KSD 2023
Kaspersky Security Day

Ударные инструменты: оглушительные технологии борьбы с целевыми атаками

Евгений Шевченко

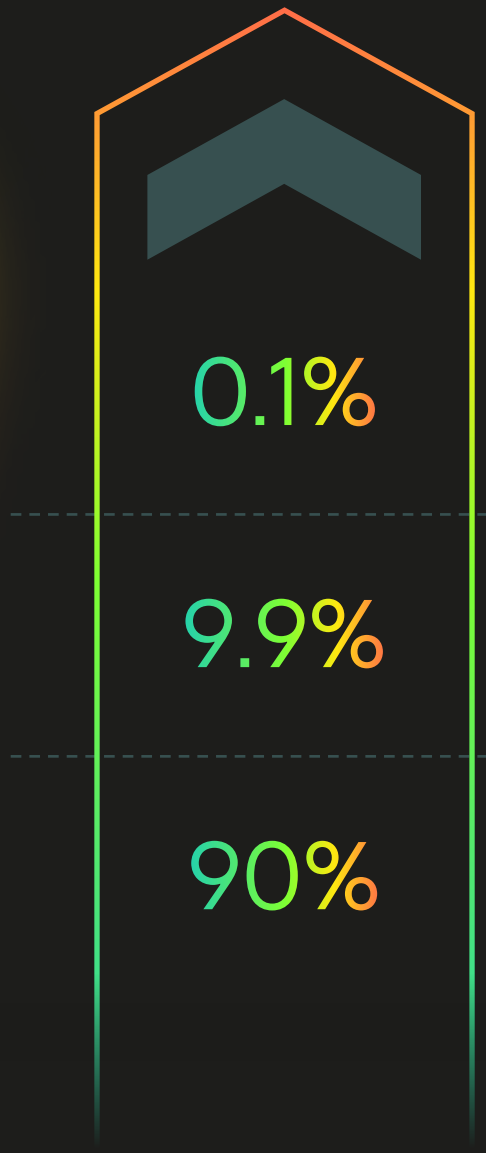
Руководитель группы по сопровождению ключевых корпоративных проектов

kaspersky

Высокоуровневый ландшафт киберугроз

99% угроз

детектируются автоматизированными системами



Кибероружие

Целевые атаки на организации

Традиционная киберпреступность

Более сложные угрозы – больше проблем

Компании сегодня придерживаются одного из подходов:

1

Игнорирование проблемы

Истории о сложных и целевых атаках не имеют к ним никакого отношения

Принятие высокого риска разрушительных последствий при продвинутой атаке

2

Использование только базовой защиты или ряда разрозненных инструментов

IT и ИБ - отделы перегружены работой

Неэффективное использование времени дорогостоящих экспертов для выполнения рутинных задач

3

Использование комплексного подхода к защите от сложных угроз и целевых атак

Сокращение количества рутинных операций, необходимых в процессе работы со сложными инцидентами

Оптимизация времени расследования и процессов реагирования на угрозы

Получение результатов без привлечения дополнительных ресурсов

Kaspersky EDR 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

Kaspersky Anti Targeted Attack

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)

Платформа KATA и KEDR Expert построены на единой технологической платформе, которая включает:

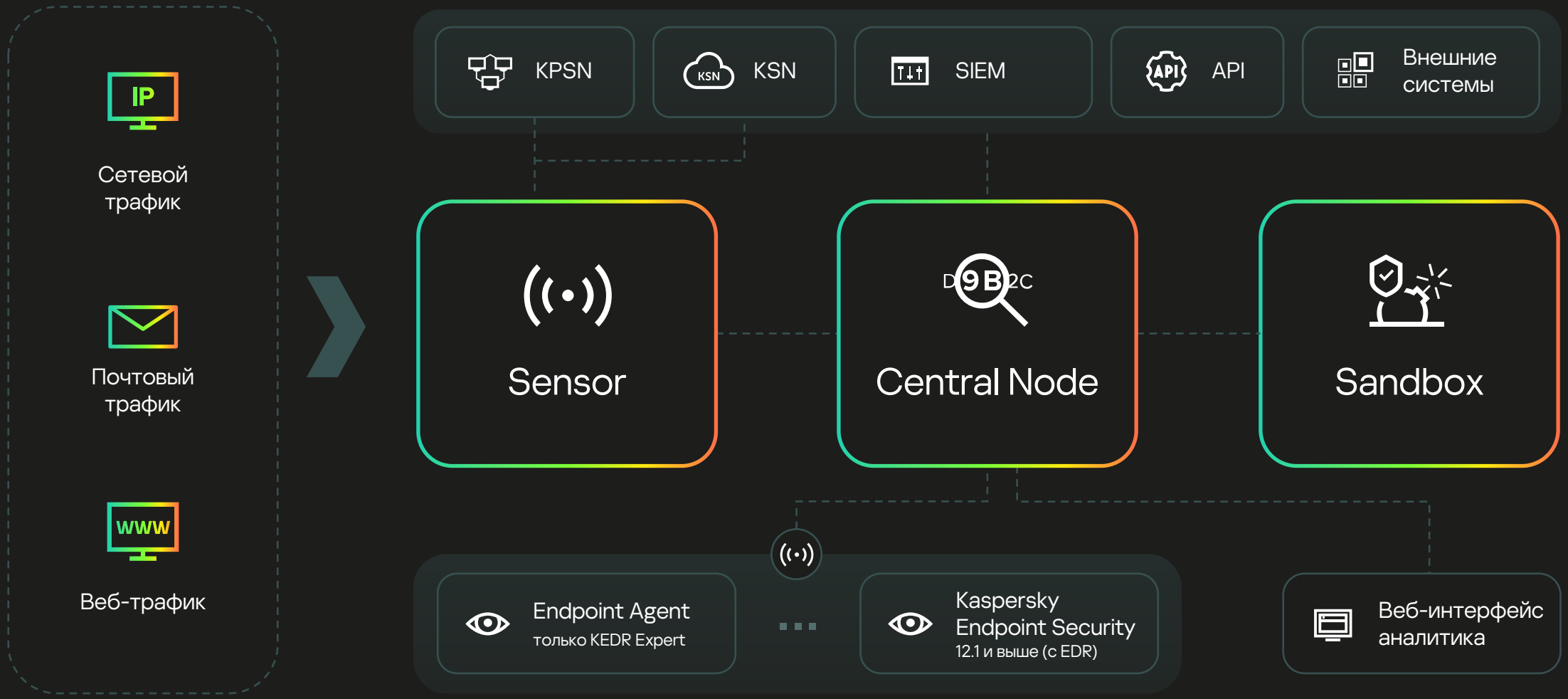
Central Node (Центр анализа)

Основной серверный компонент платформы. Выполняет проверку данных, их анализ, а также публикацию результатов исследования в веб-интерфейс программы

Sandbox (Песочница)

Запускает виртуальные образы операционных систем и отслеживает поведение файлов в них с целью обнаружения вредоносной активности и признаков целевых атак на IT-инфраструктуру организации

Архитектура решения: типовое развертывание на 3 сервера



Для автоматического сбора и последующей передачи информации для анализа, KATA и KEDR Expert используют:

Sensor (Сетевой сенсор)

Выполняет прием данных из сетевого, веб-трафика и почтового трафика, а также данных с хостов, защищаемых компонентом Endpoint Agent или Kaspersky Endpoint Security для передачи их на сервер с компонентом Central Node

Endpoint Agent (Агенты на конечных точках)

Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем семейств Microsoft Windows, GNU/Linux. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами

Компонент Central Node

На каждом сервере с компонентом Central Node работают следующие модули и технологии KATA:

Anti-Malware Engine

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

Targeted Attack Analyzer

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

Mobile Attack Analyzer

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

Kaspersky (Private) Security Network

Выполняет для KATA проверку репутации файлов и URL-адресов в базе знаний Kaspersky (Private) Security Network и предоставляет сведения о категориях веб-сайтов.

