Продвинутая защита от целенаправленных атак на всех уровнях с решениями Kaspersky

Бударин Евгений

kaspersky

Современные реалии ИБ

Расширяется и/или изменяется IT-инфраструктура, которая требует защиты

Усложняется ландшафт угроз и расширяется поверхность атаки, добавляется целевая киберагрессия и необходимость ИБ-замещения

Увеличиваются средние потери в результате одного киберинцидента

Процесс работы с инцидентами становится более сложным и ресурсозатратным

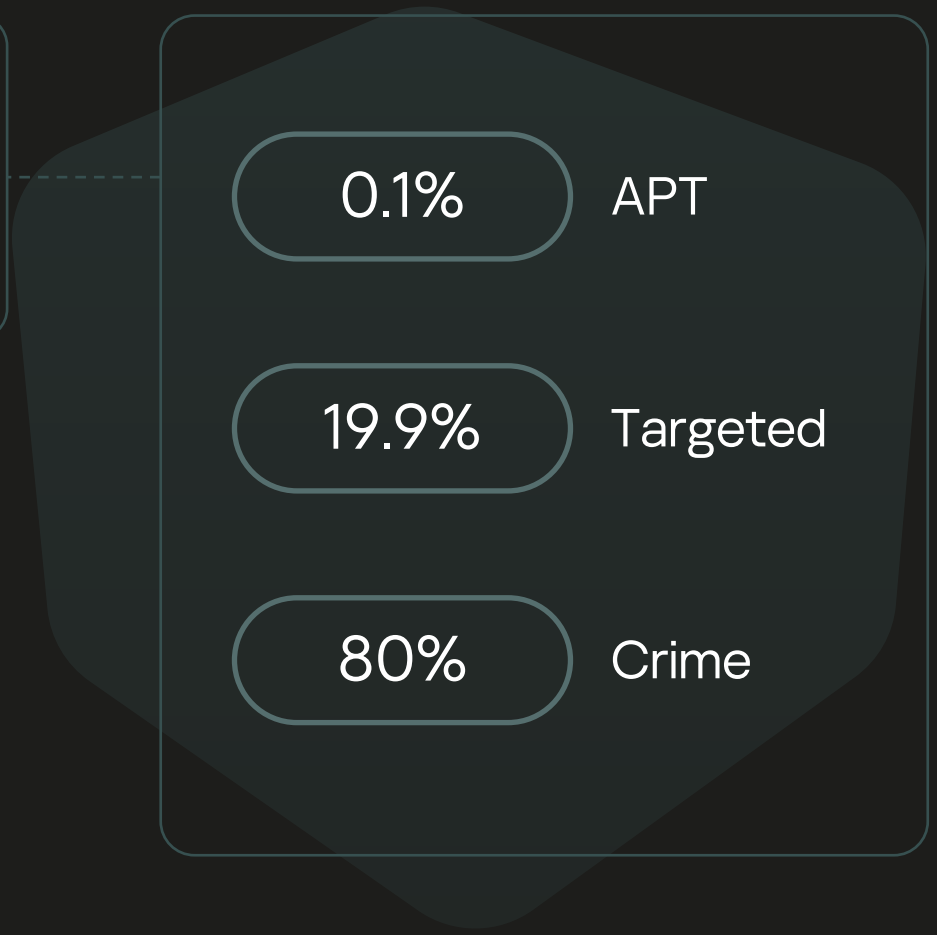
Присутствует глобальный дефицит ИБ-экспертов на рынке труда и неоптимальное использование их времени и таланта

Современные кибервызовы

Средний ущерб от успешной кибератаки

SMB: 105k$ **Enterprise:** от 1M$

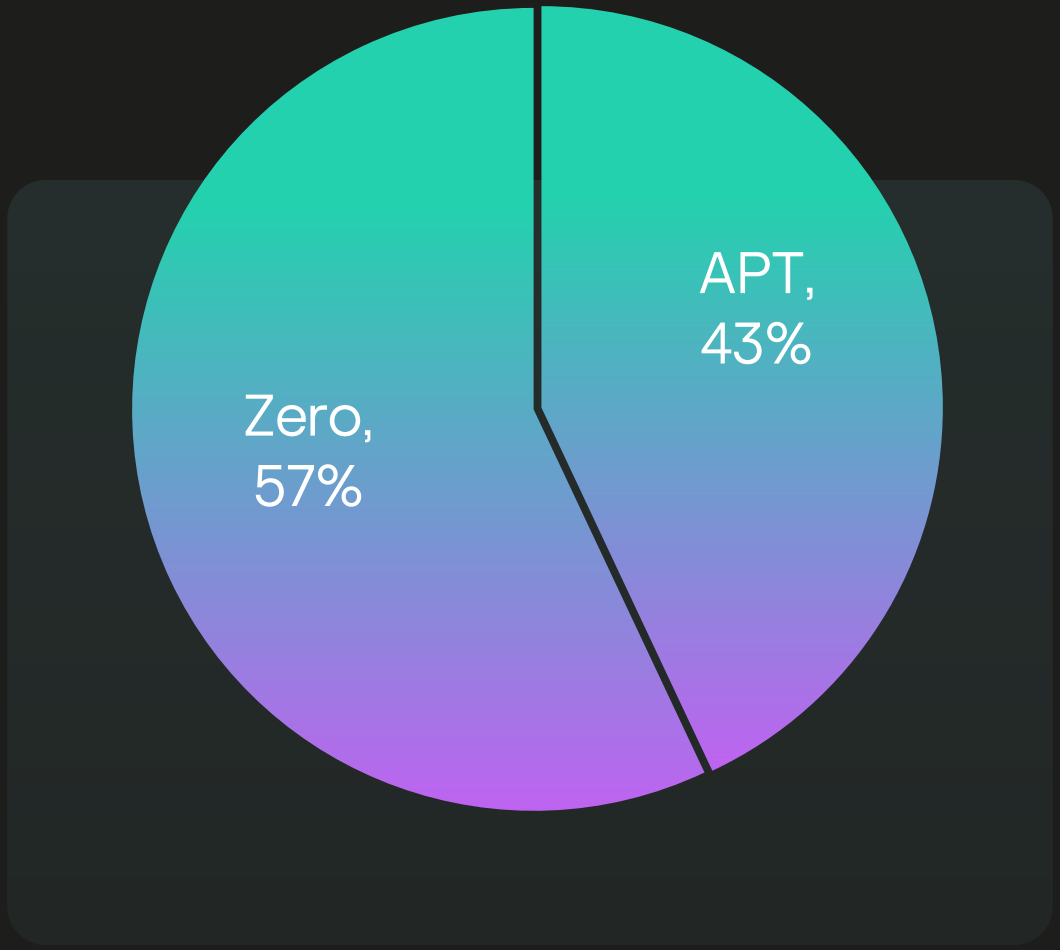
- Эксплуатация тематики COVID-19 в 2021 году и темы частичной мобилизации в России – в 2023-м
- Атаки на удаленный доступ
- Кроме Windows: Linux, Mac, роутеры
- Мобильные импланты, 0day's: iOS/Android-атаки
- Атаки на цепочки поставок
- Современные шифровальщики: Ransomware-as-a-Service, Big Game Hunting
- Количество DDoS-атак существенно возросло



