kaspersky 25 years

Защита конечных точек: почему Вам нужен EDR[1]

Никита Зайчиков
Менеджер
по продуктовому маркетингу

[1] EDR – Endpoint Detection and Response, Системы обнаружения и реагирования на угрозы

О чем будем говорить

- Угрозы
- Защита конечных точек
- EDR: кто использует
- EDR: функционал
- Как мы помогаем
- EDR: мифы
- Демо
- Выводы

1.

Угрозы

Новая реальность

Неопределенность. Больше рисков. Поиск решения

Интерактивная карта киберугроз

Подробнее

Усложнение атак

Количество киберинцидентов в российских компаниях увеличилось **в 4 раза** за первые 9 месяцев 2022 года в сравнении с 2021*

Киберагрессия

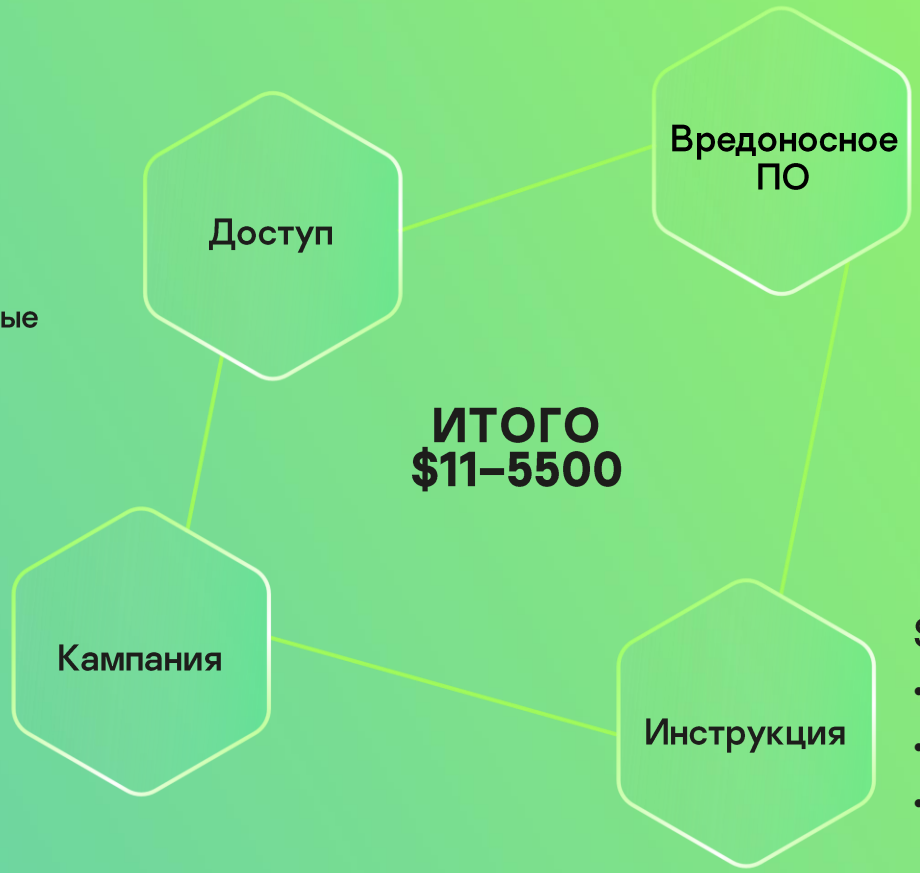
Россия **номер 1 в мире** по количеству атак

Срочное замещение

Ряд различных защитных ИБ решений становятся менее эффективными, **риски пропустить сложную кибератаку значительно повышаются**

* По данным центра реагирования на инциденты «Лаборатории Касперского»

Организация атаки не требует ни больших вложений, ни технических навыков



$0–5000[1]

- RDP
- VPN
- Учетные данные

$10–150[3]

- RDP
- VPN
- Учетные данные

$200–3500[2]

- Фишинг
- Шифровальщик
- Банковский троянец

$1–30[3]

