Решения для противодействия сложным угрозам

Бударин Евгений

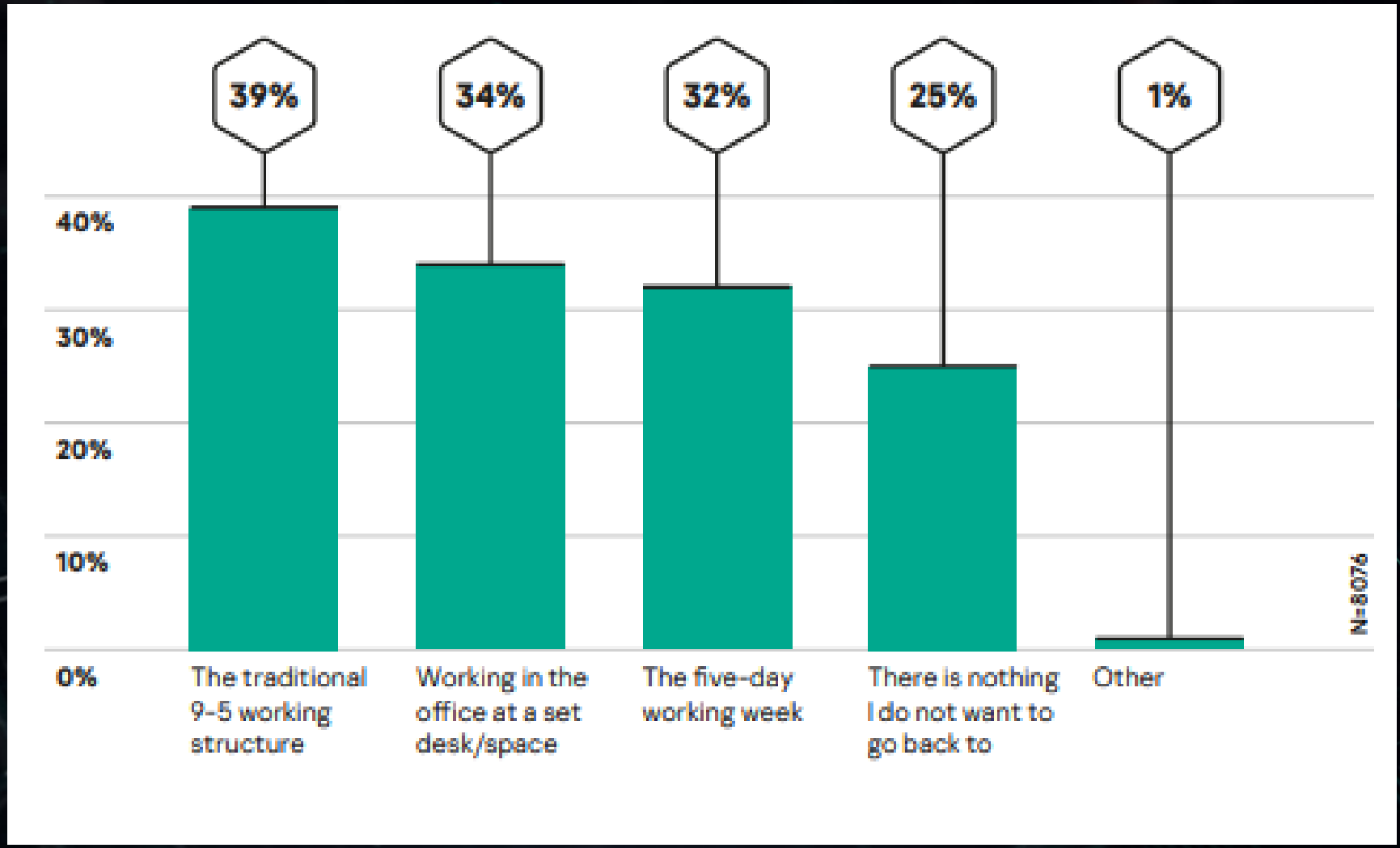
kaspersky

Кто мечтал работать на удаленке?

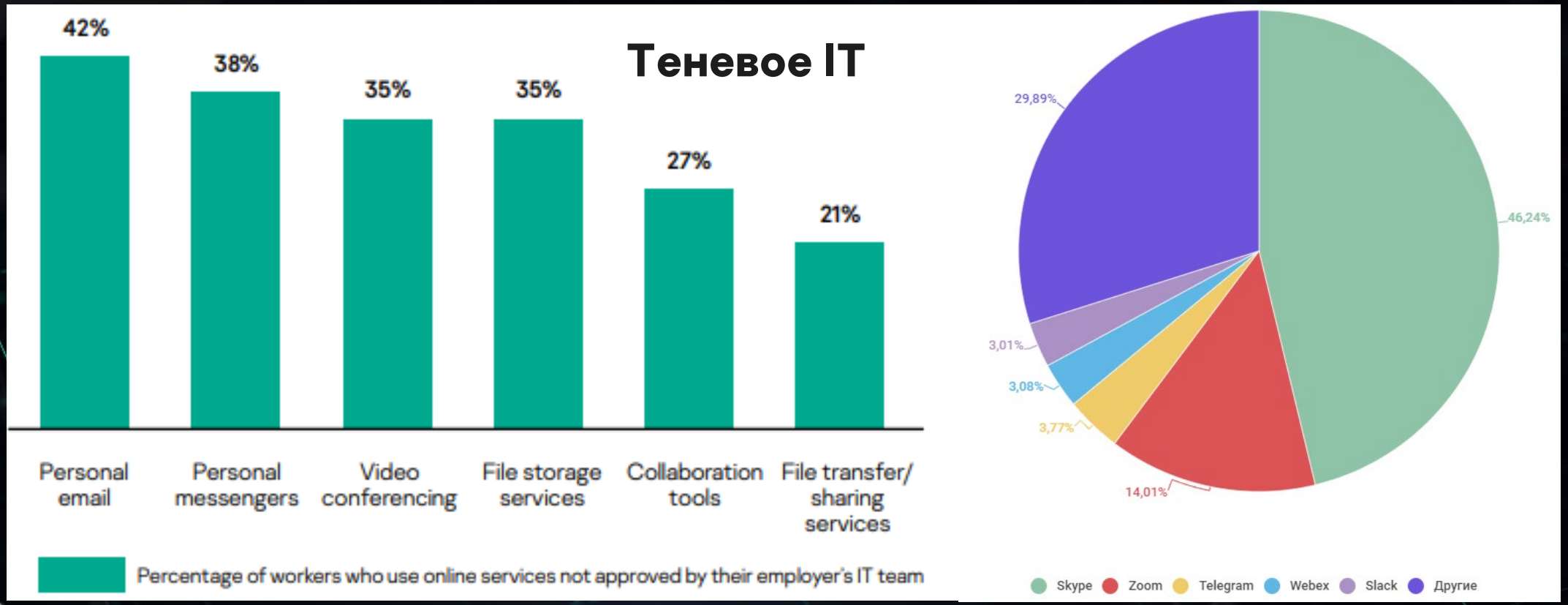
Кто поменял свой результат воображения?


RIFA-F

Результаты опроса



История 2020 года: удаленная работа



По данным нашей телеметрии, киберпреступники активно пытались маскировать свои вредоносные программы под популярные мессенджеры и приложения для онлайн-конференций, которые использовались удаленными работниками в качестве замены привычной офлайн-коммуникации. «Лаборатория Касперского» обнаружила 1,66 млн экземпляров вредоносных файлов, распространяемых под видом таких приложений.

Как новые условия работы влияют на безопасность компании?

- Сотрудники берут свои рабочие компьютеры домой и используют их в слабо защищенных домашних сетях.
- Сотрудники получают удаленный доступ к корпоративным ресурсам и могут использовать незащищенные личные устройства.
- Больше людей попадаются на простые уловки мошенников в создавшемся «хаосе».
- В случае инцидента специалистам сложно приехать на место и разобраться с произошедшим, зачастую не имеют физический доступ к атакованным компьютерам.

Как условия удаленной работы влияют на работоспособность кибер-преступников?

- Они были прекрасно подготовлены к такому переходу, всегда работают из дома.
- В их арсенале появилась новая тема, волнующая абсолютно всех.
- Количество в спешке настроенных и уязвимых точек входа в корпоративные инфраструктуры внезапно возросло.
- В дарквебе растет спрос на доступы к корпоративным сетям.

