UDP flooding secara terus-menerus ke alamat IP target, sedangkan Hping3 digunakan untuk mensimulasikan serangan berbasis protokol, seperti TCP SYN Flood, yang dirancang untuk membanjiri *port* tertentu. Tabel 3 menunjukan hasil serangan DoS Pada data center yang terdeteksi oleh Wazuh dan Suricata.

Table 3. Hasl serangan DoS

Tools	**Hasil deteksi**	**Deskripsi**
LOIC	*Suricata: Alert -SURICATA HTTP Request line incomplete*	*Alert* ini mendeteksi adanya request http yang dilakukan dari Serangan DoS menggunakan protokol http. Serangan ini mengirimkan request http yang tidak komplet kepada perangkat sehingga tidak dapat diproses..
	Suricata: Alert - SURICATA Applayer Detect protocol only one direction	*Alert* ini mendeteksi adanya protokol yang terdeteksi pada Applayer yang bersifat hanya satu arah yaitu protokol http pada *port* 80.
	Suricata: Alert - SURICATA HTTP request buffer too long	*Alert* ini mendeteksi adanya protokol yang terdeteksi pada Applayer yang bersifat hanya satu arah yaitu protokol http *port* 80.
Hping3	*Suricata: Alert – SURICATA STREAM 3way handshake*	mendeteksi adanya request paket SYN (Synchronize) dari serangan DoS menggunakan protokol http yang

	SYN resend different seq on SYN recv	ditujukan kepada IP 10.24.4.226 pada *port* 80. Serangan ini mengirimkan request paket SYN secara cepat sehingga tidak dapat diproses
	Suricata: Alert - SURICATA STREAM 3way handshake SYNACK resend with different ack	*Alert* ini mendeteksi adanya pengiriman paket ACK yang berbeda kepada IP 10.24.37.243. Pengiriman paket ini dilakukan karena paket ACK sebelumnya tidak sampai kepada target

Pembahasan

Pengujian terhadap tiga jenis serangan—*port scanning, brute force, dan Denial of Service (DoS)*—menunjukkan bahwa sistem keamanan yang terdiri atas Wazuh dan Suricata memiliki efektivitas yang berbeda dalam mendeteksi dan melaporkan serangan berdasarkan karakteristik masing-masing. Pada serangan *port scanning* yang dilakukan menggunakan Zenmap dan NetScanTools, hanya Suricata yang mampu mendeteksi aktivitas ini. Hal ini disebabkan oleh kemampuan Suricata dalam melakukan inspeksi terhadap lalu lintas jaringan secara real-time, sehingga dapat mengenali pola pemindaian *port* yang dilakukan oleh kedua *tools* tersebut. Wazuh, yang bergantung pada *log* sistem *host*, tidak secara eksplisit menangkap aktivitas ini, namun *alert* dari Suricata tetap berhasil ditampilkan pada Wazuh *dashboard* seperti pada Gambar 2.



Gambar 2. *Dashboard* Wazuh saat mendeteksi *Port scanning*

Pada pengujian serangan brute force menggunakan Hydra dan Metasploit terhadap layanan SSH (*port* 22), seluruh komponen sistem—baik Wazuh, Suricata, maupun Wazuh *dashboard*—berhasil mendeteksi dan mencatat aktivitas serangan. Ini menunjukkan efektivitas integrasi antara sistem deteksi berbasis *host* (Wazuh) dan berbasis jaringan (Suricata) dalam mengidentifikasi upaya *log*in berulang yang mencurigakan. *Log* autentikasi yang gagal dari sistem target dikumpulkan oleh Wazuh agent, sementara Suricata mengidentifikasi pola anomali lalu lintas SSH, yang secara bersama-sama menghasilkan notifikasi keamanan pada Wazuh *dashboard* seperti yang ditunjukan pada Gambar 3.



Gambar 2. *Dashboard* Wazuh saat mendeteksi *Bruteforce*

Pada serangan *Denial of Service (DoS)* yang disimulasikan menggunakan LOIC dan Hping3, Suricata menunjukkan kinerja yang lebih dominan dibandingkan Wazuh. Serangan yang menyebabkan lonjakan trafik jaringan secara drastis berhasil diidentifikasi oleh Suricata sebagai potensi serangan DoS, berdasarkan *signature traffic* dan volume koneksi abnormal. Meskipun Wazuh tidak secara langsung mendeteksi aktivitas ini melalui *log* sistem, informasi dari Suricata tetap dapat diteruskan melalui Wazuh agent dan divisualisasikan dalam Wazuh *dashboard* seperti pada Gambar 3.