Источники данных: Cybersecurity Ventures, Kaspersky

Статистика пилотов решения ANTIAPT

Почти на каждом втором проекте обнаруживаются признаки APT-атак в инфраструктуре

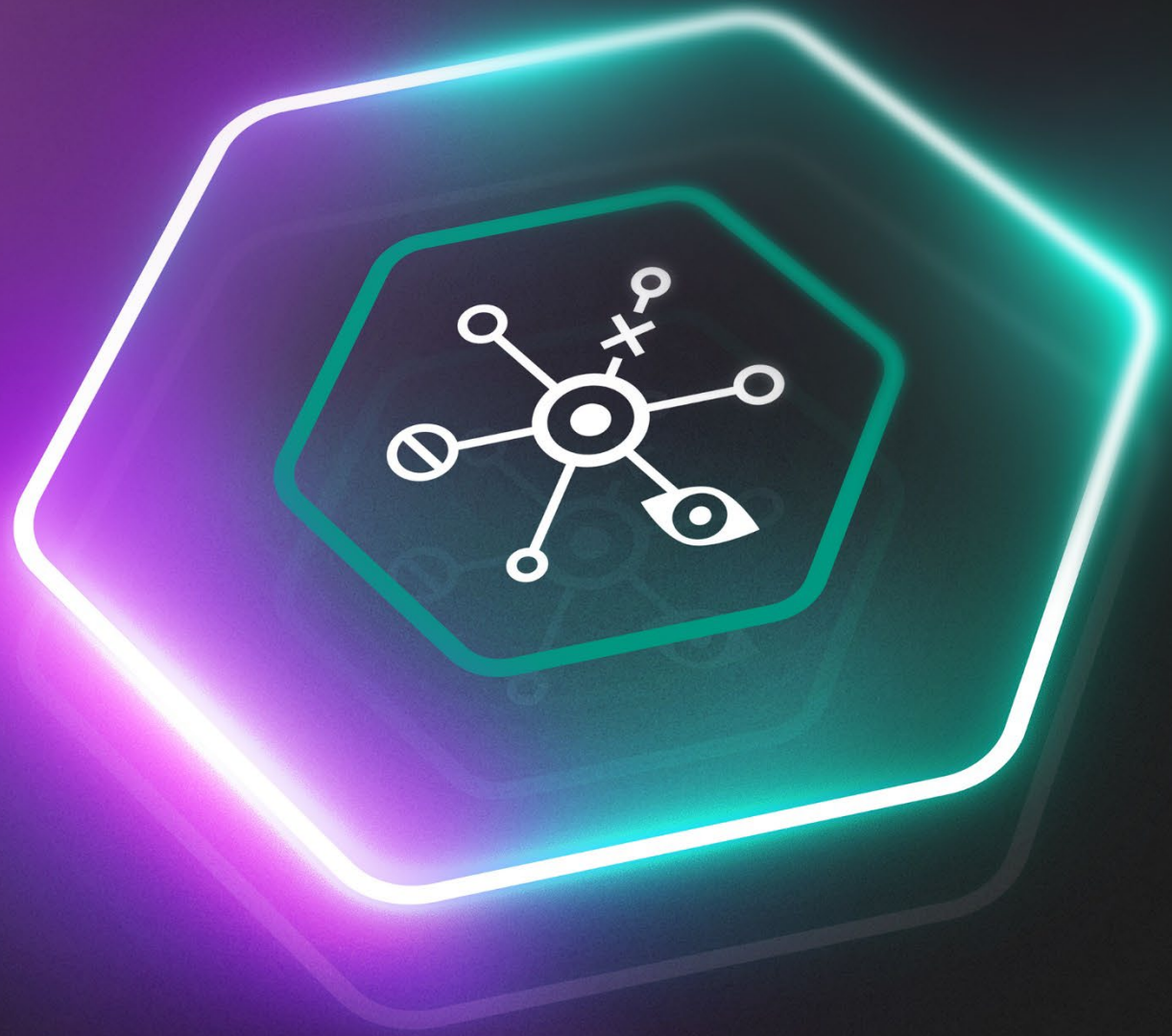


Kaspersky Anti Targeted Attack (KATA)

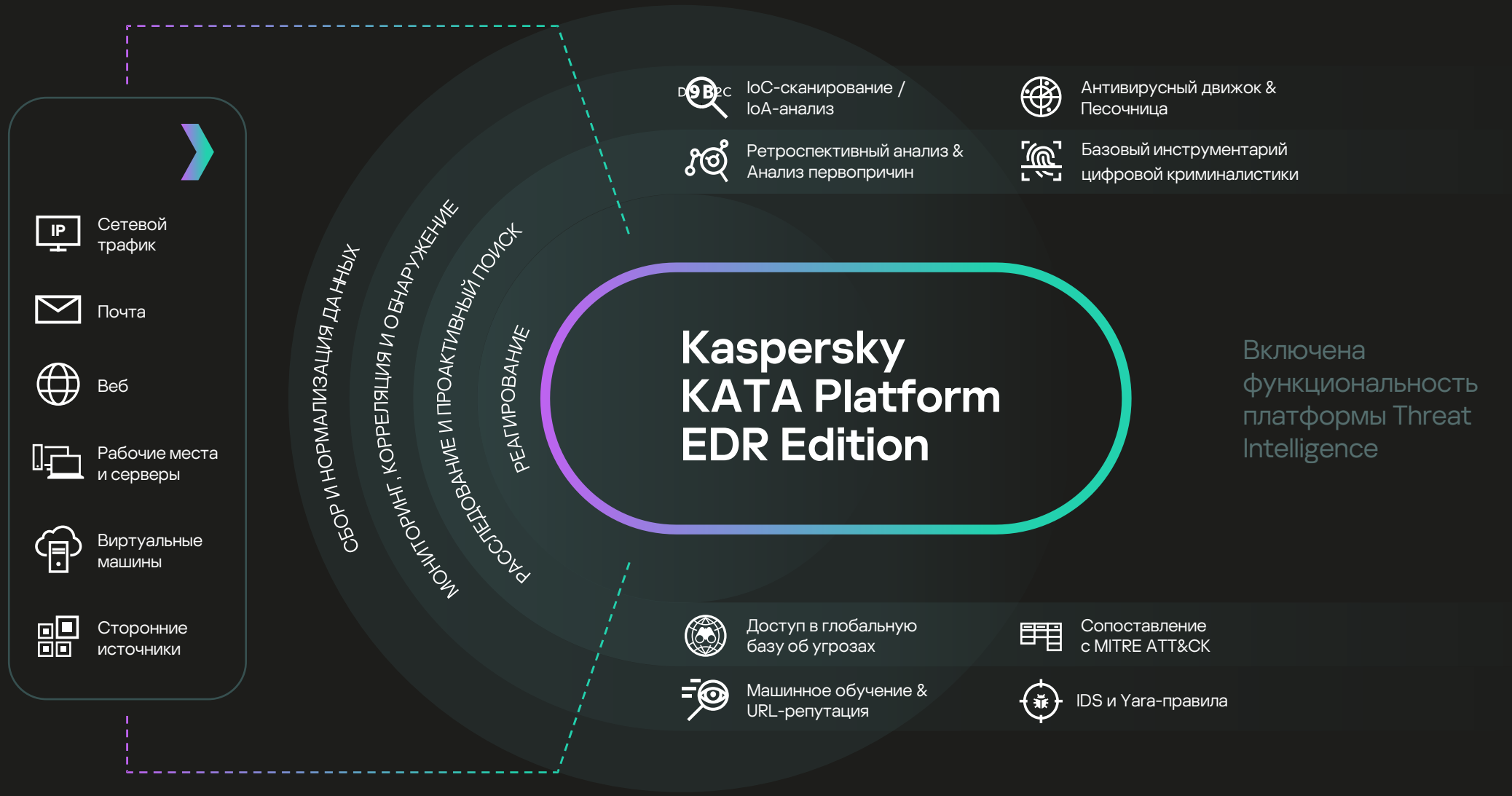
Комплексное решение для защиты от сложных угроз и APT-атак с расширенным функционалом обнаружения и реагирования на уровне сети и конечных устройств (при взаимодействии с Kaspersky EDR Expert)

