

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ SIEM-СИСТЕМ ДЛЯ ПРОАКТИВНОГО ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто ефективність використання SIEM-систем для проактивного виявлення сучасних загроз інформаційної безпеки. Проаналізовано функціональні можливості цих систем, виділено основні переваги їх застосування, зокрема в контексті зниження ймовірності успішних атак та покращення процесів моніторингу й захисту інформаційних систем. Також розглянуто проблеми, які потребують удосконалення, такі як налаштування та інтеграція систем у наявні інфраструктури.

Ключові слова: SIEM-системи, інформаційна безпека, проактивне виявлення загроз, кіберзахист.

Abstract

The paper examines the effectiveness of using SIEM systems for proactive detection of modern information security threats. The functionality of these systems is analyzed, and the main advantages of their use are highlighted, in particular in the context of reducing the likelihood of successful attacks and improving the processes of monitoring and protecting information systems. The author also considers the problems that need to be improved, such as the configuration and integration of systems into existing infrastructures.

Keywords: SIEM systems, information security, proactive threat detection, cyber defense.

Вступ

Кожного дня у світі стрімко зростає обсяг інформації, що обробляється та передається через відкриті канали зв'язку. Це, у свою чергу, збільшує ризики та кількість кіберзагроз, які вимагають не лише реактивного, а й проактивного підходу до їх виявлення. Для ефективної боротьби з цими загрозами необхідно застосовувати інструменти, які дозволяють завчасно ідентифікувати потенційні ризики. Одним із таких рішень є використання SIEM-систем.

Метою даного дослідження є аналіз ефективності використання SIEM-систем у забезпеченні проактивного підходу виявлення загроз інформаційної безпеки шляхом вивчення їх основних функціональних можливостей.

Результати дослідження

Більшість інформаційних систем виявляють проблеми лише після заподіяння збитків, таких як втрата інформації чи фінансові втрати. У таких ситуаціях усунення наслідків потребує значного часу. Класична інфраструктура безпеки складається з рішень, які реагують на активні загрози, зокрема антивірусу, IPS, пісочниці тощо. Однак ефективнішим підходом є завчасна підготовка до можливих атак. Для цього необхідно не лише реагувати на вже виявлені загрози, а й аналізувати події в реальному часі, виявляти аномалії та потенційні атаки ще до того, як вони завдадуть шкоди. Одним із найефективніших рішень у цьому напрямку є SIEM-системи.

SIEM (Security information and event management) – об'єднання двох термінів, що позначають область застосування програмного забезпечення: SIM (Security information management) – управління інформацією про безпеку і SEM (Security event management) – управління подіями безпеки. Технологія SIEM забезпечує аналіз у реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них до настання істотних збитків [1].

Наразі дослідники визначають три етапи еволюції SIEM-систем, що значно впливають на їх ефективність у виявленні загроз. Перше покоління поєднувало SIM та SEM, але через обмежене журналювання мало вузьку зону контролю. Друге покоління вдосконалило роботу з великими даними, дозволяючи порівнювати поточні події з історичними журналами. Третє покоління інтегрувало

UBA/UEBA та SOAR, що дозволяє підвищити ефективність аналізу загроз і автоматизувати реагування на інциденти [2].

Для вирішення поставлених завдань SIEM-системи першого покоління застосовують нормалізацію, фільтрацію, класифікацію, агрегацію, кореляцію та пріоритезацію подій, а також генерацію звітів та попереджень. У SIEM-системах нового покоління додаються такі важливі функції як аналіз подій, інцидентів та їх наслідків, що дозволяє не лише реагувати на події, але й прогнозувати можливі загрози [1].

Проаналізувавши роботу SIEM-систем можна виділити деякі функціональні можливості, а саме агрегацію даних з різних джерел; кореляцію подій для виявлення взаємозв'язків між загрозами; наявність інструментів аналізу подій та інцидентів безпеки; автоматизоване оповіщення про потенційні загрози; візуалізацію даних для виявлення аномалій; довготривале зберігання логів для аналізу та розслідувань; сумісність із різними системами кібербезпеки; а також можливість проведення експертного аналізу для глибшого дослідження інцидентів.

Для досягнення максимальної ефективності SIEM-систем важливо також правильно їх інтегрувати в існуючу інфраструктуру та використовувати потужні алгоритми для фільтрації та кореляції даних, щоб уникнути хибнопозитивних спрацювань.

Попри значні можливості SIEM-систем у моніторингу та аналізі подій інформаційної безпеки, їх ефективне впровадження та використання супроводжується рядом проблем. Однією з головних є великий обсяг даних. Навіть на невеликих підприємствах може генеруватися десятки подій за секунду, що робить ручний аналіз неефективним і вимагає автоматизації. Однак впровадження SIEM-систем також пов'язане зі складнощами налаштування: необхідно правильно інтегрувати систему в існуючу IT-інфраструктуру, оптимізувати джерела подій та налаштувати кореляційні правила для мінімізації хибнопозитивних спрацювань. Додатковим викликом є високі вимоги до кваліфікації персоналу, який повинен мати не лише технічні навички для налаштування та обслуговування системи, але й здатність правильно інтерпретувати великі масиви даних та приймати на їх основі ефективні рішення. Окрім цього, необхідно враховувати, що впровадження SIEM-систем може бути дорогим процесом, оскільки потребує значних ресурсів для обробки та зберігання інформації, що може призвести до перевантаження інфраструктури та збільшення витрат на її підтримку [3-4].

