https://orcid.org/0000-0001-5568-7629
https://orcid.org/0000-0002-1208-3427
https://orcid.org/0000-0002-2552-2839

УДК 004.7

В.А. ЛИТВИНОВ[*], І.М. ОКСАНИЧ[*], С.В. ГРИБКОВ[**]

ЩОДО МОЖЛИВОСТЕЙ РЕАЛІЗАЦІЇ СУМІСНОГО ФУНКЦІОНУВАННЯ LMS- і SIEM-МЕНЕДЖМЕНТУ НА ОСНОВІ FREE OPEN SOURCE ІНСТРУМЕНТІВ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна
[**]Національний університет харчових технологій, м. Київ, Україна

Анотація. *Стаття присвячена вирішенню проблеми кібербезпеки корпоративної IT-інфраструктури за допомогою використання концепції операційних центрів безпеки. Для сучасних SOC (Security Operations Center) основна технологія моніторингу виявлення загроз і реагування базується на системах SIEM (Security Information and Event Management), які об'єднують інформацію про події від усіх інструментів безпеки і мають багато спільного з системами LMS (Log Management System). У цілому системи LMS і SIEM орієнтовані на різні задачі, але мають спільну інформаційну базу у вигляді даних журналів і частково перетинаються у можливостях виконання функцій моніторингу безпеки. Стаття наводить огляд наявних free open source інструментів реалізації функцій сучасних SIEM у прив'язці до типових процесів SOC і сумісного функціонування з LMS. У статті розглядаються функції і типові процеси SOC. Належна інструментальна основа реалізації процесів представлена еволюційною схемою розвитку SIEM, запропонованою фірмою Gartner. Відсутність безоплатної повнофункціональної платформи SIEM в існуючих і очікуваних пропозиціях лідерів сучасного ринку відповідного програмного забезпечення (за магічним квадрантом Gartner-2024) обґрунтовує обмеженість можливостей вирішення поставленої задачі використанням наявних окремих інструментів — їх адаптації, поступового розвитку й інтеграції в рамках єдиної платформи. Проведено огляд доступних джерел щодо наявних free open source інструментів реалізації базових функцій SIEM і платформ IRP, SOA, TIP, UEBA, які, на думку авторів, насамперед заслуговують на увагу в контексті поставленої задачі. Відзначається, що на фоні величезної кількості платних інструментів доля безоплатних достатньо велика, і в кожній номінації схеми Gartner є відповідні пропозиції. Для першого етапу створення повнофункціональної SIEM пропонується рішення інтеграції ELK-OSSIM із подальшим поступовим розвитком і інтеграцією компонентів SOA–SOAR. Таке рішення має на першому етапі забезпечити виконання функцій оцінки вразливостей, виявлення вторгнень, кореляції подій, поведінковий моніторинг, розвідку загроз, довгостроковий інтелектуальний аналіз та ін.*

Ключові слова: *кібербезпека, процеси SOC, LOG і SIEM менеджмент, open sourse інструменти SIEM.*

Abstract. *The article is devoted to solving the problem of cybersecurity of corporate IT infrastructure by using the concept of security operations centers. For modern SOCs (Security Operations Centers), the main monitoring, threat detection and response technology is based on SIEM (Security Information and Event Management) systems, which combine event information from all security tools and have a lot in common with LMS (Log Management Systems). In general, LMS and SIEM are focused on different tasks but have a common information base in the form of log data and partially overlap in the capabilities of performing security monitoring functions. The article provides an overview of the available free open-source tools for the implementation of modern SIEM functions in connection with typical SOC processes and compatible operation with LMS. Functions and typical SOC processes are considered. An appropriate instrumental basis for the implementation of processes is represented by the evolutionary scheme of SIEM development*