- Вредоносное ПО
- Фишинг
- Взлом учетных записей

[1] «Лаборатория Касперского»
[2] CSOOnline
[3] Top10VPN

А ущерб от атаки может быть очень серьезным

Расходы атакованной организации[1]

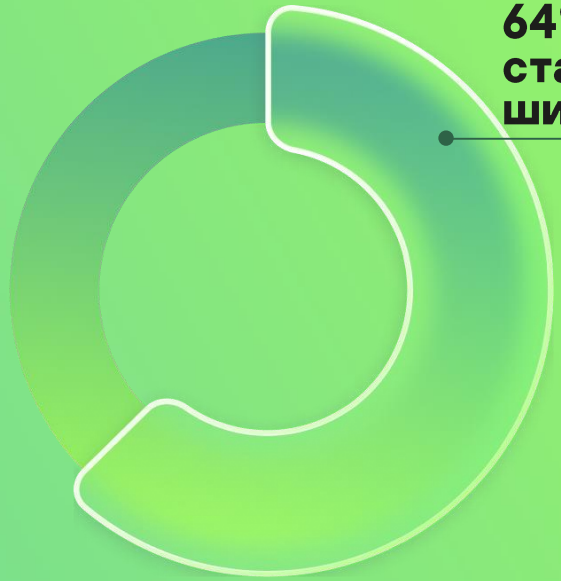
Крупные предприятия

$927 тыс.

Малый и средний бизнес

$105 тыс.

Главная угроза: шифровальщики[2]



64% компаний стали жертвами шифровальщиков

- Выкуп
- Помощь сторонних экспертов
- Улучшение инфраструктуры
- Повышение осведомленности сотрудников
- Пени и штрафы
- Коммерческие потери
- Выплата страховых взносов
- Ущерб репутации

[1] «Лаборатория Касперского»

[2] «Лаборатория Касперского»

Выплата выкупа ничего не гарантирует

Двойное вымогательство

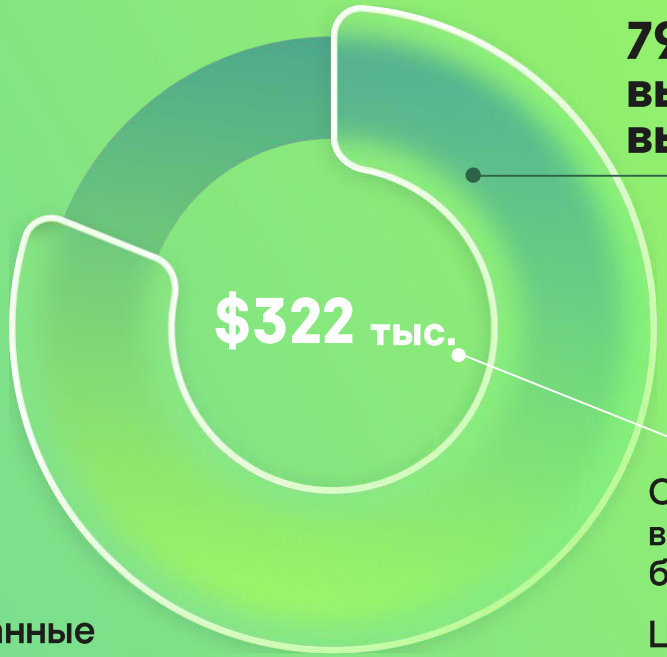
Преступники не только шифруют ваши данные, но и крадут их – и требуют выкуп за уничтожение копий

20 дней[2]

в среднем длится простой после атаки

Никаких гарантий

Злоумышленники могут так и не вернуть данные



79% компаний выплачивают выкуп[1]

Средняя сумма выкупа для среднего бизнеса.

Цена полного восстановления в **5-10 раз выше.**[3]

[1] «Лаборатория Касперского»
[2] Statista
[3] Illumio

Шифровальщики – основная угроза, но нельзя забывать и об остальных

- Шифрование
- Повреждение резервных копий
- Двойное вымогательство

- Учетные данные
- Финансовая информация
- Бизнес- и IT-процессы

Доступ к системам в будущем – злоумышленники воспользуются им сами или продадут другим

- Персональные данные
- Коммерческая тайна
- Конфиденциальная информация

Киберпреступники все лучше обходят системы защиты

Идентифицируемые характеристики постоянно меняются.

