УДК 004.056

Бутин А. А.[1], Соколова А. И.[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ОСОБЕННОСТИ ИНТЕГРАЦИИ SIEM-СИСТЕМЫ С ДРУГИМИ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В данной статье освещены особенности интеграции SIEM-системы с другими средствами защиты информации, включающие в себя проблемы, которые необходимо учитывать специалисту при разработке системы защиты информации. Проанализирована статистика увеличения компьютерных атак за последние годы. Описано назначение и приведена архитектура SIEM-системы, интегрированной с другими средствами защиты информации. Проанализировано, какие средства наиболее часто выступают в роли источников событий информационной безопасности. Отражены принципы функционирования программного обеспечения, предназначенного для сбора, нормализации и корреляции событий. Описан процесс сбора событий посредством сканирования сетевых узлов в разных режимах. Рассмотрена необходимость настройки сетевых протоколов и специализированного программного обеспечения для сбора событий, а также используемые для этого методы. Приведен принцип срабатывания правил корреляции событий. Для актуализации существующих правил предложено использование матрицы MITRE ATT&CK, в которой описаны техники, используемые злоумышленниками для реализации атак. Отражен параметр для подсчета количества событий, поступающих в SIEM-систему от средств защиты информации. Также рассмотрен современный способ масштабирования системы защиты информации с помощью улучшения технической оснащенности системы хранения.

Ключевые слова: информационная безопасность, событие информационной безопасности, инцидент информационной безопасности, SIEM-система.

Butin A. A.[1], Sokolova A. I.[1]

[1]Irkutsk State Transport University, Irkutsk, Russian Federation

FEATURES OF INTEGRATION OF THE SIEM SYSTEM WITH OTHER INFORMATION SECURITY MEANS

Annotation. This article highlights the features of the integration of a SIEM system with other information security means, including problems that must be taken into account by a specialist when developing an information security system. The statistics of the increase in computer attacks in recent years are analyzed. The purpose and architecture of a SIEM system integrated with other information security means are described. It is analyzed which tools most often act as sources of information security events. The principles of the functioning of software designed to collect, normalize and correlate events are reflected. The process of collecting events by scanning network nodes in different modes is described. The necessity of configuring network protocols and specialized software for event collection, as well as the methods used for this purpose, is considered. The principle of operation of the correlation rules is given. To update the existing rules, it is proposed to use the MITRE ATT&CK matrix, which describes the techniques used by attackers to implement attacks. The parameter for counting the number of events received by the SIEM system from information security means is reflected. A modern way of scaling the information security system by improving the technical equipment of the storage system is also considered.

Keywords: information security, information security threat, information security event, information security incident, SIEM system.

Введение. Тема расследования инцидентов информационной безопасности в настоящее время не теряет своей актуальности, растет количество кибератак, банк угроз пополняется новыми угрозами, находят новые уязвимости.

Для сравнения рассмотрим статистику увеличения числа атак на веб-ресурсы компаний с 2022 по 2023 год, приведённую на рис. 1. [1]

Рис. 1. – Число атак на веб-ресурсы компаний

Согласно статистике, приведённой Positive Technologies, количество проектов по восстановлению нарушенных бизнес-процессов возросло на 76% за первые девять месяцев 2023 года, в сравнении с показателями за весь 2022 год. Данная статистика отражена на рис.2. [2]

