KSD 2023
Kaspersky Security Day

Какую симфонию выбрать — EDR или MDR

Евгений Бударин

Руководитель отдела предпродажной поддержки,
«Лаборатория Касперского»

Ксения Кошкина

Маркетинг менеджер,
«Лаборатория Касперского»

kaspersky

Какую же симфонию выбрать: EDR или MDR

Kaspersky Symphony EDR

Kaspersky Symphony MDR

Kaspersky Symphony EDR

Kaspersky Symphony EDR: архитектура решения

Kaspersky Symphony EDR: инструментарий

Сбор данных

- Сервер
- ПК
- Ноутбук

Хранение данных

- Вердикты
- Объекты
- Телеметрия

Обнаружение угроз

- Передовое автоматическое детектирование угроз
- Детектирование на основе IoC, Yara, IoA
- Проактивный поиск угроз

Расследование инцидента

- Ретроспективный анализ
- Глобальные данные об угрозах
- Обогащение данными матрицы MITRE ATT&CK

Реагирование на инцидент

В решении Symphony EDR в рамках реагирования на инциденты доступны следующие возможности:

Изоляция скомпрометированного хоста от корпоративной сети

Завершение подозрительного процесса

Удаление вредоносного объекта или перемещение его в карантин

Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

Выполнение команд и управление службами на защищаемом хосте

Основные сценарии применения Kaspersky Symphony EDR

Автоматическое предотвращение, обнаружение и расследование сложных инцидентов на уровне конечных точек

Оперативная проверка инфраструктуры на наличие IoC, получаемых от различных источников, самостоятельный проактивный поиск угроз

Помощь в соответствии требованиям / рекомендациям регуляторов

Централизованное реагирование в распределенной инфраструктуре рабочих мест и серверов (физических и виртуальных)

Получение доступа к цифровым доказательствам, в случаях недоступности скомпрометированных станций или их зашифровки

Оптимизация затрат / сокращение трудозатрат на процесс обработки сложных инцидентов на уровне конечных точек

Kaspersky Symphony MDR

Kaspersky Symphony MDR

Включает EPP-решение (Kaspersky Symphony Security) для защиты всех видов хостов и управление через KSC

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

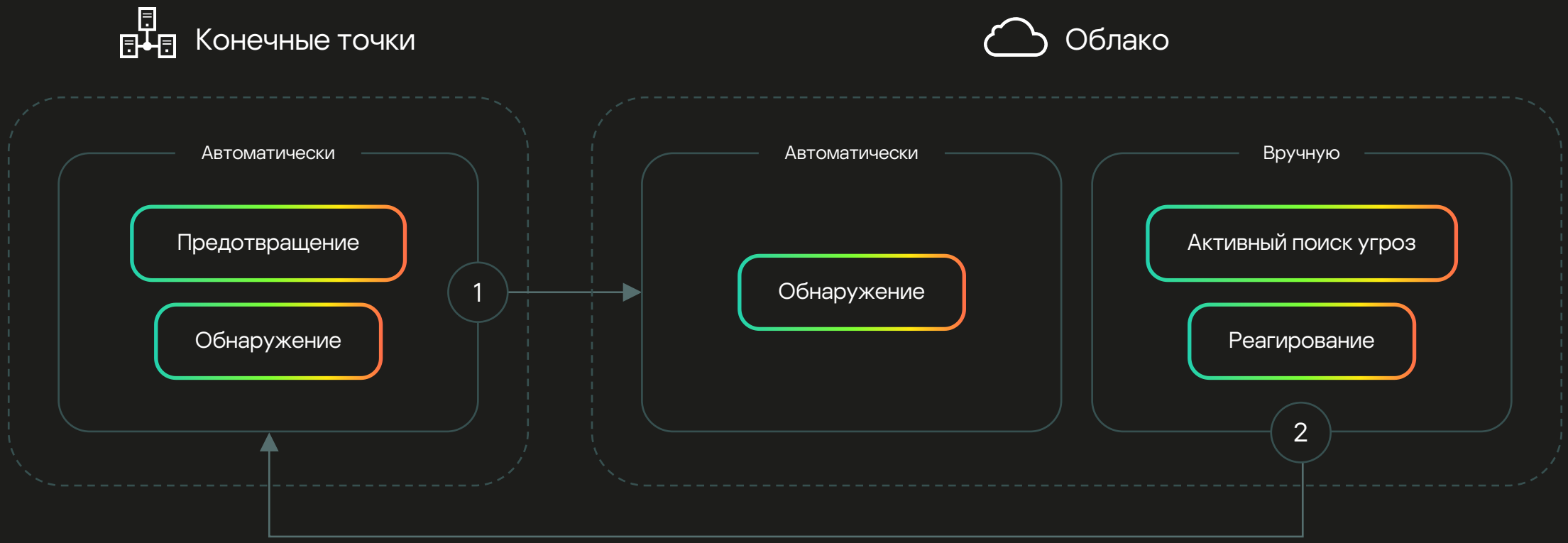
Включает выделенную команду экспертов мирового уровня работающую 24x7