Использование легитимных системных инструментов для атаки.

Проникнув в инфраструктуру, злоумышленники долго бездействуют, чтобы остаться незамеченными.

Многокомпонентное вредоносное ПО позволяет совершить атаку, даже если один из компонентов будет удален.

[1] Living-off-the-land – атака посредством легитимных инструментов

Типы угроз

Массовые

Наиболее распространены

Простое обнаружение

Легко устраняются

Решение:

- Автоматическое предотвращение
- Усиление защиты (system hardening)

Скрытые

Легко найти в даркнете

Избегают обнаружения

Значительные последствия

Решение:

- Различные механизмы обнаружения
- Прозрачность, анализ и реагирование

Продвинутые

Часто – целевые атаки

Сложны в обнаружении

Много-векторные и устойчивые

Решение:

- Продвинутые технологии обнаружения
- Глубокое расследование

2.

Защита конечных точек

Система защиты конечных точек (EPP[1])

Против угроз: Массовых

- Критически важная часть корпоративной ИБ
- Уменьшение поверхности атаки и усиление защиты (system hardening)
- Автоматическое предотвращение и обнаружение угроз
- Автоматическое устранение угроз

[1] Endpoint Protection Platform

Но такие инструменты не предназначены для защиты от скрытых угроз

Низкая прозрачность

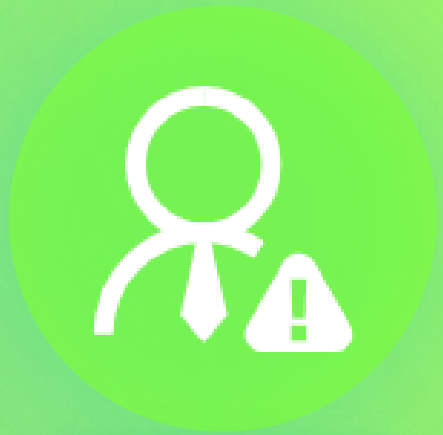
Что произошло – и на каких хостах?

Сложный анализ

Как мне проанализировать угрозу и найти первопричину?

Медленное реагирование

Как мне быстро провести реагирование и ничего не сломать?



