Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol. 34 ; No. 2| 2026

Integrated Intrusion Detection System with Security Information and Event Management

Noor R. Obeid[1*]
[1]Department of Cyber Security, College of Information Technology, University of Babylon, noorrazaq@uobabylon.edu.iq, Babil, Iraq.

***Corresponding author email:** noorrazaq@uobabylon.edu.iq ; mobile: 07818519005

نظام متكامل لكشف التسلل مع إدارة معلومات الأمان والأحداث

نور رزاق عبيد[1*]
1قسم الأمن السيبراني، كلية تكنولوجيا المعلومات، جامعة بابل، noorrazaq@uobabylon.edu.iq ، بابل ، العراق

Accepted: 25/6/2026 **Published:** 30/6/2026

ABSTRACT

The blistering development of cyber threats and the growth in the sophistication of countermeasures have made conventional security measures inadequate to protect the contemporary network infrastructures. This paper introduces the design and deployment of an all-encompassing Security Information and Event Management (SIEM) solution deployed in a simulated Security Operations Center (SOC) setup. The targeted architecture is based on a multi-layered security stack, which includes Elastic Stack (ELK), Wazuh, Suricata, and Snort deployed on a virtualized network topology with heterogeneous endpoints, such as Windows Server 2019, Windows 10, and vulnerable legacy systems (Metasploitable 2 and 3), as well as coordinated by a PfSense firewall with segmented VLAN It enables centralized log aggregation, real-time event correlation, anomaly detection and automated alerting by accepting telemetry of both host-based and network-based intrusion detection and prevention systems (HIDS/HIPS and NIDS/NIPS). A controlled adversarial simulation was performed to test detection and response capabilities with industry-standard offensive tools, including Nmap, Metasploit Framework, SQLMap, hping3, and Atomic Red Team - which includes attack methods that are mapped to the MITRE ATT&CK framework (T1003, T1055, T1555), and network-layer attacks like SYN flooding, SQL injection, and Cross The findings of the experiments prove that the integrated SIEM solution was able to aggregate more than 61,000 security events, generate 511 classified alerts of different severity, and identify malware, unauthorized access attempts, credential dumping behavior and process injection behavior with high fidelity. The Wazuh EDR module had good active detection features, such as automated threat elimination and file integrity checks. In addition, the detection rule engine on Elastic Security has been able to perform more than 104,000 rule checks with a success rate of 49% among 1,007 enabled detection rules. The results confirm that open-source SIEM systems, correctly installed and configured, are a realistic and affordable alternative to more expensive tools, delivering an enterprise-level visibility and threat-detection system to organizations of all sizes. The future directions of the research are the addition of the machine learning-based anomaly detection, behavioral analytics, and the integration with the Security Orchestration, Automation, and Response (SOAR) to make the incident response more efficient.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Background:
Threats to cybersecurity are ever increasing in complexity and occurrence, making conventional security controls inadequate to identify more advanced attacks and evasive malware. Companies are increasingly using integrated security architectures to ensure visibility on a distributed network environment.

Materials and Methods:
VMware Workstation Pro was used to create a virtualized home laboratory, which consisted of several virtual machines on different VLANs. The deployment of open-source tools, including Elastic Stack (ELK), Wazuh, Suricata, and Snort were used and connected to create a full SIEM/IDS/EDR environment. Metasploit Framework, Hping3 and Atomic Red Team were used to carry out simulated attacks.

Results:
The combined system was able to gather logs of all the monitored virtual machines. Wazuh identified and graphically visualized numerous MITRE ATT&CK methods (T1003, T1055, T1555) and Elastic SIEM aggregated more than 61,000 events and issued 511 actionable notifications. The vulnerability scanner used by Wazuh found thousands of CVEs among monitored endpoints.

Conclusion:
Open-source SIEM, IDS/IPS, and EDR tools integrated can offer a low-cost but technically sound cybersecurity solution. The suggested system proves to be practically viable in terms of deployment in education, as well as small-to-middle enterprise settings, with multi-layered detection coverage that minimizes security blind spots considerably.

