Ступенчатый подход к информационной безопасности. Оптимальный уровень защиты

Шаромова Анна

Менеджер по работе с партнерами СФО и ДФО

kaspersky

Ключевые проблемы

Сложные угрозы

Современные угрозы более сложные и требуют продвинутых инструментов

Атака – вопрос времени

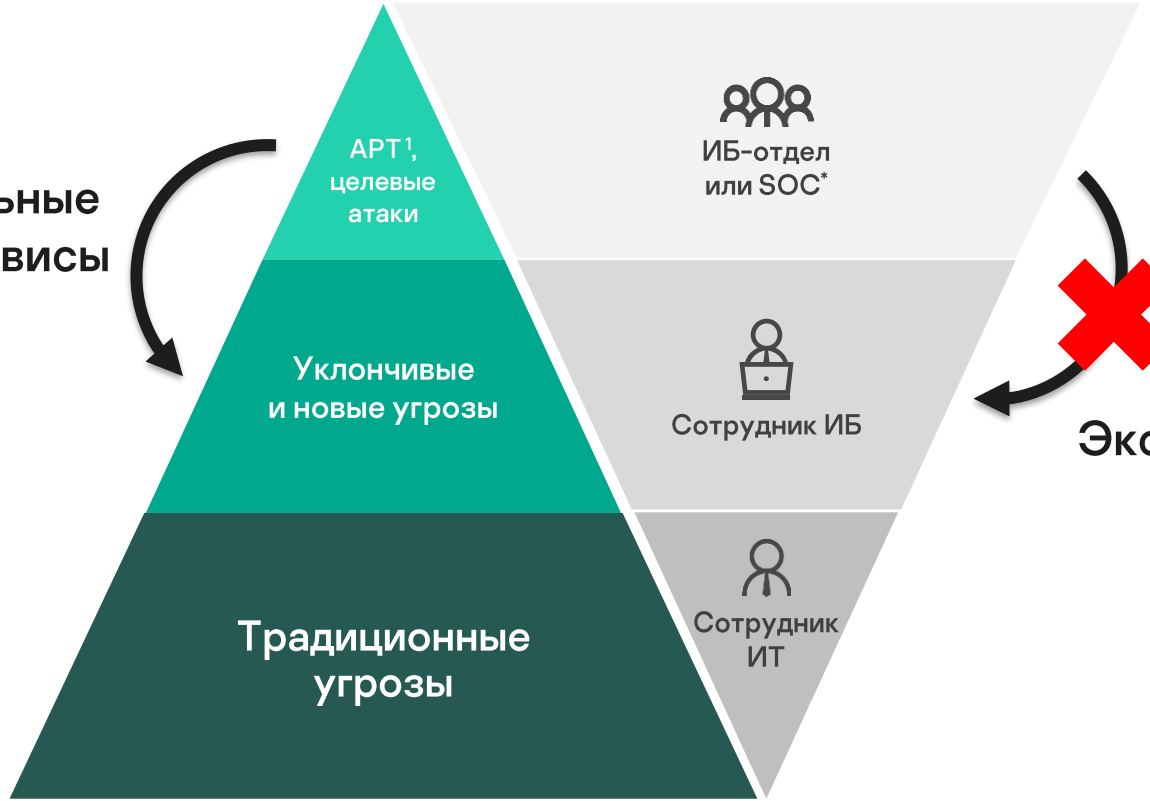
Количество таких угроз возрастает и атаки осуществляются не только на крупные компании

