Kaspersky Symphony XDR

Новые возможности комплексной защиты

kaspersky

Экспертиза мирового уровня

~ 5 000

Высококвалифицированных специалистов

50%

Наших сотрудников — R&D-специалисты и исследователи

35+

Лучших мировых ИБ-экспертов, звезд в области кибербезопасности

5

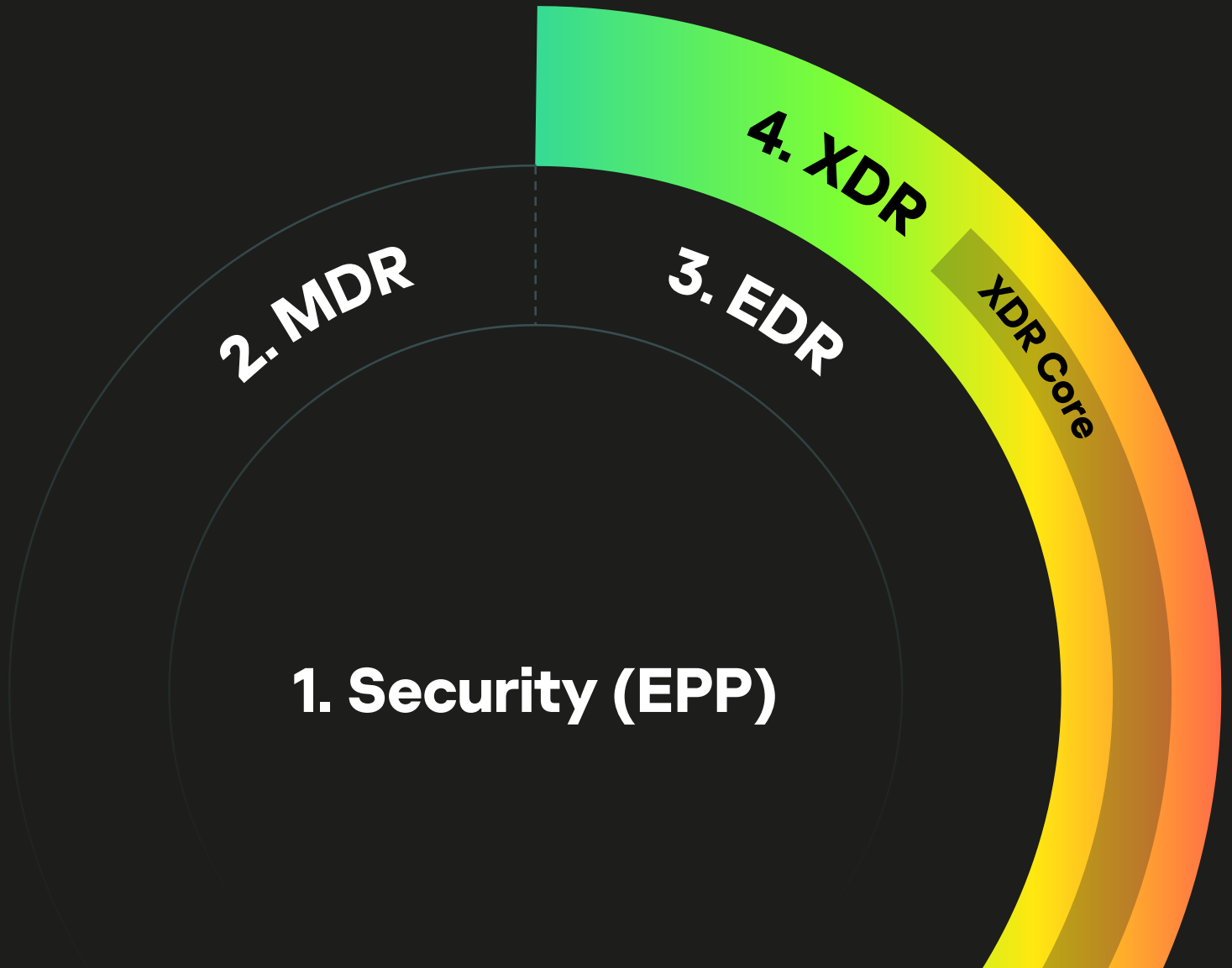
Ведущих комплексных центров экспертизы «Лаборатории Касперского»

Центры экспертизы «Лаборатории Касперского»

О Kaspersky Symphony

Гибкий выбор

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



Kaspersky Symphony XDR

Kaspersky Symphony XDR

XDR Core

Включает в себя ключевой набор продуктов для выстраивания защиты класса XDR. Решение идеально подходит организациям, для которых важна гибкость в построении мощной XDR защиты: как на базе всех продуктов от Kaspersky, так и с добавлением сторонних.

