International Journal of Engineering Materials and Manufacture (2024) 9(4) 136-144
https://doi.org/10.26776/ijemm.09.04.2020.02

Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries

Md Rafiqul Islam and Raisa Rafique

Received: 12 July 2024
Accepted: 20 October 2024
Published: 30 October 2024
Publisher: Deer Hill Publications

ABSTRACT

Security of IT infrastructure is critical in the modern digital environment, particularly for industries that manufacture clothing. The application of the Wazuh Security Information and Event Management (SIEM) system to improve security monitoring and compliance for an IT system in the apparel industry is the main topic of this study. To improve the apparel industry cyber threat monitoring system in real-time monitoring, detecting the threat vectors that support the centralized management system, to meet these objectives of the company, an SIEM security management system has been installed and configured with the components of Wazuh manager, indexer, Wazuh agent, and Wazuh dashboard as well. An Oracle virtual lab environment was created to install and configure the Wazuh system a robust Linux operating system was installed at the server level and Windows 10 was installed on the client end to the authenticity failure of the security system. To implement the Wazuh system, the project management guideline was followed which ensured the planning and implementation of the project, testing phases, and along with review and maintenance. Wazuh security management system successfully identified the authentical failure reports and vulnerabilities and generated automated reports from the system that showed the result of 1 critical, 19 high, and 5 medium levels of vulnerabilities shown in Figure 6, and the necessary patch recommended to solve the critical issues. On the other hand, the system also generated security events as well as integrity monitoring system reports. The deployment of the Wazuh security management system ensured the robust cost-effective security management system with high quality for detecting cyber threats which supports the regulatory and compliance requirements and is a viable tool for the apparel industry to protect the stakeholders' interest.

Keywords: Wazuh, Apparel, Dashboard, SIEM, Vulnerability.

1 INTRODUCTION

Security of IT infrastructure is critical in today's digital environment, particularly for industries that manufacture clothing. The main purpose of this research is to implement the Wazuh security system to enhance and monitor the security system of the apparel sector. This security concern is also the compliance and regulatory requirements. This security system ensures real-time threat detection and monitoring by using the Wazuh centralized system, and the generation of automated vulnerability reports from the system with the help of the Wazuh components such as manager, indexer, agent, and dashboard [1-2].

In the 21st century, a robust and user-friendly information technology platform is highly required for the apparel industry like other sectors to meet the users' requirements to ensure the supply chain management, online product searching and procurement facilities, and complete the billing process as well. On the other hand, there is a high risk of potential threats of cyber threats and a huge amount of money steals through these cyber-crimes all over the world [3-4]. Not only that to ensure the stakeholders' equity and their brand images, but it is also a mandatory requirement to comply with regulators' guidelines.

1.1 Problem Statement

The apparel industries produce different products to serve our society which is a basic requirement in the daily life of the people. Ensuring the security threats in the apparel sector is a huge challenge for the IT and security operation centre (SOC) team. To ensure the security of the company's security monitoring system and to improve it, a robust security SIEM solution is needed [5]. The organization's ability to combat potential security threats and compliance

Md Rafiqul Islam[1] and Raisa Rafique[2]
[1]Bengal Commercial Bank PLC, 94 Gulshan Avenue, Dhaka, Bangladesh
E-mail: rafiqul.islam@bgcb.com.bd engrrafiqul@gmail.com
[2]Department of Fashion Business Management, Fashion Institute of Technology
227 W 27th St, New York, NY 10001, USA
E-mail: raisa_rafique@fitnyc.edu raisa.rafique01@gmail.com

Reference: Islam, M. R. and Raisa R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture*, 9(4), 136-144.

issues like inconsistent security monitoring, manual incident response, lack of visibility, and compliance challenges has decreased due to the absence of a centralized and real-time security monitoring system [6-7].

1.2 Objective

The primary goal of this project/paper is to use Wazuh to monitor the apparel's IT security system through the implementation of a comprehensive Security Incident and Event Management (SIEM) system. The Wazuh server, agent, indexer, and dashboard must be deployed and configured correctly to create a strong security system. Nonetheless, this configuration facilitates the garment's efficient detection and monitoring of possible cyber threats. The primary goals of this initiative are as follows.

1. To install and configure the Wazuh server, indexer, agent, and dashboard.
2. To create automatic reports regularly to record the IT system of the company's security posture.
3. To generate different reports on vulnerabilities, authentication failure, and alert summaries.

The problem statement, project goals, suggested remedy and tools used in the Wazuh SIEM system installation for the apparel sectors are described in this introduction. To clearly understand the objectives of this research paper, the literature review part has been discussed in section 2, the methodology and solution have been placed in section 3, the result and discussion part belongs to section 4, and finally conclusion has been orchestrated in section 5.

2 REVIEW OF THE RESEARCH

To address the problem statement and the objectives of this research work, a reliable and cost-effective solution Security Incident and Incident Management (SIEM) is required to be implemented in the apparel industry. To protect and ensure the security system of the IT infrastructure in the apparel sector, the Wazuh system is reliable and cost-effective and very renowned worldwide because the system has a building option for the Wazuh manager to ensure the controlling part of the server, agents help to collect the information from the end-users, indexer organized the data, and dashboard help to generate the automated IT system vulnerability reports [8-9].

2.1 Wazuh Monitoring System

Strong real-time monitoring capabilities are provided by the Wazuh system, which is crucial for the IT infrastructure of the clothing sector [10]. The system collected the data from the users' end and instantly identified the vulnerabilities and corresponding risks in the IT system in the apparel industry. Based on this information the information security team of the company can take the corrective measure to protect the IT system [11-12]. One of the best features of the Wazuh system is the monitoring and system checking option that is in real-time.