Тренды сегодняшних атак

Финансовое влияние сложного инцидента, вызванного утечкой данных, в 2020 году

$745 тыс.
Прямые потери

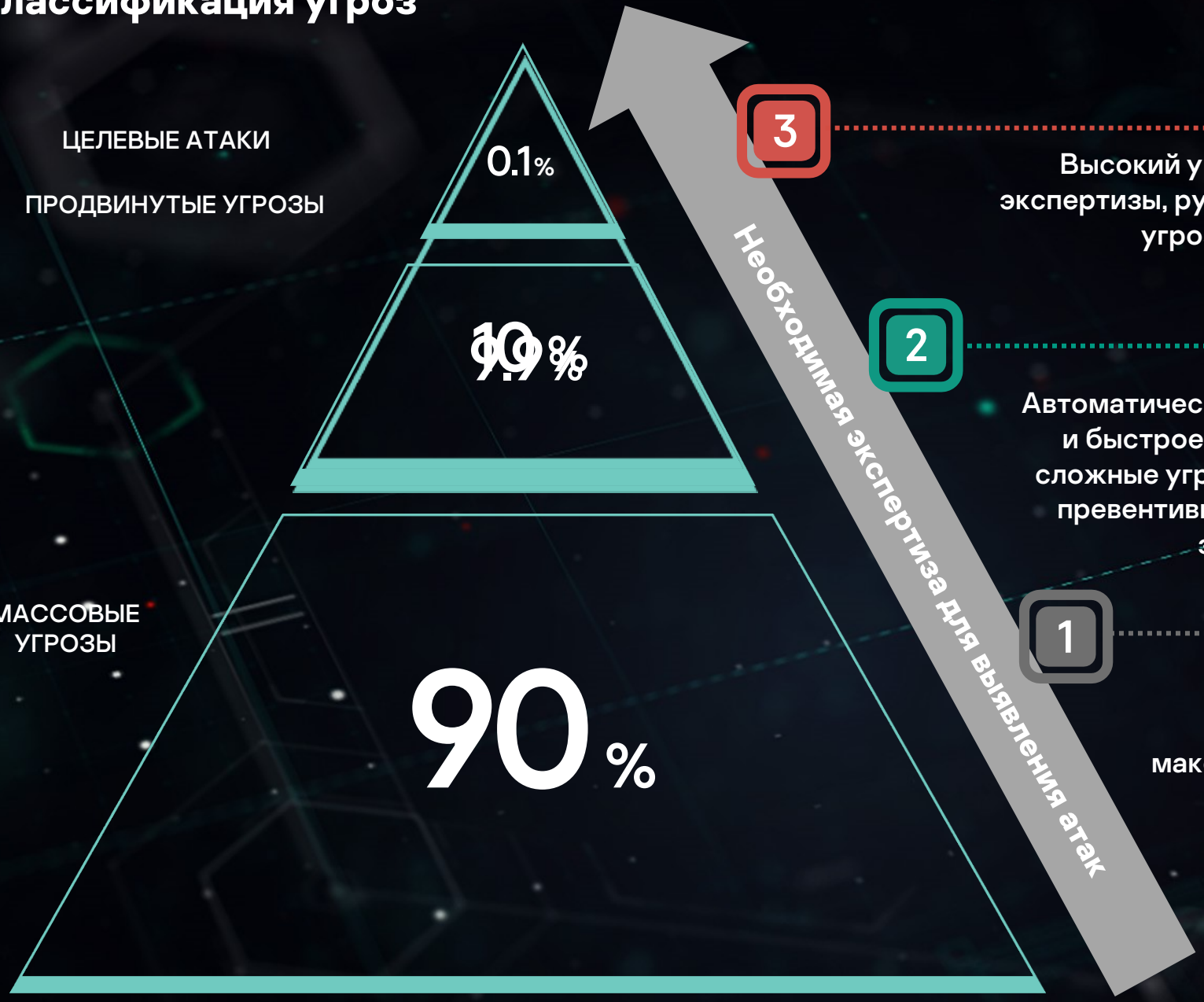
$347 тыс.
Последующие траты

Упущенная выгода	$141 тыс.
Дополнительные выплаты сотрудникам	$134 тыс.
Обращение к сторонним экспертам	$132 тыс.
Снижение кредитного рейтинга / рост страховых выплат	$129 тыс.
Дополнительные PR-мероприятия (для восстановления имиджа бренда)	$127 тыс.
Компенсации	$51 тыс.
Пени и штрафы	$31 тыс.
Улучшение ПО и инфраструктуры	$126 тыс.
Обучение	$112 тыс.
Новые сотрудники	$109 тыс.

$1.092 млн.
Средняя сумма расходов крупной компании в мире в результате утечки данных

Источник: IT security economics in 2020, Kaspersky

Классификация угроз



3

Высокий уровень экспертизы, ручной поиск угроз

ИНТЕГРИРОВАННЫЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ

2

Автоматическое детектирование и быстрое реагирование на сложные угрозы, пропущенные превентивными средствами защиты

ПЕРЕДОВАЯ ЗАЩИТА

1

Автоматическое блокирование максимально возможного числа угроз

ОСНОВЫ БЕЗОПАСНОСТИ

Портфолио Лаборатории Касперского

Экспертная защита

УРОВЕНЬ 3

АРТ И ЦЕЛЕВЫЕ АТАКИ

Expert Security

Зрелый уровень ИБ-экспертизы

- Глобальная аналитика угроз: Kaspersky Threat Intelligence
- Повышение внутренней экспертизы: Kaspersky Cybersecurity Training
- Расширенное обнаружение и реагирование: Kaspersky EDR; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack Platform
- Экспертная Поддержка: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

Оптимальная защита

УРОВЕНЬ 2

ПЕРЕДОВЫЕ УГРОЗЫ

Optimum Security

Базовая ИБ - экспертиза

- Дополнительная защита: Kaspersky Sandbox
- Наглядность и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Обогащение данных: Kaspersky Threat Intelligence Portal
- Люди: Kaspersky Security Awareness

Основа безопасности

УРОВЕНЬ 1

МАССОВЫЕ УГРОЗЫ

Security Foundations

IT

- Рабочие места: Kaspersky Security для бизнеса; Kaspersky Embedded Systems Security; Kaspersky Security для виртуальных и облачных сред
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security для интернет-шлюзов
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

Kaspersky Optimum Security

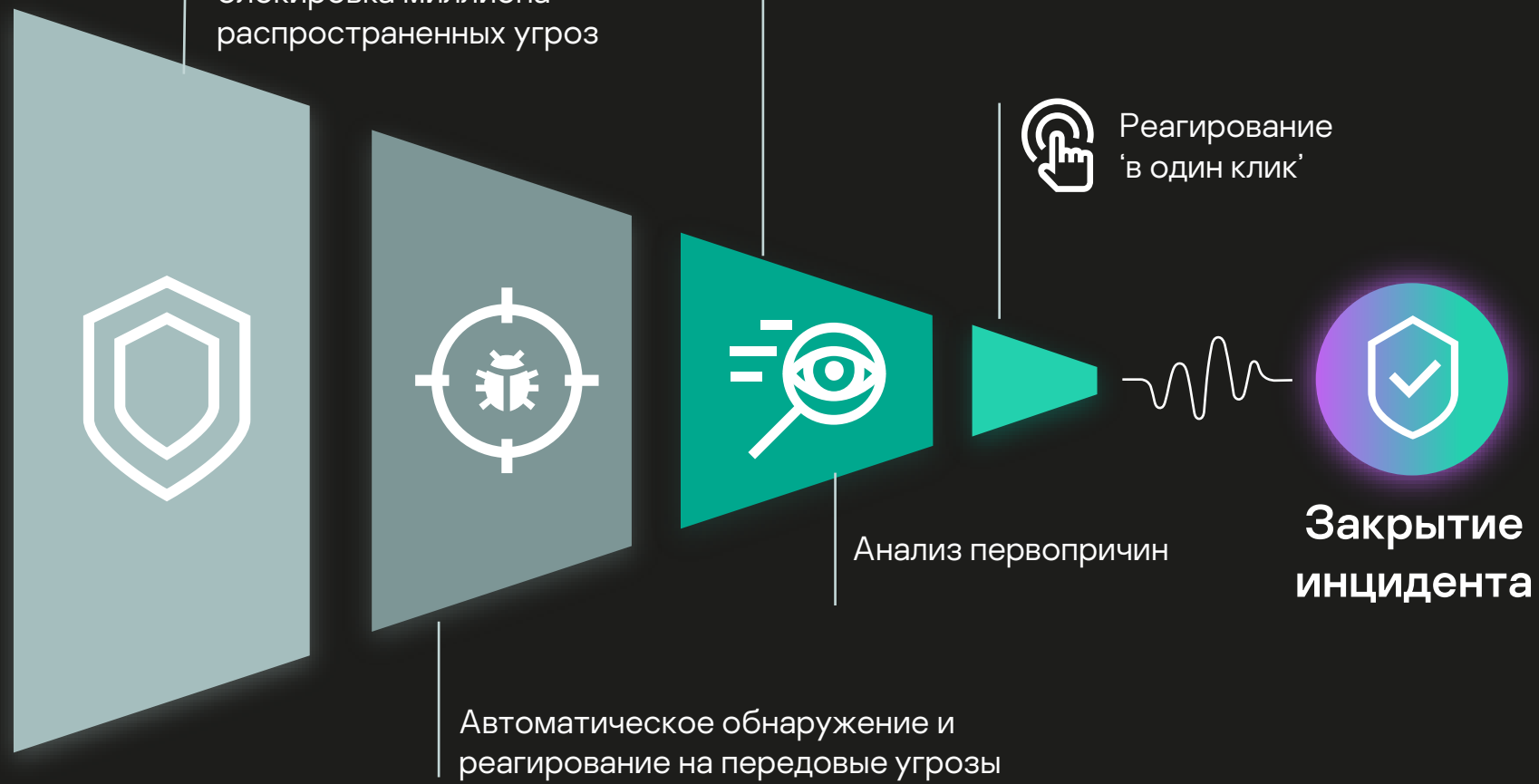
Защита от передовых угроз

Усиление защиты за счет встроенных интеграций решений

- Встроенный базовый EDR-функционал в дополнение к мощным возможностям EPP (Kaspersky Endpoint Security для бизнеса Расширенный)
- Анализ первопричин критических инцидентов
- Обнаружение на основе индикаторов компрометации (IoC)
- Кастомные возможности создания индикаторов компрометации (IoC) и автоматическое реагирование на рабочих местах на их основе
- Поддержка мер по сдерживанию и реагированию на угрозы в ‘один клик’
- Обнаружение угроз при помощи песочницы с автоматическим реагированием
- Облачная и локальная консоль