Kaspersky EDR Expert (KEDR Expert)

Мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутого обнаружения, эффективного расследования, проактивного поиска угроз и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств

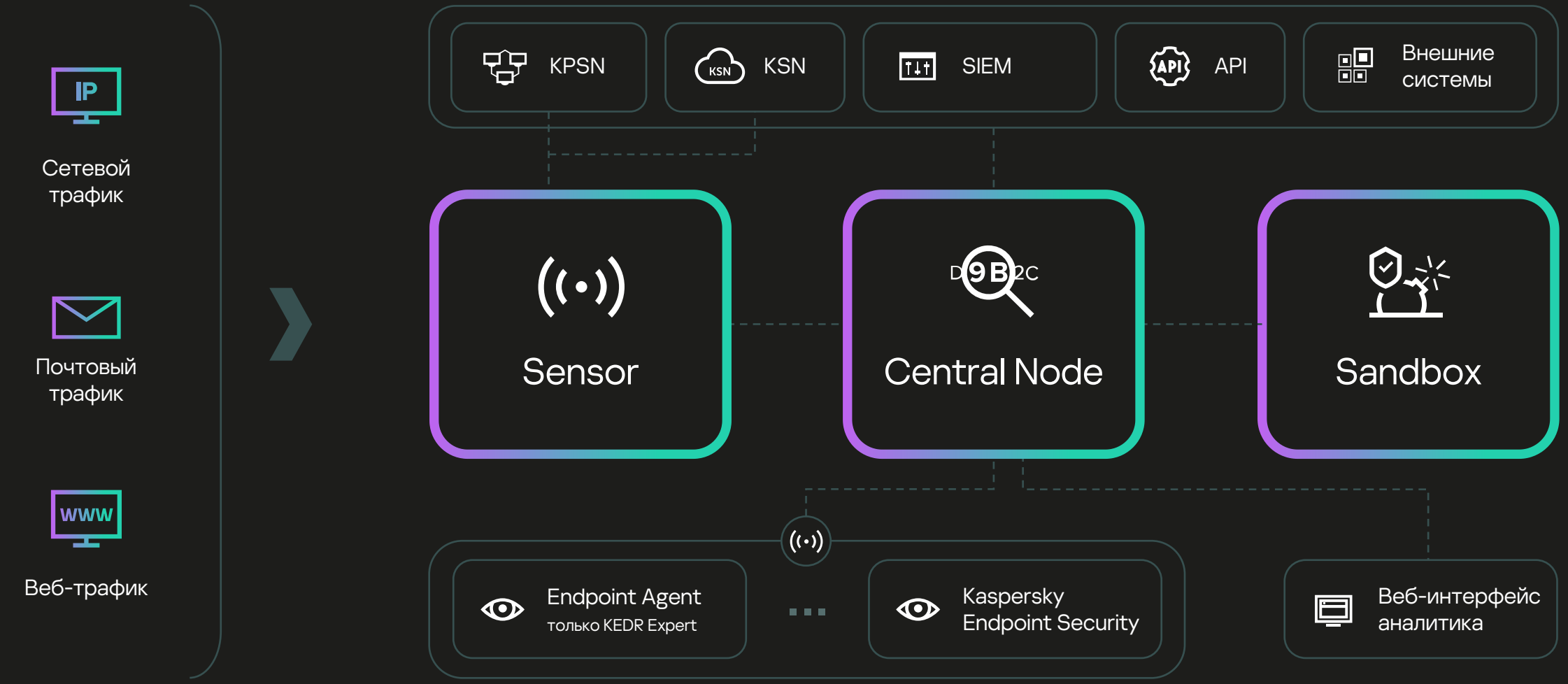


Ключевые возможности

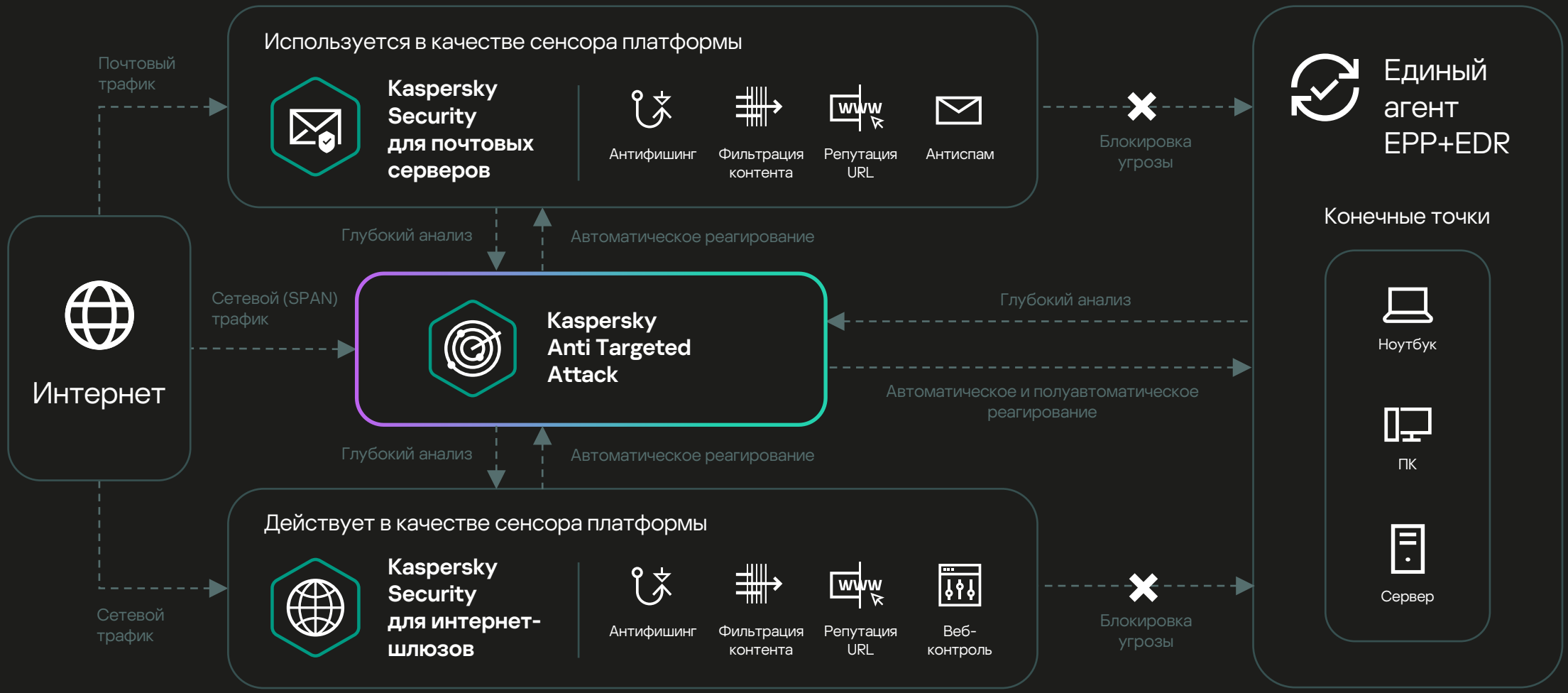


Архитектура решения

Архитектура решения



Автоматическое реагирование с помощью шлюзов



ICAP-интеграция с NGFW в режиме блокировки

Расширение базовой интеграции ICAP за счет отправки вердикта с информацией о том, является ли контент вредоносным. ICAP-клиент использует вердикт для регистрации информации, блокировки контента или его одобрения без дальнейшего анализа.

3 типа интеграции ICAP с режимом блокировки:

Отключено

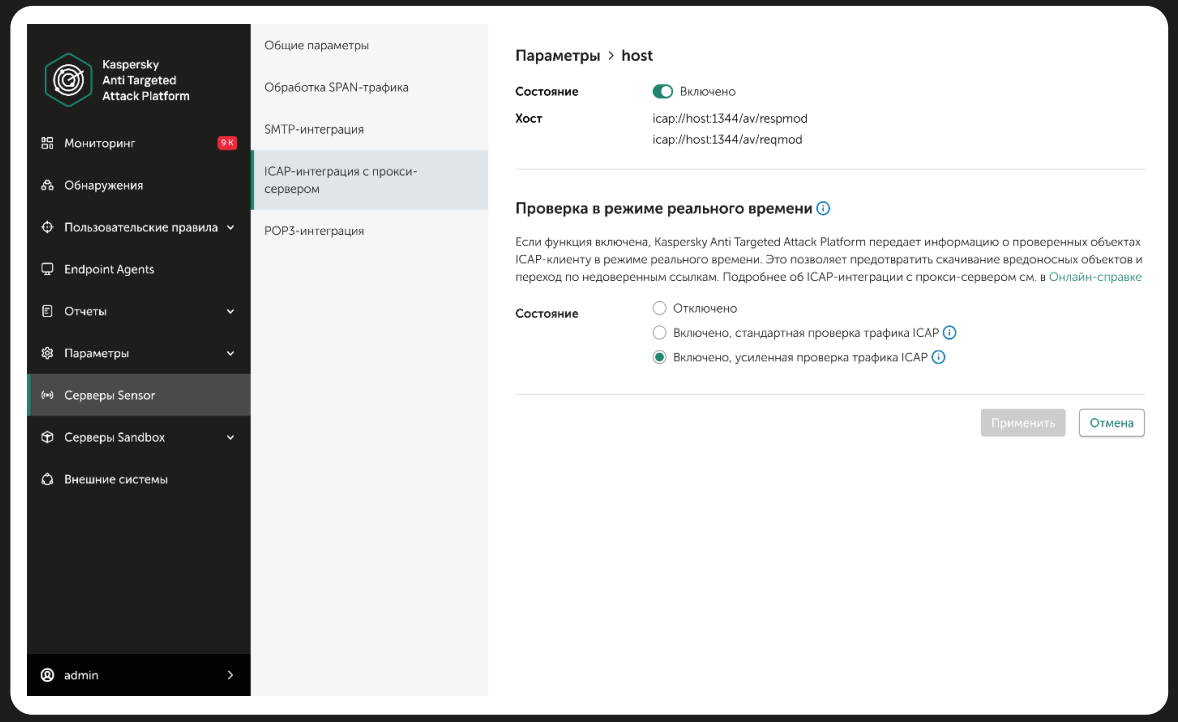
Вердикт не передается ICAP-клиенту

Стандартный (быстрый режим)

Вердикт отправляется ICAP-клиенту. Используются антивирус, YARA, KSN и кэш Sandbox

Расширенный

Вердикт отправляется ICAP-клиенту. Используются антивирус, YARA, KSN и полная эмуляция Sandbox



Детектирование угроз

Основные детектирующие технологии

Любые полученные данные проходят многоуровневую обработку различными компонентами системы:

Anti-Malware Engine

Выполняет проверку файлов и объектов на вирусы и другого вредоносного ПО, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

Mobile Attack Analyzer

Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

YARA

Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями KATA.

Targeted Attack Analyzer

Обнаруживает индикаторы атак (Indicators of attack, IOA) по обновляемым и пользовательским правилам в событиях телеметрии, поступающих от компьютеров.

URL Reputation

Обнаруживает вредоносные, фишинговые, а также связанные с APT URL-адреса, которые ранее использовались злоумышленниками для целевых атак и вторжений в IT-инфраструктуру организаций.

Intrusion Detection System

Технология позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки. В числе поддерживаемых протоколов: TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.

