Kaspersky Symphony XDR

kaspersky
Platinum Partner

Руководите направления решений
«Лаборатории Касперского»
Михаил Усачёв

ПОЛИКОМ про

Интересные факты об XDR

XDR

Это современная концепция, которая представляет собой кросс-продуктовую историю, обогащенную поверх дополнительными функциональными возможностями, в том числе Threat Intelligence

XDR не равно EDR

XDR основан на расширении технологии EDR и контроля потенциальных точек входа злоумышленника за пределами рабочих мест и серверов

Минимальный комплект XDR

Охват наиболее популярных точек проникновения в инфраструктуру: рабочие станции, виртуальные машины, серверы, сеть, почтовый трафик и Threat Intelligence

EDR

Это ключевой элемент XDR. Без EDRне может быть XDR. XDR должен строиться на сильном EDR в синергии с EPP

Буква «X»

«X» в начале сокращенного вариант названия «XDR» означает разнообразие подключаемых источников продуктов

XDR и SIEM

Это не про вытеснение одного из классов решений с рынка, а про их объединение или отличное дополнение друг друга

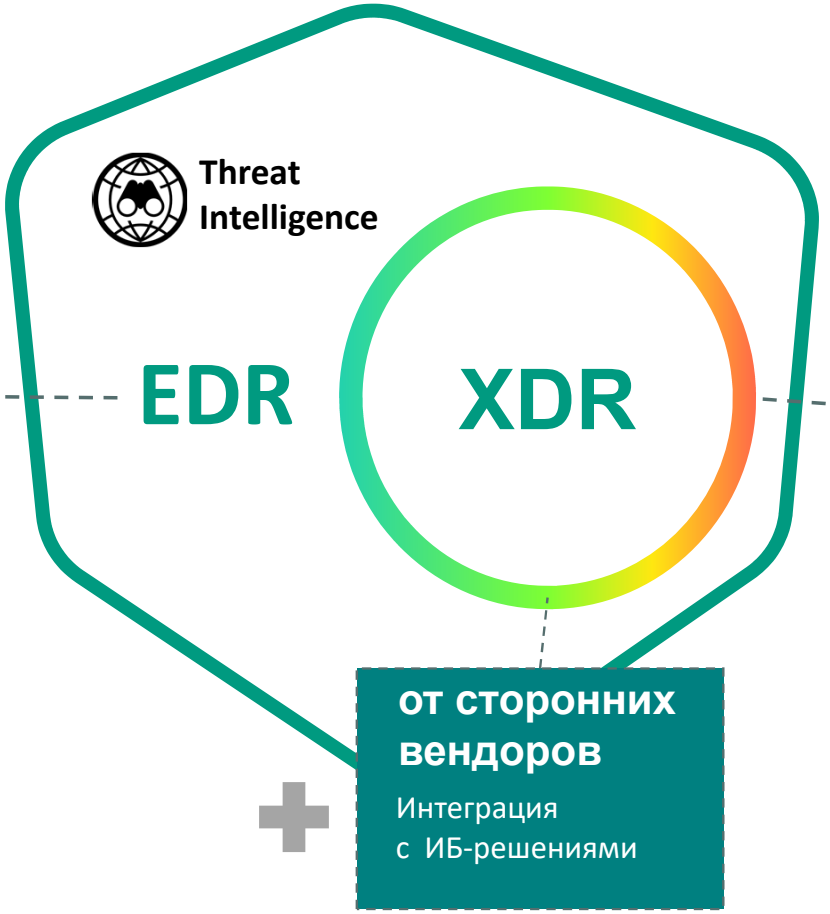
Предпосылки к XDR

Наиболее привлекательные функциональные возможности XDR

Пример состава решения класса XDR

от XDR-вендора
Защита конечных точек

- ПК
- Ноутбуки
- Серверы
- Виртуальные машины
- Различные ОС
- Мобильные устройства