Высокий риск

Endpoint Detection and Response

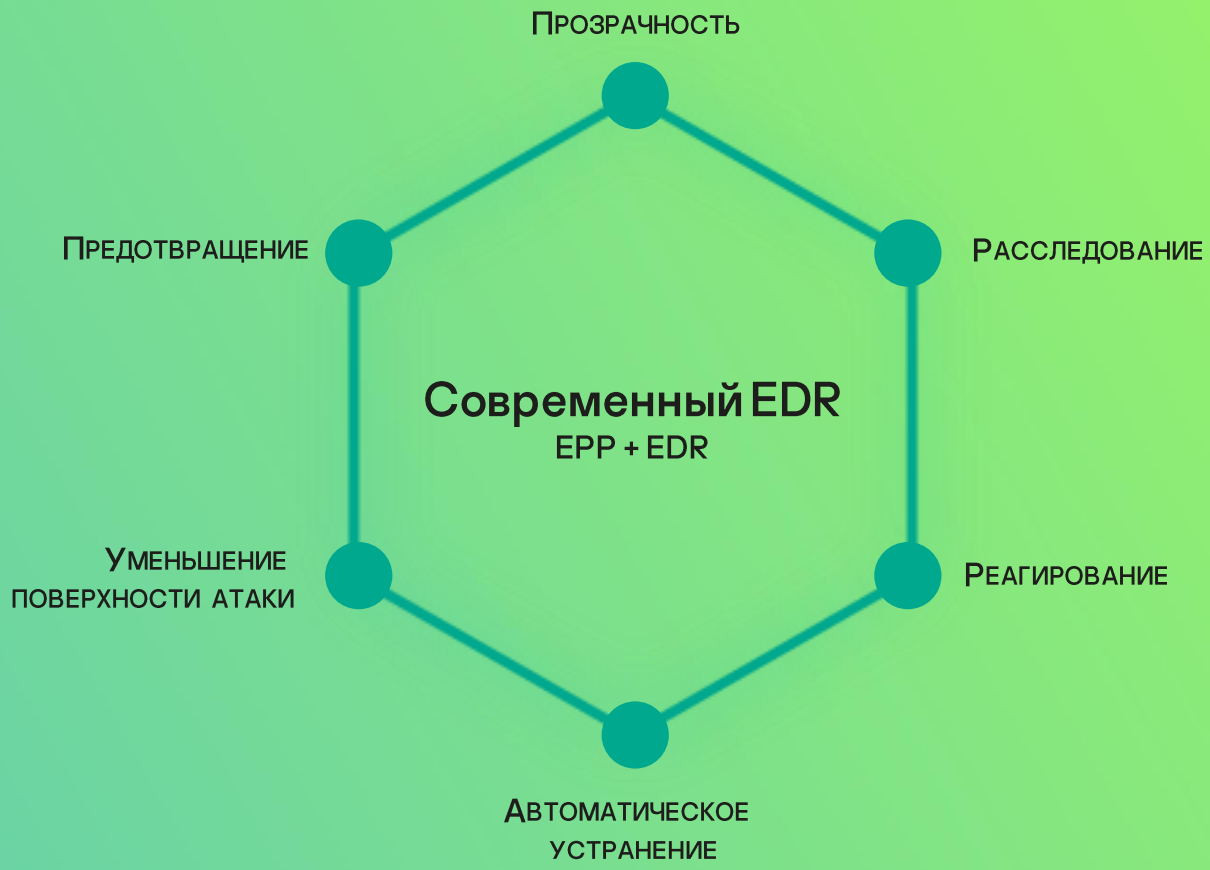
Против угроз: Скрытых Продвинутых

- Продвинутые технологии обнаружения
- Прозрачность угроз и инфраструктуры
- Инструменты для расследования угроз
- Быстрое и точное реагирование

Когда используется EPP, а когда – EDR

Критерий	EPP	EDR
Класс угроз	Массовые	Скрытые и продвинутые
Ключевая цель	Автоматически защищать от постоянного потока угроз	Найти и обезвредить более сложные атаки
Ключевое действие	Предотвращение	Анализ и реагирование
Время использования	Защита в реальном времени	Расследовать и устранить активные атаки
Участие человека	Минимальное наблюдение	Активное участие
Обнаружение	Автоматическое детектирование	Продвинутое детектирование и обнаружение угроз, которое сложно найти обычными средствами
Контекст угрозы	Фокусируется на автоматической защите и не показывает контекст угрозы	Помогает службе ИБ получить полные данные об атаке и проанализировать их
Реагирование	Автоматическое устранение обнаруженных угроз	Автоматизированное и ручное реагирование на угрозы, которые невозможно нейтрализовать автоматически

Современная защита конечных точек



3.

EDR: кто использует

	Сейчас	Рост
Отрасль	ИТ и телекоммуникации	Розничная торговля
Размер	Крупный бизнес	Средний бизнес
Регион	Северная Америка	Азия и Россия
Установка	Локальная	Облако или локально

Источник Allied Market Research

Типы организаций

Тип A

- Активное развитие ИТ, поддержанное существенным бюджетом
- ИТ используется в качестве конкурентного преимущества

Тип B

- Стабильное развитие ИТ с достаточным бюджетом
- ИТ используются для продуктивности

Тип C

- Консервативное использование ИТ, не склонны к риску
- Минимизация ИТ бюджета при поддержании работоспособности

Требования к EDR: тип A

Сценарий

Дать своим экспертам инструменты для поиска и нейтрализации продвинутых угроз.