Компонент Sandbox

Компонент Sandbox запускает объекты в шаблонах операционных систем и анализирует их поведение для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Проверке подлежат не только запускаемые объекты, но и дочерние (например, скачиваемые из Интернета в процессе запуска исходного файла):

≈ 200

Несколько тысяч детектов с конкретными вердиктами (основаны на вредоносном и аномальном поведении). Из них около 200 правил с детектированием подозрительного поведения (suspicious activity)

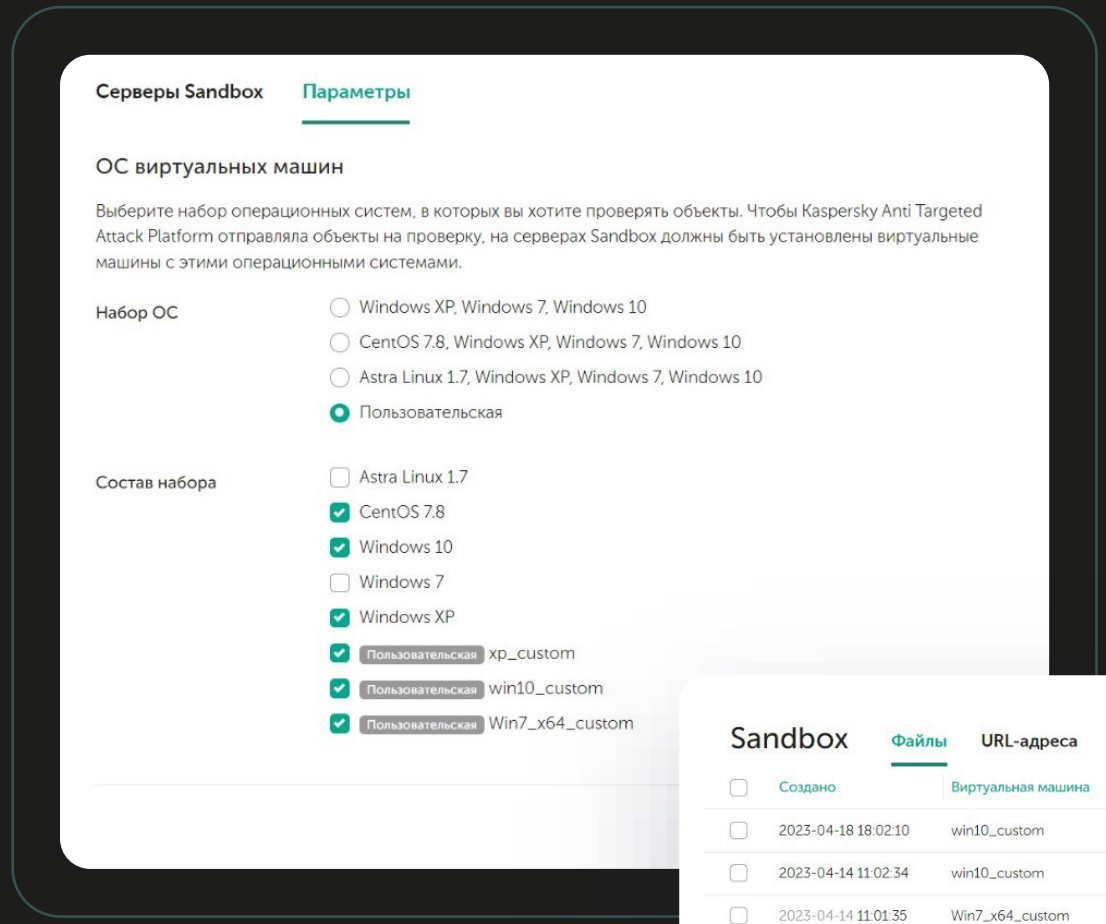
≈ 30 000

Вызовов API находятся под наблюдением

≈ 15 000

Правил для сетевого трафика (генерируемого исследуемым объектом внутри Sandbox)

Кастомизация образов Sandbox



Для компонента Sandbox имеется возможность установки пользовательских образов операционных систем Windows. Вы можете настраивать:

- Имя компьютера
- Локализацию ОС
- Учетные записи
- Необходимое ПО

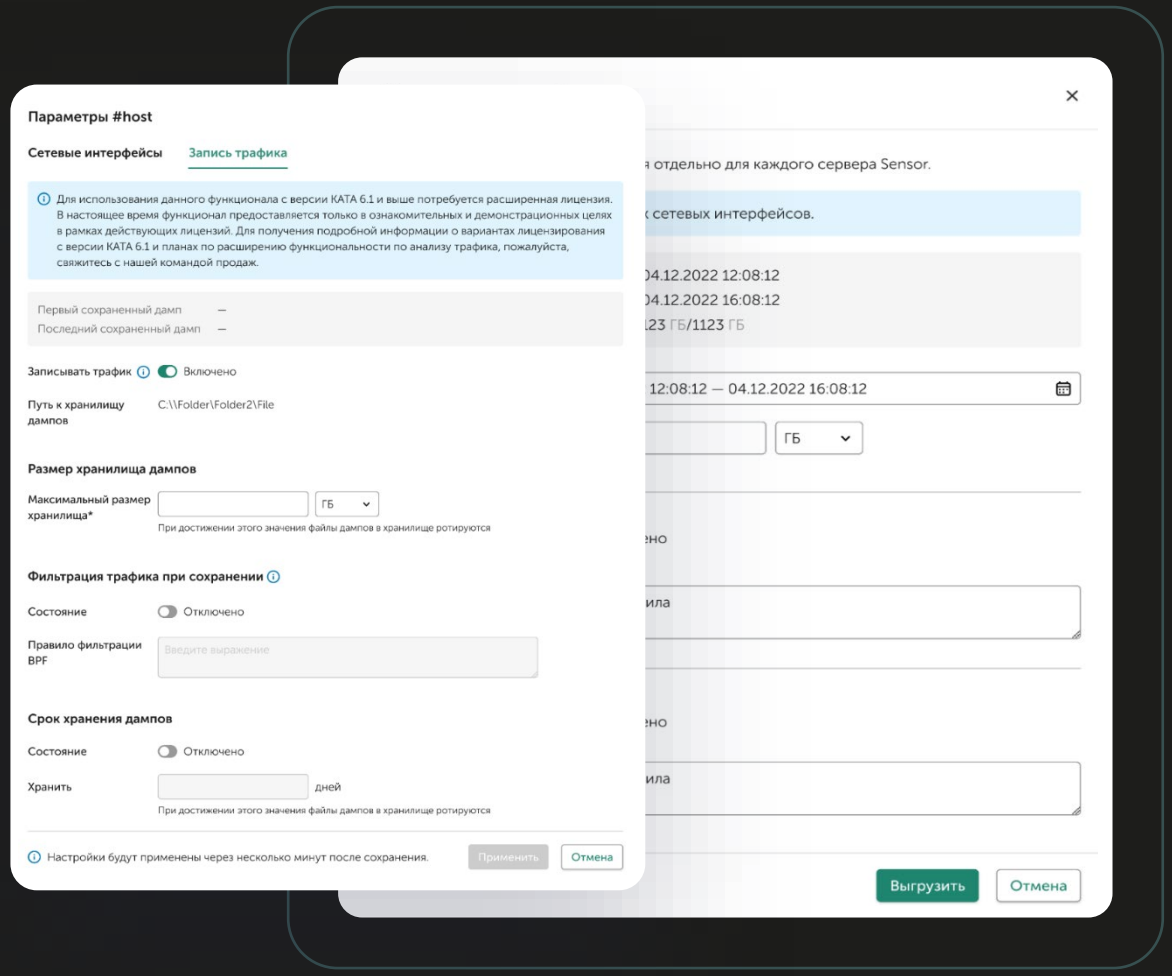
Чтобы приложение отправляло объекты на проверку в этих операционных системах, требуется создать пользовательские правила Sandbox.