ISSN 1028-9763. Математичні машини і системи. 2025. № 1

proposed by Gartner. The absence of a free full-featured SIEM platform in the existing and expected offers of the leaders of the modern market of corresponding software (according to the magic quadrant of Gartner-2024) justifies the limitation of the possibilities of solving the given task using the available separate tools, their adaptation, gradual development, and integration within the framework of a single platform. A review of available sources on existing free open-source tools for implementing the basic functions of SIEM and IRP, SOA, TIP, and UEBA platforms has been conducted. According to the authors, these tools primarily deserve attention in the context of the given task. It is noted that against the background of a huge number of paid tools, the share of free ones is quite large, and there are corresponding offers in each nomination of the Gartner scheme. For the first stage of creating a full-featured SIEM, an ELK-OSSIM integration solution is proposed with further gradual development and integration of SOA-SOAR components. At the first stage, such a solution should ensure the performance of the functions of vulnerability assessment, intrusion detection, event correlation, behavioral monitoring, threat intelligence, long-term intelligence analysis, etc.
Keywords: *cybersecurity, SOC processes, LOG and SIEM management, open source SIEM tools.*

DOI: 10.34121/1028-9763-2025-1-55-63

1. Вступ

У теперішній час в області технологій забезпечення кібербезпеки IT-інфраструктур одержала розповсюдження концепція створення Операційних центрів безпеки SOC (Security Operations Center) — команди фахівців з IT-безпеки, яка контролює всю IT-інфраструктуру організації для виявлення подій кібербезпеки і координує вирішення проблем. Для сучасних SOC основна технологія моніторингу виявлення загроз і реагування на них базується на системах Управління інформацією і подіями безпеки SIEM (Security Information and Event Management), яка об'єднує журнали пристроїв, застосунків та інформацію про події від усіх інструментів безпеки. Рішення і можливості повнофункціональних сучасних SIEM «другої генерації» стали важливим фактором оптимізації процесів забезпечення інформаційної безпеки.

Роботам по SIEM у світі приділяється багато уваги, на ринку доступні кілька десятків інструментів і готових систем, ведуться фундаментальні наукові роботи по концептуальному вдосконаленню систем SIEM і в Україні. Все це визначає загальну актуальність досліджень із відповідної тематики.

Системи SIEM мають багато спільного з системами LMS (Log Management System), які розглядалися нами в контексті можливостей попереднього прототипування програмного забезпечення LMS мережі ситуаційних центрів (СЦ) органів державної влади (ОДВ) [1]. Загалом системи LMS призначені для збору, впорядкування і різнобічного аналізу даних системних журналів (лог-файлів), а SIEM насамперед орієнтовані саме на аналіз попереджень безпеки, що генеруються застосунками і мережевим обладнанням у режимі реального часу. В цілому системи LMS і SIEM орієнтовані на різні задачі, але мають спільну інформаційну базу у вигляді даних журналів і частково перетинаються у виконанні функцій моніторингу безпеки. В багатьох джерелах взагалі LMS вважається функціональною й інформаційною підмножиною SIEM. Все це обгрунтовує правомірність досліджень і розробки архітектури інтеграційних рішень щодо сумісного функціонування систем SIEM і LMS у рамках SOC (зокрема, мережі СЦ) та аналізу наявних можливостей попередньої прототипізації повнофункціональної реалізації цих рішень.

Мета статті полягає в огляді наявних free open source інструментів реалізації функцій сучасних SIEM у прив'язці до типових процесів SOC і сумісного функціонування з LMS.

2. Функції і процеси SOC

Загальна мета створення SOC полягає в оптимізації процесів обробки інцидентів безпеки на основі впорядкування сумісної роботи аналітиків безпеки [2–4]. Центральним інструментальним компонентом сучасних SOC є, як вже відзначалося, повнофункціональна

SIEM нової генерації, що об’єднує дані журналів обладнання і застосунків, дані щодо подій від різних локальних інструментів безпеки, і на їх об’єднанні створює повне уявлення про можливі загрози для IT-інфраструктури, що дозволяє реагувати на них до настання суттєвої шкоди. Інтегруючу роль SIEM ілюструє рис. 1 [5].