2.2 Detection of Cyber Threat in Wazuh System

The algorithm for the detection and identification capability of cyber threats is built into the Wazuh system which can identify the signature-based security threats for the company. This system is also capable of identifying behavioural-based system vulnerabilities. By using these two features, the Wazuh system is widely used in the garment sectors and others where the system can detect malware and other types of sophisticated attacks which ensures running the company's business smoothly [13-14].

2.3 Log Management in Wazuh System

The Wazuh system has the strength to record the logs of the IT system centrally which helps to analyse the trend of the system, vulnerability, risk grading, operating system updates, and any other types of misconfigurations of the system [15]. The Security Operation Centre (SOC) team can take immediate remedy to protect the system from cybercrime. All the logs from different end-users accumulated in the central database which helps to do the system audit as well [16-17].

2.4 Report Management System in Wazuh

The Wazuh system dashboard is very user-friendly as well as a powerful tool to display reports that can be customized as per the users' requirements, especially in the apparel industry. The implementation and customized administration of the system and user manual are available in the open-source platform on the Wazuh website [18-19]. The automated reporting system helps to generate the reports centrally.

2.5 Using Wazuh for Compliance

All over the world, every country has its compliance guidelines which are imposed by the regulators. So, for apparel industry is one the most income-generating sectors for many countries like Bangladesh, Vietnam, India, China, Sri Lanka, and other non-developed countries [20] To comply with the regulators' requirements is highly important to sustain their business in this sector. The Wazuh system is one the powerful systems that can ensure all sorts of reports that can address the regulators' standard requirements as per their compliance guidelines [21].

3 METHODOLOGY AND SOLUTION

To research the security system of the IT platform of the apparel sectors, Wazuh is a strong SIEM security system that ensures the smooth installation, configuration, monitoring, and reporting the vulnerabilities, threat detections, event log management, and integrity monitoring system. This section strictly follows the project deployment guidelines such as planning which gathers the requirements of the garments industry, and implementation of the Wazuh system as per the requirement of the project owners. The others such as testing have been completed properly with appropriate and adequate evaluation of the system, and finally, observing and maintaining the security system. The research project was segregated into different phases which produced the result successfully.

Before implementing the Wazuh system for apparel's IT infrastructure, a lab environment was created where the Linux operating system was deployed in the server, and the Wazuh agents were installed in the user-end where the operating system was Windows 10. The authentication failure testing has been completed by using Windows 10 user credentials.

The high-end laptop with core i7 and 64GB DDR4 RAM were used whereas Windows 11 was used as the operating system. The Oracle Virtual Box is used as a lab environment in this high-end laptop to perform tasks smoothly. The operating system for this Oracle virtual box was a Linux operating system for a server where the Wazuh manager was installed, and Windows 10 was installed at the user end for the Wazuh agent. The following sections detail the steps involved in the research methodology:

3.1 Phase 1: Planning of Wazuh System

Before implementing the Wazuh SIEM system, the current Information Technology (IT) security system and its requirements have been analysed properly through a comprehensive study. A thorough project plan that includes deliverables, deadlines, and milestones. The implementation plan of the Wazuh system is shown below in Figure 1.

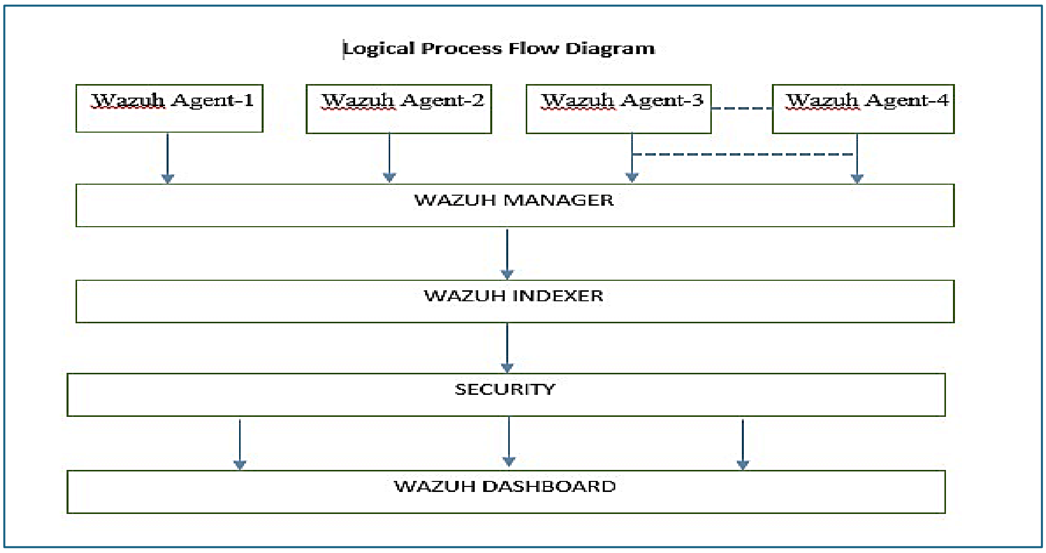
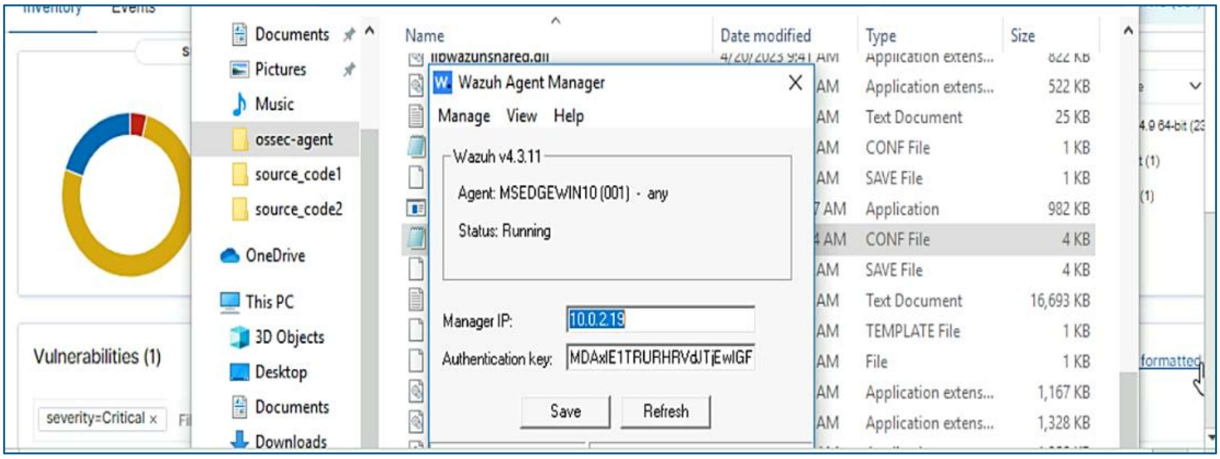


