IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14162

TStrengthening Cybersecurity with Wazuh: Log-Based Threat Detection for a Resilient Digital World

Ranjana[1], Sarvottam Dixit[2], Pooja Tripathi[3]

Research Scholar, CSE, Mewar University, Chittorgarh, Rajasthan[1]

Professor, CSE, Mewar University, Chittorgarh, Rajasthan [2]

Professor, Co Supervisor, Mewar University, Rajasthan3

Abstract: The increasing sophistication of cybersecurity threats necessitates prompt detection and response by enterprises. An open-source security platform called Wazuh aids in efficient threat monitoring. Protecting vital systems and data requires effective threat detection, monitoring, and response.Among other things, it offers capabilities for malware detection, integrity checks, and log gathering. Conventional security solutions frequently operate independently, which might result in sluggish reactions and insufficient insights. In order to solve this, Wazuh offers a single platform that incorporates essential security functionalities like configuration evaluation, log analysis, intrusion detection, and vulnerability management. The major components of Wazuh—server, indexer, and dashboard—as well as how it gathers, analyzes, and presents data are described in this paper. Wazuh's modular design makes it simple to integrate with other platforms offering real-time detection and actionable insights to tackle modern security challenge**s**

Keywords: Wazuh, web-server, network, security, monitoring, attack.

.

I. INTRODUCTION

As organizations face more complex IT environments and increased cyber threats, Wazuh offers an open-source platform to simplify threat detection, compliance management, and incident response. Wash’s modular and scalable architecture enables organizations to monitor diverse environments, ranging from on-premises systems to cloud-based infrastructures, providing real-time insights and proactive threat mitigation. By combining advanced analytics with intuitive visualization capabilities, Wazuh empowers Security teams to identify and respond to anomalies swiftly. Traditional security tools often operate in silos, leading to fragmented insights and delayed responses. Wazuh addresses these challenges by offering a comprehensive, unified platform that integrates critical security functionalities such as log analysis, intrusion detection, vulnerability management, and configuration assessment.

This paper provides a detailed exploration of Wazuh’s core components including the Wazuh Server, Indexer, and Dashboard and explains the operational workflows that drive its effectiveness. The discussion highlights how Wazuh's architecture seamlessly integrates with endpoints and scales to meet the demands of modern IT ecosystems, offering a versatile and comprehensive solution for managing today’s security As organizations face more complex IT environments and increased cyber threats, Wazuh offers an open-source platform to simplify threat detection, compliance management, and incident response. Wash’s modular and scalable architecture enables organizations to monitor diverse environments, ranging from on-premises systems to cloud-based infrastructures, providing real-time insights and proactive threat mitigation. By combining advanced analytics with intuitive visualization capabilities, Wazuh empowers Security teams to identify and respond to anomalies swiftly. Traditional security tools often operate in silos, leading to fragmented insights and delayed responses. Wazuh addresses these challenges by offering a comprehensive, unified platform that integrates critical security functionalities such as log analysis, intrusion detection, vulnerability management, and configuration assessment.

This paper provides a detailed exploration of Wazuh’s core components including the Wazuh Server, Indexer, and Dashboard and explains the operational workflows that drive its effectiveness. The discussion highlights how Wazuh's architecture seamlessly integrates with endpoints and scales to meet the demands of modern IT ecosystems, offering a versatile and comprehensive solution for managing today’s security

.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

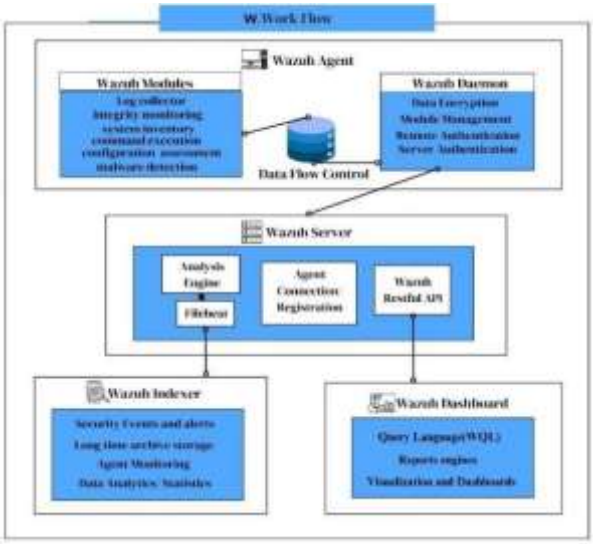
DOI: 10.17148/IJARCCE.2025.14162

II. WAZUH OVERVIEW

Wazuh is an open-source security platform that provides threat detection, security monitoring, and compliance management. By combining multiple security tools into one platform, Wazuh simplifies operations and creates a seamless approach to cybersecurity. Its modular and scalable design makes it suitable for organizations of all sizes, from small businesses to large enterprises with complex IT systemsYour paper must be in single column format with a space of 4.22mm (0.17") between columns.

