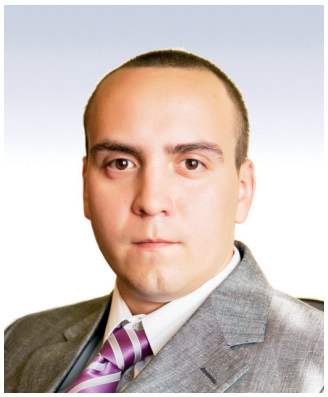
Практика внедрения и эксплуатации систем SIEM-/SIP-классов

В статье рассматриваются различные практические аспекты (синхронизация времени, ошибки при сборе событий, корреляция событий и др.) внедрения и эксплуатации систем SIEM-/SIP-классов (Security Information and Event Management – SIEM и Security Intelligence Platform – SIP).

Александр Кузнецов – CISM, руководитель ОБИС ООО «НТЦ «Вулкан».



Алексей Фёдоров – ведущий инженер ОБИС ООО «НТЦ «Вулкан».

Александр Черныхов – инженер ОБИС ООО «НТЦ «Вулкан».

Введение

В текущих условиях развития ИТ-инфраструктур, а также ландшафта угроз безопасности информации, системы классов Security Information and Event Management (SIEM) и Security Intelligence Platform (SIP) (далее – SIEM-системы), становятся неотъемлемой частью современных систем управления информационной безопасностью (СУИБ) предприятий.

При этом, к сожалению, проекты по внедрению данных систем, сопряженные с множеством организационных и технических аспектов, зачастую превращаются в «формальные» (включили и забыли) или «бесконечные» (тянутся из года в год без видимого результата). На наш взгляд, данная негативная практика связана с некорректным позиционированием самих технических решений, и, как следствие, обманутыми ожиданиями заказчиков, а также «нежеланием» интегратора полноценно понять потребности и особенности предприятия-заказчика.

В статье приведены несколько практических примеров, которые могли бы продемонстрировать, насколько комплексными и при этом интересными являются проекты, связанные с SIEM-системами, а также многогранными задачи, решаемые в их рамках.

RSA Security Analytics

Рассмотрим современное решение производства компании RSA, The Security Division of EMC, – «RSA Security Analytics» (RSA SA), впитавшее в себя лучшее от двух признанных на рынке продуктов – RSA enVision и RSA NetWitness.

RSA SA – это многокомпонентная система, включающая в себя:

– *Log Decoder* – сбор событий по протоколу Syslog, нормализация данных, хранение сырых (RAW) данных;
– *Log Collector* – сбор событий по протоколам (технологиям), отличным от Syslog;
– *Virtual Log Collector* – виртуальная машина, которая может быть использована для распределения нагрузки по сбору событий (частных случай LogCollector) с возможностью также сбора событий по протоколу Syslog;
– *Windows Legacy Collector* – сбор событий с версий ОС семейства Microsoft Windows 2000/2003, приложений NetApp (ОС Data ONTAP);
– *Decoder* – захват сетевых пакетов, нормализация данных, хранение сырых (RAW) данных;
– *Concentrator* – иерархически объединяет, хранит и индексирует нормализованные данные (мета-данные), полученные от Log Decoder;
– *Broker* – иерархически объединяет все данные от Concentrator'ов для обработки запросов;
– *Archiver* – обеспечивает долговременное хранение сырых (RAW) и нормализованных данных;
– *Event Stream Analysis (ESA)* – обеспечивает расширенный механизм корреляции мета-данных;
– *Malware* – обеспечивает анализ сетевого трафика на наличие вредоносного кода;
– *Warehouse* – кластер, обеспечивающий долговременное хранение большого объема данных с быстрым доступом к ним (технология BigData);