Key words: SIEM, IDS, IPS, EDR, Wazuh, Elastic Stack, Suricata, Snort, SOC, Cybersecurity, Network Security, Intrusion Detection.

INTRODUCTION

The high rate of proliferation of cyber threats and the increasing complexity of networked systems have made cybersecurity an urgent issue to both small and large organizations. The growing number of attacks such as malware, denial-of-service (DoS), and advanced persistent threats (APTs) have underscored the weaknesses of conventional security mechanisms [7]. These issues have necessitated the development of more advanced and integrated security solutions that can provide real-time monitoring, detection, and response to them. Security Information and Event Management (SIEM) systems have come to become a fundamental element of contemporary cybersecurity frameworks. SIEM platforms enable a centralized gathering, normalization, and matching security occasions coming via various sources, e.g. firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and endpoint devices. Centralization also allows security analysts to have a single perspective of the overall infrastructure, also known as a single pane of glass, enhancing situational awareness and decision-making efficiency [3][7]. Moreover, not all sophisticated cyberattacks can be identified by means of solitary tracking of particular systems. Multiplexing of network and host layer events is necessary to detect effectively. SIEM systems can help overcome this issue through the use of advanced analytical techniques such as rule-based correlation, anomaly detection, and behavioral analysis to identify latent attack patterns and reduce false positives. This might go a

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

long way in making Security Operations Centers (SOCs) more effective in detecting and responding to security incidents in real-time [2][11]. The current study intends to design, deploy, and test an integrated cybersecurity environment, which integrates the SIEM with the IDS/IPS and Endpoint Detection and Response (EDR) technologies in this context. The given system is entirely based on open-source tools that are installed on top of a virtualized home laboratory setup, which allows simulating enterprise environments and fully testing detection capabilities with a wide range of cyber threats [1][5].

2. RELATED WORK

The effectiveness and weaknesses of SIEM systems in contemporary cybersecurity settings have been researched in several studies. Makris tested the detection features of the open-source SIEM system HELK, showing that it can be used to process large amounts of security data, but with performance and scalability issues related to open-source deployments [4].

Vielberth et al. used a systematic review of Security Operations Centers (SOCs) and revealed that the main issues are alert fatigue, a high rate of false-positives and the growing workload of analysts. They have highlighted in their work that there is a necessity to enhance correlation methods and automation in SIEM systems in order to increase operational effectiveness [2].

Singh has discussed the use of SIEM with other related technologies like User and Entity Behavior Analytics (UEBA) and Security Orchestration, Automation, and Response (SOAR) and shown that a combination of these technologies can greatly enhance the accuracy of threat detection and incident response [3].

Hristov et al. suggested incorporating Splunk Enterprise SIEM to detect DDoS attacks within IoT systems, demonstrating that SIEM systems can successfully detect large-scale network malfunctions in combination with real-time monitoring technologies [1].

Abbas et al. have made an extensive review of the IDS and IPS detection methods: signature-based methods, anomaly-based methods, and hybrid methods and noted the significance of implementing more than one detection method to enhance the accuracy and resilience of the system [5].

Sani established the importance of using Host-based Intrusion Detection Systems (HIDS) together with the SIEM architectures to augment the visibility of endpoints and the detection of threats at the host endpoint [6].

The current work is based on such contributions, but it introduces a multi-layered SIEM environment, which incorporates both network-based and host-based detection, and integrates Elastic SIEM with Wazuh XDR/EDR capabilities in a single virtualized topology.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 1: Comparison of related work

Study	Techniques used	Focus Area	Limitations	Key Contributions
[1]	Splunk SIEM	DDoS Detection in IoT	Limited to IoT scenarios	Effective detection of DDoS attacks
[2]	SIEM Systems	SOC Analysis	No implementation framework	Identified SOC challenges (alert fatigue, workload)
[3]	SIEM, UEBA, SOAR	SIEM + UEBA + SOAR Integration	Limited real-world validation	Improved detection and response
[4]	HELK	Open-source SIEM Evaluation	Scalability concerns	Benchmarking SIEM performance
[5]	IDS, IPS	IDS/IPS Review	Theoretical (no implementation)	Classification of detection techniques
[6]	HIDS	Log Monitoring (HIDS)	Limited integration scope	Improved endpoint monitoring

