ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.492.3

Эффективное обеспечение безопасности с помощью SIEM

Д.Г. Кирсанов, А.Р. Айдинян
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Проанализированы сведения о системах управления информацией и событиями безопасности, их роли в обеспечении эффективной работы в современных IT-инфраструктурах. Тем самым расширены существующие теоретические и практические знания в области информационной безопасности. Рассмотрены основные принципы работы SIEM-систем и определена их значимость для эффективного обеспечения безопасности информационных систем, систематизированы существующие знания и предложены новые методы анализа и повышения эффективности SIEM-систем в условиях возрастающих киберугроз. Научная новизна статьи заключается в выявлении оптимальных стратегий применения SIEM для мониторинга событий, обнаружения угроз, соответствия требованиям и автоматизации процессов безопасности. Проведенные исследования позволили дать практические рекомендации для эффективного обеспечения безопасности и показали, что предлагаемые подходы к управлению событиями на предприятии с использованием SIEM-систем обеспечат поддержание требуемого уровня защищенности информационной системы предприятия в условиях динамически изменяющихся и развивающихся угроз информационной безопасности.

Ключевые слова: SIEM (Security Information and Event Management), системы управления информационной безопасностью, обнаружение инцидентов, безопасность информационных систем, методы обнаружения киберугроз

Для цитирования. Кирсанов Д.Г., Айдинян А.Р. Эффективное обеспечение безопасности с помощью SIEM. *Молодой исследователь Дона.* 2024;9(3):45–49.

Effective Security Ensuring with SIEM

Dmitrii G. Kirsanov, Andrei R. Aidinyan
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article expands theoretical and practical knowledge in the field of information security by analyzing the existing knowledge about information and security event management systems, their role in ensuring security and efficiency in modern IT infrastructures. The article analyzes the basic principles of SIEM systems and their significance for effective information security of information systems, systematizes the existing knowledge, and proposes new methods for analyzing and improving the effectiveness of SIEM systems in the context of increasing cyber threats. The scientific novelty of the article lies in the identification of optimal strategies of SIEM application for event monitoring, threat detection, compliance and automation of security processes. The conducted research allowed us to provide practical recommendations for effective security and showed that the proposed approaches to event management at the enterprise using SIEM systems would ensure the maintenance of the required level of security of the enterprise information system in conditions of dynamically changing and developing threats to information security.

Keywords: SIEM (Security Information and Event Management), information security management systems, incident detection, information systems security, cyber threat detection methods

For citation. Kirsanov DG, Aidinyan AR. Effective Security Ensuring with SIEM. *Young Researcher of Don.* 2024;9(3):45–49.

Введение. С ростом числа кибератак в контексте геополитической нестабильности становится ясно, что эффективное управление инцидентами в системах безопасности информации — необходимая составляющая защиты компаний различного масштаба и их информационно-технологических систем. Метод управления инцидентами Security Information and Event Management (SIEM) представляет собой интеграцию функций управления информацией о безопасности (SIM) и управления событиями безопасности (SEM) в единую систему. Это позволяет осуществлять оперативный анализ и идентификацию событий безопасности в реальном времени. Шабля В.О., Коноваленко С.А., Едунов Р.В. в работе «Анализ процесса функционирования SIEM-систем» представили разработанную типовую модель существующей центральной подсистемы сбора, хранения и корреляции событий информационной безопасности системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также описали предназначение ее основных функциональных элементов [1]. Кузнецова А.Д., Сахаров Д.В. в обзоре по результатам исследований информационной безопасности и применения SIEM-систем высказали мнение, что несмотря на широкое применение SIEM эффективность его использования в контексте современных угроз недостаточно изучена [2]. В настоящем исследовании сделана попытка заполнить этот пробел в научном знании путем проведения анализа эффективности SIEM в условиях увеличивающегося числа киберугроз [3, 4]. Цель данной работы — проанализировать эффективность метода SIEM в контексте современных угроз информационной безопасности и определить возможные способы его улучшения.

