SOC: ВНЕШНИЙ ИЛИ ВНУТРЕННИЙ? ВЫБОР НЕИЗБЕЖЕН

ОШИБКА ОБХОДИТСЯ ДОРОГО: ЗАРЫТЫЕ В «ЗЕМЛЮ» ДЕНЬГИ И НЕОБХОДИМОСТЬ ПОДДЕРЖИВАТЬ РАБОТУ СТРУКТУРЫ, НЕ ПРИНОСЯЩЕЙ ОТДАЧИ

Иван МЕЛЕХИН
директор
по развитию АО НИП
Информзащита

Иван Мелехин рассказывает BIS Journal о плюсах и минусах внешних и внутренних центров управления безопасности (SOC), о том, что следует учитывать при заключении SLA между компаниями-заказчиками и компаниями-аутсорсерами, и о том, каким должен быть приближённый к идеалу SOC.

— Иван, поделитесь своим экспертным мнением: какие сервисы должны предоставляться современными SOC, чтобы полностью отвечать ожиданиям заказчиков?

— Не бывает двух одинаковых заказчиков, у каждого есть свои проблемы, запросы и предпочтения. Также на стороне заказчиков сильно отличаются уровни зрелости функций ИБ: запросы по конфигурации сервисов у стартапа и крупного банка зачастую несопоставимы. Поэтому, если мы говорим о внешнем центре управления безопасности (SOC), то он должен быть достаточно гибким, для того чтобы наиболее полно соответствовать потребностям клиентов. Если же мы говорим о базовом наборе сервисов, из которого можно выбрать конфигурацию под потребности практически любого заказчика, то можно назвать следующие:

- Сбор и хранение логов и событий информационной безопасности
- Автоматизированный анализ потока событий с использованием адаптируемых сценариев мониторинга и обогащением данных от различных внешних источников
- Ручная обработка инцидентов командой аналитиков с учётом особенностей вашей инфраструктуры, информационных сервисов и нормативно-организационной документации
- Оповещение об инцидентах по выбранным каналам связи (телефон, электронная почта, мессенджеры) и представление рекомендаций по реагированию
- Автоматизированный регулярный анализ защищённости и рекомендации по устранению уязвимостей
- Регулярная аналитическая отчётность
- Управление инцидентами и заявками

В качестве дополнительных сервисов, которые пользуются популярностью, можно назвать следующие:

- Анализ защищённости (пентесты, red team)
- Расследование инцидентов
- Управление СЗИ и реагирование на инциденты
- Киберразведка и киберучения
- Взаимодействие с регуляторами

— Внутренний и внешний SOC? Иногда банки, приступающие к решению этой задачи, долго размышляют, какому бы из этих вариантов отдать предпочтение. В чём, по вашему мнению, плюсы и минусы каждой из этих опций?

— К основным плюсам внешнего SOC можно отнести скорость подключения к сервису, существенную экономию бюджета (2–3 раза на промежутке в три года) и высокую квалификацию персонала, ежедневно сталкивающегося с большим количеством разнообразных инцидентов у клиентов. Также внешний SOC обычно имеет большой набор глубоко проработанных сценариев мониторинга и реагирования. К минусам внешнего SOC можно отнести сложности перехода между поставщиками услуг, отсутствие принадлежащего организации контента — сценариев мониторинга и реагирования и слабое формирование профильных компетенций внутри организации. Фактически если поставщик внешнего SOC покинет организацию, то она вернется к тому же состоянию, что и до подключения SOC, капитализации вложений не произойдёт. Также зачастую персонал внешнего SOC при большом количестве подключённых организаций может формально относиться к потребностям заказчика.