Поддерживает платформы: Windows Desktops, Windows Servers, Mac OS Machines, Linux Machines

Использует более 1000 уникальных индикаторов атак (IoA) для обнаружения

Использует механизмы ИИ для автоматической фильтрации ложно-положительных срабатываний

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

Обогащение телеметрии

Телеметрия

Телеметрия обогащается аналитикой угроз из разных источников

KSN
Kaspersky Security Network

GREAT
Центр глобальных исследований и анализа угроз

Kaspersky Threat Intelligence

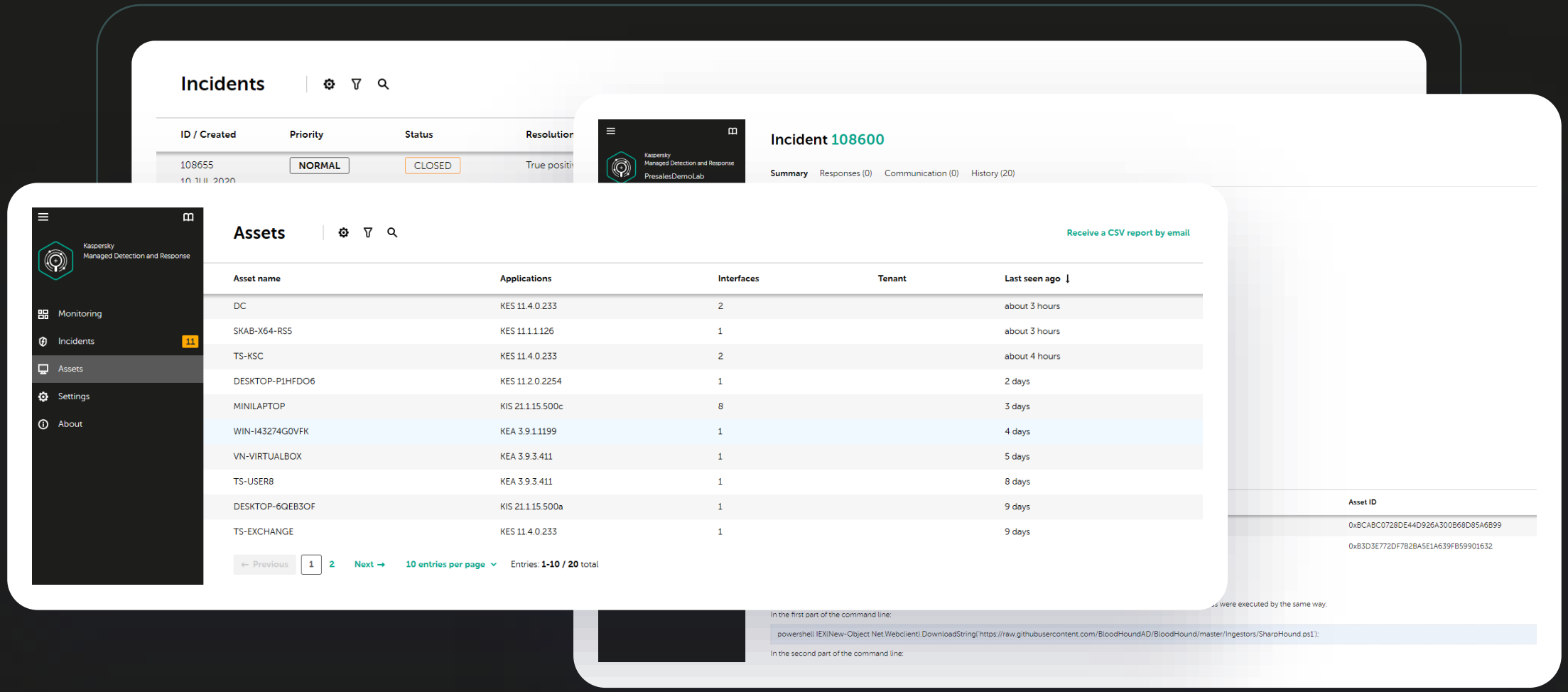
GERT
Международная группа реагирования

Threat Research

Kaspersky ICS CERT

Kaspersky Symphony MDR

Интерфейс MDR



Kaspersky Symphony MDR

Круглосуточный мониторинг

Автоматизированный 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»