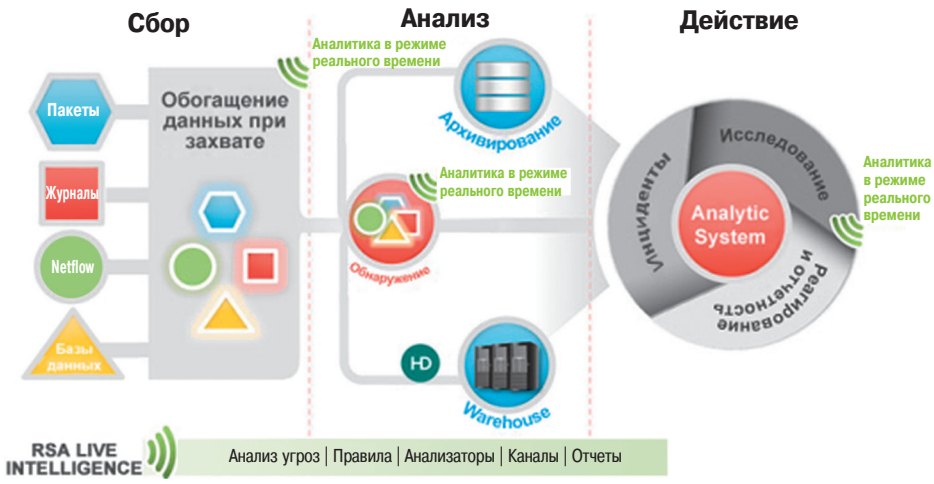


Рис. 1. Процесс работы системы RSA Security Analytics.

– *Analytic System* – обеспечивает интерфейс взаимодействия оператора и компонентов RSA SA.

Существует также специализированный репозиторий компании RSA (Content Management System, CSM) – «Live», поставляющий сведения об актуальных угрозах безопасности информации в виде новых шаблонов, правил и т.п.

Процесс работы SIEM-системы можно логически разделить на три части (рис. 1): сбор, анализ и действие. Совместно данные компоненты позволяют не просто собирать и хранить информацию о том, что происходит в ИТ-инфраструктуре предприятия, но также и в режиме реального времени автоматически анализировать ее, выделять наиболее важные события, формировать инциденты ИБ и соответствующую отчетность.

Сверим часы

Понимание того, когда произошло то или иное событие, является первостепенным в работе оператора SIEM-системы. В данном случае синхронизация времени на источниках событий и компонентах SIEM-системы – очень важный аспект, которому на практике при внедрениях далеко не всегда уделяется должное внимание.

В случае с RSA SA данная «халатность» может привести к отказу сбора событий при разнице во времени между источником событий и компонентом SIEM-системы, отвечающим за сбор более чем на 490 секунд (это меньше 10 минут). Плюс разное время на источнике событий и в SIEM-системе не даст актуальной временной картины происходящего в ИТ-инфраструктуре предприятия.

В процессе внедрения мы рекомендуем, чтобы источники событий и все компоненты RSA SA использовали один и тот же Network Time Protocol (NTP) сервер для синхронизации времени.

Еще одним «временным аспектом» является то, что RSA SA оперирует мировым временем в формате Zulu Time (UTC). Таким образом, если источник события оперирует временем в формате Zulu Time (UTC), при просмотре исходного события с источника событий (RAW-формат) время будет отображено без сдвигов с учетом вашего часового пояса. Как показывает практика, многих операторов это пугает, но в этом заложен определенный смысл. RSA SA изначально разрабатывалась как распределенная система уровня Enterprise, способная одновременно работать в разных часовых поясах. В данном случае использование времени UTC оправдано: ведь только так можно понять, когда же на самом деле началась какая-либо активность. На самом деле, этот же принцип используется в ОС Microsoft Windows – события в ней хранятся с использованием времени UTC, а при отображении в Event Viewer к UTC прибавляется часовой пояс, актуальный для текущих настроек ОС. Однако если мы откроем XML-вид события – там будет указано время UTC.

Следует также обратить внимание на то, что некоторые источники событий при передаче событий не указывают время (например, Squid в определенной конфигурации).

Но оператору нужно значение времени для работы с событиями. В связи с этим в RSA SA существует два поля:

– *time* – время, когда событие поступило в RSA SA (UTC + часовой пояс, указанный в ОС RSA SA);

– *event.time* – время, когда событие произошло на источнике события (UTC – в случае, если источник события оперирует временем в формате Zulu Time).

В связи с этим возникает ряд особенностей, которые необходимо учитывать:

– при работе с событиями в разделе *Investigate* значение в поле *time* учитывает часовой пояс, указанный именно в разделе *Investigate*, а не в ОС RSA SA;

– при формировании отчетов будет использоваться *time*, т.е. отчет, сформированный за период времени с 12:00 до 15:00 при установленном часовом поясе UTC+3 будет иметь временной диапазон в отображаемом поле *event.time*: с 09:00 до 12:00.