3. MATERIALS AND METHODS

3.1 SIEM Definition and Architecture

The operation of SIEM software is based on the gathering of log and event data produced by host systems, security devices, and applications across the infrastructure of an organization and assembling it on a centralized platform. The normalized log data is usually stored three to six months to enable historical analysis as well as forensic analysis. This data is processed by a rule-based correlation engine based on behavioral analytics, anomaly detection, and external threat intelligence to produce actionable alerts to SOC analysts [7].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

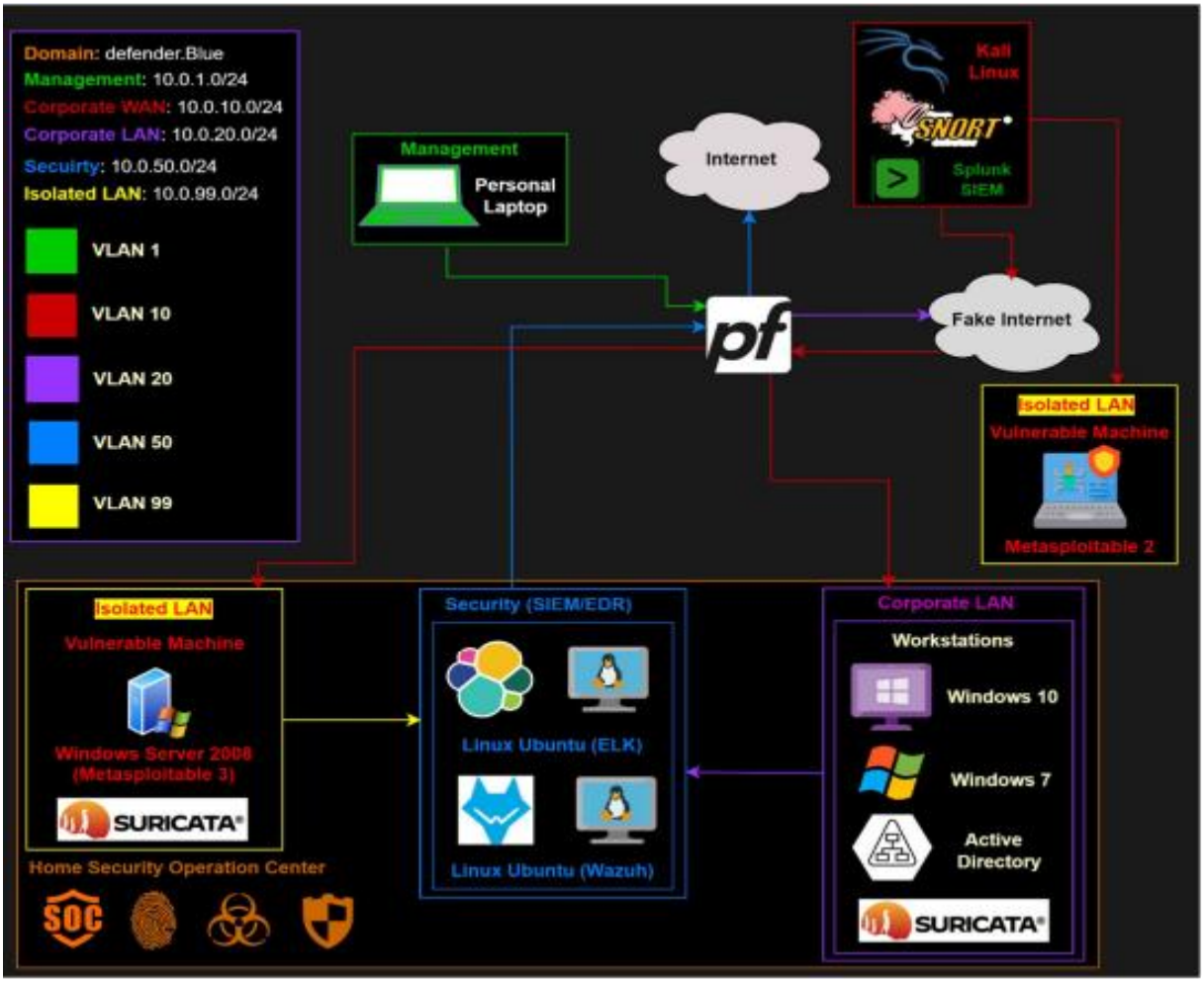

Figure (1): The Network Topology used

3.2 Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) identify and thwart security violations by observing the network traffic and system activity in real-time. The four major types of IDPS that were used in this study are summarized in Table 2.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 2. IDPS Types and Characteristics

Type	Abbrev.	Description	Action
Network-Based IDS	NIDS	Monitors inbound network traffic; compares against known attack signatures	Alert only
Network-Based IPS	NIPS	Scans inbound traffic; blocks malicious traffic before it enters the network	Block & Alert
Host-Based IDS	HIDS	Installed on individual hosts; monitors local activities and incoming traffic	Alert only
Host-Based IPS	HIPS	Installed on hosts; identifies and remediates threats, blocks unapproved actions	Block & Alert

3.3 Detection Methods

IDS systems are based on three main detection methodologies that have certain strengths and limitations [5]:

• Signature-Based Detection: Compares traffic on the network to a list of known attack signatures. Very precise with attacks that are familiar but useless when dealing with new zero-day attacks.

• Anomaly-Based Detection: This will give a normal behavior baseline and issue warnings when there is an aberration. Performs well in situations where threats not well understood but may result in large false-positive.

• Hybrid Detection: It is a mixture of signature and anomaly methods in order to reduce both false positives and false negatives.

