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

Strengthening 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

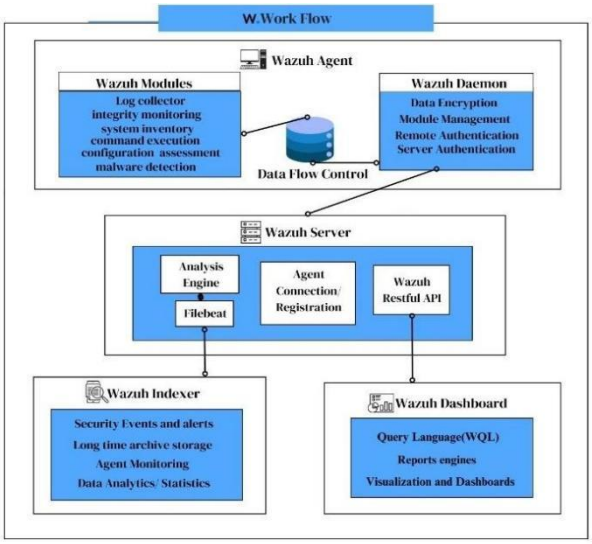
DOI: 10.17148/IJARCCE.2025.14162

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

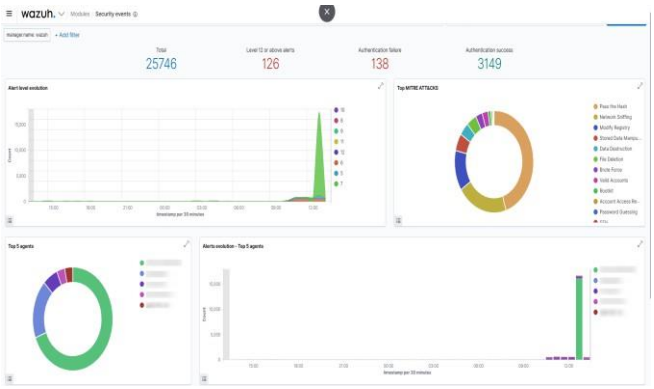


Figure-2: Wazuh Security Events for Monitoring

IV. KEY FEATURES OF WAZUH

- Log Collection and Analysis: Wazuh agents collect and forward logs from various endpoints, devices, and applications, enabling centralized log management.
- Intrusion Detection System (IDS): Wazuh incorporates rule-based intrusion detection capabilities to monitor for suspicious activities and policy violations.
- File Integrity Monitoring (FIM): The platform monitors critical files and directories for unauthorized changes, helping organizations maintain data integrity and identify potential breaches or tampering.
- Vulnerability Detection: Wazuh does vulnerability assessments by comparing system configurations and installed software against known vulnerabilities and address potential security weaknesses proactively.
- Configuration Assessment: The platform ensures that systems comply with security best practices by evaluating configurations against industry standards such as CIS benchmarks and NIST guidelines. This feature is crucial for maintaining regulatory compliance.
- Compliance Management**:** Wazuh simplifies compliance with various regulatory standards, including PCI DSS, GDPR, HIPAA, and SOX, by providing preconfigured Rules, reporting capabilities, and audit trails.
- Threat Intelligence Integration: Wazuh integrates with external threat intelligence feeds to stay updated on the latest cyber threats, enhancing its ability to detect and respond to emerging risks.
- Scalability and Flexibility: Designed to handle diverse IT infrastructures, Wazuh can scale from small deployments to enterprise-level environments, supporting cloud-native, hybrid, and on-premises systems.

V. WAZUH COMPONENTS

The Wazuh Security Information and Event Management (SIEM) solution comprises of three core components—namely, the Wazuh Manager, Wazuh Indexer, and a visualization interface Wazuh dashboard, supplemented by a lightweight yet powerful Wazuh agent. The agent is deployed on monitored endpoints, where it efficiently collects and forwards security-related data, such as system logs, file integrity information, and vulnerability reports, to the Wazuh Manager for processing.

Wazuh Indexer:

The Wazuh Indexer is a core component of the Wazuh platform, serving as the centralized data repository where log data is stored and indexed for analysis. The integration of Wazuh Indexer with the Wazuh Manager ensures seamless flow and organization of information, enabling administrators to access actionable insights efficiently. Its compatibility with dashboards like Kibana simplifies monitoring through customizable visualizations and reports.