XDR

Всеобъемлющий подход к защите бизнеса с обширным набором уже включенных решений Kaspersky в дополнение к составу XDR Core, в том числе адаптирующийся к существующей инфраструктуре. Решение подходит для компаний-новаторов среднего и крупного бизнеса любых индустрий, выбирающих Kaspersky как своего основного партнера по кибербезопасности.

Kaspersky Symphony XDR Core

Kaspersky
Symphony XDR

Включенная защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Включенная платформа киберграмотности

- Kaspersky Automated Security Awareness Platform

Kaspersky Symphony XDR Core

- Kaspersky Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Symphony EDR + песочница

Интеграции с ИБ-решениями

Сторонние решения

Решения Kaspersky

Включенное потоковое обогащение

- Kaspersky Threat Data Feeds
  - Malicious URL
  - Phishing URL
  - IP Reputation
  - Malicious Hashes
  - Botnet C&C URL
  - Ransomware URL
- Kaspersky CyberTrace

Включенный поисковый портал о киберугрозах и взаимосвязях

- Kaspersky Threat Lookup

Kaspersky Symphony XDR

Kaspersky Symphony XDR

Kaspersky Symphony XDR Core

- Kaspersky Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Symphony EDR + песочница

Интеграции с ИБ-решениями

- Сторонние решения
- Решения Kaspersky

Включенная защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Включенная платформа киберграмотности

- Kaspersky Automated Security Awareness Platform

Включенное потоковое обогащение

- Kaspersky Threat Data Feeds
  - Malicious URL
  - Phishing URL
  - IP Reputation
  - Malicious Hashes
  - Botnet C&C URL
  - Ransomware URL
- Kaspersky CyberTrace

Включенный поисковый портал о киберугрозах и взаимосвязях

- Kaspersky Threat Lookup

Ключевые элементы Kaspersky Symphony XDR

Публичные истории успеха KUMA & KATA Platform

Ростелеком

Телеком провайдер

Оптима Банк

НОВОСТАЛЬ-М

Металлургический холдинг

hh

hh.ru

ФОСАГРО®

Производитель минеральных удобрений

ТГК-2

Энергетическая компания

Крупнейший перевозчик среди пригородных пассажирских компаний России

РоссельхозБанк

AGP

Оператор проекта строительства газовой магистрали Казахстан — Китай в СНГ

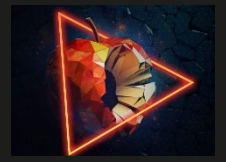
Правительство Ростовской области

МТС

Телеком провайдер

РЖД

РОССЕТИ



KUMA помогла обнаружить* новую APT-атаку на устройства iOS

Подробнее

Развитие ключевых продуктов Kaspersky Symphony XDR в 2023

Kaspersky EDR Expert

- Переход на единый агент с KES
- Поддержка новых дистрибутивов Linux систем
- Снижены аппаратные требования
- Новые возможности реагирования на Linux-системах
- Получен сертификат ФСТЭК как СОВ уровня узла

Kaspersky Unified Monitoring and Analysis Platform

- ~100 новых источников и ~150 новых правил корреляции из коробки
- Реализована возможность холодного хранения событий
- Поддержана полная отказоустойчивость системы
- Контент в виде кода и расширение схемы событий
- Расширены возможности по реагированию через собственные продукты и 3rd party

Kaspersky Anti Targeted Attack

- Расширена поддержки Linux систем
- Увеличена скорость обработки трафика
- Поддержка блокирующего режима по ICAP
- Поддержка хранения и работы с полной копией сырого трафика

Развитие ключевых продуктов Kaspersky Symphony XDR в 2023

Kaspersky EDR Expert

- Переход на единый агент с KES
- Поддержка новых дистрибутивов Linux систем
- Снижены аппаратные требования
- Новые возможности реагирования на Linux-системах
- Получен сертификат ФСТЭК как СОВ уровня узла

Kaspersky Unified Monitoring and Analysis Platform

- ~100 новых источников и ~150 новых правил корреляции из коробки
- Реализована возможность холодного хранения событий
- Поддержана полная отказоустойчивость системы
- Контент в виде кода и расширение схемы событий
- Расширены возможности по реагированию через собственные продукты и 3rd party

