SIEM СИСТЕМА - УНИВЕРСАЛЬНЫЙ ИНСТРУМЕНТ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Быков А.А.

Быков Андрей Андреевич – студент магистратуры,
кафедра защищенных систем связи, факультет инфокоммуникационных сетей и систем,
Санкт-Петербургский государственный университет телекоммуникаций им. профессора М.А. Бонч-Бруевича,
инженер технической поддержки ключевых клиентов,
ПАО «Мегафон», г. Санкт-Петербург

***Аннотация**: в эпоху развития новейших технологий информация стала для нас самой дорогой и, несомненно, неотъемлемой частью нашей жизни. «Кто владеет информацией, тот владеет миром» — так говорил Ротшильд Н.М. Данную цитату можно применить и к компаниям, которые тщательно контролируют весь поток информации, который проходит на предприятии. У каждой, без исключения, компании есть своя конфиденциальная информация, распространения которой она бы не пожелала. И защита такой информации — обязательная мера, которую должны соблюдать все без исключения.*
***Ключевые слова:** SIEM, безопасность, информация, утечка, система, данные, угрозы, управление, контроль, инцидент.*

Как только начали появляться первые средства защиты информации, встали многочисленные вопросы – как нам узнать, что эти средства информационной безопасности (далее – ИБ) действительно работают и приносят необходимую защиту? Как наиболее быстро реагировать на угрозы? Каким образом можно автоматизировать все процессы ведения журналов событий нарушения безопасности, которые при ручном прочтении займут неисчисляемое количество времени, т.к. каждому ответственному сотруднику придется открывать различные приложения, консоли и только потом читать эти журналы?

К утечке информации может привести что угодно: но, в первую очередь, ничто так не вредит безопасности компании, как человеческий фактор. Для того чтобы бороться с этой проблемой, были придуманы системы предотвращения утечки данных или так называемые DLP-системы, а также системы анализа и сбора информации SIEM.

Системы защиты данных появились и существуют уже довольно давно, они прогрессируют вместе с развитием современных технологий. И так как компаниям принципиально важно следить за тем, что делают сотрудники, интерес к таким системам возрастает с каждым днем. При организации такого вида контроля необходимо также понимать, что такие системы довольно часто вторгаются в личную, приватную жизнь сотрудников, поэтому многим соискателям приходится подписывать различные договоры о том, что их любая их деятельность на предприятии может быть тщательно отслеживаема в целях обеспечения безопасности. Бытует мнение, что сами по себе такие системы нелегитимны вовсе. Поэтому очень важно при внедрении этих систем иметь юридическую поддержку или необходимую юридическую базу.

С каждым днем в любой крупной развивающейся компании растет объем источников информации, от которых поступают данные, содержащие в себе сведения о текущей защищенности системы. В связи с этим становится сложно контролировать все происходящие процессы, связанные с информационной безопасностью. Если своевременно не предотвращать возникающие угрозы, то все попытки оградить критически важную информацию и активы компании от утечки сводятся на нет. Для улучшения эффективности работы службы безопасности компании на помощь приходят SIEM (Security Information and Event Management) системы.

Системы ИБ, включающие в себя мониторинг, корреляцию событий, связанных с каким-либо объектом, извещениями и выводом информации на конечные устройства под управлением администратора, называют Security event management, а системы, отвечающие за хранение, отчетность и анализ аккумулированных данных, - Security information management. Понятие SIEM включает в себя оба этих аспекта, объединяет их в единой системе и предоставляет централизованное управление обеими областями.

Задачи, которые ставятся перед SIEM системами [1]:

1. Обеспечение возможности анализа событий и расследования инцидентов администратором системы.
2. Обработка и корреляция событий по заданным правилам и политикам, установленным в системе.
3. Хранение журналов событий от различных источников (сетевых устройств, приложений, журналов ОС, средств защиты) и их консолидация.
4. Оповещение и инструментарий для управления и необходимой работы с инцидентами.

Благодаря своей логике, такая система, как SIEM, является уникальным и универсальным инструментом. Но для того чтобы она корректно работала и все поставленные задачи успешно

выполнялись — необходимы полезные источники, которые будут подавать на вход системы полезные данные для последующей обработки, и заданные, в соответствии с требованиями компании, правила корреляции.

Основными источниками SIEM систем являются: [2]

- Контроль доступа, аутентификация (привилегии пользователей, контроль доступа к информационным системам, мониторинг).
- Журналы событий серверов и АРМ (отказоустойчивость, контроль доступа, соблюдение норм ИБ компании).
- Активное сетевое оборудование (сетевой трафик, контроль изменений, аварийные Log-сообщения).
- IDS\IPS. (изменение конфигураций, сетевые атаки, доступ к устройствам).
- Антивирусная защита (работоспособность ПО и баз данных, изменение политик и конфигураций, выявление вредоносного ПО).
- Сканеры уязвимостей (информация о слабых местах ПО или сетевых устройств).
- GRC-системы (выявление рисков и наиболее критичных угроз, повышение приоритета инцидента).
- Другие системы ИБ и контроля, например, DLP.
- Системы инвентаризации (контроль активов компании).
- Системы учета трафика.

SIEM система состоит из несколько компонентов [2]:

- Клиентские агенты – они устанавливаются на инспектируемую информационную систему (агент - это резидентная программа (демон или сервис), которая собирает журналы событий на локальной машине и передает их на сервер);
- Коллекторы на агентах, они представляют собой модули или библиотеки для понимания того или иного журнала событий или системы;
- Серверы-коллекторы - служат для предварительного сбора событий от множества различных источников;
- Сервер-коррелятор - собирает информацию от коллекторов и агентов и обрабатывает её по правилам и алгоритмам, заданным в системе;
- Сервер хранилища и баз данных, необходимый для хранения всей полезной информации.

С помощью SIEM можно добиться почти абсолютной автоматизации процесса выявления угроз. При корректном внедрении такой системы подразделение ИБ переходит на абсолютно новый уровень предоставления сервиса. SIEM позволяет акцентировать внимание только на критических и действительно важных угрозах, работать не с событиями, а с инцидентами, своевременно выявлять аномалии и риски, предотвращать финансовые потери и повышать эффективность и безопасность работы компании в целом.

Список литературы

1. Хабрхабр. [SIEM: ответы на часто задаваемые вопросы]. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/post/172389/ (дата обращения:13.06.2017).
2. Securitylab. [Что такое SIEM?]. [Электронный ресурс]. Режим доступа: http://www.securitylab.ru/analytics/430777.php/ (дата обращения: 13.06.2017).