MaxPatrol SIEM: 10% рынка за год

По результатам прошедшего 2015 г. решение MaxPatrol SIEM в течение первого года своего существования заняло более 10% российского рынка, объем продаж по итогам года составил около 180 млн руб., в 2016 году компания Positive Technologies планирует увеличить его до 400 млн руб., а в следующем году вывести продукт на европейский рынок. Сегодня MaxPatrol SIEM создают 80 разработчиков и инженеров по качеству. Уже завершено 26 проектов и находятся в работе еще 25 «пилотов». MaxPatrol SIEM используют российские Министерство обороны и Министерство транспорта, энергетическая компания «Россети», Департамент информационных технологий Москвы, Комитет по информатизации и связи Санкт-Петербурга. Об основных особенностях решения рассказывает Алексей Андреев – директор по разработке MaxPatrol SIEM.

Алексей Андреев – директор по разработке MaxPatrol SIEM, PositiveTechnologies.

SN. MaxPatrol SIEM 2.0 – это система мониторинга угроз или их предотвращения в реальном времени?

А.А. Да, это система мониторинга и выявления угроз в реальном времени. Вовремя выявленное начало атаки помогает нам предотвратить её. Ведь это не Firewall, который позволяет при определении зловредного трафика сразу же его заблокировать. Например, мы видим по логам системы документооборота, что идет брутфорс-атака с некоторых пользовательских сетей. В системе документооборота мы не можем заблокировать эти подсети ни функционально (такого механизма попросту нет), ни организационно (пользователи должны продолжать работать с системой), но вовремя выявленный инцидент даёт оператору ИБ время на определение и локализацию точной проблемы. Скажем, наличия вредоносного ПО на ряде рабочих станций.

SN. Есть ли возможность автоматического (или по выбору) блокирования угрозы/процесса, если ее порог превышает заданный уровень?

А.А. На данный момент в самом решении нет функционала или кнопки, которые позволяют выполнять блокирующие действия. Однако MaxPatrol SIEM изначально разрабатывается с API, открытым практически ко всем компонентам и процессам обработки. Таким образом, уже сегодня есть примеры интеграций с другими решениями или запуска кастомных скриптов на основании нового инцидента, за счет чего, например, на основе определенного инцидента несложно заблокировать учётную запись в AD.

Но вообще это весьма интересный вопрос, который в силу своей сложности и многогранности охватить в рамках ответа невозможно. Приведу простой пример из реальной жизни другой SIEM-системы: заказчик хотел блокировать "учётку" после множественного удалённого входа, после скрупулёзной работы над логами и выявления всех служебных записей за несколько месяцев. Такая политика была создана, однако буквально в конце недели одно из ключевых бизнес-приложений остановилось. Оказалось, что некоторые из синхронизирующих процессов запускались только раз в квартал и использовали «не совсем» служебную учетную запись. Не стоит говорить, что ИТ-подразделение во всем винило именно ИБ, а те, в свою очередь, «плохой» продукт.

Без качественного и эффективного мониторинга большого смысла в возможности автоматической блокировки нет. Качественный мониторинг – это то, что мы даём нашим клиентам сегодня, и то, чего очень не хватает на российском рынке.

SN. Приведите примеры коротких (несанкционированное подключение, подбор пароля, неправомерные управляющие команды, потенциально опасные действия персонала и др.), длительных и комплексных угроз, с которыми можно бороться с помощью MaxPatrol SIEM 2.0.

А.А. Решение можно настроить на обнаружение разного типа атак: «короткие» атаки, такие, как брутфорс, несанкционированное подключение, нарушение внутренних политик, события ИБ на критичных активах и т.д. Длительные и комплексные угрозы чаще всего выявляются не при помощи какого-то очень длинного и сложного правила, а раскручиваются через форенсику (forensic) в момент расследований тех самых «коротких» угроз. Поэтому для SIEM-системы так важно не только оперативно выявлять угрозы, но и предоставлять удобный интерфейс для работы с логами. А это зачастую – колоссальный объём событий, исчисляемый миллиардами штук. При этом система должна сохранять быстрый поиск сортировку и группировку по ним.

SN. Какое время срабатывания на угрозу (длительность ее обнаружения, примеры)?

А.А. Если говорить об обнаружении базовых кирпичиков компрометации, то временная задержка от старта до уведомления оператора ИБ по почте составляет в среднем минуту. В случае сетевых атак этот интервал составляет секунды, а инциденты, связанные с приложениями (или тем более с физической безопасностью), будут иметь более существенный лаг по времени. Общей формулы здесь нет – от секунд до нескольких дней.

SN. В разветвленной инфраструктуре ЦОД могут происходить сотни тысяч событий в секунду. Как масштабируется система по производительности и объему событий с учетом их корреляции с предшествующими событиями? Развертывается самостоятельная система или используются уже существующие ресурсы?

