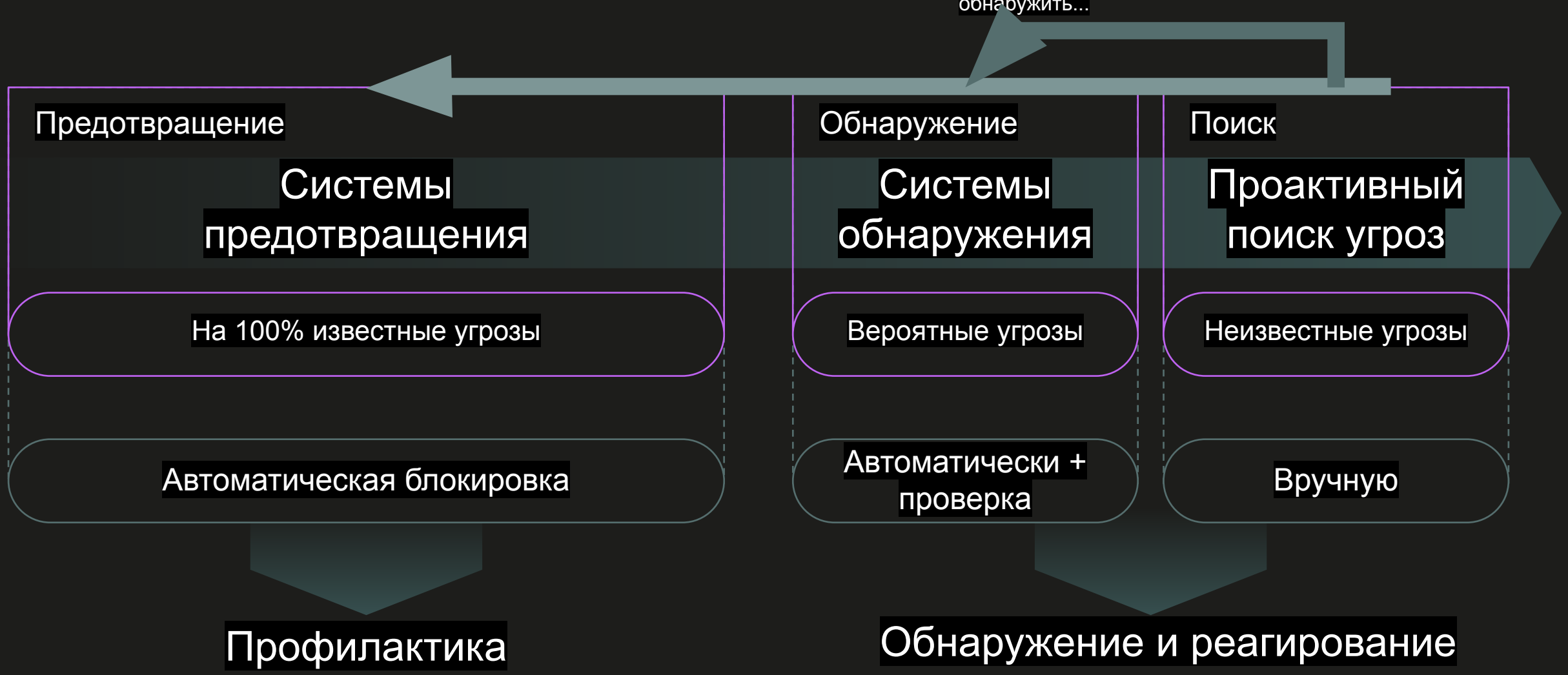
# Kaspersky MDR

# Атаки становятся более изощренными и разрушительными

- Рост количества угроз
- Усложнение сценариев атак
- Финансовый ущерб от атак
- Нехватка квалифицированных специалистов
- Неспособность своевременно обрабатывать оповещения