Wazuh Manager:

The Wazuh Manager serves as the central analytical engine of the platform, orchestrating the processing and analysis of security data collected from agents deployed across endpoints.

It leverages predefined rules, advanced correlation algorithms, and real-time threat intelligence feeds to identify anomalies, detect potential threats, and generate actionable alerts. Beyond analytics, the Manager oversees critical operational functions such as agent registration, secure communication using encryption protocols, and centralized configuration management for consistent policy enforcement. The Manager's modular architecture allows for the creation of custom decoders and rules, providing organizations with the flexibility to tailor the system to their unique operational and security requirements. This adaptability enhances its effectiveness in addressing diverse and evolving

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

cybersecurity challenges while maintaining a proactive defense strategy.

Wazuh Dashboard:

The Wazuh Dashboard is an intuitive web-based interface for visualizing security data, managing alerts, and generating detailed reports. It delivers real-time insights through interactive charts, graphs, and customizable dashboards, enabling security teams to monitor events effectively and respond swiftly. With support for advanced querying using the Wazuh Query Language (WQL), it allows precise filtering and analysis of large datasets to identify anomalies or trends. The Dashboard simplifies compliance efforts through prebuilt reporting templates aligned with industry standards, reducing the complexity of audits and regulatory documentation. Centralized control enhances efficiency by consolidating data visualization and operational management into a unified platform. It offers robust customization options, allowing users to tailor views to specific organizational needs. This streamlined approach aids decision-making, accelerates threat response, and strengthens overall security operations, making the Wazuh Dashboard a cornerstone of efficient cyber security management.

The custom dashboard visualizes the "Top 25 Event Generators" within the Wazuh platform, offering a clear and intuitive representation of data sources generating the most events. Each segment's size correlates with the volume of events generated, providing immediate insights into the most active sources.

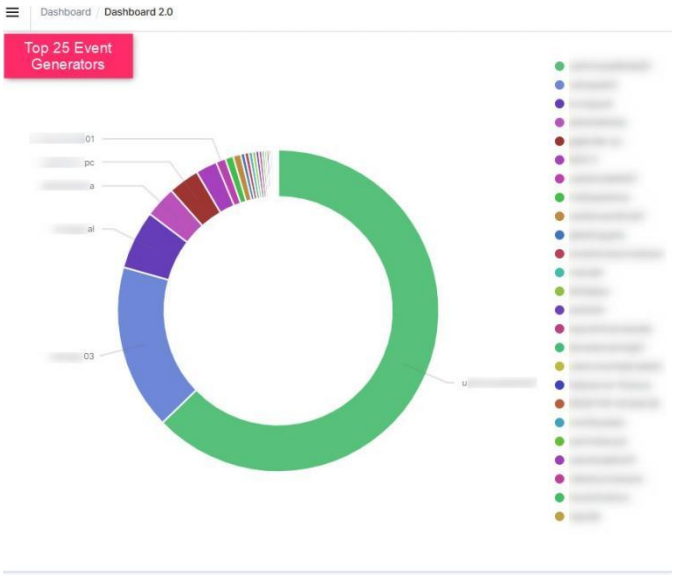


Figure-3: Custom Wazuh Dashboard

This dashboard allows security teams to quickly identify which systems, applications, or endpoints are contributing most significantly to event logs, enabling prioritization for investigation or optimization. Its design is user-friendly and integrates seamlessly into the overall monitoring and analysis workflows.

Wazuh Agent:

The Wazuh Agent is a lightweight software component deployed on endpoints to gather and monitor security-related data. It performs essential tasks like log collection, file integrity monitoring, rootkit detection, and vulnerability assessment, providing a comprehensive view of endpoint activities. The agent also conducts configuration assessments to ensure systems comply with security policies and standards. It securely transmits collected data to the Wazuh Manager for centralized analysis, enabling real-time threat detection and response. Designed for cross-platform compatibility, it operates seamlessly on Windows, Linux, MacOS, and other systems, making it versatile for diverse environments. Its proactive monitoring helps identify anomalies and potential risks before they escalate into critical issues. The Wazuh Agent is optimized for minimal resource usage, ensuring high performance without disrupting endpoint operations. Additionally, it supports dynamic configuration updates from the Manager, allowing flexible policy enforcement. As a core component of the Wazuh architecture, it enables robust security monitoring, compliance management, and enhanced visibility across distributed infrastructures.

