ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2024-51-1-173-179 Оригинальная статья /Original article

Принципы сбора данных для построения защищенной инфраструктуры предприятия на базе SIEM систем

А.Д. Попов, А.Н. Никитенко
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Целью статьи является представление основных возможностей и преимуществ внедрения и использования SIEM-систем. **Метод.** Для реализации поставленной цели использован метод системного анализа. **Результат.** Описаны основные системы класса SIEM, перечислены их основные возможности, преимущества и недостатки, а также рассмотрены различные варианты построения таких систем и принципы сбора данных. **Вывод.** Изучение функционирования SIEM-систем позволяет оценить возможность их использования в построении систем безопасности различных масштабов и архитектур. Для максимального использования возможностей SIEM-систем необходимо провести её адаптацию и настройку под конкретные требования информационной безопасности. Перспективой дальнейших исследований будет применение гибридных подходов, основанных на промежуточных хранилищах с использованием потоковой передачи данных.

Ключевые слова: SIEM система, сбор данных, хранение данных, интеграция, информационная безопасность

Для цитирования: А.Д. Попов, А.Н. Никитенко. Принципы сбора данных для построения защищенной инфраструктуры предприятия на базе SIEM систем. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(1):173-179. DOI:10.21822/2073-6185-2024-51-1-173-179

Principles of data collection for building a secure enterprise infrastructure based on SIEM systems

A.D. Popov, A.N. Nikitenko
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. The purpose of the article is to present the main capabilities and advantages of implementing and using SIEM systems**. Method.** System analysis method was used. **Result.** The main systems of the SIEM class are described, their main capabilities, advantages and disadvantages are listed, and various options for constructing such systems and principles of data collection are considered. **Conclusion.** Studying the functioning of systems of this type allows us to assess the possibility of their use in the construction of security systems of various scales and architectures. To make maximum use of the capabilities of SIEM systems, it is necessary to adapt and configure it to specific information security requirements. The prospect for further research will be the use of hybrid approaches based on intermediate storage using data streaming.

Keywords: SIEM system, data collection, data storage, integration, information security

For citation: A.D. Popov, A.N. Nikitenko. Principles of data collection for building a secure enterprise infrastructure based on SIEM systems. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(1):173-179. DOI:10.21822/2073-6185-2024-51-1-173-179

Введение. В современном мире информация является ключевым ресурсом. Первостепенная задача всех организаций, будь то коммерческих, государственных или силовых структур, заключается в обеспечении надлежащего хранения, получения, обработки и пере-

дачи информации. Для решения подобных задач может внедряться целый парк программного обеспечения (файловые, почтовые, веб сервера и т.д.), который требует контроля со стороны средств информационной безопасности. Данная задача может усложняться тем, что структурные подразделения организации могут находиться в различных географических точках и выполнять разные задачи с точки зрения специфики использования программного обеспечения.

Постановка задачи. Выработка политики информационной безопасности и внедрение новых технологий (инструментов), способных улучшить защиту информации, становится актуальной задачей. Одним из таких инструментов являются SIEM (Security Information and Event Management) системы.

SIEM - системы (Security Information and Event Management) представляют собой решения для управления информацией и событиями безопасности, которые собирают данные из различных источников, анализируют их и предоставляют общую картину состояния информационной безопасности.

SIEM (Security Information and Event Management) системы включают в себя следующие основные подсистемы (рис. 1):

– Сбора данных: SIEM системы собирают данные об инцидентах безопасности из различных источников, включая сетевые устройства, СУБД, антивирусные системы и др.

– Хранения данных: собранные данные хранятся в специализированной базе данных.

– Анализа данных: SIEM система проводит анализ данных об инцидентах безопасности, выявляя аномалии и подозрительную активность.

– Визуализации данных: результаты анализа отображаются в виде графиков, диаграмм и других наглядных представлений.

– Создания отчетов: SIEM система может создавать отчеты о состоянии безопасности в организации.

– Интеграции: SIEM системы могут интегрироваться с другими системами безопасности, такими как системы предотвращения вторжений, межсетевые экраны и системы обнаружения вредоносного программного обеспечения.

– Управления инцидентами: SIEM система помогает управлять инцидентами безопасности, предоставляя рекомендации по их устранению и предотвращению.