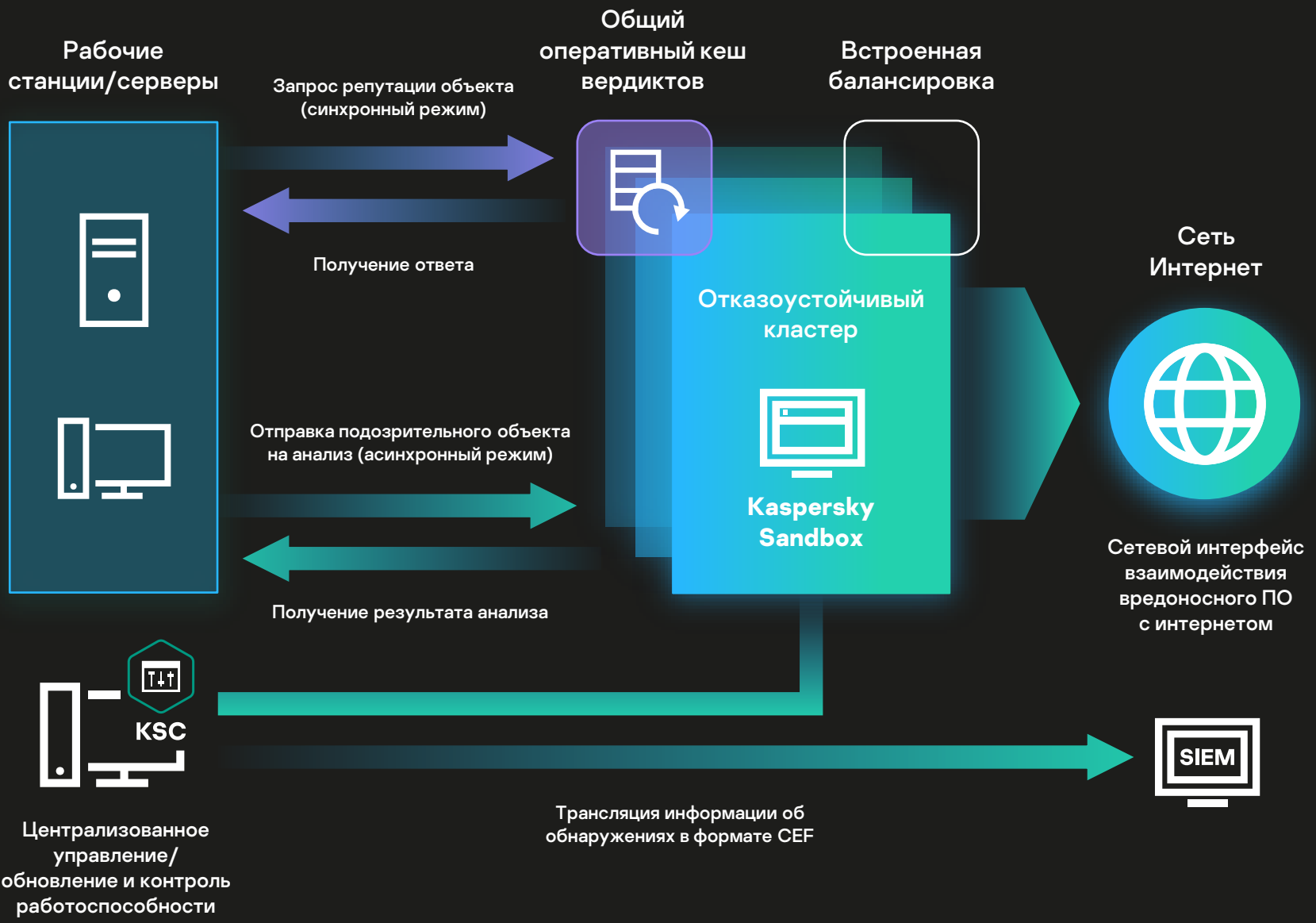
Kaspersky EDR для бизнеса Оптимальный

- Распространенные угрозы
- Эксплойты нулевого дня
- Неизвестное вредоносное ПО
- Бесфайловые угрозы
- Новые вирусы-вымогатели
- Другие виды трудно обнаруживаемых и продвинутых угроз



Включена функциональность Kaspersky Endpoint Security для бизнеса	**Максимальная автоматизация**	**Простота эксплуатации**	**Единая консоль**	**Единый агент**

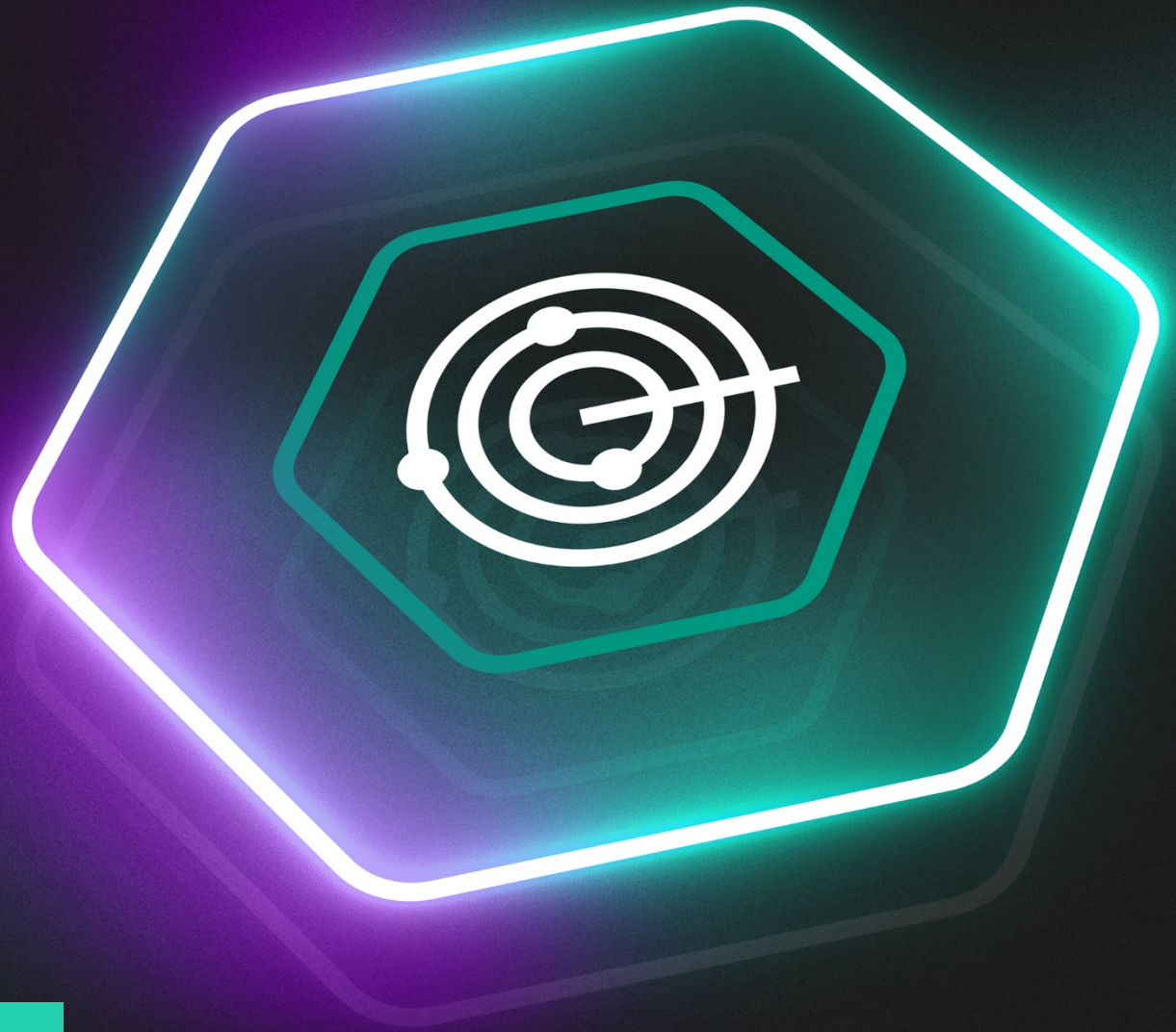
Архитектура Kaspersky Sandbox



Поддерживает проверку объектов в двух режимах — синхронном и асинхронном, что позволяет:

- Оперативно обрабатывать подозрительные объекты
- Снизить нагрузку на серверы Kaspersky Sandbox
- Повысить скорость и эффективность реагирования на угрозы

Kaspersky Expert Security



Защита от целевых атак

Предложение для ИБ-команд с высоким уровнем экспертизы

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК ОТ СЛОЖНЫХ И APT-ПОДОБНЫХ АТАК

ЗАЩИТА СЕТИ И КОНЕЧНЫХ ТОЧЕК ОТ ЦЕЛЕВЫХ И APT-ПОДОБНЫХ АТАК

Kaspersky EDR

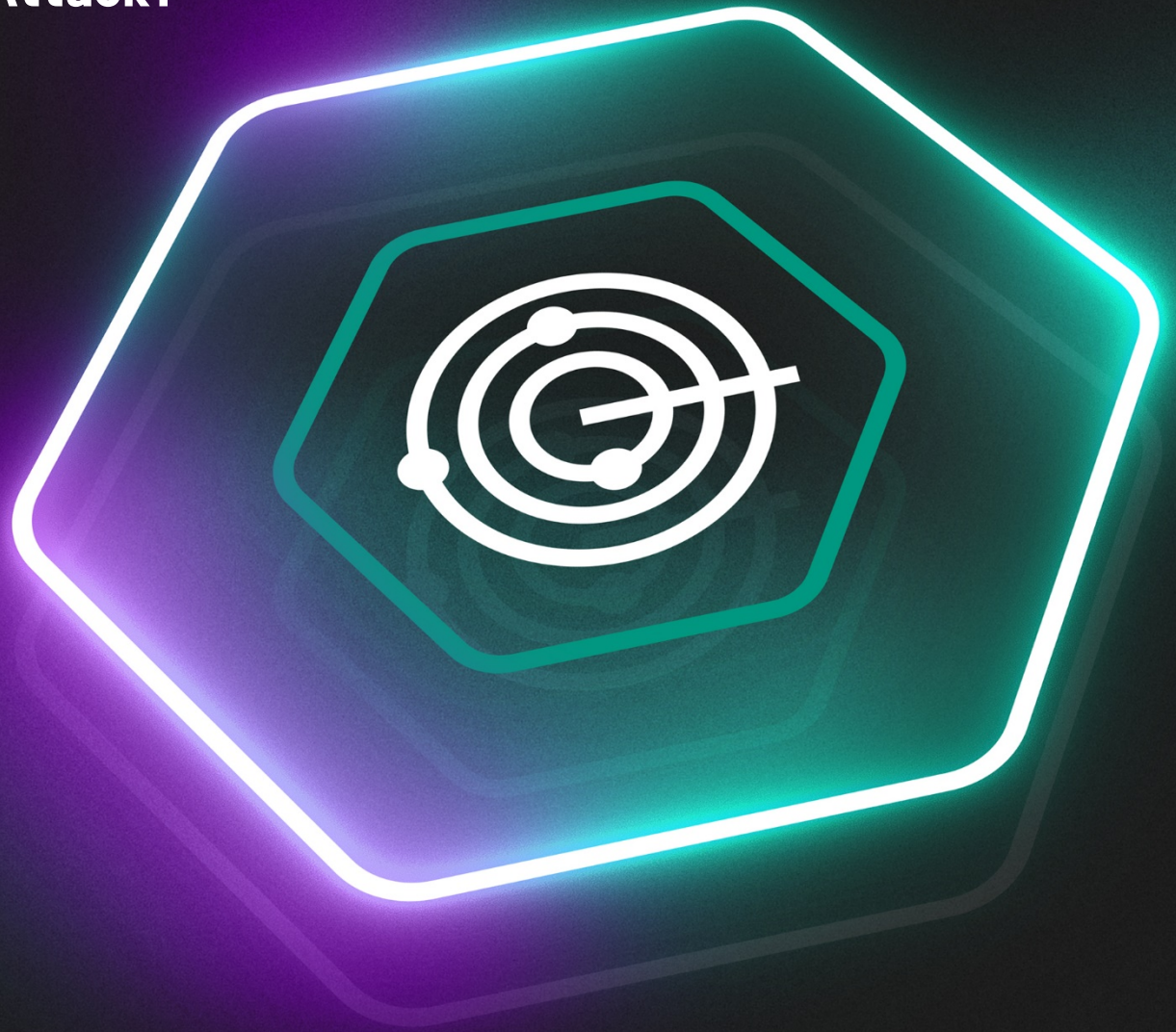
- Высокий уровень защиты конечных устройств и повышение эффективности SOC
- Мощный EDR-инструмент в дополнение к Kaspersky Security для бизнеса (+Kaspersky Security for Windows Security) и Kaspersky Hybrid Cloud Security, а также работает совместно со сторонними EPP
- Продвинутые возможности обнаружения угроз, ретроспективный анализ и детальное расследование
- Уникальные индикаторы атак (IoA), доступ в базу знаний об угрозах и сопоставление с матрицей тактик и техник злоумышленников MITRE ATT&CK
- Проактивный поиск угроз (Threat Hunting)
- Оперативное централизованное реагирование (в т.ч. на основе рекомендаций)