«Растворение» периметра

Роль конечных точек возрастает с увеличением популярности работы вне офиса

Типы атак

Киберкриминальные инструменты и сервисы

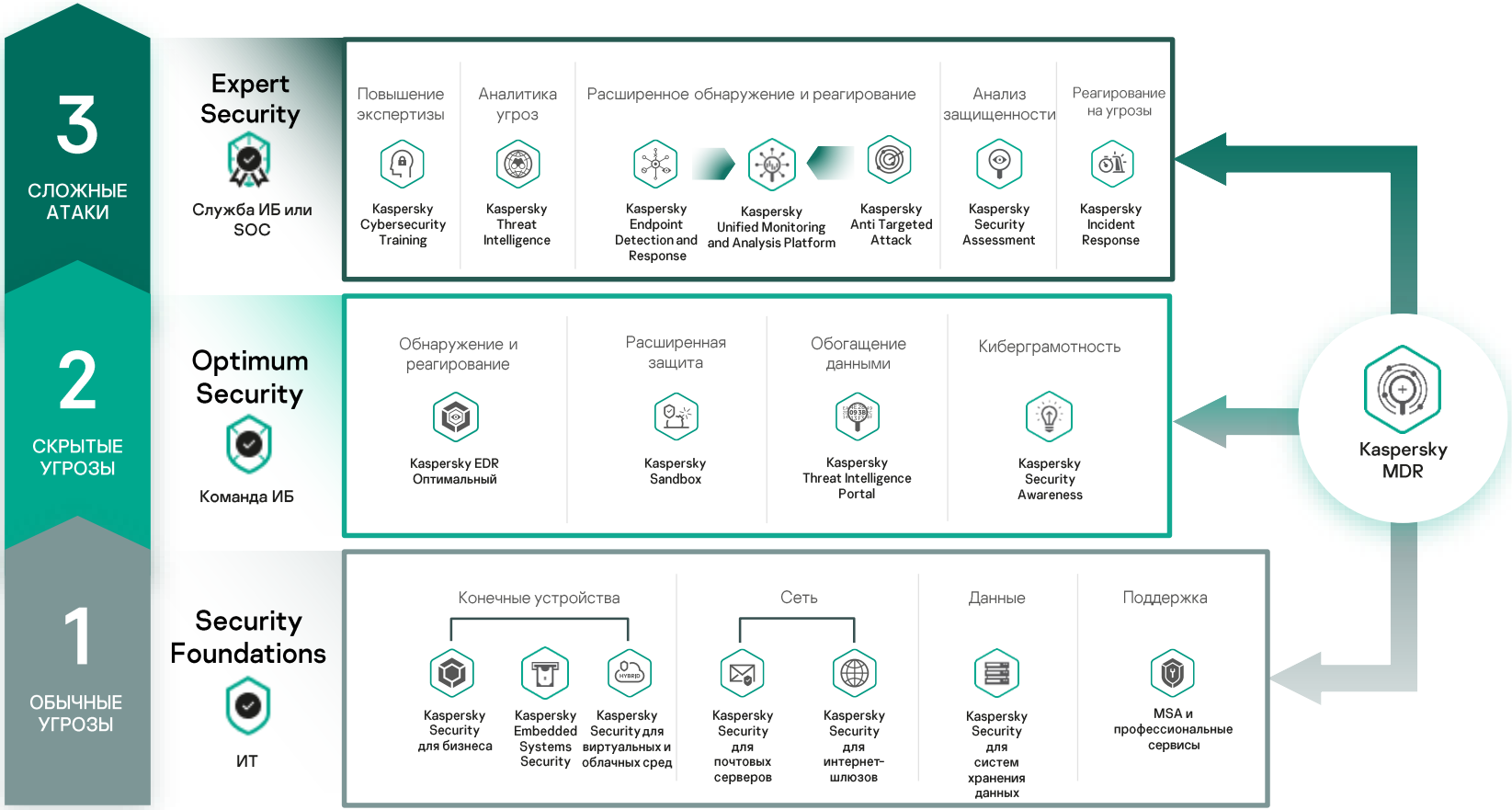


Экспертиза

[1] – Advanced Persistent Threats, целенаправленная устойчивая угроза

*Security Operation Center

Портфолио решений для бизнеса



Конечные точки – самый уязвимый элемент.
Является основной точкой входа в инфраструктуру.
На них приходится порядка 76% атак.
В 84% случаев в инцидент вовлечены более 1 рабочей станции/сервера

Детектирование
Определить масштаб, причины и последовательность атаки

Реагирование
Предотвратить или минимизировать негативные последствия атаки

Экономия ресурсов
Оптимизация загрузки персонала и ресурсозатрат

А вы когда-нибудь задавались вопросами:

Атакует ли меня кто-то прямо сейчас?