А.А. Вопрос касается, скорее, архитектуры решения, которая проектировалась изначально для enterprise-рынка. Во-первых, в разветвленной инфраструктуре необходимо использовать распределенную архитектуру, собирать события требуется как можно «ближе» к самим источникам, иначе корпоративная сеть начнёт работать на SIEM, а не на бизнес. При этом на центральные компоненты возрастает нагрузка и, какая бы ни была производительность, один сервер всё равно не справится. Это решается при помощи следующих составляющих:

- все компоненты системы взаимодействуют через универсальную шину, и таким образом их можно разносить на разные физические серверы. Например, отделить базу данных от сервера корреляции, при этом для небольших инсталляций можно установить всё на один сервер или даже одну виртуальную машину (кстати, MaxPatrol SIEM, пожалуй, единственный SIEM, который может работать на одной виртуальной машине под управлением ОС Windows);
- распараллеливание нагрузки, то есть балансировка;
- ну и наконец – выстраивание иерархической архитектуры проекта. Например, у гипотетического заказчика, скажем, в Новосибирске собственная служба ИБ и там же установлен их собственный полноценный SIEM, с головным офисом (предположим в Санкт-Петербурге) настраивается двустороння связь для обмена политиками и инцидентами.

Также стоит заметить, что MaxPatrol SIEM является программным решением, которое можно установить как на выделенное оборудование, так и развернуть целиком в рамках виртуальной среды.

SN. Используется ли параллельная обработка, например, на базе hadoop-кластеров? Используются NoSQL БД для обработки логов, например, mongoDB, elastic и т.п.?

А.А. Применяется широкий спектр решений, ориентированных на обработку и хранение больших данных – это mongodb, elasticsearch, redis совместно с mssql. Активно исследуем и тестируем решение на базе технологий apache.

SN. Осуществляется ли корреляция внешних и внутренних событий (например, на нешаблонное поведение пользователя). Имеется в виду то, что при сложных атаках внешние угрозы могут являться лишь отвлекающими для совершения кражи инсайдером.

А.А. Такая возможность в решение заложена.

SN. Используется ли поведенческая аналитика для выявления аномалий поведения процессов/клиентов, идентификации клиентов?

А.А. Поведенческий анализ, выявление аномалий, как и алгоритмы самообучения – все это мы сегодня активно исследуем. Используя при этом богатый опыт, накопившийся при создании PT Application Firewall, методы защиты которого используют, в первую очередь, алгоритмы самообучения и были отдельно отмечены рынком (в том числе аналитическим агентством Gartner), как особо перспективные.

По большому счету сегодня мы не видим на рынке реально рабочих прототипов – в основном только маркетинговые заявления. Поэтому для нас так важно не просто запустить этот функционал «для галочки», но создать для наших клиентов перспективный и рабочий инструмент.

SN. Используются ли алгоритмы самообучения?

А.А. Пока нет.

SN. Запоминает ли система шаблоны атак? Например, для максимально быстрого выявления угроз при их повторении.

Да, в случае выявления атаки пользователь может зафиксировать паттерн поведения атаки так, чтобы система начала фиксировать атаку такого типа.

SN. Проводит ли MaxPatrol SIEM 2.0 аудит ИТ-инфраструктуры/настроек безопасности на соответствие корпоративным требованиям перед развертыванием? Если да, что тестируется и как?

А.А. Мы делаем не просто SIEM – мы создаём платформу, в рамках которой объединяются множество различных классов систем. Одной из них является MaxPatrol – система анализа защищенности и соответствия стандартов, которая уже сегодня эффективно решает, в том числе, задачи аудита инфраструктуры. С самого начала создания платформы мы ясно понимали, что SIEM, который анализирует только события, не может эффективно выявлять инциденты ИБ, поэтому уже сегодня в MaxPatrol SIEM мы собираем и можем использовать данные о конфигурации в связке с событиями.

SN. Возможно ли задание приоритетов (и их уровней) отслеживания угроз для разных процессов/приложений/сервисов? Можно ли менять приоритеты для одних и тех же процессов во времени (днем/ночью)?

А.А. Можно достаточно гибко настроить систему и её поведение в зависимости от времени, дней и т.д.

SN. Отслеживается ли изменение политик безопасности, например, при миграции ВМ в другую среду/облака?

А.А. Контроль соответствия политикам сегодня успешно выполняет MaxPatrol 8, со временем этот функционал полностью перейдет в новую платформу, которая уже сегодня работает с событиями и таким образом способна отслеживать факт изменения, например, при миграции ВМ.

SN. Какие ОС, гипервизоры, файловые системы, сети, протоколы, платформы, процессоры поддерживаются?

