Available *online* at : http://jitce.fti.unand.ac.id/

JITCE (Journal of Information Technology and Computer Engineering)

| ISSN (Online) 2599-1663 |

Research Article

Real-time Defense Against Cyber Threats: Analyzing Wazuh's Effectiveness in Server Monitoring

Alde Alanda[1] *,H.A. Mooduto*[1]*, Ronal Hadi*[1]

[1]*Information Technology Department Politeknik Negeri Padang, Kampus Limau Manis, Kota Padang 25163, Indonesia*

ARTICLE INFORMATION

Received: February 8th, 2023
Revised: August 24th, 2023
Available online: September 30th , 2023

KEYWORDS

Cloud-computing security, server monitoring, Wazuh

CORRESPONDENCE

Phone: +62 (0751) 12345678

E-mail: alde@pnp.ac.id

ABSTRACT

As cloud computing grows exponentially, organizations face escalating cybersecurity challenges due to increased cyber threats and attacks on cloud-based networks. Monitoring cloud servers is one action that can be taken to improve the security. This can be done with the help of various server monitoring tools, such as Wazuh. The study investigates Wazuh's effectiveness in real-time monitoring of three AWS EC2 instance-based cloud servers. Wazuh's capabilities such as log data collection, malware detection, active response automation, and Docker container monitoring, are examined. The research reveals detailed insights into user activities, web server access, and database operations. Wazuh proves adept at tracking file integrity, detecting malware, and responding actively, as evidenced by the 342 alerts generated during a 24-hour monitoring period. The result shows that Wazuh is a particularly effective tool for protecting cloud environments from cyberattacks because it provides quick and ongoing security monitoring, which is essential for securing intricate cloud infrastructures.

INTRODUCTION

Cloud computing is a framework for facilitating and delivering services over the Internet [1]. Its primary goal is to offer computer services—like servers, storage, databases, networking, software, analytics, and intelligence—over the Internet. With cloud computing, organizations are not required to buy expensive hardware and software to set up physical on-site data centers. It automates organizations by storing their software systems and services on remote servers. Most organizations adopt this trend, increasing with every passing year [2]. According to Precedence Research's analysis, the worldwide cloud computing industry was estimated at USD 480 billion in 2022 and is projected to grow at a compound annual growth rate of 17% from 2023 to 2032, reaching USD 2297.37 billion [3].

However, there are some security risks and protection issues with it. [1]. Cybercriminals may attack the cloud computing servers' data, services, and applications. The organization affected by cyberattacks loses its financial and reputation[4]. According to research by Trend Micro Incorporated (TYO: 4704; TSE: 4704), cloud criminals are using cloud services and technology to speed up attacks, decreasing the time enterprises have to identify and respond to a breach[5]. Check Point Research's 2023 Security Report reveals a significant surge in the frequency of attacks on cloud-based networks per organization. The data indicates a substantial 48% increase in such attacks in 2022 when compared to the previous year[6].

Maintaining a high-security level is the responsibility of the end-user and the cloud computing server [7]. One effort is to monitor the server. Server monitoring is necessary to ensure that essential and confidential data remains safe and is not damaged or stolen by cybercriminals. This can be done with the help of various server monitoring tools, one of which is Wazuh. Wazuh is an open-source security platform known for its comprehensive security monitoring, threat detection, and incident response capabilities. To inspect for potential cybersecurity vulnerabilities extensively, the platform centrally gathers and integrates security-related data from multiple sources, including logs, events, and network traffic. Wazuh also integrates proactive and reactive response mechanisms with real-time threat detection to handle security events and swiftly eliminate possible threats[8].

This study conducted testing and analyzed the use of Wazuh in

https://doi.org/10.25077/jitce.7.02.56-62.2023

gathering information and detecting cyber-attacks in real-time. Three servers with different functions monitor file integrity, active response, and docker monitoring using Wazuh.

METHOD

Wazuh is capable of numerous monitoring tasks. Wazuh's capabilities will be put to the test in this study, including[9]:

a) Log data collection: gathering and consolidating logs from different endpoints.

b) Malware detection: examining a computer system or network to check for the presence of harmful files and software.

c) Active response: automate response actions based on specific triggers

d) Docker container monitoring: provides insight into the activities of the containers, such as network connections, file system changes, and process executions.