Kaspersky Anti Targeted Attack

- Расширена поддержки Linux систем
- Увеличена скорость обработки трафика
- Поддержка блокирующего режима по ICAP
- Поддержка хранения и работы с полной копией сырого трафика

KUMA — центральный элемент XDR

Лидирующее SIEM решение в РФ и центральный элемент XDR

Эффективность команд SOC

Автореагирование, единый список событий для расследования и хантинга

Гибкость

Сложные схемы развёртывания, широкие возможности корреляции, мощный поиск

Производительность

Современная архитектура и стек технологий, проверенная производительность

Коннекторы «из коробки»

200+

Поддерживаемых источников «из коробки»

340+

Правил корреляции

С момента релиза KUMA 2.1 до релиза KUMA 3.0.2 было выпущено:

57 Новых пакетных ресурсов;

55 пакетов с новыми или переработанными нормализаторами.

Данные нормализаторы позволили подключить к KUMA в качестве источников событий или улучшить поддержку нормализации для 62 систем

Сторонние источники

Microsoft DNS

Microsoft Terminal Server

pfSense (OpenVPN)

Linux (auth,rights, owner,FW)

Unbound

Dovecot

Nginx

Apache

Bind

Cisco ASA

Cisco IOS (R&S)

Cisco WSA

VmWare ESXi

VmWare Horizon

Any CEF certified source

FortiAnalyzer

Juniper VSRX, EX4600, 4300, 2300

Windows Event logs

Palo Alto NGFW & Panorama

FortiGate UTM, FortiMail

Linux (auth,rights, owner,FW)

CheckPoint (Syslog/CEF)

Netflow v5/v9/ IPFIX

~ 200 источников

Функциональные возможности SMP

Kaspersky Symphony XDR

Kaspersky Symphony XDR

Kaspersky Symphony XDR Core

- Kaspersky Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Symphony EDR + песочница

Интеграции с ИБ-решениями

- Сторонние решения
- Решения Kaspersky

Включенная защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Включенная платформа киберграмотности

- Kaspersky Automated Security Awareness Platform

Включенное потоковое обогащение

- Kaspersky Threat Data Feeds
  - Malicious URL
  - Phishing URL
  - IP Reputation
  - Malicious Hashes
  - Botnet C&C URL
  - Ransomware URL
- Kaspersky CyberTrace

Включенный поисковый портал о киберугрозах и взаимосвязях

- Kaspersky Threat Lookup

Kaspersky Symphony XDR 2.0

Kaspersky Symphony XDR

Kaspersky Symphony XDR Core

Kaspersky Single Management Platform

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Symphony EDR + песочница

Включенная защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Включенная платформа киберграмотности

- Kaspersky Automated Security Awareness Platform

Интеграции с ИБ-решениями

- Сторонние решения
- Решения Kaspersky

Включенное потоковое обогащение

- Kaspersky Threat Data Feeds
  - Malicious URL
  - Malicious Hashes
  - Phishing URL
  - Botnet C&C URL
  - IP Reputation
  - Ransomware URL
- Kaspersky CyberTrace