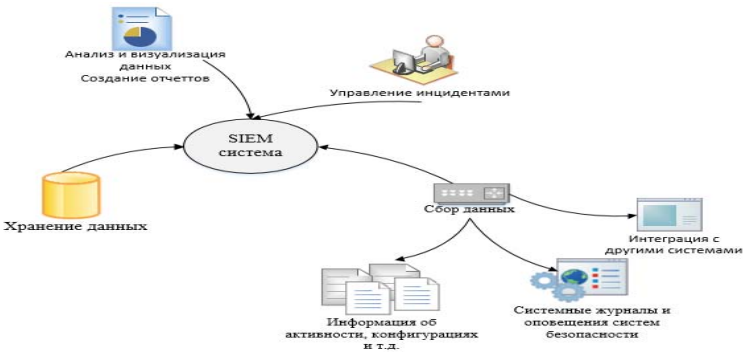

Рис.1. Состав SIEM системы
Fig.1. Composition of the SIEM system

Методы исследования. Существует множество современных SIEM-систем, которые популярны как в России, так и за рубежом. Приведем некоторые из них:

– Splunk Security – SIEM-система, которая предлагает широкие возможности для анализа и визуализации данных, а также имеет открытый API для интеграции с другими системами;

– Kaspersky Unified Monitoring and Analysis Platform (KUMA) – это центральный элемент единой платформы безопасности от «Лаборатории Касперского. Решение имеет встроенные сценарии автореагирования на выявленные события по безопасности и благодаря модулю ГосСОПКА полностью интегрировано с технической инфраструктурой Национального координационного центра по компьютерным инцидентам (НКЦКИ);

– MaxPatrol SIEM – это система мониторинга и анализа событий информационной безопасности (SIEM), разработанная компанией Positive Technologies;

– KOMRAD Enterprise SIEM (SIEM) – программное решение, которое помогает организациям отслеживать, анализировать угрозы безопасности и реагировать на них в режиме реального времени.

Проведенный анализ показал, что SIEM системы имеют следующие преимущества:

– выявляют угрозы и уязвимости в системе безопасности;

– собирают и анализируют данные с различных источников в режиме реального времени;

– автоматизируют процесс управления инцидентами;

– позволяют получить полную картину о состоянии безопасности.

Помимо преимуществ подобные системы имеют недостатки:

– высокая стоимость;

– сложность настройки;

– низкая скорость обработки данных при большом объеме;

– Некоторые SIEM-системы имеют ограниченные возможности интеграции с другими системами и приложениями;

– при увеличении объема данных или количества источников информации, системы имеют высокую ресурсопотребляемость, что может потребовать масштабируемости.

SIEM могут собирать журналы и события из различных источников и устройств. Каждое устройство или программное обеспечение генерирует события каждый раз, когда происходит обращение к нему или изменение в его настройках. В дальнейшем происходит обобщение, обработка и хранение всех событий.

Выделим основные четыре метода сбора информации SIEM системами:

1. Через агента, установленного на устройстве (рис.2). Является наиболее распространенным методом сбора.

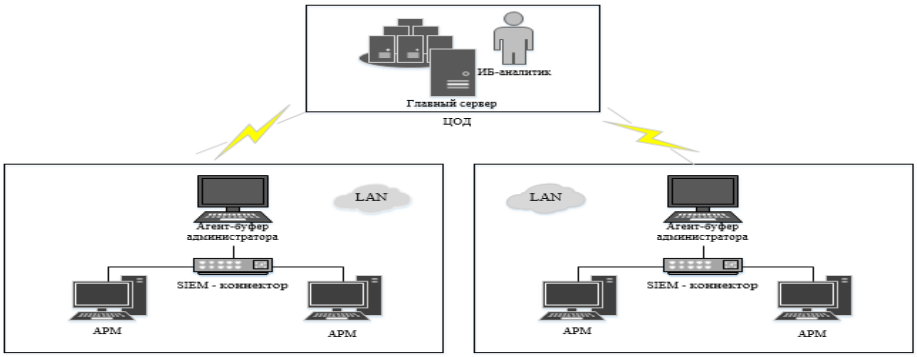

Рис. 2. Сбор информации через установку агента
Fig. 2. Collecting information through agent installation

Преимущества:

– Улучшение безопасности за счет сбора информации в режиме реального времени;

– Централизованный сбор данных;

– Гибкость настройки для различных устройств;

– Поддержка различных операционных систем и платформ;

– Непрерывный мониторинг;

– Устранение «слепых зон»: установка агентов на устройствах позволяет собирать данные, которые могут быть пропущены другими методами мониторинга, такими как сбор событий с сервера или сети.