Kaspersky Anti Targeted Attack

- Комплексная XDR платформа для APT-защиты с расширенным функционалом обнаружения и реагирования на угрозы, единой серверной архитектурой и централизованным управлением из одной веб консоли
- Защита потенциальных точек входа угроз на уровне сети (+веб и почта) и конечных устройств (в состав платформы включен Kaspersky EDR)
- Комплексный инструментарий для обнаружения многомерных угроз , детального расследования, проактивнго поиска угроз и централизованного реагирования на сложные инциденты, включая меры на основе рекомендаций и реагирования на уровне шлюзов.

Что такое платформа Kaspersky Anti Targeted Attack?

Платформа Kaspersky Anti Targeted Attack (KATA) сочетает расширенный функционал для обнаружения угроз на уровне сети и возможности EDR* и представляет собой решение класса XDR. Это комплексное решение для обнаружения и реагирования на угрозы на основе унифицированной серверной архитектуры и централизованного управления из единой веб-консоли.

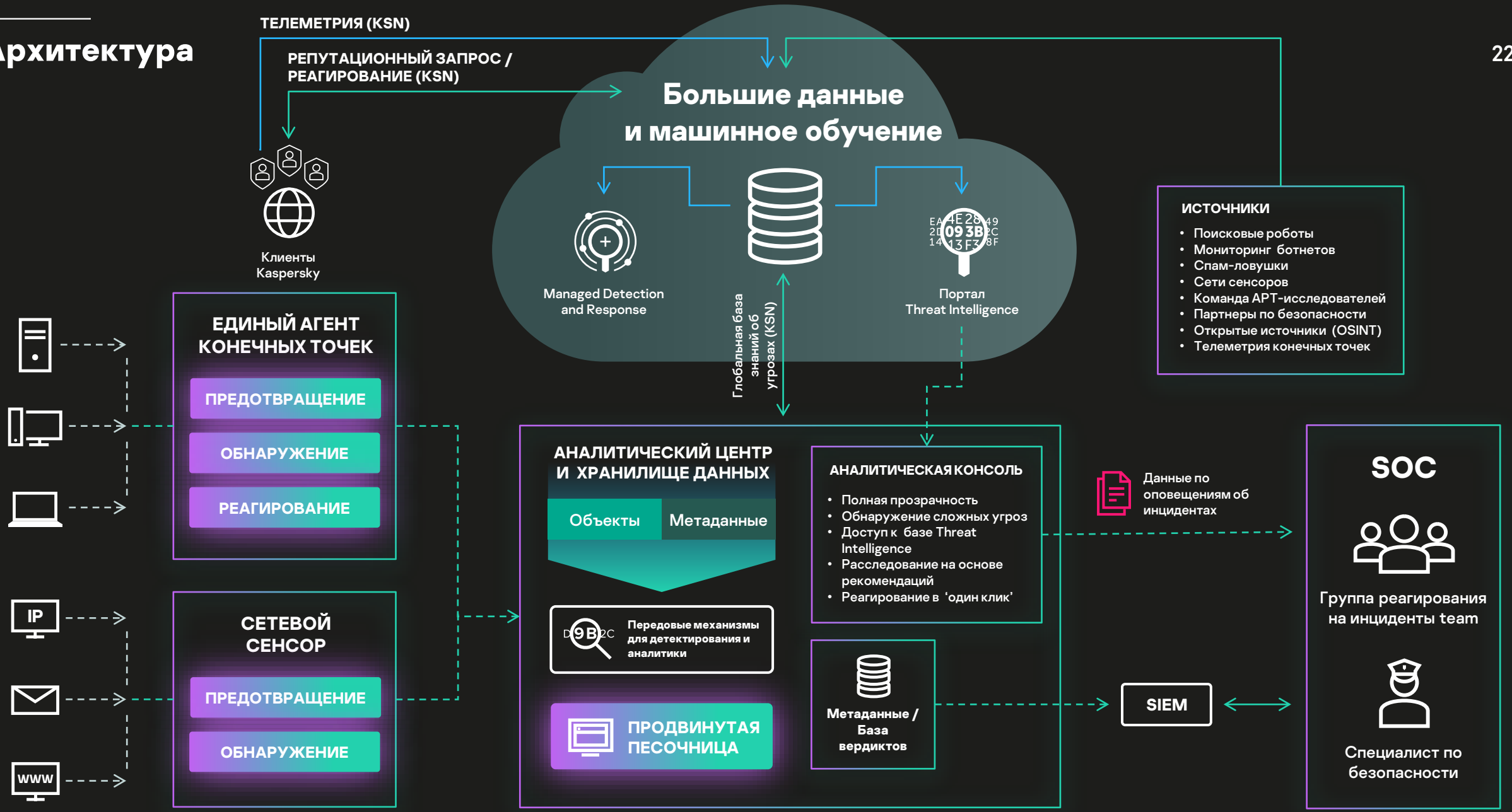


Практическое применение

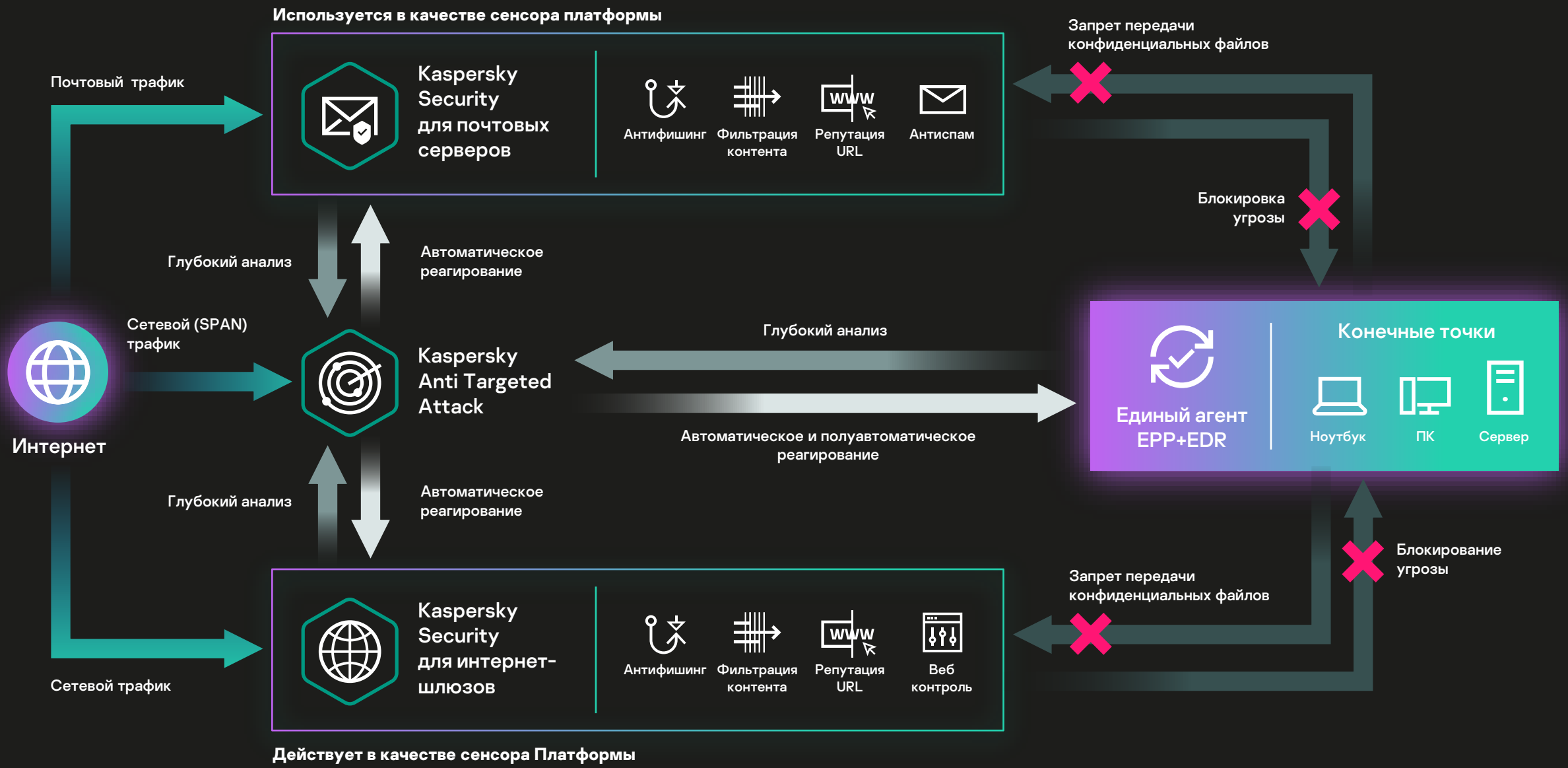
- Защита популярных потенциальных точек проникновения угроз (сеть, веб, почта, конечные точки, серверы, виртуальные машины)
- Предоставление подробных данных о событиях на уровне всей IT-инфраструктуры организации
- Комплексный инструментарий для многомерного обнаружения угроз, подробного расследования, проактивного поиска угроз и централизованного реагирования на сложные инциденты.
- Автоматическое реагирование на уровне шлюзов