III. WAZUH WORKFLOW

Wazuh is an open-source security platform that provides unified XDR and SIEM capabilities. Its workflow involves several key components working together to monitor, detect, and respond to security threats across an organization's infrastructure. Here's an overview of Wazuh's workflow



Wazuh Agents: Installed on monitored endpoints (servers, workstations, cloud instances, etc.), these agents collect security-related data, including log events, file integrity.
Data Collection: Agents continuously gather data from their respective endpoints.
Data Forwarding: The collected data is securely transmitted from the agents to the Wazuh Server. Communication between agents and the server is encrypted
Wazuh Server: It receives data from all connected agents. It performs real-time analysis, correlates events, detects anomalies, and generates alerts based on predefined rules and threat intelligence feeds.
Event Analysis and Correlation: The server analyses incoming data to identify potential security threats. It correlates events from different sources to detect complex attack patterns, policy violations, or suspicious activities that may indicate a security incident.
Alert Generation: When a potential threat is identified, the server generates an alert detailing the nature of the issue, affected systems, severity level, and recommended actions. It helps security teams to prioritize and respond to incidents effectively.
Data Indexing and Storage: This allows for efficient searching, querying, and analysis of historical data, facilitating forensic investigations and compliance reporting.
Wazuh Dashboard: A web-based user interface that provides visualization and management capabilities. Security analysts can use the dashboard to monitor alerts, analyse security data, create custom dashboards, and manage the Wazuh deployment. **Response and Remediation:** Upon receiving alerts, security teams can initiate response actions directly from the Wazuh Dashboard. This may include isolating affected systems, blocking malicious IP addresses, or executing custom scripts to remediate identified threats.
Integration with External Tools: Wazuh integrates with various external tools and platforms, such as SIEM solutions, ticketing systems, and threat intelligence services, enhancing its capabilities and allowing for a more comprehensive security posture.

This workflow helps to maintain continuous security monitoring, promptly detect and respond to threats, and ensure compliance with regulatory requirements.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14162

Figure-2: Wazuh Security Events for Monitoring

IV. PAGE STYLE

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Text Font of Entire Document

The entire document should be in Times New Roman. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.
Recommended font sizes are shown in Table 1.

B. Title and Author Details

Title must be in 24 pt Regular font. Author name must be in 11 pt Regular font. Author affiliation must be in 10 pt. All title and author details must be in single-column format and must be centred. Every word in a title must be capitalized except for short minor words such as "a", "an", "and", "as", "at", "by", "for", "from", "if", "in", "into", "on", "or", "of", "the", "to", "with". Author details must not show any professional title (e.g. Managing Director), any academic title (e.g. Dr.) or any membership of any professional organization (e.g. Senior Member IEEE).

To avoid confusion, the family name must be written as the last part of each author name (e.g. John A.K. Smith). Each affiliation must include, at the very least, the name of the company and the name of the country where the author is based (e.g. Causal Productions Pty Ltd, Australia).

C. Section Headings

No more than 3 levels of headings should be used. All headings must be in 10pt font. Every word in a heading must be capitalized except for short minor words as listed in Section III-B.
Level-1 Heading: A level-1 heading must be in Small Caps, centered and numbered using uppercase Roman numerals. For example, see heading "III. Page Style" of this document. The two level-1 headings which must not be numbered are "Acknowledgment" and "References".

Level-2 Heading: A level-2 heading must be in Italic, left-justified and numbered using an uppercase alphabetic letter followed by a period. For example, see heading "C. Section Headings" above.
Level-3 Heading: A level-3 heading must be indented, in Italic and numbered with an Arabic numeral followed by a right parenthesis. The level-3 heading must end with a colon.

D. Figures and Table

Figures and tables must be cantered in the column. Graphics must not use stipple fill patterns because they may not be reproduced properly. Please use only *SOLID FILL* colors which contrast well both on screen and on a black-and-white hardcopy, as shown in Fig. 1.

Figure Captions
Figures must be numbered using Arabic numerals. Figure captions must be in 10 pt Regular font. Captions of a single line must be centered whereas multi-line captions must be justified. Captions with figure numbers must be placed after their associated figures, as shown in Fig. 1.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14162