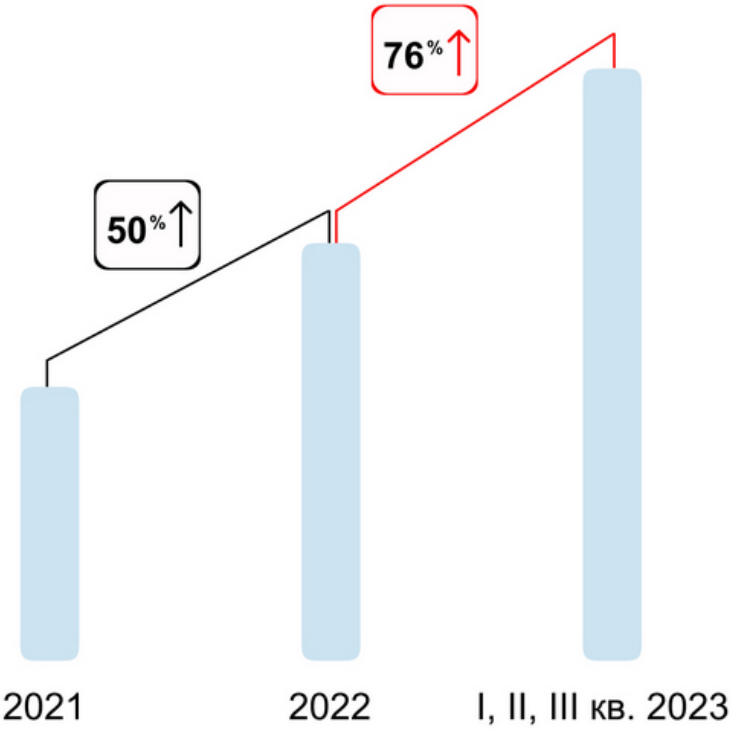

Рис. 2 – Количество проектов по расследованию инцидентов в 2021-м, 2022-м и за I—III квартал 2023 года

В связи с возросшей необходимостью отражать атаки всё больше компаний задумывается над построением системы защиты, способной обработать огромное количество информационных поток предприятия.

С целью сбора и анализа информации с различных средств защиты информации таких, как DLP, IDS, IPS, антивирусы, средства VPN, разработаны SIEM-системы. Но интеграция таких систем является сложным процессом, включающим в себя ряд особенностей, которые будут рассмотрены в данной статье.

Назначение SIEM-системы. SIEM (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информацией о безопасности, и SEM (Security event management) — управление событиями безопасности. [3]

К функциям SIM-системы относятся сбор, хранение и анализ записей журналов, а также формирование необходимой отчетности. К функциям SEM-системы относится мониторинг событий безопасности в реальном времени, а также выявление уязвимости и реагирование на инциденты безопасности. [4]

Пример архитектуры данной системы представлен на рис. 3.

Рис. 3. – Архитектура SIEM-системы

Источники событий. Интеграция SIEM-системы с средствами защиты имеет ряд особенностей, которые необходимо учитывать при разработке архитектуры системы защиты информации.

Важным шагом в разворачивании SIEM-системы является выбор источников событий.

Источники событий информационной безопасности — специализированное программное и аппаратное обеспечение для информационной безопасности, порождающее события информационной безопасности.

Источники событий сообщают о тех или иных явлениях в автоматизированной системе без оценки уровня их защищенности.

Компонент сбора событий сканирует IT-инфраструктуру предприятия, собирает сведения о сетевых узлах и события с источников. Собранные данные передаются компоненту управления. [5]

Примеры источников событий информационной безопасности: IDS/IPS (для сбора данных о сетевых атаках), средства антивирусной защиты (обнаружение вредоносных программ). Статистика наиболее часто подключаемых источников событий информационной безопасности представлена на рис. 4. [6]