Figure 1: Logical Process Flow Diagram of Wazuh System

3.2 Phase 2: Implementation of Wazuh System

The following configuration and setup procedure have been completed to implement the Wazuh system. The installation screenshots are shown in Figure 2, Figure 3, and Figure 4 for Wazuh Manager, Agent, and Dashboard.

- Wazuh Manager: install and configure Wazuh Manager, the central server for security event management and analysis.
- Wazuh Agents: Install and configure Wazuh Agents to gather security data on a variety of IT end-users and servers.
- Wazuh Indexer: Configure Wazuh Indexer to index and store gathered data, enabling effective retrieval and search.
- Wazuh Dashboard: Dashboard installation and configuration to monitor the IT cyber threat monitoring system



Name	Date modified	Type	Size
libwazunshared.dll	4/20/2023 9:41 AM	Application extens...	822 KB
	AM	Application extens...	522 KB
	AM	Text Document	25 KB
	AM	CONF File	1 KB
	AM	SAVE File	1 KB
	7 AM	Application	982 KB
	4 AM	CONF File	4 KB
	AM	SAVE File	4 KB
	AM	Text Document	16,693 KB
	AM	TEMPLATE File	1 KB
	AM	File	1 KB
	AM	Application extens...	1,167 KB
	AM	Application extens...	1,328 KB

Wazuh Agent Manager

Manage View Help

Wazuh v4.3.11

Agent: MSEDGEWIN10 (001) - any

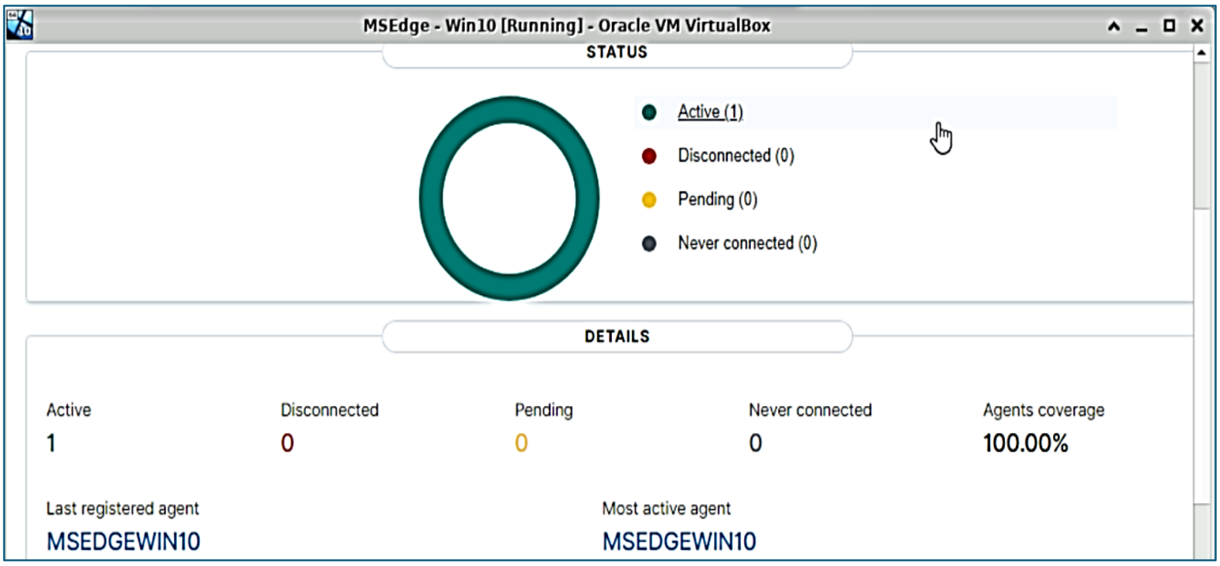
Status: Running

Manager IP: 10.0.2.19

Authentication key: MDAxIE1TRURHRVdJTjEwIGF

Save Refresh

Figure 2: Wazuh Manager Configuration


MSEdge - Win10 [Running] - Oracle VM VirtualBox

STATUS

● Active (1)

● Disconnected (0)

● Pending (0)

● Never connected (0)