*доступны только при покупке дополнительных лицензий EDR

Архитектура

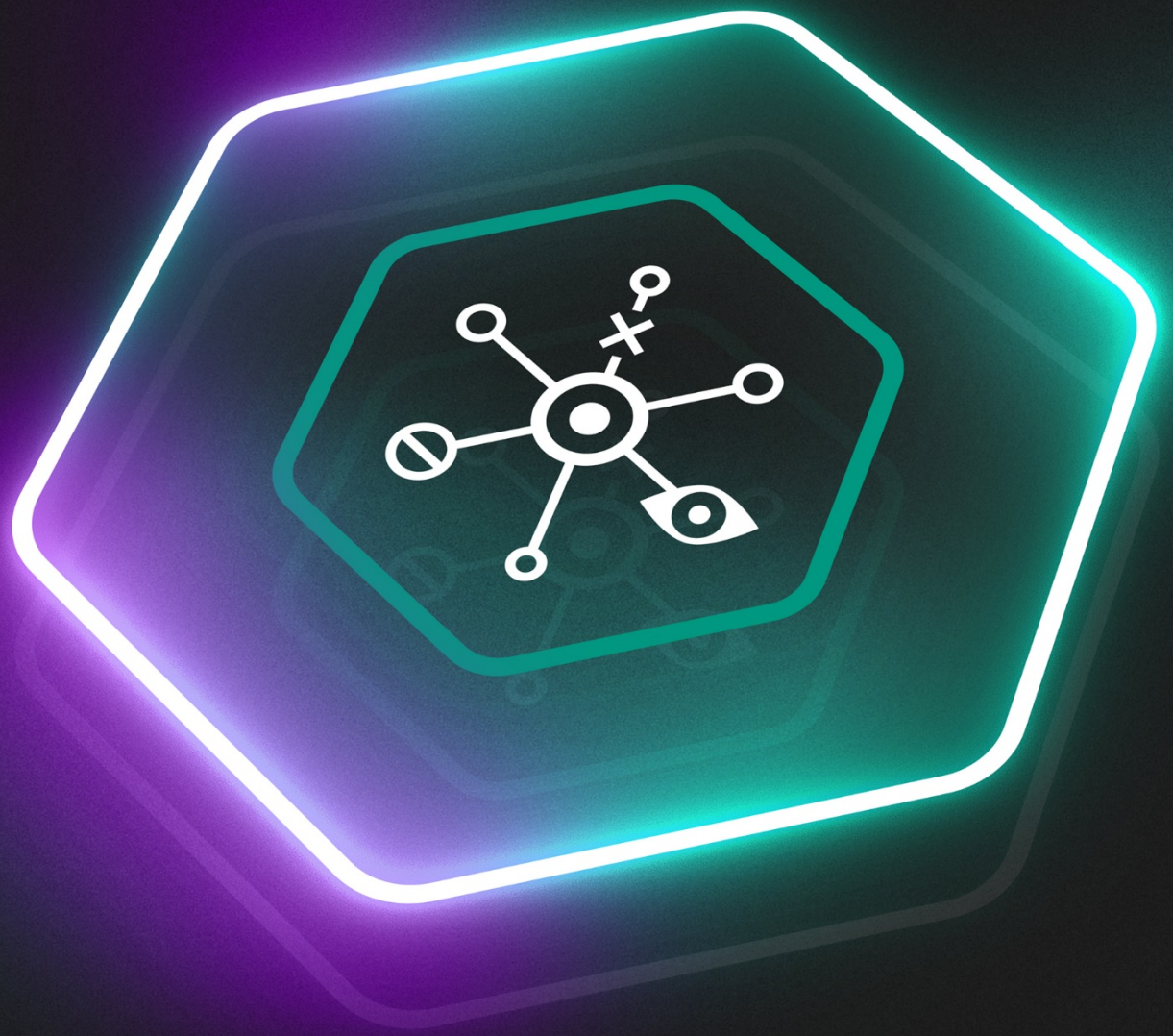


Автоматическое реагирование с помощью шлюзов



Что такое Kaspersky EDR?

Kaspersky EDR - мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутой эффективной защиты, обнаружения, проактивного поиска и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств.



Практическое применение

- Эффективное обнаружение (подтверждено оценкой MITRE ATT&CK) и оперативное реагирование на атаки
- Сбор исходных данных и вердиктов для проведения эффективного расследования и ретроспективного анализа
- Централизованное управление инцидентами с расследованием на основе рекомендаций на всех конечных устройствах
- Проактивный поиск сложных угроз
- Единый агент с Kaspersky Endpoint Security для бизнеса для всеобъемлющей защиты конечных точек
- Kaspersky EDR может входить в состав платформы Kaspersky Anti Targeted Attack (KATA), предоставляя решение с расширенными опциями обнаружения и реагирования на угрозы на уровне сети и рабочих мест (решение класса XDR)

Kaspersky Endpoint Detection and Response

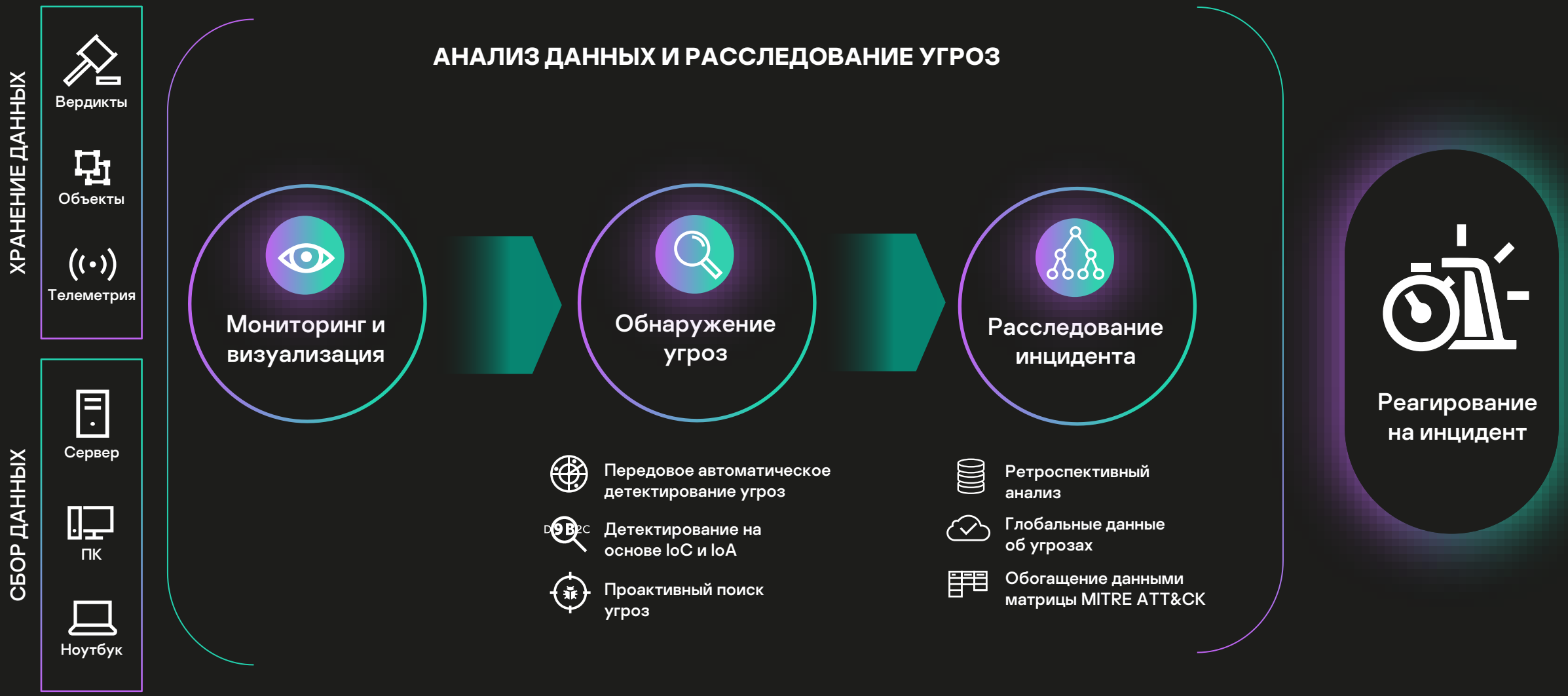


Схема централизованного реагирования на инциденты

Основные преимущества Платформы KATA с EDR

Один программный продукт с единой веб-консолью

Автоматизация рутинных операций и наглядное представление

Быстрый поиск IoC, анализ IoA и сопоставление с матрицей MITRE ATT&CK, доступ в TI