Требования

- Возможность проактивного поиска угроз
- Управление инцидентами
- Тонкая настройка

Решение

- Продвинутое детектирование
- Ретроспективный анализ
- Доступ к аналитическим данным[1]
- Настройка логики детектирования
- Сопоставление с базой MITRE ATT&CK
- Широкий набор опций реагирования

[1] Threat Intelligence

Требования к EDR: тип B

Сценарий

Начать развивать процессы реагирования на инциденты и защититься от скрытых угроз.

Требования

- Анализ и реагирование
- Быстрое обучение
- Автоматизация и масштабирование

Решение

- Единая карточка инцидента
- Быстрый обзор угрозы
- Рекомендации по реагированию
- Визуализация атаки
- Простой процесс расследования
- Автоматизированное реагирование

Требования к EDR: тип C

Сценарий

Добавить прозрачности автоматической защите для периодического использования.

Требования

- Строится на базе мощного EPP
- Максимальная автоматизация
- Низкие затраты ресурсов

Решение

- Базовый EDR функционал поверх EPP
- Визуальный анализ первопричин
- Простой интерфейс
- Единая консоль и агент
- Автоматическое устранение угроз
- Возможность ручного и автоматизированного реагирования

4.

EDR: функционал

Не существует универсальных решений

Экспертный EDR

Тип A

Требования

- **Интегрируется** с EPP
- Возможность проактивного поиска угроз
- Полная телеметрия
- Управление инцидентами
- Тонкая настройка

Базовый EDR

Тип B+C

Требования

- **Строится на базе** мощного EPP
- Анализ и реагирование
- Автоматизация и масштабирование
- Низкие ресурсные затраты
- Простое обучение

Тип A

Экспертный EDR

Интегрируется с EPP

Современные технологии обнаружения угроз

Включает TI[1]

Сканирование индикаторов компрометации

Обнаружение

На основе знаний о тактиках и техниках злоумышленников – с помощью индикаторов атаки (IoA).

Проактивный поиск

Сбор телеметрии и ретроспективный анализ, тонкая настройка логики детектирования (YARA).

Реагирование

Запрет запуска, удаление файла, сетевая изоляция, завершение процесса, получение файла и др.

Управление

Создание инцидента из нескольких обнаружений для назначения аналитику и исследования.

[1] Threat Intelligence, аналитические данные об угрозах

Тип B+C

Базовый EDR

Интегрируется с EPP

Современные технологии обнаружения угроз

Включает TI[1]

Сканирование индикаторов компрометации

Прозрачность

Единое место сбора данных об обнаружении.

Анализ

Необходимые данные и визуализация пути атаки для быстрого расследования.

Реагирование

Несколько ключевых опций реагирования: сетевая изоляция, карантин и запрет запуска.

Автоматизация

Рекомендации по реагированию и автоматизация реагирования и поиска индикаторов компрометации.

[1] Threat Intelligence, аналитические данные об угрозах

5.

Как мы помогаем

Базовый EDR: Kaspersky EDR для бизнеса Оптимальный

Продвинутая защита конечных точек

- Защита от новейших угроз, в том числе от бесфайловых вирусов
- Адаптивный контроль аномалий
- Автоматическое устранение угроз
- Развертывание в облаке или локально

Расследование

- Анализ первопричин
- Детали по инциденту
- Обогащение данными Threat Intelligence

Прозрачность

- Визуализация пути атаки
- Сканирование индикаторов компрометации
- Единая карточка обнаружения

Реагирование

- Рекомендации по реагированию
- Реагирование «в одно нажатие» и автоматическое реагирование
- Сетевая изоляция, запрет запуска, карантин

Связанные продукты и сервисы:

- Kaspersky MDR Optimum
- Kaspersky Symphony

Экспертный EDR: Kaspersky EDR Expert

Продвинутая защита конечных точек

- Предотвращение угроз
- Поддержка нескольких ОС
- Интегрируется с EPP

Проактивный поиск угроз

- Централизованное хранение полной телеметрии
- Сопоставление с MITRE ATT&CK
- Доступ к порталу Kaspersky Threat Intelligence
- Создание запросов поиска угроз