# Общий подход к эффективной IT-безопасности





# Обзор Kaspersky Managed Detection and Response



## Известные угрозы

- Блокировка или автоматическое обнаружение угроз

Продукты, оповещения

КОМПРОМЕТАЦИЯ

## Неизвестные угрозы

- Выявление сложных
- угроз
- Расследование

Поиск киберугроз

## Сдерживание угроз

- Реагирование и пошаговые рекомендации

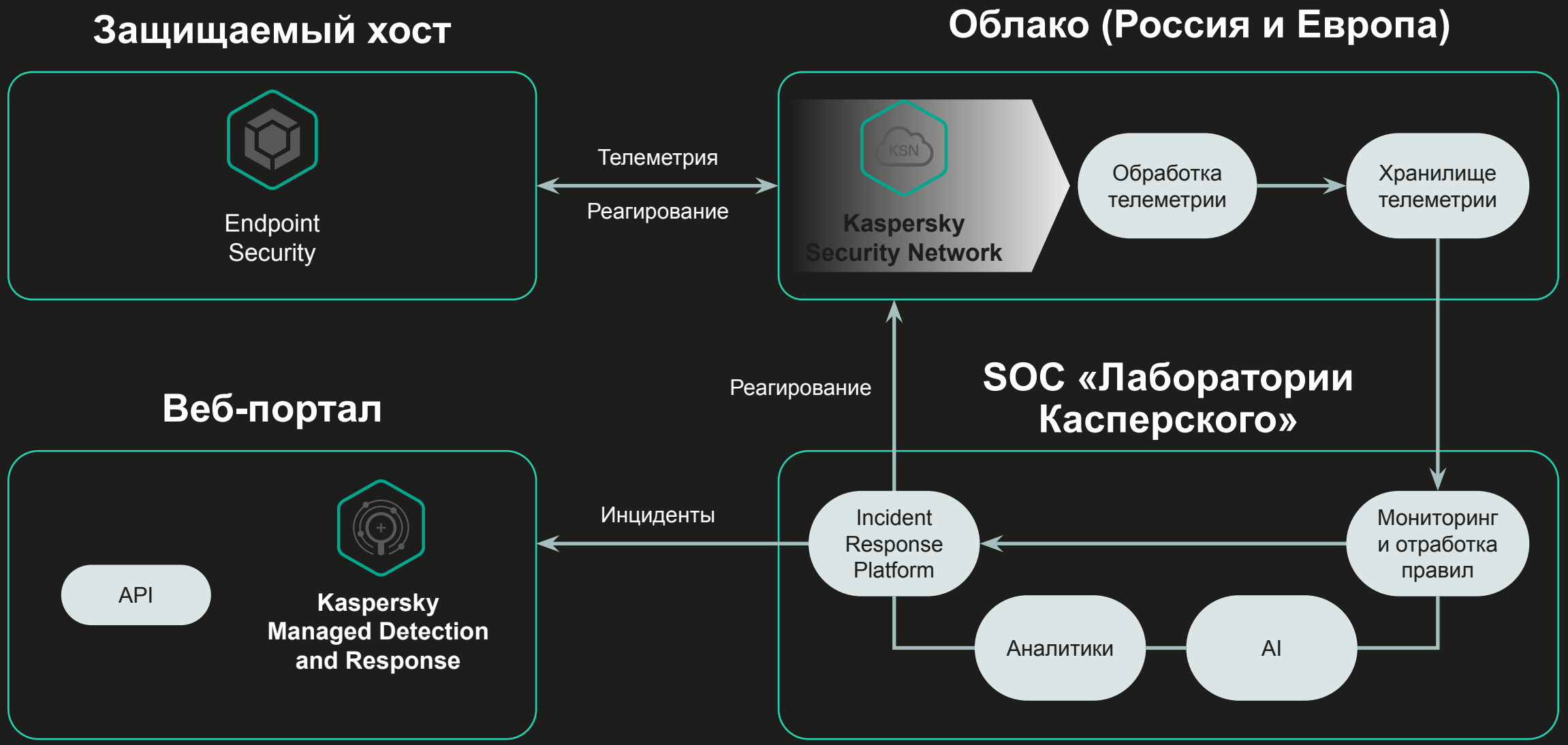
Реагирование на инциденты

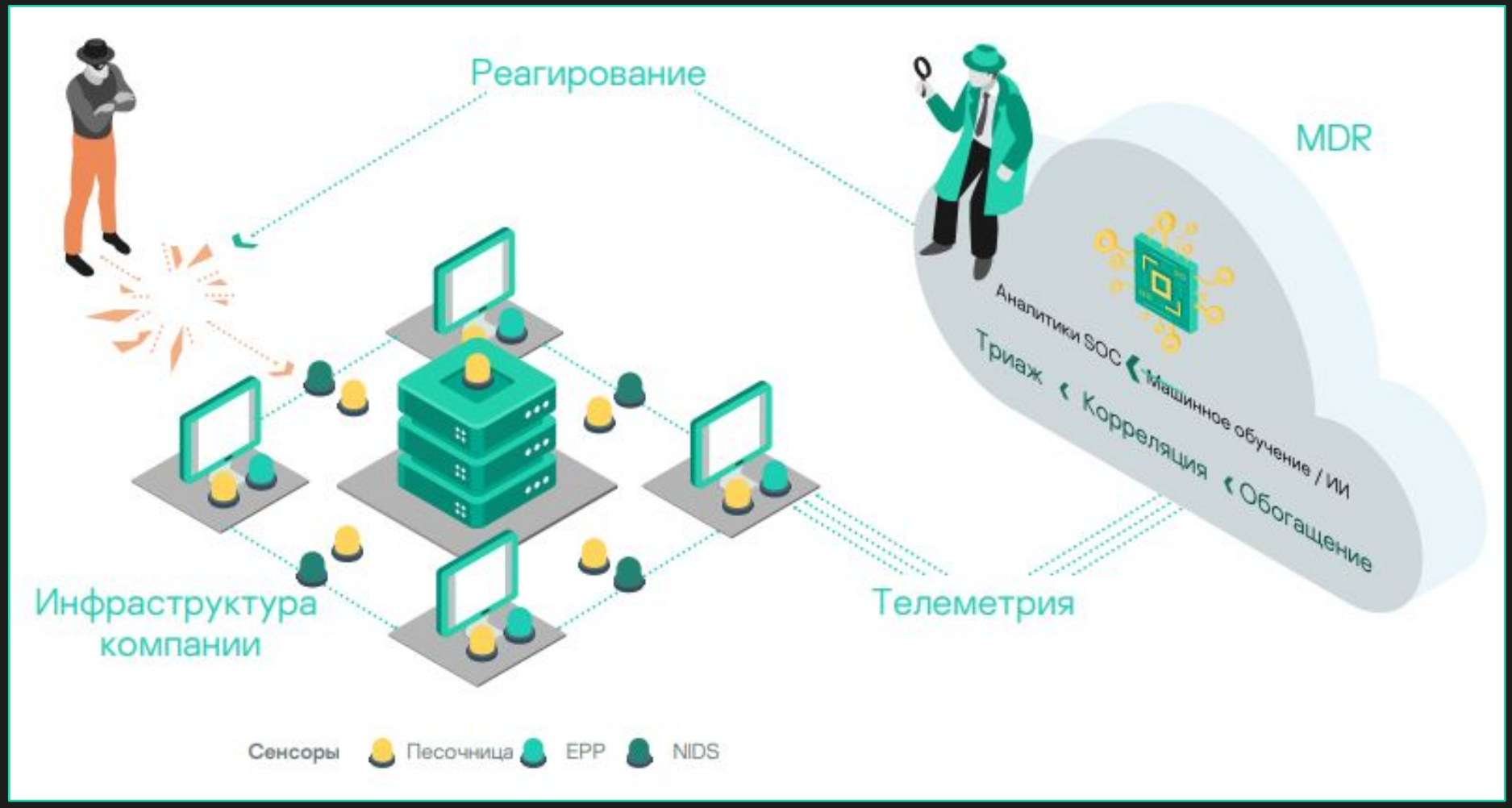
До компрометации

После компрометации

В
р

## Сервисная архитектура




Реагирование
MDR
Аналитики SOC
Машинное обучение / ИИ
Триаж
Корреляция
Обогащение
Инфраструктура компании
Телеметрия
Сенсоры
Песочница
EPP
NIDS