3.4 The ELK Stack

ELK is a stack of four integrated components: Beats (data shippers that are lightweight), Logstash (data aggregation and processing pipeline), Elasticsearch (distributed indexing and storage engine), and Kibana (visualization and analysis dashboard). All these tools combine to create a robust SIEM platform that can ingest, enrich, index, and visualize security data on an enterprise scale [17].

3.5 Wazuh

Wazuh is an open-source and free security platform uniting XDR and SIEM endpoint and cloud workload protection. It offers intrusion detection, threat hunting, log management and compliance monitoring. Wazuh architecture consists of four key components namely Wazuh Indexer, Wazuh Server, Wazuh Dashboard and Wazuh Agent [16].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

4. PROPOSED SYSTEM DESIGN

4.1 Architecture Overview

The suggested system is a simulation of an enterprise Security Operations Center (SOC) in a home laboratory using VMware Workstation Pro. Several VLANs are configured with multiple virtual machines, and a pfSense firewall is the DHCP server and traffic controller. The architecture will isolate the attacker machines with the SIEM infrastructure and will also allow monitored machines to send their logs to the ELK and Wazuh SIEM servers [18].

4.2 Network Topology and VLANs

The network topology will be structured into five VLANs to provide adequate traffic segmentation and isolation of security as explained in Table 3.

Table 3. Network VLAN Configuration

VLAN	Network	Purpose
VLAN 1 (Management)	10.0.1.0/24	Management network for personal laptop and pfSense
VLAN 10 (Corporate WAN)	10.0.10.0/24	Attacker Kali Linux machine
VLAN 20 (Corporate LAN)	10.0.20.0/24	Windows workstations (Win10, Win7) and Domain Controller
VLAN 50 (Security)	10.0.50.0/24	ELK SIEM server and Wazuh SIEM server (isolated from Kali)
VLAN 99 (Isolated LAN)	10.0.99.0/24	Vulnerable machines: Metasploitable 2 and Metasploitable 3

4.3 Virtual Machines and Tools

Table 4 summarizes the virtual machines deployed in the laboratory, along with their operating systems and assigned roles.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 4. Virtual Machine Inventory

