SIEM-платформа RSA enVision

Изменения состояния ИТ-инфраструктуры, которые имеют значение для ее безопасности, управления или работоспособности, регистрируются в журналах событий. Их анализ — важный элемент повседневной деятельности по обеспечению ИБ.

В больших корпоративных сетях регистрация и обработка миллионов событий без применения специальных технологий практически невозможна. Это приводит к выпадению из контура управления ИБ важнейших источников информации об уровне защищенности ИТ-систем и сервисов.

Чтобы избежать подобной ситуации, необходимо применять современные технические решения, такие как SIEM-платформа RSA enVision.

Возможности системы

Реализуя функции управления событиями, SIEM-платформа RSA enVision предоставляет следующие возможности:

- безагентный сбор событий более чем от трехсот видов источников событий (приложений, ОС, СУБД, средств защиты информации, сетевых устройств);
- сбор событий от неподдерживаемых штатно («экзотических») источников;
- работу на потоках до нескольких сотен тысяч EPS;
- нормализацию информации о событиях с использованием специальной классификации (таксономии);
- фильтрацию и поиск событий по любым полям в их описании;
- обработку и корреляционный анализ событий;
- визуализацию информации о событиях, в том числе на интегрированных консолях (Dashboards);
- информирование персонала и реагирование на определенные события (цепочки событий);
- формирование многоуровневой отчетности;
- управление ИБ-инцидентами с помощью встроенных средств или передача данных во внешний ServiceDesk;
- централизованное долгосрочное хранение событий в неизменном виде.

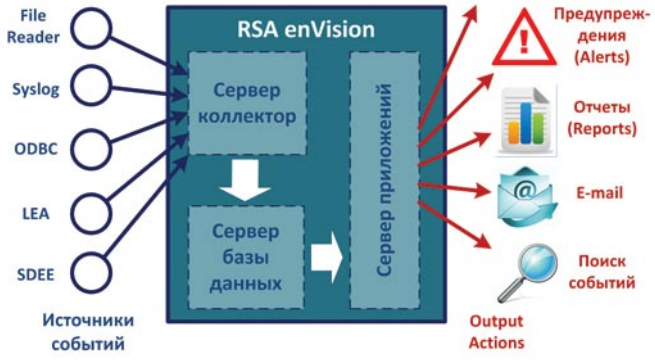
Архитектура и масштабирование

SIEM-платформа RSA enVision состоит из трех компонентов, которые могут быть объединены в одном устройстве (серия ES) либо разнесены по нескольким аппаратным комплексам (серия LS) в зависимости от масштаба контролируемой ИТ-инфраструктуры.

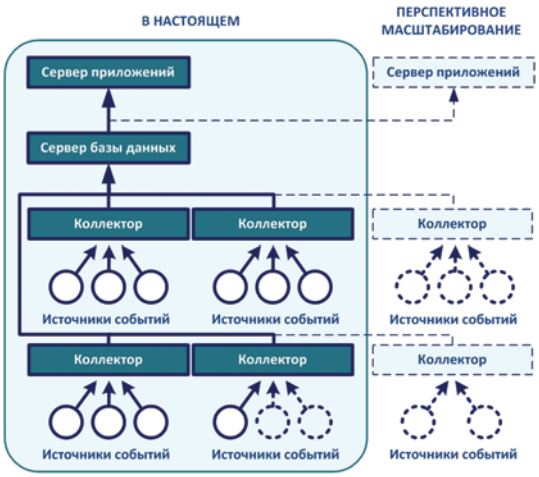
Коллектор взаимодействует с источниками, получает информацию о событиях и передает ее другим компонентам SIEM-платформы для дальнейшей обработки.

Сервер базы данных обеспечивает хранение полученной информации в неизменном (RAW-формат) либо в нормализованном виде. Сервер базы данных имеет возможность подключения внешних систем хранения.

Сервер приложений предоставляет интерфейс пользователя для анализа полученной информации в режиме реального времени посредством ретроспективных выборок.



Линейка продуктов RSA enVision позволяет системе расти вместе с организацией как горизонтально, так и вертикально. Возможность развертывания решения в виртуальной инфраструктуре VMware позволяет заказчикам применять современные подходы по оптимизации ИТ-ресурсов.



НТЦ ВУЛКАН

RSA
The Security Division of EMC

Целевая аудитория

Круг заказчиков SIEM-платформы RSA enVision включает крупные организации различного профиля деятельности, в которых под управлением департамента ИТ (ИБ) находится масштабная гетерогенная ИТ-инфраструктура, интенсивно задействованная в бизнес- и производственных процессах.