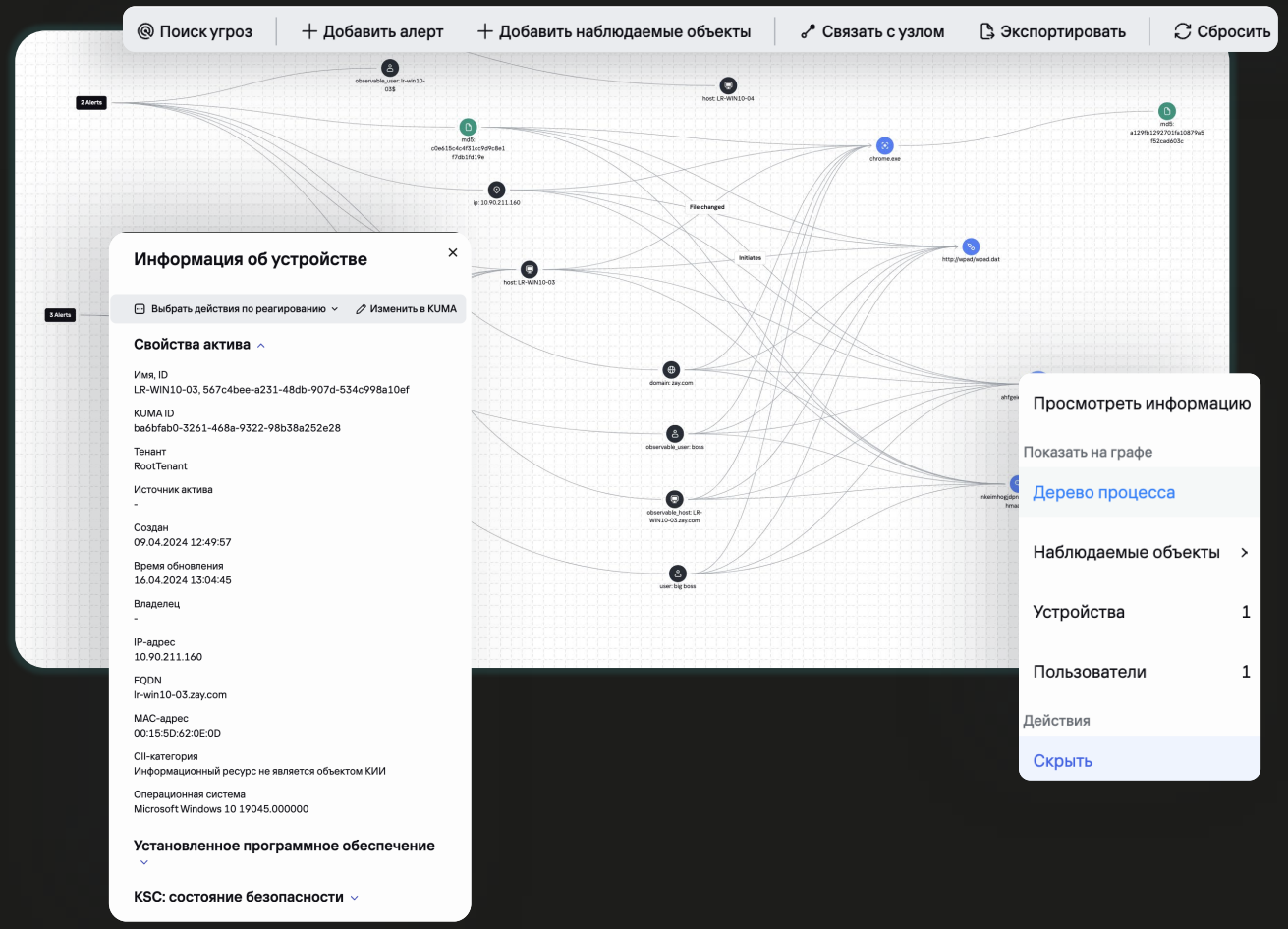
Включенный поисковый портал о киберугрозах и взаимосвязях

- Kaspersky Threat Lookup

Kaspersky Symphony XDR: архитектура

Kaspersky Symphony XDR: архитектура

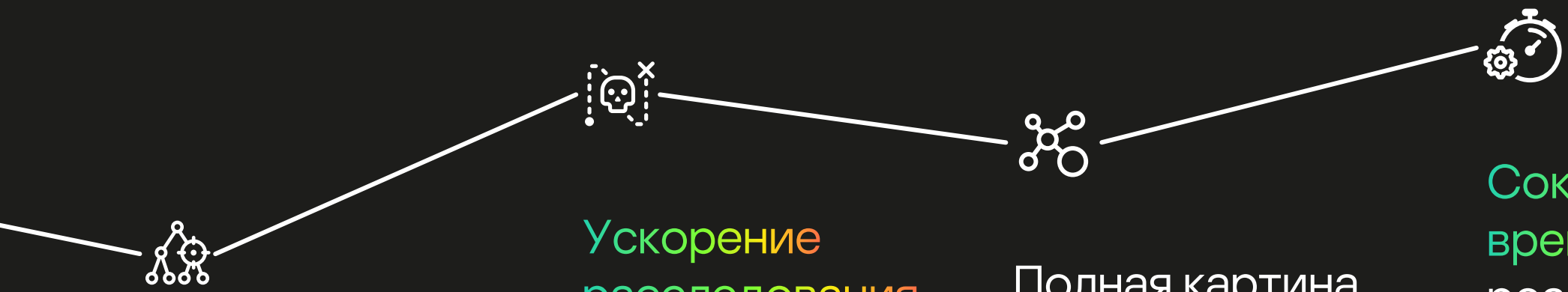
Граф расследований



Визуализация связей между элементами инцидента ИБ

Совместное расследование аналитиков на одном графе с возможностью сохранять «прогресс» и делиться им с коллегами для последующего анализа