Machine	OS	Role / Tools
ELK-Ubuntu-Server	Ubuntu 22.04.3 LTS	ELK SIEM, Wazuh Agent, Fleet Server
Wazuh-Ubuntu-Server	Ubuntu 22.04.3 LTS	Wazuh SIEM/XDR/EDR, ELK Agent
Windows-Server-2019	Windows Server 2019	Domain Controller, ELK Agent, Wazuh Agent, Suricata
Metasploitable3	Windows Server 2008	Vulnerable target: ELK Agent, Wazuh Agent, DVWA
Windows 10	Windows 10 v22H2	Workstation target: ELK Agent, Wazuh Agent
pfSense Firewall	FreeBSD v2.7.1	DHCP, traffic filtering, VLAN routing
Attacker-Kali	Kali Linux (Debian)	NMAP, Hping3, Metasploit, Splunk+Snort

4.4 System Integration

Both SIEM platforms enrolled agents by special enrollment procedures. In the case of the ELK platform, a Fleet Server was set up on the ELK-ubuntu machine and Elastic Agents were installed on each host under monitoring with the help of enrollment tokens and TLS encryption. The following integrations were also provided in the agent policy: System (OS-level log collection), Elastic Defend (EDR), Suricata (network IDS via eve.json), and Zeek (network connection analysis) [15]. In the case of Wazuh, the agents were registered using the Wazuh Manager web interface by specifying the target operating system, server IP address (10.0.50.64), and running the generated command of the installation in each endpoint. All agent-server communications were secured with TLS/SSL authentication.

5. ATTACK SIMULATION AND TESTING

5.1 Reconnaissance — Network Scanning with NMAP

The attacker machine (Kali Linux, 10.0.10.60) began reconnaissance of VLAN 99 with a TCP SYN stealth scan (nmap -sSV 10.0.99.60). This method does not involve the three-way handshake completion, thus minimizing the detectability of the firewall connection logs. A scan of Metasploitable 2 showed 22 open ports, such as FTP (21), SSH (22), Telnet (23), HTTP (80), Samba (139/445), and VNC (5900), all with outdated and vulnerable versions of the services [14].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

5.2 Exploitation — Metasploitable 2

The Metasploit Framework (MSF) and related tools were used to exploit several vulnerabilities, as outlined in Table 5 .

Table 5. Exploitation Summary — Metasploitable 2

Attack	Port/Service	Tool	Result
FTP Backdoor (vsftpd 2.3.4)	21/FTP	MSF exploit/unix/ftp/vsftpd_234_backdoor	Root shell obtained
SSH Brute Force	22/SSH	MSF auxiliary/scanner/ssh/ssh_login	Credentials found
Samba Exploit	139/445 Samba	MSF exploit/multi/samba/usermap_script	Root shell via reverse netcat
VNC Brute Force	5900/VNC	MSF auxiliary/scanner/vnc/vnc_login	Login successful
DoS SYN Flood	All ports	Hping3 –flood	852,813 packets transmitted

5.3 Web Application Attacks — DVWA on Metasploitable 3

Two major web attack techniques were aimed at the Damn Vulnerable Web Application (DVWA) that was running on Metasploitable 3 (10.0.99.62). SQL Injection (SQLi) was conducted with the help of a manual payload (admin' OR '1'='1) to list all users of the database, and then SQLMap was applied to automatically exploit it, recognize MySQL as the back-end database management system, and retrieve the contents of tables. Reflected Cross-Site Scripting (XSS) was shown by entering a JavaScript alert payload into the DVWA XSS Reflected form, which was successfully executed within the browser context [9].

5.4 MITRE ATT&CK Simulations with Atomic Red Team

The Windows Server 2019 machine was configured with the Invoke-AtomicRedTeam PowerShell framework in order to implement three MITRE ATT&CK techniques and test their ability to be detected [12]:

T1003 - Credential Dumping: Attempted NPPSpy, Credential Manager and Gsecdump. Wazuh and Elastic were to identify the use of credentials.

• T1055 - Process Injection: It tried various approaches of injection, such as Shellcode Execution through VBA and LSASS Remote Process Injection through Mimikatz. Elastic Defend detected the malicious activity on the fly.