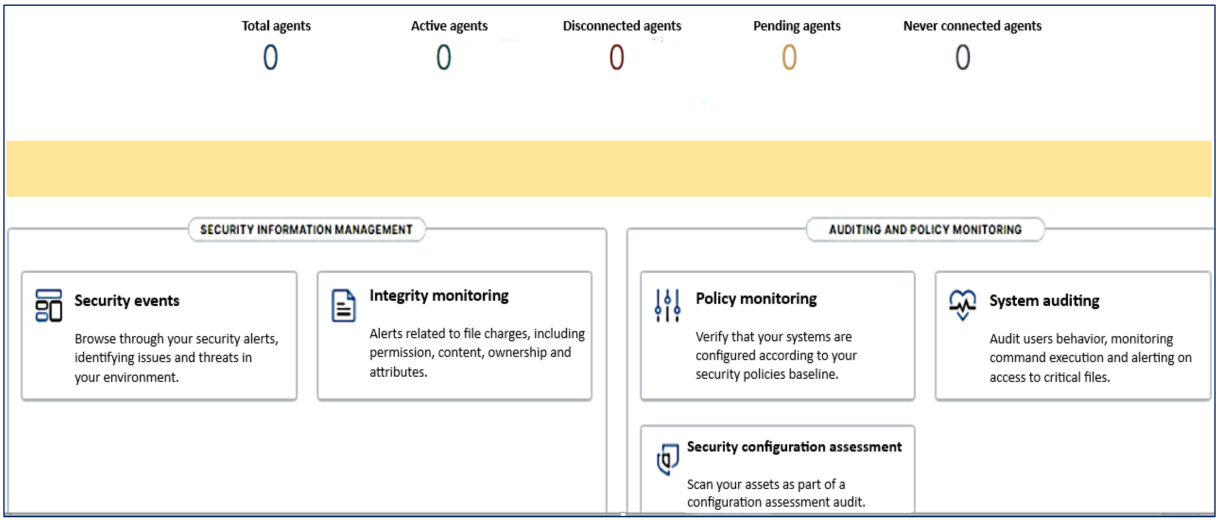
DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent
MSEDGEWIN10

Most active agent
MSEDGEWIN10

Figure 3: Wazuh agent Configuration


Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file charges, including permission, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

Figure 4: Wazuh dashboard

3.3 Phase 3: Testing of Wazuh System

To test the implementation, configuration, and system function properly the following activities have been checked properly which are as:

- Ensure the Agents, Indexer, Wazuh Manager, and Dashboard are all installed and set appropriately.
- Verify that accurate data collection, storage, and indexing of security is occurring.
- Evaluate the Wazuh system's performance under various load scenarios to make sure it can manage the amount of data from the IT system.
- Enhance system performance to reduce latency and guarantee prompt security issue detection and response.

3.4 Phase 4: Evaluation of the Wazuh System

To evaluate the Wazuh SIEM system, the following actions were taken which are below:

- Checking the trends, patterns, and possible weaknesses in the security data gathered from the Wazuh system.
- Checking of automated reports to track IT security systems.

3.5 Phase 5: Overview and Maintenance

The following steps were taken to ensure the functionality of the Wazuh security management system of the IT system that is as follows:

- To ensure the machine state is always in the save mode before down the virtual lab environment.
- To check all the components and installation status of the Wazuh manager, indexer, agents, and dashboard for proper functioning.

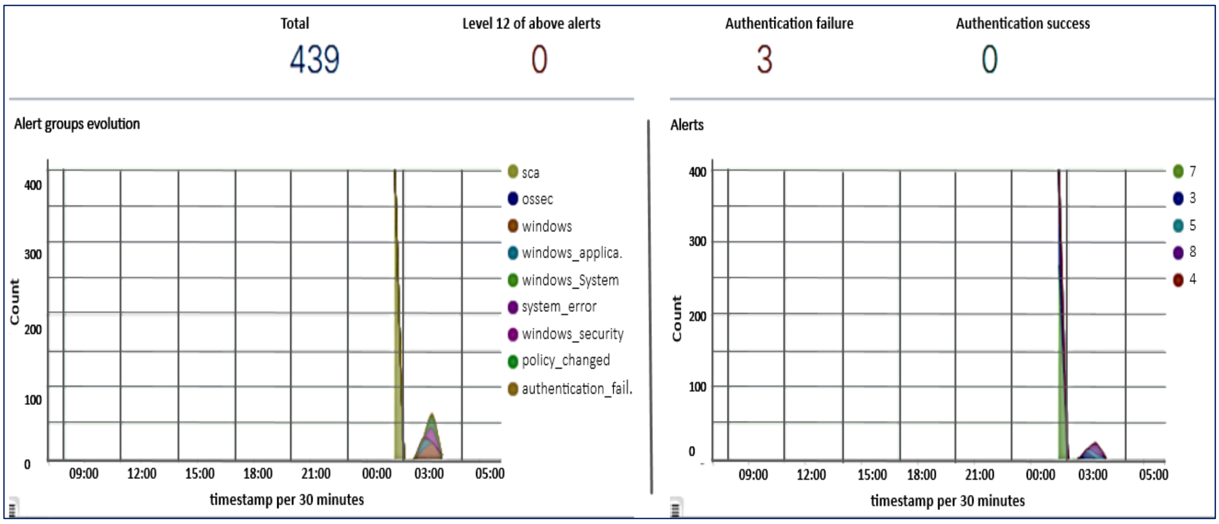
4 RESULTS AND DISCUSSIONS

The Wazuh SIEM solution was deployed, and the company's IT security posture has significantly improved since then. The system was tested and produced positive results in the Oracle Virtual lab setting. The Wazuh SIEM system, a complete security monitoring solution, was installed in the lab setting. This allowed it to quickly detect and handle any threats, guaranteeing robust protection against cyberattacks. The Wazuh dashboard, discussion sections, and results, however, have been arranged individually and in detail below.

4.1 Outcomes

4.1.1 Authentication Failure Log

After three unsuccessful attempts to log in using the incorrect password from Windows 10 (Wazuh agent), the Wazuh system manager was able to locate the authenticity failure logs, which are displayed in Figure 5 below. Three separate attempts were made to verify the system, which is depicted in Figure 5 under authentication failure in the security events, to test the authentication failure checking procedure.

