We know we can

softline

Managed Endpoint Detection and Response на базе Microsoft Defender for Endpoint и Security Operation Center компании Softline

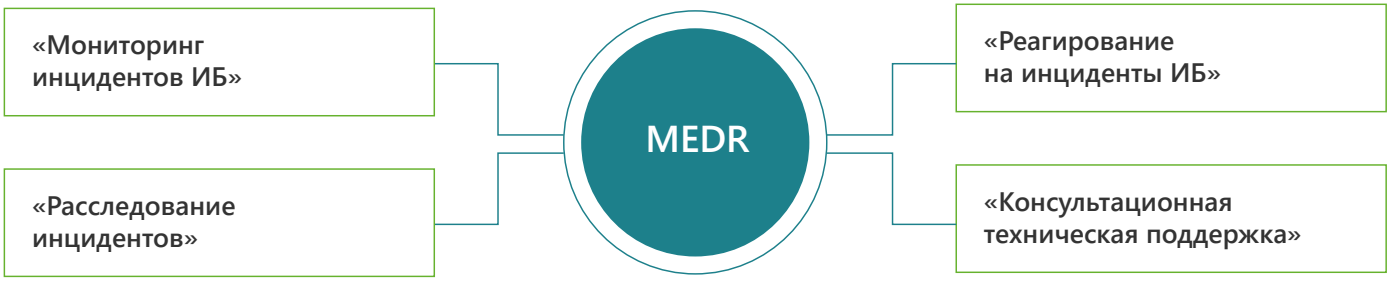
MEDR – это сервис реагирования на события информационной безопасности в отношении конечных точек, которые защищены Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint — это комплексное облачное решение для:

- обеспечения безопасности конечных точек. Основной функционал:
- средства контроля и оценки уязвимостей на основе рисков;
- сокращение поверхности атаки;
- современная защита на базе облачных технологий и поведенческого анализа;
- обнаружение и нейтрализация атак на конечные точки;
- автоматическое исследование и исправление;
- служба направленной охоты на угрозы;
- различные API и универсальные инструменты управления безопасностью.

Для высокой эффективности защиты конечных точек необходимы надлежащие процессы и квалифицированные специалисты, которые реагируют на инциденты ИБ.
Компания Softline предлагает вам увеличить пользу от EDR, подключив услугу мониторинга и реагирования на события ИБ в вашей инфраструктуре. Эти действия будут осуществлять эксперты нашего центра кибербезопасности (SOC).

Сервисы Softline



Мониторинг инцидентов ИБ

1. Круглосуточный автоматизированный мониторинг событий информационной безопасности на хостах в инфраструктуре Заказчика средствами Microsoft Defender в режиме 24x7x365.
2. Автоматическое оповещение сотрудников Заказчика о возникших инцидентах ИБ по e-mail в течение 15 минут с момента регистрации инцидента.
3. Поддержание в актуальном состоянии схем оповещения.
4. Подготовка и предоставление ежемесячных отчётов в электронном виде о выявленных инцидентах ИБ.

Реагирование на инциденты ИБ

- Обработка исходных данных инцидента, переданного конечным исполнителям в системе СервисДеск.
- Верификация (подтверждение) действий.
- Коммуникации с сотрудниками Заказчика в рамках выявленного события/инцидента.
- Эскалация инцидента с результатами обработки и необходимыми контрмерами для применения на инфраструктуре Заказчика.

Реагирование на инциденты занимает не более 15 минут с момента регистрации инцидента ИБ или завершения процедуры автоматизированного реагирования (если она проводилась) в формате 24x7x365.

Расследование инцидентов ИБ

В рамках расследования инцидентов специалисты Softline проводят следующие действия:

- исследование узла на наличие угроз/заражений, нераспознаваемых штатными средствами антивирусной защиты Заказчика;
- исследование узла на наличие индикаторов заражения, не имеющих сигнатурного детектирования;
- исследования, направленные на анализ содержимого узла, событий системных журналов, сетевой активности, проведение динамических и статических анализов подозрительных образцов (файлы, письма, предоставленные Заказчиком) на предмет содержания угроз ИБ;
- оценка благонадежности внешних ресурсов (URL/IP-адрес), с которым выявлено сетевое взаимодействие;
- определение маркеров вредоносного поведения образцов и индикаторов компрометации (взаимодействие с внешними ресурсами, изменения реестра и файловой системы) для передачи специалистам Заказчика на проверку инфраструктуры.

Консультационная техническая поддержка

- Консультационная техническая поддержка по работе системы, а также по решению технических проблем.
- Взаимодействие с технической поддержкой вендора.

Преимущества для заказчика

Снижение рисков информационной безопасности, и, как следствие, снижение риска возникновения финансовых потерь, прерываний в деятельности компании и утечки данных

Защита устройств от сложных целенаправленных атак

Мониторинг и реагирование в режиме 24x7x365

Гарантированный уровень сервиса

Оптимизация расходов (персонал, оборудование, перевод капитальных издержек в операционные)

Возможность перейти на более высокий уровень сервиса – Soc-as-a-Service (требуется подключение дополнительных источников событий ИБ)

+7(495) 232-0023
info@softline.com

softline®
We know we can