На сегодняшний день существует еще не вошедшее в официальный релиз тестируемое обновление, которое исключает данные особенности, если они для вас актуальны. Получить данное обновление можно, обратившись в техническую поддержку компании RSA.

«Это потеря потерь!» – некоторые ошибки при сборе событий

Будучи уверенным, что событие произошло в указанный момент SIEM-системы, оператор начинает экспертно-аналитическую работу, и здесь необходимо не потерять важные данные.

В отличие от конкурентных решений, RSA SA не «обрезает» события на входе. Если событие слишком большое (больше указанного в настройках SIEM-системы размера), то оно может быть разбито на несколько более мелких и «сшито» в SIEM-системе.

Но есть факторы, связанные с потерей событий и лежащие вне зоны ответственности RSA SA. Например, при сборе событий с ОС Microsoft Windows, как правило, причиной служит известная «ошибка», присутствующая в версиях ОС Microsoft Windows Server 2008 R2 и 2012 R2 в событии *Event ID: 4661* из журнала *Security*.

Проблема заключается в неправильном значении поля *Privileges*. Для исправления данной ошибки необходимо установить пакет исправлений *KB2956014* на соответствующий источник события.

Есть еще одна причина, когда события с ОС Microsoft Windows могут приходить «обрезанными». Чаще всего это проявляется на англоязычных версиях ОС (рис. 2). В данном случае необходимо вручную указать в RSA SA локализацию, используемую данным источником событий (например, en-US), и проблема будет решена.

На практике достаточно часто происходит неполный разбор событий – от непопулярных на Западе источников событий, заявленных в официальной поддержке компанией RSA. Например, широко известные в России и странах СНГ средства антивирусной защиты Kaspersky. По факту обновление парсеров таких продуктов для SIEM-системы не успевает за обновлением самого программного продукта, в результате чего SIEM-системы не могут нормализовать новые события или старые события в новом формате.

Есть несколько путей выхода из сложившейся ситуации.

Во-первых, направить сообщение производителю SIEM-системы с просьбой добавить новые события в официально поддерживаемый парсер. Нередко этот процесс растягивается во времени, и изменения происходят только при выпуске очередного массового обновления, что может быть неприемлемо для предприятия-заказчика.

Во-вторых, можно освоить механизм формирования новых парсеров или редактирования уже существующих. Мы рекомендуем именно данный вариант.

Наконец, можно привести новые сообщения о событиях и изменившиеся старые к виду, используемому в официально поддерживаемом парсере. На наш взгляд, это самый сложный и самый затратный путь, который может повлечь за собой, например, создание вручную новых таблиц и представлений в БД продукта.

«Вокруг шум», или «Спасибо за тюнинг!»

С первых дней работа оператора абсолютно любой SIEM-системы будет сопряжена с минимизацией «шума», т.е. сокращения количества малоинформативных событий.

Для оптимизации работы RSA SA и любых других SIEM-систем рекомендуется осуществлять «тюнинг» сбора событий. RSA SA имеет очень гибкие механизмы по «тюнингу» и позволяет осуществлять его на компонентах Log Collector и Log Decoder/Decoder.

Например, на компоненте Log Collector мы можем исключить передачу в SIEM-систему событий с идентификатором – *System^(10120)**). Данное событие будет записываться в журнал *System* на всех ис-

*) Reference ID 10120 содержит текст: «The WinRM service has received an unsecure HTTP connection from SA_IP. This is not a secure configuration. User Action Set Allow Unencrypted to False in WinRM configuration to ensure packets are encrypted on the wire».

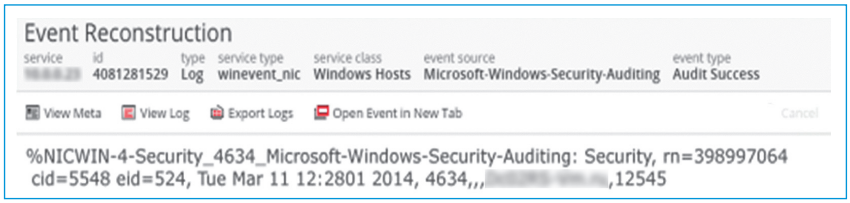


Рис. 2. Неполное событие из журнала Security, ОС Windows Server 2008 R2.

