Создание систем управления событиями и инцидентами ИБ (SIEM)

Александр Кузнецов, *руководитель отдела безопасности информационных систем НТЦ "Вулкан"*
Дарья Муравьева, *специалист отдела безопасности информационных систем НТЦ "Вулкан"*

Сегодня уже мало кто недооценивает важность регистрируемой в информационных системах (ИС) информации об обращении к данным, их создании, модернизации, удалении… События, порождаемые процессами и пользователями информационных систем, в том числе имеющие отношение к вопросам информационной безопасности (ИБ), требуют учета и анализа. Они же служат основой для выявления инцидентов ИБ, а также прогнозирования и обнаружения сбоев в работе IT-инфраструктуры.

Но подобных событий происходит тысячи и сотни тысяч в день! Обработать и проанализировать такое количество информации вручную физически невозможно. На помощь специалистам приходят технические решения класса Security Information and Event Management (SIEM). Но "голыми" технологиями решить данную задачу нельзя. О том, как создать полноценную систему управления событиями и инцидентами ИБ, мы и поговорим далее.

Система управления событиями

Система управления событиями – это комплекс мер, направленных на регистрацию, хранение, обработку, анализ событий и реагирование на них. Поскольку создание такой системы сложно как организационно, так и технологически, частой практикой является привлечение к решению данной задачи компании-интегратора. Тем не менее вне зависимости от того, чьими силами реализуется проект, есть несколько общих элементов, из которых складывается мозаика. Давайте посмотрим на процесс создания системы управления событиями "с высоты птичьего полета".

Конечно же, во главу угла ставятся задачи, которые должна решать система. С учетом этих задач решается вопрос – события с каких элементов IT-инфраструктуры могут дать необходимые исходные данные. Таким образом определяются типы и количество источников событий (Event Sources). При этом в качестве источника выступает не абстрактный компьютер или устройство, а более конкретные объекты: ОС, приложения, СУБД, средства защиты информации и т.п. То есть, например, на одном сервере фактически может находиться N источников событий.

После этого необходимо разобраться, какие именно события из регистрируемых на источнике представляют интерес. Здесь начинается работа по настройке политик аудита и ведения журналов регистрации событий на источниках (Log Management), так как если событие не сгенерировано, то оно не может быть обработано.

Чтобы количественно оценить ожидаемый поток событий, измеряемый в EPS (Events per Second), можно использовать различного рода калькуляторы, предлагаемые производителями SIEM-решений: HP (продукт ArcSight), EMC (RSA enVision), IBM (QRadar) и др. При расчете следует учитывать не только средние показатели, но и данные в период пиковых нагрузок, так как некоторые SIEM-решения имеют жесткое ограничение по количеству EPS.

SIEM-решения

После определения перечня источников и значений EPS можно переходить к выбору SIEM-продукта. На сегодняшний день на рынке представлено свыше 80 подобных решений. Для выбора наиболее подходящего целесообразно ориентироваться на следующие ключевые критерии:

- реализация – программная или программно-аппаратная, плюс возможность виртуализации;
- перечень поддерживаемых штатно источников событий;
- показатели EPS;
- способы получения событий (Syslog, ODBC, SNMP, FTP и т.д.);
- возможность подключения внешних систем хранения данных.

Отдельно стоит сказать об архитектуре SIEM-решений. Это могут быть интегрированные устройства (all-in-one) либо двух-трехкомпонентные комплексы. Распределенная архитектура чаще всего предполагает большую производительность и лучшие возможности по масштабированию, а также позволяет развернуть SIEM-решение в IT-инфраструктурах с несколькими площадками.

При осознанном выборе SIEM-продукта важным этапом принятия решения будет проведение пилотного проекта. Предварительное тестирование позволит в течение нескольких недель поработать с SIEM-системой и увидеть ее возможности вживую.

Опуская вопросы технического проектирования и разработки документации на SIEM, отметим, что это является очень важным этапом, без которого процедура развертывания решения может быть сопряжена с затруднениями и техническими проблемами, вызванными отсутствием должной проектной проработки.

Перейдем к внедрению системы. После установки и инициализации компонентов SIEM-решения производится подключение источников. Здесь существуют два основных варианта:

Под событием понимается изменение состояния, которое имеет значение для безопасности, управления или работоспособности ИС или ее компонента, а также зарегистрированная в журнале информация о данном событии.

