Сервис MDR от вендора: союзник или конкурент для Managed SOC?

kaspersky

Вениамин Левцов

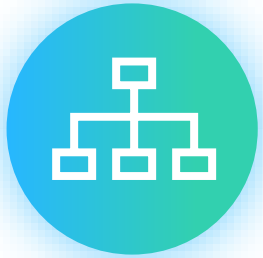
Директор глобального центра экспертизы по корпоративным решениям

Способы повышения эффективности подразделения ИБ

Оптимизация процессов, **обучение, расширение** штата

Внедрение средств **автоматизации управления** систем ИБ

(Modern SOC, SOAR, IRP, XDR)



Вовлечение поставщиков управляемых услуг (MSS)

Управляемые сервисы в ИБ

Администрирование

Управляемые ИТ-сервисы

Развертывание, настройка, поддержка и администрирование продуктом, возможно владение лицензией

Управление элементами системы ИБ

ИБ как сервис

Владение или управление SIEM, ИБ-интеграции, управление подсистемами и политиками ИБ

Проактивный поиск угроз и реагирование

Обнаружение сложных угроз

Детектирование сложных угроз при помощи анализа телеметрии в облаке и реагирование

Managed Service Provider (MSP)

Managed Detection and Response (MDR)

Managed Security Service Provider (MSSP)

Общая схема оказания сервиса MDR

Сбор расширенной телеметрии с конечных точек в сети заказчика и с удаленных рабочих мест

1 Сбор телеметрии

- **Filesystem events**
  (file creation, modification)
- **Process events**
  (process start, injection)
- **Network events**
  (e-mail, file downloading, connection, DNS query)
- **System events**
  (registry key change, events log, autorun)
- **Endpoint security events**
  (detect, quarantining, scan result)
- **Security events**

Общая схема оказания сервиса MDR

Загрузка отчета об инциденте
на портал, консультации по отчету

2 Поиск угроз и отчет об инциденте

- Анализ телеметрии на базе MITRE ATT&CK®
- Использование глобальной базы Threat Intelligence
  (включая APT атрибуты)
- Поведенческий анализ в песочнице
- ML-based авто-анализ
- Команда операционного анализа
- Команда исследователей

Общая схема оказания сервиса MDR

3 Удаленное реагирование

- Изоляция конечной точки
- Запрос файла с конечной точки
- Удаление файлов
- Удаление ключей реестра
- Остановка процесса

Особенности и ограничения MDR сервиса от вендора

MDR сервис от вендора

- Относительно высокие затраты на оказание и цена
- Предполагает доступ к порталу с отчетом об инциденте (peer-2-system) и консультациям по отдельным вопросам
- Отчет об инциденте требует компетенции на стороне заказчика
- Стандартное соглашение Terms & Condition
- Стандартный SLA
- Хранение данных в облаке
- Фокус на расширенном детекте на основе анализа телеметрии поверх продукта

Сильные стороны регионального провайдера услуг ИБ

Гибкость SLA / T&C

Кастомизация уровней сервиса с учетом параметров недопустимого ущерба для конкретного заказчика

Широкая зона покрытия

Область контроля выходит за пределы конечных точек, включает контроль облачных сред, LDAP, платформы идентификации, сетевое оборудование, web и mail траффик, VPN, удаленные рабочие места и терминалы, БД

Сервисы для различных доменов ИБ

включая Управление уязвимостями, Управление сетевой безопасностью, Управление удаленными рабочими местами и т.д.

Комплексное представление

об инфраструктуре заказчика

Поддержание полного цикла

реагирования на инцидент

Сервис-менеджер

как единая точка для обращения и взаимодействия (peer-2-peer)

Модель кооперации провайдера ИБ услуг и MDR сервиса от вендора

Чтобы сделать разумный выбор, надо прежде всего знать, без чего можно обойтись.

Эммануил Кант (1724 – 1804),
немецкий философ

Спасибо!

Вениамин Левцов
veniamin.levtsov@kaspersky.com

kaspersky