Kaspersky Symphony MDR

Безопасность как искусство

kaspersky

Ежегодно

Усложняется ландшафт угроз,
киберпреступники совершенствуют свои методы

Расширяется поверхность атаки
и количество точек входа злоумышленников

Усиливаются требования регуляторов,
особенно в отношении обеспечения защиты КИИ

+ Добавилось

Наступила эра хактивизма
и целевой киберагрессии

Больше лазеек
из-за полного ухода ИБ-вендоров или приостановки обновлений их решений

Началась активная фаза
информационного суверенитета

Актуальные ИБ-задачи

Противодействие всем видам угроз в киберагрессивной среде

ИБ-замещение ушедших поставщиков в короткие сроки

Соответствие усиливающимся требованиям регуляторов

Что делать компаниям в новых ИБ-реалиях? Как решать актуальные ИБ-задачи?

1

В первую очередь защититься от массовых угроз

2

Во-вторых выстроить защиту от сложных угроз

Самостоятельно: постепенно или сразу

Выбрать управляемую защиту

О Kaspersky Symphony

Почему Symphony?

Кибербезопасность в виртуозном исполнении:

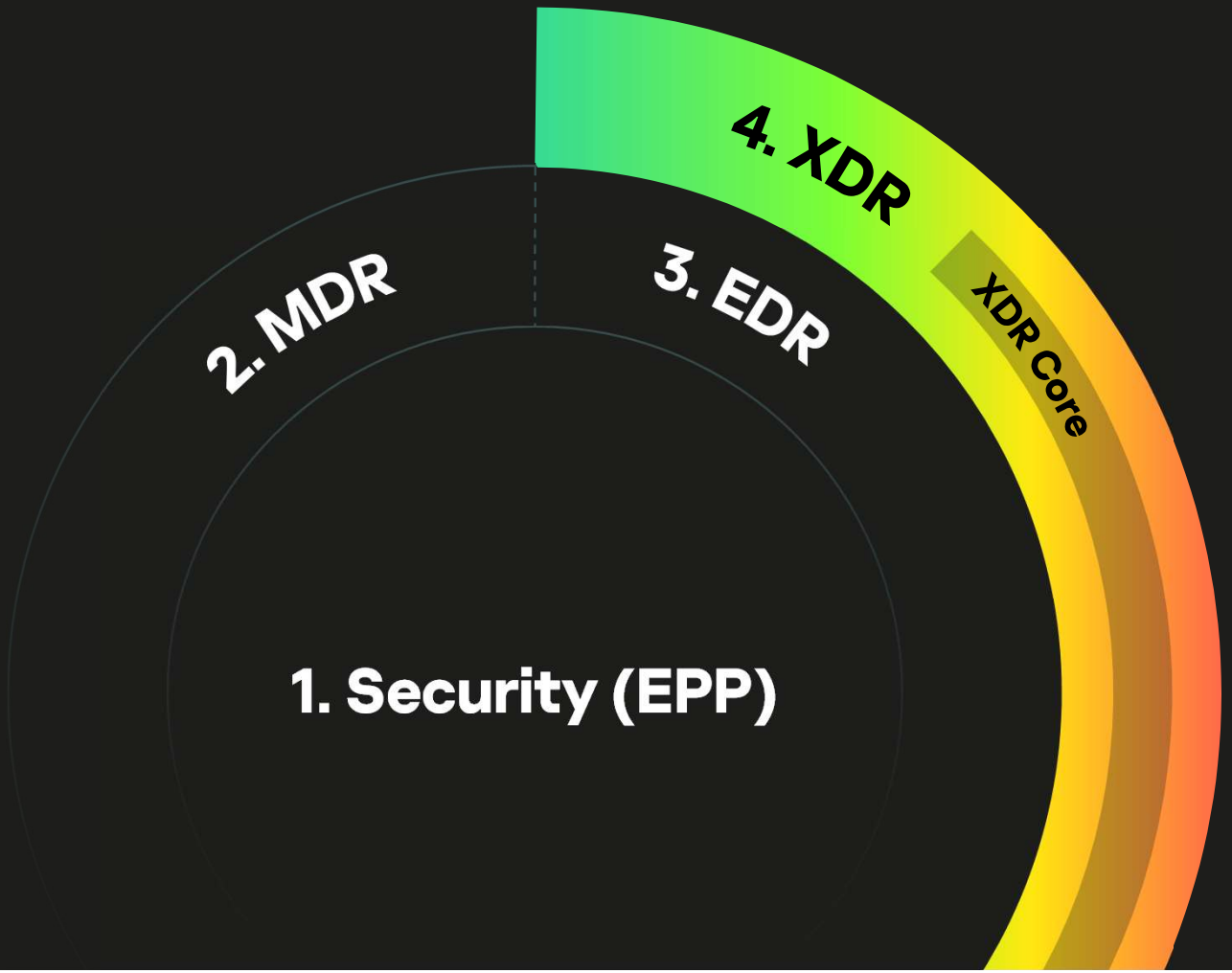
Когда все защитные решения действуют, как слаженный оркестр