• T1555 - Credentials in Password Stores: LaZagne was run to get the credentials in Windows Credential Manager and LSA secrets, and two passwords were extracted successfully, and logs were recorded.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

6. RESULTS AND DISCUSSION

6.1 Wazuh SIEM Results

After all the simulated attacks were finished, the Wazuh dashboard offered detailed per-agent data. Table 6 generalizes the detection performance of the machines monitored.

Table 6. Wazuh Detection Performance Summary

Machine	Total Events	High Alerts (≥12)	Auth Failures	CVEs Found
Metasploitable3	5,999	80	26	2,295
Windows Server 2019	1,728	26	0	571
Windows 7 (Victim-PC)	2,923	54	0	1,959
Windows 10 (Win10)	6,237	41	0	—

Wazuh's MITRE ATT&CK module successfully mapped detected events to attack tactics including Defense Evasion, Persistence, Privilege Escalation, Initial Access, Execution, and Lateral Movement. The File Integrity Monitoring (FIM) module tracked all file additions, modifications, and deletions across all agents in real time. Wazuh's vulnerability detector identified thousands of CVEs, with Metasploitable3 alone yielding 74 critical and 1,514 high-severity vulnerabilities — providing actionable intelligence for prioritized remediation [16].

6.2 Elastic SIEM Results

The Elastic SIEM dashboard was used to consolidate 61,258 events of the Suricata integration alone and the Detection and Response module was used to produce 511 total alerts (356 Medium, 95 High, 60 Low). The Elastic platform revealed key findings that included: 87 high-severity Malware Prevention Alerts that were as a result of T1055 process injection attempts; 800+ logon attempts that were monitored and the source IP was attributed through the Windows Security dashboard; 675,804 network events that were captured across 22,273 unique Suricata flow IDs [11][17].

6.3 Splunk and Snort (Supplementary)

One more Splunk Enterprise version was installed on the Kali Linux machine that is integrated with Snort IDS additional monitoring. Snort also identified 216 events of 8 different sources but the best classification was Pilot Activity (64.8 percent), Non-Application Attack (17.8 percent) and Generic ICMP Event (6.9 percent). Snort was able to verify effectively the NMAP reconnaissance phase by identifying the TCP Port Scanning activities that came out of the attacker machine [1][11].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

CONCLUSIONS

This experiment outlined the design, implementation, and assessment of an integrated cybersecurity infrastructure utilizing SIEM, IDS/IPS, and EDR technologies with open-source technology in a virtualized home lab. The experimental findings validated that SIEM systems, when adequately combined with other complementary detection technology, offer a much better visibility in both network and host environments. Wazuh was able to map detected events to several MITRE ATT&CK techniques such as credential dumping (T1003), process injection (T1055) and credential access out of password stores (T1555), as well as Elastic SIEM aggregated over 61,000 events and emitted 511 actionable alerts using its correlation engine. The net effect of the network-based detection (Suricata, Snort) and host-based monitoring (Wazuh agents, Elastic Defend) was that they introduced overlapping layers of detection that significantly minimized security blind spots - neither would have provided the same extent of detection on its own. Automated vulnerability scanning identified by Wazuh allowed discovering thousands of CVEs on the monitored endpoints, highlighting the importance of SIEM platforms in facilitating active vulnerability management and prioritized remediation. However, it is also accepted that the nature of SIEM deployments is such that they produce considerable volumes of alerts, which require constant rule refinement and specialized analyst skills to appropriately deal with false positives . Overall, the results of the current research confirm that open-source SIEM systems, and in particular, the integration of Wazuh, Elastic Stack, Suricata, and Snort, is an affordable and technologically sound solution to the task of cybersecurity monitoring that can be deployed by both academic institutions and small-to-medium enterprises. Future research ought to investigate how machine learning-based anomaly detection, SOAR, and external threat intelligence feeds can be combined to further improve the accuracy and efficiency of detection.

FUTURE WORK

There are a number of promising lines of developing this research:

• AI and Machine Learning Integration: Explore the potential to use ML methods to improve threat detection by detecting and analyzing anomalies, recognizing patterns, and predicting, thereby improving accuracy and decreasing false-positive rates.