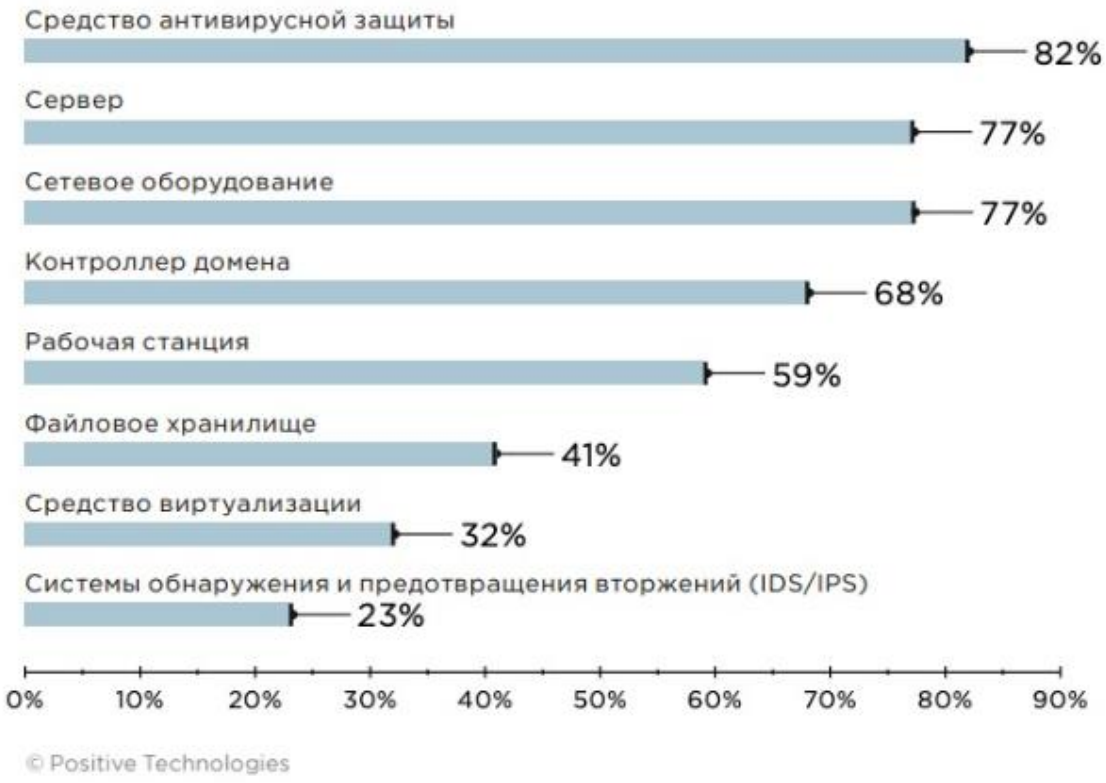

Рис. 4. – Наиболее часто подключаемые источники событий

Оператор SIEM-системы может обнаруживать новые активы источников событий с помощью встроенных модулей. Это происходит посредством сканирования сетевых узлов в режимах белого ящика (модулем audit) и черного ящика (модулем pentest).

Настройка отправки событий. Также одной из основных задач для специалиста, разворачивающего систему в инфраструктуре предприятия, является настройка отправки событий.

Зачастую это реализуется посредством настройки протокола syslog.

Syslog-сервер – это внешний сервер для сбора событий. Он хранит и анализирует полученные события, а также выполняет другие действия по управлению журналами. [7]

Стоит учитывать, что для сбора событий с некоторых источников событий требуются специализированные коннекторы.

Коннектор – специализированное ПО, предназначенное для сбора событий информационной безопасности, хранящихся в базе данных, и последующей первичной обработки полученных событий к единому внутреннему стандарту SIEM (преобразование к нормализованному виду).

Сбор событий может осуществляться в активном режиме – сборщик событий сам подключается к источнику по различным протоколам (RPC, SMB и т.д.) и собирает у него события. Или же источник сам присылает события посредством протокола Syslog или SNMP. [8]

Нормализация событий. Не менее важным при интеграции SIEM-системы со сторонними средствами защиты информации являются правила нормализации событий. События, получаемые от источников в «сыром» виде, необходимо привести к единой структуре, чтобы SIEM-система могла распознать их для последующей корреляции. При нормализации определяются, как минимум, основные сущности события: субъект, объект, источник, канал взаимодействия. [9]

Правила корреляции. Кроме того, для конкретных источников событий пишут отдельные правила корреляции. В них описываются критерии возникновения угрозы и реакция на них.

В SIEM-систему поступает огромный поток событий. Для того, чтобы связать их в одно событие информационной безопасности в правилах корреляции прописываются необходимые для этого условия (симптомы). Например, попытка неуспешного входа. Сервер корреляции отвечает за понимание инцидентов и отсеивание простых событий от общего потока. [10]

Счетчик подсчитывает количество совпадений по одному правилу. При определённом количестве событий SIEM-система может создать инцидент информационной безопасности. [11]

Принцип срабатывания правила корреляции приведен на рис. 5.