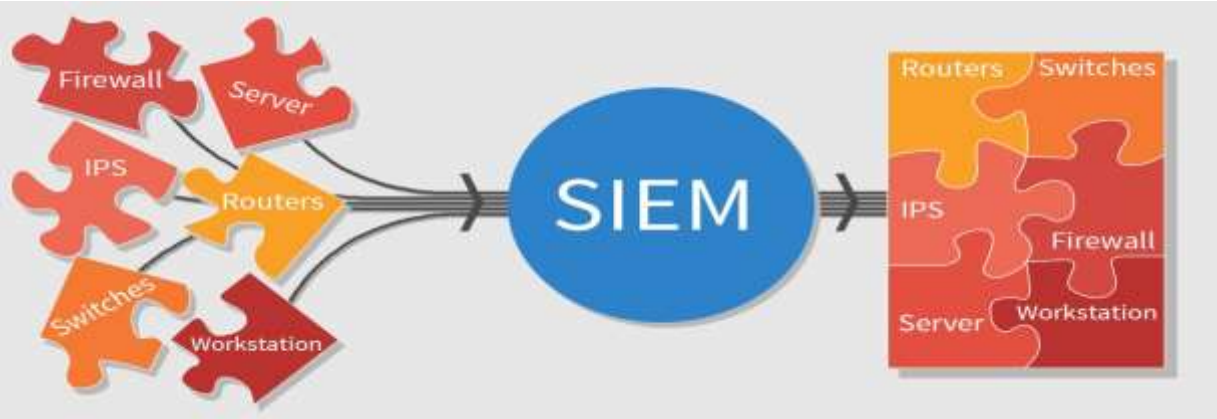

Рисунок 1 — Інтегруюча роль SIEM

Створення повної безпекової картини IT-інфраструктури пов’язано з одержанням величезних обсягів даних. Для крупних корпоративних IT-систем звичайним є щоденне одержання сотен мільйонів журнальних записів [6], більша частина з яких не має відношення до безпеки. Джерела інформації і системи SOC генерують велику кількість попереджувальних сповіщень, значна частина яких не відноситься до реальних інцидентів безпеки і може зайняти зайвий час роботи аналітиків безпеки у збиток виявленню реальних попереджень. Сучасні SIEM у змозі надати аналітикам можливість послідовно скоротити початкову кількість логів із 500 мільйонів до 50 подій, що заслуговують на увагу, і з них сформувати біля 10 предметів розслідування. Приклад результатів послідовності такої фільтрації ілюструє рис. 2 [6].

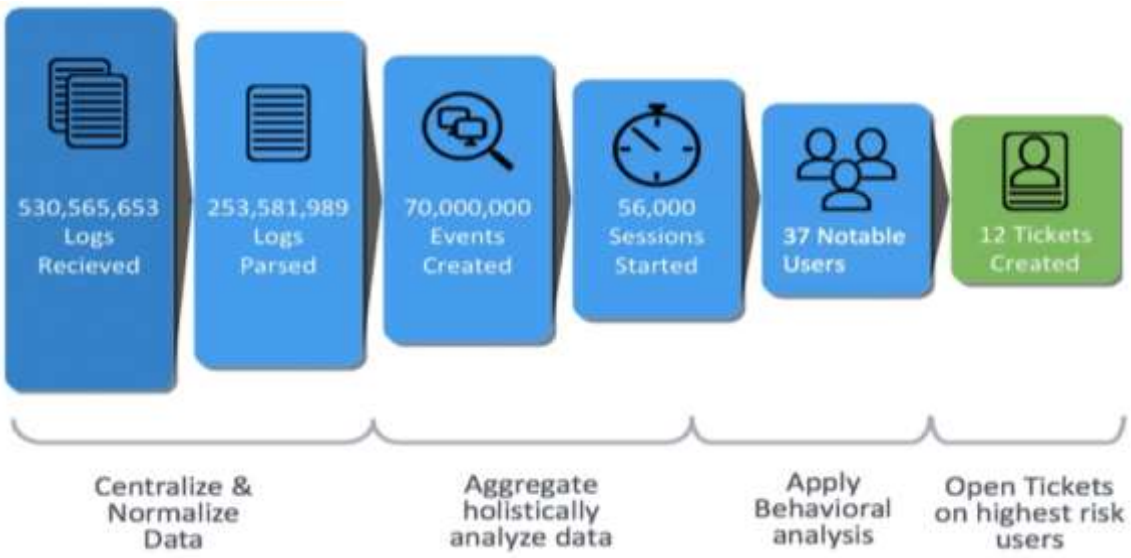

Рисунок 2 — Кількісні оцінки процесів фільтрації

Загальне завдання команди аналітиків SOC полягає у швидкому та ефективному виявленні інцидентів кібербезпеки та реагуванні на них у режимі реального часу. Розв'язання цього завдання містить виконання різними спеціалістами команди SOC низки

певних процесів. Базова модель реагування на інциденти (потенційні та реальні) містить такі основні процеси [3].