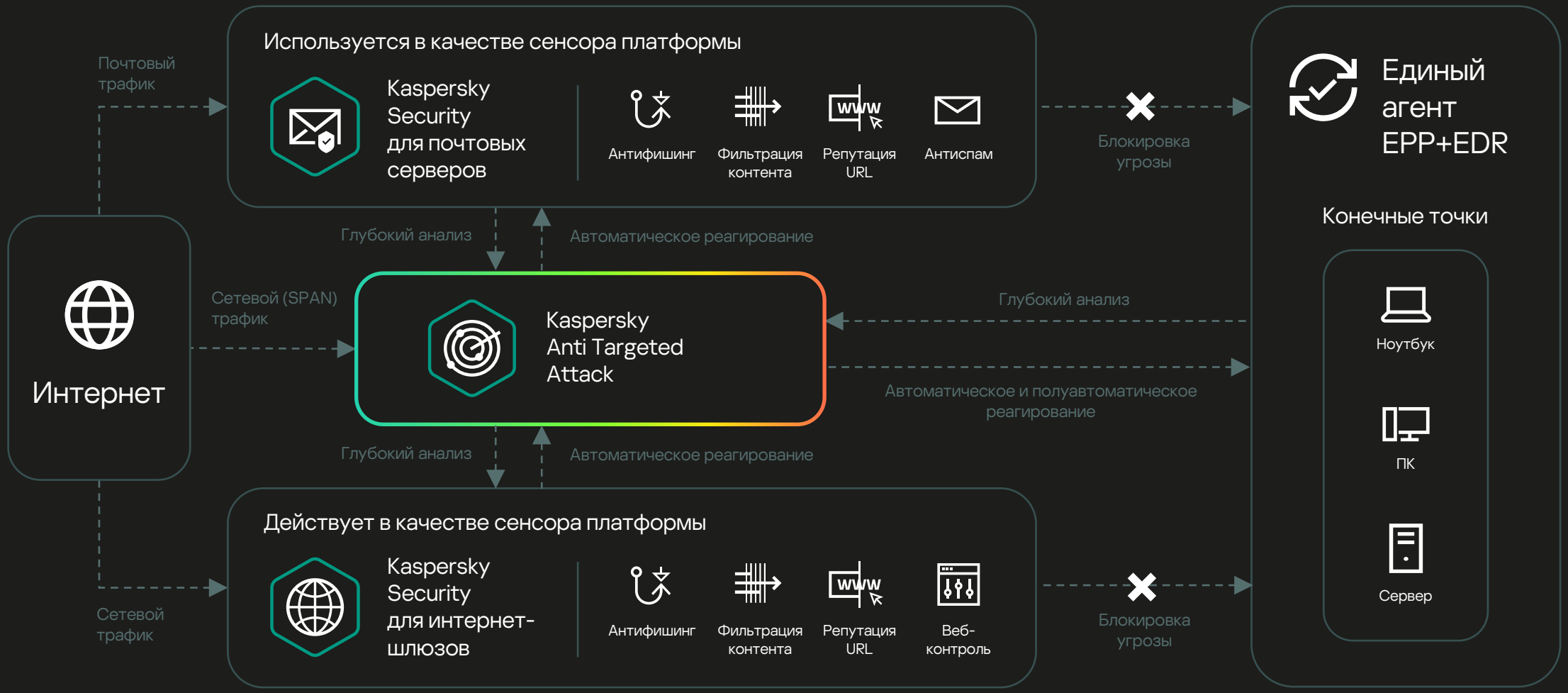
YARA

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

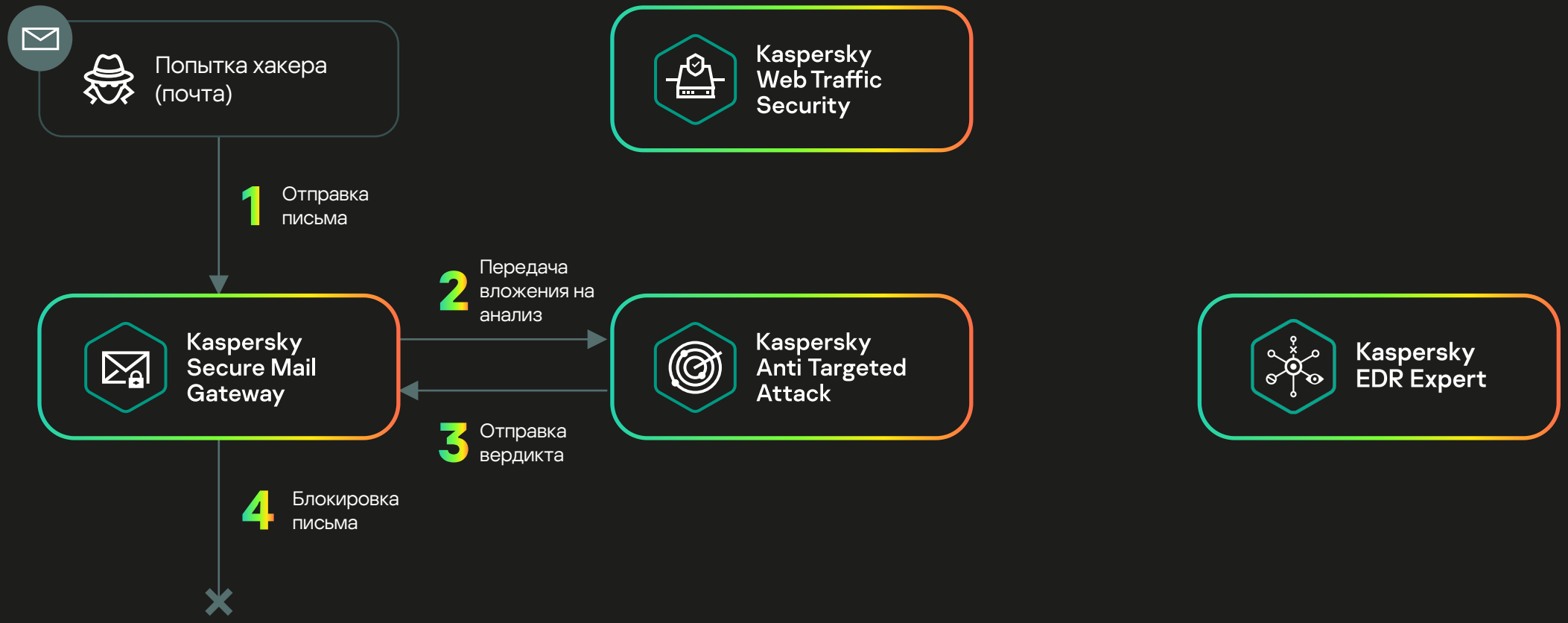
Intrusion Detection System

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.

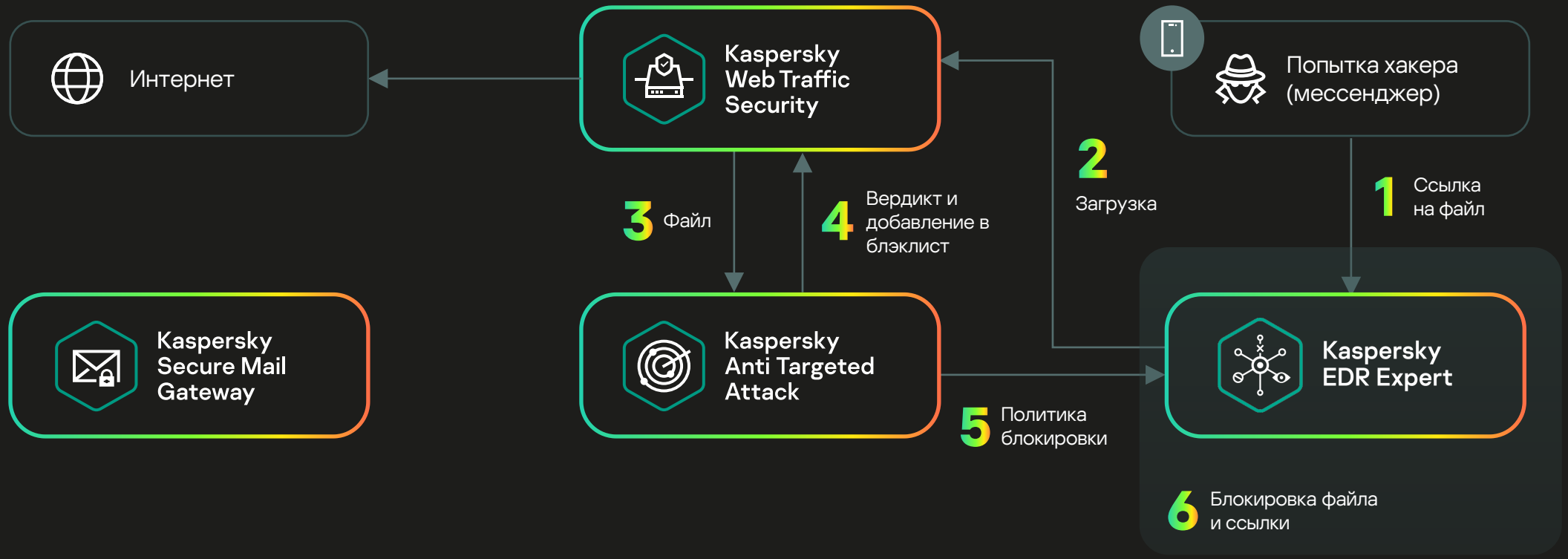
Автоматическое реагирование с помощью шлюзов



Демонстрация интеграции с KSMG и KWTS. Сценарий 1



Демонстрация интеграции с KSMG и KWTS. Сценарий 2



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)