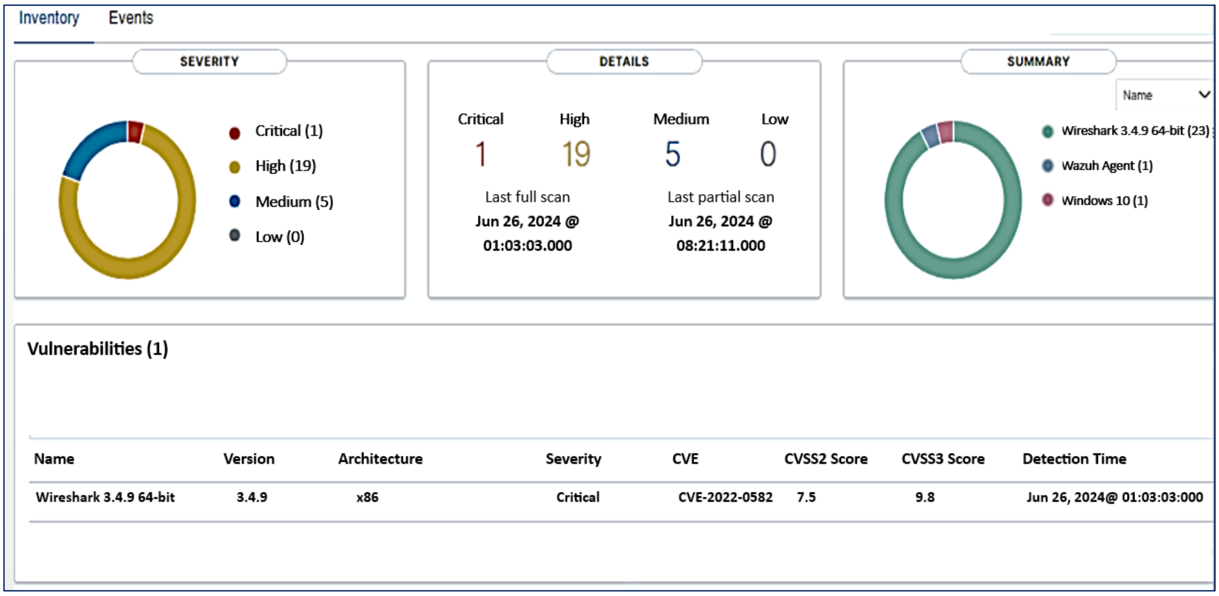


Total	Level 12 of above alerts	Authentication failure	Authentication success
439	0	3	0

Figure 5: Authentication failure logs

4.1.2 Analysis of Vulnerability Dashboard

After a thorough analysis, the vulnerability dashboard showed that there was a total of 1 critical, 19 high, 5 medium, and 0 low vulnerabilities in Figure 6.



Critical	High	Medium	Low
1	19	5	0

Last full scan Jun 26, 2024 @ 01:03:03.000

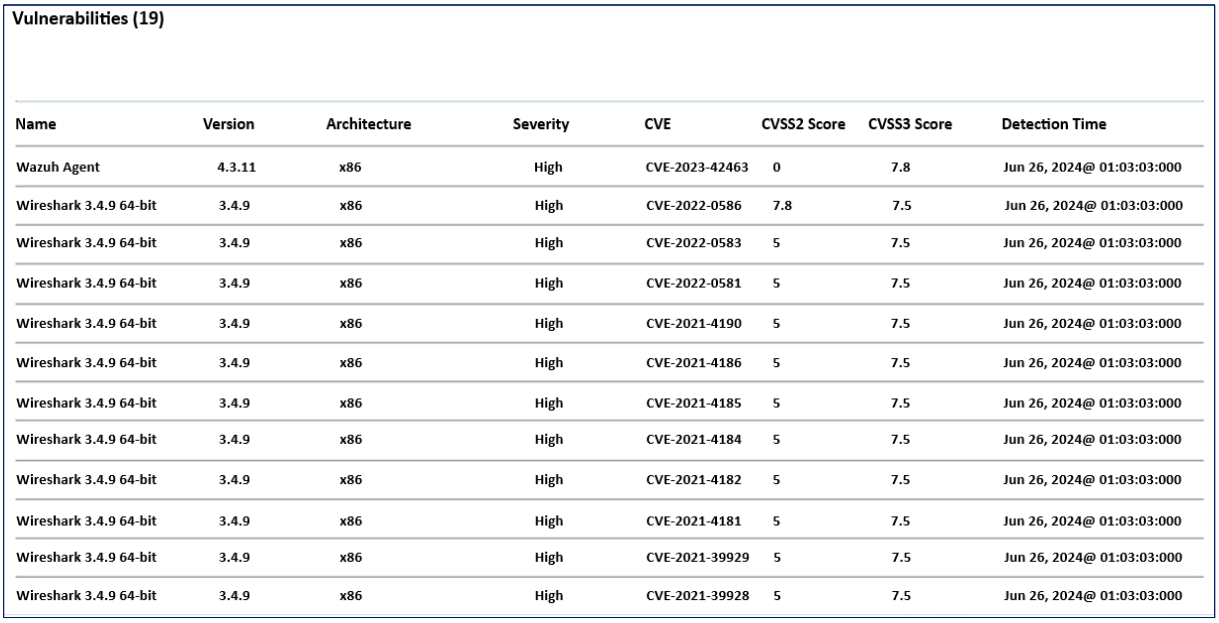
Last partial scan Jun 26, 2024 @ 08:21:11.000

Vulnerabilities (1)

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
Wireshark 3.4.9 64-bit	3.4.9	x86	Critical	CVE-2022-0582	7.5	9.8	Jun 26, 2024@ 01:03:03:000

Figure 6: Vulnerability shown in Wazuh Dashboard

The following results, such as 1 critical, 19 high, 5 medium, and 0 low vulnerabilities, were found from the Wazuh dashboard after the vulnerability dashboard in Figure 6 was examined. The operating system version 3.4.9 was utilized in this lab, and the advice is to reduce the cyber threat of critical vulnerability, which is under CVE-2022-0582. Patch 3.4.11 was suggested in this instance to address the critical vulnerability. The Wazuh dashboard found a total of 19 high vulnerabilities, which are also shown in Figure 7, which shows 12 vulnerabilities instead of 19 vulnerabilities.