В наши дни использование SIEM-систем становится все более распространенным в различных сферах бизнеса. Исследования показывают, что подавляющее большинство крупных предприятий прибегают к этим системам для обеспечения безопасности своих данных и информационных ресурсов. Это говорит о том, что SIEM становится не просто модным трендом, а необходимым элементом инфраструктуры для больших и малых компаний [5].

Согласно отчетам и аналитическим данным, доля компаний, использующих SIEM, составляет более 70 %, и это число продолжает расти. Этот факт отражает стремление организаций к повышению уровня защиты данных и эффективной борьбе с киберугрозами. SIEM становится не просто инструментом безопасности, но и ключевым элементом стратегии информационной безопасности, обеспечивающим защиту от различных угроз и инцидентов. На рис. 1 приведена статистика выявляемых инцидентов информационной безопасности.

Рис. 1. Статистика выявляемых инцидентов информационной безопасности [6]

Основная часть. Инструменты для управления информацией и событиями в области безопасности (SIEM) играют ключевую роль в обеспечении безопасности данных, являясь важным компонентом всей системы. Они объединяют данные из различных источников и проводят анализ для выявления подозрительных действий и возможных кибератак. SIEM собирает информацию о событиях с устройств организации и технических систем компании, систематизируя данные для более эффективного анализа [6].

Использование инструментов SIEM не ограничивается только сбором и объединением журналов данных с хост-систем и приложений. Эти инструменты также позволяют собирать информацию с сетевых устройств и устройств безопасности, таких как брандмауэры и антивирусные фильтры. Основная их цель заключается в обеспечении всесторонней защиты от разнообразных угроз [7]. В результате компании получают возможность не только контролировать состояние своей инфраструктуры, но и оперативно реагировать на потенциальные угрозы и атаки, обеспечивая таким образом надежную защиту своих данных и ресурсов. Инструменты SIEM идентифицируют и классифицируют события для дальнейшего анализа.

Системы SIEM могут использоваться для упрощенного выявления потенциальных проблем и улучшения процессов отчетности в рамках всего предприятия. Автоматизация анализа и обработки данных позволяет оперативно реагировать на угрозы безопасности и обеспечивать более высокий уровень защиты информационных ресурсов организации.

Управление событиями на предприятии охватывает:

1) определение атипичной активности в корпоративной системе;

2) обнаружение неудачных попыток аутентификации в системе, потенциальных угроз и вредоносного программного обеспечения;

3) генерацию предупреждений для выявления проблем и инцидентов для оперативного реагирования на потенциальные угрозы;

4) централизованное хранение журналов для обеспечения доступности информации о произошедших инцидентах и анализа данных;

5) выявление подозрительной активности и угроз для обеспечения непрерывной безопасности информационных ресурсов компании;

6) мониторинг изменений в системах и других административных действий для обнаружения потенциальных нарушений и соблюдения политики безопасности;

7) разработку и внедрение стратегий защиты данных на основе анализа прошлых инцидентов и уязвимостей, что помогает предотвратить будущие атаки и улучшить общую безопасность предприятия.

Существует множество способов использования SIEM, в их число входят следующие:

1) мониторинг изменений в системах и других административных действиях, а также проверка соответствия их установленной политике безопасности;

2) отслеживание атак на веб-приложения и их последствий путем анализа логов веб-сервера, использования WAF (Web Application Firewall) и логов приложений;

3) отслеживание подозрительного исходящего трафика и передаваемых данных по сети путем анализа логов брандмауэра, журналов веб-прокси и NetFlow;

4) мониторинг заражений вредоносными программами, который включает в себя обнаружение вредоносного программного обеспечения по исходящим логам брандмауэра, журналам веб-прокси, внутренним журналам подключения и сетевым потокам;

5) отслеживание процесса аутентификации и выявление подозрительной активности, связанной с аккаунтами пользователей и администраторов;

6) обнаружение попыток компрометации веб-приложений путем анализа различных отчетов и данных об активности;

7) выявление случаев кражи данных и других подозрительных внешних подключений;

8) оценка эффективности собственных защитных мер и политики безопасности с помощью анализа данных о прошлых инцидентах и уязвимостях, что позволяет компаниям улучшить свои стратегии безопасности и повысить общий уровень защиты от киберугроз [8].