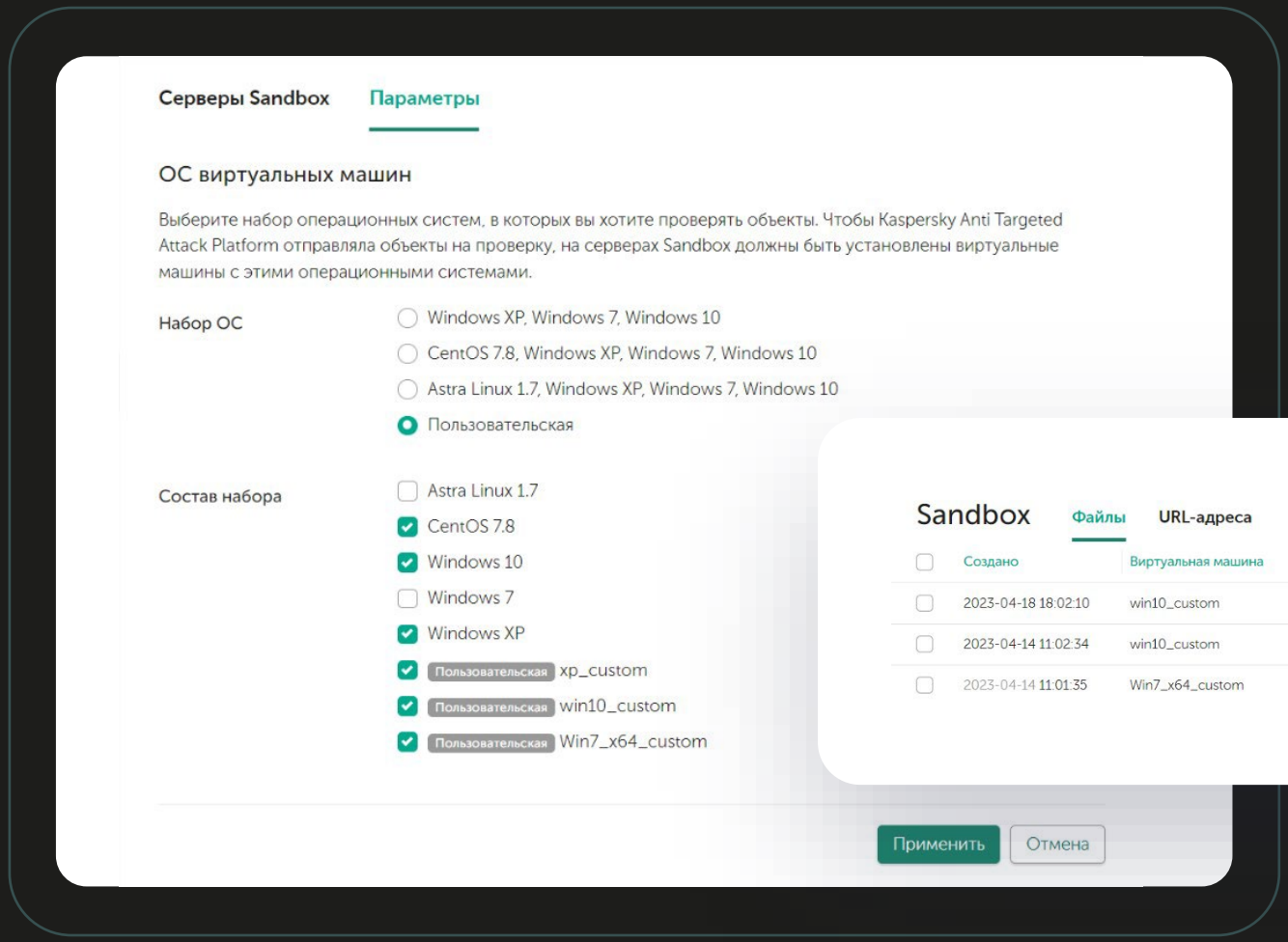
≈ 30 000

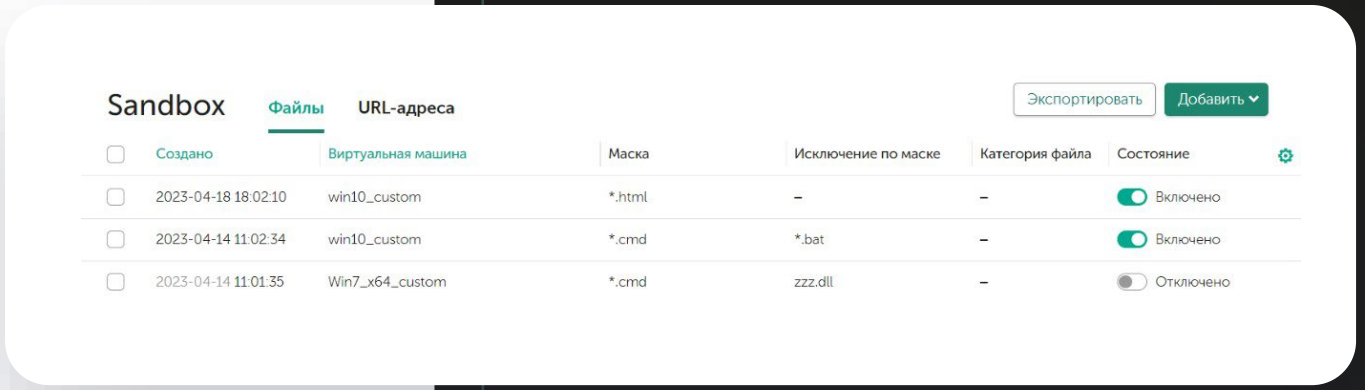
Вызовов API находятся под наблюдением

≈ 15 000

Правил для сетевого трафика (генерируемого исследуемым объектом внутри Sandbox)

Кастомизация образов Sandbox





Образ CentOS и Astra подключается опционально. Также возможен выбор собственного набора операционных систем, на основе которого будут формироваться задачи на проверку объектов в компонент Sandbox.

Компонент Endpoint Agent

KATA с KEDR Expert. Этапы взаимодействия с системой

1 Детектирование угроз

2 Визуализация атак

3 Расследование инцидентов

4 Реагирование на угрозы

5 Администрирование и интеграция

Детектирование угроз

Комплексный набор возможностей помогает обеспечить высокоэффективное обнаружение угроз на основе поведенческого анализа:

Сопоставление поведения объекта
с базой знаний MITRE ATT&CK

Ускорение системного времени
на виртуальных машинах

Проверка трафика
движком IDS на виртуальных машинах при запуске файла

Моделирование
активности пользователя

Рандомизация
среды ОС

И многое другое

Алгоритм работы Sandbox в платформе KATA

Сбор

Источники файлов и URL-адресов

- Сетевой и веб-трафик
- Конечные точки
- Почта
- Ручная загрузка

Анализ событий

Интернет

Запуск виртуальных машин

- Windows XP
- Windows 10
- Свой образ
- Windows 7
- CentOS
- Astra Linux

Мониторинг взаимодействия файла с внешними серверами

Анализ загружаемых модулей в случае обнаружения многоступенчатой атаки

1. Эмуляция
   - Противодействие техникам обхода
   - Моделирование действий пользователя
   - Ускорение времени в виртуальных машинах
   - И др.
2. Сбор артефактов
3. Анализ