Что вредоносная программа успела сделать?

Что бы на моем месте сделали эксперты?

Зачем Иван Васильевич опять открыл незнакомый PDF?

Высокая загрузка ИБ-специалистов

Отчетность

Политики

Сотрудники

Оценка соответствия требованиям

Реагирование на инциденты

Настройка

Инновации

Администрирование

Защита от скрытых угроз на всех этапах атаки

Проникновение

Заражение системы через переход по фишинговой ссылке

Установка

Установка злоумышленниками вредоносных компонентов, связи с сервером управления и изучение среды

Закрепление

Закрепление вредоносного ПО в системе с целью перемещения по сети

Повышение кибер-грамотности сотрудников

Расширенные механизмы обнаружения, включая поведенческий анализ на основе машинного обучения и песочницу

Уменьшение поверхности атаки

Автоматизированный активный поиск угроз с помощью IoA[1]

Анализ первопричин и поиск IoC[2]

Автоматическое предотвращение угроз

Автоматическое, удаленное реагирование и реагирование по инструкциям

1 Indicators of Attack – индикаторы атаки
2 Indicator of Compromise – индикаторы компрометации

Kaspersky EDR для бизнеса Оптимальный

Возможность расследовать скрытые угрозы и предотвратить их в будущем

Прозрачность
Возможность увидеть детали и контекст инцидентов, а также узнать – находитесь ли вы под атакой

Анализ
Возможность определить первопричину угрозы, откуда она появилась и как развивалась

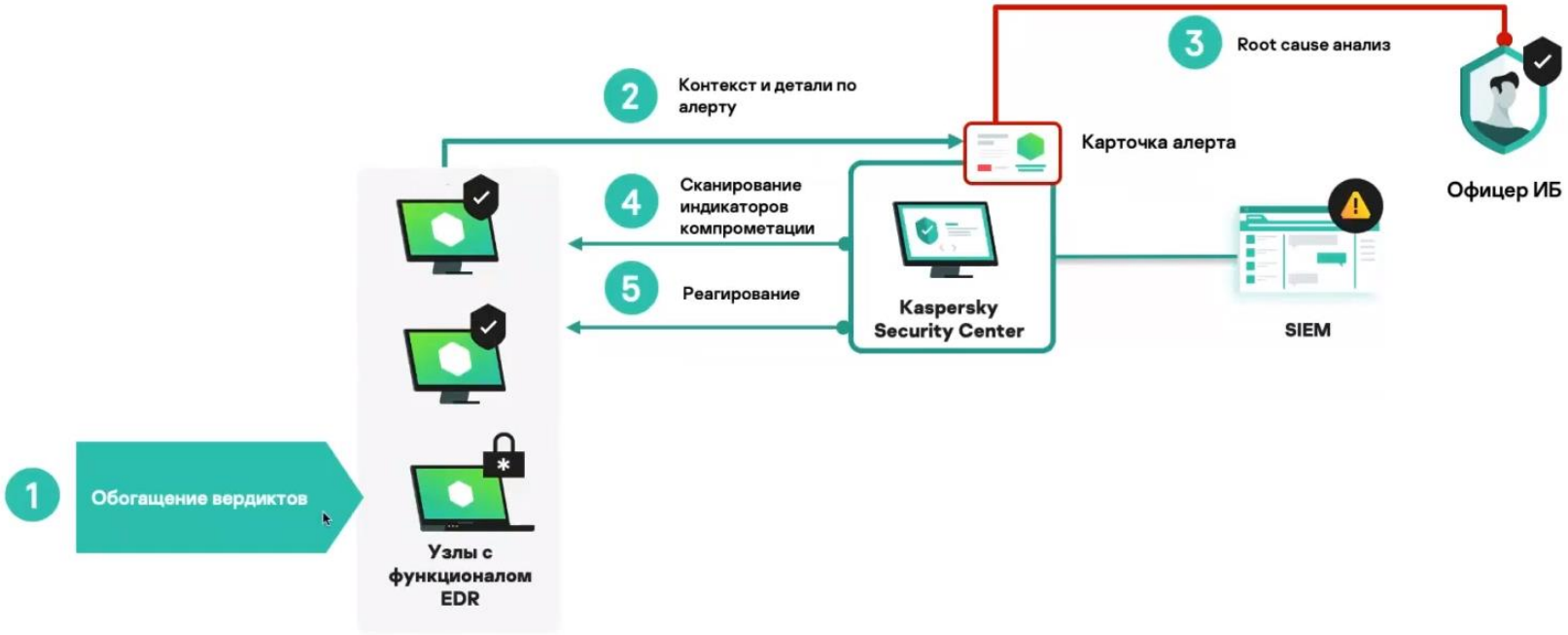
Реагирование
Автоматизация реагирования – «в одно нажатие», или при обнаружении индикатора компрометации