1. Класифікація подій безпеки.

Полягає в аналізі відповідних оповіщень журналів та засобів забезпечення безпеки, їх пріоритезації з урахуванням важливості та достовірності й виявлення подій, що заслуговують на подальшу увагу, тобто, потенційних інцидентів.

2. Розслідування інцидентів.

Більш детальне вивчення підозрілих подій та виявлення реальних інцидентів. Збір додаткових даних для встановлення джерела та визначення характеру атаки, підготовка рекомендацій щодо реагування на інцидент.

3. Реагування на інциденти.

Вжиття термінових заходів щодо зупинення можливого розвитку атаки, локалізації інциденту та мінімізації тяжкості можливих наслідків, відновлення системи (повернення до нормальної роботи) з подальшим виправленням конкретних причин виникнення інциденту.

4. Криміналістичне розслідування.

Подальше історичне розслідування докорінних причин інциденту в контексті супутніх обставин на основі глибокого аналізу журналів, мережевого трафіка та інших даних.

5. Виправлення.

Розробка та здійснення заходів щодо усунення вразливостей системи, що допускають атаку, полегшують її та/або посилюють її наслідки.

Успішному виконанню ланцюжка перерахованих дій сприяють допоміжні процеси: розвідка потенційних загроз на основі міжкорпоративного професійного досвіду виявлення та усунення атак, системна оцінка атак та заходів щодо їх усунення та ін.

В організації технології виконання сукупності перелічених процесів істотне значення мають фактори, які значною мірою впливають на їх трудомісткість та швидкість. Перелічимо їх нижче.

• Використання чітко визначених типових процедур виконання процесів за заздалегідь розробленими та оціненими сценаріями, що задають чітку структуровану логіку роботи аналітиків SOC. Якщо провести аналогію зі стандартизованими технологіями розробки програмного забезпечення, то організація процесів ідентифікації кібератак має наближатися до 5-го рівня технологічної зрілості відповідної моделі CMM [7].

• Алгоритмізація сценаріїв та забезпечення автоматизації виконання робочих процедур реагування на загрози з метою зниження стомлюваності персоналу поряд із можливістю централізовано управляти процесами («оркеструвати»).

• Використання штучного інтелекту та машинного навчання для поведінкового аналізу системи та вирішення відповідних проблем.

Загалом, аналізуючи функції та процеси SOC, можна зробити висновок про доречність або принаймні можливість трактування SOC як спеціалізованого ситуаційного центру, призначеного для аналітичного проблемного моніторингу кіберзагроз та вирішення надзвичайних ситуацій у цій сфері. Така інтерпретація не має суттєво практичного значення для виконання розглянутих вище процесів, проте може бути корисною у плані уніфікації рішень щодо створення SOC саме мережі ситуаційних центрів.

3. Інструменти реалізації повнофункціональної SIEM

Трактування застосованого нами терміна «повнофункціональна» і «дорожню карту» створення таких SIEM, яку запропонувала відома дослідницька фірма Gartner, ілюструє рис. 3 [8].

