КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1211
UDC 004.056:004.8

Ganna Grynkevych
PhD, Associate Professor,
Professor of the Department of Telecommunication Systems and Networks
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-1922-5165
ggrynkevych@ukr.net

Volodymyr Vasylenko
PhD, Associate Professor,
Associate Professor of the Department of Computer Science
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-8465-6178
oknelisavvova172@gmail.com

Dmytro Rudin
Platform Engineer
Capital One, Plano, Texas, USA
ORCID: 0009-0007-4171-4973
itelecombox@gmail.com

LOCAL OPEN-SOURCE PLATFORM FOR CYBER INCIDENT MONITORING AND RESPONSE WITH AI SUPPORT AS AN ALTERNATIVE TO EDR/XDR SOLUTIONS

Abstract. The paper presents an approach to designing a local cybersecurity monitoring and incident response platform based on open-source technologies with integrated artificial intelligence support. The relevance of the study is driven by the growing complexity of cyber threats, the increasing number of endpoints in modern infrastructures, and the need for continuous monitoring and rapid response within Security Operations Centers. Traditional EDR and XDR solutions provide high levels of automation and detection capabilities but rely on subscription-based models that introduce long-term operational constraints and limit flexibility in infrastructure management. The study examines the functional roles of EDR, XDR, SIEM, and SOC within enterprise environments and identifies key challenges related to scalability, data ownership, and dependency on proprietary platforms. Particular attention is given to the limitations of centralized commercial solutions when applied to distributed infrastructures with hundreds of managed endpoints. The paper proposes a model of a local cybersecurity platform that integrates endpoint monitoring, event correlation, and log management within a unified architecture. The proposed solution is based on Wazuh for endpoint detection and SIEM functions, OpenSearch-compatible indexing for event storage and analytics, and on-premises storage systems for secure and scalable log retention. A dedicated local AI analysis layer is introduced to support SOC processes by automating alert summarization, correlating related events, generating hypotheses about incident origins, and assisting analysts in decision-making without exposing sensitive data to external services. The results include a description of the system architecture, hardware configuration, data processing workflows, and storage strategies. The proposed approach emphasizes transparency, flexibility, and adaptability to specific organizational requirements. Additionally, the model incorporates a structured proof-of-concept methodology to evaluate detection coverage, system performance, and the effectiveness of AI-assisted workflows. The study demonstrates that the integration of open-source tools with local AI capabilities can enhance the efficiency of cybersecurity operations while maintaining control over data and infrastructure. The proposed platform provides a viable alternative to traditional EDR/XDR solutions in scenarios where customization, cost predictability, and data sovereignty are critical factors.

Keywords: cyber incident response; endpoint security monitoring; security analytics; threat detection systems; open-source security platform; AI-assisted analysis; SOC operations.

INTRODUCTION

Modern information systems operate in an environment characterized by a continuous increase in the complexity of cyber threats, driven by the rapid expansion of digital infrastructures and the growing level of automation in attack techniques. The proliferation of endpoints, integration of cloud services, and interconnection of heterogeneous systems lead to the generation of large volumes of security events that require continuous monitoring and timely analysis. Under such conditions, traditional approaches focused primarily on preventive protection are no longer sufficient and must be complemented by detection and response mechanisms [1, 2].

In current cybersecurity practice, EDR and XDR solutions play a central role by providing visibility into endpoint activities, enabling the detection of anomalous behavior, and supporting incident response processes. These systems aggregate telemetry from multiple sources and facilitate correlation of events, allowing organizations to identify complex and multi-stage attacks. Their effectiveness, however, depends heavily on the capabilities of Security Operations Centers, which are responsible for analyzing alerts, prioritizing threats, and coordinating response actions [3, 8].

Another important trend is the integration of artificial intelligence technologies into cybersecurity workflows. Recent approaches focus on applying machine learning models and large language models to process large volumes of data, automate incident analysis, and support decision-making within SOC environments. This contributes to reducing analysis time and improving the quality of threat assessment, especially in environments with high event density [4, 9].

At the same time, the adoption of commercial EDR/XDR platforms introduces several limitations. These include dependency on vendors, restricted flexibility in system configuration, and high operational costs associated with subscription-based licensing models. Such constraints become more pronounced in infrastructures with a large number of endpoints, where scaling directly increases the total cost of ownership.

As a result, there is growing interest in alternative approaches based on open-source technologies and on-premises deployment models. These approaches allow organizations to retain control over their data, increase transparency of system behavior, and adapt architectures to specific operational requirements. Additional benefits can be achieved through the integration of local AI components, which enable advanced analytical capabilities without transferring sensitive data to external services [12, 13].