Проактивный поиск угроз (Threat Hunting) силами экспертов SOC

Преимущества использования Kaspersky Symphony MDR

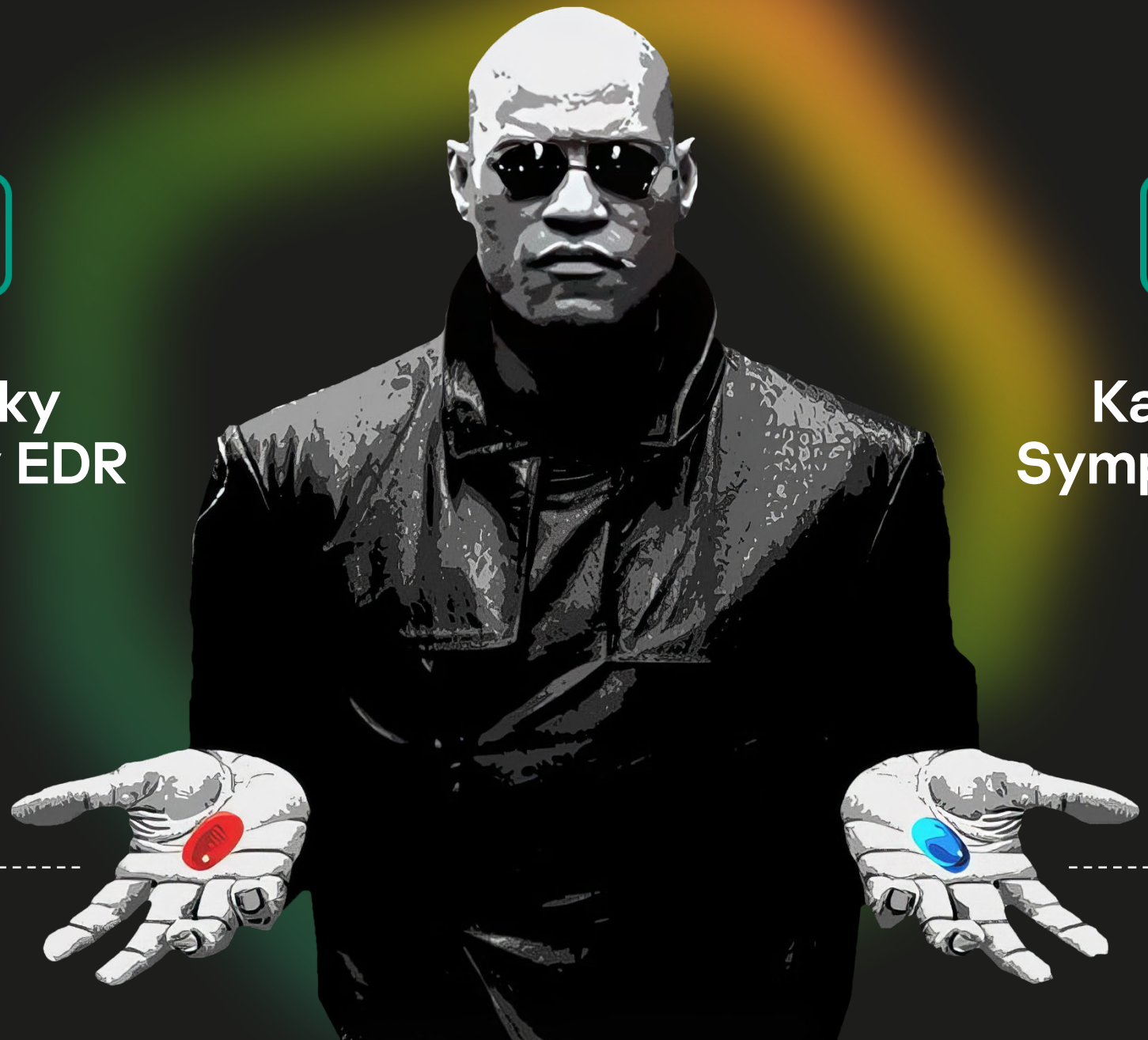
Уверенность в том, что вы находитесь под постоянной защитой

Возможность пользоваться преимуществами центра SOC, не имея его внутри компании

Возможность оперативно получить защиту от экспертов мирового уровня

Сокращение расходов из-за отсутствия необходимости нанимать ИБ-специалистов и строить свой собственный SOC центр

Kaspersky
Symphony EDR



Kaspersky
Symphony MDR

Спасибо!