К основным плюсам внутреннего SOC можно отнести то, что на вложенные деньги организация не только получает сиюминутный сервис, но и фактически инвестирует их в развитие своей инфраструктуры и компетенций. Правда, к сожалению, посчитать возврат от этих инвестиций зачастую очень сложно. Также организация в случае выбора этого варианта получает сильно адаптированный под нужды организации сервис, тесно интегрированный со смежными бизнес- и вспомогательными функциями. К основным минусам внутреннего SOC можно отнести крайне высокие затраты на внедрение инфраструктуры и поддержание функционирования: например, затраты на содержание всего лишь двух аналитиков могут превысить 6 млн рублей в год, с учётом всех налогов и косвенных затрат, а в случае круглосуточного режима работы нужно не менее семи квалифицированных аналитиков. Также необходимо отметить отсутствие на рынке достаточного количества квалифицированного персонала и взвинченные высокой конкуренцией зарплатные ожидания, не всегда соответствующие уровню компетенций соискателей. Назову и ещё один минус: организация, строящая свой SOC, сталкивается с большими сложностями и трудозатратами по разработке контента (сценариев реагирования и мониторинга). К сожалению, внешний купленный контент (или поставляемый поставщиками SIEM из «коробки») зачастую практически бесполезен.

— Итак, и в том, и в другом варианте есть серьёзные плюсы и минусы. По вашему опыту, к какому выбору чаще склоняются компании-заказчики, и в силу каких причин?

— Как специалист, общающийся с заказчиками со стороны внешнего коммерческого SOC, я вижу несколько однобокую картину этого рынка. К нам приходят люди, которые осознанно не хотят или не могут построить свой SOC, или те, кто попробовал его построить, но безуспешно и с большими издержками. К сожалению, часто приходится видеть ситуацию, когда заказчику продали продвинутую техническую инфраструктуру SOC — начиная от SIEM и заканчивал IRP, но про процессы или забыли, или не смогли их внедрить. В результате заказчик имеет зарытые в «землю» капитальные вложения и плюс к этому он сталкивается с необходимостью поддерживать работу SOC, который не приносит организации какой-либо значимой пользы и ощутимой отдачи.

— Ваши советы в связи с этим?

— Прежде всего, мы рекомендуем подходить к этому вопросу итеративно — начать с полностью внешнего SOC для того, чтобы понять, какие сервисы и какой контент нужен заказчику и в какой конфигурации. Подключение внешнего SOC проходит быстро (в течение одного-двух месяцев) и является вполне приемлемым с бюджетной точки зрения. По мере осознания своих потребностей, можно переносить к себе или в зону своей ответственности части инфраструктуры и процессов SOC, например, внедрив у себя IRP или SOAR-систему, тесно интегрированную со своей инфраструктурой. Или наоборот, можно передавать внешним подрядчикам такие сервисы как реагирование на инциденты и управление СЗИ.

— Как следует правильно прописать разделение зон ответственности между компанией-заказчиком и компанией-аутсорсером в том случае, если мониторинг ИБ передаётся на аутсорсинг? Что компании-заказчику необходимо предусмотреть в данном случае?

— Во-первых, хотелось бы, чтобы компании, выступающие в роли заказчиков, не воспринимали внешний аутсорсинг мониторинга ИБ как некого рода серебряную пулю, которая позволит им защититься от любой нечисти. Иногда приходится видеть, как в SLA, например, пытаются включить требования по обнаружению в течение пяти минут любых атак с уязвимостями нулевого дня. Это принципиально невозможно. Если во внешний SOC не передаются события от источников, например, фиксирующих определённую активность на рабочих станциях, то выявить некоторые инциденты можно только достаточно поздно и по косвенным признакам. Поэтому определение зоны ответственности — это итеративный договорной процесс, результат общения между поставщиком услуги и заказчиком.

Для ряда типовых сценариев мониторинга, безусловно, есть понимание матрицы ответственности. Но если разрабатываются сильно кастомизированные сценарии, то процесс определения ответственности может быть довольно долгим и сложным. Также необходимо помнить, что заказчик никогда не передаёт на аутсорсинг одному поставщику все функции, необходимые для реагирования и выявления инцидентов: нужно учитывать и интегрировать в матрицу ответственности между поставщиком и заказчиком ответственность ИТ-подразделений заказчика в части выполнения рекомендаций и требований, ответственность руководства и финансов в части поддержки и финансирования корректирующих мер.

Также крайне сложно определить финансовую ответственность поставщика услуг SOC за те или иные инциденты: с одной стороны, из-за сложности определения реального ущерба, а с другой стороны, из-за того, что рекомендации аутсорсера никогда не соблюдаются в полном объёме как из-за финансовых ограничений, так и из-за баланса требований бизнеса и безопасности. Таким образом, устанавливать от-

ветственность поставщика сервиса SOC необходимо в тех границах, в которых у этого поставщика есть ресурсы для принятия на себя этой ответственности. Это выражается в том, что в SLA практически всегда включаются исключительно временные метрики по реализации тех или иных процессов на стороне SOC, такие как время принятия в работу или время первичного реагирования. Также могут включаться метрики по доступности сервисов.

— Насколько эффективным инструментом для разрешения дальнейших споров (например, о том, с какой скоростью следует реагировать на инциденты) является соглашение SLA? Особенно этот вопрос интересен в российских условиях.

— SLA является приложением к контракту, соответственно является достаточным инструментом для решения любых споров законными методами, включая судебные разбирательства. Другое дело, что зачастую реальных механизмов контроля SLA у заказчика нет, и он ориентируется на данные, представляемые исполнителем. Объективности ради добавлю, что построение системы контроля атсорсера за целым рядом внутренних процессов на «стороне» заказчика представляется крайне затруднительной задачей. Её решение возможно только в случае, если вся техническая инфраструктура SOC находится под управлением заказчика.

— Как, по вашему мнению, следует решать вопрос о допуске аутсорсера к критически важным для компании-заказчика данным и системам?

— Аутсорсер мониторинга информационной безопасности в штатном режиме работы обычно не имеет доступа ни к критичным данным, ни к критичным системам. Он имеет доступ к логам и событиями информационной безопасности, которые, безусловно, могут содержать некую критичную информацию. Доступ к данным и системам может потребоваться либо в случае выполнения расследований, либо в случае, если реагирование и управление СЗИ также передаётся на внешнюю «сторону». Но при любом раскладе правильно спроектированная система защиты должна в модели нарушителей учитывать и своих и внешних администраторов, и аутсорсеров, и поставщиков услуг и сервисов. И в любом случае между поставщиком сервисов и заказчиком заключается соглашение о конфиденциальности.

— Как избежать зависимости внутренней службы ИБ от аутсорсера?

— Если мы говорим о внешнем СОКе, то первым шагом, который можно сделать для облегчения процесса переключения между различными поставщиками и снижения зависимости от аутсорсера может являться реализация внутреннего хранилища логов. В этом случае, зеркалируя события, поступающие в такое хранилище можно достаточно безболезненно менять поставщиков услуг мониторинга. Необходимо отметить, что в этом случае организация должна иметь достаточно глубоко проработанную политику мониторинга, реализованную на ИТ инфраструктуре. Также очень важно иметь возможность выгрузки из систем провайдера всей информации касательно имевших место инцидентов, либо впоследствии реализовать IRP платформу внутри организации.

— Какие решения и услуги в сфере SOC предоставляет ваша компания? В чём их конкурентное преимущество?

— Мы предоставляем весь набор сервисов, перечисленных в первом вопросе. Также, так как наш SOC работает в рамках крупнейшего интегратора на рынке ИБ, мы можем предоставить большое количество смежных сервисов, начиная от аудитов заканчивая сервисным сопровождением систем защиты. В рамках наших сервисов SOC мы основной упор делаем на качество контента — сценариев реагирования и мониторинга, предоставляемых Заказчику. Мы имеем большой набор типовых сценариев, которые мы можем достаточно быстро адаптировать под нужды Заказчика, а также можем разработать кастомизированные сценарии, причём для самых различных случаев применения — от мониторинга облачной инфраструктуры до выявления мошеннических действий. Также мы делаем упор на удобство взаимодействия Заказчика с нами, начиная от использования различных каналов для общения, включая мессенджеры заканчивая разработкой удобного клиентского портала.

— Как вы видите процесс дальнейшего развития SOC?

— Если не рассматривать коммерческие вопросы, то одними из основных направлений развития SOCа я вижу разработку качественного контента, адаптированного под специфические нужды заказчиков из разных отраслей, и разную инфраструктуру (например, активно используемые технологии контейнеризации), реализацию мультивендорной технологической платформы SIEM, активную разработку своих кастомных решений для автоматизации деятельности SOC. Также, хотелось бы видеть больше активности в части взаимодействия различных SOC друг с другом.