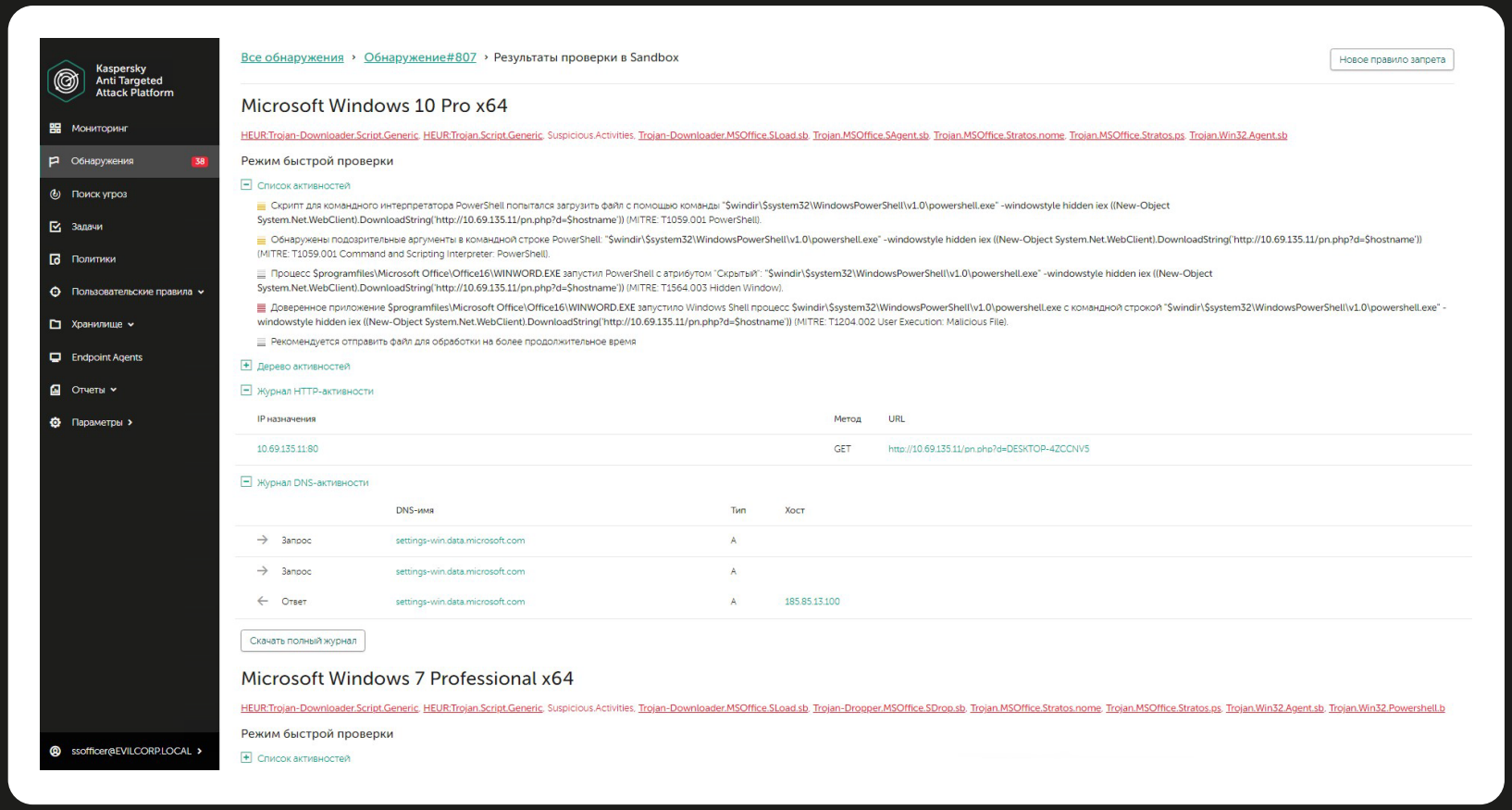
Получение вердикта

Вердикт

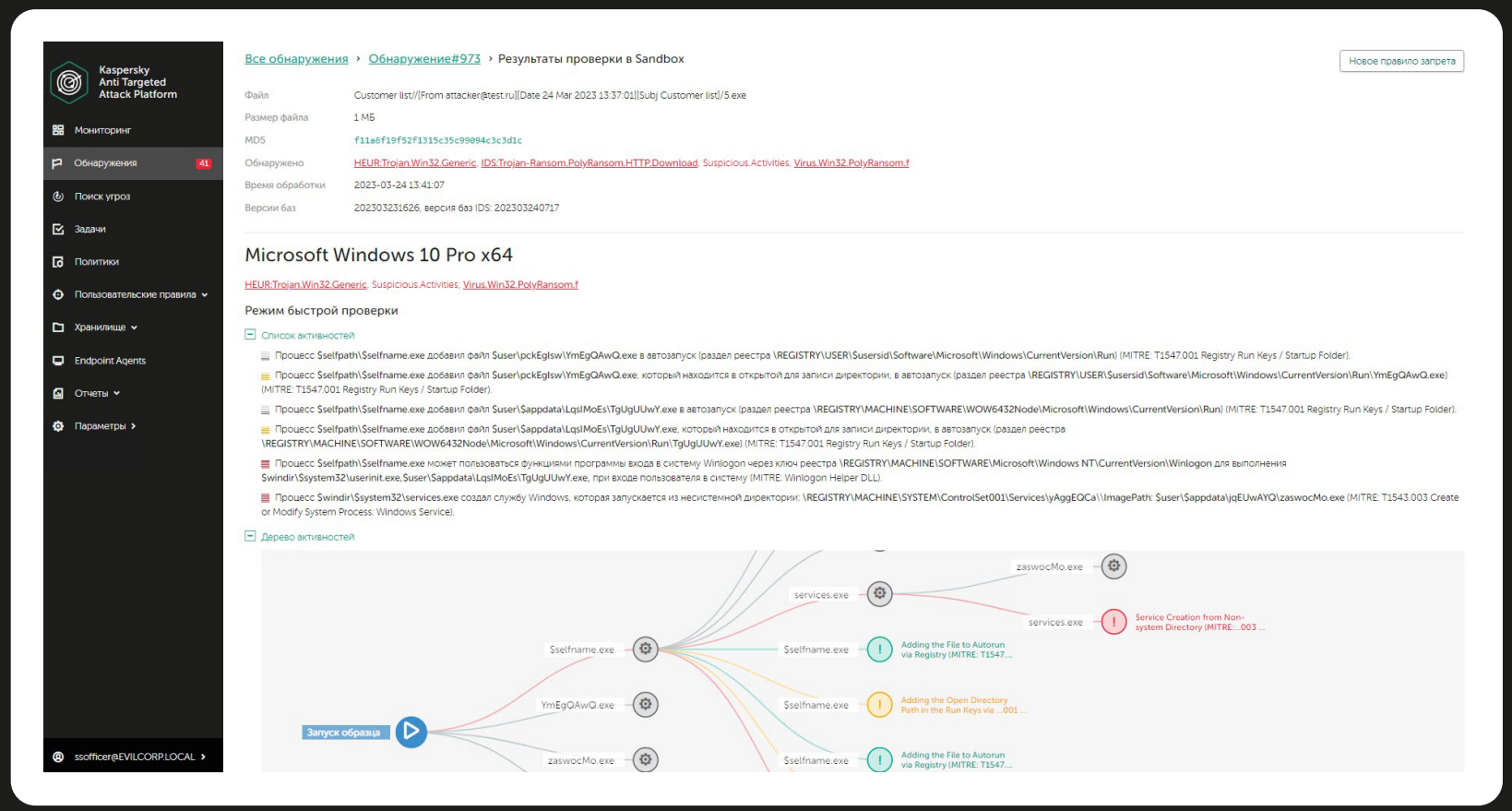
Отправка вердикта в Central Node

Расследование и реагирование

Эмуляция запуска объектов в Sandbox



Сопоставление результатов запуска файлов с MITRE ATT&CK



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

Intrusion Detection System (IDS)

Технология обнаружения вторжений включает в себя как традиционные средства обнаружения угроз в сетевом трафике посредством сигнатурного анализа, так и расширенную экспертизу базы Kaspersky Security Network и Threat Intelligence для оперативного реагирования на меняющийся ландшафт киберугроз.

В основе движка IDS — уникальный набор правил для анализа сетевого трафика, который позволяет распознать и обнаружить сетевую активность в более чем 80 протоколах. В число поддерживаемых протоколов входят: 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.

Сканирование трафика на предмет наличия признаков сетевых атак (IDS-правила) включает:

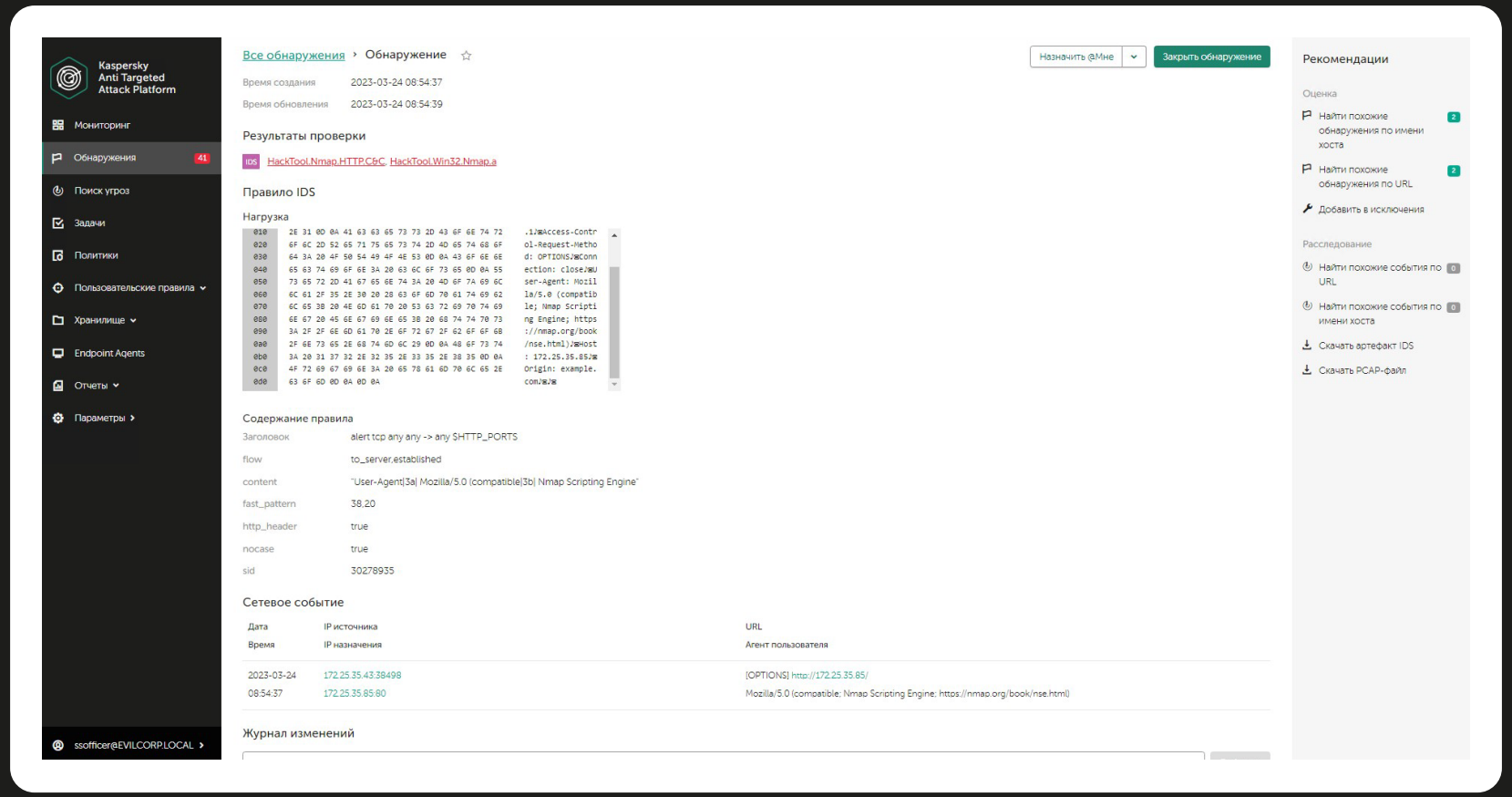
1

IDS-сигнатуры
от экспертов Kaspersky

2

Возможность загрузки
собственных правил в формате
Snort или Suricata

Пример карточки обнаружения движка IDS



Обнаружение индикаторов компрометации (IoC)