# Обогащение телеметрии



# Более 700 правил автоматического поиска угроз/индикаторы атак (IoA)

- Каждое правило создано экспертами из нашего SOC
- Правила основаны на нашей аналитике угроз и базе знаний MITRE ATT&CK
- Правила регулярно обновляются на основе информации наших аналитических служб

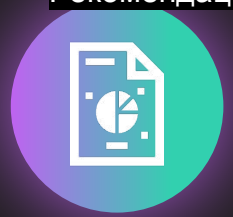
# Технические детали

# Анатомия MDR



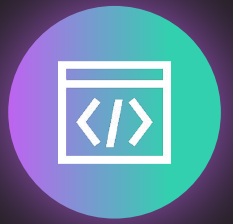
## Технологии обнаружения и поиск угроз

- Защита от вредоносного ПО на основе машинного обучения
- Поведенческий анализ
- Анализ сетевого трафика
- Расширенная песочница
- Индикаторы атак (IoA)
- Сопоставление с данными MITRE ATT&CK
- Автоматизированный активный поиск угроз
- Управляемый активный поиск угроз силами экспертов «Лаборатории Касперского»
- Рекомендации аналитиков SOC «Лаборатории Касперского»



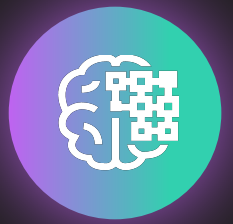
## Полная прозрачность (единая консоль)

- Управление доступом на основе ролей
- Уведомления об
- инцидентах
- Карточки инцидентов
- Карточки ресурсов
- Панели мониторинга и отчеты



## Рекомендации по реагирование на инциденты

- Изоляция хоста
- Помещение файлов в карантин
- Удаление файлов
- Завершение процессов
- Запрос файлов с хоста
- Запуск программы на хосте
- Реагирование через рекомендации и пр.