Vulnerabilities (19)

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
Wazuh Agent	4.3.11	x86	High	CVE-2023-42463	0	7.8	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2022-0586	7.8	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2022-0583	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2022-0581	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4190	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4186	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4185	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4184	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4182	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-4181	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-39929	5	7.5	Jun 26, 2024@ 01:03:03:000
Wireshark 3.4.9 64-bit	3.4.9	x86	High	CVE-2021-39928	5	7.5	Jun 26, 2024@ 01:03:03:000

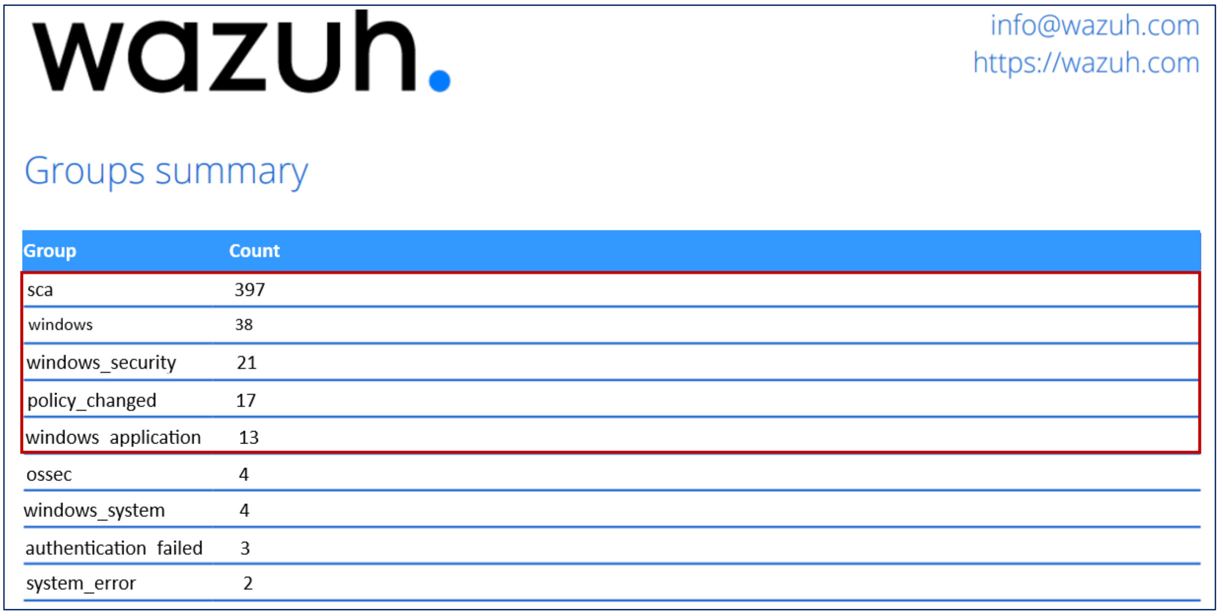
Figure 7: High-severity vulnerabilities

4.2 Report Generation from Wazuh Dashboard

By using the Wazuh dashboard 2 types of reports named i) Security Events, and ii) Integrity Monitoring were generated to analyze the severity of the IT security system.

4.2.1 Report on Security Events

The type and frequency of different security warnings are shown in the group summary and security events report (Figures 8 and 9). Changes to the Windows audit policy, audit failures, unsuccessful login attempts, and adherence to security standards were among the main problems (Table 1). Configuration assessments (397 alarms), Windows security events (38), policy modifications (17), and Windows apps (13) were the top 5 alert groups (Table 2).