Рис. 5 – Принцип срабатывания правила корреляции

Правила корреляции должны постоянно актуализироваться экспертами. Поскольку меняются не только угрозы, но и инфраструктура предприятия. Для актуализации правил, например, можно использовать матрицу MITRE ATT&CK, отслеживая техники, которые используют злоумышленники в инцидентах информационной безопасности. [12]

Производительность при обработке большого количества событий. При внедрении SIEM-системы также важно рассчитать число обрабатываемых событий в секунду – EPS (events per second), получаемых от источников событий. [13]

Чтобы увеличить производительность хранилища событий и сократить расходы на аппаратное обеспечение, разработали гибридную схему хранения данных. В этом случае последние суточные индексы будут записываться на высокоскоростные твердотельные накопители (SSD) и со временем будут постепенно перезаписываться на более доступные накопители на жестких магнитных дисках. Это позволяет увеличить скорость обработки событий при одновременном выполнении поисковых запросов. [14]

Немаловажным является возможность масштабирования и отказоустойчивости системы, в особенности, если планируется увеличение количества средств защиты информации в инфраструктуре предприятия. [15]

Заключение. Интеграция SIEM-системы с другими средствами защиты информации является многоэтапным и сложным процессом. После проведения анализа того, какие средства

защиты информации станут источниками событий для системы мониторинга, специалисту необходимо настроить процесс отправки событий, проработать правила нормализации и корреляции, а также рассчитать количество обрабатываемых событий. Необходимо постоянно учитывать особенности архитектуры информационной системы и меняющиеся угрозы информационной безопасности. Только при непрерывной работе над улучшением системы защиты информации SIEM-система станет эффективным инструментом для контроля и устранения уязвимостей информационной системы предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кибербезопасность в 2023-2024 гг.: тренды и прогнозы. Часть третья (ptsecurity.com) [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (Дата обращения: 10.04.2024).
2. Итоги расследований инцидентов ИБ в 2021–2023 годах (ptsecurity.com) [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (Дата обращения: 10.04.2024).
3. SIEM (ru.wikipedia.org) [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/SIEM (Дата обращения: 10.04.2024).
4. Абденов А. Ж., Трушин В. А., Сулайман К. Анализ, описание и оценка функциональных узлов SIEM-системы: учебное пособие. – Новосибирск: НГТУ, 2018. – 122 с. (Дата обращения: 10.04.2024).
5. Алгоритм работы MaxPatrol SIEM и схема взаимодействия компонентов (help.ptsecurity.com) [Электронный ресурс]. – URL: https://help.ptsecurity.com/ru-RU/projects/siem/8.0/help/2189382283 (Дата обращения: 10.04.2024).
6. Выявление инцидентов ИБ с помощью SIEM: типичные и нестандартные задачи, 2020 (ptsecurity.com) [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/incidents-siem-2020/ (Дата обращения: 11.04.2024).
7. Настройка параметров интеграции с SIEM (support.kaspersky.com) [Электронный ресурс]. – URL: https://support.kaspersky.com/KSWS/11/ru-RU/146650.htm (Дата обращения: 10.04.2024).
8. И снова про SIEM (habr.com) [Электронный ресурс]. – URL: https://habr.com/ru/companies/otus/articles/773430/ (Дата обращения: 11.04.2024).
9. Глубины SIEM: корреляции «из коробки». Часть 3.2. Методология нормализации событий (securitylab.ru) [Электронный ресурс]. – URL: https://www.securitylab.ru/blog/company/pt/345379.php (Дата обращения: 12.04.2024).
10. SIEM – Security Information and Event Management (www.securityvision.ru) [Электронный ресурс]. – URL: https://www.securityvision.ru/blog/siem-security-information-and-event-management/ (Дата обращения: 12.04.2024).
11. Корреляция SIEM – это просто. Сигнатурные методы (securitylab.ru) [Электронный ресурс]. – URL: https://www.securitylab.ru/analytics/431459.php?ysclid=luwe2xur4h87421031 (Дата обращения: 12.04.2024).
12. Сколько правил нужно SIEM-системе (kaspersky.ru) [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/siem-rules/35597/ (Дата обращения: 12.04.2024)
13. Внедрение SIEM – что нужно знать про него (habr.com) [Электронный ресурс]. – URL: https://habr.com/ru/sandbox/97147/ (Дата обращения: 12.04.2024)
14. MaxPatrol SIEM теперь обрабатывает до 60 000 событий в секунду (ptsecurity.com) [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/about/news/maxpatrol-siem-teper-obrabatyvaet-do-60-000-sobytij-v-sekundu/ (Дата обращения: 12.04.2024).
15. Как правильно выбрать и внедрить SIEM-систему (anti-malware.ru) [Электронный ресурс]. – URL: https://www.anti-malware.ru/practice/methods/How-to-choose-and-implement-SIEM-correctly (Дата обращения: 12.04.2024).

