Автор:

Кравцов Андрей Андреевич

студент

ФГБОУ ВО «Государственный университет морского

и речного флота им. адмирала С.О. Макарова»

г. Санкт-Петербург

DOI 10.21661/r-474921

SIEM – ИНСТРУМЕНТ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация*: в данной статье рассмотрены решения по управлению информацией и событиями безопасности – SIEM. Дано определение и указаны задачи, для которых применяются SIEM-системы. Приведены: базовые возможности, модульная структура и пример работы некоторой организации без/с внедрённой SIEM-системой. Проведён краткий обзор рынка и сравнение двух ведущих SIEM-систем на рынке. На основе обзора рынка и результатов сравнения даны рекомендации приобретению SIEM как систем централизованного ведения журнала регистрации и помощи в обнаружении, анализе и смягчении событий безопасности.*

Ключевые слова*: SIEM, управление безопасностью, журналы событий, сбор информации, анализ информации.*

SIEM-система

SIEM (Security information and event management) – данное название системы происходит от двух других терминов, обозначающих разные области применения: SIM (Security information management) – управление информационной безопасностью и SEM (Security event management) – управление событиями безопасности.

Основной задачей SIEM системы является – анализировать (в реальном времени) регистрируемые в защищаемой инфраструктуре события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные

действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

SIEM системы не являются гарантией безопасности организации, они представляют собой лишь механизмы для сбора и анализа информации из других систем, таких как DLP, коммутаторы, маршрутизаторы, систем антивируса, межсетевых экранов, АРМ пользователей и т. д. Но они также важны для любого крупного предприятия, т.к. при большом количестве аппаратно программных средств, отдел информационной безопасности просто не сможет (на физическом уровне) покрыть и зафиксировать все инциденты ИБ. Поэтому, к основным потребителям SIEM систем на рынке, можно отнести всего несколько типов предприятий:

– предприятия из финансовой сферы;

– крупные предприятия (предприятия, обладающие большой инфраструктурой – более 1000 единиц оборудования).

Возможности и структура SIEM системы

Базовые возможности системы SIEM является обеспечение решение следующих задач:

– сбор и хранение инцидентов ИБ;

– обработка и анализ инцидентов ИБ;

– обнаружение атак и нарушений политик безопасности в реальном времени;

– выявление и регистрация инцидентов ИБ;

– формирование отчетов.

Кроме того, к современным решениям SIEM предъявляются дополнительные требования с целью обеспечить реализацию следующих функциональных возможностей:

– оценка защищенности ресурсов контролируемой системы;

– проверка соответствия системы управления ИБ существующим требованиям и нормам;

– управление рисками ИБ и др.

Функциональная модель системы SIEM объединяет следующие функциональные подсистемы:

– коллекторы;

– хранилища данных;

– корреляторы;

– консоль управления.

Коллекторы – системы отвечающие за сбор информации с различных источников. Поддерживают большое количество протоколов и сервисов: Syslog, SDEE, SNMP Trap, клиентов баз данных (MSSQL, Oracle и т. п.). Являются весьма важной частью системы, т.к. от каждого источника в информационной системе могут приходить данные различных форматов. Поэтому правильная обработка данных на коллекторе может упростить работу для следующих систем.

Хранилища данных – являются весьма важной частью системы. Важно чтобы хранилище было способно обработать поток событий как в пиковые часы, так и в среднем. При этом необходимо распределить нагрузку, при необходимости обеспечив балансировку данной нагрузки.

Корреляторы – обеспечивают обработку, анализ и выявление коррелирующих зависимостей между различными событиями ИБ.

Консоль управления – обеспечивает визуализацию, настройку и управление получаемыми данными. Можно заметить, что функция визуализации может выполняться отдельными компонентами.

Хочу обратить внимание, что данный перечень не является идеальным, т.к. полный состав можно предоставить лишь в условиях реализации в отдельной организации, и может меняться в зависимости от архитектуры решения, размеров инфраструктуры и параметров производительности системы организации в целом.

Обобщенная последовательность обработки событий безопасности в системе SIEM поясняется рисунком 1.