This study created a cloud computing system using AWS (Amazon Web Services). As shown in Figure 1, four servers were built: one as Wazuh manager and the other three as Wazuh agents. Wazuh manager is the system that analyzes the data received from all registered agents and triggers alerts when an event coincides with a rule [10]. Meanwhile, the Wazuh Agent is installed on the endpoint device to take system readings, collect logs, and send them to the Wazuh Manager. In this study, the names of the three agent servers are by each server's application or purpose, i.e., "Lamp" as agent-1, "Amazon" as agent-2, and "Docker" as agent-3.

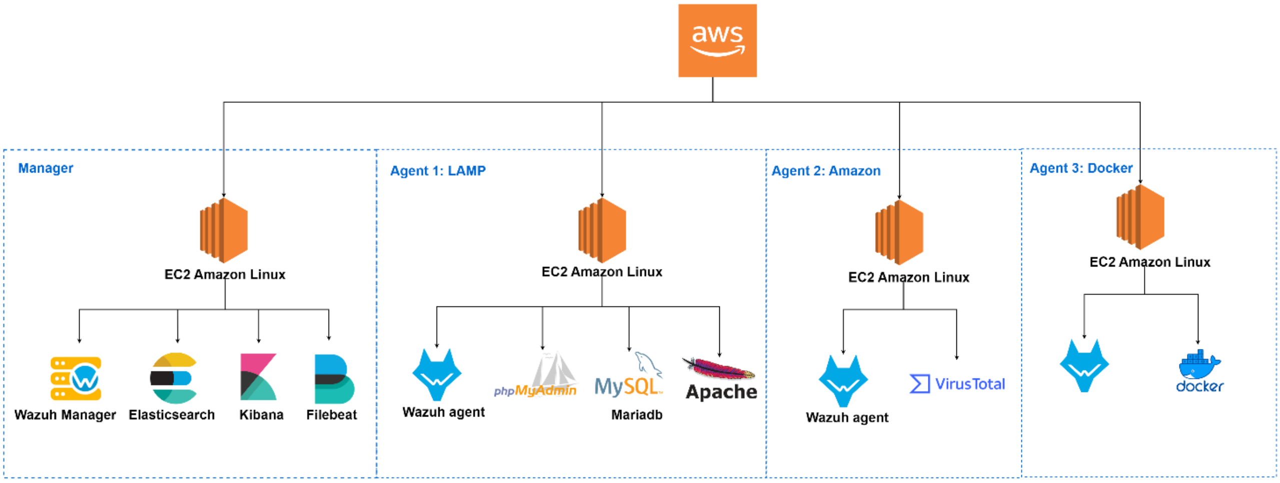

Figure 1 Architecture of the cloud-computing system

The four servers were constructed utilizing AWS EC2 Instances (Elastic Compute Cloud). EC2 stands as a platform facilitating the deployment of servers in the cloud. It is scalable, allowing significant adjustments in the number of deployed server instances to meet changing computational requirements. Within Amazon's EC2, an instance denotes a virtual server employed for running applications, akin to a distinct component of a large computer with storage, network connectivity, operating system, and more. [11]. The specification for all servers is shown in Table 1.

Table 10 Servers Specification in AWS EC2 Instances

Item	Manager	Agent1	Agent2	Agent3
Processor	Intel® Xeon® CPU E5-2676 v3 @2.40GHz	Intel® Xeon® CPU E5-2676 v3 @2.40GHz	Intel® Xeon® CPU E5-2676 v3 @2.40GHz	Intel® Xeon® CPU E5-2676 v3 @2.40GHz
Memory	4GB	2GB	2GB	4GB
Operating System	Amazon Linux 8	Amazon Linux 8	Amazon Linux 8	Amazon Linux 8
Hardisk	8GB	8GB	8GB	8GB
Wazuh version	Wazuh *manager v4.2.1*	Wazuh *agent v4.2.1*	Wazuh *agent v4.2.1*	Wazuh *agent v4.2.1*

Wazuh Manager

This server consists of Wazuh Manager software and Elastic Stack tools (i.e. Elasticsearch, Kibana, and Filebeat):

1). Wazuh manager

2). Elasticsearch: is a distributed search and analytics engine built on Apache Lucene[12].

3). Filebeat: an agent installed on the server to forward and centralize log data. It monitors the log files to collect the log events and forward them to Elasticsearch [13].

4). Kibana: is a flexible and intuitive web interface for hosting and visualizing events and archives stored in Elasticsearch[14].

Wazuh Agents

On each EC2 instance allocated as an agent, the Wazuh Agent software and other tools are installed. A more detailed explanation of each agent is discussed below. After each agent is complete, it is deployed to the Wazuh manager server. Three agents can be seen on the Wazuh manager with the following information, Table 2.