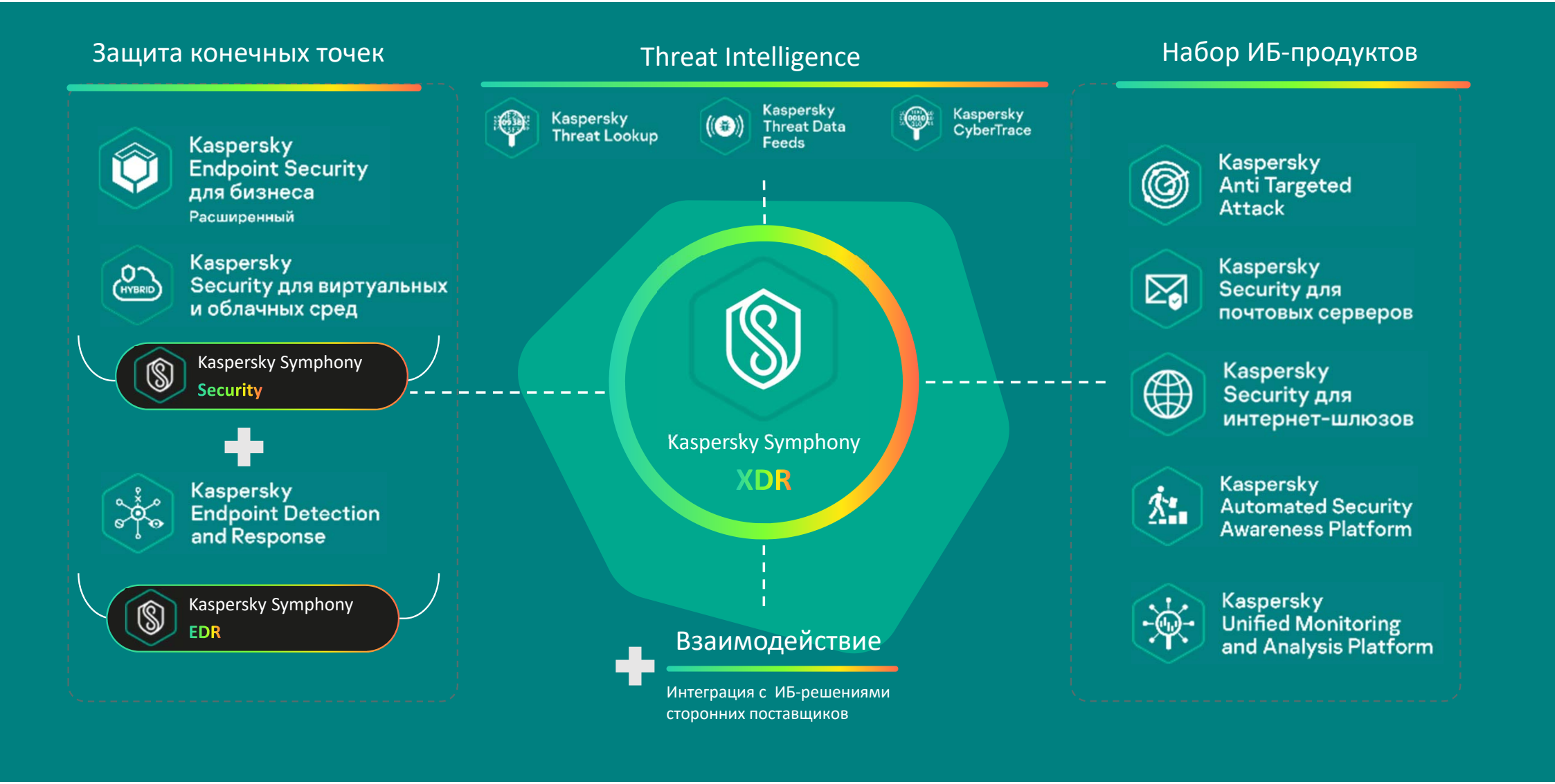
от XDR-вендора
Набор ИБ-продуктов

- Защита сети
- Защита почты
- Защита облаков и контейнеров
- Защита учетных записей
- Повышение осведомленности сотрудников
- Другие ИБ-решения

Kaspersky Symphony XDR: Расширенные возможности защиты

ПОЛИКОМ про

Продуктовый состав Kaspersky Symphony XDR



Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Автоматические

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике

Автоматическая блокировка на уровне почтового шлюза неизвестных вредоносных объектов, обнаруженных детектирующими механизмами KATA (до доставки получателю)

Взаимодействие веб-шлюза и KATA через API для передачи объектов из веб-трафика на проверку в песочницу и последующей их автоматической блокировки в случае выявленной вредоносной нагрузки

Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace

Передача релевантных сложных атакам событий с KATA, KES, KEDR, KSMG, KWTS в KUMA для корреляции с данными от сторонних источников

Передача сырой телеметрии с EDR в KUMA
Реагирование через EDR на найденные угрозы в KUMA

Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя*

Полуавтоматические

Доступ в Threat Lookup для получения дополнительного контекста для эффективного расследования

Построение модели активов в KUMA на основании данных из KSC

Принудительный запуск обновления баз и антивирусной проверки через KSC с карточки инцидента в KUMA

Запуск действий по реагированию через EDR с карточки инцидента в KUMA*

Возможность назначить обучение по повышению киберграмотности из карточки инцидента в KUMA*

Передача информации о произошедших инцидентах в НКЦКИ, благодаря встроенному в решение модулю ГосСОПКА

Сильные стороны Kaspersky Symphony XDR

Kaspersky Symphony XDR

Фокус на конечные точки

Включен EDR в синергии с EPP – они уже защищают более чем 60 миллионов корпоративных рабочих мест по всему миру

Фокус на аналитику об угрозах

Включена признанная лучшей в мире аналитика об угрозах (по результатам Forrester Wave: External Threat Intelligence Services 2021)

Фокус на киберграмотность

Включены модуль контроля и повышение осведомленности рядовых сотрудников

Фокус на взаимодействие

Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии, гибкость сетевой защиты (Netflow, движки KATA, загрузка TI в сторонние инструменты – IDS&APT фиды). Взаимодействие с решениями сторонних поставщиков.

Фокус на соответствие

Помогает обеспечить соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА

Kaspersky Symphony XDR позволяет:

Создать адаптивную систему безопасности, эффективную против кибератак любой сложности

Надежно защитить главные векторы проведения кибератак

Предотвратить или снизить последствия ущерба от продвинутых кибератак

Уменьшить нагрузку на специалистов ИБ за счет удобных инструментов и продуманной автоматизации

Снизить роль человеческого фактора благодаря платформе для повышения киберграмотности

Обеспечить соответствие требованиям законодательства и регулирующих органов

kaspersky
Platinum Partner

Благодарю за внимание!

Руководитель направления решений
«Лаборатории Касперского»
Михаил Усачёв

тел: + 7 (812) 325 84 00
моб: + 7 911 929 60 04

e-mail: Mikhail.Usachev@polikom.ru

ПОЛИКОМ про