Problem statement. Despite the significant progress in cybersecurity monitoring systems, the problem of designing an efficient and cost-effective infrastructure for incident detection and response in large-scale environments remains unresolved. Commercial EDR/XDR solutions provide high levels of automation and integration, but their deployment is associated with substantial recurring costs and limited adaptability.

Open-source solutions, on the other hand, offer flexible tools for building monitoring systems, including data collection, correlation, and storage. However, their effective use requires the integration of multiple components and additional effort in configuration and maintenance. Furthermore, the potential of local artificial intelligence in enhancing SOC operations within such architectures is not yet fully explored.

Therefore, a practical and research-oriented challenge arises in developing a model of a local cybersecurity monitoring and response platform that combines the flexibility of open-source tools with the analytical capabilities of AI, while maintaining a high level of functionality and reducing dependency on proprietary solutions.

Analysis of recent research and publications. Recent studies in cybersecurity focus on the development of detection systems, behavioral analysis of endpoints, and event correlation in distributed environments. Frameworks such as MITRE ATT&CK provide structured knowledge about adversarial techniques and are widely used as a foundation for designing detection and monitoring systems [1].

A significant body of research is dedicated to SIEM and XDR platforms, which enable centralized collection and analysis of security events from diverse sources. These systems improve detection capabilities by correlating data across endpoints, networks, and applications, allowing identification of sophisticated attack patterns [6, 7].

In parallel, there is increasing attention to the application of artificial intelligence in cybersecurity. Recent works explore the use of machine learning and large language models to automate event analysis, detect anomalies, and assist analysts in decision-making processes [4, 5, 10]. Some studies specifically investigate the role of AI in SOC environments, highlighting its potential to improve efficiency and reduce cognitive load on analysts [9, 11].

However, most existing research focuses either on commercial solutions or on individual open-source tools, without addressing the integration of these components into a unified and efficient architecture. The combination of open-source platforms with local AI-based analytical layers for supporting SOC operations remains insufficiently explored, particularly in the context of real-world deployment and scalability [14, 15].

Thus, there is a need for a comprehensive approach that integrates open-source cybersecurity tools with modern AI technologies to create an effective platform for monitoring and responding to cyber incidents.

Purpose of the article. The purpose of this article is to develop and substantiate a model of a local cybersecurity monitoring and incident response platform based on open-source technologies with integrated artificial intelligence support for SOC processes, which can serve as an alternative or complement to commercial EDR/XDR solutions in large-scale environments with a significant number of endpoints.

To achieve this purpose, the following research objectives are defined:

1. To analyze current approaches to cybersecurity monitoring, including EDR, XDR, SIEM, and SOC frameworks.
2. To identify the limitations of commercial EDR/XDR solutions in terms of scalability, flexibility, and long-term operational costs.
3. To design a local open-source architecture that enables efficient collection, correlation, and storage of security events.
4. To justify the integration of a local AI analysis layer for supporting SOC operations, including alert summarization, event correlation, and decision support.
5. To evaluate the resource requirements of the proposed system, including hardware configuration, data storage, and processing capabilities.
6. To compare different deployment strategies, including full replacement, hybrid models, and continued use of commercial solutions.
7. To identify potential limitations and risks of the proposed approach and define criteria for evaluating its effectiveness during a proof-of-concept implementation.

THEORETICAL FOUNDATIONS OF THE STUDY

The development of modern cybersecurity monitoring systems is based on a set of concepts and technological approaches that define how threats are detected, analyzed, and mitigated within complex digital environments. A key shift in recent years has been the transition from preventive security models to detection-driven approaches, where continuous monitoring and behavioral analysis play a central role [1, 2].

One of the fundamental components of such systems is Endpoint Detection and Response (EDR). EDR focuses on collecting and analyzing telemetry from endpoints, including process execution, file system activity, and network interactions. This enables the identification of malicious behavior that may not be detected by traditional signature-based methods. EDR systems also support incident investigation and remediation by providing detailed contextual information about security events.

Extended Detection and Response (XDR) expands the capabilities of EDR by integrating data from multiple sources, such as network traffic, cloud services, identity systems, and application logs. This integrated approach allows for more effective detection of complex, multi-stage attacks that span different layers of the infrastructure. XDR platforms rely heavily on correlation mechanisms that combine heterogeneous data to identify patterns indicative of advanced threats [6, 7].