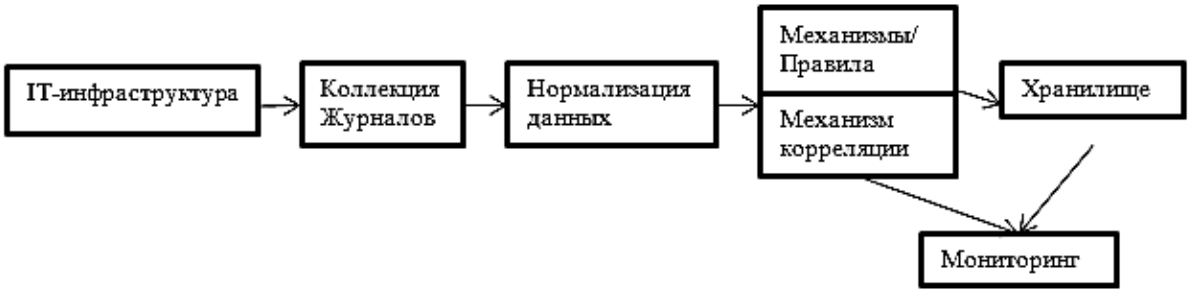

Рис. 1. Последовательность обработки Инцидентов ИБ

Пример необходимости SIEM системы

Как было сказано выше, сама SIEM система не может защитить организацию от инцидентов ИБ. Но она и не предназначена для этого, SIEM система может предоставить полную информацию о произошедшем инциденте ИБ в виде различных отчётов и графиков, что в свою очередь позволит службе информационной безопасности пресечь утечку информации или косвенно повлиять на неэффективное использование/управление ресурсами предприятия.

Предположим, у нас есть некая структура организации включающая в себя:

1. IT-инфраструктуру – все аппаратно программные средства компании.

2. IT-департамент – может включать в себя все отделы связанные непосредственно с IT-технологиями на предприятии (отдел системного администрирования, отдел информационной безопасности и т. п.).

3. CIO (Chief Information Officer)/CISO(Chief Information Security Officer) – директор по информационным технологиям (IT-директор) / директор по IT-безопасности.

4. ТОП-менеджмент – руководители организации, несущие ответственность за эффективное управление организацией.

Представим себе, что может быть с данной системой без SIEM:

Данные поступают от IT-инфраструктуры в IT-департамент, что влечёт за собой:

– перегруженность данными;

– возможная потеря событий;

– неполный анализ событий;

– затруднения в представление информации и т. д.

После этого IT-департамент пытается каким-то образом предоставить информацию CIO/CISO, и уже у них возникают проблемы:

– как представить результаты работы IT;

– как объяснить текущие проблемы IT-департамента на языке бизнеса;

– как обосновать нужды IT-департамента на языке бизнеса;

Далее информация переходит в руки ТОП-менеджмента:

– непонимание текущей проблемы IT;

– непонимание нужд IT-департамента;

– неэффективное планирование стратегии развития IT-департамента.

Вследствие все вышепересказанные проблемы выливаются в:

– неэффективное управление ресурсами;

– неэффективное планирование;

– неадекватное реагирование на инциденты ИБ;

– потеря контроля над инцидентами ИБ;

– неудовлетворение нужд IT-департамента;

– возможные потери прибыли.

Но если мы представим, что в нашей системе появилась SIEM:

В таком случае, данные от IT-инфраструктуры будут проходить полный цикл обработки информации в SIEM системе после чего переходят в IT-департамент и вследствие этого они имеют:

– сгенерированные инциденты ИБ;

– категорированные данные;

– выполненные анализы инцидентов ИБ;

– подготовленные отчёты.

Все необходимые документы переходят из IT-департамента к CIO/CISO, теперь они имеют:

– наглядное представление проблем: графики, диаграммы и т. п.;

– отчёты, составленные по стандартам ИБ;

– обоснованные нужды IT-департамента, подкреплённые соответствующими документами.

Далее CIO/CISO могут в полной мере отразить необходимую информацию для ТОП-менеджмента, вследствие они имеют:

– понимание текущей ситуации и проблем IT по организации в целом;

– адекватное планирование развития IT-департамента.