Недостатки:

– Потребность в настройке;

– Установка агента на устройство может снизить его производительность, так как часть ресурсов будет использоваться для сбора и передачи данных;

– Установка агента может создать новые уязвимости в системе безопасности, так как это дополнительное программное обеспечение с возможными ошибками;

– Разработка, поддержка и обновление агентов требует дополнительных ресурсов и может стать сложной задачей для организаций с большим количеством устройств.

– Нестабильность сетевого подключения может вызвать связанные со сбором данных с конечных узлов.

2. Путем прямого подключения к устройству с помощью сетевого протокола или вызова API (рис. 3).

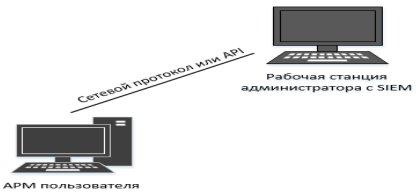

Рис. 3. Схема прямого подключения к устройству с помощью сетевого протокола или вызова API

Fig. 3. Diagram of direct connection to a device using a network protocol or API call

Основными преимуществами являются:

– Простота установки и настройки;

– Отсутствие агента на устройстве снижает его нагрузку, что улучшает производительность;

– SIEM-системы с таким подходом к сбору данных обычно более совместимы с различными устройствами и операционными системами;

– Отсутствие агента снижает вероятность уязвимостей в системе безопасности;

– SIEM-систему с таким подходом можно легко масштабировать для обработки большого количества устройств или данных;

– Прямой сбор данных позволяет получить более широкий спектр информации и использовать более продвинутые методы анализа.

К недостаткам можно отнести:

– Обновление устройств или изменение конфигурации может быть сложным без использования агента, который обеспечивает автоматическую синхронизацию;

– Интеграция по некоторым протоколам и с устройствами специального назначения может быть сложной и требовать более глубокой проработки;

– Некоторые данные могут быть недоступны или менее детализированы без использования агента;

– Сбор данных напрямую зависит от стабильности подключения устройства к сети.

3. Путем доступа к файлам журналов из промежуточного хранилища, сбор данных в котором, может быть организован в различных форматах (например, в виде системного журнала) (рис. 4).

Преимущества:

– Автоматическое обновление;

– Журналы доступны через стандартные протоколы, что облегчает интеграцию с SIEM системой;

– Журналы содержат большое количество разрозненной информации, что позволяет централизовано отправлять в аналитический сегмент SIEM систем;

– Уменьшенная нагрузка на АРМ пользователя, в отличие от агентов и уменьшенная нагрузка на каналы связи в отличие от прямого подключения;

– Поскольку SIEM система не имеет прямого доступа к устройствам, она менее уязвима для атак, но в тоже время для задач промежуточного хранения данных устанавливается узконаправленного программное обеспечение, которое требует дополнительного контроля с точки зрения информационной безопасности.

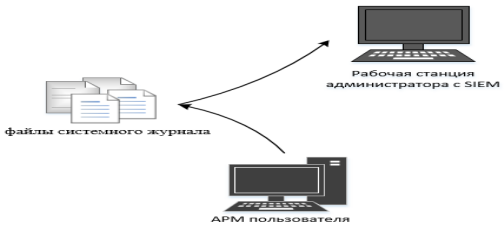

Рис. 4. Схема доступа к файлам журналов из промежуточного хранилища
Fig. 4. Scheme for accessing log files from staging storage

Недостатки:

– Данные из журналов могут быть сложными для анализа и требуют специализированных инструментов или навыков;

– Данные в журналах могут быть устаревшими, особенно если устройства не обновляются или не перезаписывают журналы;

– SIEM системе может потребоваться адаптация для работы с различными форматами журналов.