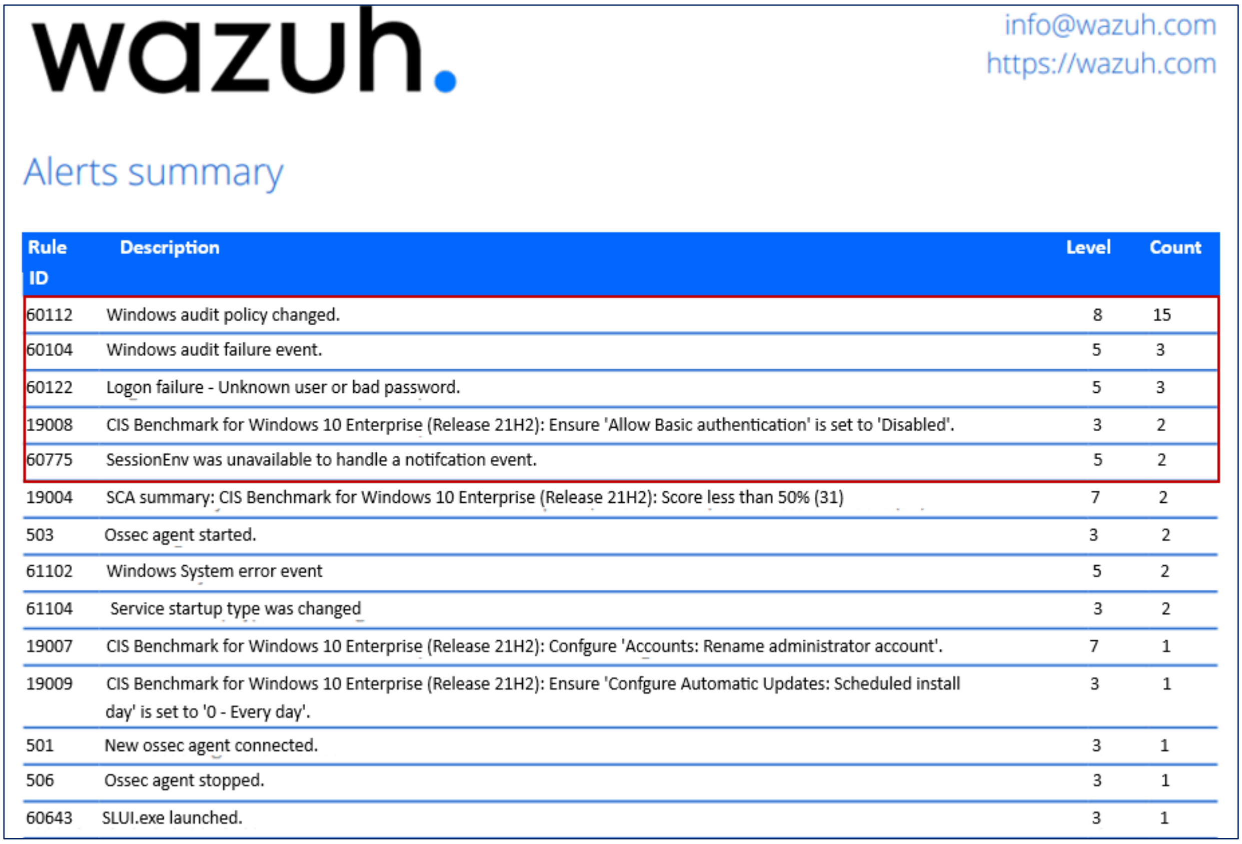


info@wazuh.com
https://wazuh.com

Groups summary

Group	Count
sca	397
windows	38
windows_security	21
policy_changed	17
windows application	13
ossec	4
windows_system	4
authentication failed	3
system_error	2

Figure 8: Wazuh alerts summary



info@wazuh.com
https://wazuh.com

Alerts summary

Rule ID	Description	Level	Count
60112	Windows audit policy changed.	8	15
60104	Windows audit failure event.	5	3
60122	Logon failure - Unknown user or bad password.	5	3
19008	CIS Benchmark for Windows 10 Enterprise (Release 21H2): Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
60775	SessionEnv was unavailable to handle a notifcation event.	5	2
19004	SCA summary: CIS Benchmark for Windows 10 Enterprise (Release 21H2): Score less than 50% (31)	7	2
503	Ossec agent started.	3	2
61102	Windows System error event	5	2
61104	Service startup type was changed	3	2
19007	CIS Benchmark for Windows 10 Enterprise (Release 21H2): Confgure 'Accounts: Rename administrator account'.	7	1
19009	CIS Benchmark for Windows 10 Enterprise (Release 21H2): Ensure 'Confgure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	1
501	New ossec agent connected.	3	1
506	Ossec agent stopped.	3	1
60643	SLUI.exe launched.	3	1

Figure 9: Wazuh groups summary

Table 1: Analysis of alert group based on the top 5 alerts

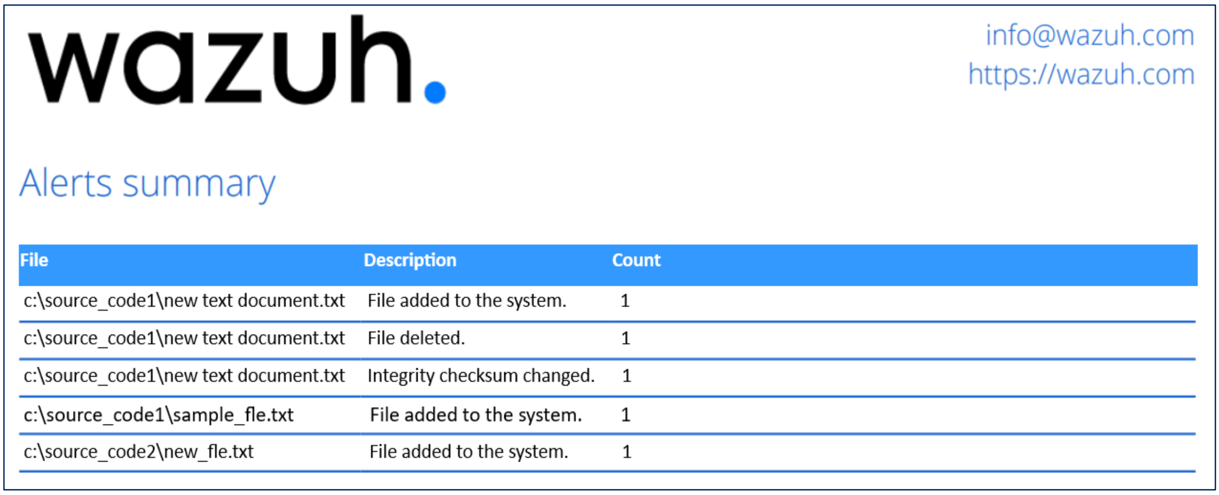
No.	Issues	Description
1	Changes to the Windows Audit Policy (ID: 60112)	Indicates modifications to the audit policy, which may have an impact on security surveillance.
2	The event ID for the Windows Audit Failure (ID: 60104)	Draws attention to unsuccessful audit events, indicating possible setup errors or security breaches
3	Incorrect Password or Unknown User-Login Failure (ID: 60122)	Indicates failed attempts at logging in, which may be a sign of efforts at unauthorized access.
4	Verify that "Allow Basic Authentication" is deactivated in the CIS Benchmark for Windows 10 Enterprise (ID: 19008).	Assures adherence to security standards, which is essential for keeping an environment safe.
5	Session Environment Not Able to Process Event Notification (ID: 60775)	Indicates problems with notification handling, which may impair system responsiveness.

Table 2: Analysis has been completed based on the top 5 rule groups.