Table 11 The Agents of the system

id	Name	IP
006	Docker	172.31.18.204
019	Amazon	172.31.19.108
020	Lamp	172.31.22.128

Agent-1: LAMP

In this study, this server is named after its framework, a popular website framework comprising four open-source components: Linux, Apache, MySQL, and PHP, abbreviated as LAMP. The agent acts as a web server. This agent consists of 1) Wazuh agent software; 2) Apache, which is one of the most popular web server software; 3) Mariadb as a database; and 4) phpMyadmin as a server-side scripting language.

Agent 2: Amazon

The server acts as a computer on which the VirusTotal software is installed. VirusTotal is a popular online anti-malware scanning service. It applies more than 70 anti-malware engines to analyze user-submitted files and returns back engines’ detection results [10]. It also scan the URL to identify websites that conduct phishing or distribute malicious software. VirusTotal forwards URLs to vendors, such as online scanning services or anti-virus engines, after they receive a URL submitted using the scan API. The VirusTotal database will hold the findings of the scanning process [11].

Agent 3: Docker

This server acts as a docker server. Docker is a platform for containerization. Containerization is a technology that combines the application, related dependencies, and system libraries organized to build in the form of a container. The applications that are built and organized can be executed and deployed as a container, which makes sure that the application works in every environment [15].

RESULTS AND DISCUSSION

Agent-1: LAMP

User login

The first scenario is that a user will attempt to log on to the server as root. An incorrect password is entered when prompted for a password, and the user needs to log in. In the Wazuh web interface, there will be an incoming event from the server agent activity that the wrong root password was entered. Wazuh displays this information on Security events with detailed data shown in Table 3. In the full_log section, we can find that “authentication failure” information indicates a login failure.

The second scenario is that the user accesses by entering the correct password. In this case, information is displayed in Table 3. It can be seen that there is information in the full_log: Accepted publickey for ec2-user from 182.1.56.115 port 56594, indicating that the user has successfully logged in.

Table 12 User login log information- authentication failure

agent.id	: 020
agent.ip	: 172.31.22.128
agent. Name	: lamp
data.dstuser	: root
data.euid	: 0
data.logname	: ec2-user
data.srcuser	: ec2-user
data.tty	: pts/0
data.uid	: 1000
decoder.name	: pam
full_log	:Sept23 02:18:06 LAMP su:pam_unix(su:auth): authentication failure: logname=ec2-user uid:1000 tty=pts/0 ruser=ec2-user rhosst= user=root
id	: 1632363487.20128
input.type	: log
location	: var/log/secure
manager.name	: Usermanager

Table 13 User login log information- authentication failure

geolocation.city_name	: Medan
geolocation.county_name	: Indonesia

geolocation.location	: {
	“lon”: 98.6629
	“lat” : 3.5844
	}

geolocation.region_name	: North Sumatera
agent.id	: 020
agent.ip	: 172.31.22.128
agent.name	: lamp
data.dstuser	: ec2-user
data.scrip	: 182.1.56.115
decoder.name	: sshd
decoder.parent	: sshd
full_log	: Sept23 02:27:18 LAMP sshd[4658]: Accepted publickey for ec2-user from 182.1.56.115 port 56594 ssh2: RSA SHA256: vMQ4Cd0pSZ0ZM/h8IdCgGN90p1K0d3POTUpSjGGhnYA
input.type	: log
location	: /var/log/secire
manager.name	: Usermanager
predecoder.hostname	: LAMP
predecoder.program_name	: sshd
predecoder.timestamp	: Sep 23 02:27:18
rule.description	: sshd: authentication success
rule.firedtimes	: 2
rule.gdpr	: IV_32.2
rule.gpg13	: 7.1, 7.2
rule.groups	: syslog, sshd, authentication_success
rule.hipaa	: 164.312.b
rule.id	: 5715
rule.level	: 3
rule.mail	: false
rule.mitre.id	: T1078, T1021
rule.mitre.tactic	: Defense Evasion, Initial Access, Persistence, Privilege Escalation, Lateral Movement

https://doi.org/10.25077/jitce.7.02.56-62.2023

Webserver access

In this test, the user accesses a website with an IP address of 114.125.7 using the GET protocol. Wazuh monitors this activity with detailed information shown in Table 5.