точниках событий типа ОС Microsoft Windows при каждом обращении RSA SA к данному источнику событий по протоколу HTTP и порту 5985. При этом оператор SIEM-системы понимает, что данное действие является санкционированным, а событие не несет в себе «полезной нагрузки» и его можно исключить из рассмотрения, тем самым разгрузив себя и SIEM-систему.

Механизмы RSA SA на компоненте Log Decoder/Decoder позволяют нам осуществить еще более глубокую фильтрацию, тем самым снизив нагрузку на компонент Concentrator, передавая на нормализацию только те события, которые подпадают под нужные нам шаблоны. Например, на компоненте Log Decoder/Decoder с помощью Application Rule можно исключить события, отвечающие за вход и выход пользователей в/из ОС Microsoft Windows для учетных записей, содержащих на конце «$», т.е. доверенных учетных записей компьютеров. Таким образом, в метаполе *username* мы будем видеть только реальные учетные записи, которые использовались для входа/выхода пользователей, что сильно упростит работу оператора SIEM-системы. При этом важные данные не будут потеряны.

«Тюнинг» также способствует увеличению срока хранения данных в RSA SA.

Отметим, что процесс «тюнинга» сбора событий может и должен происходить на протяжении всего жизненного цикла SIEM-системы, но он подразумевает наличие соответствующих знаний об особенностях работы подключенных источников событий.

В рамках проектной деятельности мы сталкиваемся с тем, что многие рассчитывают на то, что SIEM-система должна самостоятельно отфильтровать «ненужные» события. Безусловно, RSA SA обладает определенными предустановленными шаблонами правил, которые позволяют выделить то, на что стоит обратить внимание в первую очередь с точки зрения компании-производителя – RSA. Как компания-интегратор мы, предлагаем свои «черные списки» событий, которые можно «оттюнинговать». Но решения «out of the box» не всегда могут отвечать требованиям конкретного предприятия-заказчика. SIEM-система предназначена для автоматизации и оптимизации работы оператора по выявлению инцидентов ИБ, но не должна делать работу за него. В связи с этим наличие понимания, какие события и с каких источников событий поступают в SIEM-систему, а также какую информацию «несут» – является краеугольным камнем для сотрудников предприятия-заказчика. Это «понимание» и его реализация в рамках обслуживания не только SIEM-системы, но и всей инфраструктуры Управления событиями позволят получить операторам SIEM-системы действительно значимый и актуальный результат.

Коррелировали, коррелировали и накоррелировали

Как было сказано выше, экспертно-аналитическая работа оператора «жаждет» получить на вход уже предварительно обработанные и отранжированные сведения в виде «кандидатов на инциденты ИБ». Практика показывает, что формирование списка «кандидатов» только на базе данных из журналов событий недостаточно. Решение RSA SA является модульным, способным сочетать в себе как компоненты для решения задач в части обработки журналов событий, так и в части сетевых пакетов. Максимальный эффект достигается при комбинировании данных подходов и использовании специализированного корреляционного «движка» – модуля Event Stream Analysis (ESA).

Данный модуль необходим, когда заходит речь о так называемой «сложной» корреляции: построении последовательностей действий на базе событий и/или зависимостей событий и времени. ESA использует Event Processing Language (EPL) от Esper, способный эффективно использовать память, SQL-запросы и работать с минимальной задержкой в режиме, близком к реальному времени. Архитектура RSA SA позволяет использовать всего один модуль ESA в независимости от масштаба инсталляции SIEM-системы. Дополнительно на этом модуле располагается БД для встроенного функционала *Управления инцидентами*. Таким образом, наличие в инсталляции SIEM-системы модуля ESA решает проблему как с высокоэффективной корреляцией данных, так и с наличием механизмов для обработки и управления инцидентами ИБ.

Выше SIEM могут быть только GRC

Все больше и больше ИБ-специалистов приходят к тому, что недостаточно просто отслеживать события, происходящие в ИТ-инфраструктуре предприятия: необходимо иметь инструменты для создания и полномасштабного расследования сформированных инцидентов ИБ. Казалось бы, модуль ESA со встроенным функционалом по *Управлению инцидентами* должны решать данную проблему, но это только базовый функционал, который не всегда удовлетворяет потребности предприятий с высоким уровнем зрелости.

В этом случае «на арену выходят» решения класса Governance, Risk and Compliance (GRC).

В рамках настоящей статьи будет рассматриваться платформенное GRC-решение производства компании RSA, The Security Division of EMC, – «RSA Archer».