Автоматический сбор и централизованное хранение данных

Инструментарий для проактивного поиска угроз

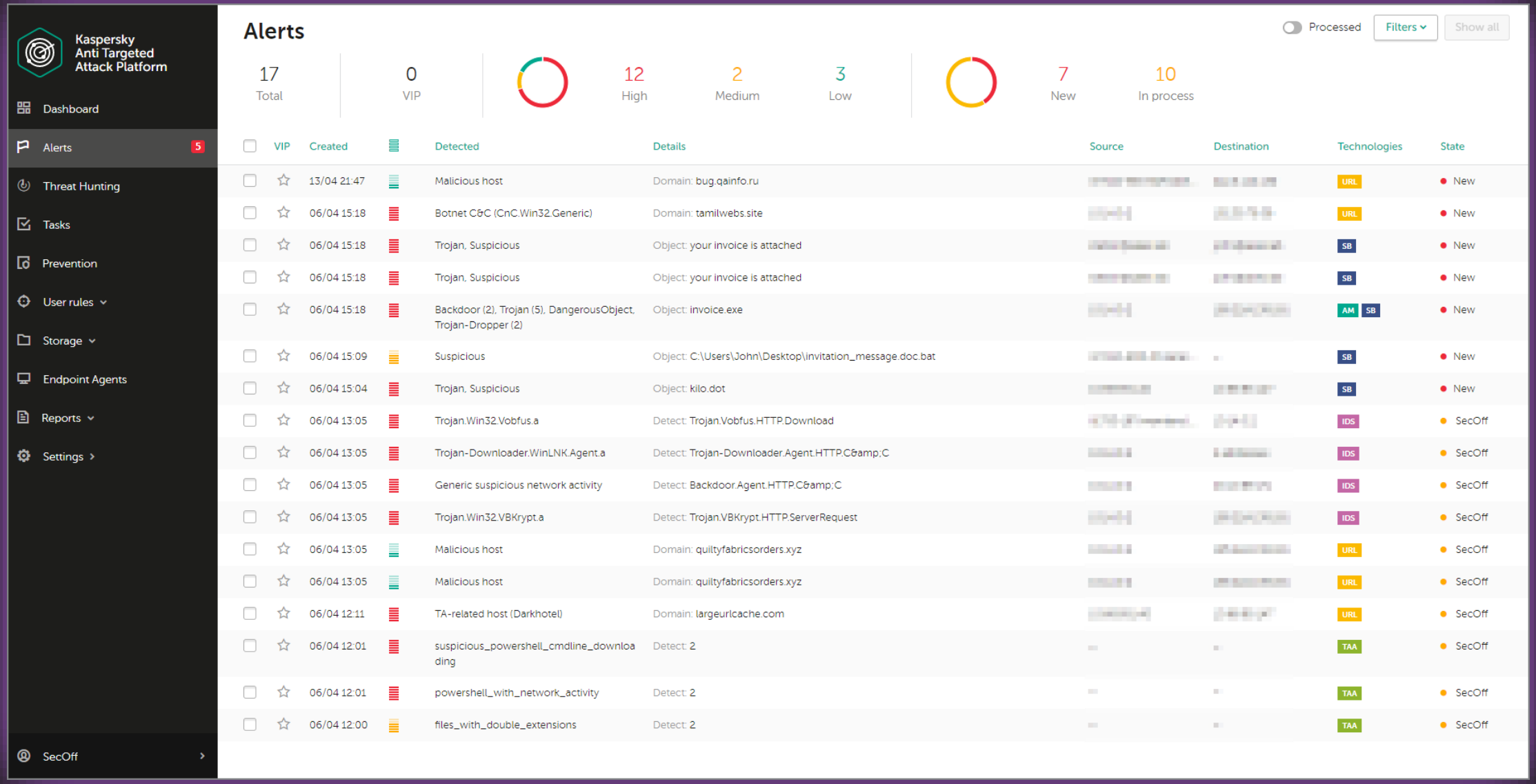
Взаимодействие с превентивными технологиями и обогащение SIEM/SOC

Централизованный процесс реагирования

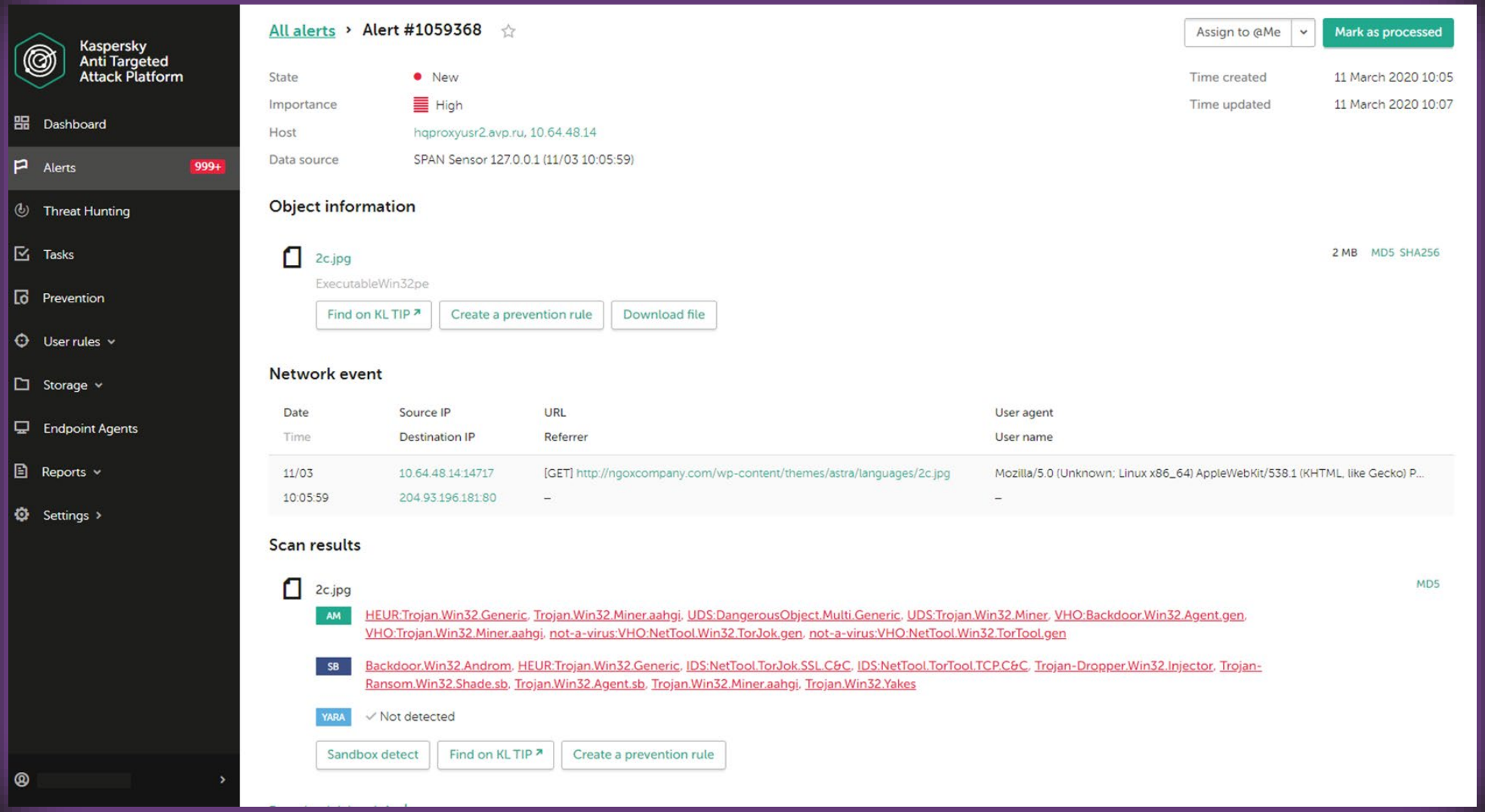
- Предоставляет комплексный единый инструментарий защиты
- Защищает множество точек входа потенциальной атаки
- Создает целостную картину происходящего
- Автоматизирует рутинную ручную работу
- Оптимизирует рабочую нагрузку экспертов
- Уменьшает количество ложных срабатываний и время для анализа
- Сокращает среднее время обнаружения и реагирования на инциденты (MTTD / MTTR)
- Повышает эффективность процесса реагирования на инциденты

Консоль платформы KATA – главная панель

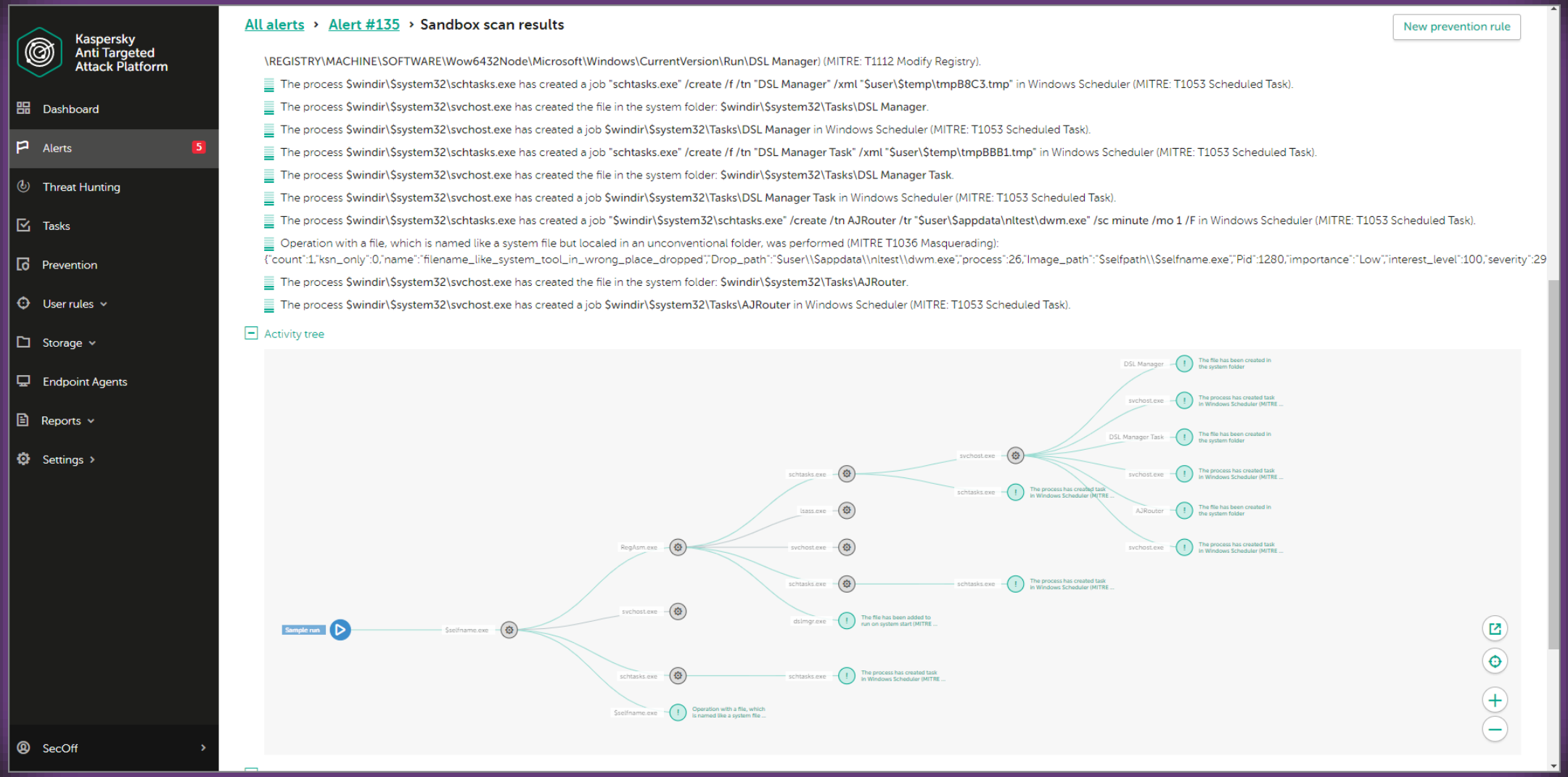
Консоль платформы KATA – Обнаружение угроз



