О тенденциях в области управления событиями ИБ (SIEM)

Тема Больших Данных сегодня находится на пике популярности. Основные вопросы, которые ставятся во главу угла, связаны не столько с хранением данных, сколько с проблемами нормирования и качественного анализа информации. Если речь идет о событиях безопасности, то к ним добавляются также вопросы сбора и консолидации данных

Именно сбор, агрегирование и анализ событий информационной безопасности — основные задачи решений класса SIEM. С момента своего появления решения класса SIEM активно развивались. Сегодня классическое SIEM-решение уже не может удовлетворить всех потребностей зрелой компании. Связано это, прежде всего, с изменением потребностей рынка ИБ и изменением характера и ландшафта угроз. Процессы защиты информации требуют новых механизмов и технологий, которые способны выявлять, предотвращать и разрешать все более и более сложные инциденты ИБ.

История понятия SIEM

Термин SIEM (Security Information and Event Management) был введен в 2005 году сотрудниками аналитического агентства Gartner (Mark Nicolet и Amrit Williams). В правильной трактовке SIEM — это комбинация понятий SIM (Security Information Management) и SEM (Security Event Management). Основные функции — мониторинг в реальном времени, корреляция событий, оповещение об инцидентах, долгосрочное хранение информации, периодическая отчетность и т. д.

Что умели делать SIEM

Впервые потребность в SIEM-решениях возникла в связи с возросшими объемами логов (событий) от разных устройств безопасности. Потребовалось решение, способное осуществлять централизованный сбор логов ИБ от разных источников, нормирование, корреляцию и оповещение об инцидентах. Под источником надо понимать любое устройство, способное генерировать и передавать информацию о событиях ИБ. Это и активное сетевое оборудование (маршрутизаторы, коммутаторы), и системы детектирования и предотвращения вторжений (IDS/IPS), системы межсетевого экранирования (Firewall), антивирусные решения, серверы, рабочие станции, мобильные устройства, сетевые принтеры и т. д. На первом этапе этого функционала было достаточно.

С каждым годом ИТ-инфраструктура компаний все больше усложнялась, вместе с ней росли потребности пользователей SIEM-систем в сторону лучшей визуализации, большей информативности и расширения источников данных.

В процессе усложнения инфраструктуры остро встал вопрос о необходимости обнаружения специализированных, или целевых, атак (Advanced Persistent Threat — APT). Злоумышленники стали прибегать к нетривиальным способам, зачастую задействуя ресурсы внутренних рабочих станций. Такие атаки «изнутри» невозможно поймать «периметральными» средствами защиты. Появилась потребность в анализе внутреннего трафика и выявлении пользователей, имеющих отношение к происходящим событиям.

Новые SIEM

Производители SIEM-решений оперативно отреагировали на возросшие потребности рынка, значительно расширив функционал SIEM-продуктов. Что же могут делать SIEM нового поколения?

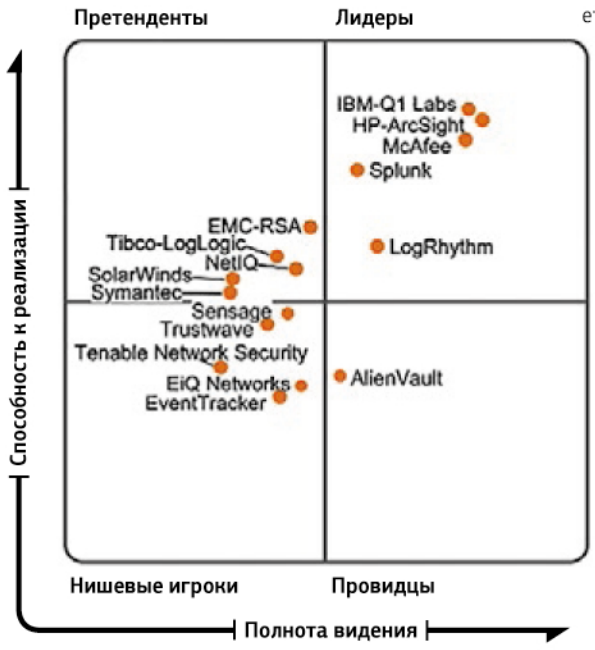
В первую очередь расширились источники сбора информации. Теперь это не только оконечные системы, генерирующие события информационной безопасности, но и непосредственно информация о сетевой активности и активности пользователей (для привязки к событиям), анализ активности виртуальной среды, анализ действий приложений, анализ изменений конфигураций устройств и т. д. Все это дало возможность добиваться большей точности при идентификации событий, нарушающих политику ИБ, а также снизило вероятность ложного срабатывания.