Граф расследований



Целостное представление о ландшафте инцидента

Ускорение расследования за счет визуализации

Полная картина инцидента с учетом данных со сторонних источников

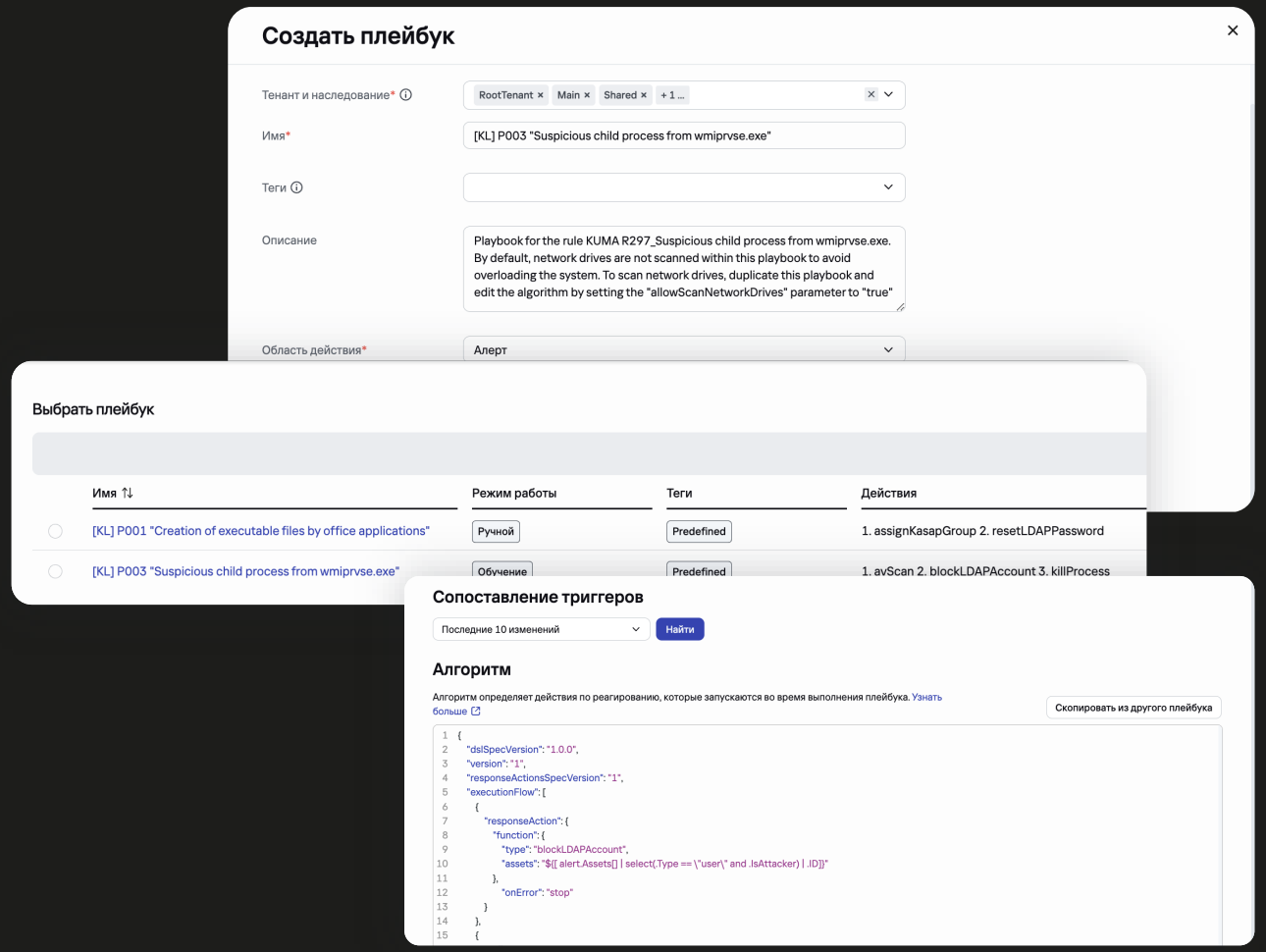
Сокращение времени реагирования

Плейбуки

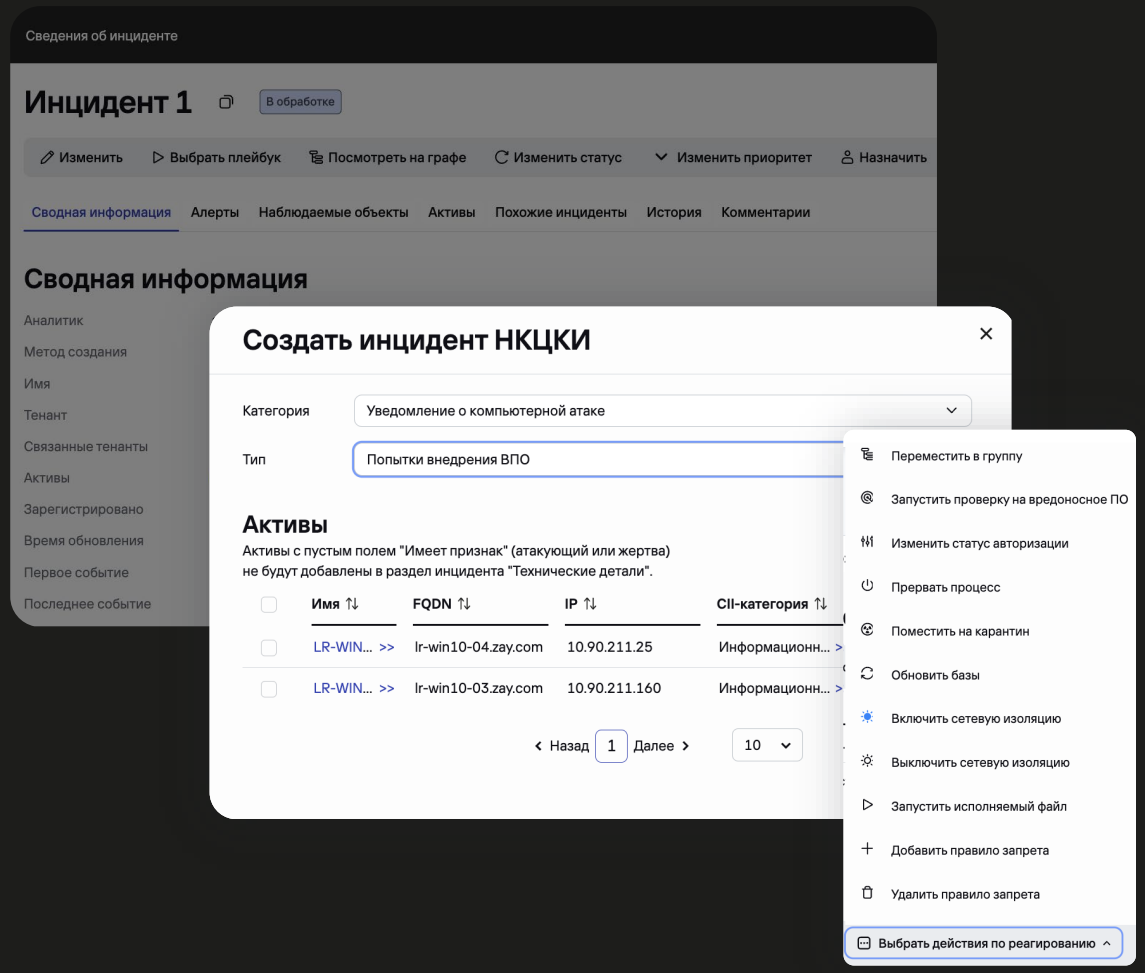
Автоматизация процессов расследования и реагирования на инциденты с помощью готовых и пользовательских сценариев

Сокращение количества рутинных операций и ускорение расследования

Разные способы запуска плейбука: автоматически или вручную



Управление инцидентами



Эффективное управление инцидентами расширяет возможности ИБ-команд по обнаружению и расследованию, повышает эффективность обработки алертов, а также способствует скоординированному реагированию.

Ближайший Roadmap

Дальнейшее развитие

Расширение функциональности управления инцидентами

Комплексные многоуровневые плейбуки

Визуальный редактор плейбуков

Сильные стороны Kaspersky Symphony XDR

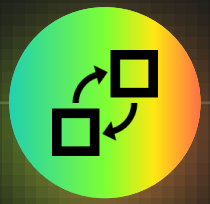
Kaspersky Symphony XDR

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 взаимодействие

Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии, взаимодействие с другими решениями сторонних поставщиков, единая платформа управления

Фокус на соответствие

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

Фокус на качество

В состав входят продукты, заслужившие признание аналитиков, независимых лабораторий и клиентов по всему миру

Gartner peerinsights customers' choice 2021

FORRESTER® IDC

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

SE Labs AAA ADVANCED SECURITY (EDR)

AV TEST

MITRE | ATT&CK®

Спасибо!