Продвинутое обнаружение

- Обнаружение с помощью индикаторов компрометации (IoC) и индикаторов атак (IoA)
- Настройка YARA правил
- Анализ в песочнице

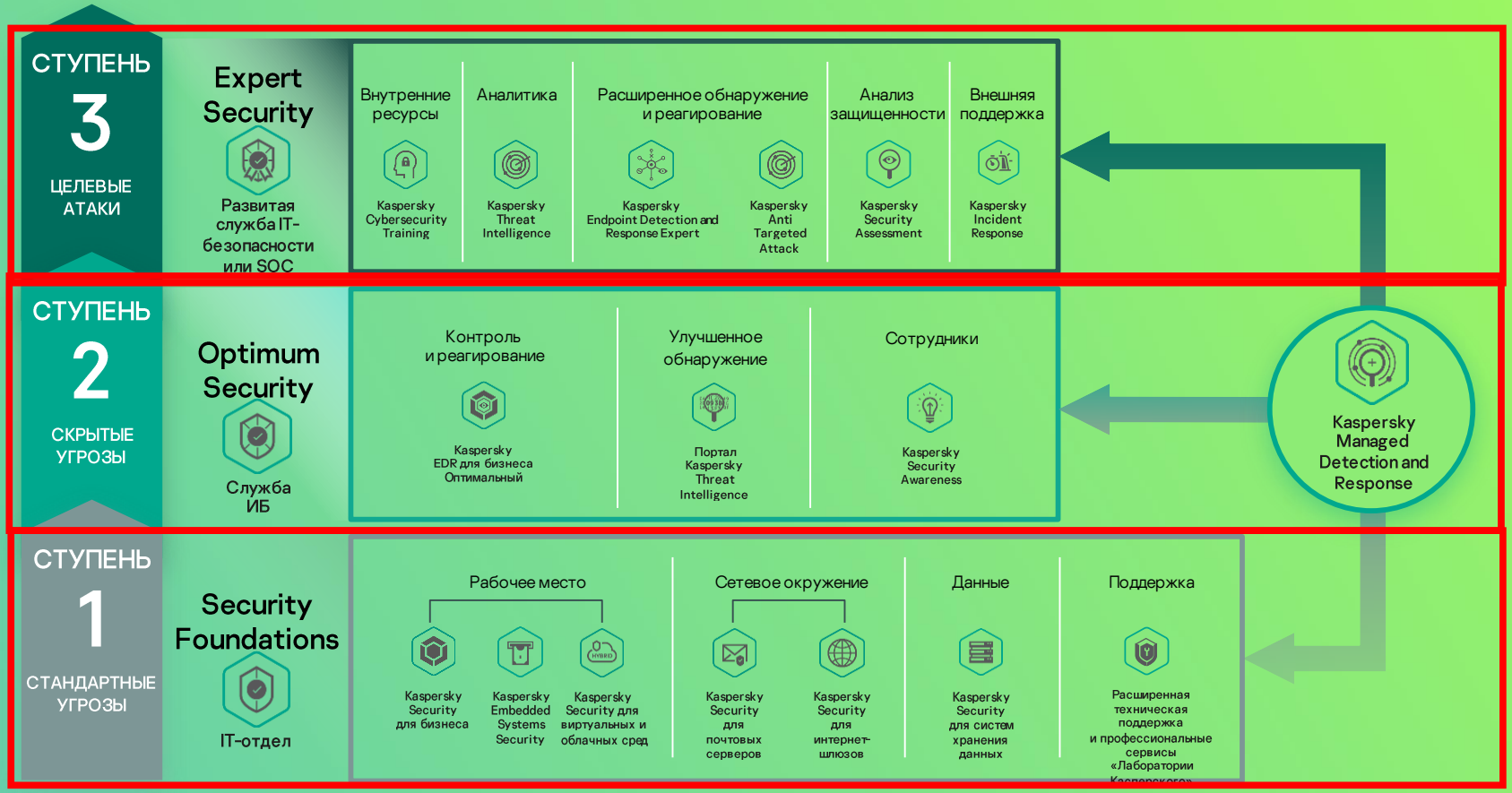
Реагирование на инциденты

- Автоматизированное реагирование и рекомендации
- Множество опций реагирования
- Возможность реагировать на целые группы конечных точек

Связанные продукты и сервисы:

- Kaspersky Symphony
- Kaspersky Anti Targeted Attack
- Kaspersky Threat Intelligence

EDR – лишь малая часть нашего портфолио



6.

