УДК 004.056.5-047.36

ИССЛЕДОВАНИЕ ОПТИМАЛЬНОГО МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ В SIEM СИСТЕМАХ СРЕДСТВАМИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕЙРАМБЕК М. М., БУРАМБАЕВА Н. А.

Евразийский Национальный Университет имени Л.Н. Гумилева
(г.Астана, Казахстан)

E-mail: moldirm09@mail.ru

Аннотация. С каждым годом увеличивается разнообразие и количество угроз, связанных с нарушением целостности и конфиденциальности информации. Безопасность современной информационной инфраструктуры имеет большое значение. Необходимо добавить новые компоненты в системы безопасности и расширить инфраструктуру информационной безопасности. Если в сети несколько систем информационной безопасности, то будет сложно ими управлять и понимать, что происходит в инфраструктуре. Следовательно, централизация системы управления журналами повышает безопасность и тем самым повышает степень защиты данных. Таким образом, системы управления информационной безопасностью и событиями безопасности (SIEM) были внедрены для решения проблем безопасности, путем централизованного управления журналами. В этой статье рассматриваются методы защиты информации в SIEM системах.

Abstract. Every year the variety and number of threats associated with violation of the integrity and confidentiality of information increases. The security of modern information infrastructure is of great importance. It is necessary to add new components to security systems and expand the information security infrastructure. If there are several information security systems in the network, it will be difficult to manage them and understand what is happening in the infrastructure. Therefore, centralizing the log management system improves security and thereby increases the degree of data protection. Therefore, Security Information and Event Management (SIEM) systems have been implemented to address security issues by centralized log management. This article discusses information security methods in SIEM systems.

Введение

В настоящее время обеспечение информационной безопасности является важной задачей для различных организации. Поэтому проблема мониторинга событий информационной безопасности, а также выявления и обработки возникающих инцидентов информационной безопасности становится все более актуальнее.

Постоянный рост информационных потоков не позволяет вручную отслеживать все тенденции и обеспечивать информационную безопасность. Корпоративная сеть постоянно находится под угрозой, если не настроены системы мониторинга активности в сети.

Системы информационной безопасности и управления событиями (SIEM) стали важным компонентом корпоративных сетей. Обычно они объединяют и сравнивают события на разных системах и платформах, а также проводят анализ на основе расширенных правил обнаружения угроз.

Система управления информационной безопасностью и событиями безопасности или SIEM – это метод управления безопасностью, который сочетает в себе функции: управление информацией о безопасности – Security Information Management (SIM) и управления событиями безопасности – Security Event Management (SEM) [1]. SIEM системы получили широкое распространение в качестве мощного инструмента для предотвращения, обнаружения кибератак и реагирования на них.

Основная часть

SIEM (Security information event management) – класс систем обеспечения информационной безопасности, появившихся в результате слияния SEM-систем и SIM-систем.

Основным функциональным отличием данных систем является то, что SEM-системы предназначены для анализа информации в режиме реального времени, а SIM-системы анализируют уже накопленную информацию [2].

Термин SIEM впервые был использован в статье опубликовано компанией Gartner, она была написана Марком Николетт и Амрит Уильямс, в которых они описали особенности продукта [3], [4]. Основной функцией SIEM - систем является анализ информации, поступающей от разных источников, таких как системы DLP, средства антивирусной защиты информации, межсетевые экраны, системы учета трафика, сканеры уязвимости и т.д. [5].

Информация о безопасности и управление событиями – это процедура анализа безопасности, которая позволяет получить общий обзор безопасности в организации. Инструменты SIEM собирают, анализируют, нормализуют и коррелируют все файлы, а также анализируют данные, поступающие с различных устройств, и предоставляют централизованный просмотр журналов.

Некоторые из преимуществ SIEM включают [6]:

– уменьшает время, необходимое для выявления угроз, уменьшая ущерб от этих угроз;

– обеспечивает целостную картину среды информационной безопасности оргнизации, которая упрощает сбор и анализ информации о безопасности для обеспечения безопасности системы – все данные доставляются в централизованное хранилище, где они хранятся и легко доступны;

– компании могут использовать данные или журналы для различных вариантов использования, включая программы безопасности, аудит и отчеты о соответствии, службы поддержки и устранение неполадок в сети;

– поддерживает большие объемы данных, чтобы организации могли продолжать масштабировать и увеличивать свои данные;

– обеспечивает обнаружение угроз и оповещения о безопасности;

– в случае серьезных нарушений безопасности может быть выполнен полноценный анализ.

Системы информации о безопасности и управления событиями были разработаны в ответ на это, чтобы помочь администраторам разрабатывать политики безопасности и управлять событиями из различных источников. Как правило, простая SIEM состоит из отдельных блоков (например, исходное устройство, сбор журналов, нормализация синтаксического анализа, механизм правил, хранилище журналов, мониторинг событий), которые могут работать независимо друг от друга, но без из совместной работы SIEM не будет функционировать должным образом [7]. На рисунке 1 изображены основные компоненты обычного SIEM решения.