Помимо расширения источников данных, появились новые механизмы обнаружения нарушений. В SIEM начального уровня события собирались, анализировались и коррелировались, после чего на основе правил выявлялись подозрительные активности. В SIEM нового поколения дополнительно включен механизм анализа на основе метаданных и контекста. То есть учитывается географическое расположение IP-адресов, строится профиль злоумышленника, автоматически обнаруживаются новые ресурсы.

Наверное, самым революционным нововведением является независимый анализ трафика на предмет аномалий. Эта функция исторически никакого отношения к SIEM не имела, так как система SIEM была лишь сборщиком информации и базировалась на результатах работы инфраструктурных элементов. Сегодня SIEM анализирует трафик самостоятельно. Но это не значит, что системы обнаружения вторжений (IDS) можно заменить SIEM-продуктом. Во-первых, IDS анализирует трафик, проходящий через периметр, а SIEM видит внутренний трафик между корпоративными системами; во-вторых, SIEM анализирует те аспекты, которые только дополняют информацию от IDS.

И наконец, результатом этих изменений стала более удобная визуализация результатов работы SIEM. Теперь анализ событий можно смотреть по разным признакам: в географическом разрезе, по пользователям и другим новым характеристикам.

МАГИЧЕСКИЙ КВАДРАНТ GARTNER ДЛЯ РЫНКА SIEM



Главные игроки SIEM-рынка

На основании отчета Gartner, представленного в мае 2013 года, на сегодняшний день на рынке SIEM решений можно выделить пятерку лидеров:

- IBM-Q1 Labs,
- HP-ArcSight,
- McAfee-Nitro,
- Splunk,
- LogRythm.

Нужно признать, что первые три компании, приобретя лидеров рынка SIEM систем, пополнили свои продуктовые портфели очень хорошими решениями. Как видно из квадранта, позиции всех трех компаний очень близки, что и подтверждается практически одинаковым уровнем качества и функционала.

Из необычного можно отметить то, что бывшие лидеры в лице EMC-RSA и Symantec теряют позиции, но если посмотреть внимательнее, то они проигрывают на данный момент скорее стратегически, чем тактически.

Перспективы

Очевидно, что функционал существующих SIEM-решений достаточно обширен. Трудно себе представить, что в этой сфере можно придумать что-то новое. Однако процесс развития на этом не останавливается. SIEM-продукты постепенно перебираются туда, где исторически находились продукты класса GRC, по управлению, соответствию и риск-менеджменту. Сегодня SIEM аккумулирует в себе события от всех ИТ-систем и является своего рода «всевидящим оком» компании.

Кому нужны SIEM-решения

Современная инфраструктура любой компании, у которой часть внутренних сервисов базируется на ИТ, представлена несколькими категориями устройств: рабочие станции (ОС, антивирус), серверы (разные ОС, почтовая система, бухгалтерия и кадры), коммутаторы и маршрутизаторы, межсетевой экран и средство предотвращения вторжений, сетевые принтеры. Каждое из этих устройств генерирует тысячи событий в день. И если у администраторов стоит задача наблюдения за ИТ-инфраструктурой, то даже в небольшой технологичной компании такое решение жизненно необходимо. Внутренним заказчиком такого решения может быть ИБ-департамент (анализ угроз, события ИБ и т. д.), ИТ-департамент (централизованный сбор и хранение логов, мониторинг на основе данных логирования), руководство (консолидированные отчеты о событиях и угрозах, тренды, верхнеуровневая статистика).

В результате внедрения SIEM существенно упрощается расследование инцидентов, повышается прозрачность инфраструктуры и растет эффективность служб ИБ и ИТ.

— Джабраил Матиев, руководитель отдела информационной безопасности системного интегратора IBS Platformix