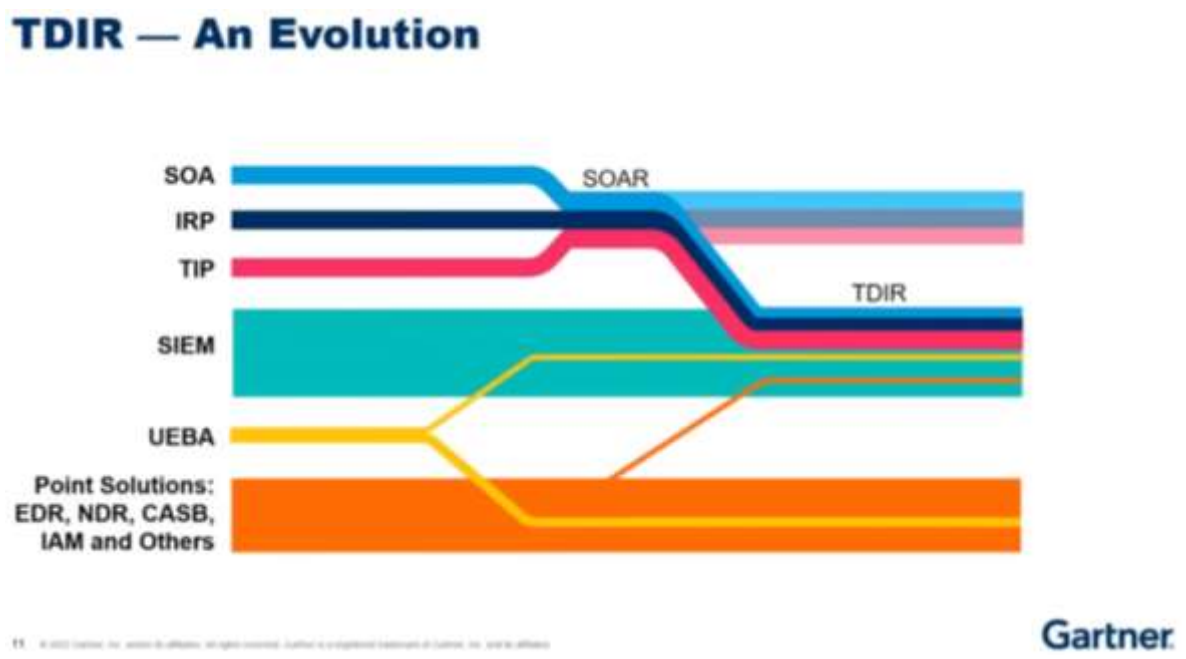

Рисунок 3 — Схема еволюції SIEM

Повнофункціональний набір інструментів має містити платформи, що забезпечують:

– виконання базових функцій SIEM — безпековий моніторинг журналів, кореляція подій безпеки, довгостроковий інтелектуальний аналіз;

– автоматизацію процесів моніторингу, обліку і реагування на інциденти інформаційної безпеки — стримування, усунення наслідків і відновлення після атаки (IRP — Incident Response Platform);

– «оркестрування» й автоматизацію процесів попередження і протидії кібератакам (SOA — Security Orchestration and Automation);

– розвідку кіберзагроз (TIP — Threat Intelligence Platform);

– контроль облікових записів користувачів і виявлення аномалій в їх поведінці (UEBA — User and Entity Behavior Analytics).

Наведені комплексні інструменти у складі SIEM інтегруються в загальну платформу попередження, виявлення і реагування на загрози TDIR.

У теперішній час на ринку відповідного програмного забезпечення пропонується велика кількість систем і окремих інструментів SIEM, і цей сегмент ринку динамічно розвивається. На рис. 4 наведено «магічний квадрант» Gartner, що оцінює найбільш вагомих і популярних постачальників інструментів і технологій SIEM в системі координат «повнота бачення — здатність реалізації» станом на січень 2024-го року [9]. Динаміку розвитку сегмента ілюструє аналогічний квадрант станом на квітень 2021-го року (рис. 5 [10]).

Рисунок 4 — Магічний квадрант для SIEM станом на 01.2024

Source: Gartner (June 2021)

Рисунок 5 — Магічний квадрант для SIEM станом на 04.2021

Сучасні лідери ринку (Splunk, Microsoft, IBM) пропонують платні системи, які в достатньо повній мірі відповідають сформульованим вище вимогам. Але повнофункціональної open source платформи SIEM, на жаль, не існує, і навряд чи вона з'явиться, враховуючи наявні ринкові тенденції до скорочення безоплатних пропозицій, що видно, зокрема, за станом у сегменті платформ SOAR. Тому в контексті поставленої задачі лишається тільки рішення з використанням наявних окремих інструментів, їх адаптації, поступового розвитку й інтеграції в рамках єдиної платформи. Огляд доступних найбільш показових джерел [11–23] свідчить про такі можливості щодо free open source інструментів, які, на думку авторів, насамперед заслуговують на увагу в контексті поставленої задачі.