Впоследствии мы имеем:

– эффективное управление ресурсами;

– эффективное планирование;

– адекватное реагирование на инциденты ИБ;

– контроль над инцидентами ИБ;

– удовлетворение нужд IT-департамента;

– возможное увеличение прибыли.

Представленный выше пример не является истиной для многих предприятий, но он наглядно показывает, как может повлиять внедрение SIEM системы.

Обзор рынка

Ранние услуги и продукты SIEM имели репутацию как предназначенных для крупных организаций с расширенными возможностями безопасности. Основной мотивацией этих развертываний было дублирование журналов сетевой безопасности в централизованном месте, чтобы администраторы и аналитики безопасности могли просматривать все журналы в одной консоли, а также потенциально коррелировать события в журнальных источниках в поддержку обнаружения инцидентов и реальных событий, время реагирования.

С тех пор системы SIEM превратились в основной компонент безопасности. По мере увеличения количества источников записей в журнале безопасности, необходимо просматривать, анализировать и сообщать о событиях безопасности, охватываемых этими записями журнала, с одной консоли.

Даже малым и средним организациям, как правило, нужен инструмент SIEM для соблюдения целей – автоматическое создание отчетов, которые свидетельствуют о соблюдении организацией различных требований соответствия.

Стоимость внедрения SIEM широко варьируется в зависимости от двух основных факторов: надежности, возможностей SIEM и выбранной архитектуры развертывания.

С точки зрения надежности некоторые SIEM предлагают легкое решение, которое обеспечивает базовые функции управления журналом и отчетов без использования современных методов анализа и других функций, поддерживаемых другими SIEM.

Архитектура развертывания также имеет очевидные финансовые последствия для внедрения SIEM. Большинство SIEM требуют приобретения оборудования или программного обеспечения, в то время как плата за использование определяет стоимость облачных услуг SIEM.

В дополнение к приобретению продукта SIEM организации могут иметь другие авансовые затраты. Например, системы SIEM все чаще поддерживают использование источников информации об угрозах, которые содержат самую последнюю информацию об организациях угроз, наблюдаемых во всем мире. Угрозы интеллектуального анализа могут значительно повысить точность возможностей обнаружения инцидентов SIEM, но использование таких источников информации обычно требует выплаты существенной абонентской платы.

Рассматривая рынок SIEM систем, нельзя сказать, что он является слишком обширным, но можно быть уверенным, что даже предприятия малого и среднего бизнеса смогут найти себе подходящие под их нужды системы.

Ниже приведен краткий обзор ведущих поставщиков SIEM.

Splunk Enterprise Security (*ES*)

Система SIEM Splunk имеет высокую оценку и популярность, но затраты на лицензирование могут вывести ее за пределы некоторых малых и средних. Он лучше всего подходит для более крупных, хорошо укомплектованных ИТ-организаций, которые готовы платить за высокую эффективность.

IBM Security QRadar

QRadar высоко оценивается большинством аналитических фирм. Сложность внедрения может ограничить его привлекательность для средних и

крупных предприятий, которым требуются основные возможности SIEM, а также для тех, кто ищет единую платформу, охватывающую широкий спектр технологий мониторинга безопасности и эксплуатации.

LogRhythm SIEM

LogRhythm – еще один поставщик SIEM с высокими рейтингами и популярностью. Он проще развёртывается, чем некоторые другие высокопроизводительные продукты SIEM, но он не может масштабироваться для поддержки очень больших объемов событий. Данный вариант лучше всего подходит для небольших и средних организаций, которые уже обладают некоторой функциональностью для анализа угроз и аналитики.

AlienVault Unified Security Management (USM)

AlienVault предлагает недорогую запись с удивительно надежными функциями для небольших и средних компаний. Пусть он может не давать все возможности, которые ищут предприятия, но для небольших и средних организаций, которые ищут свой первый продукт SIEM, AlienVault трудно превзойти.