Новые возможности NTA

Хранение копий трафика необработанных данных с настраиваемым временем хранения: поддерживайте сетевую безопасность, обеспечивайте соблюдение законодательных и нормативных требований и проводите расследования.

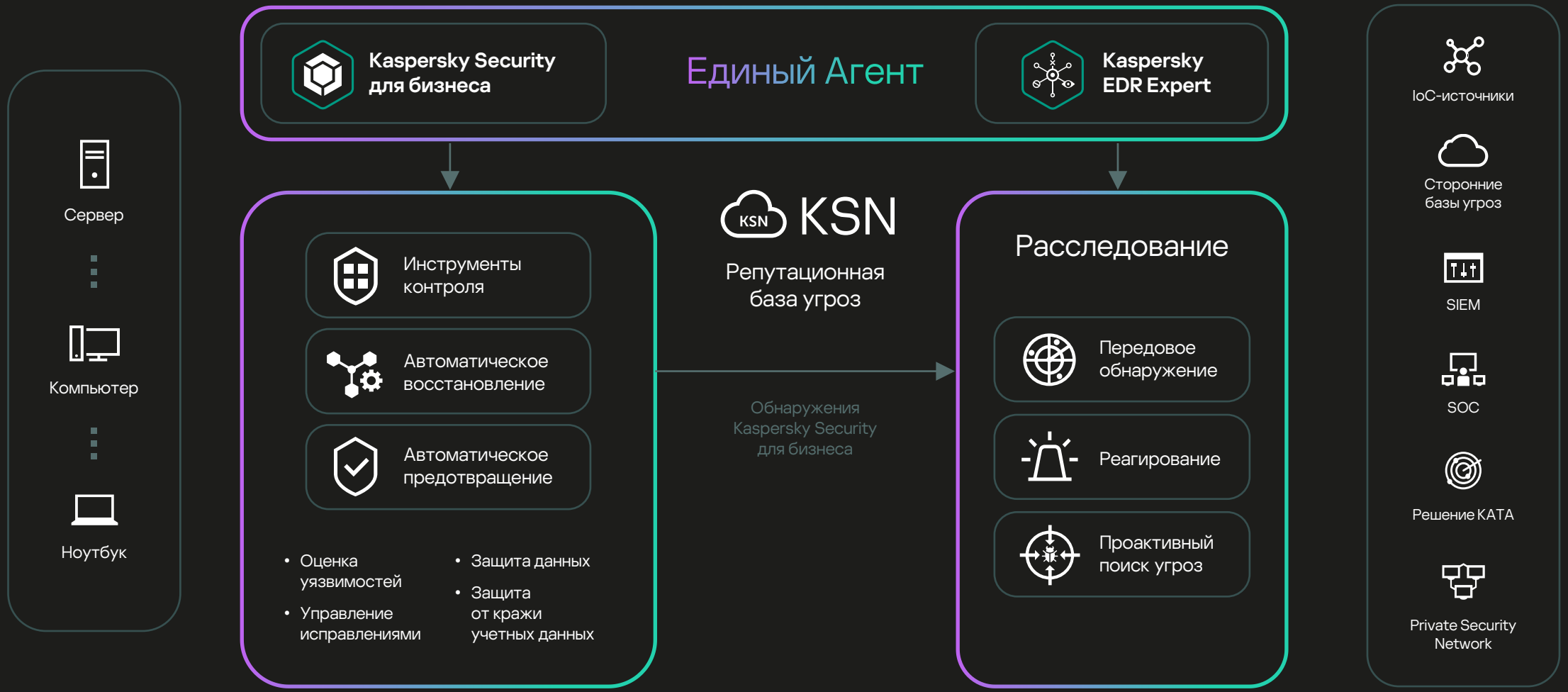
Поиск по копиям трафика необработанных данных, что упрощает процесс расследования: выявляйте и исследуйте предыдущие угрозы безопасности с помощью гибких инструментов поиска.

Файлы трафика в формате PCAP можно скачивать в фоновом режиме.



Компонент Endpoint Agent

Агенты на уровне конечных точек собирают все необходимые данные с конечных устройств в инфраструктуре организации



Анализатор целевых атак

Анализатор целевых атак (Targeted Attack Analyzer, TAA) обнаруживает подозрительную активность, используя расширенный эвристический анализ аномалий для автоматического поиска угроз в реальном времени

Поддерживает автоматический анализ событий и их сопоставление с уникальным набором индикаторов атак (IoA), поставляемых специалистами «Лаборатории Касперского».

Каждый раз, когда TAA обнаруживает аномалию в телеметрии с хостов, специалист по ИБ получает полную информацию о возможном инциденте: описание, рекомендации (например, по снижению риска повторного появления события), данные о степени уверенности в вердикте и серьезности события – для удобства классификации и ускорения реагирования.

Поиск индикаторов атаки (IoA) в событиях на защищаемых хостах с помощью Targeted Attack Analyzer:

Поиск индикаторов атак

в событиях, собираемых с защищаемых хостов в режиме реального времени

Возможность создания

и импорта собственных IoA-правил

Встроенные IoA-правила

от экспертов «Лаборатории Касперского»

Автоматизация

Обнаруженные инциденты автоматически сопоставляются с базой знаний MITRE ATT&CK

Визуализация атак

Для улучшения видимости происходящего в защищаемой инфраструктуре используются:

Настраиваемые дашборды с виджетами (возможность экспорта данных в PDF)