Существуют два пути интеграции RSA SA и RSA Archer:

– *«облегченный вариант»* предполагает использование продукта «RSA Security Operation Management (SecOps)», который является специализированным решением (solution) для RSA Archer, позволяющим объединять все инциденты ИБ в одной веб-консоли;

– *«полномасштабный вариант»* рассчитан на полноценные инсталляции RSA Archer, включающие в свой состав специализированное решение (solution) «Incident Management».

Во втором случае для платформы в качестве коннектора выступает бесплатное приложение «RSA Connector Framework», которое принимает информацию от RSA SA и отправляет ее напрямую в решение «Incident Management».

Технически процесс формирования инцидентов ИБ на основе оповещений (Alert), поступающих от RSA SA, выглядит следующим образом:

– в ИТ-инфраструктуре предприятия происходит событие (ряд событий), указывающее на возможный инцидент ИБ;

– RSA SA получает данное событие и в соответствии с используемыми правилами создает оповещение;

– оповещение автоматически направляется ответственному лицу по e-mail и на сервер с ПО «RSA Connector Framework», которое автоматически создает инцидент ИБ в solution «Incident Management» либо дописывает новую информацию в уже существующий и «привязывает» к нему все данные, связанные с событием, вызвавшим данный инцидент;

– все заинтересованные лица получают возможность работы с данными по инциденту ИБ с использованием единой веб-консоли.

Данный подход позволяет предприятию снизить время на расследование инцидентов ИБ, создать единую информационную среду для упрощенной коммуникации между заинтересованными лицами предприятия.

Для обогащения инцидентов также может использоваться компонент «RSA Archer Vulnerability Manager», который аккумулирует информацию об активах сети предприятия на основе данных, полученных от сканеров безопасности. Таким образом, у оператора появляется информация не только об инциденте ИБ, кото-

рый произошел в ИТ-инфраструктуре, но и дополнительная информация об атакуемом активе, его уязвимостях и значимости для предприятия в целом.

Нестандартный функционал

Несмотря на то, что SIEM- и GRC-системы в связке представляют мощный инструментарий по обнаружению и расследованию инцидентов ИБ, существуют предприятия, которые не просто хотят решать «стандартные SIEM-задачи», но и реализовать нестандартный функционал, например, использовать SIEM-систему как Antifraud. Одной из таких задач применения RSA SA, стал поиск подозрительных транзакций в банковской системе. Данная задача включала в себя анализ поведенческой активности пользователей, что нехарактерно для SIEM-систем. Но, несмотря на это, при четком целеполагании, а также при добросовестном использовании стандартных инструментов удалось достичь положительного результата.

Конкретная задача состояла в выявлении «вывода» больших сумм с технических счетов банка на никогда ранее не используемые счета за пределами банка.

Для решения данной задачи в БД платежей была создана отдельная таблица, куда вошли следующие поля:

- счет отправителя;
- счет получателя;
- сумма.

Также были созданы списки технических банковских счетов и когда-либо использовавшихся в данном контексте счетов за пределами банка, обновляемые автоматически.

Данные из таблиц, а также счета, представленные в созданных списках, использовались для построения соответствующего правила корреляции. При тестировании данного правила SIEM-система смогла выявить все подозрительные транзакции, подпадающие под соответствующие условия.

Данное правило может быть усовершенствовано набором дополнительных условий, таких как: «черные» и «белые» списки счетов и пользователей, время, в которое происходит событие, количество событий, которые позволяют уменьшить число ложных срабатываний и количество затрачиваемого времени на расследование данных инцидентов.

Заключение

В заключение хотелось бы обратить внимание на то, что предприятиям-заказчикам нужно быть готовыми к тому, что каждый проект по внедрению SIEM-системы является уникальным, и «работа из коробки» в большинстве случаев не даст требуемого эффекта. В связи с этим вовлечение специалистов предприятия-заказчика является плановым и обязательным. Плюс к этому следует сразу же закладывать ресурсы (людские, временные и т.п.) на экспертно-аналитическую работу с данной системой, ее поддержание и развитие, а также на интеграцию с «выше-стоящими» системами (в случае их наличия) своими силами или силами внешних интеграторов.

Александр Кузнецов,
Алексей Фёдоров,
Александр Черныхов,
ООО «НТЦ «Вулкан»