Another essential element is Security Information and Event Management (SIEM), which provides centralized collection, storage, and analysis of security logs. SIEM systems enable organizations to aggregate data from diverse sources, perform event correlation, and support compliance requirements. They also serve as a foundation for historical analysis and forensic investigations.

The operational aspect of cybersecurity monitoring is represented by Security Operations Centers (SOC), which integrate people, processes, and technologies to ensure continuous monitoring and incident response. SOC analysts are responsible for interpreting alerts, prioritizing incidents, and coordinating response actions. The effectiveness of a SOC depends not only on the underlying technologies but also on the ability to process large volumes of data efficiently.

In this context, artificial intelligence has emerged as a significant enabler for enhancing cybersecurity operations. Machine learning techniques are used to detect anomalies, classify events, and reduce false positives. More recently, large language models have been introduced to support analytical workflows by summarizing alerts, correlating events, and providing natural language explanations for complex incidents [4, 9, 10]. These capabilities are particularly valuable in SOC environments, where analysts are required to process large amounts of information under time constraints.

Despite the advantages of AI integration, its application in cybersecurity must be carefully controlled. In many cases, AI is used as a decision-support tool rather than an autonomous system, ensuring that critical response actions remain under human supervision. This approach reduces the risk of incorrect automated decisions while still leveraging the efficiency gains provided by AI technologies.

The combination of EDR, XDR, SIEM, and AI-supported SOC processes forms the theoretical basis for the design of modern cybersecurity monitoring platforms. However, the implementation of these concepts varies significantly depending on whether proprietary or open-source solutions are used. This creates the need for research into architectures that can integrate these components effectively while maintaining flexibility, scalability, and control over data.

METHODOLOGY OF THE STUDY

The research methodology is based on a combined analytical and design-oriented approach aimed at developing and evaluating a local cybersecurity monitoring and incident response platform. The study integrates theoretical analysis of existing cybersecurity frameworks with practical modeling of a system architecture applicable to enterprise environments with a large number of endpoints.

The research process consisted of several stages. At the initial stage, an analysis of current cybersecurity monitoring approaches was conducted, focusing on EDR, XDR, SIEM, and SOC models. This stage included the identification of key functional components, typical architectural patterns, and limitations associated with commercial and open-source solutions.

At the next stage, a conceptual model of the proposed system was developed. The model is based on the integration of open-source tools for endpoint monitoring, event processing, and data storage, combined with a local artificial intelligence layer for analytical support. The architecture was designed to ensure scalability, fault tolerance, and adaptability to different operational requirements.

The experimental basis of the study is a modeled enterprise environment consisting of approximately 600 endpoints, including systems running different operating systems such as Windows, macOS, and Linux. The infrastructure includes components for data collection, centralized processing, storage, and analysis. Special attention was given to simulating realistic data ingestion rates and operational workloads typical for such environments.

The evaluation of the proposed model was carried out using a set of criteria that reflect both technical and operational aspects of cybersecurity systems. The main evaluation parameters include:

- detection capability, defined as the ability to identify known attack techniques;
- false positive rate, reflecting the accuracy of alert generation;
- processing efficiency, measured by the time required to analyze and respond to events;
- scalability, defined as the system’s ability to handle increasing data volumes;
- resource utilization, including hardware and storage requirements;
- operational impact on SOC processes, including workload distribution and response time.

In addition, a scenario-based evaluation approach was applied, considering different deployment models such as full replacement of commercial EDR/XDR systems, hybrid configurations, and baseline scenarios using proprietary solutions. This allowed for a comparative analysis of system performance and operational efficiency under varying conditions.

A structured proof-of-concept methodology was also incorporated into the research. The proposed evaluation framework includes staged deployment, system tuning, and validation using predefined metrics such as detection rate, alert accuracy, and reduction in analyst workload. This approach ensures that the proposed architecture can be assessed in conditions that closely resemble real-world operational environments.

Overall, the methodology combines theoretical analysis, system design, and scenario-based evaluation, providing a comprehensive foundation for assessing the feasibility and effectiveness of the proposed cybersecurity monitoring platform.

RESULTS OF THE STUDY

System Architecture. The proposed cybersecurity monitoring and response platform is based on a modular architecture that integrates open-source components and a local artificial intelligence layer. The system is designed for environments with a large number of endpoints and supports continuous monitoring and incident response processes.

The architecture includes endpoint agents deployed on Windows, macOS, and Linux systems. These agents collect telemetry data, including system events, process activity, and network interactions. The collected data is transmitted to a centralized processing layer based on Wazuh, where initial analysis and rule-based detection are performed.