Kaspersky EDR Оптимальный

Возможности:

- Простота в установке и использовании
- Обогащение обнаружений KES для возможностей расследования
- Функции реагирования на инциденты
- Реагирование в один клик

Архитектура решения



Kaspersky Sandbox

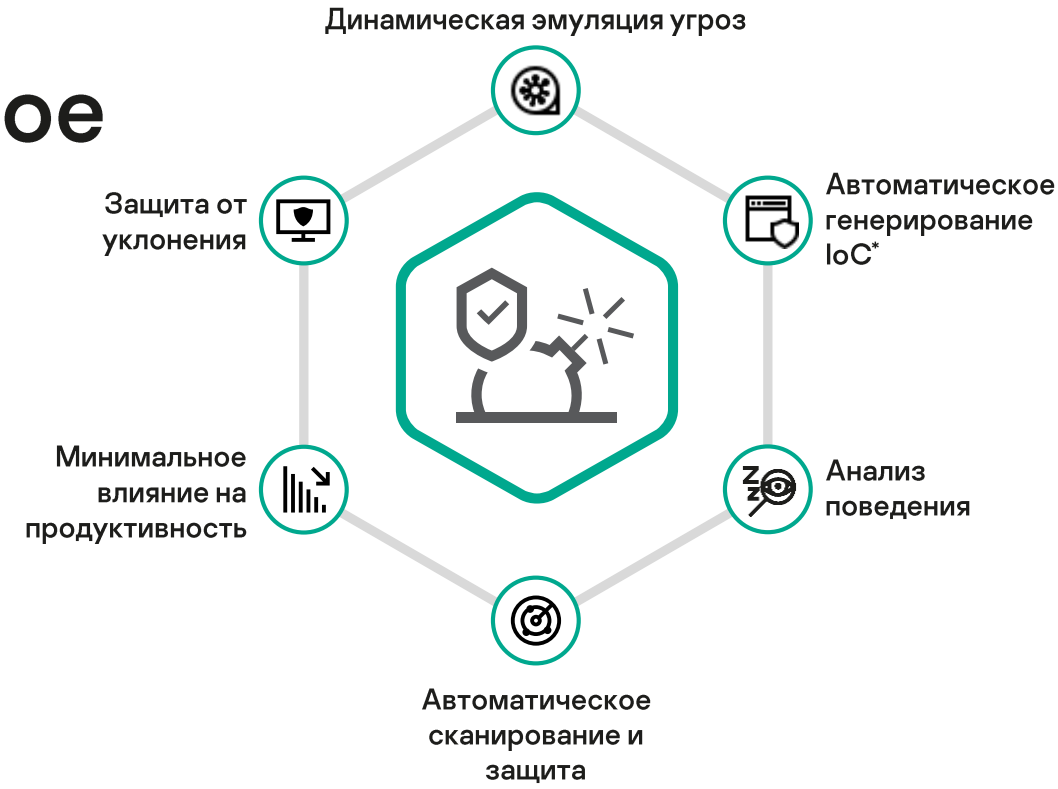
Автоматическое детектирование и устранение скрытых угроз