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

This dashboard allows security teams to quickly identify which systems, applications, or endpoints are contributing most significantly to event logs, enabling prioritization for investigation or optimization. Its design is user-friendly and integrates seamlessly into the overall monitoring and analysis workflows.

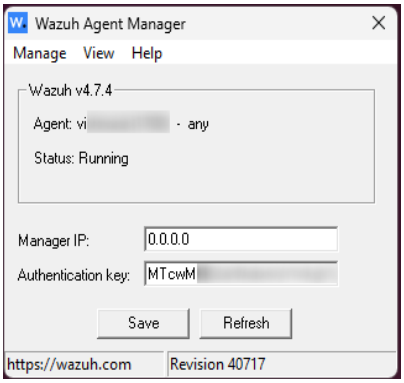


Figure-4: Wazuh agent manager at endpoint

VI. WAZUH ARCHITECTURE

Wazuh's architecture is designed to provide a distributed and scalable security monitoring solution for enterprises of all sizes. The Wazuh Agent can be installed on a variety of systems, including servers, workstations, and network devices, enabling the collection of detailed data from multiple sources. The agent performs real-time monitoring of system activities, such as user logins, file modifications, and application behaviour. Additionally, it ensures the integrity of critical files by tracking unauthorized changes and provides visibility into potential vulnerabilities or misconfigurations

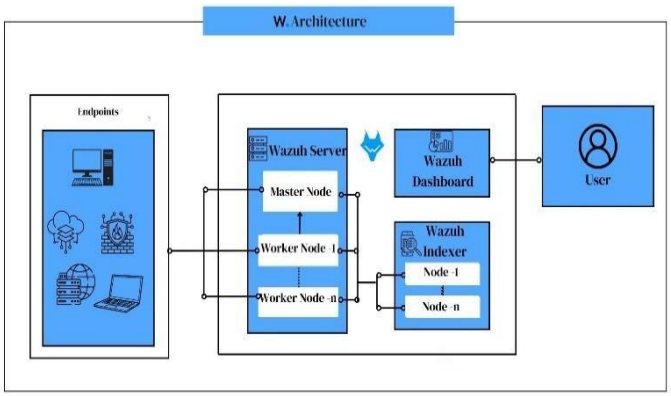


Figure-5: Wazuh Architecture

The Wazuh Manager acts as the brain of the system, responsible for processing and analysing the data sent by the agents. It applies a set of predefined and customizable detection rules, which helps identify security incidents like brute force attacks, failed logins, and abnormal system behaviour. The Wazuh Manager also facilitates centralized monitoring, enabling security teams to have a unified view of the security s The integration with visualization tools like Kibana provides real-time dashboards, making it easier to monitor security events and incidents. This architecture enables real-time monitoring, threat detection, and compliance management in a scalable and flexible manner.

VII. COMPREHENSIVE WEB SERVER ATTACK DETECTION WITH WAZUH

The Wazuh platform enhances web server protection through its robust attack detection capabilities. It provides real-time visibility into web server logs, analysing them for suspicious activity, such as SQL injection, cross-site scripting (XSS), or denial-of-service (DoS) attacks. By integrating with various threat intelligence feeds and utilizing machine learning-based anomaly detection, Wazuh identifies patterns of malicious behaviour and triggers immediate alerts. Furthermore, its ability to correlate log data across various systems enhances its detection accuracy, enabling the identification of complex, multi-vector attacks.



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

With a centralized management interface, Wazuh offers administrators the ability to monitor, analyse, and respond to threats in a comprehensive and scalable manner, ensuring that web servers are protected against evolving security risks.

VIII. WAZUH MODULES

1) Security Information Management

Security Events:

Wazuh collects, analyses, and correlates logs from various sources such as operating systems, applications, and network devices. It detects suspicious events and applies rule-based logic to generate alerts for security teams to act upon.

Integrity Monitoring:

The platform monitors critical files and directories for unauthorized changes. It generates alerts when files are modified, created, or deleted, providing visibility into potential tampering or malware activity.

2) Auditing and Policy Monitoring

Policy Monitoring:

Wazuh helps ensure adherence to organizational policies by tracking configuration changes and access violations. It generates alerts when deviations from established baselines occur.

System Auditing

Wazuh audits system activities, such as user logins, privilege escalations, and changes to critical settings. It helps detect insider threats and ensures transparency in system usage.