Когда все инструменты идеально настроены

Когда есть всё, чтобы уверенно и просто дирижировать системой безопасности

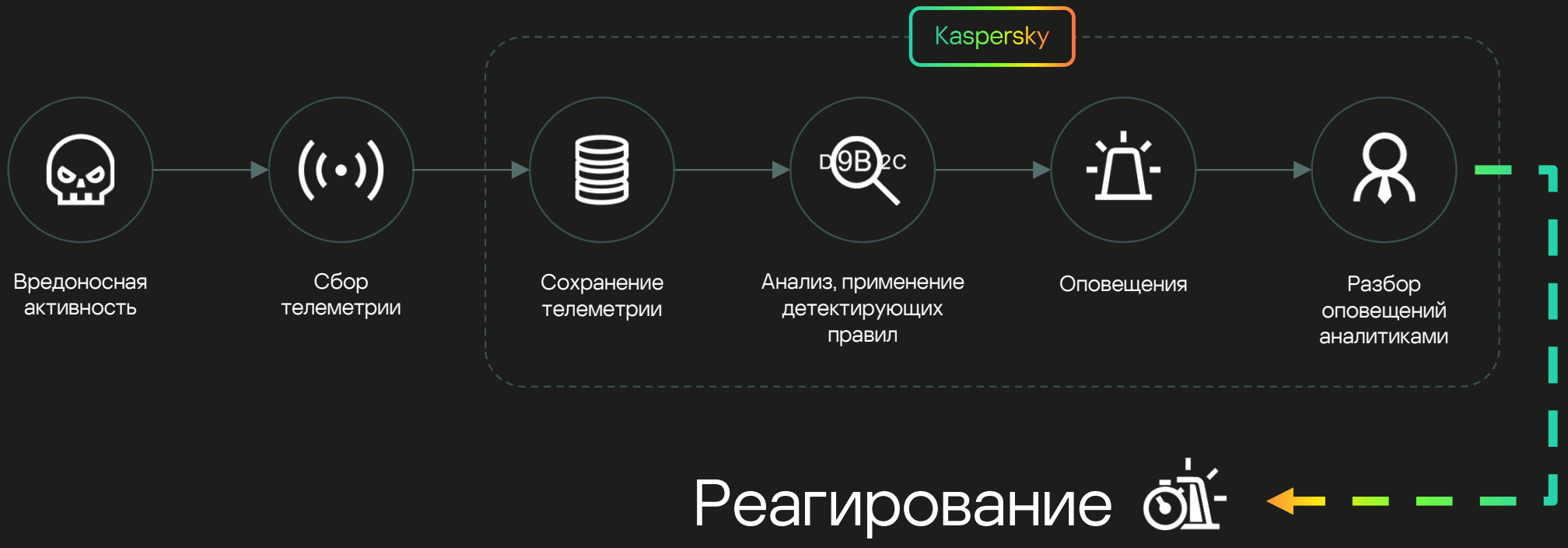
Гибкий выбор

- Kaspersky Symphony XDR
  - XDR Core
- Kaspersky Symphony MDR
- Kaspersky Symphony EDR
- Kaspersky Symphony Security