4. С помощью протокола потоковой передачи событий, такого как SNMP, Netflow или IPFIX (рис. 5).

Рис. 5. Схема SIEM системы со сбором информации с помощью протокола потоковой передачи событий

Fig. 5. Diagram of a SIEM system with information collection using the event streaming protocol

Преимущества:

– Протоколы потоковой передачи событий обеспечивают быстрый и непрерывный сбор данных в режиме реального времени;

– Широко распространённые протоколы;

– Потоковые протоколы обычно предоставляют более детализированные данные, чем другие методы сбора, что может быть полезно для анализа;

– Системы, построенные по этому принципу, хорошо масштабируются и могут обрабатывать большие объемы данных;

– Изменение конфигурации или обновление устройств обычно не влияет на SIEM систему с потоковой передачей данных.

Недостатки SIEM систем, использующих протоколы потоковой передачи событий:

– Настройка потоковой передачи данных более сложная;

– Сбор потоковых данных зависит от наличия и стабильности сетевого подключения;

– Менее исследованная предметная область, в отличие от предыдущих способов сбора данных.

Обсуждение результатов. Значимость рассмотренных преимуществ и недостатков различных подходов к сбору данных SIEM-системами может варьироваться в зависимости от стратегии информационной безопасности в организации. Выбор того или иного подхода для использования в SIEM-системах может быть основан на следующих выводах:

– Использование агентов для сбора информации является одним из наиболее распространенных способов в SIEM системах. Агенты устанавливаются на конечных устройствах (сервера, рабочие станции и т.д.) и собирают данные о событиях и активности в

режиме реального времени. Этот способ обеспечивает высокую гибкость и контроль над сбором данных, позволяя настраивать агентов для сбора только необходимой информации. Однако, использование агентов требует дополнительных ресурсов для установки и обслуживания на каждом устройстве.

– Интеграция с помощью API позволяет взаимодействовать с различными приложениями и системами для получения данных. Этот способ позволяет автоматизировать процесс сбора информации и получать данные в режиме реального времени. API также обеспечивает гибкость в выборе источников данных и позволяет настраивать параметры сбора. Однако, для использования API необходимо иметь доступ к соответствующим интерфейсам и настроить правильные аутентификационные механизмы для безопасной передачи данных.

– Использование промежуточного хранилища (например, базы данных или хранилища файлов) позволяет сохранять данные в промежуточном хранилище перед их передачей в SIEM систему. Это может быть полезно в случаях, когда требуется обработка большого объема данных или когда сетевая пропускная способность ограничена. Промежуточное хранилище также может использоваться для сохранения данных в случае временной недоступности SIEM системы. Однако, использование промежуточного хранилища требует дополнительных ресурсов для его установки и обслуживания.

– Использование протоколов быстрой передачи событий, таких как Syslog или SNMP, позволяет передавать данные о событиях в режиме реального времени. Эти протоколы обеспечивают высокую скорость передачи данных и широкую поддержку в различных устройствах и системах. Однако, протоколы быстрой передачи событий могут быть ограничены в возможностях настройки и выборе источников данных.

Основной особенностью архитектуры современной информационной системы является то, что она имеет большой масштаб и территориально распределена по регионам страны от центра. Помимо территориального расположения, система может функционировать в выделенной сети, что также стоит учесть при формировании архитектуры SIEM. Поэтому для успешного внедрения SIEM необходимо провести предварительное исследование информационных систем, входящих в структуру и определить требования к архитектуре SIEM. Внедрение SIEM-системы поспособствует оптимизации управления политикой информационной безопасности в структуре информационного обеспечения организации. Использование SIEM позволит эффективно контролировать, анализировать и коррелировать события безопасности, происходящие в информационных системах, что обеспечит своевременное выявление возможных угроз и инцидентов безопасности.

Вывод. В статье рассмотрены способы доставки данных о событиях информационной безопасности в SIEM системах. Описаны структура, ключевые функции, преимущества и недостатки этой системы, а также проанализированы возможные варианты архитектур и способы их реализации.