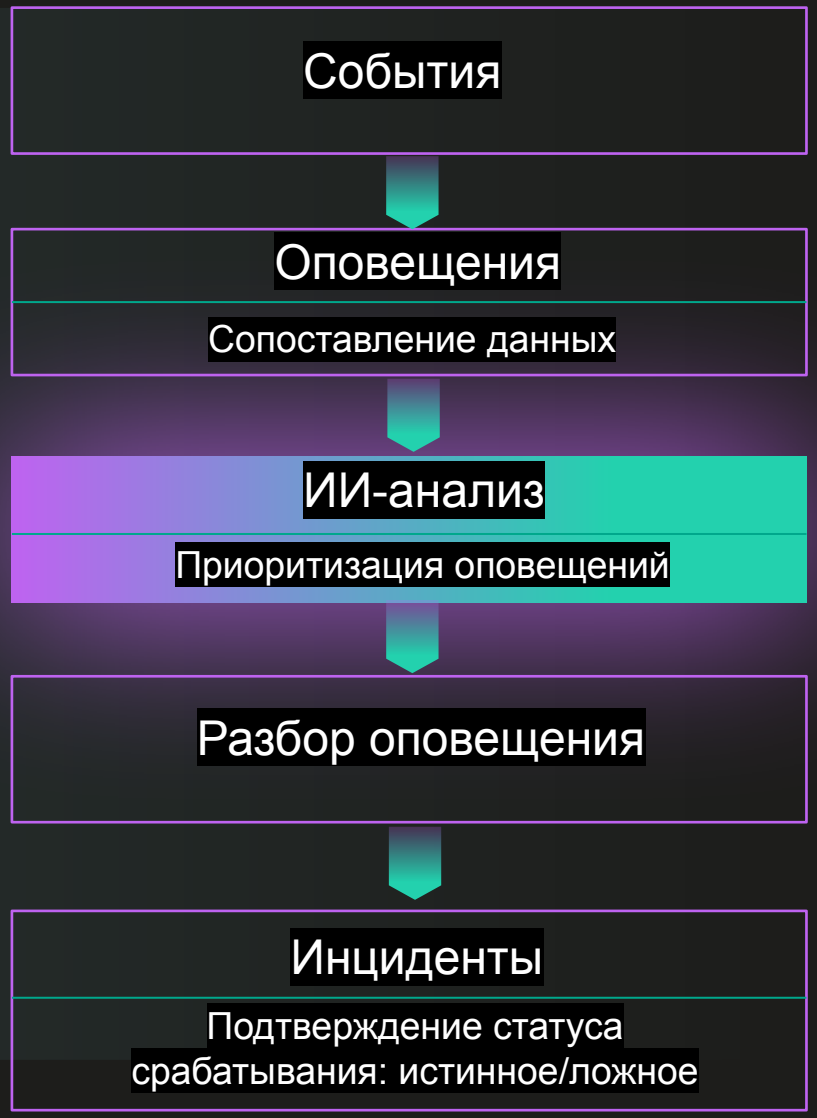
## Машинное обучение и ИИ-помощник

- Обнаружение
- Оценка
- Фильтрация
- Приоритизация

# Механизмы искусственного интеллекта (ИИ) в Kaspersky 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



# Уровни защиты Kaspersky MDR



## Optimum

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Рекомендации по реагированию и удалённое реагирование на инциденты
- Проверка работоспособности всех защитных механизмов и обзор защищаемых ресурсов
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанных данных в течение 1 месяца

Kaspersky
Managed Detection
and Response

Дополнительно:

- **ГИБКИЕ ВОЗМОЖНОСТИ**
  хранения данных для соответствия нормативным требованиям и поддержки цифровой криминалистики
- **СЕРВИС ПО РЕАГИРОВАНИЮ**
  на инциденты разной степени сложности
- **ОЦЕНКА КОМПРОМЕТАЦИИ**
  и проверка эффективности текущей защиты
- **ПРАКТИЧЕСКИЕ ТРЕНИНГИ**
  для ИБ-экспертов по реагированию на инциденты

## Expert

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Рекомендации по реагированию и удалённое реагирование на инциденты
- Проверка работоспособности всех защитных механизмов и обзор защищаемых ресурсов
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года

**ТОЛЬКО В EXPERT**

- Хранение необработанных данных в течение 3 месяцев
- Проактивный поиск угроз (threat hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Доступ к порталу Kaspersky Threat Lookup
- API для загрузки данных