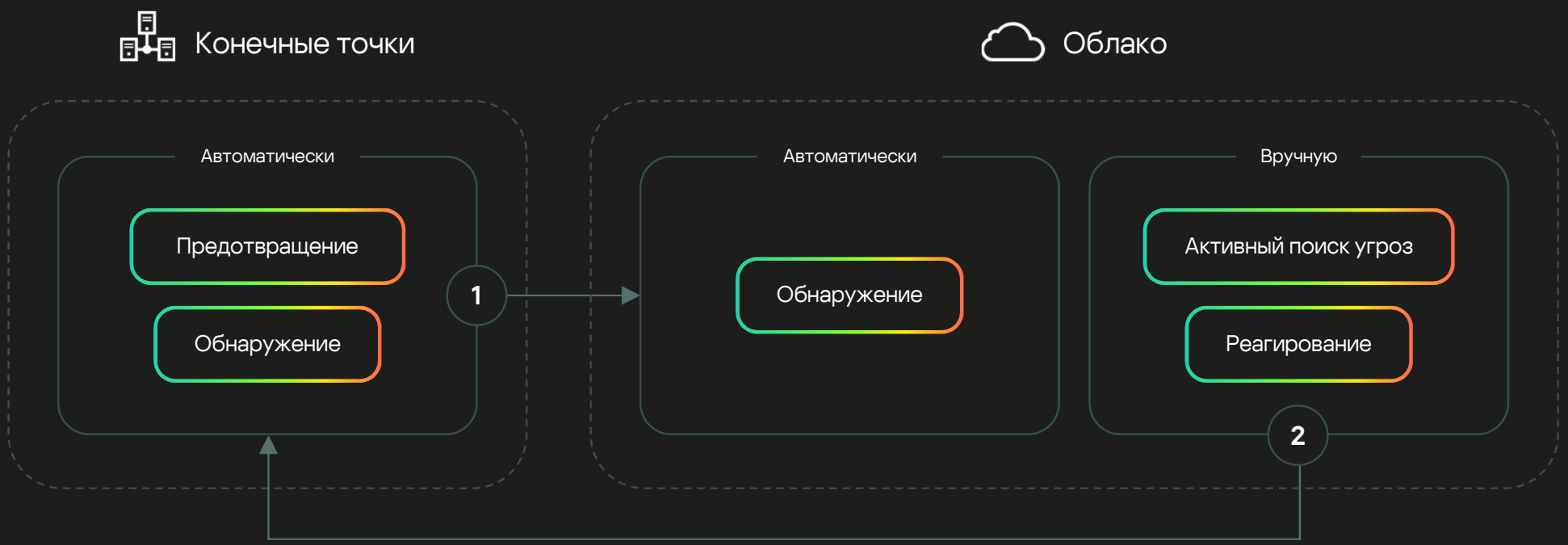
Kaspersky Symphony MDR

Управляемая защита, охота за угрозами: Kaspersky Symphony MDR



Предоставление рекомендаций по реагированию
и удаленное реагирование

Многоуровневая архитектура Kaspersky Symphony MDR



1 **Телеметрия** Стандартные события безопасности EDR. Точные и неточные детекты EPP-решения

2 **Реагирование** Стандартные меры реагирования EDR. Обновление детектов EPP-решения

Телеметрия

События файловой системы

Создание, модификация файлов

События создания процессов

Запуск процесса, инъекции в процессы, загрузка секции, и т.п.

Сетевые события

Соединение, DNS запросы, HTTP-запросы, загрузка файлов по HTTP, email, и т.п.

Специфичные для ОС

Реестр, события журналов , WMI и т.п.

События с хостовых средств защиты

Детекты AM-движка

События об обнаружении закрепления

~ autoruns

Служебные события

Пример. Поля события создания процесса


```
"processcmdline": "\"C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\PowerShell.exe\" -NoLogo
"processfilemd5": "0x234B54B8BB71EF6D13BDB51A6C464CD9",
"processfilepath": "c:\\windows\\ccm\\systemtemp\\84c17278-7077-4826-96fd-ae3ad25d3305.ps1",
"processlogonsessionid": "0x85FA3",
"processlogontype": 2,
"processpid": 10000,
"processuniquepid": "0xDB0702CF60C5AEC3",
"processuserid": "S-1-5-21-1430328663-2098613005-1233803906-143945",
"processversioninfodescription": "Windows PowerShell",
"processversioninfooriginalfilename": "PowerShell.EXE",
"processversioninfoproductname": "microsoft\u00ae windows\u00ae operating system",
"processversioninfovendorname": "Microsoft Corporation",
"productinfo": "kes 11.3.0.773 Windows 10 RS5 x64",
"statsource": 1,
"storageaddedfiletype": 2,
"type": "aps",
"user_description": "mdr_iro23",
```