• Behavioral Analytics (UEBA): Learn about User and Entity Behavior Analytics to detect insider threats and APTs based on the analysis of deviations in a set of behavioral norms. SOAR Integration: Study the advantages of other SIEM-based integrations with Security Orchestration, Automation, and Response platforms to automate incident response processes and shorten mean time to respond (MTTR).

• Threat Intelligence Feeds: Add OSINT feeds and commercial threat intelligence feeds to the SIEM to enhance event correlation and provide the ability to proactively hunt down threats.

• Compliance Automation: Use the power of the SIEM to automate compliance reporting of the standards like GDPR, HIPAA, and PCI DSS, and minimize manual audit work.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Conflict of interests.

There are non-conflicts of interest.

References

[1] M. Hristov, M. Nenova, G. Iliev, and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT," 2021.
[2] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," IEEE Access, vol. 8, 2020.
[3] K. Singh, "Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab," 2020.
[4] C. Makris, "Evaluation of the Detection Capabilities of the Open Source SIEM HELK," 2020.
[5] S. H. Abbas, W. Naser, and A. Abbas, "Subject Review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," Global Journal of Engineering and Technology Advances, vol. 14, no. 2, 2023.
[6] J. Sani, "Improved Log Monitoring using Host-based Intrusion Detection System," 2023.
[7] A. Asswad, "Analysis of Attacks and Prevention Methods in Cybersecurity," Diss. University of Brescia, 2022.
[8] S. M. Othman et al., "Survey on Intrusion Detection System Types," International Journal of Cyber-Security and Digital Forensics, vol. 7, no. 4, 2018.
[9] M. Baklizi et al., "A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap," International Journal of Intelligent Systems and Applications in Engineering, vol. 10, no. 3, 2022.
[10] M. M. Islam et al., "Cyber-Security: DoS Attack Outcomes are Dangerous," European Journal of Electrical Engineering and Computer Science, vol. 5, no. 3, 2021.
[11] C. Yinka-Banjo et al., "Intrusion Detection using Anomaly Detection Algorithm and Snort," Illumination of AI in Cybersecurity and Forensics, Springer, 2022.
[12] J. Elgh, "Comparison of Adversary Emulation Tools for Reproducing Behavior in Cyber-Attacks," 2022.
[13] R. Iudica, "A Monitoring System for Embedded Devices Widely Distributed," Politecnico di Torino, 2022.
[14] M. Tabassum et al., "Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework," International Journal of Innovation in Computational Science and Engineering, vol. 2, no. 4, 2021.
[15] P. Veerasingam et al., "Intrusion Detection and Prevention System in SME's Local Network using Suricata," Malaysian Journal of Computing and Applied Mathematics, vol. 6, no. 1, 2023.
[16] Wazuh Official Documentation. [Online]. Available: https://wazuh.com
[17] Elastic Stack Documentation. [Online]. Available: https://www.elastic.co/elasticsearch
[18] pfSense Documentation. [Online]. Available: https://www.pfsense.org/download/
[19] Metasploitable3. [Online]. Available: https://github.com/rapid7/metasploitable3
[20] MITRE ATT&CK Framework. [Online]. Available: https://attack.mitre.org