У номінації SIEM

OSSEK — система виявлення хост-вторгнень. Відслідковує на хості безпековий стан журналів, цілісність файлів, наявність руткітів тощо.

Snort — система виявлення мережевих вторгнень. Виконує аналіз трафіку і викриває можливі напади.

OSSIM — платформа з функціоналом виявлення вторгнень, поведінкового моніторингу, кореляції подій, ідентифікації та оцінки вразливостей. Інтегрує в своєму складі OSSEK, Snort і багато інших інструментів. Вважається однією з найбільш популярних відкритих платформ SIEM.

Стек ELK — багато джерел відносять ELK, що номінально є платформою лог-менеджменту, до засобів SIEM. Підставою для цього є можливість і практика використання складових інструментів ELK для аналізу і візуалізації IT-подій при застосуванні інших платформ та інструментів SIEM.

У номінації IRP

Cynet — IR-платформа реагування на інциденти, реалізує сукупність дій із нейтралізації заражених хостів, шкідливих файлів, підозрілих облікових записів користувачів та мережевого трафіку. Вважається у цій номінації одним із найкращих безкоштовних інструментів.

GRR Rapid Response, масштабована система для ідентифікації та віддаленого проведення розслідувань інцидентів. Дозволяє в режимі реального часу аналізувати файли та реєстри, допомагає аналітикам швидко класифікувати та аналізувати події, а також автоматизувати виконання завдань, що повторюються.

The Hive Project — IR-платформа coworking аналітиків у розслідуваннях інцидентів.

OSSIM ряд джерел також відносять до IR-платформ завдяки передусім його можливостям виявлення вразливостей, загроз, вторгнень і створення більш повного уявлення про систему.

У номінації TIP

Yeti — платформа з централізованим уніфікованим репозиторієм загроз, який містить дані, що створені і підтримуються різними службами реагування на інциденти. Репозиторій об'єднує індикатори загрозливості подій та інформацію щодо особливостей методів, які використовують зловмисники.

MISP — відкрита платформа для обміну інформацією щодо індикаторів загрозливості і вразливостей систем із механізмами визначення кореляції між ними. Платформа адаптивна, масштабована і частково автоматизована.

Open CTI (Cyber Threat Intelligence) — платформа для обробки й аналізу даних розвідки кіберзагроз. Оптимізує процеси збору, зберігання і співставлення даних.

Type DB-CTI — відмінна, як стверджується в одному з джерел, платформа аналізу загроз на основі єдиної бази даних інцидентів.

Додатково є декілька систем, що забезпечують накопичення з різних джерел, актуалізацію і обробку даних щодо інцидентів і потенціальних загроз (Open Threat Exchange та ін.).

У номінації UEBA

Open UBA — система для моделювання поведінки користувачів (у розробці). Містить відкриту для поповнення і використання бібліотеку моделей аналізу поведінки користувачів і інших об'єктів.

Apach Metron — комплексна SIEM-платформа з функцією виявлення аномалій у поведінці об'єктів на основі машинного навчання.

OSSIM — поряд з іншими функціями має функцію аналізу поведінки користувачів.

У номінації SOA

Tines, Stuffle — платформи автоматизації виконання робочих процесів підтримки — безоплатно початковий рівень функціонала.

LogicHub — платформа, що забезпечує автономне виявлення загроз і автоматизацію реагування на інциденти з використанням машинного навчання (безоплатно, але, як відзначається, зареєстрованим користувачам США та Канади, можливо, виключно).

Пропонується багато платних платформ із безоплатним випробувальним терміном.

4. Висновки

Результати проведеного огляду дають підстави для таких висновків.

1. У контексті задачі інтеграції LMS-SIEM питання з вибором ELK — Graylog [1] для LMS-менеджмента має вирішуватися на користь стека ELK, який, поряд із наданням основної частини вхідної інформації, може використовуватися ще і як додатковий інструмент SIEM.