O**penSCAP:**

Wazuh integrates with OpenSCAP, a framework for auditing and automating compliance checks against industry standards. It supports checks for vulnerabilities, misconfigurations, and system hardening guidelines.

CIS-CAT:

The platform integrates with CIS-CAT (CIS Configuration Assessment Tool) to perform configuration assessments against CIS benchmarks. This ensures that systems align with best practices for security.

Security Configuration Assessment:

Wazuh evaluates system configurations against security standards, identifying deviations and providing recommendations for corrective actions to enhance the security posture.

3) Threat Detection and Response

Vulnerabilities:

Wazuh identifies vulnerabilities by correlating system inventory with databases like CVE. This allows security teams to prioritize patching efforts and address critical vulnerabilities proactively.

Osquery:

Wazuh integrates with Osquery, enabling security teams to perform powerful system queries in real time. This module facilitates in-depth investigation of endpoints.

MITRE ATT&CK:

Wazuh maps security events to the MITRE ATT&CK framework, providing context for detected threats. This helps security teams understand the tactics and techniques used by attackers and improve their defenses accordingly.

4) Regulatory Compliance

The Wazuh platform is commonly employed to address the technical aspects of regulatory compliance standards. It not only offers the essential security features like host intrusion detection, configuration assessment, log analysis, and vulnerability detection to fulfil compliance requirements but also leverages its SIEM (Security Information and Event Management) capabilities to centralize, analyse, and enhance security data. To assist with regulatory compliance, Wazuh's rules are aligned with compliance needs. When an alert is triggered (indicating a rule condition has been met), the alert automatically includes compliance-related information. The platform supports various standards, including PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation), NIST SP 800-53, GPG13

IX.KEY FEATURES OF WAZUH'S WEB SERVER ATTACK DETECTION

Log Collection and Analysis: Wazuh agents collect logs from web servers like Apache, Nginx, and IIS, and parse them for suspicious patterns are then analysed for abnormal activity, such as repeated failed login attempts, suspicious URLs, or unexpected resource access.

Rule-based Detection*:* Wazuh includes a set of predefined detection rules that can identify common web server attacks, including SQL injection, cross-site scripting (XSS), remote file inclusion (RFI), and directory traversal attacks.

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

***Brute-force Detection**:* Wazuh can detect brute-force attack and it can trigger alerts when a threshold of failed attempts from the same IP address is reached, indicating a potential attack.
Real-time Alerts and Incident Response: Wazuh generates real- time alerts based on the analysis of logs and rules. These alerts are correlated with other security events to give a comprehensive view of the attack. Security teams can then respond by investigating the alert, blocking malicious IPs, or taking action to mitigate the attack.
Customizable Rules: Wazuh allows customization of detection rules to adapt to specific use cases and environments.
Integration with SIEM: Wazuh integrates with SIEM platforms like Elastic search, Kibana, and Splunk to provide deeper insights into web server attack data. These platforms can be used for historical searches, visualization, and reporting, helping security teams monitor trends and detect new attack patterns.

X. EXPERIMENT, RESULTS AND SYSTEM PERFORMANCE

This section outlines the experimental setup and results obtained from the evaluation of the security system's performance to assess the ability of the security system to detect potential SQL injection attempts in a web application. The primary objective was to evaluate the system's detection capabilities. The experiment involved simulating SQL injection attempts through various input methods, specifically targeting URL parameters with time-based techniques like the SLEEP function. The attacks were monitored and logged by the security system, and the primary focus was on the detection of malicious activity. Alerts generated from these detection events were then analyzed to determine the system's effectiveness in identifying potential threats for further action.

The security system leveraged custom-defined rules to detect anomalies indicative of SQL injection attempts. These rules were designed to identify patterns of suspicious activity, such as abnormal query strings or unusual response times caused by time-based injection techniques. During the experiment, the system generated alerts for each detected attack, and the resulting data was collected for further analysis. The analysis focused on evaluating the accuracy of the detection mechanism, specifically assessing false positive rates, detection latency, and the system's ability to distinguish between legitimate and malicious requests. This analysis provided valuable insights into the effectiveness of the detection framework and informed potential improvements for future security measures.