# Принцип работы Kaspersky MDR Expert



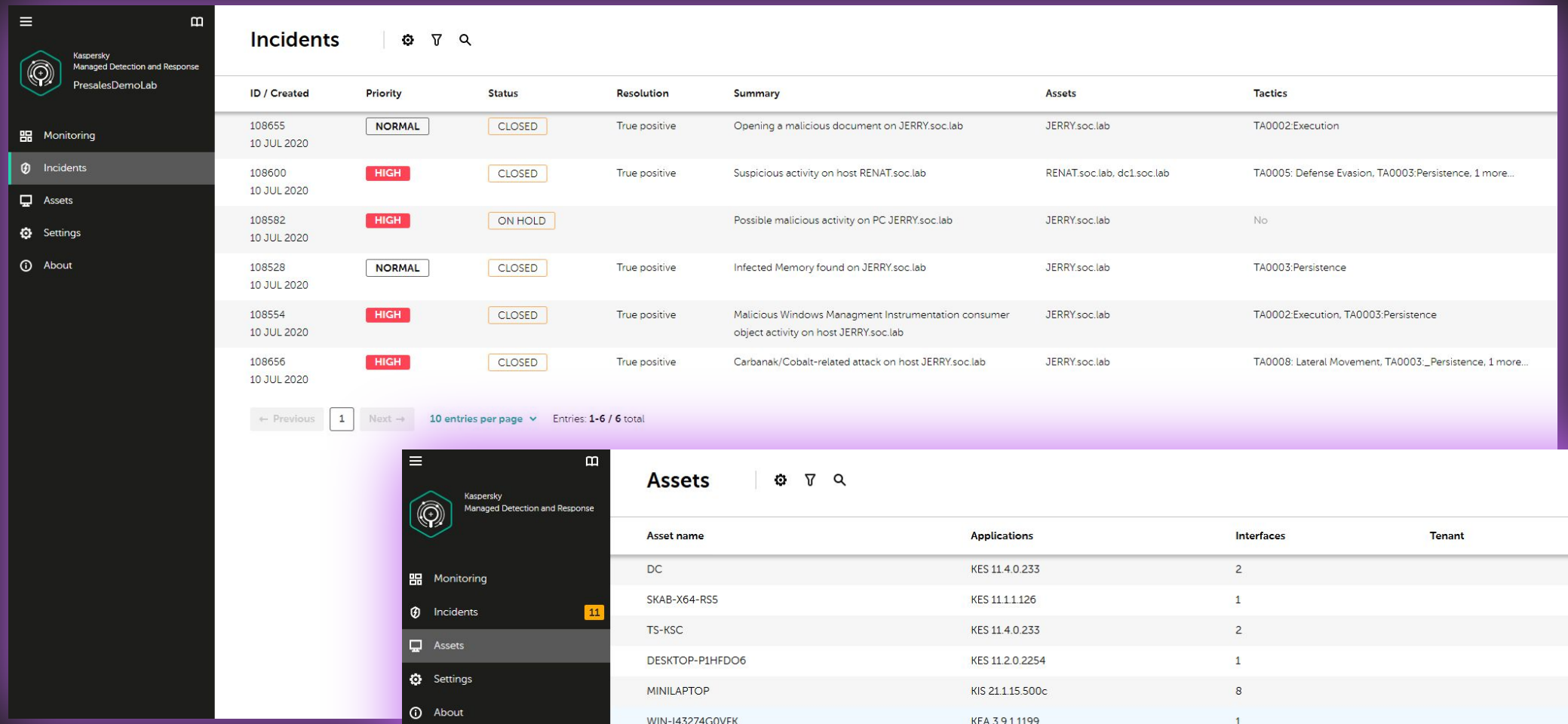
# Интерфейс Kaspersky