Обогащение телеметрии

Телеметрия

Телеметрия обогащается аналитикой угроз из разных источников

KSN
Kaspersky Security Network

GREAT
Центр глобальных исследований и анализа угроз

Kaspersky Threat Intelligence

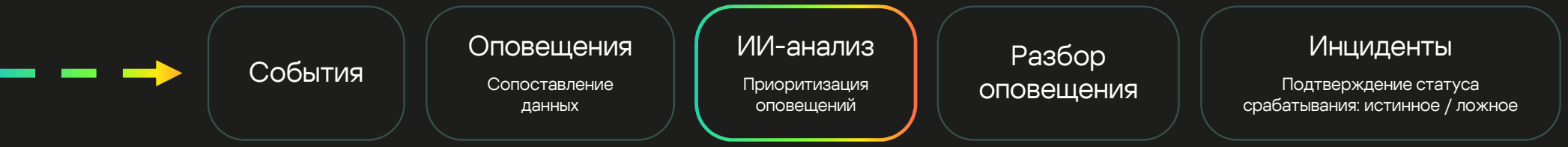
GERT
Международная группа реагирования

IoA
Правила автоматического поиска угроз

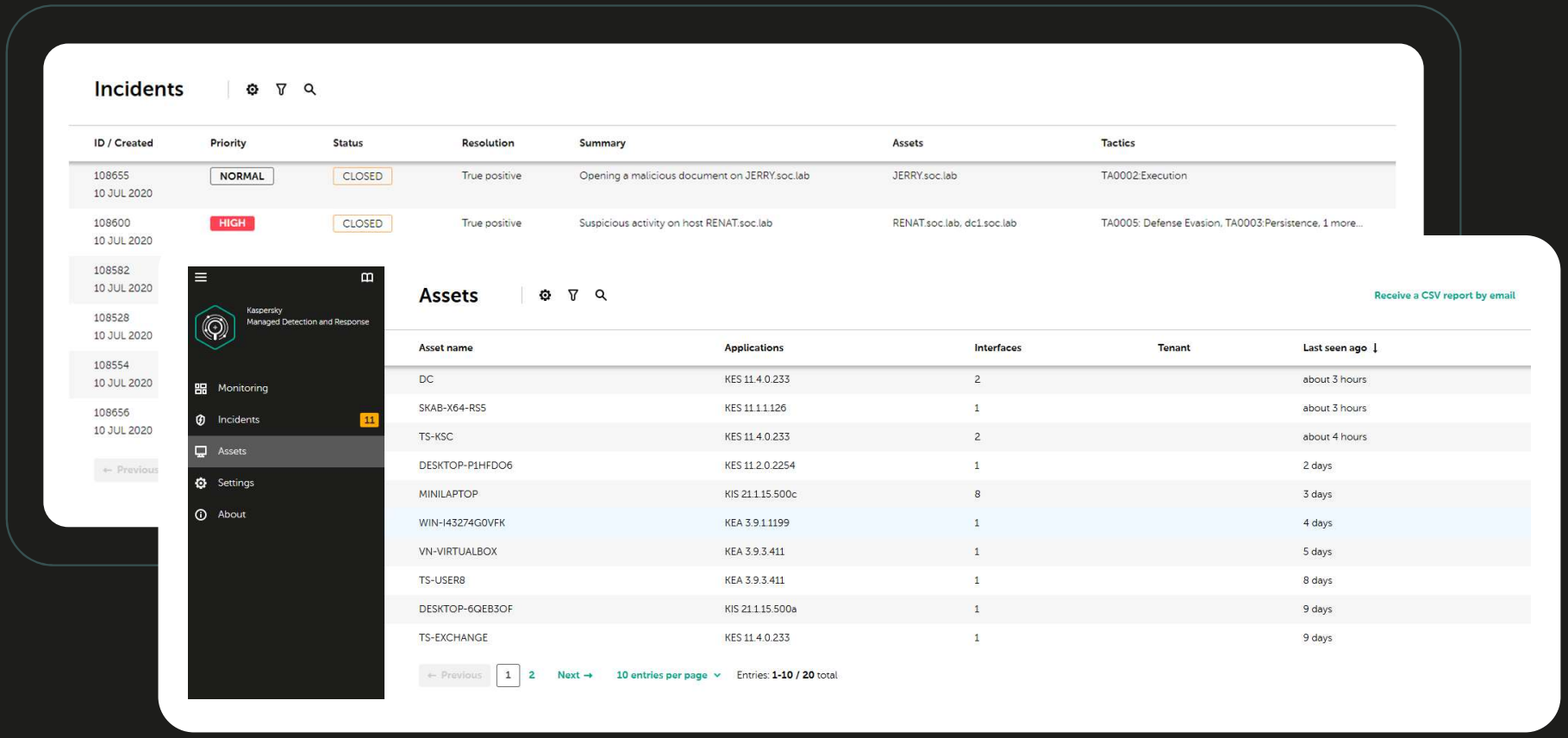
Kaspersky ICS CERT

Kaspersky Symphony MDR

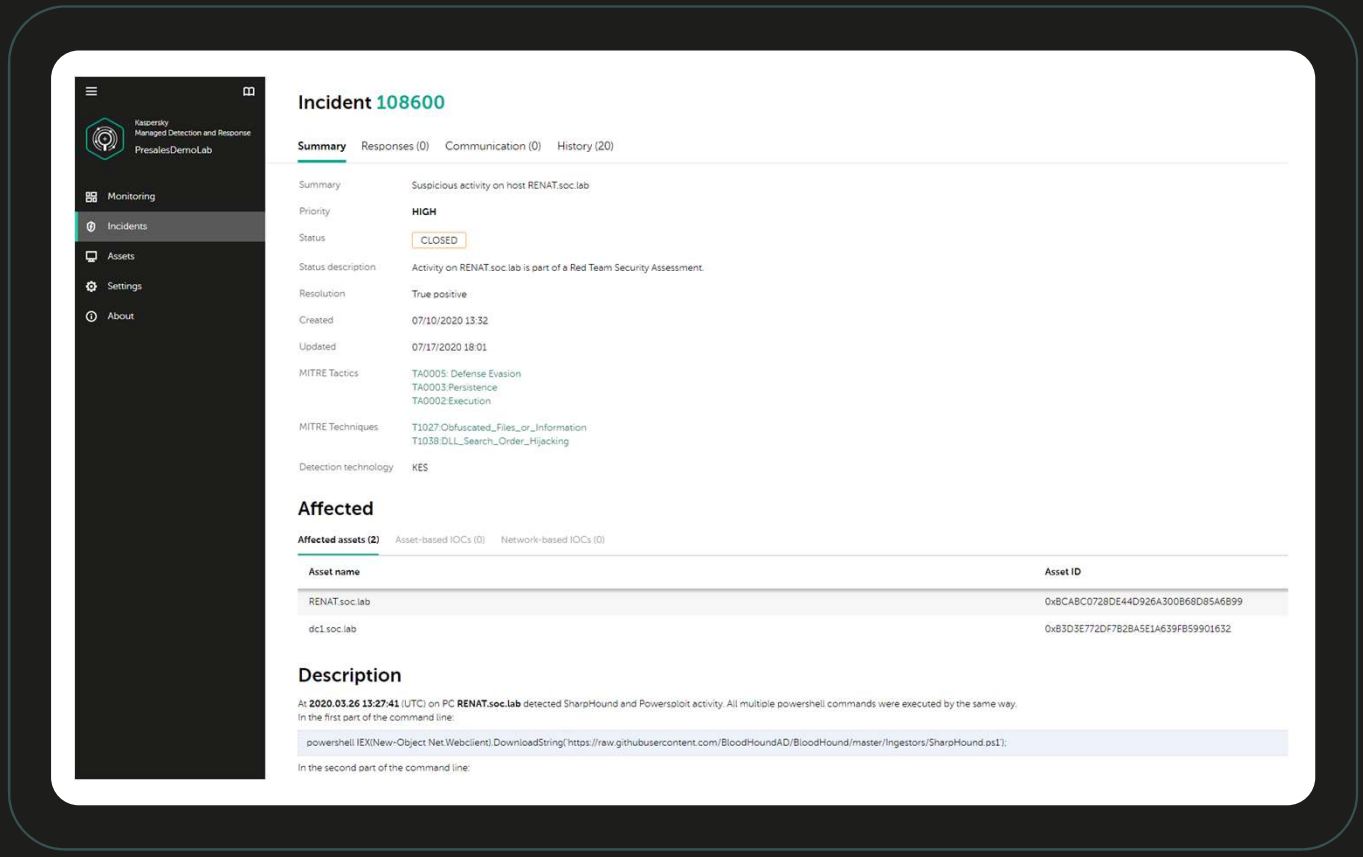
Механизмы ИИ автоматически фильтрует ложноположительные срабатывания, значительно повышая производительность аналитиков.
В результате уменьшается среднее время на приоритизацию и на обнаружение и реагирование — MTTD / MTTR