SIEM-системы могут быть классифицированы по различным критериям, включая их функциональные возможности, методы анализа данных и масштаб применения. На рис. 2 приведена классификация SIEM-систем по различным критериям.

Рис. 2. Классификация SIEM-систем

SIEM-системы могут включать в себя модули, каждый из которых выполняет определенные функции:

– модуль сбора и агрегации данных отвечает за сбор информации из различных источников, таких как журналы событий, системы мониторинга сетевого трафика и др. После сбора данных они агрегируются для дальнейшего анализа;

– модуль анализа событий выполняет анализ собранных данных с целью выявления потенциально опасных событий и угроз безопасности;

– модуль управления инцидентами отвечает за реагирование на обнаруженные инциденты безопасности, включая их регистрацию, классификацию, анализ и реагирование;

– модуль управления доступом и аудита обеспечивает контроль доступа к информации и аудит действий пользователей для обеспечения соответствия правилам безопасности.

SIEM-системы могут использовать различные методы анализа данных [9]:

– правила и сигнатуры — основаны на заранее заданных правилах и сигнатурах, которые определяют типы событий и угроз;

– алгоритмы искусственного интеллекта — для обнаружения аномальных паттернов в данных;

– анализ поведения, основанный на моделировании типичного поведения пользователей и системы — позволяет выявлять аномалии и подозрительные действия.

При применении SIEM-систем в организациях различного масштаба могут быть выявлены следующие особенности [10]:

– на малых и средних предприятиях SIEM-системы могут использоваться для защиты от базовых угроз безопасности и обеспечения соответствия требованиям регулирующих органов;

– в крупных корпорациях SIEM-системы могут обрабатывать большие объемы данных и обнаруживать сложные угрозы безопасности;

– в государственных учреждениях SIEM-системы могут быть использованы для защиты критической информации и инфраструктуры от целенаправленных кибератак.

В системах управления информационной безопасностью (SIEM) основными методами обнаружения являются сбор и анализ событий, а также мониторинг сетевого трафика и работы приложений. Сбор и анализ событий заключается в получении информации о происходящих событиях в информационной инфраструктуре предприятия и их последующем анализе с целью выявления потенциальных угроз и нештатных ситуаций. Данные собираются из хост-систем, приложений, сетевых устройств, устройств безопасности и др. для дальнейшего анализа.

Мониторинг сетевого трафика и работы приложений направлен на выявление аномального поведения в сети или на конечных устройствах, что может свидетельствовать о возможных атаках или нарушениях безопасности. SIEM-системы могут анализировать журналы сетевого трафика и активности приложений для выявления подозрительных действий.

На рис. 3 приведена диаграмма SIEM-процесса.

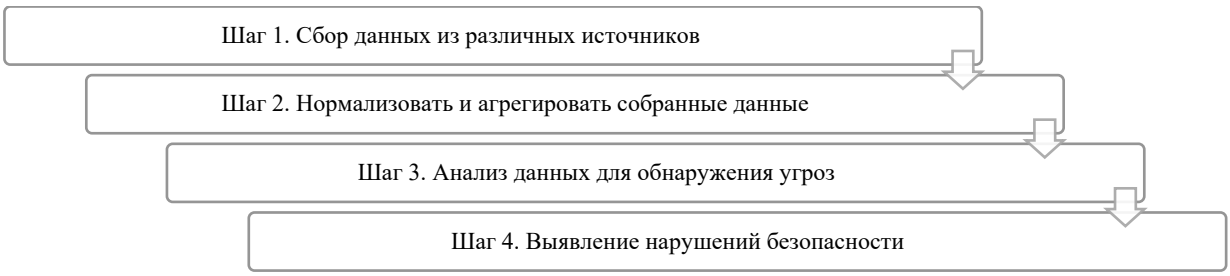

Рис. 3. Последовательность шагов SIEM-процесса

К известным SIEM-системам относятся Splunk Enterprise Security, IBM QRadar, McAfee Enterprise Security Manager, LogRhythm NextGen SIEM, Elastic SIEM (ранее известный как as Elasticsearch).