The Wazuh manager cluster is responsible for event correlation and aggregation. It enables the identification of suspicious patterns and supports alert generation. Processed data is forwarded to the indexing layer based on OpenSearch, which provides efficient storage, search, and visualization capabilities.

The system also includes a centralized storage component implemented on on-premises infrastructure, which ensures secure and scalable log retention. A local artificial intelligence layer is integrated into the architecture to support analytical processes within the SOC. This component processes security events and provides additional insights to analysts.

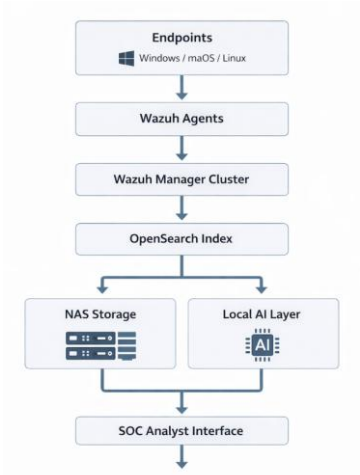

Fig. 1. Architecture of the proposed cybersecurity monitoring and response platform

Data Processing and AI-Assisted Analysis. The proposed system processes large volumes of security events generated by endpoints. Event data is collected, normalized, and enriched before being indexed for further analysis. The AI component enhances this process by providing analytical support rather than replacing human decision-making.

The main functions of the AI layer include summarization of alerts, correlation of events from different sources, identification of potential attack scenarios, and generation of recommendations for incident response. The use of natural language explanations allows analysts to better understand complex incidents and reduces the time required for investigation.

This approach improves the efficiency of SOC operations by reducing manual workload and enabling faster decision-making. At the same time, the system maintains human control over critical actions, which is important for minimizing the risks associated with automated responses.

Comparative Analysis of Deployment Approaches. To evaluate the effectiveness of the proposed solution, three deployment approaches were analyzed. These include the use of commercial EDR or XDR platforms, a fully open-source architecture, and a hybrid model that combines both approaches.

Table 1

Comparison of cybersecurity monitoring approaches

Approach	Initial Cost	Operational Cost	Flexibility	Vendor Dependency
Commercial EDR/XDR	Low	High	Limited	High
Open-source platform	Medium	Low	High	Low
Hybrid model	Medium	Medium	Moderate	Moderate

The comparison shows that open-source solutions provide higher flexibility and better control over infrastructure, while commercial platforms offer higher levels of automation. The hybrid model can be considered as a transitional approach that balances these characteristics.

Resource and Performance Considerations. The proposed architecture requires a distributed infrastructure to ensure stable performance. The system must handle continuous data ingestion from multiple endpoints and support real-time analysis. The performance depends on data volume, indexing efficiency, and computational resources available for processing.

Scalability is achieved by distributing system components across multiple nodes. This allows the system to adapt to increasing workloads without significant performance degradation. Storage requirements depend on data retention policies and the level of logging detail.

Limitations and Practical Considerations. The implementation of the proposed model requires additional effort related to system configuration and integration of multiple components. The absence of fully automated

response mechanisms increases the reliance on SOC analysts. In addition, tuning detection rules is necessary to reduce false positive alerts.

The use of a local AI component introduces additional computational requirements and requires careful configuration to ensure reliable operation. Despite these limitations, the proposed approach provides a flexible and controllable alternative to commercial cybersecurity solutions.

CONCLUSIONS AND FUTURE RESEARCH

The study presents a model of a local cybersecurity monitoring and incident response platform based on open-source technologies and supported by artificial intelligence. The proposed approach integrates endpoint monitoring, centralized event processing, and AI-assisted analysis into a unified architecture designed for large-scale environments. The results demonstrate that it is possible to achieve a functional level comparable to EDR and XDR solutions while maintaining control over data and system configuration. The use of open-source components provides flexibility in system design and allows adaptation to specific operational requirements. At the same time, the integration of a local AI layer improves the efficiency of SOC processes by supporting event analysis, reducing investigation time, and assisting in decision-making.

The comparative analysis confirms that the proposed architecture offers advantages in terms of long-term operational cost predictability and reduced dependency on proprietary platforms. The system also supports scalability through modular deployment and distributed processing of security data. At the same time, the study identifies several limitations. These include the need for additional configuration and integration efforts, the absence of fully automated response mechanisms, and increased requirements for technical expertise. The effectiveness of the system depends on proper tuning and continuous maintenance.