Table 14 Webserver access log information

agent.id	: 020
agent.ip	: 172.31.22.128
agent.name	: lamp
data.id	: 304
data.protocol	: GET
data.srcip	: 114.125.7.171
data.url	: /
decoder.name	: web-accesslog
full_log	: 114.125.7.171 - - [30/Sept/2022: 18:02:32 +0000] “GET / HTTP/1.1” 304 - “-“ “Mozilla/5.0 (Windows NT 10.0: Win64: x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.62 Safari/537.36”
id	163302453.221620
input.type	Log
location	/vat/log/httpd/access_log
manager.name	Usermanager
rule.description	Web server access
rule.firedtimes	1
rule.groups	Web, accesslog

Database creation

In this test, the user accesses phpMyAdmin and creates a database called "mahasiswa". Inside the database, the user creates a table called "datadiri". In the Wazuh Manager integrity monitoring section, an event will be generated by the user's activity, with detailed information shown in Table 6. This table shows that there has been an addition to the table in the database, which is summarised in the full_log section: '/var/lib/mysql.student/datadir.frm' added.

Table 15 Database creation log information

agent.id	: 020
agent.ip	: 172.31.22.128
agent.name	: lamp
decoder.name	: syscheck_new_entry
full_log	:File ‘/var/lib/mysql.mahasiswa/datadir.frm ‘added Mode: Realtime
id	:1632366815.100336
input.type	: log
location	: syscheck
manager.name	: Usermanager
rule.description	: File added to the system
rule.firedtimes	: 2
rule.gdpr	: II_5.1.f
rule.gpg13	: 4.11
rule.groups	:Ossec, syscheck, syscheck_entry)added, syscheck_file
rule.hipaa	: 164.312.c.1, 164.312.c.2
rule.id	: 554
rule.level	: 5

Agent 2: Amazone

File addition and deletion

In this test, the agent has created a file named ”uji.txt” in the home directory. In the Wazuh Manager integrity monitoring section, we can see an incoming event with the agent name Amazon-Agent, and the location of the creation of the Uji.txt file is in the home directory with a description that the file has been added, shows in Table 7.

Table 16 File addition log information

agent.id	: 019
agent.ip	: 172.31.19.108
agent. name	: Amazon-Agent
decoder.name	: syscheck_new_entry
full_log	: File ‘/home/uji.txt’added Mode: whodata
id	: 1632465682.638027
input.type	: log
location	: syschec
manager.name	: Usermanager
rule.descriprion	: file added to the system
rule.firedtimes	: 1
rule.gdpr	: II_5.1.f
rule.gpg13	: 4.11

Meanwhile, when a file is deleted, the log information about this deletion activity is shown in Table 8. In the full.log section, we can see that the file '/home/uji.txt' was deleted.

Table 17. File deletion log information

agent.id	: 019
agent.ip	: 172.31.19.108
agent. Name	: Amazon-Agent
Decoder.name	: syscheck_deleted
Full_log	: File ‘/home/uji.txt’ deleted Mode: whodata
Id	: 1632466116.647805
Input.type	: log
Location	: syscheck
Manager.name	: Usermanager
Rule.descriprion	: file deleted
Rule.firedtimes	: 4
Rule.gdpr	: II_5.1.f
Rule.gpg13	: 4.11

Malware Detection and Active Responses

This test was conducted to assess Wazuh's ability to detect and provide action against malware. In this test, ten viruses were first downloaded by the Wazuh agent. Then, the Wazuh manager will display a malware download event. Downloaded files will generate information that varies depending on how much malware is detected in the file.

VirusTotal works to detect malware downloaded by agents. Downloaded files will generate information that varies depending on how much malware is detected in the file. If any positive malware is found, VirusTotal will display the amount and type of malware on the VirusTotal dashboard. Then, active-response will work to delete files detected by VirusTotal containing dangerous malware. Then, if no positive malware is found from the downloaded file, the active response will not execute the file and will be allowed to be downloaded by the agent. The virus detected and the response are shown in Table 9.

Based on the results of this test, of the ten viruses that were downloaded, three were left to be downloaded. This is because the file is not in the VirusTotal Database, and there are no records in the VirusTotal Database. Meanwhile, seven other viruses were removed by active-response.