Визуализация поведения эмулируемого объекта в Sandbox

Настройка нотификации об инцидентах на электронную почту

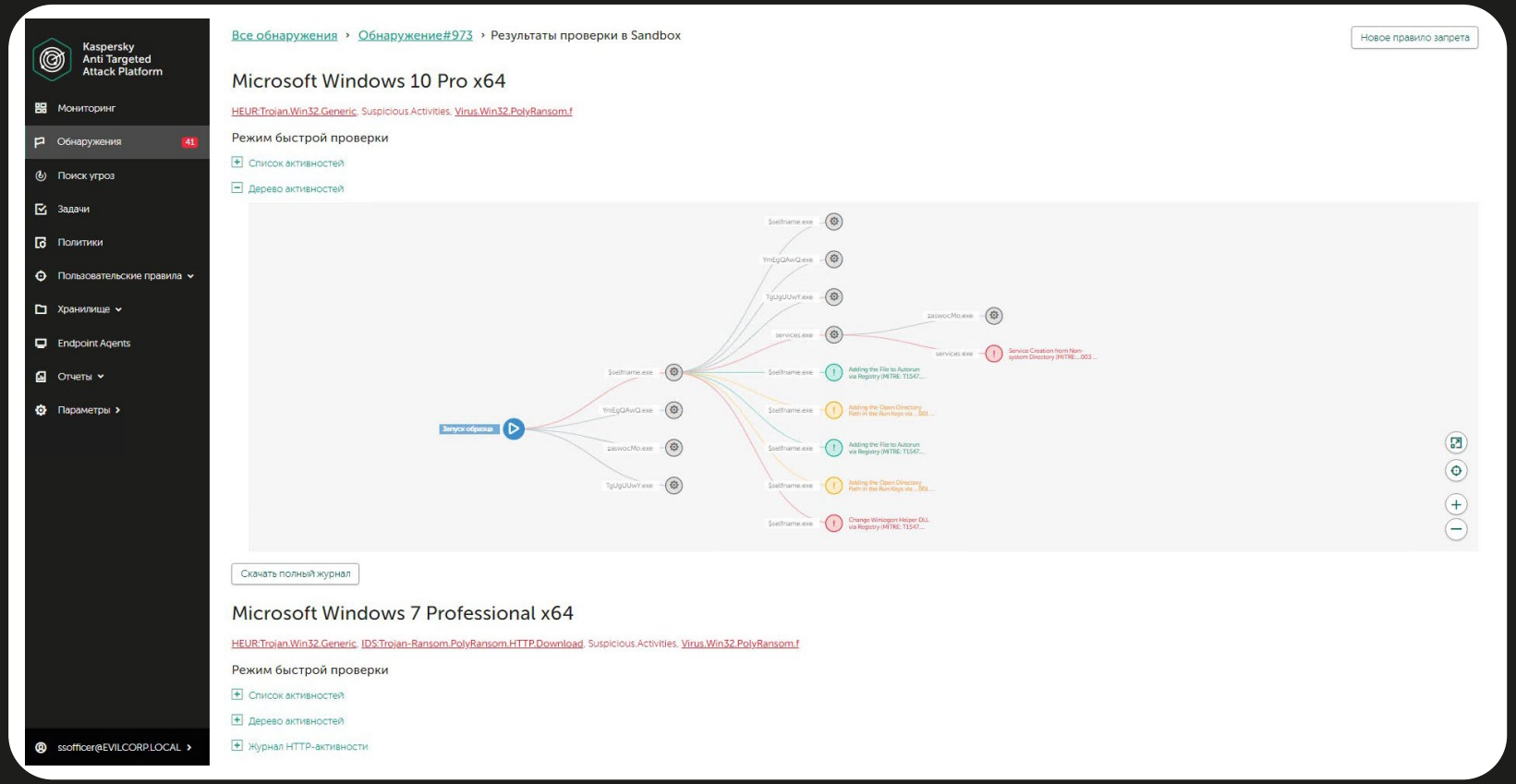
Отображение обнаружений в трафике и на хостах с указанием важности обнаружения, источника, используемой технологии детектирования

Визуализация дерева процессов, запускаемых на защищаемых хостах

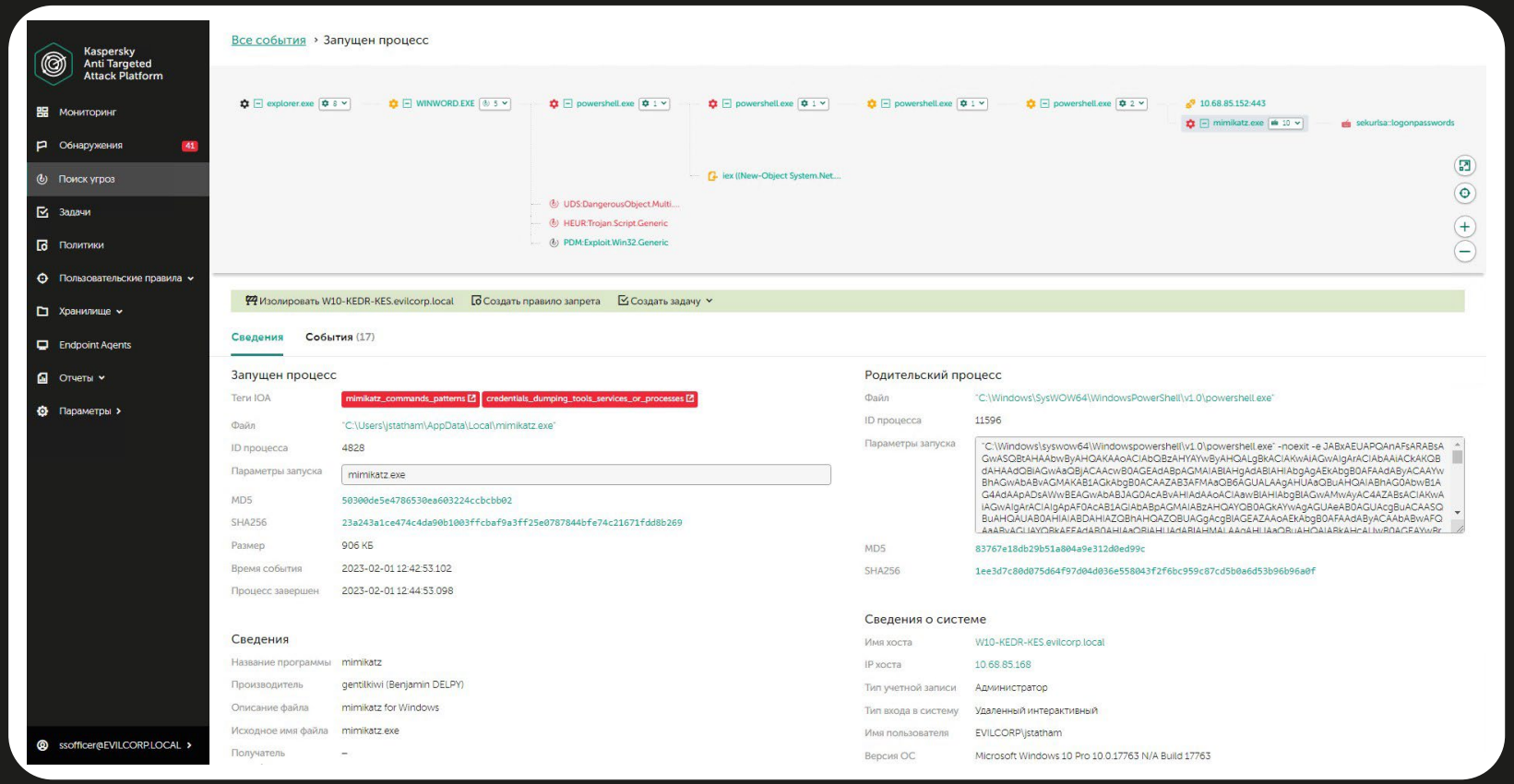
Создание и загрузка отчетов (HTML- и PDF-формат)