TABLE-1 SQL Injection Overview

Parameter	Data
GeoLocation.country_name	United States
GeoLocation.location.lat	37.751
GeoLocation.location.lon	-97.822
_id	Fud564rghf87o
_index	wazuh-alerts-4.x-2022.04.05
data.srcip	35.60.4.87
data.agentip	210.101.136.18
decoder.name	custom-1
decoder.parent	custom-1
full_log	35.60.4.87 - - 210.101.136.18 [24/Dec/2024:18:16:14 +0530] GET /listing?cat=6&filter=1&job-type=1&keywords=Mr.&location=1 &order=desc&placeid=US&placetyp e=country&range1=1&range2=1)%2 0AND%20(SELECT%201864%20F ROM%20(SELECT(SLEEP(6)))gOG h)%20AND%20(6900=6900&salary-type=1&sort=id&subcat HTTP/1.1 404 207 Mozilla/5.0 (Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36 -
id	2536476658.98796575
input.type	log
location	/var/log/access.log
manager.name	wazuh



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

rule.description	SQL Injection attempt
rule.gdpr	IV_35.7.d
rule.groups	Custom_web_ttestrule, attack, sql injection
rule.id	100068
rule.level	9
rule.mail	FALSE
rule.mitre.id	T1190
rule.mitre.tactic	Intial Access
rule.mitre.technique	Exploit Public-Facing Application
rule.nist_800_53	SA.11, SI.4
rule.pci_dss	6.5,11.4,6.5.1
rule.tsc	CC6.6, CC7.1, CC8.1, CC6.1, CC6.88, CC7.2, CC7.3
timestamp	24/Dec/2024:18:16:14.097+530

The detected log represents a SQL injection attempt using the SLEEP function, commonly employed in time-based blind SQL injection. The attack originated from the IP address 35.60.4.87, with a source port and user agent indicating the attacker's environment. The request was logged on December 24, 2024, and was flagged by Wazuh under a custom rule designed to detect SQL injection activities. The attacker's goal was to manipulate the SQL query by adding a condition that would cause a delay (SLEEP (6)) in the server's response. This behavior was detected as suspicious, and the alert was triggered with a high severity level of 9. Geolocation data indicates the request originated from the United States. Rule definitions such as those from GDPR, PCI-DSS, and MITRE were linked to the alert, categorizing it under "Initial Access" and "Exploit Public- Facing Application." The full log provided details of the attacker's actions and the web server's response, which included a 404 error code. The server successfully detected and logged the suspicious activity in real time.

System performance and resource utilization

The Wazuh manager outlined in this paper is deployed on an Ubuntu Server with 150GB of RAM, 8 CPU cores, and 200GB of storage. It collects and processes data from 50 servers within the network. Currently, the system utilizes around 60GB of RAM, experiences minimal CPU load, and has approximately 120GB of storage in use. The system has been running for 5 months without interruption.

CONCLUSION

This paper comprehensively reviewed the capabilities of the Wazuh tool for **detecting cyberattacks through log analysis**. The Wazuh platform, with its modular and scalable architecture, integrates diverse security functionalities such as log collection, intrusion detection, file integrity monitoring, vulnerability detection, and compliance management into a unified solution. By processing and correlating security data from endpoints and systems, Wazuh enables real-time threat detection and facilitates rapid response to potential security incidents. The integration of advanced features such as rule-based detection, custom rule support, and seamless collaboration with SIEM platforms ensures that Wazuh is an effective tool for modern cybersecurity challenges. Furthermore, its ability to monitor and detect attacks targeting web servers, as demonstrated through the analysis of a SQL injection attack, highlights the tool's practicality in safeguarding critical infrastructures. The Wazuh platform's performance and resource utilization, tested with substantial deployments, proves its efficiency in real-world environments.

REFERENCES

[1]. M. Moh, S. Pininti, S. Doddapaneni, T.S. Moh "Detecting Web Attacks Using Multi-Stage Log Analysis", 6th IEEE International Conference on Advanced Computing,2016.
[2]. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis Stefan Stanković, Slavko Gajin, and Ranko Petrović, Member, IEEE.
[3]. O. Negotia, M. Carabas "Enhanced Security Using Elastic Search and Machine Learning", Advances in Intelligent Systems and Computing, vol. 1230.
[4]. Wazuh documentation components,https://documentation.wazuh.com/current/getting-started/components/index.html
Wazuhdocumentation Architecture,https://documentation.wazuh.com/current/getting- tarted/architecture.html