Table 18 Malware detection and active respons in VirusTotal

No	Malware	Malware data	Description
1.	240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762.zip	10 engines detect malicious files	Active-response deletes the file located at root/240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762.zip
2.	YW4BB6TMALWARESAMPLE.rar	3 engines detected malicious files	active-response removes the threat located at /root/YW4BB6TMALWARESAMPLE.rar
3.	maltrieve_pdfs_20140603.rar	No record in VirusTotal Database	The file is allowed to download.
4.	yitaly.exe.zip	2 engines detected malicious files	active-response removes the threat located at /root/yitaly.exe.zip
5.	942e275de833c747d0f8a5ebe519c62157c1136cbf467d079d7f84890018aa84.zip	No record in VirusTotal Database	The file is allowed to download.
6.	45a4bd970485ca539c95d746fbe8866f868972dcf7f1d196199ed7ea8b50be5b.zip	No positives found	The file is allowed to download.
7.	Eicar.com	56 engines detect malicious files	active-response removes the threat located at /root/eicar.com
8.	0.exe.zip	2 engines detect malicious files	active-response removes the threat located at /root/0.exe.zip
9.	340s.exe.zip	10 engines detect malicious files	active-response removes the threat located at /root/340s.exe.zip
10.	eh.exe.zip	10 engines detect malicious files	active-response removes the threat located at /root/eh.exe.zip

Agent 3: Docker

Docker container monitoirng

In this test, there are two containers running on Docker, namely phpMyAdmin and MariaDB. Then, the kill action is given to the phpMyAdmin container. Docker activity information when killing phpMyAdmin can be seen in the following Table 10.

Table 19 Log information of the kill activity

Agent.id	: 006
Agent.ip	: 172.31.18/204
Agent.name	: Docker-lamp
data.docker.Action	: Kill
Data.docker.Actor.Attributes.image	: Phpmyadmin:5.1.1
Data.docker.Actor.Attributes.name	: My-phpmyadmin
Data.docker.Actor.Attributes.org.opencontainers.image.authors	: The phpMyAdmin Team <developers@phpmyadmin.net>
Data.docker.Actor.Attributes.org.opencontainers.image. description	: Run phpMyAdmin with Alpine, Apache and PHP FPM
Data.docker.Actor.Attributes.org.opencontainers.image.documentation	: https://github.com/phpmyadmin.docker#readme

Monitoring agents activity

In this study, testing was carried out for 24 hours on the agents's activity. From the tests conducted, there were 342 alerts detected by Wazuh. The detected alerts start from level 3 to level 12, as shwon in Figure 2.

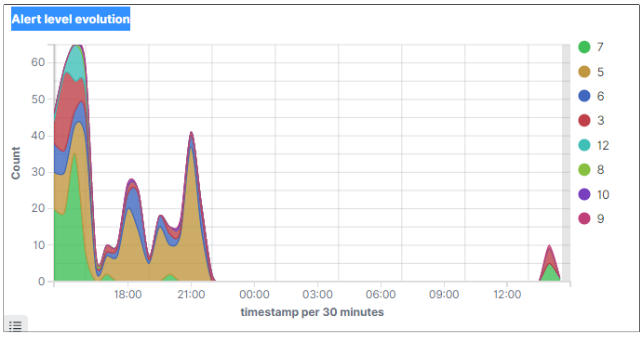

Fig 2. Alert Classification

Based on the number of detected alerts can be grouped based on the type of alerts detected within 24 hours, as shown in Figure 3 and Table 11. From the results of the grouping of alert types, it can be seen that 53% of the detected alerts were brute-force attacks

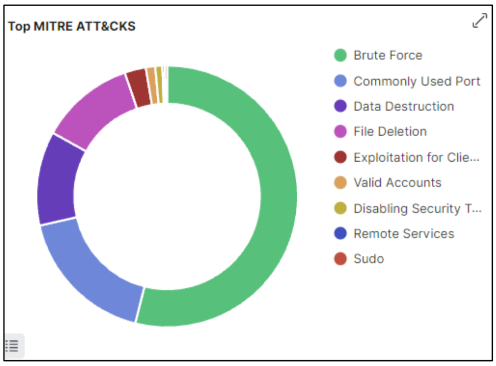

Figure 3. Alert Clasification

Tabel 11 Alert Clasification

No	Alert Type	Number of Alert
1.	Brute Force	185 (53.94%)
2	Commonly Used Port	60 (17.49%)
3	Data Destruction	40 (11.66%)
4	File Deletion	40 (11.66%)
5	Exploitation for Client	9 (2.62%)
6	Valid Account	4 (1.17%)
7	Disabling Security	3 (0.87%)
8	Sudo	1 (0.29%)
Total		342

In this study, tests were carried out on agent activity displayed on the dashboard, as shown in Figure 12. Every 30 minutes, there will be several alerts received by the agent. The agent that receives the most alerts at 15.00 is Amazon-Agent, with 20 alerts. Lamp-agent with 7 alerts, then docker-lamp with 3 alerts. Then at 15.30, the number changes again depending on the agent's activity, where Amazon-Agent gets 54 alerts, docker-lamp gets 7 alerts, and lamp-agent gets 4 alerts. This data will continue to change depending on the alerts each agent receives every 30 minutes.