Гибкий механизм создания шаблонов отчетов

Граф активности объекта в Sandbox



Дерево запуска процессов на хосте



Расследование инцидентов

Для проведения расследования инцидентов у специалиста существуют следующие возможности:

Рекомендательная система для оперативного реагирования

Автоматическая приоритизация обнаружений

Создание базового workflow-реагирования на инциденты

Сбор дополнительной информации с защищаемых хостов с целью форензики

Поиск неизвестных угроз (Threat Hunting):

- ретроспективный анализ по событиям, ранее собранным с защищаемых хостов
- возможность создания запросов в формате BPF для поиска индикаторов атак в сохраненном сетевом трафике
- гибкий инструмент написания запросов поиска

Детализированные описания угроз на портале threats.kaspersky.com

Интеграция с Threat intelligence для обогащения знаний по обнаруженным IoC

Сопоставление событий с техниками матрицы MITRE ATT&CK

Реагирование на угрозы

В решении KATA 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

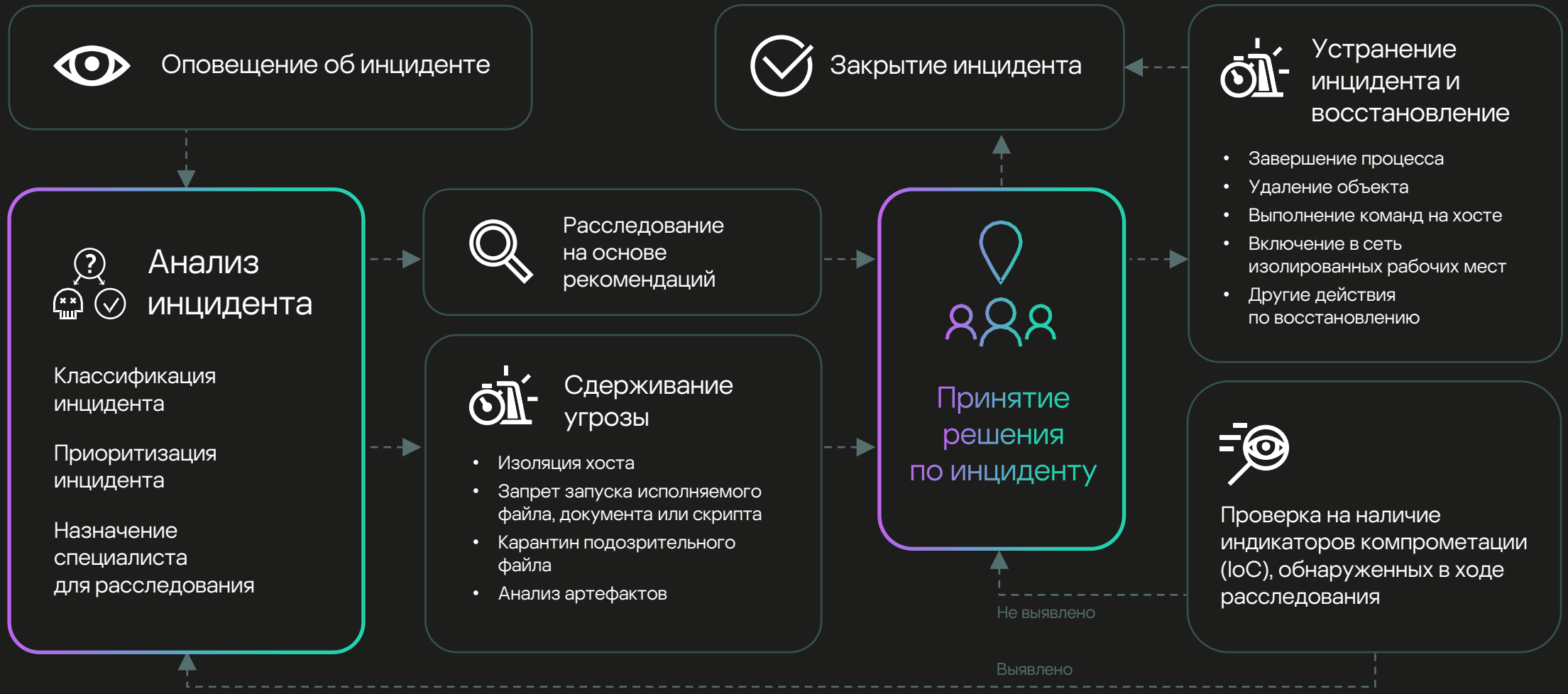
Автоматическое создание правил блокировки запуска подозрительных объектов в результате обнаружения Sandbox

Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

Выполнение команд и управление службами на защищаемом хосте

Запуск YARA-проверки

Схема централизованного реагирования на инциденты



Что нового планируется в версии 6.1 и 7.0

KATA Platform EDR Edition — дальнейшее развитие

Апрель 2024

6.1

Обнаружение угроз в зашифрованном трафике (TLS Fingerprinting)

Обнаружение угроз технологией TAA на основе цепочек событий (улучшение логики детектирования атак на защищаемых хостах)

MSSP: Поддержка подписочных лицензий

Ноябрь 2024

7.0 (NEW! Модуль NDR)

Сбор и отправка сетевой статистики с KES в модуль NDR

Расширение возможностей IDS KATA по детектированию сложных угроз

Инвентарный список активов и построение карты сети

Расширение списка определяемых протоколов и построение таблицы сетевых сессий для улучшения процесса поиска угроз

Интеграция KES с KATA Sandbox для отправки файлов с рабочих станций

Обогащение телеметрии EDR новыми типами событий

Поддержка использования sigma-правил

Поддержка группировки хостов

Новые response сценарии в EDR-агенте для Linux (карантин, создание правил запрета запуска файлов)

Отображение скриншотов в результате анализа файлов технологией Sandbox

Расширение возможностей по масштабированию продукта (подключение до 150 Secondary Central Node к Primary)

Поддержка развертывания всех компонентов продукта на виртуализации «Брест»

Спасибо!