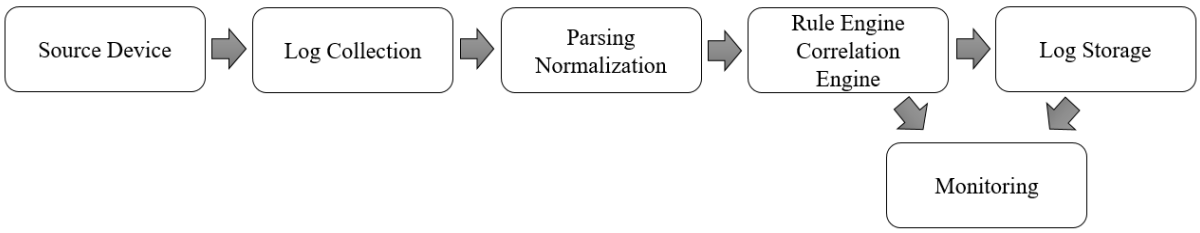

Рис. 1. Основные компоненты SIEM

Архитектура SIEM системы. SIEM система имеет архитектуру «агенты» - «хранилище данных» - «сервер приложений» [8].

Агенты выполняют сбор событий безопасности, обрабатывают их и фильтруют.

Собранная и отфильтрованная информация о событиях безопасности поступает в хранилище данных, где она хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений.

Сервер приложений реализует основные функции защиты информации. Он анализирует информацию, хранимую в хранилище данных, и преобразует ее для выработки предупреждений или управленческих решений по защите информации.

В SIEM системе можно выделить следующие три архитектурных уровня ее построения (рисунок 2) [9]: сбора данных, управления данными, анализа данных.

Рис. 2. Архитектура типовой SIEM-системмы

На первом уровне сбор данных осуществляется от источников различных типов, таких как файловые серверы, серверы баз данных, Windows-серверы, межсетевые экраны, рабочие станции, системы противодействия атакам, антивирусные программы и т.п.

На втором уровне осуществляется управление данными о событиях безопасности, которые хранятся в хранилище данных.

Данные , хранящиеся в хранилище данных, выдаются по запросам моделей анализа данных.

Результатами обработки информации в SIEM системе, получаемыми на третьем уровне, являются отчеты в предопределенной и произвольной форме, оперативная (on-line) корреляция данных о событиях, а также предупреждения, вырабатываемые в режиме on-line и передаваемые по электронной почте.

В настоящее время на рынке доступны разные средства защиты информации и управления событиями для защиты информации от взломов. В этой статье сравниваются два популярных SIEM инструмента: IBM QRadar и Splunk.

IBM QRadar может использоваться как единое решение “все в одном” и как опция виртуального устройства для сбора и обработки журналов сетевого потока, полных пакетных данных и точек на дюйм. QRadar включает в себя поддержку криминалистики инцидентов, улучшенную поддержку запросов, потоковые данные, анализ угроз, устройства хранения данных и данные об активах. Аутентичные события могут быть проанализированы с использованием существующих правил корреляции, обеспечивающих обзор журналов и событий. IBM Security предоставляет дополнительный компонент QRadar Risk Manager для мониторинга конфигурации сети и брандмауэра. IBM QRadar обладает ограниченными возможностями для развертывания расширенных вариантов использования и аналитики с ограниченной настройкой [10].

IBM QRadar SIEM способен поддерживать модульный подход к SIEM на основе устройств, разработанный для удовлетворения потребностей в оценке безопасности, таких как анализ сетевых потоков, регистрация событий и другие аналитичиские потребности организаций.

Основные характеристики IBM QRadar [11]:

– он собирает необходимую информацию из локальных и облачных источников;

– он объединяет взаимосвязанные действия для определения приоритетности инцидентов;
– IBM QRadar оснащен гибкой архитектурой, которую легко развернуть локально или в облаке;
– встроенная аналитика поможет эффективно выявлять угрозы;
– масштабируемая и самоуправляемая база данных.

Продукты Splunk для предприятий и облаков, поддерживаемые языком обработки поиска Splunk., облегчают поиск, оповещение, корреляцию в реальном времени и виртуализацию. Может быть заблокирован как программное обеспечение, в общедоступном или частном облаке или как программное обеспечение как услуга (SaaS), а лицензия основана на индексированном объеме. Splunk предоставляет гибкую аналитическую панель мониторинга, которая улучшает возможности виртуализации журналов. Мощная виртуализация Splunk, а также поведенческая прогностическая и статистическая аналитика помогают обнаруживать многочисленные данные об угрозах из коммерческих и открытыз источников [12].