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

الخلاصة

أدى التطور المتسارع للتهديدات السيبرانية وتزايد تعقيد التدابير المضادة إلى جعل التدابير الأمنية التقليدية غير كافية لحماية البنى التحتية للشبكات الحديثة. تقدم هذه الورقة تصميم ونشر حل شامل لإدارة معلومات وأحداث الأمان (SIEM) في بيئة محاكاة لمركز عمليات أمنية (SOC). يعتمد التصميم المستهدف على بنية أمنية متعددة الطبقات، تشمل ELK (Elastic Stack) وWazuh وSuricata وSnort، موزعة على بنية شبكة افتراضية ذات نقاط نهاية متنوعة، مثل Windows Server 2019 وWindows 10 وأنظمة قديمة معرضة للاختراق (Metas و3)، وذلك بالتنسيق مع جدار حماية PfSense متطور مزود بشبكات VLAN مجزأة. يتيح هذا الحل تجميع السجلات مركزياً، وربط الأحداث في الوقت الفعلي، واكتشاف الحالات الشاذة، والتنبيهات الآلية، وذلك من خلال استقبال بيانات القياس عن بُعد لأنظمة كشف ومنع الاختراق القائمة على المضيف والشبكة (HIDS/HIPS وNIDS/NIPS). أُجريت محاكاة معادية مُحكمة لاختبار قدرات الكشف والاستجابة باستخدام أدوات هجومية قياسية في المجال، بما في ذلك Nmap وMetasploit Framework وSQLMap وhping3 وAtomic Red Team، والتي تتضمن أساليب هجوم مُطابقة لإطار عمل MITER ATT&CK (T1003، T1055، T1055)، وشبكات الطبقة الأولى مثل هجمات SYN flooding وSQL Injection وCross. أثبتت نتائج التجارب أن حل SIEM المُدمج قادر على تجميع أكثر من 61,000 حدث أمني، وتوليد 511 تنبيهًا مُصنفًا بدرجات خطورة مُختلفة، وتحديد البرامج الضارة ومحاولات الوصول غير المُصرح بها وسلوكيات تسريب بيانات الاعتماد وسلوكيات المعالجة بدقة عالية. يتميز مُكوّن Wazuh EDR بميزات كشف نشطة جيدة، مثل الإزالة التلقائية للتهديدات وفحوصات سلامة الملفات. بالإضافة إلى ذلك، تمكن مُحرك قواعد الكشف في Elastic Security من إجراء أكثر من 104,000 فحص قاعدة بنسبة نجاح 49% من بين 1,007 قواعد كشف مُفعّلة. تؤكد النتائج أن أنظمة إدارة معلومات الأمان والأحداث (SIEM) مفتوحة المصدر، عند تثبيتها وتكوينها بشكل صحيح، تُعد بديلاً واقعياً وميسور التكلفة للأدوات الأكثر تكلفة، حيث توفر نظاماً متكاملاً للكشف عن التهديدات والرؤية الشاملة للمؤسسات من جميع الأحجام. وتشمل التوجهات المستقبلية للبحث إضافة تقنيات الكشف عن الحالات الشاذة القائمة على التعلم الآلي، وتحليلات السلوك، والتكامل مع نظام أتمتة وتنسيق الاستجابة الأمنية (SOAR) لتعزيز كفاءة .

المقدمة:

تتزايد التهديدات للأمن السيبراني باستمرار من حيث التعقيد والتكرار، مما يجعل ضوابط الأمان التقليدية غير كافية لكشف الهجمات الأكثر تطوراً والبرمجيات الخبيثة المراوغة. ولذلك، تلجأ الشركات بشكل متزايد إلى استخدام بنى أمنية متكاملة لضمان الرؤية الشاملة في بيئة الشبكات الموزعة.

طرق العمل:

استُخدم برنامج VMware Workstation Pro لإنشاء مختبر منزلي افتراضي، يتألف من عدة أجهزة افتراضية موزعة على شبكات VLAN مختلفة. وتمّ نشر أدوات مفتوحة المصدر، بما في ذلك ELK (Elastic Stack) وWazuh وSuricata وSnort، وربطها معًا لإنشاء بيئة SIEM/IDS/EDR متكاملة. كما استُخدمت أدوات Metasploit Framework وHping3 وAtomic Red Team لتنفيذ هجمات محاكاة.

الاستنتاجات:

يمكن أن توفر أدوات SIEM وIDS/IPS وEDR مفتوحة المصدر المتكاملة حلاً منخفض التكلفة ولكنه متين تقنيًا للأمن السيبراني. وقد أثبت النظام المقترح جدواه العملية من حيث النشر في قطاع التعليم، وكذلك في بيئات الشركات الصغيرة والمتوسطة، مع تغطية كشف متعددة الطبقات تقلل بشكل كبير من الثغرات الأمنية.

الكلمات المفتاحية: SIEM، IDS، IPS، EDR، Wazuh، Elastic Stack، Suricata، Snort، SOC، الأمن السيبراني، أمن الشبكات، كشف التسلل.