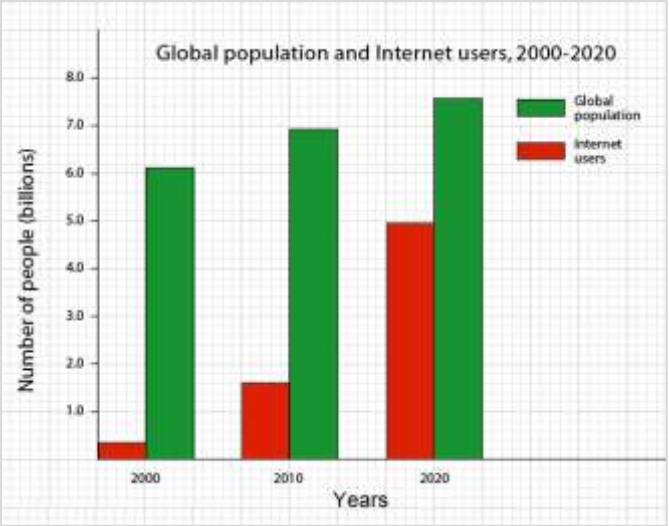


Fig. 1 A sample graph

Table Captions

Tables must be numbered using uppercase Roman numerals. Table captions must be centred and in 10 pt. Captions with table numbers must be placed before their associated tables, as shown in Table 1.

TABLE I FONT SIZES FOR PAPERS

Font Size	**Appearance (in Time New Roman or Times)**		
	Regular	**Bold**	**Italic**
10	table caption (in Small Caps), figure caption		
8	reference item		reference item (partial)
10	author address (in Courier), cell in a table	abstract body	abstract heading (also in Bold)
10	level-1 heading (in Small Caps), paragraph		level-2 heading, level-3 heading, author affiliation
11	author name		
24	title		

E. Page Numbers, Headers and Footers

Page numbers, headers and footers must not be used.

F. Links and Bookmarks

All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL your paper, you must type out the address or URL fully in Regular font.

G. References

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]). When referring to a reference item, please simply use the reference number, as in [2].

Examples of reference items of different categories shown in the References section include:

- example of a book in [1]
- example of a book in a series in [2]
- example of a journal article in [3]
- example of a conference paper in [4]
- example of a patent in [5]

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14162

- example of a website in [6]
- example of a web page in [7]
- example of a databook as a manual in [8]
- example of a datasheet in [9]
- example of a master's thesis in [10]
- example of a technical report in [11]
- example of a standard in [12]

V. CONCLUSION

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained.

REFERENCES

[1]. B. McMahan et al., "Communication-Efficient Learning of Deep Networks From Decentralized Data", *Artificial Intelligence and Statistics Proc. PMLR*, vol. 10, no. 1, pp. 1273-82, 2017.
[2]. C. En Guo, S.-C. Zhu and Y. N. Wu, "Primal Sketch: Integrating Structure and Texture", *Computer Vision and Image Understanding*, vol. 106, no. 1, pp. 5-19, 2007.
[3]. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, no. 2, pp. 569–571,1999.
[4]. Hogade, N., Pasricha, S. and Siegel, H.J, "Energy and Network Aware Workload Management for Geographically Distributed Data Centers". IEEE Transactions on Sustainable Computing, vol.7, no. 2, pp.400–413. 2021
[5]. A. Wierman, Z. Liu, I. Liu and H. Mohsenian-Rad, "Opportunities and challenges for data center demand response", Proc. Int. Green Comput. Conf., vol.7, no. 6, pp.1-10, 2014.
[6]. J. D. Jenkins et al., "The benefits of nuclear flexibility in power system operations with renewable energy", Appl. Energy, vol. 22 no. 2, pp. 872-884, 2018.
[7]. Haoying Dai, Yanne Kouomou Chembo, "RF Fingerprinting Based on Reservoir Computing Using Narrowband Optoelectronic Oscillators", Journal of Lightwave Technology, vol.40, no.21, pp.7060-7071, 2022.
[8]. Floris Van den Abeele, Jeroen Hoebeke, Girum Ketema Teklemariam, Ingrid Moerman, Piet Demeester, "Sensor Function Virtualization to Support Distributed Intelligence in the Internet of Things", Wireless Personal Communications, vol.81, no.4, pp.14-18, 2015.
[9]. J. Hwang, J. Kim and H. Choi, "A review of magnetic actuation systems and magnetically actuated guidewire-and catheter-based microrobots for vascular interventions", Intell. Serv. Robot., vol. 13, no. 1, pp. 1-14, 2020.
[10]. D. G. Feitelson, D. Tsafrir and D. Krakov, "Experience with using the parallel workloads archive", J. Parallel Distrib. Comput., vol. 74, no.3, pp. 2967-2982, 2014.
[11]. B. Accou, J. Vanthornhout, H. V. Hamme and T. Francart, "Decoding of the speech envelope from eeg using the vlaai deep neural network", Scientific Reports, vol. 13, no. 1, pp. 812, 2023.
Serim Lee, Nahyun Kim, Junhyoung Kwon, Gunhee Jang, "Identification of the Position of a Tethered Delivery Catheter to Retrieve an Untethered Magnetic Robot in a Vascular Environment", Micromachines, vol.14, no.4, pp.724, 2023.