Решение KATA позволяет централизованно загружать индикаторы компрометации из потоков данных об угрозах и поддерживает возможность создания запланированных задач сканирования IoC, повышая эффективность работы аналитиков

Ретроспективное сканирование базы данных позволяет повысить качество информации о ранее замеченных событиях и инцидентах безопасности

Сканирование защищаемых хостов на предмет наличия индикаторов компрометации (IoC):

1

Возможность импорта/экспорта собственных IoC-правил в формате OpenIOC

2

Возможность поиска IoC по действию пользователя в ретроспективных данных (в событиях с хостов)

3

Возможность проверки хостов на наличие IoC по расписанию

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.

Схема взаимодействия с глобальной аналитикой киберугроз

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

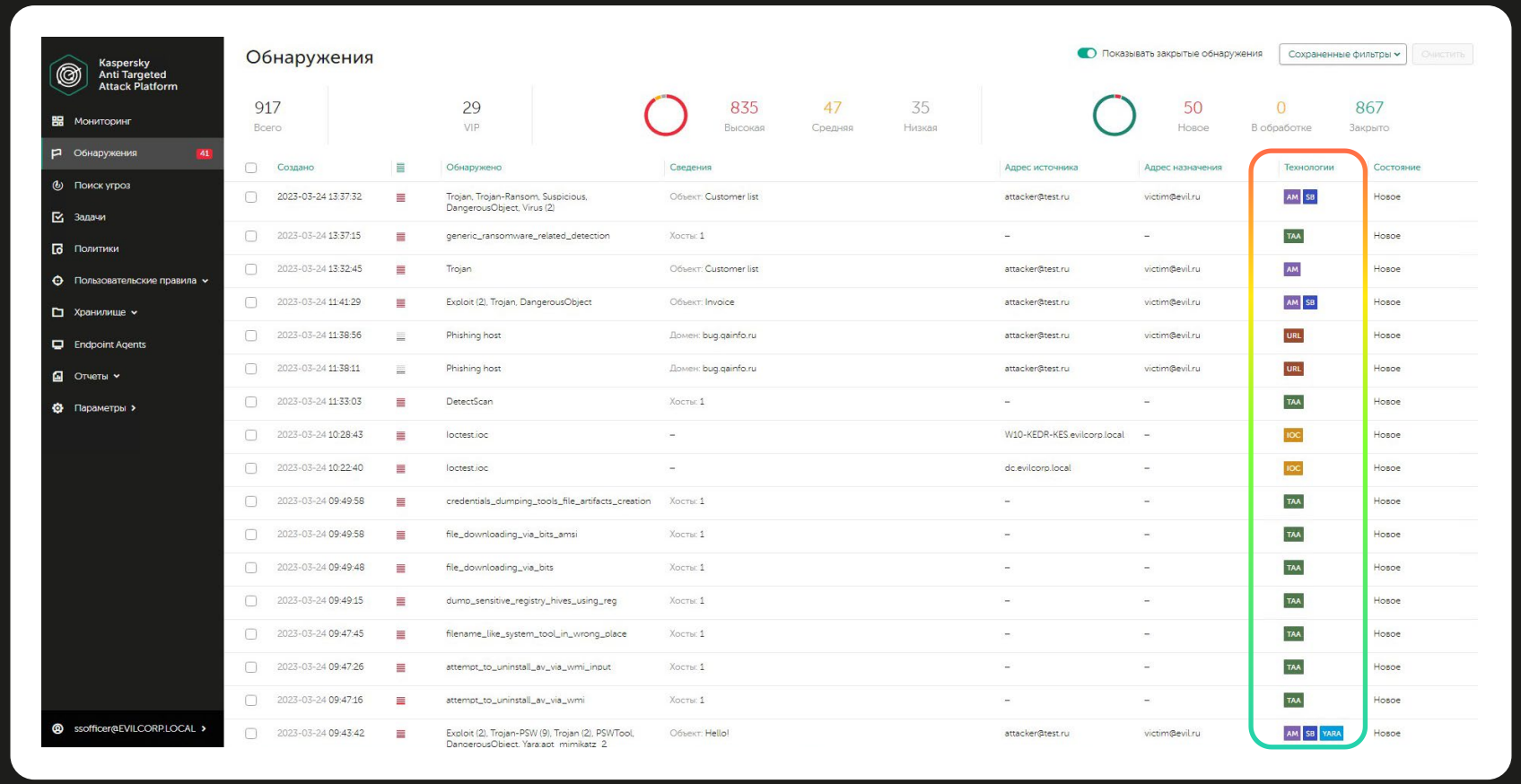
Отображение обнаружений в трафике и на хостах с указанием важности обнаружения, источника, используемой технологии детектирования

Визуализация дерева процессов, запускаемых на защищаемых хостах

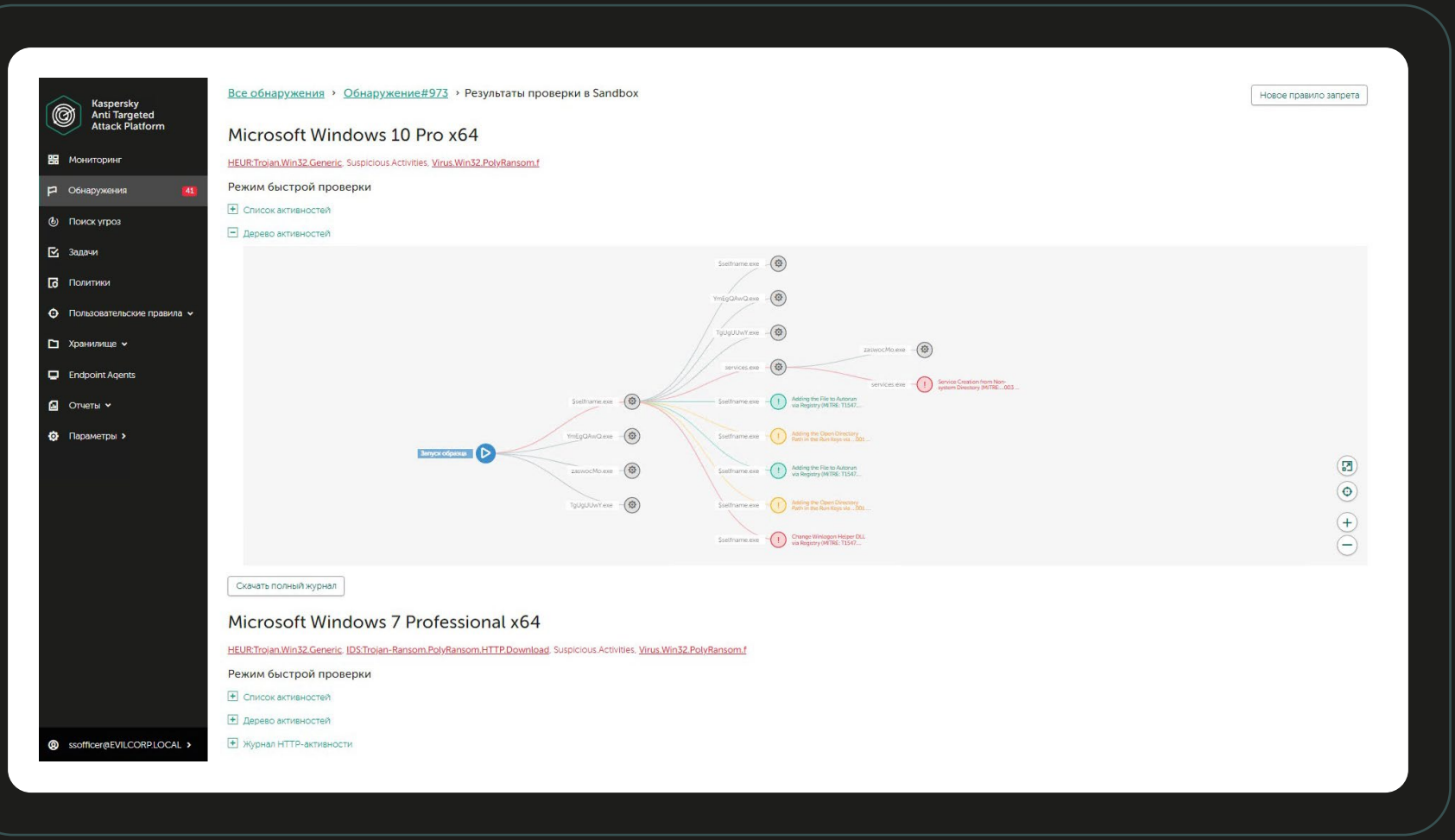
Создание и загрузка отчетов (HTML- и PDF-формат)