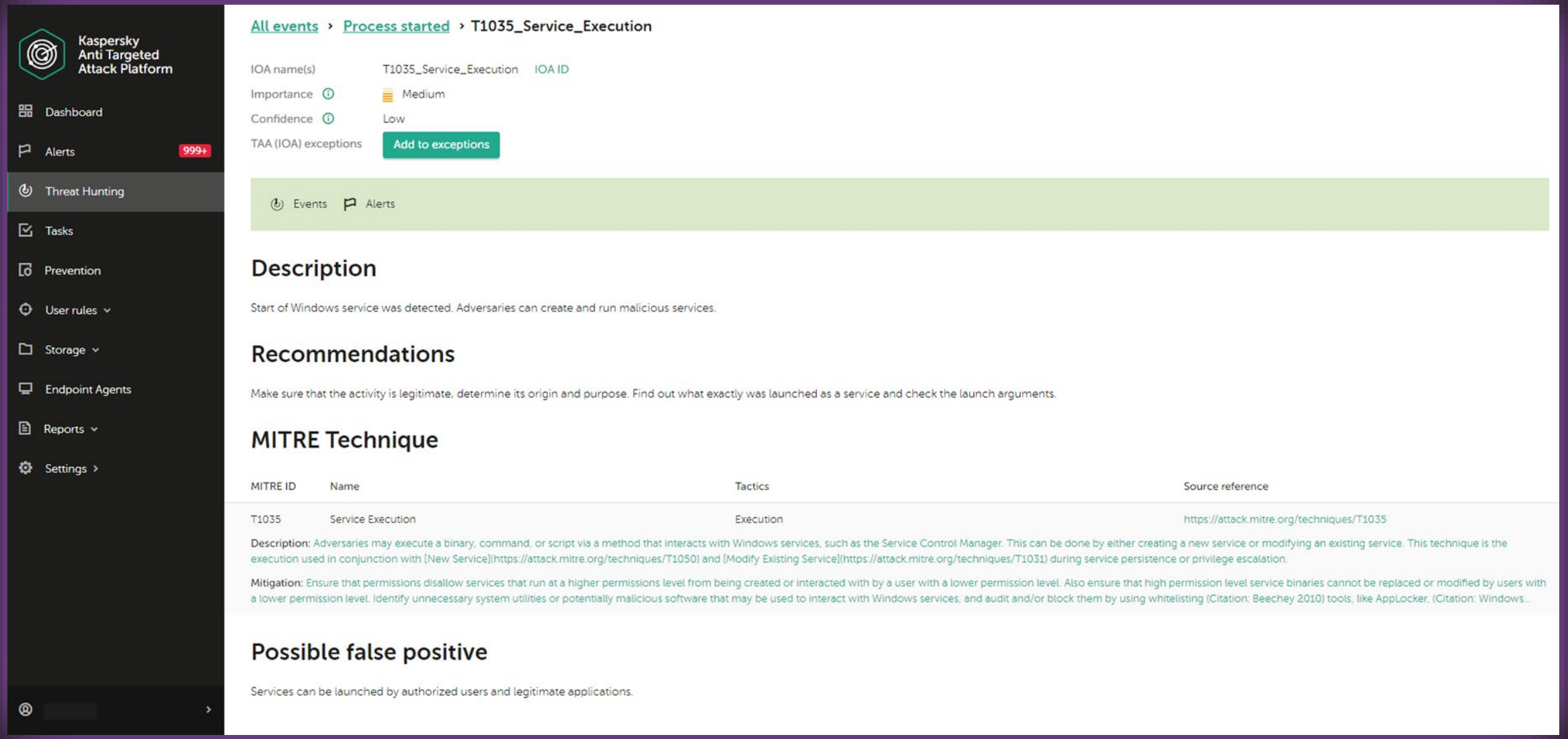
Консоль платформы KATA – Срабатывание в «песочнице» и предотвращение заражения в автоматическом режиме



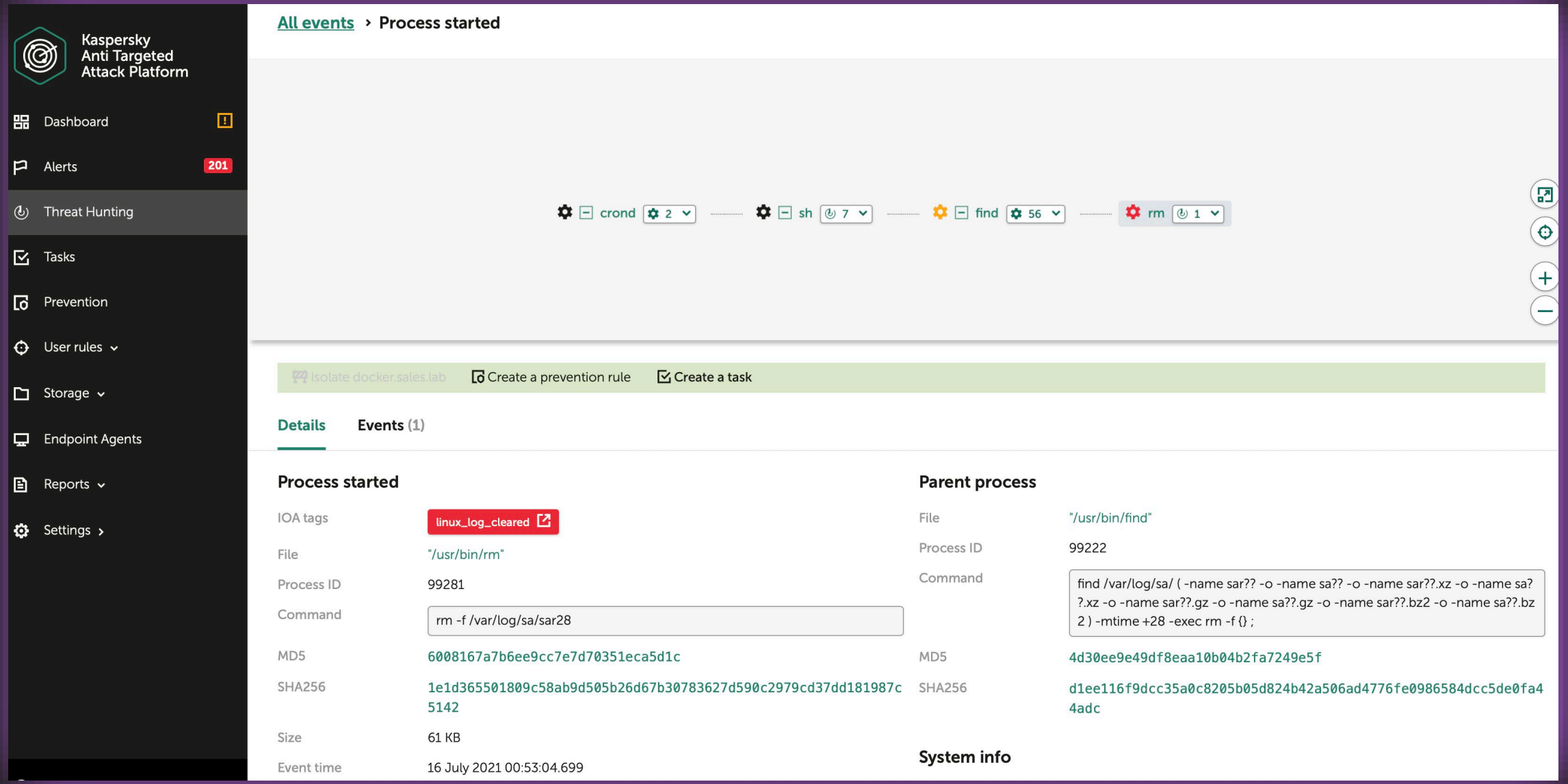
Срабатывание «в песочнице» – дерево активности, сопоставление с матрицей MITRE ATT&CK