Future research directions include practical implementation of the proposed model in a real organizational environment and experimental evaluation of its performance. Further work may focus on improving AI-assisted analysis, optimizing detection rules, and enhancing the automation of response processes. Additional attention should be given to evaluating system performance using quantitative metrics such as detection accuracy, false positive rates, and response time.

REFERENCES

1. MITRE Corporation. (2024). *MITRE ATT&CK® framework*. https://attack.mitre.org
2. National Institute of Standards and Technology (NIST). (2022). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. https://doi.org/10.6028/NIST.SP.800-53r5
3. National Institute of Standards and Technology (NIST). (2023). *Guide to cyber threat information sharing (SP 800-150)*. https://doi.org/10.6028/NIST.SP.800-150
4. Srinivas, S., et al. (2025). *AI-augmented SOC: A survey of LLMs and agents for cybersecurity operations*. https://www.mdpi.com/2624-800X/5/4/95
5. Sharma, A. (2025). *Explainable artificial intelligence in cybersecurity: A comprehensive review*. https://www.sciencedirect.com/science/article/pii/S2405959525001584
6. Mohamed, N. (2025). *Cutting-edge advances in AI and machine learning for cybersecurity*. https://www.tandfonline.com/doi/full/10.1080/23311975.2025.2518496
7. Aboudrar, Y., Bouragba, K., & Ouzzif, M. (2025). *AI-driven firewall log analysis: Enhancing threat detection with deep learning techniques*. https://thesai.org/Downloads/Volume16No7/Paper_79-AI_Driven_Firewall_Log_Analysis.pdf
8. Binbeshr, F. (2025). *The rise of cognitive SOCs: A systematic literature review*. https://www.computer.org/csdl/journal/oj/2025/01/10858372
9. Singh, R., et al. (2025). *LLMs in the SOC: An empirical study of human-AI collaboration in security operations centres*. https://arxiv.org/abs/2508.18947
10. Sahay, R., et al. (2026). *Policy-guided threat hunting: An LLM-enabled framework with SOC triage*. https://arxiv.org/abs/2603.23966
11. Omar, M. (2024). *Integrative approaches in cybersecurity and artificial intelligence*. https://arxiv.org/abs/2408.05888
12. Schneuwly Purdie, M. (2025). *AI-powered SOC operations: Cybersecurity incident response and management*. https://www.researchgate.net/publication/389350761
13. Microsoft. (2024). *Security Copilot: AI for cybersecurity*. https://www.microsoft.com/security/copilot
14. Vectra AI. (2024). *AI-driven threat detection platform overview*. https://www.vectra.ai
15. Gartner Research. (2025). *Continuous threat exposure management (CTEM) framework overview*. https://www.gartner.com

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Ганна Гринкевич
Доктор технічних наук, доцент
Професор кафедри телекомунікаційних систем та мереж
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-1922-5165
ggrynkevych@ukr.net

Володимир Василенко
Кандидат технічних наук, доцент
Доцент кафедри комп'ютерних наук
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0001-8465-6178
oknelisavvova172@gmail.com

Дмитро Рудін
Platform Engineer
Capital One, Plano, Texas, USA
ORCID: 0009-0007-4171-4973
itelecombox@gmail.com

ЛОКАЛЬНА ПЛАТФОРМА З ВІДКРИТИМ ВИХІДНИМ КОДОМ ДЛЯ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ЯК АЛЬТЕРНАТИВА РІШЕННЯМ EDR/XDR