CONCLUSIONS

This study demonstrates Wazuh's monitoring capabilities for three cloud servers constructed with AWS EC2 instances. The conclusion of this study shows that Wazuh has good capabilities in real-time monitoring three cloud servers built using EC2 instances from AWS. Wazuh is able to provide very detailed information related to logs, and can even track user activity including the location of the user. Wazuh's ability is also seen in providing detailed information related to accessing website pages. In the aspect of file integrity, Wazuh is effective in monitoring file creation, deletion, and changes to the server database. Malware detection capabilities and active response to malware based on alert level also look very good. In addition, Wazuh is able to monitor container activity in Docker, including kill actions on certain containers.

Wazuh can efficiently monitor server agents by offering a total of 342 alerts, as demonstrated by its 24 hours server monitoring. These findings demonstrate that Wazuh is capable of conducting responsive and constant monitoring of a wide range of actions that may jeopardize server security, in addition to providing trustworthy threat detection. Thus, the results of this study provide strong support for the effectiveness of Wazuh in the context of complex and dynamic server monitoring.

REFERENCES

[1] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electron.*, vol. 9, no. 9, pp. 1–25, 2020, doi: 10.3390/electronics9091379.

[2] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electron.*, vol. 11, no. 1, pp. 1–34, 2022, doi: 10.3390/electronics11010016.

[3] P. Research, "Cloud Computing Market Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023 – 2032," 2022. [Online]. Available: https://www.precedenceresearch.com/cloud-computing-market.

[4] H. F. El-Sofany, "A new cybersecurity approach for protecting cloud services against DDoS attacks," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 2, pp. 205–215, 2020, doi: 10.22266/ijies2020.0430.20.

[5] TrendMicro, "Cybercriminals Use Cloud Technology to Accelerate Business Attacks." [Online]. Available: https://newsroom.trendmicro.com/2020-11-16-Cybercriminals-Use-Cloud-Technology-to-Accelerate-Business-Attacks.

[6] Checkpoint, "Check Point Press Releases." https://www.checkpoint.com/press-releases/check-point-software-releases-its-2023-security-report-highlighting-rise-in-cyberattacks-and-disruptive-malware/.

[7] Y. A. Najm, S. Alsamaraee, and A. A. Jalal, "Cloud computing security for e-learning during COVID-19 pandemic," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 3, pp. 1610–1618, 2022, doi: 10.11591/ijeecs.v27.i3.pp1610-1618.

[8] M. Kaheh, D. K. Kholgh, and P. Kostakos, "Cyber Sentinel : Exploring Conversational Agents ' Role in Streamlining Security Tasks with GPT-4."

[9] Wazuh, "Malware detection." https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/index.html.

[10] Wazuh, "Wazuh Server Administration," 2023. https://documentation.wazuh.com/current/user-manual/manager/index.html (accessed Feb. 02, 2023).

[11] A. Choudhary, "A walkthrough of Amazon Elastic Compute Cloud (Amazon EC2): A Review," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 9, no. 11, pp. 93–97, 2021, doi: 10.22214/ijraset.2021.38764.

[12] AWS, "Elasticsearch," 2023. https://aws.amazon.com/what-is/elasticsearch/?nc1=h_ls (accessed Feb. 02, 2023).

[13] G. Calderon, G. del Campo, E. Saavedra, and A. Santamaría, "Monitoring Framework for the Performance Evaluation of an IoT Platform with Elasticsearch and Apache Kafka," *Inf. Syst. Front.*, 2023, doi: 10.1007/s10796-023-10409-2.

[14] Elastic, "Kibana—your window into Elastic," 2023. https://www.elastic.co/guide/en/kibana/current/introduction.html#introduction (accessed Feb. 05, 2023).

[15] A. M. Potdar, D. G. Narayan, S. Kengond, and M. M. Mulla, "Performance Evaluation of Docker Container and Virtual Machine," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1419–1428, 2020, doi: 10.1016/j.procs.2020.04.152.

AUTHORS BIOGRAPHY

Alde Alanda is a lecturer at the State Polytechnic of Padang. Currently, his research focus revolves around Computer Network, Network Security, Service Computing, and Cloud Computing.

https://doi.org/10.25077/jitce.7.02.56-62.2023