- источник сам инициирует передачу событий (например, отправляет по syslog-протоколу);
- события с источника надо забирать.

С первым вариантом все достаточно просто: на источнике указывается IP-адрес устройства, осуществляющего сбор событий (коллектора), и события "текут" в нужную сторону. Второй вариант включает агентный или безагентный сбор информации, причем в некоторых SIEM-системах для части источников доступны оба способа. Агентный способ предполагает использование специальной программы-агента, безагентный – спецнастройки источника событий, такие как создание дополнительных учетных записей, разрешение удаленного доступа и/или использования дополнительных протоколов. Если есть выбор, какой способ подключения использовать, необходимо оценить все плюсы и минусы и по возможности опробовать оба варианта в "пилоте".

С учетом того что информация о состоянии различных ИС может быть интересна разным специалистам с различным статусом и уровнем доступа к корпоративной информации, необходимо провести настройку прав доступа к SIEM-системе. В большинстве SIEM-решений реализован ролевой принцип доступа, поддерживаются доменная идентификация и двухфакторная аутентификация.

Когда все источники подключены и роли заданы, выполняется настройка правил обработки событий, отчетов и уведомлений. Пожалуй, это наиболее кропотливая часть внедрения. Работа с событиями и результатами их анализа в большинстве SIEM-продуктов осуществляется с использованием отчетов (Reports) и запросов (Query). Здесь все зависит от возможностей конкретного SIEM-решения и потребностей заказчика.

Наконец, необходимо отметить важную вещь. Управление событиями включает в себя и реакцию на них. Но об этом очень часто забывают, получая на базе SIEM-системы, по сути, всего лишь… "продвинутый" ИБ-мониторинг.

Как правило, SIEM-решения предлагают следующие варианты реакции на заданное событие (цепочку событий):

- "красная лампочка" на рабочей панели (Dashboard) администратора;
- отправка сообщений по электронной почте или SMS;
- выполнение заданного командного сценария (скрипта) на источнике;
- создание инцидента ИБ во встроенном или внешнем сервисе HelpDesk/ServiceDesk.

В реальной практике в качестве реакций на события используется сразу несколько перечисленных методов.

Управление инцидентами ИБ

Сегодня управление инцидентами – это не только рекомендации из области Best Practices, но и обязательные требования для большой группы организаций (например, для участников НПС или для банков, присоединившихся к СТО БР ИББС).

Стоит отметить, что необходимо разделять процессы управления событиями и управления инцидентами ИБ, а если смотреть шире, то и управления проблемами, так как данные процессы преследуют разные цели, но при этом взаимосвязаны между собой.

SIEM-решения позволяют автоматически формировать БД инцидентов и помогают автоматизировать следующие элементы процесса управления инцидентами ИБ:

- создание и регистрация инцидента;
- категоризация и назначение приоритета;
- локализация (требуется работа оператора);
- эскалация (автоматически или вручную);
- подготовка материалов для расследования (требуется работа оператора);
- закрытие инцидента.

Большинство SIEM-решений обладают широкими возможностями в данной области, а также поддерживают интеграцию с решениями класса Governance, Risk and Compliance (GRC). Ключевым моментом здесь является возможность добавления доказательств в виде событий к описанию инцидента ИБ, а также получение сведений о состоянии IT-инфраструктуры до и после возникновения инцидента, и все это в одном интерфейсе.

Однако не стоит ожидать от SIEM-решения участия в ликвидации последствий инцидента ИБ и/или восстановлении работоспособности ИС – полный цикл управления инцидентами ИБ только на базе SIEM реализовать не получится. Зато максимально обеспечить информационную поддержку этого процесса – легко.

Единое окно

Создание системы управления событиями и инцидентами ИБ позволяет организовать "единое окно", в котором в доступном виде предоставляется информация о защищенности и состоянии ИС. Учитывая наличие средств своевременного оповещения и реагирования, такая система становится незаменимым помощником ИБ/IT-специалистов.

Таким образом, грамотная и последовательная реализация проекта по созданию системы управления событиями – важный этап развития системы менеджмента ИБ, а долгосрочную практическую пользу применения технологий SIEM способны обеспечить правильная постановка задач, полный учет технических особенностей и, разумеется, внимание к деталям. ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru

Под инцидентом понимается незапланированное прерывание работы ИС или снижение показателей ее работы, а также зарегистрированная в БД инцидентов информация о нем.