Примером применения SIEM-систем может быть их использование для контроля безопасности информационных систем, выявления и реагирования на инциденты безопасности, анализа журналов событий и составления отчетов о произошедших событиях.

Один из практических примеров — атака с использованием фишинга. Злоумышленник проник в сеть организации через фишинговое письмо для сбора информации о сети. Благодаря SIEM-системе проникновение было выявлено.

Кроме того, SIEM-системы могут применяться для обеспечения соответствия нормативным требованиям в области информационной безопасности и для проведения расследований инцидентов.

Заключение. Предложенные в статье методы повышения информационной безопасности в контексте современных угроз с использованием SIEM-систем являются актуальными. Показано, что эффективность обнаружения угроз с помощью управления событиями на предприятии с помощью SIEM-систем связана прежде всего с тем, что SIEM-системы представляют собой неотъемлемую часть современных стратегий информационной безопасности и играют важную роль в обеспечении информационной безопасности информационных ресурсов компаний, а также дают возможность компаниям соответствовать требованиям законодательства и регуляторов.

Список литературы

1. Шабля В.О., Коноваленко С.А., Едунов Р.В. Анализ процесса функционирования SIEM-систем. *E-Scio*. 2022;5(68):284–295. URL: https://cyberleninka.ru/article/n/analiz-protsessa-funktsionirovaniya-siem-sistem (дата обращения: 26.04.2024).

2. Кузнецова А.Д., Сахаров Д.В. Обзор состояния исследований информационной безопасности и применение SIEM-систем. В: *Сборник научных статей VIII Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2019).* В 4 т. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; 2019. С. 626–631.

3. Иванов О. Что такое SIEM-системы, и для чего они нужны? *Anti-Malware.ru.* URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases (дата обращения: 12.01.2024).

4. *SIEM Solutions Overview*. URL: https://www.ibm.com/security/what-is-siem (дата обращения: 12.01.2024).

5. *The Evolution of SIEM: What's Next?* URL: https://www.fireeye.com/solutions/security-operations.html (дата обращения: 12.01.2024).

6. *Выявление инцидентов ИБ с помощью SIEM: типичные и нестандартные задачи, 2020*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/incidents-siem-2020/ (дата обращения: 12.01.2024).

7. Мишнев Д.А., Золотарев Д.В. Возможности XDR в локальных сетях. В*: Материалы XV Всероссийской молодежной научной конференции «Мавлютовские чтения».* В 7 томах. Том 4. Уфа: Уфимский государственный авиационный технический университет; 2021. С. 463–471.

8. Медведева А.О. О необходимости внедрения SIEM-системы как важного элемента системы защиты информации. В: *Сборник материалов V Всероссийской молодежной научно-практической конференции «Информационные технологии обеспечения комплексной безопасности в цифровом обществе».* Уфа: Башкирский государственный университет; 2022. С. 141–145.

9. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности. *Вестник Адыгейского государственного университета.* Серия 4. Естественно-математические и технические науки. 2023;3(326):65–72. https://doi.org/10.53598/2410-3225-2023-3-326-65-72

10. Бруй И.Ю. Кибербезопасность компьютерных сетей военного назначения. В: *Материалы XXIII Международной научно-технической конференции «Новые информационные технологии в телекоммуникациях и почтовой связи».* Минск: Белорусская государственная академия связи. 2023;1(1):252–253.

Об авторах:

Дмитрий Георгиевич Кирсанов, магистрант кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), dmitriy5688@yandex.ru

Андрей Размикович Айдинян, кандидат технических наук, доцент кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), andstyle@mail.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Dmitrii G. Kirsanov, Master's Degree Student of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), dmitriy5688@yandex.ru

Andrei R. Aidinyan, Cand. Sci. (Eng.), Associate Professor of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), andstyle@mail.ru

Conflict of interest statement: the authors do not have any conflict of interest.

All authors have read and approved the final manuscript.