EDR: мифы

Миф: EDR сложный и затратный

Часть 1

Недостаточно персонала

Миф:

Нам нужен отдельно выделенный человек – настоящий эксперт с глубоким знанием ИБ

Реальность:

На самом деле да, желательно иметь хотя бы базовые навыки ИБ, понимать что такое цепочка атаки и индикатор компрометации. Однако, это зависит от компании и Ваших целей.
Выбранное EDR решение должно помогать специалистам обучаться через рекомендации и простой интерфейс.

Часть 2

Сложное решение

Миф:

EDR решения слишком сложные и требуют больших затрат времени и ресурсов

Реальность:

- Поддерживает любую инфраструктуру
- Единый агент
- Низкое влияние на производительность
- Автоматизированные сценарии работы

Базовый EDR не сложнее любого другого ИТ-инструмента, а Экспертный понадобится, когда у Вас уже будет время и ресурсы.

Миф: EDR это только для крупного бизнеса

Часть 1

Сложные угрозы

Миф:

Нужен для защиты от сложных угроз, которые актуальны только для больших компаний

Реальность:

- Помогает защититься от различных типов угроз
- Скрытые угрозы атакуют даже малый бизнес

Часть 2

Высокая цена

Миф:

У нас нет бюджета ни для чего кроме антивируса

Реальность:

Мы предлагаем единое решение с простой модернизацией – построенное на нашем EPP

Часть 3

Затратно по времени

Миф:

Специалист не может себе позволить тратить на это время

Реальность:

Правильный инструмент наоборот экономит время, которое иначе пришлось бы тратить на расследование в ручную.
А автоматизация и реагирование сразу на группу ПК помогает быть ещё эффективнее.

Что останавливает заказчиков в России от внедрения EDR

8% Непонятная функциональность

Быстрое расследование и реагирование на обнаруженные инциденты.

16% Высокая цена и стоимость владения

Продукт входит в линейку Kaspersky Security для бизнеса, использует ту же консоль и не требует значительных ресурсов.

10% Агенты снижают производительность ПК

Используется один агент с Kaspersky Security для бизнеса других уровней.

10% Подход в целом слишком затратный и сложный

Начать строить процессы реагирования на инциденты можно с простых инструментов и подходов, а затем использовать более продвинутые.

40% Требует высокой экспертизы

Продукт прост в установке, обучении и использовании. Прямо в интерфейсе есть рекомендации и подсказки по реагированию.

16% Другое

Функциональность – необходимая. Переход с других продуктов - простой. Затраты – минимальные.

Источник: Данные опроса Anti-Malware

7.

Демонстрация
и новые возможности

Денис Кащеев
Инженер
предпродажной поддержки

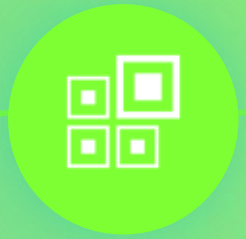
8.

Выводы

Выводы о современных EDR решениях

Необходимый функционал

EDR всё больше становится стандартом в области ИБ, и без предоставляемых им возможностей трудно защищаться от скрытых, сложных и продвинутых угроз



Единая защита

EPP и EDR должны работать вместе, создавая оптимальную защиту против всех типов угроз

Разные предложения

Не существует универсального EDR предложения, т.к. у разных заказчиков – разные потребности и сценарии использования

Пробуйте Kaspersky EDR для бизнеса Оптимальный!

Бесплатно на 30 дней

https://kas.pr/edr-optimum-trial-ru

kaspersky 25 years