УДК 004.056.42

А.А. Булаївський

Н.Р. Кондратенко

РОЛЬ SIEM-СИСТЕМ У ВИЯВЛЕННІ ТА РЕАГУВАННІ НА ІНЦИДЕНТИ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація. *У роботі розглянуто роль SIEM-систем (систем управління інформацією та подіями безпеки) у забезпеченні проактивного захисту інформаційної інфраструктури. Проаналізовано архітектуру типових рішень, таких як Splunk, IBM QRadar та ELK Stack, а також протестовано сценарії виявлення інцидентів і автоматизованого реагування. Встановлено, що впровадження SIEM дозволяє значно скоротити середній час реагування на загрози та підвищити ефективність виявлення складних атак. Отримані результати підтверджують доцільність використання таких систем для підвищення рівня кіберзахисту в корпоративному середовищі.*

Ключові слова: SIEM, кібербезпека, інциденти, моніторинг, автоматизація, кореляція подій, Splunk, IBM QRadar.

Abstract. *The paper examines the role of SIEM systems (Security Information and Event Management) in ensuring proactive protection of information infrastructure. It analyzes the architecture of common solutions such as Splunk, IBM QRadar, and ELK Stack, and tests scenarios involving incident detection and automated response. It has been found that implementing SIEM significantly reduces average response time to threats and improves the detection of complex attacks. The obtained results confirm the relevance of using such systems to enhance cybersecurity in corporate environments.*

Keywords: SIEM, cybersecurity, incidents, monitoring, automation, event correlation, Splunk, IBM QRadar.

Вступ

У сучасному цифровому середовищі зростає як кількість, так і складність кібератак. Традиційні засоби захисту вже не здатні ефективно виявляти загрози на ранніх етапах, що створює потребу в централізованому аналізі подій безпеки в режимі реального часу. Саме SIEM-системи (Security Information and Event Management) забезпечують моніторинг, кореляцію та автоматизоване реагування на інциденти, підвищуючи ефективність кіберзахисту в організаціях різного рівня.

Результати дослідження

У ході дослідження було проаналізовано архітектуру та функціональні можливості сучасних SIEM-систем, зокрема Splunk, IBM QRadar та ELK Stack. За даними Blessing M. (2023), SIEM-рішення дозволяють обробляти понад 1 мільйон подій безпеки на добу в середовищі великого підприємства, забезпечуючи централізовану кореляцію загроз і швидке реагування на інциденти [1]. Це особливо актуально у зв'язку зі зростанням кількості складних атак, які залишаються непоміченими традиційними засобами захисту.

У результаті моделювання типових інцидентів (сканування портів, підбір паролів, доступ до конфіденційних файлів) в тестовому середовищі з налаштованою SIEM-системою QRadar було виявлено, що середній час виявлення загроз склав 34 хвилини, а точність виявлення – понад 91% [2]. Для порівняння, в системі Splunk із активованими кореляційними правилами та базовим машинним навчанням час спрацювання був скорочений до 22 хвилин [3]. Ці результати демонструють високу чутливість систем до аномальної поведінки у мережевому трафіку.

Особливої уваги було надано автоматизації процесів реагування. Згідно з дослідженням Doris L. та Shad R. (2024), інтеграція SIEM із системами SOAR дозволяє зменшити навантаження на аналітиків безпеки майже на 40% за рахунок автоматичного блокування підозрілих IP-адрес, ізоляції хостів та створення інцидентів у системах Service Desk [4].

Виявлено також залежність якості виявлення загроз від коректності налаштувань кореляційних правил, сегментації мережі та рівня підготовки персоналу. Yan H. та ін. (2024) вказують, що в середовищах із неправильно налаштованими шаблонами подій рівень хибнопозитивних спрацювань може перевищувати 18%, що створює зайве навантаження на аналітиків SOC [5].

Таким чином, результати дослідження підтверджують ефективність SIEM-систем у виявленні складних атак, скороченні часу реагування та підвищенні загального рівня кіберзахисту. Їх впровадження є доцільним для організацій, що працюють із критичною інформацією або великою кількістю користувачів.

Висновки

Проведене дослідження засвідчило, що SIEM-системи є ключовим елементом сучасної стратегії кіберзахисту. Вони забезпечують централізоване збирання, аналіз і кореляцію подій безпеки, що дозволяє виявляти інциденти на ранніх стадіях та оперативно реагувати на них. Експериментальні результати продемонстрували високу ефективність таких систем, як Splunk та IBM QRadar, у сценаріях, наближених до реальних умов корпоративного середовища. Особливої цінності набуває поєднання SIEM із автоматизованими рішеннями типу SOAR, що дозволяє не лише виявити, а й миттєво нейтралізувати загрозу. Водночас ефективність таких рішень значною мірою залежить від правильного налаштування кореляційних правил, якості вхідних даних та рівня підготовки аналітичного персоналу.

У перспективі розвиток SIEM-систем має орієнтуватися на інтеграцію технологій штучного інтелекту, розширення поведінкової аналітики та адаптивне навчання моделей. Це дозволить не лише підвищити точність виявлення загроз, а й зменшити кількість хибнопозитивних спрацювань. У підсумку, SIEM є невід'ємною складовою системи проактивної безпеки, що забезпечує надійний захист IT-інфраструктури від сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Blessing M. Аналіз часових рядів у SIEM-системах для виявлення кібератак [Електронний ресурс] // *Journal of Cybersecurity and Information Management*. – 2023. – Т. 7, № 3. – С. 22–29. – Режим доступу: https://cyberjournal.org/timeseries_cyber_attacks (дата звернення: 08.06.2025).
2. Mohammed J. M., Gazi A., Awad A. M., Jasim K. M. Evaluating QRadar's efficiency in identifying coordinated network threats [Електронний ресурс] // *International Journal of Computer Applications*. – 2025. – Т. 184, № 17. – С. 12–19. – Режим доступу: https://doi.org/10.5120/ijca2025905732 (дата звернення: 08.06.2025).
3. Yan H., Zhu J., Lee J. K. Enhanced Threat Detection using Splunk SIEM with ML Algorithms [Електронний ресурс] // *Applied Mathematics and Nonlinear Sciences*. – 2024. – Т. 9, № 1. – С. 1–15. – Режим доступу: https://sciendo.com/article/10.2478/amns-2024-2480 (дата звернення: 08.06.2025).
4. Doris L., Shad R. Automating Incident Response via SIEM-SOAR Integration [Електронний ресурс] // *International Research Journal of Engineering and Technology (IRJET)*. – 2024. – Т. 11, № 4. – С. 370–375. – Режим доступу: https://www.irjet.net/archives/V11/i4/IRJET-V11I4370.pdf (дата звернення: 08.06.2025).
5. Yan H., Zhu J., Lee J. K. Cybersecurity risk assessment through behavioral log analysis [Електронний ресурс] // *Applied Mathematics and Nonlinear Sciences*. – 2024. – Т. 9, № 1. – С. 45–58. – Режим доступу: https://sciendo.com/article/10.2478/amns-2024-2485 (дата звернення: 08.06.2025).

Булаївський Артем Андрійович – студент 2 курсу групи 2БС-23Б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: artembulaivskiy@gmail.com.

Кондратенко Наталія Романівна – к.т.н., проф., професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: kondratenko.natalia@vntu.edu.ua.

Bulaivskyi Artem Andriyovych – second-year student of group 2BS-23B, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: artembulaivskiy@gmail.com.

Kondratenko Nataliia Romanivna – Phd in Technical Sciences, Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: kondratenko.natalia@vntu.edu.ua.