Гибкий механизм создания шаблонов отчетов

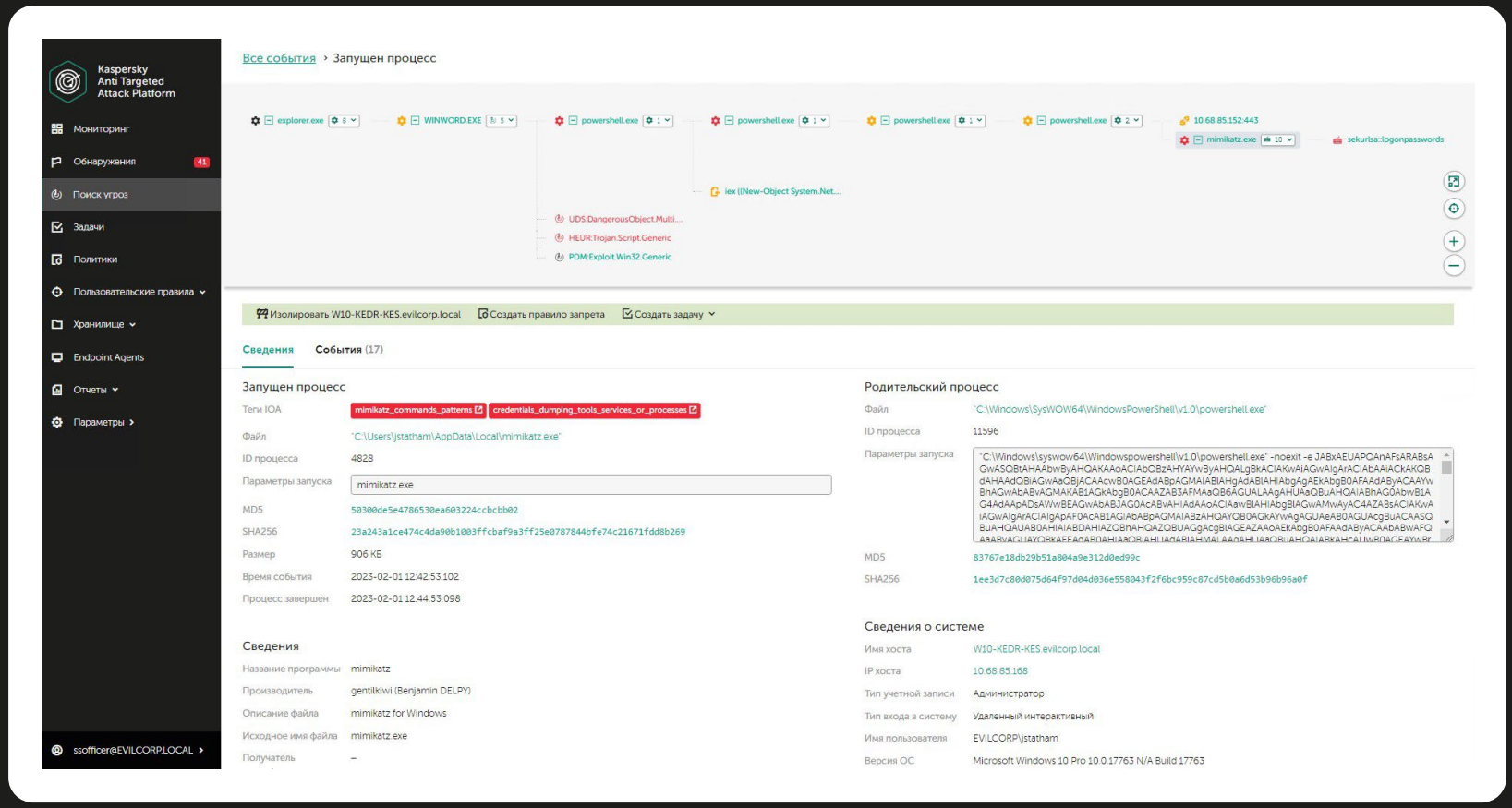
Обнаружение угроз с помощью различных технологий



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):

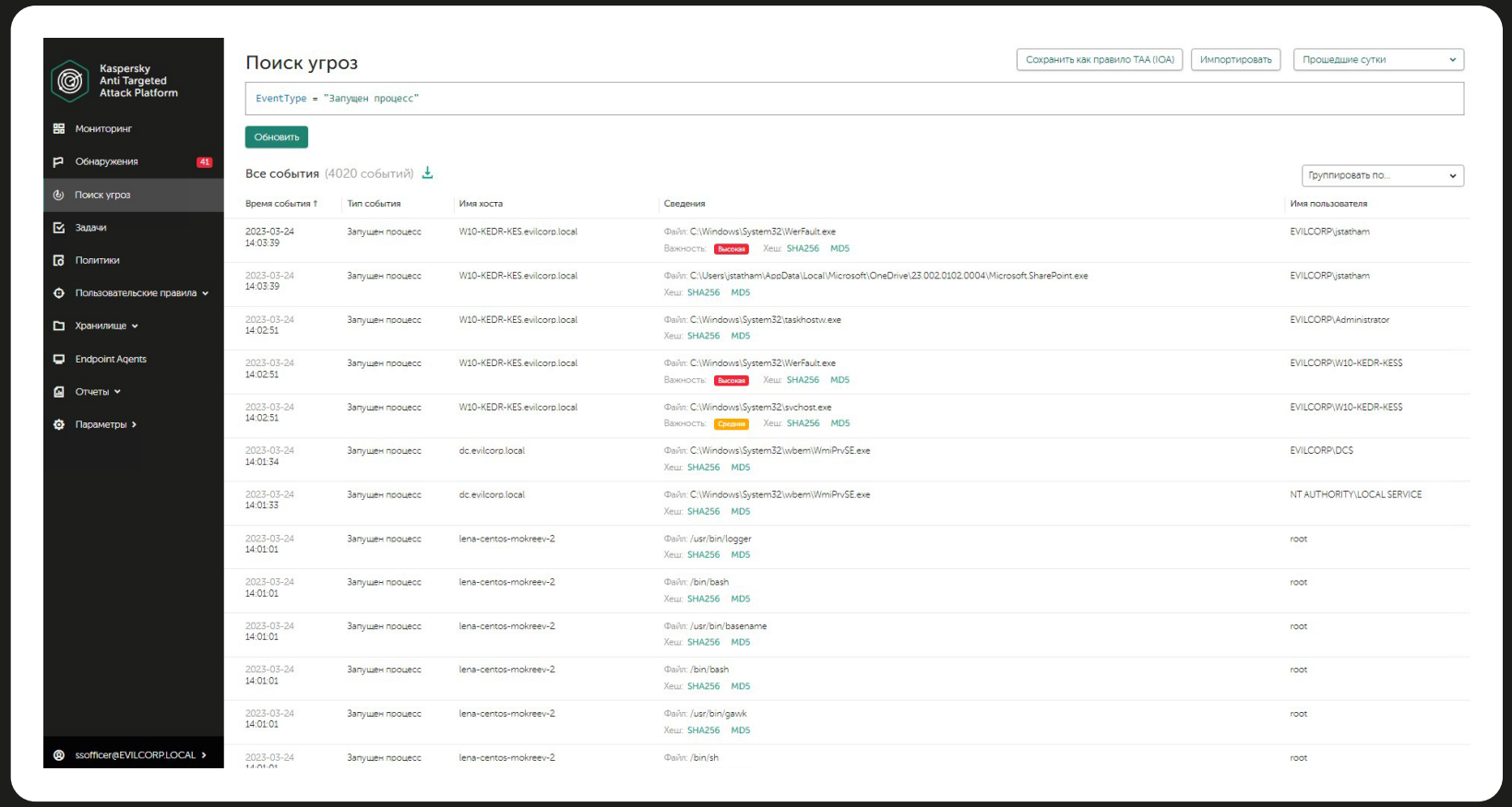
- Ретроспективный анализ по событиям, ранее собранным с защищаемых хостов
- Гибкий инструмент написания запросов поиска