Динамический анализ
Детектирование скрытых угроз за счёт их детонирования в изолированной среде и анализа поведения

Надежная защита
Вредоносное ПО не поймёт, что находится в песочнице – за счёт использования патентованных технологий

Простота
Автоматизация управления и детектирования позволяет улучшить безопасность – без лишних сложностей

Автоматическое обнаружение сложных угроз



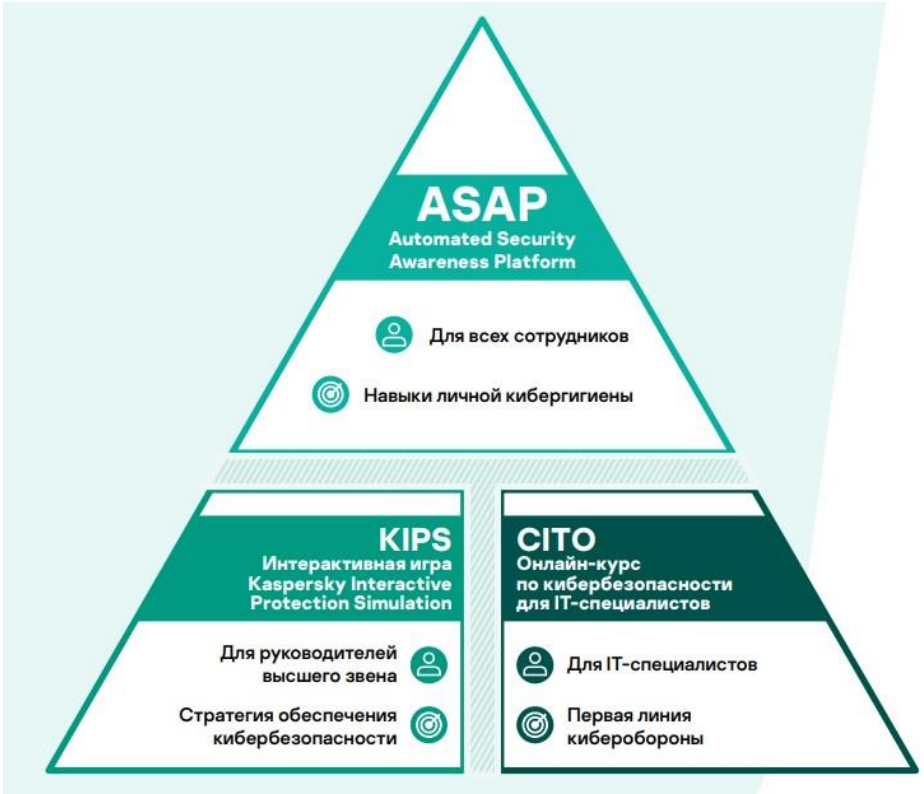
* Indicators of compromise – индикаторы компрометации

Kaspersky Sandbox

- Дополняет Kaspersky Endpoint Security новыми сценариями обнаружения новых и целевых угроз без ущерба для производительности рабочих станций
- Экономия трудозатрат специалистов ИБ для решения более важных задач и сложных угроз
- Решение не требует дополнительных инвестиций в экспертизу персонала
- Возможность интеграции со сторонними решениями через RESTful API позволит достичь максимальной эффективности решения в комплексных системах ИБ клиентов

Kaspersky
Security
Awareness

Повышение ИБ-осведомленности сотрудников



Последовательное усиление защиты конечных точек

Kaspersky Security для бизнеса Расширенный
надежная защита конечных точек

- Анализ поведения
- Машинное обучение
- Адаптивный контроль рабочих мест
- Оценка уязвимостей и установка обновлений

Kaspersky EDR для бизнеса Оптимальный
+ базовый функционал EDR

- Понимание масштаба инцидента
- Root cause анализ
- Поиск индикаторов компрометации
- Автоматизированное реагирование на атаки

Kaspersky Total Security Plus для бизнеса
+ песочница
+ email, web, MSA

- Автоматическое обнаружение уклончивых угроз
- Патентованная технология эмуляции угроз
- Защита email и web

Давайте обсудим

kaspersky