На основании проведенного анализа можно сделать вывод, что SIEM-системы являются эффективными инструментами для управления событиями информационной безопасности и информацией в современной инфраструктуре. Однако, для использования SIEM-систем требуется определенный уровень знаний и навыков, затраты на внедрение, поддержку и обучение. Для максимального использования возможностей SIEM необходимо провести её адаптацию и настройку под конкретные требования информационной безопасности. В целом, технологии SIEM являются важным компонентом современной системы информационной безопасности. Дальнейшее их изучение позволит совершенствовать технологии такого типа и разрабатывать новые системы обеспечения безопасности информации. Считаем, что перспективой дальнейших исследований будет применение гибридных подходов, основанных на промежуточных хранилищах с использованием потоковой передачи данных.

Библиографический список:

1. David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Security Information and Event Management (SIEM) Implementation. - McGraw Hill Professional, 2010. - 496 с.
2. Mark Talabis, Robert Mcpherson, I. Miyamoto, and Jason Martin Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. - Syngress, 2014. - 182 с.
3. Jay Jacobs, Bob Rudis Data-Driven Security Analysis, Visualization and Dashboards. Wiley, 2014. - 352 с.
4. SIEM Architecture: Technology, Process and Data // exabeam URL: https://www.exabeam.com/ (дата обращения: 06.10.2023).
5. Different types of logs in SIEM and their log formats // ManageEngine Log360 URL: https://www.manageengine.com/ (дата обращения: 06.10.2023).
6. Ворона В. А., Тихонов В. А. Комплексные (интегрированные) системы обеспечения безопасности. - Москва: Горячая линия-Телеком, 2013. - 160 с.
7. Оценка относительного ущерба безопасности информационной системы: монография / Дубинин Е.А., Тебуева Ф.Б., Копытов В.В. - Москва: РИОР, 2013. - 288 с.
8. Защита информации. Компьютерная безопасность: монография / Дубинин Е.А., Тебуева Ф.Б., Копытов В.В. - Москва: РИОР, 2022. - 192 с.
9. Evan Wheeler Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. - 1 изд. - Kindle, 2011. - 582 с.
10. Королев И. Д., Попов В.И., Ларионов В.А. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах // Инновации в науке. - 2018. - №12. - С. 19-25.

References

1. David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Security Information and Event Management (SIEM) Implementation. McGraw Hill Professional, 2010: 496.
2. Mark Talabis, Robert McPherson, I. Miyamoto, and Jason Martin Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014: 182.
3. Jay Jacobs, Bob Rudis Data-Driven Security Analysis, Visualization and Dashboards. Wiley, 2014: 352.
4. SIEM Architecture: Technology, Process and Data // exabeam URL: https://www.exabeam.com/ (access date: 10/06/2023).
5. Different types of logs in SIEM and their log formats. ManageEngine Log360 URL: https://www.manageengine.com/ (access date: 10/06/2023).
6. V. A. Vorona, V. A. Tikhonov. Complex (integrated) security systems. Moscow: Hotline-Telecom, 2013: 160. (In Russ)
7. Assessing the relative damage to the security of an information system: monograph / Dubinin E.A., Tebueva F.B., Kopytov V.V. Moscow: RIOR, 2013: 288. (In Russ)
8. Information protection. Computer security: monograph / Dubinin E.A., Tebueva F.B., Kopytov V.V. Moscow: RIOR, 2022: 192 (In Russ)
9. Evan Wheeler Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. - 1st ed. - Kindle, 2011: 582.
10. Korolev I. D., Popov V. I., Larionov V. A. Analysis of the problems of information management systems and security events in information systems. *Innovations in Science*. 2018;12: 19-25. (In Russ)

Сведения об авторах:

Попов Антон Дмитриевич, кандидат технических наук, доцент кафедры автоматизированных информационных систем органов внутренних дел; anton.holmes@mail.ru

Никитенко Анастасия Николаевна, слушатель, радиотехнический факультет; nastena.yefimova0001@.mail.ru

Information about authors:

Anton D. Popov, Cand. Sci. (Eng.), Assoc. Prof., Department of automated information systems of internal organs; anton.holmes@mail.ru,.

Anastasia N. Nikitenko, Student of the Radio Engineering faculty; nastena.yefimova0001@.mail.ru

Конфликт интересов / Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 25.11.2023.

Одобрена после рецензирования / Reviced 17.12.2023.

Принята в печать /Accepted for publication 17.12.2023.