Gambar 3. *Dashboard* Wazuh saat mendeteksi *DoS*.

KESIMPULAN

Berdasarkan hasil pengujian terhadap tiga jenis serangan siber, yaitu *port scanning*, *brute force*, dan *Denial of Service (DoS)*, dapat disimpulkan bahwa integrasi antara Wazuh dan Suricata mampu mendeteksi berbagai bentuk ancaman keamanan secara efektif, meskipun dengan karakteristik deteksi yang berbeda. Suricata menunjukkan kemampuan baik dalam mendeteksi serangan yang berbasis jaringan, seperti *port scanning* dan DoS, melalui analisis trafik secara *real-time*. Sementara itu, Wazuh lebih unggul dalam menangani serangan yang berkaitan dengan aktivitas sistem dan autentikasi, seperti brute force, dengan memanfaatkan *log* sistem *host*.

Deteksi terbaik terjadi pada serangan brute force, di mana kedua sistem, baik Wazuh maupun Suricata, mampu bekerja untuk menghasilkan notifikasi keamanan yang detail dan akurat melalui Wazuh *dashboard*. Hal ini membuktikan bahwa kombinasi antara pendekatan berbasis *host* dan jaringan yang efektif dalam membangun sistem pemantauan ancaman yang adaptif dan responsif. Visualisasi data yang ditampilkan pada Wazuh *dashboard* juga memberikan kemudahan dalam analisis insiden dan pengambilan keputusan keamanan secara cepat.

Secara keseluruhan, implementasi sistem deteksi yang menggabungkan Wazuh dan Suricata terbukti efektif dalam meningkatkan visibilitas dan kesiapan infrastruktur data center terhadap berbagai vektor serangan siber. Hasil pengujian ini mendukung pentingnya penerapan keamanan yang terintegrasi dan dapat disesuaikan dengan karakteristik ancaman, untuk memastikan ketersediaan layanan dan perlindungan terhadap sistem informasi.

REFERENCES

Alpauji, A. (2021). *Implementasi Security Information And Event Management Menggunakan Tools Elastic Serta Suricata Sebagai Sistem Pendeteksi Intrusi Pada Sistem Operasi Linux Ubuntu Di Perusahaan Pt. Itsec Asia*. Politeknik Negeri Jakarta.

Cinque, M., Cotroneo, D., & Pecchia, A. (2018). Challenges And Directions In Security Information And Event Management (Siem). *Proceedings - 29th Ieee International Symposium On Software Reliability Engineering Workshops, Issrew 2018*, 95–99. Https://Doi.Org/10.1109/Issrew.2018.00-24

Hussein, M. A., & Hamza, E. K. (2022). Secure Mechanism Applied To Big Data For Iiot By Using Security Event And Information Management System (Siem). *International Journal Of Intelligent Engineering And Systems*, *15*(6), 667–681. Https://Doi.Org/10.22266/Ijies2022.1231.59

Kamal, M. R. (2022). *Implementasi Security Information And Event Management (Siem) Dengan Splunk Untuk Analisis Tren Ancaman Siber Pada Jaringan Uii*.

Khotimah, H., Bimantoro, F., Silas Kabanga, R., Bagus, I., & Widiartha, K. (2022). *Implementasi Security Information And Event Management (Siem) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat (Implementation Of Security Information And Event Management (Siem) In The Sms Center Application For The West Nusa Tengg. 3*(2), 213–219. Http://Begawe.Unram.Ac.Id/Index.Php/Jbti/

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2022). Integrated Security Information And Event Management (Siem) With Intrusion Detection System (Ids) For Live Analysis Based On Machine Learning. *Procedia Computer Science*, *217*(2022), 1406–1415. Https://Doi.Org/10.1016/J.Procs.2022.12.339

Pratama, M. D., Nova, F., & Prayama, D. (2022). Wazuh Sebagai *Log* Event Management Dan Deteksi Celah Keamanan Pada Server Dari Serangan Dos. *Jitsi : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. Https://Doi.Org/10.30630/Jitsi.3.1.59

Wazuh. (2023). *Getting Started With Wazuh*. Https://Documentation.Wazuh.Com/Current/Getting-Started/Index.Html

Widodo, T., & Aji, A. S. (2022). Pemanfaatan Network Forensic Investigation Framework Untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (Ids). *Jiska (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 46–55. Https://Doi.Org/10.14421/Jiska.2022.7.1.46-55