Интерфейс MDR



Интерфейс MDR



Состав Kaspersky Symphony MDR

Kaspersky Symphony MDR

- **Kaspersky Endpoint Security для бизнеса**
  Расширенный
- **Kaspersky Security для виртуальных и облачных сред**
- **Kaspersky EDR для бизнеса**
  Оптимальный
- **Kaspersky Managed Detection and Response**

Kaspersky Symphony MDR

Круглосуточный мониторинг

Автоматический поиск угроз

Сценарии реагирования и автоматическое реагирование на инциденты

Обзор всех защищаемых ресурсов с их текущим статусом

Консоль управления с панелями мониторинга и аналитическими отчетами

Хранение истории инцидентов безопасности в течение 1 года

Хранение необработанных данных в течение 1 месяца

Консультации аналитиков SOC «Лаборатории Касперского»

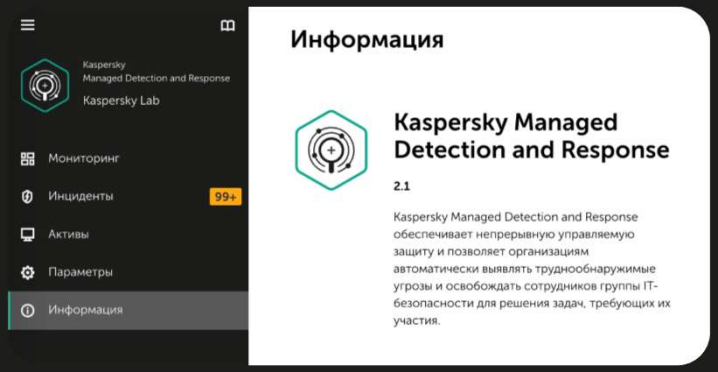
Поддерживаемые платформы

Platforms

Windows Desktops	Kaspersky Endpoint Security for Windows	Kaspersky Security for Virtualization Light Agent
Windows Servers	Kaspersky Security for Windows Servers	
Mac OS Machines	Kaspersky Endpoint Security for Mac	
Linux Machines	Kaspersky Endpoint Security for Linux	

Managed Detection and Response — Метрики Соглашения об уровне сервиса (SLA)

Уровень критичности	Время реакции	Целевой показатель
High (Человек или большое влияние)	1 ч	90%
Medium (ВПО, нет подтверждения Человека)	4 ч	90%
Low (ПНПО (PUP), малый риск)	24 ч	90%



Время с момента автоматического обнаружения the (время createdAt алерта) до публикации на портале MDR/API (время publishedAt инцидента)

Доля количества инцидентов, для которых выполняется метрика SLA

Включает EPP-решение (Kaspersky Symphony Security) для защиты всех видов хостов

Включает базовые EDR-возможности (EDR Оптимальный) для самостоятельного контроля

Управление из Kaspersky Security Center

Больше автоматизации для стандартных сценариев

Более 1000 индикаторов атак (IoA)

Выделенная команда экспертов мирового уровня

Преимущества использования Kaspersky Symphony MDR

Уверенность в том, что вы находитесь под постоянной защитой

Сокращение расходов из-за отсутствия необходимости нанимать ИБ-специалистов

Возможность пользоваться преимуществами центра SOC, не имея его внутри компании

Почему «Лаборатория Касперского»

Экспертиза мирового уровня

~ 5 000

высококвалифицированных специалистов

50%

наших сотрудников — R&D-специалисты

35+

ведущих мировых экспертов в области кибербезопасности

7

уникальных центров экспертизы

Kaspersky: цифры говорят больше слов

>400 млн

Пользователей используют наши защитные решения

>220 тыс.

Компаний по всему миру мы оберегаем от киберугроз

>400 тыс.

Уникальных вредоносных объектов мы обнаруживаем ежедневно

>200

Крупных APT-группировок отслеживается нами

Стратегический партнер по кибербезопасности

Глобальный охват и международное признание

Доказанная эффективность технологий

Прозрачность и соответствие стандартам

Опыт и знания мирового уровня

Высокий статус в индустрии ИБ

Более 25 лет безупречной работы

Спасибо!