Анотація. У статті представлено підхід до проєктування локальної платформи моніторингу кібербезпеки та реагування на інциденти на основі технологій з відкритим вихідним кодом із інтегрованою підтримкою штучного інтелекту. Актуальність дослідження зумовлена зростаючою складністю кіберзагроз, збільшенням кількості кінцевих точок у сучасних інфраструктурах, а також необхідністю безперервного моніторингу та оперативного реагування в межах центрів операцій безпеки (SOC). Традиційні рішення класу EDR та XDR забезпечують високий рівень автоматизації та можливостей виявлення, однак базуються на підписках моделях, що створюють довгострокові операційні обмеження та знижують гнучкість управління інфраструктурою. У дослідженні розглянуто функціональні ролі EDR, XDR, SIEM та SOC в корпоративних середовищах і визначено ключові виклики, пов'язані з масштабованістю, володінням даними та залежністю від пропрієтарних платформ. Особливу увагу приділено обмеженням централізованих комерційних рішень при їх застосуванні в розподілених інфраструктурах із сотнями керованих кінцевих точок. У роботі запропоновано модель локальної платформи кібербезпеки, що об'єднує моніторинг кінцевих точок, кореляцію подій та управління журналами в межах єдиної архітектури. Запропоноване рішення базується на використанні Wazuh для функцій виявлення загроз на кінцевих точках і SIEM, індексації подій із сумісністю з OpenSearch для зберігання та аналітики, а також локальних систем зберігання даних для забезпечення безпечного та масштабованого зберігання журналів. Введено окремий локальний рівень аналізу на основі штучного інтелекту для підтримки процесів SOC, який забезпечує автоматичне узагальнення сповіщень, кореляцію пов'язаних подій, формування гіпотез щодо джерел інцидентів і допомогу аналітикам у прийнятті рішень без передачі чутливих даних до зовнішніх сервісів. Результати дослідження включають опис архітектури системи, апаратної конфігурації, процесів обробки даних та стратегій зберігання. Запропонований підхід акцентує увагу на прозорості, гнучкості та адаптивності до специфічних вимог організації. Крім того, модель передбачає використання структурованої методології proof-of-concept для оцінки покриття виявлення, продуктивності системи та ефективності процесів із використанням штучного інтелекту. Дослідження демонструє, що інтеграція інструментів з відкритим вихідним кодом із локальними можливостями штучного інтелекту дозволяє підвищити ефективність операцій кібербезпеки, зберігаючи контроль над даними та інфраструктурою. Запропонована платформа є практичною альтернативою традиційним рішенням класу EDR/XDR у сценаріях, де критичними є кастомізація, передбачуваність витрат та суверенність даних.

Ключові слова: реагування на кіберінциденти, моніторинг безпеки кінцевих пристроїв, аналітика безпеки, системи виявлення загроз, платформа безпеки з відкритим вихідним кодом, аналіз із використанням штучного інтелекту, операції центру моніторингу безпеки (SOC).

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. MITRE Corporation. (2024). *MITRE ATT&CK® framework*. https://attack.mitre.org
2. National Institute of Standards and Technology (NIST). (2022). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. https://doi.org/10.6028/NIST.SP.800-53r5
3. National Institute of Standards and Technology (NIST). (2023). *Guide to cyber threat information sharing (SP 800-150)*. https://doi.org/10.6028/NIST.SP.800-150
4. Srinivas, S., et al. (2025). *AI-augmented SOC: A survey of LLMs and agents for cybersecurity operations*. https://www.mdpi.com/2624-800X/5/4/95
5. Sharma, A. (2025). *Explainable artificial intelligence in cybersecurity: A comprehensive review*. https://www.sciencedirect.com/science/article/pii/S2405959525001584
6. Mohamed, N. (2025). *Cutting-edge advances in AI and machine learning for cybersecurity*. https://www.tandfonline.com/doi/full/10.1080/23311975.2025.2518496
7. Aboudrar, Y., Bouragba, K., & Ouzzif, M. (2025). *AI-driven firewall log analysis: Enhancing threat detection with deep learning techniques*. https://thesai.org/Downloads/Volume16No7/Paper_79-AI_Driven_Firewall_Log_Analysis.pdf
8. Binbeshr, F. (2025). *The rise of cognitive SOCs: A systematic literature review*. https://www.computer.org/csdl/journal/oj/2025/01/10858372
9. Singh, R., et al. (2025). *LLMs in the SOC: An empirical study of human-AI collaboration in security operations centres*. https://arxiv.org/abs/2508.18947
10. Sahay, R., et al. (2026). *Policy-guided threat hunting: An LLM-enabled framework with SOC triage*. https://arxiv.org/abs/2603.23966
11. Omar, M. (2024). *Integrative approaches in cybersecurity and artificial intelligence*. https://arxiv.org/abs/2408.05888
12. Schneuwly Purdie, M. (2025). *AI-powered SOC operations: Cybersecurity incident response and management*. https://www.researchgate.net/publication/389350761
13. Microsoft. (2024). *Security Copilot: AI for cybersecurity*. https://www.microsoft.com/security/copilot
14. Vectra AI. (2024). *AI-driven threat detection platform overview*. https://www.vectra.ai
15. Gartner Research. (2025). *Continuous threat exposure management (CTEM) framework overview*. https://www.gartner.com

Отримано редакцією журналу / Received: 08.02.26
Прорецензовано / Revised: 21.02.26
Схвалено до друку / Accepted: 25.06.26