Micro Focus Sentinel Enterprise

Micro Focus Sentinel Enterprise может не подходить большинству крупных предприятия, т.к. она отстаёт от некоторых конкурентов в функциональности и полноте видения предприятия. Но данная система определенно может быть рассмотрена небольшими и средними организациями, которые не имеют SOC с высокой степенью зрелости и не имеют требований для полного управления инцидентами ИБ.

McAfee Enterprise Security Manager (ESM)

McAfee может быть позади IBM, Splunk и LogRhythm в общей полноте SIEM, но его готовые устройства и простота развертывания, а также интеграция с другими инструментами McAfee, делают его сильным соперником во многих коротких списках SIEM.

Trustwave SIEM Enterprise и Log Management Enterprise

Trustwave SIEM ориентирован на пользователей среднего и корпоративного уровня. Он особенно привлекателен для текущих пользователей других

инструментов Trustwave, а также для покупателей с различными ИТ-средами. Одним из недостатков является отсутствие аналитики угроз из коробки, заставляя пользователей покупать или включать дополнительные инструменты для аналитики угроз.

RSA NetWitness Suite

RSA NetWitness популярен на крупных предприятиях с хорошо обученными, ветеранскими командами ИТ-безопасности, особенно в финансовых, правительственных, энергетических и телекоммуникационных организациях. Он может не иметь некоторые из особенностей SIEM лидеров, таких как Splunk, LogRhythm и IBM, но имеет определенное преимущество в существующих магазинах RSA, Dell и EMC.

Диспетчер журналов и событий SolarWinds

SolarWinds может не иметь полного набора безопасности конкурентов, но он хорошо ценится за простоту развертывания, стоимость, производительность и поддержку. Его формат виртуального устройства делает его хорошим выбором для малых и крупных организаций с ограниченными ИТ-ресурсами.

Так же я бы хотел привести краткое сравнение, нескольких из ведущих SIEM систем на рынке, по отзывам людей, пользующихся данными системами, а имена я бы хотел сравнить IBM Security QRadar и Splunk Enterprise Security.

Таблица 1

Сравнение по отзывам

IBM QRadar	*Splunk*
Отзывы	
Из-за силы, надежности и стоимости данного решения я считаю, что он лучше всего подходит для крупных предприятий. Хотя средний бизнес наверняка найдет в ней ценность, эта система не для слабонервных. Qradar хорошо подходит для сред с большим количеством входящих данных, где ручной анализ может быть не подходящим.	Splunk – отличный инструмент для анализа данных, если у вас есть большой объем данных для анализа. Splunk обеспечивает точный анализ данных в режиме реального времени через свою панель. Но если вы не совсем технический человек или не хотите изучать Splunk перед его использованием, я не буду рекомендовать его вам. Кроме того, Splunk менее подходит для статических данных.
Преимущества	
– создание правил интуитивно и быстро помогает в чрезвычайных ситуациях; – обслуживание платформы очень просто, в то время как приложение имеет почти безупречное время безотказной работы; – генерация отчетов очень функциональна и эффективна; – обеспечение видимости в режиме реального времени для обнаружения угроз и определения приоритетов – QRadar SIEM обеспечивает контекстное и эффективное наблюдение во всей ИТ-инфраструктуре; – он очень стабилен; – это улучшило широкую видимость того, что происходит по периметру и внутри IT структуры предприятия; – первоначальная настройка не является слишком сложной; – это система улучшает эффективность персонала в вопросах безопасности.	– Splunk отлично подходит для визуализации ваших данных в формате, который может указывать на тенденции; – Splunk может помочь вам определить первопричину и последовательно ассимилировать разнородные источники данных; – Splunk может помочь вам найти проблемы с иглой в стоге сена, без необходимости входить в систему на разных устройствах; – Splunk может быть настроен для поиска симптомов, которые могут вызывать проблемы в вашей среде, а также предупреждать об этом или запускать действие; – это решение помогает повысить производительность персонала; – он прост в использовании и применении; – положительные функции включают возможности репликации, комплекты разработки программного обеспечения и архитектуры; – это универсальное решение для мониторинга и оповещения для операций и анализа приложений для большинства систем.
Недостатки	
– существует крутая кривая обучения по сравнению с другими платформами. Qradar невероятно мощный, но требует некоторой домашней работы;	– это может быть дорогостоящим, но стоящим того решением; – обучение пользователей немного сложно; – были проблема, когда Splunk потерпел неудачу, и потребовалось пару дней, чтобы восстановиться;