Детализированные описания угроз на портале threats.kaspersky.com

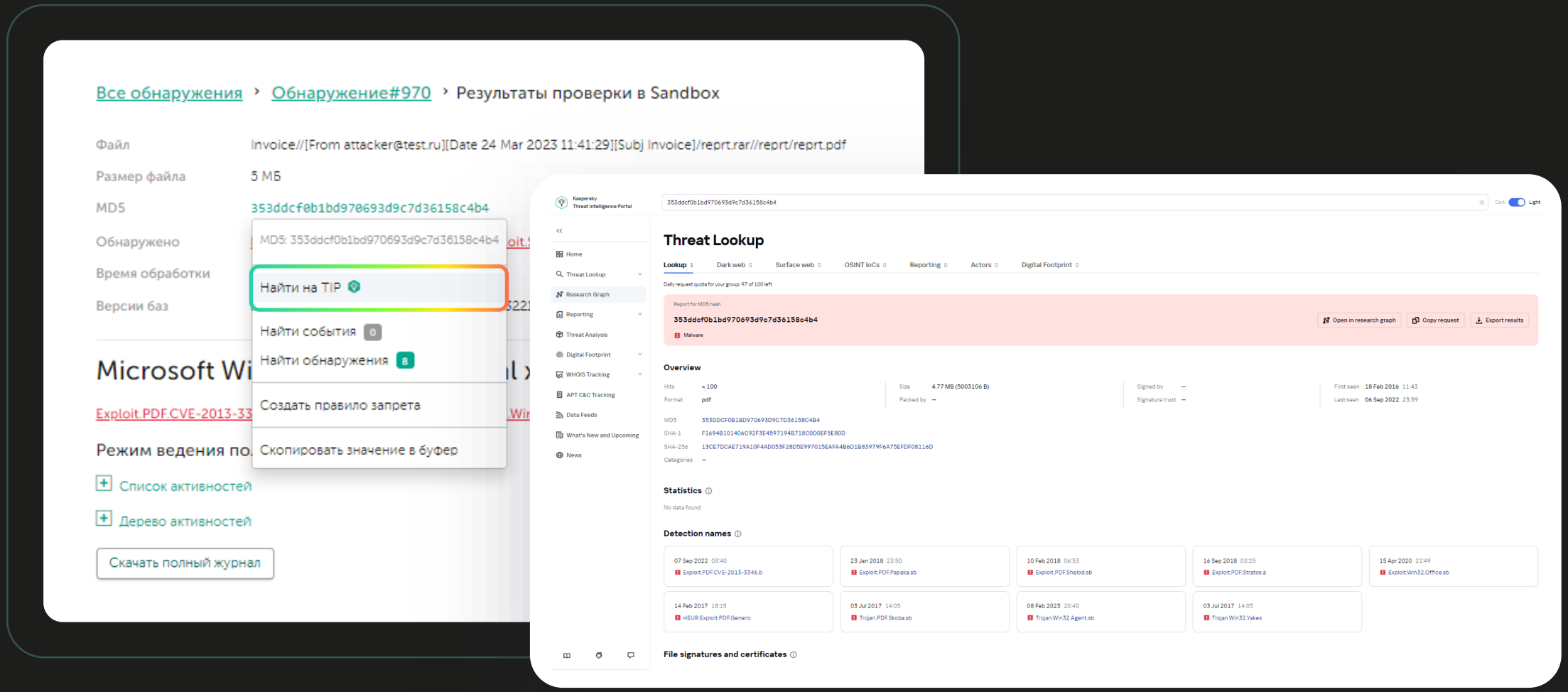
Интеграция с Threat intelligence для обогащения знаний по обнаруженным IoC

Сопоставление событий с техниками матрицы MITRE ATT&CK

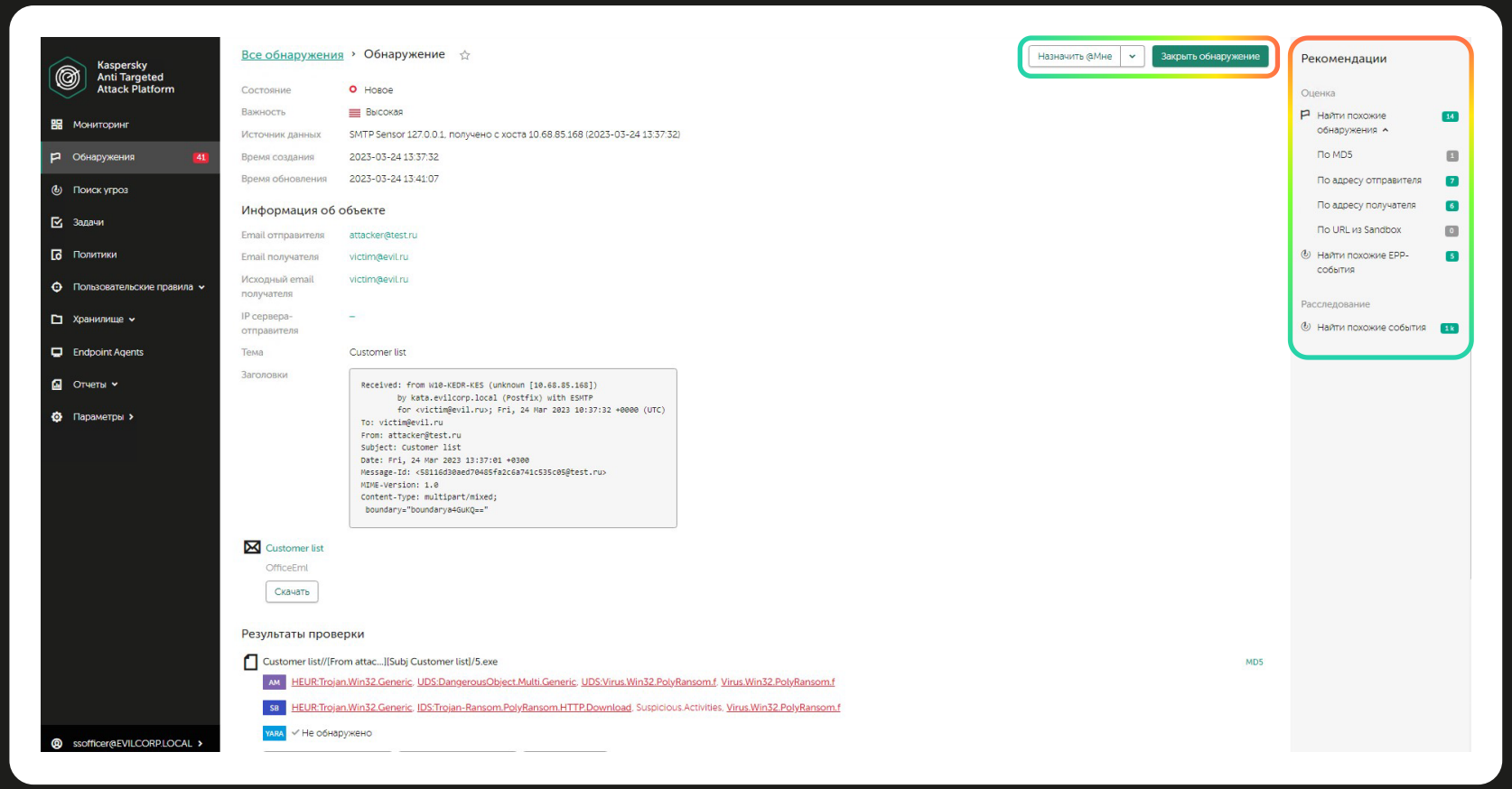
Поиск неизвестных угроз по ретроспективным данным с защищаемых хостов



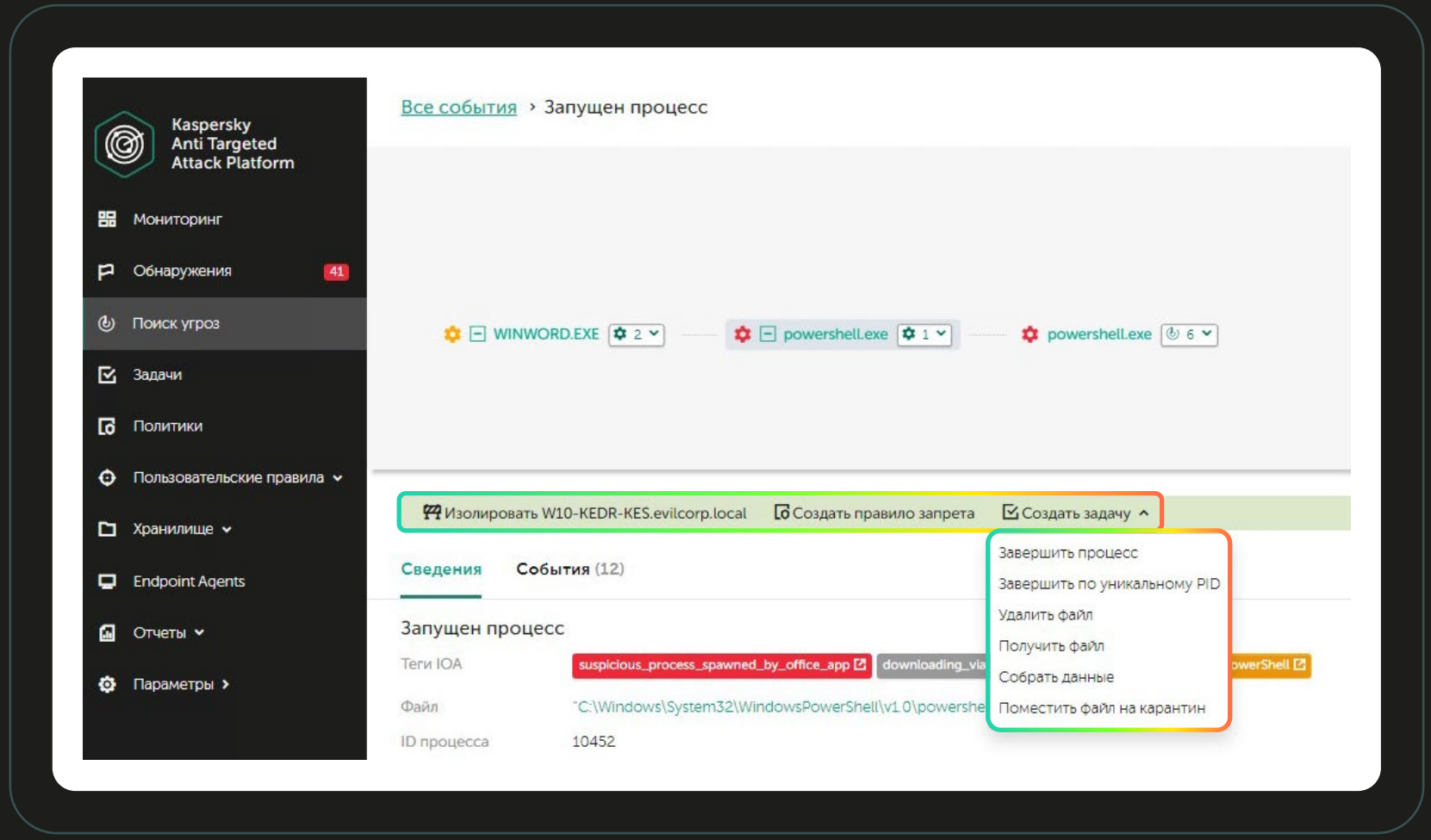
Интеграция с Threat intelligence (tip.kaspersky.com) для обогащения знаний по обнаруженным IoC