Незважаючи на ці труднощі, SIEM-системи залишаються невід'ємною частиною сучасного кіберзахисту, оскільки дозволяють організаціям ефективно управляти інформаційною безпекою. Основними перевагами їх використання є централізований збір і аналіз даних про потенційні загрози, що надає змогу своєчасно виявляти інциденти та оперативно на них реагувати.

Однією з ключових переваг SIEM є можливість моніторингу подій у реальному часі, що підвищує швидкість реагування на такі загрози як: мережеві атаки, фішинг, вірусна активність, спроби несанкціонованого доступу та шахрайство. Завдяки розширеному аналізу даних SIEM-системи допомагають фахівцям швидше ідентифікувати складні атаки, зокрема APTs, бекдори та експлойти, які можуть залишатися непомітними для традиційних засобів безпеки [5].

Крім того, SIEM сприяє забезпеченню відповідності нормативним вимогам, автоматизуючи створення звітів та полегшуючи аудит безпеки. Система також дозволяє прозоро відстежувати дії користувачів, програм і пристроїв, що допомагає у виявленні аномальної активності та можливих внутрішніх загроз. Загалом, SIEM-системи оптимізують робочі процеси кіберзахисту, надаючи спеціалістам інструменти для централізованого управління загрозами, аналізу ризиків і підвищення загальної безпеки організації.

Таким чином, хоча SIEM-системи мають певні труднощі в налаштуванні та обробці великих обсягів даних, їхнє використання виявляється надзвичайно важливим для проактивного виявлення загроз і покращення загальної інформаційної безпеки.

Висновок

Результати дослідження підтверджують, що використання SIEM-систем є важливим елементом проактивної стратегії виявлення та реагування на загрози інформаційної безпеки. Завдяки здатності виявляти аномалії та корелювати події в реальному часі, SIEM-системи дозволяють оперативно реагувати на потенційні ризики ще до того, як вони завдадуть істотної шкоди. Ці системи не тільки спрощують процес моніторингу, але й підвищують ефективність захисту завдяки автоматизованим попередженням та глибокому аналізу подій.

Хоча впровадження та налаштування SIEM-систем можуть бути складними та потребувати значних ресурсів, їхні переваги значно перевищують труднощі. Вони дозволяють організаціям значно знизити ймовірність успішних атак, завдяки чому стають важливим компонентом для забезпечення довгострокової кібербезпеки.

У майбутньому використання таких систем буде ще ефективнішим завдяки впровадженню новітніх технологій, таких як штучний інтелект і машинне навчання. Ці інновації дозволять підвищити точність виявлення складних загроз і автоматизувати реагування на інциденти.

З огляду на це, можна очікувати, що роль SIEM-систем у кіберзахисті буде лише збільшуватися, оскільки ці системи продовжуватимуть вдосконалюватися завдяки новим технологіям та рішенням, ставши незамінним елементом сучасних інструментів для управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с
2. Що таке "Інформація про безпеку та управління подіями" (SIEM)? | Gridinsoft. ТОВ "Гріндінсофт". URL: <https://gridinsoft.ua/siem#evolution> (дата звернення: 25.01.2025).
3. Харламова, К. О. Проблеми при впровадженні SIEM-систем / К. О. Харламова, В. М. Ткач // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 13–14 травня 2021 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2021. – С. 437–438. URL: <https://ela.kpi.ua/server/api/core/bitstreams/c417748e-3881-4422-b25b-316c81f80bb8/content> (дата звернення: 27.02.2025)
4. Северінов О. В. Аналіз проблем використання SIEM систем / О. В. Северінов, О. В. Чубенко // Проблеми інформатизації : тези доповідей восьмої міжнародної науково-технічної конференції, 26-27.11.2020. – Черкаси: ЧДТУ; Х.: НТУ «ХП»; Баку: ВА ЗС АР; Бельсько-Бяла: УТІГН; ДП «ПД ПКНДІ АП», 2020, Т. 1: секції 1-3. – С. 111.. URL: <https://openarchive.nure.ua/entities/publication/0140fc11-c8cc-4b8d-9336-e7df6e1486b4> (дата звернення: 27.02.2025).
5. Що таке SIEM? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem> (дата звернення: 29.02.2025).

Осадчук Катерина Дмитрівна – студентка групи 2KITS-21b, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: osadcukkata88@gmail.com

Науковий керівник: **Салієва Ольга Володимирівна** – доктор філософії за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Osadchuk Kateryna Dmytrivna – student of group 2KITS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: osadcukkata88@gmail.com

Scientific supervisor: Saliieva Olha Volodymyrivna – Doctor of Philosophy in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua