Иван ЛОПАТИН
технический эксперт
АО «ДиалогНаука»

НА НОВОМ УРОВНЕ

ТЕХНИЧЕСКИЕ ТРУДНОСТИ РЕАЛИЗАЦИИ МОДЕЛИ СЕРВИС-ПРОВАЙДЕРА УСЛУГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (MSSP) И ПУТИ ИХ РЕШЕНИЯ

В этой статье мы постараемся приоткрыть занавес технических проблем со стороны SIEM-систем и их компонентов, с которыми сталкиваются организации при переходе на следующий уровень развития собственного ситуационного центра (SOC) в модели сервис-провайдера услуг по информационной безопасности (MSSP, Managed Security Service Provider).

Реалии развития современных SIEM-архитектур подталкивают крупные государственные и частные компании в сторону централизации сбора событий информационной безопасности и дальнейшего расследования инцидентов в головном подразделении, где есть высококвалифицированные кадры для расследования сложных таргетированных атак.

С целью коммерциализации своей деятельности и получения дополнительной финансовой прибыли ряд компаний переводят свои ситуационные центры в модель оказания услуг информационной безопасности SaaS (Security as a Service), выступая в роли MSSP-провайдеров. При этом на первом этапе компании, как правило, начинают предоставлять услуги только для собственных дочерних предприятий, а затем уже выходят на рынок предоставления услуг для сторонних организаций.

БАЗОВЫЕ РЕКОМЕНДАЦИИ

Чтобы начать процесс построения MSSP модели, необходимо убедиться в наличии:

- квалифицированных кадров;
- документальной базы (политики ИБ, регламенты, инструкции и т.д.);
- выстроенных процессов выявления и реагирования на инциденты;
- эффективно работающей SIEM-системы;
- проверенного контента в SIEM-системе для выявления инцидентов ИБ (правила, фильтры, отчёты, дашборды и др.);
- компонентов и дополнительных программных комплексов для реализации SOC;
- шины данных и специализированных программных средств для работы клиентов MSSP.

Если Вы приняли решение начать предоставлять MSSP-услуги другим лицам и компаниям на базе вашего SOC, то мы рекомендуем учитывать следующее:

1. Масштабируемость SIEM-систем зачастую является проблемой, когда необходимо подключить несколько заказчиков и правильно распределить потоки поступающей информации.

2. Чёткое проектирование каналов связи и «кратчайших путей» до вашей входной точки в SOC будет немаловажным подспорьем при реализации MSSP модели.

3. Изучение специфики и особенностей каждого подключающегося заказчика к вашей услуге является отправной точкой к фильтрации бескрайнего количества событий, которые будут поступать к Вам. В противном случае SOC просто «захлебнётся» и не сможет обработать поступающие события.

4. Организация работы первой линии уже не будет выглядеть настолько просто, что можно брать на неё студентов и людей с низкой компетенцией.

5. Каждый монитор первой линии в вашем SOC больше не может показывать «возможно-нужную» информацию — необходимость в оперативном мониторинге и качество визуализации метрик SOC будет стоять на первом месте.

6. Существующий контент в SIEM системе должен в автоматическом режиме перестраиваться под каждого заказчика и добавлять оперативную информацию в события каждого клиента.

7. Предоставление отчётности и визуализации каждому клиенту является неотъемлемой частью оказания услуги MSSP.

8. Необходимо предусмотреть механизм добавления или изменения подключённых услуг клиенту MSSP.

9. Необходимо продумать механизмы оповещения о выявленных инцидентах ИБ в ночное и нерабочее время, так как привлечение сотрудников разных подразделений (ИТ, ИБ, Network, Руководителей проектов и др.) — задача, требующая отдельной проработки. Для организации оповещений зачастую используются механизмы интеграции со Skype, Telegram bot и другие.

10. Ведение услуг MSSP предполагает наличие руководителей проекта для клиента и заказчика, так как интеграционные работы зачастую схожи по уровню сложности с работами по внедрению компонентов SIEM.

Далее рассмотрим более подробно некоторые аспекты построения модели MSSP.

SIEM КАК УСЛУГА MSSP

На сегодняшний день большое количество владельцев SOC уверены, что они готовы принимать «на борт» нагрузку потенциальных клиентов без каких-либо трудностей. Однако их мечты в большинстве случаев обречены разбиться о входной EPS (объём событий поступающих в секунду), отсюда вытекает следующее:

Проблема MSSP № 1. Клиент зачастую сам не знает, что нужно собирать и обрабатывать.

Правило MSSP № 1. Собирать и обрабатывать следует только те события, под которые у вас есть необходимый контент в SIEM-системе.

Ваша SIEM должна быть готова обрабатывать в режиме реального времени такой объём поступающих событий, который будет достаточным и необходимым для покрытия всех пиковых значений Ваших заказчиков и клиентов.

Основным инструментом для выявления инцидентов ИБ является Ваш контент в SIEM (правила, фильтры, отчеты, дашборды и другое). Такой контент должен удовлетворять следующим требованиям:

- создан по мировым практикам реализации MSSP моделей;
- прост и удобен в эксплуатации — в случае необходимости должен быть изменён любым членом команды SOC, ответственным за контент;
- классифицирован — классификация событий и инцидентов ИБ необходима для реализации модели выявления инцидентов и их визуализация для каждого заказчика;
- оптимизирован — быстродействие работы всех компонентов SIEM-системы — это залог быстрой обработки поступающих событий. Также немаловажную роль играет отсутствие неиспользуемых ресурсов и\или ресурсов тестового назначения в продуктивной среде;
- разграничительным, — обладающим функциями работы для любого из заказчиков без дополнительной настройки;
- масштабируемый — контент должен легко масштабироваться для лёгкого перехода на следующий уровень развития SOC — MSSP.

На сегодняшний день на российском рынке есть несколько предложений по готовому контенту для SIEM-систем. Так, например, компания «ДиалогНаука» предлагает самодостаточный SOC-пакет правил корреляции собственной разработки, который в том числе может использоваться для реализации MSSP-модели.

МАНИПУЛЯЦИЯ УСЛУГАМИ MSSP

Необходимо понимать, что предоставляемый сервис MSSP — это возможность заказчика выбирать те услуги и компоненты, в которых у него есть потребность в данный момент, а также возможность отключать услуги в случае их неактуальности (DDoS, вирусная эпидемия).

Разработка механизма выбора услуги и её автоматической активации в случае необходимости является основной задачей разработки архитектуры, так как ручное управление клиентскими услугами уже уходит в прошлое. В данный момент аналогичные механизмы широко применяются при разворачивании виртуальных серверов и сервисов через личный кабинет облачных провайдеров. Отсюда возникает следующая проблема.

Проблема MSSP № 2. Для предоставления услуг должного уровня количество разрабатываемых и необходимых к оптимизации сервисов для MSSP возрастает в несколько раз.

Правило MSSP № 2. Использование решений с открытым исходным кодом (Open Source) в MSSP не всегда плохо, а зачастую просто необходимо (например, TheHive, Elastic Stack, Metron, Hadoop).

ОТЧЁТНОСТЬ И ВИЗУАЛИЗАЦИЯ

Необходимо понимать, что под услугой MSSP понимается весь спектр сопутствующих задач, которые клиент хочет получить от сервис-провайдера, включая визуализацию, расчёт метрик KPI, получение отчётности и оперативное оповещение об инцидентах высокой критичности.

В случае MDR-архитектуры дополнительно потребуется предоставление информации об этапности реализации атаки (kill chain), классификации угрозы и возможных объектов, находящихся в зоне риска. Отсюда можно сделать следующий вывод:

Проблема MSSP № 3. Качественная визуализация — отдельный программный комплекс, входящий в состав SOC и требующий компетентных специалистов.

Правило MSSP № 3. Отчётность и визуализация — главный инструмент для анализа эффективности работы сервиса MSSP для клиента.

Визуализация должна быть для каждого клиента индивидуальная, как и KPI. Основной проблемой будет являться быстрое разграничение доступов к ресурсам SIEM и шине данных для визуализации и отчётности без изменения большого количества правил, фильтров и других ресурсов.

Примером отчётности могут послужить уведомления об инциденте ИБ в Telegram или другой корпоративный мессенджер. Основная идея заключается в том, что при наступлении инцидента ИБ корреляционное правило запускает скрипт, который добавляет в клиентский telegram-канал всю необходимую информацию.

* * *

Мы постарались изложить свой взгляд на те проблемы, с которыми может столкнуться компания на пути трансформации в сервис-провайдера услуг по информационной безопасности. Мы искренне надеемся, что наши рекомендации позволят избежать целого ряда проблем и дадут возможность быстрее и эффективнее предоставлять услуги в рамках модели MSSP и в последующем MDR.