MDR

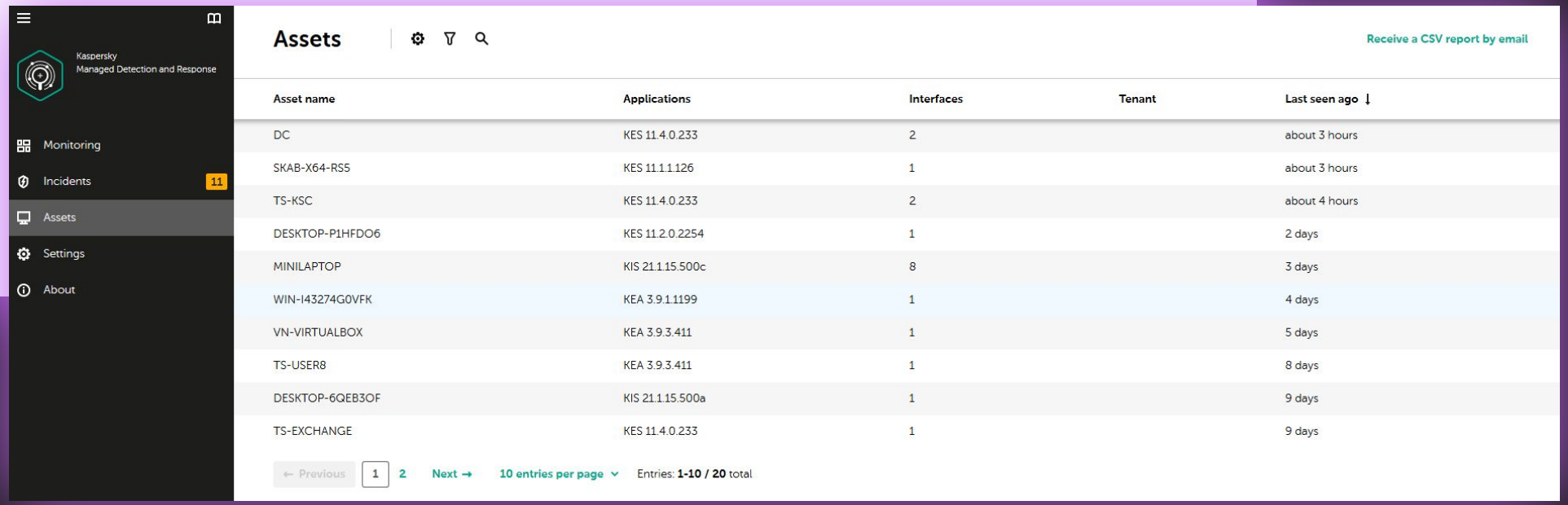
# Интерфейс Kaspersky Managed Detection and Response