Splunk извлекает скрытую информацию из машинных данныз или других форм больших данных и предупреждает организацию, если какие-либо подозрительнеы действия пытаются украсть данные. Splunk способен считывать любые данные. После завершения чтения данных позволяет выполнять посик, помечать, создавать отчеты и панели мониторинга на основе этих данных.

Особенности Splunk [13]:
– поиск, сбор и индексирование днных;
– анализ и визуализация;
– автоматическое обнаружение вредоносных действий в сетях;
– мониторинг в режиме реального времени;
– пользовательский интерфейс клиента;
– достаточно гибкий, чтобы удовлетворить любые организационные потребности.

Таблица 1. Сравнительная таблица QRadar и Splunk

Параметры	QRadar	Splunk
Реализация и использования	выигрывает в простате внедрения	выигрывает в простате использования
Совместимость	лучше работает с инструментами IBM	хорошо работает с компонентами внутри системы
Сравнение облачных и локальных	облако и локальное аппаратное обеспечение, выигрывает в локальной среде	программное обеспечение и облако, выигрывает в облаке
Сравнение интеграции	хорошо интегрируется со многими инструментами безопасности, которые входят в состав QRadar, возможности интеграции за пределами мира IBM ограничены	способность интегрировать потоки данных из огромного оличества источников, поддерживает широкий спектр форматов данных
Сравнение аналитики и поиска	выигрывает от долгосрочного лидерства IBM в области искусственного интеллекта	предлагает множество функций визуализации и анализа в реальном времени

Цены	основан на количестве событий в секунду. Локальное оборудование стоит от 10 400 долларов; облако начинается с 800 долларов в месяц	зависит от использования данных в день, независимо от количества пользователей. Для 10 ГБ в день, 24 900 долларов в месяц для неограниченного количества пользователей

QRadar и Splunk – оба считаются лидерами, предназначенный для решения множества задач, связанных с безопасностью и мониторингом производительности.

Заключение

Современный мир во многом зависит от информации. Защита информации представляет собой непрерывный целенаправленный процесс, продолжающийся на протяжении всего жизненного цикла информационной системы. Система управления информацией и событиями безопасности является важным подходом к защите данных организации. Современные инструменты SIEM включают в себя большие данные и продвинутые уровни интеграции аналитики, что помогает специалистам по безопасности эффективно проводить оценку. В этой статье проводится сравнительный анализ между QRadar и Splunk. В конце концов, все сводится к потребностям. Те, кто хочет получить всеобъемлющую платформу безопасности и управления ИТ, найдут Splunk ближе к своим потребностям. QRadar тоже выигрывает на многих фронтах, а также предлагает множество других преимуществ в области безопасности.

Список использованных источников

1. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.1 / С.В. Запечинков. - М.: ГЛТ, 2006. - 536 с.
2. Алексей Дрозд, Обзор SIEM-систем. SearchInform [Электронный ресурс]. – URL: http://www.antimalware.ru/analytics/Technology_ Analysis/Overview_SECURITY_systems_global_and_Russian_market (дата обращения: 27.04.2016).
3. L. Johnson, Security Controls Evaluation, Testing, and Assessment Handbook. Syngress, 2015.
4. K. Detken, D. Scheuermann, and B. Hellmann, “Using extensible metadata definitions to create a vendor-independent SIEM system,” in International Conference in Swarm Intelligence, 2015, pp. 439–453.
5. SIEM-системы. Инфобезпека [Электронный ресурс]. – URL: http://www.infobezpeka.com/publications/SIEM_osobennosti_siem (дата обращения: 27.04.2016).
6. Максим Гарусев. «Системы корреляции событий: революция или тэволюция?». Адрес сайта: http://www.setevoi.ru/cgi-bin/text.pl/magazines/2003/7/30
7. Miller, D.; Harris, S.; Harper, A.; Van Dyke, S.; Blask, C. Security Information and Event Management (SIEM) Implementation; Mc Graw Hill: New York, NY, USA, 2010.
8. Miller D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch. Security Information and Event Management (SIEM) Implementation. McGraw–Hill Companies. 2011. 430 p.
9. Stevens M. Security Information and Event Management (SIEM). Presentation // TheNEbraska CERT Conference, August 9–11, 2005. http://www.certconf.org/presentations/2005/files/WC4.pdf
10. WhitePaper, “IBM QRadar security intelligence platform,” [Online] Available http://www-03.ibm.com/software/products/en/qradar.
11. https://mindmajix.com/ibm-qradar-tutorial
12. Techincal Paper, “Using splunk software as a SIEM,” [Online]. Available: https://www.splunk.com/pdfs/technical-briefs/splunk-as-a siem-tech-brief.pdf.
13. https://mindmajix.com/overview-of-splunk-architecture