Потребность использования SIEM-платформы RSA enVision возникает в тех случаях, когда:

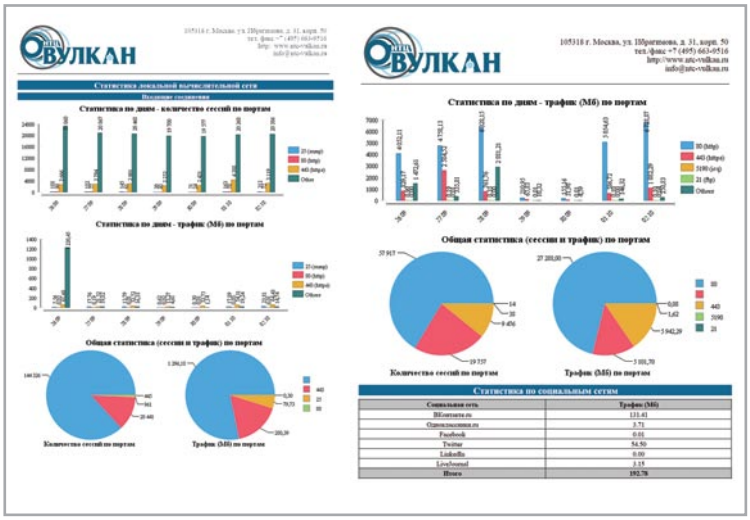
- необходимо обеспечить единую точку сбора, хранения и анализа информации о событиях ИБ, генерируемых ИТ-инфраструктурой и средствами защиты информации;
- нужна фактура для расследования ИБ-инцидентов, при этом требуется обеспечить глубокую ретроспективу «логов» (годы, месяцы);
- необходимо оперативно выявлять ИБ-инциденты по данным корреляционного анализа событий;
- требуется автоматизировать процесс оценки соответствия требованиям (Compliance);
- в компании создается центр управления ИБ (SOC);
- в компании внедряются процессы управления ИТ на основе методологий ITSM.

Ценность для бизнеса, ИТ и ИБ

Построение системы управления информационной безопасностью и событиями на базе SIEM-платформы RSA enVision обеспечивает:

- централизованную базу с информацией о событиях от всех источников в ИТ-инфраструктуре («слепок» информационной среды);
- возможность расширенного поиска и анализа информации, в том числе по параметрам специальной классификации (таксономии);
- доступную визуализацию оперативной информации об уровне защищенности сети;
- уменьшение времени реакции персонала на ИБ-инциденты и времени прерывания ИТ-услуг;
- уменьшение затрат на рутинные операции обслуживания ИТ-инфраструктуры за счет автоматической реакции на события (цепочки событий) путем выполнения заданного командного сценария (скрипта) на источнике;

- наличие материалов (доказательной базы) для расследования ИБ-инцидентов;
- повышение прозрачности работы ИТ-инфраструктуры в разрезе ИБ;
- автоматизацию процедур Compliance;
- оптимизацию работы ИБ-персонала за счет аккумулирования сведений, имеющих практическую ценность, в рамках одной системы («единое окно»);
- наличие статистических данных для анализа рисков ИБ;
- регулярную многоуровневую отчетность с возможностью дальнейшей обработки в системах BI и GRC.



Профессиональный сервис

НТЦ «Вулкан», авторизованный партнер RSA, The Security Division of EMC, предлагает:

- демонстрацию возможностей SIEM-платформы RSA enVision и проведение пилотных проектов;
- разработку инженерно-технических решений по применению RSA enVision;
- разработку технической и эксплуатационной документации на русском языке;
- подбор (sizing), поставку и внедрение RSA enVision;
- интеграцию с другими системами (ServiceDesk, eGRC) и средствами анализа защищенности;
- организацию сертификации по требованиям безопасности информации экземпляров продукции;
- разработку кастомизированных отчетов, в том числе уровня BI;
- разработку профилей для проведения оценок соответствия (Compliance) российским нормативно-методическим документам в области защиты конфиденциальной информации (ПДн, СТО БР ИББС, НПС, КТ);
- организацию на базе RSA enVision систем управления ИБ-инцидентами;
- создание на базе RSA enVision центров оперативного управления ИБ (SOC);
- техническую поддержку на русском языке, в том числе выездную.

НТЦ «Вулкан»
105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
info@ntc-vulkan.ru
www.ntc-vulkan.ru