Консоль платформы KEDR – описание сопоставления с матрицей MITRE ATT&CK



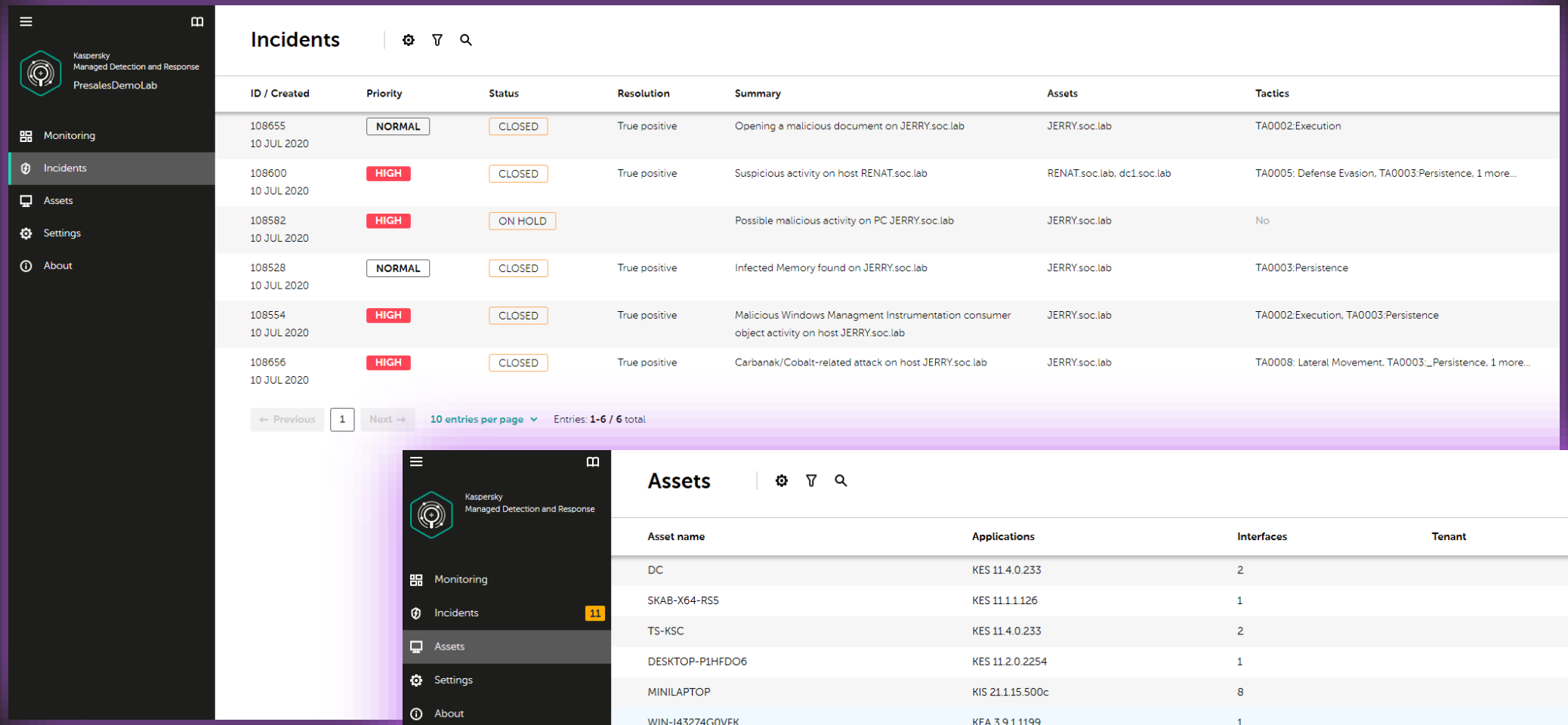
Платформа KEDR: Расследование инцидента

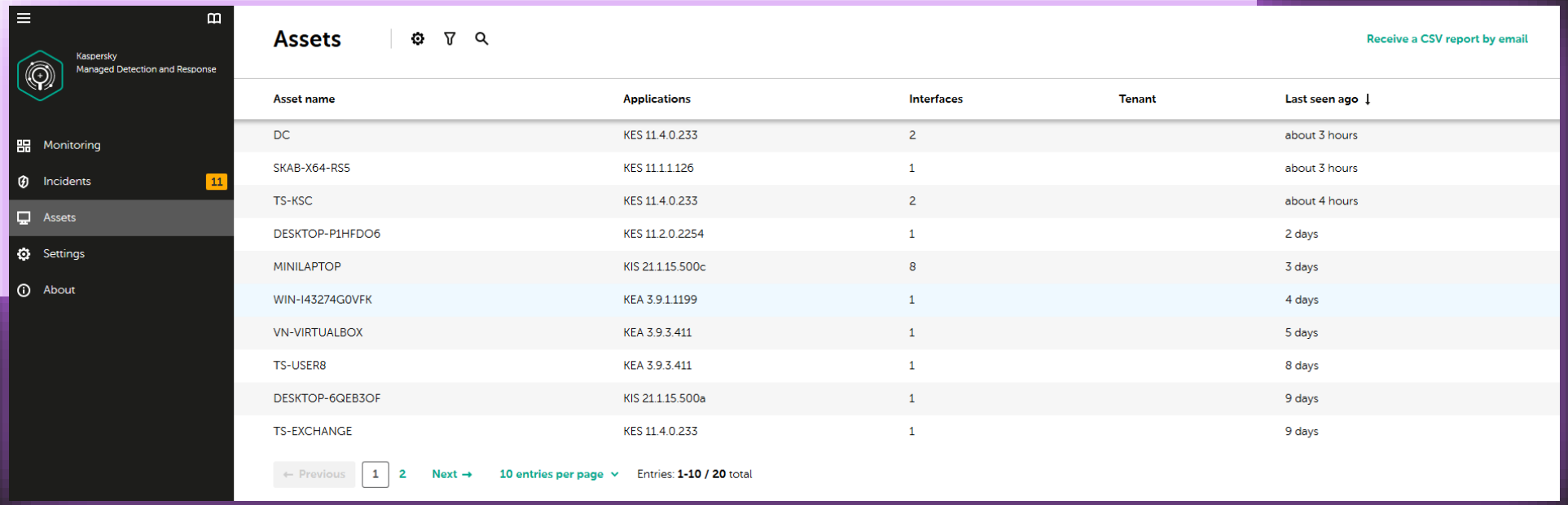


Kaspersky Managed Detection and Response

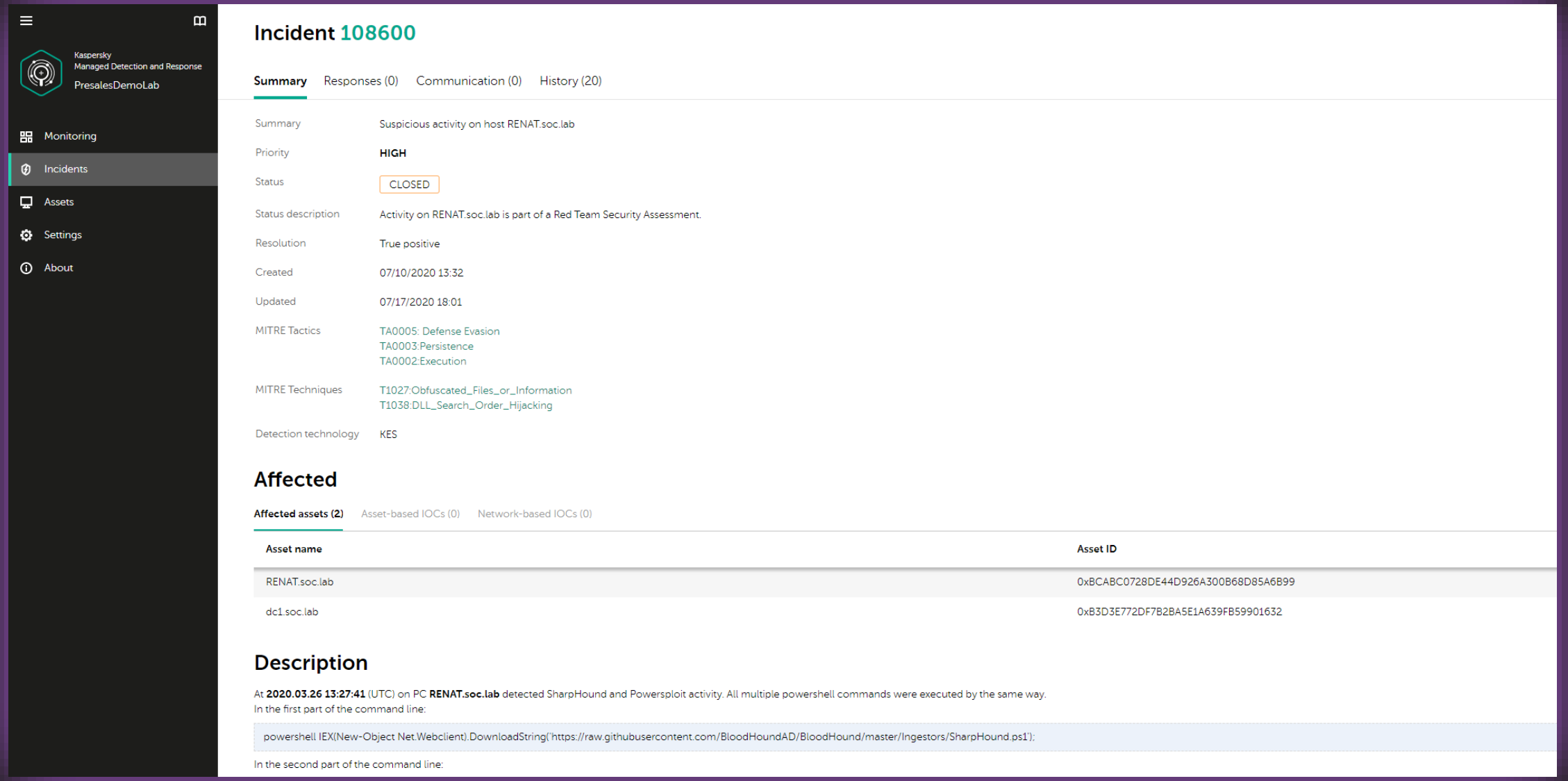
Принцип работы Kaspersky MDR

Интерфейс Kaspersky Managed Detection and Response





Интерфейс Kaspersky Managed Detection and Response



Спасибо

kaspersky