REFERENCES

1. Cybersecurity in 2023-2024 гг.: trends and forecasts. Part three (ptsecurity.com) [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (Date of the operation: 10.04.2024).
2. Results of investigations of information security incidents in 2021-2023 (ptsecurity.com) [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (Date of the operation: 10.04.2024).
3. SIEM (ru.wikipedia.org) [Electronic resource]. – URL: https://ru.wikipedia.org/wiki/SIEM (Date of the operation: 10.04.2024).
4. Abdenov A. J., Trushin V. A., Sulaiman K. Analysis, description and evaluation of functional nodes of the SIEM system: a training manual. – Novosibirsk: NSTU, 2018. – 122 p. (Date of the operation: 10.04.2024).
5. MaxPatrol SIEM algorithm and component interaction scheme (help.ptsecurity.com) [Electronic resource]. – URL: https://help.ptsecurity.com/ru-RU/projects/siem/8.0/help/2189382283 (Date of the operation: 10.04.2024).
6. Identification of information security incidents using SIEM: typical and non-standard tasks, 2020 (ptsecurity.com) [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/incidents-siem-2020/ (Date of the operation: 11.04.2024).
7. Configuring the parameters of integration with SIEM (support.kaspersky.com) [Electronic resource]. – URL: https://support.kaspersky.com/KSWS/11/ru-RU/146650.htm (Date of the operation: 10.04.2024).
8. And again about SIEM (habr.com) [Electronic resource]. – URL: https://habr.com/ru/companies/otus/articles/773430/ (Date of the operation: 11.04.2024).
9. SIEM depths: out-of-the-box correlations. Part 3.2. Event normalization methodology (securitylab.ru) [Electronic resource]. – URL: https://www.securitylab.ru/blog/company/pt/345379.php (Date of the operation: 12.04.2024).
10. SIEM – Security Information and Event Management (www.securityvision.ru) [Electronic resource]. – URL: https://www.securityvision.ru/blog/siem-security-information-and-event-management/ (Date of the operation: 12.04.2024).
11. SIEM correlation is simple. Signature methods (securitylab.ru) [Electronic resource]. – URL: https://www.securitylab.ru/analytics/431459.php?ysclid=luwe2xur4h87421031 (Date of the operation: 12.04.2024).
12. How many rules does the SIEM system need (kaspersky.ru) [Electronic resource]. – URL: https://www.kaspersky.ru/blog/siem-rules/35597/ (Date of the operation: 12.04.2024)
13. SIEM implementation – what you need to know about it (habr.com) [Electronic resource]. – URL: https://habr.com/ru/sandbox/97147/ (Date of the operation: 12.04.2024)
14. MaxPatrol SIEM now processes up to 60,000 events per second (ptsecurity.com) [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/about/news/maxpatrol-siem-teper-obrabatyvaet-do-60-000-sobytij-v-sekundu/ (Date of the operation: 12.04.2024).
15. How to choose and implement a SIEM system correctly (anti-malware.ru) [Electronic resource]. – URL: https://www.anti-malware.ru/practice/methods/How-to-choose-and-implement-SIEM-correctly (Date of the operation: 12.04.2024).

Информация об авторах

Александр Алексеевич Бутин – к. ф.-м. н., доцент, доцент кафедры «кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск

Алена Игоревна Соколова – студент, Иркутский государственный университет путей сообщения, г. Иркутск

Authors

Aleksander Alekseevich Butin, Candidate of Physico-Mathematical Sciences, Doctor, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk

Alena Igorevna Sokolova, student, Irkutsk State Transport University, Irkutsk

Для цитирования

Соколова А.И., Бутин А.А. Особенности интеграции SIEM-системы с другими средствами защиты информации // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №2. – С. 38-46. – Режим доступа: https://ismm.irgups.ru/toma/222-2024, свободный. – Загл. с экрана. – Яз. рус., англ.

For citations

Sokolova A.I., Butin A.A. Features of integration of the SIEM system with other information security means // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2024. No. 2. P. 38-46.