No.	Events	No of alerts
1	Configuration Assessment (SCA)	397 alarms
2	Windows	38
3	Windows Security	21
4	Policy	17
5	Windows application	13

4.2.2 Report on Integrity Monitoring

The integrity monitoring report gave a thorough explanation of system integrity over time based on Figure 10 and the values are also shown in Table 3.



wazuh.

info@wazuh.com
https://wazuh.com

Alerts summary

File	Description	Count
c:\source_code1\new text document.txt	File added to the system.	1
c:\source_code1\new text document.txt	File deleted.	1
c:\source_code1\new text document.txt	Integrity checksum changed.	1
c:\source_code1\sample_fle.txt	File added to the system.	1
c:\source_code2\new_fle.txt	File added to the system.	1

Figure 10: Wazuh alert Summary

Table 3: Analysis of integrity report

No.	Events	No of Count
1	c:\source_code1\new text document.txt File added to the system	1
2	c:\source_code1\new text document.txt File deleted	1
3	c:\source_code1\new text document.txt Integrity checksum changed	1
4	c:\source_code1\sample_file.txt File added to the system	1
5	c:\source_code2\new_file.txt File added to the system.	1

5 CONCLUSIONS

The major goal of this project is to deploy the Wazuh SIEM system into place, which might improve the apparel sector's threat monitoring and detection system. Along with assuring adherence to security policies, this system can also identify proactive threats. The SIEM system is implemented using the Wazuh Manager, Wazuh Agents, and Wazuh Indexer. The following are advantages that users of the Wazuh security system will experience:

1. Users ought to be able to identify possible security threats and lessen their ability to affect the system.
2. A centralized management system that facilitates the assessment of the ICT security system.
3. Although Wazuh is an open-source solution, it is a well-known and efficient SIEM system at a reasonable price.
4. An automated reporting system that may help to comply with the regulatory requirements.

REFERENCES

[1] Šuškalo, D., Morić, Z., Redžepagić, J., & Regvart, D. (2023). Comparative analysis of IBM QRadar and Wazuh for security information and event management. The 34th DAAAM International Symposium, B. Katalinic (Ed.), Vienna, Austria.

[2] Moiz, S., Majid, A., Basit, A., Ebrahim, M., Abro, A. A., & Naeem, M. (2024). Security and Threat Detection through Cloud-Based Wazuh Deployment. IEEE 1st Karachi Section Humanitarian Tech Conf (KHI-HTC), Tandojam, Pakistan, 1-5.

[3] Stefan, S., Slavko G., & Ranko P. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. IEEE Proceedings, IX International Conference IcETRAN, Novi Pazar, Serbia, 6-9.

[4] Mulyadi, F., Annam, L.A., Promya, R. & Charnsripinyo, C. (2020). Implementing Dockerized Elastic Stack for Security Information and Event Management. 5th Int Conf on Information Tech (InCIT), Chonburi, Thailand, 243-248.

[5] Marwan, A. H. & Ekhlas K. H. (2022). Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM). International Journal of Intelligent Engineering & Systems; 15(6), 667-681.

[6] Resevoa, M. M., Indrarini, D. I., & Muhammad, I. (2021). Integrated Security System Implementation for Network Intrusion. Journal of Hunan University Natural Sciences, 48(6), 183-188.

[7] Zahid, H., Hina, S., Hayat, M.F. and Shah, G.A., 2023. Agentless approach for security information and event management in industrial iot. Electronics, 12(8), 1-26.

[8] Akshai, N., Sankar, & Fasila, K. A. (2023). Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring, 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 350-354.

[9] Francesco, A., Stefano, A., Vincenzo, C., Antonio, F., Enrico, F., Attibene, Federico, F., Daniele, L., Diego, M., & Lucia, M. (2024). General purpose data streaming platform for log analysis, anomaly detection, and security protection; EPJ Web of Conferences 295, 01032.

[10] Manzoor, J., Waleed, A., Jamali, A.F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLoS ONE 19(3): e0301183.

[11] James, S. & Improved, L. (2023), Monitoring using Host-based Intrusion Detection System, Advanced International Journal of Multidisciplinary Research. 1(1), 15-22.

[12] Akarshita, S. & Vijay, M. (2024). A Framework for Cybersecurity Alert Distribution and Response Network (ADRIAN), 17(5), 396-420.

[13] Marwan, A. H. & Ekhlas, K. H. (2023). Design and Implementation of Security Gateway for IoT Devices Security. Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE), 23(2), 95-111.

[14] Bassey, C., Ebenezer, T., Chinda, C. & Samson, I. (2024). Building a Scalable Security Operations Center: A Focus on Open-Source Tools. Journal of Engineering Research and Reports, 26 (7):196-209.

[15] Suryantoro, T., Purnomosidi, B. D. P. & Andriyani, W. (2022). The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods. 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 1-6.

[16] Adem, Ş., & Ahmet, K. (2023). Detection of Advanced Persistent Threats using SIEM Rulesets. International Journal of 3D Printing Technologies and Digital Industry. 7(3), 471-477.

[17] Bezzateev, S. V., Fomicheva, S. G. & Zhemelev, G. A. (2021). Agent-based ZeroLogon Vulnerability Detection. 2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 1-5.

[18] Zhu, H., Wang, C., Hou, B., Tang, Y. & Cai, Z. (2024). A Critical Server Security Protection Strategy Based on Traffic Log Analysis. In: Jin, H., Pan, Y., Lu, J. (eds) Computer Networks and IoT. IAIC 2023. Communications in Computer and Information Science, 2060.

[19] Cristiana, M. & Filipe, M. (2022). Impact of the GDPR on the Design of SIEM Solutions. CAPSI Proceedings, AIS eLibrary. [Available]: https://aisel.aisnet.org/capsi2022/

[20] Touloumis, K., Michalitsi-Psarrou, A., Kapsalis, P., Georgiadou, A & Askounis, D. (2021). Vulnerabilities Manager, a platform for linking vulnerability data sources. IEEE International Conference on Big Data, Orlando, FL, USA, 2178-2184.

[21] Ogruţan, P. L., & Titus, C. B. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors, 23(15), 6757.