# Интерфейс Kaspersky Managed Detection and Response

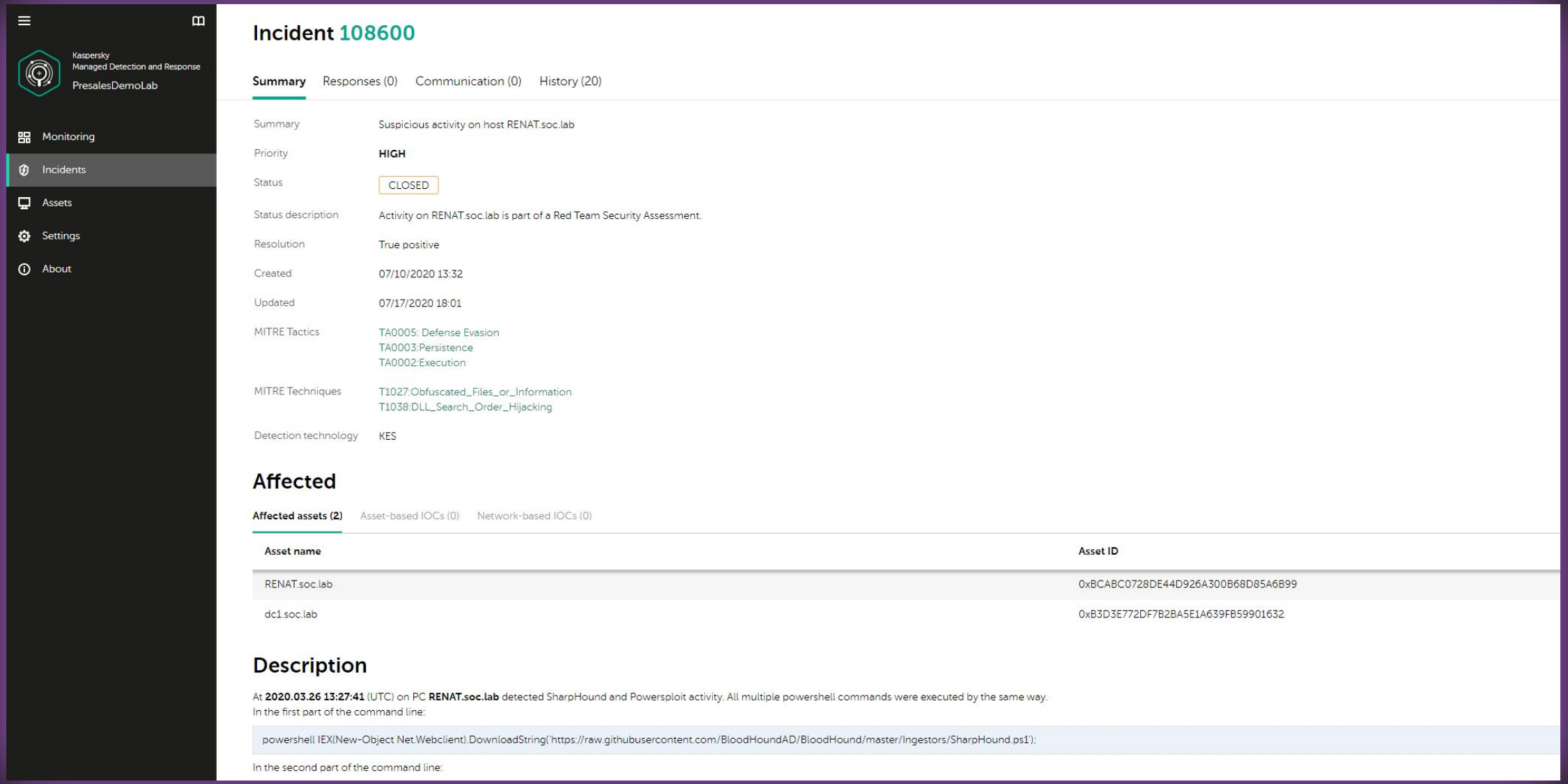




# Интерфейс Kaspersky Managed Detection and Response





# Поддерживаемые продукты, приложения и уровни обслуживания SLA

# Поддерживаемые продукты и приложения



| Платформы | Kaspersky Endpoint Security для бизнеса | Kaspersky Managed Detection and Response |
|---|---|---|
| Настольные компьютеры Windows | Kaspersky Endpoint Security для Windows | Да |
| Серверы Windows | Kaspersky Security для Windows Server | Да |
| | Kaspersky Endpoint Security для Windows | Да |
| Компьютеры macOS | Kaspersky Endpoint Security для Mac | Да |
| Компьютеры Linux | Kaspersky Endpoint Security для Linux | Да |
| Виртуальные среды | Kaspersky Security для виртуальных сред Легкий агент | Да |

Kaspersky EDR для бизнеса Оптимальный, Kaspersky EDR и Kaspersky Anti Targeted Attack поддерживаются только при наличии Kaspersky Endpoint Security для бизнеса

# Соглашения об уровне обслуживания (SLA)



| Уровень приоритета | Время ответа | Целевое значение |
|---|---|---|
| Высокий (пример: целевые атаки) | 1 час | 90% |
| Средний (пример: неизвестное вредоносное ПО) | 4 часа | 90% |
| Низкий (пример: распространенное ВПО) | 24 часа | 90% |

- **Время ответа** – это время от обнаружения инцидента (время создания) до публикации данных о нем в Kaspersky MDR (время обновления)
- **Целевое значение** – это количество инцидентов, для которых время ответа и время реагирования соответствуют заданным параметрам, в процентном выражении

Подробная информация, в том числе о критериях инцидентов, изложена в Положениях и условиях

# Преимущества Kaspersky Managed Detection and Response



# Мировое признание



Доказанная эффективность сочетания наших технологий и экспертных знаний

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

Сервис Kaspersky MDR разработан на основе аналитических данных об APT-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского»

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете Advanced Persistent Threat (APT) Protection в 2021 г.

MITRE | ATT&CK®

Качество обнаружения угроз в Kaspersky MDR подтверждено оценкой MITRE ATT&CK в 2020 году (детекты MSSP)

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave: External Threat Intelligence Services 2021)

# Спасибо!