– может потребоваться значительное количество настроек во время развертывания с очень малой информацией о вторжениях «из коробки»; – все превосходно, но нуждаются в улучшениях; – техническая поддержка хороша, но не велика; – индийская техническая поддержка не помогает; – QRadar требует много тонкой настройки; – качество технической поддержки зависит от лица, поддерживающего IBM. Иногда трудно найти нужного человека на другой стороне.	– брандмауэр веб-приложений отправляет вам слишком много информации, поскольку он больше посвящен безопасности, чем обычный брандмауэр; – он должен иметь лучший способ экспортировать динамические представления, не требуя тонны кода и пользователя / пароля; – он нуждается в интеграции с решением для управления конфигурацией; – улучшенный пользовательский интерфейс наряду с поддержкой нескольких арендаторов будет полезен.
Цена	
– это очень дорого; – хорошим подходом было бы начать с подписки On Cloud, а затем сделать более точный размер; – Ценообразование и лицензирование являются конкурентоспособными. Их новые варианты лицензирования позволяют журналам обходить механизм корреляции с фиксированной ставкой, что также привлекательно для журнальных данных, которые управляются по требованию за небольшую сумму денег; – ценообразование (на основе EPS) будет более точным.; – это дорого. Это не продукт, который я могу предоставить для SMB. Это программа, которую могут обеспечить только для действительно крупных предприятий; – расходы на обслуживание очень высоки.	– можно использовать лицензию разработчика, которая составляет до 10 ГБ в день объемного трафика, чего обычно достаточно для большинства случаев использования; – это может быть дорого, особенно расходы на лицензирование; – Splunk немного дороже, но преимущества и рентабельность инвестиций огромны; – это довольно дорогостоящее решение, но если у вашей организации есть средства, это может принести много преимуществ; – расходы на персонал сохраняются, не привлекая разработчиков домена из нескольких команд при отслеживании проблемы, охватывающей несколько платформ.

Вывод

Подводя итоги, я бы хотел сказать, что продукты и услуги SIEM служат двум целям: обеспечению централизованного ведения журнала регистрации и отчетности для организации и оказанию помощи в обнаружении, анализе и смягчении событий безопасности.

Организации, рассматривающие приобретение продукта SIEM, должны тщательно рассматривать весь предлагаемый им функционал и точно знать, для чего им нужна данная система, т.к. расходы на внедрение и развертывание SIEM, как правило, аналогичны другим крупным развертываниям инструментов безопасности с одним заметным исключением: интеграция. Служба SIEM не имеет значения, если она не может легко получать и анализировать данные журнала из самых разных источников журнала безопасности. Включение этого может потребовать обширной настройки SIEM или разработки настраиваемого кода для преобразования данных журнала источника в формат, который SIEM может понять и обработать.

Список литературы

1. Security Information and Event Management (SIEM) [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Security_Information_and_Event_Management_(SIEM)

2. What is log management and how to choose the right tools [Электронный ресурс]. – Режим доступа: https://www.csoonline.com/article/2126060/network-security/network-security-what-is-log-management-and-how-to-choose-the-right-tools.html

3. A comprehensive guide to SIEM products [Электронный ресурс]. – Режим доступа: https://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products

4. Top 10 SIEM Products [Электронный ресурс]. – Режим доступа: https://www.esecurityplanet.com/products/top-siem-products.html

5. Evaluation criteria for SIEM [Электронный ресурс]. – Режим доступа: https://www.csoonline.com/article/2124605/network-security/network-security-evaluation-criteria-for-siem.html

6. IBM QRadar vs. Splunk [Электронный ресурс]. – Режим доступа: https://www.itcentralstation.com/products/comparisons/ibm-qradar_vs_splunk

7. IBM QRadar vs. Splunk Enterprise [Электронный ресурс]. – Режим доступа: https://www.trustradius.com/compare-products/ibm-qradar-vs-splunk-enterprise