А.А. Что касается источников информации, то это практически все широко используемые сетевые устройства, ОС, приложения и средства защиты. Даже более: в системе реализованы так называемые «транспорты», при помощи которых возможно подключить практически любой источник (в том числе самописное ПО). Если же говорить о том, в какой среде может работать сама система, то тут также очень мало ограничений (в силу того, что мы не являемся ПАКом, не разрабатываем собственные ОС и т.д.), фокусируясь лишь на технологиях ИБ.

SN. Как MaxPatrol SIEM 2.0 интегрируется с мобильными/периферийными устройствами и контролирует их безопасность при работе с корпоративным контентом?

А.А. Решение строит модель всей инфраструктуры предприятия на сетевом, аппаратном и программном уровнях, что позволяет глубоко интегрироваться с инфраструктурами разной степени сложности.

SN. Работает ли MaxPatrol SIEM 2.0 с дедуплицированными/шифрованными данными? Может ли интегрироваться с DLP-системами?

А.А. Всё зависит от конкретного источника данных. 09 июня 2016 г. компания Positive Technologies обеспечила автоматическое подключение системы InfoWatch Traffic Monitor Enterprise в качестве источника событий информационной безопасности для системы MaxPatrol SIEM. На данный момент MaxPatrol SIEM поддерживает InfoWatch Traffic Monitor Enterprise версии 4.1, наиболее широко представленной в компаниях различных сфер российского бизнеса, благодаря чему события из DLP-системы доступны для обработки и анализа в общей системе мониторинга и корреляции событий информационной безопасности MaxPatrol SIEM.

Согласно нашим исследованиям, в 2015 г. в 86,3% случаев утечка информации в российских компаниях происходила по вине (или неосторожности) именно внутреннего нарушителя. И это без учета инцидентов, когда система выявляла мошеннические действия, коррупционные схемы или саботаж со стороны сотрудников. Даже один подобный инцидент может повлечь за собой и финансовые, и репутационные риски, поэтому сочетание решений классов SIEM и DLP в разы повышает эффективность работы служб информационной безопасности.

Несколько раньше, в апреле этого года, Positive Technologies и «Смарт Лайн Инк» объединили технологии для защиты корпоративных ресурсов: теперь PT MaxPatrol SIEM может автоматически подключать DeviceLock DLP Suite в качестве источника событий информационной безопасности.

Также MaxPatrol SIEM поддерживает средства защиты большинства отечественных производителей: «Доктор Веб», «Лаборатория Касперского», «Код безопасности», «С-Терра СиЭсПи», «Смарт Лайн Инк», InfoWatch, «ИнфоТеКС» и др. Количество поддерживаемых источников – одна из ключевых характеристик SIEM-системы. Но заказчику важна не сама эта цифра, а уверенность в том, что будут поддержаны источники событий именно его IT-инфраструктуры. А для российского заказчика в приоритете поддержка средств защиты информации отечественного производства.

В любом случае сегодня мы еще не встречали источник, который было бы невозможно подключить к MaxPatrol SIEM.

SN. Примеры визуализации угроз, доступ к средствам визуализации угроз?

А.А. Работа с решением происходит, как правило, от инцидента, создаваемого в автоматическом и ручном режимах с фиксацией всей информации, необходимой для проведения анализа и, при необходимости, расследования.

SN. Проводилось ли тестирование системы на устойчивость атакам? Если да, кто это проводил и как?

А.А. С самого начала мы планировали создать решение, способное вбирать в себя нашу богатую экспертизу в области ИБ (здесь стоит отметить, что наш исследовательский центр является одним из крупнейших в Европе). Тогда как сегодня SIEM-системы не имеют даже функциональной возможности использовать накопленную базу знаний экспертов у заказчика. SIEM`ы в первую очередь оценивают по функционалу, а не по базе знаний. Именно поэтому мы ввязались в такую сложную и долгую задачу по созданию нашей платформы. И в течение этого года мы планируем вывести в продуктив ряд интересных фич, связанных в первую очередь с передачей экспертизы в продукт, например, информации о новых сценариях атак и новых патернов поведения хакеров.

SN. Ваши ближайшие планы по развитию решения MaxPatrol SIEM?

А.А. Подход компании Positive Technologies подразумевает создание платформы, ключевым элементом которой является MaxPatrol SIEM. Построенная на активоцентрическом подходе и создании новой модели инфраструктуры, данная платформа должна быть легко управляема, адаптируема к динамично изменяющейся инфраструктуре организации и решать ее реальные задачи. В соответствии с уникальным видением развития индустрии SIEM и новой эры решений класса Threat Intelligence сформированы планы развития продукта на ближайшие три года, включающие четыре ключевых релиза ежегодно. Так, к третьему кварталу 2016 г. выйдет релиз, в котором появится облачный механизм обновления данных об уязвимостях, а к осени запланировано внедрение механизма автокорреляций на основе моделирования векторов атак. Быстрый выпуск обновлений позволяет оперативно вносить исправления и доработки по результатам пилотных внедрений.■