2. На фоні величезної кількості платних інструментів SIEM–SOAR доля безоплатних достатньо велика, і в кожній номінації схеми Gartner є пропозиції, що можуть бути використані для вирішення поставленої задачі.

3. Враховуючи широкі початкові можливості OSSIM, для першого етапу вирішення задачі напрошується рішення інтеграції ELK-OSSIM із подальшим поступовим розвитком і інтеграцією компонентів SOA–SOAR. Таке рішення на першому етапі має забезпечити виконання функцій централізованої обробки та аналізу журналів, оцінки вразливостей, виявлення вторгнень, кореляції подій, поведінкового моніторингу, розвідки загроз, довгострокового інтелектуального аналізу, візуалізації подій (надання dashboard) та ін.

СПИСОК ДЖЕРЕЛ

1. Литвинов В.А., М'якшило О.М., Брацький В.О. Задача централізованого управління журналами в мережі ситуаційних центрів ОДВ і підходи до прототипування її програмних рішень. *Математичні машини і системи*. 2023. № 4. С. 33–42.

2. URL: https://www.manageengine.com/log-management/siem/components-of-security-operations-center-soc.html.

3. Security Operations Center (SOC) Roles and Responsibilities. URL: https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities.

4. SOC and SIEM: The Role of SIEM Solutions in the SOC. URL: https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/.

5. Що таке SIEM? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem.

6. 10 Must-Have Features to be a Modern SIEM. URL: https://www.exabeam.com/explainers/next-gen-siem/10-must-have-features-to-be-a-modern-siem/.

7. Capability Maturity Model (CMM) — Software Engineering. URL: https://www.geeksforgeeks.org/software-engineering-capability-maturity-model-cmm/.

8. Тенденции в сегменте решений класса SIEM / SAP. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/352442.php.
9. GARTNER ® MAGIC QUADRANT™ 2024 ДЛЯ SIEM. URL: https://www.securonix.com/resources/2024-gartner-magic-quadrant-for-siem.
10. SIEM Tools: Top 6 SIEM Platforms, Features, Use Cases and TCO. URL: https://www.exabeam.com/explainers/siem-tools/siem-buyers-guide.
11. Top 5 Free Open Source SIEM Tools: Updated 2023. URL: https://www.exabeam.com/explainers/siem-tools/7-open-source-siems/.
12. 10 Most Valuable SIEM tools for 2024 (Open Source). URL: https://logz.io/blog/open-source-siem-tools/.
13. 10 Best Free and Open-Source SIEM Tools. 2019. URL: https://www.dnsstuff.com/free-siem-tools.
14. 10 Open Source Tools For Incident Response. URL: https://www.cyberlands.io/top10incidentresponsetools.
15. The 7 Best Free and Open-Source Incident Response Tools. URL: https://www.cynet.com/blog/the-7-best-free-and-open-source-incident-response-tools/.
16. Top 5 Open-Source Incident Response Tools. URL: https://dev.to/eddiesegal/top-5-open-source-incident-response-tools-4k4j.
17. Open Source Threat Intelligence Platform — Best Alternatives for Your Company. Top 7 Open Source Threat Intelligence Platforms that Provide Real-time Updates on Global and Internal Security Threats. 2024. URL: https://heimdalsecurity.com/blog/open-source-threat-intelligence-platform-tip/.
18. Best Open Source Threat Intelligence Platforms and Feeds. URL: https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-threat-intelligence-platforms-and-feeds.
19. Open Source Threat Intelligence Tools & Feeds: A Complete 2023 List. URL: https://flare.io/learn/resources/blog/open-source-threat-intelligence/.
20. Top Free Security Orchestration, Automation, and Response (SOAR) Software. URL: https://www.g2.com/categories/security-orchestration-automation-and-response-soar/free.
21. Top 10+ SOAR Tools to Enhance Your SecOps Experience Best Open-Source SOAR Tools. URL: https://heimdalsecurity.com/blog/soar-tools/.
22. Announcing the Free Edition of LogicHub SOAR. URL: https://securityboulevard.com/2022/03/announcing-the-free-edition-of-logichub-soar/.
23. Best Free SOAR Software. URL: https://www.capterra.com/soar-software/s/free/.

Стаття надійшла до редакції 19.02.2025