Рекомендуемые действия по расследованию обнаружения



Рекомендуемые действия для оперативного реагирования на инцидент



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

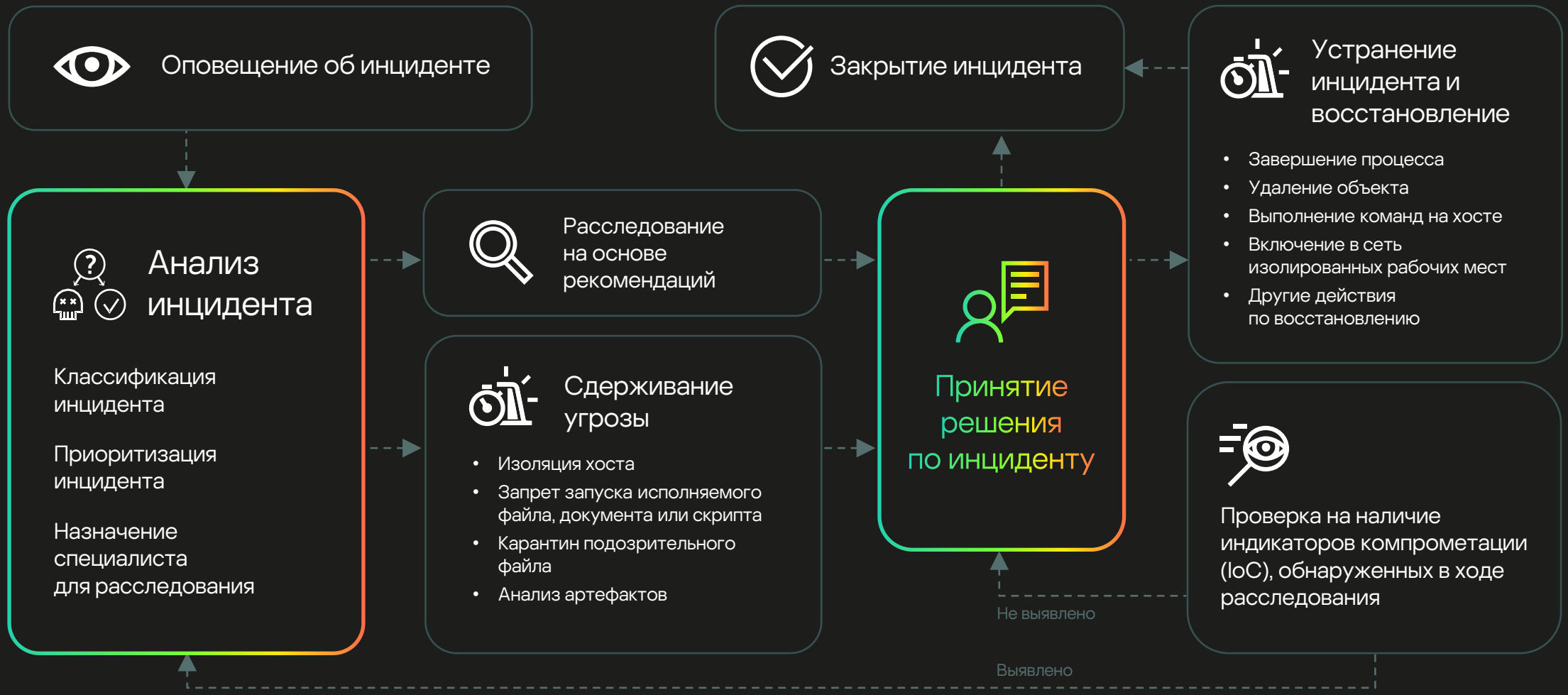
Автоматическое создание правил блокировки запуска подозрительных объектов в результате обнаружения Sandbox

Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

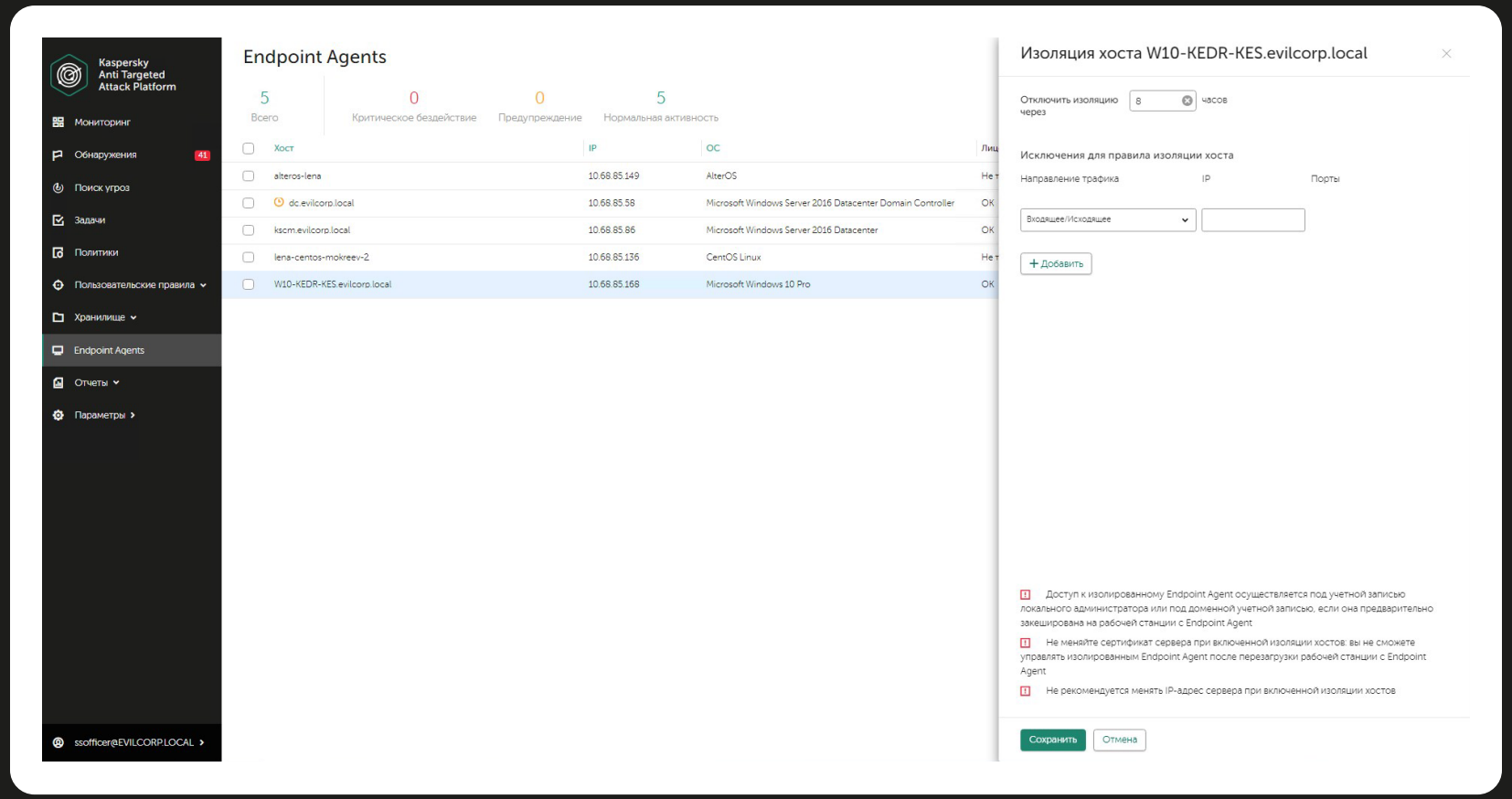
Выполнение команд и управление службами на защищаемом хосте

Запуск YARA-проверки

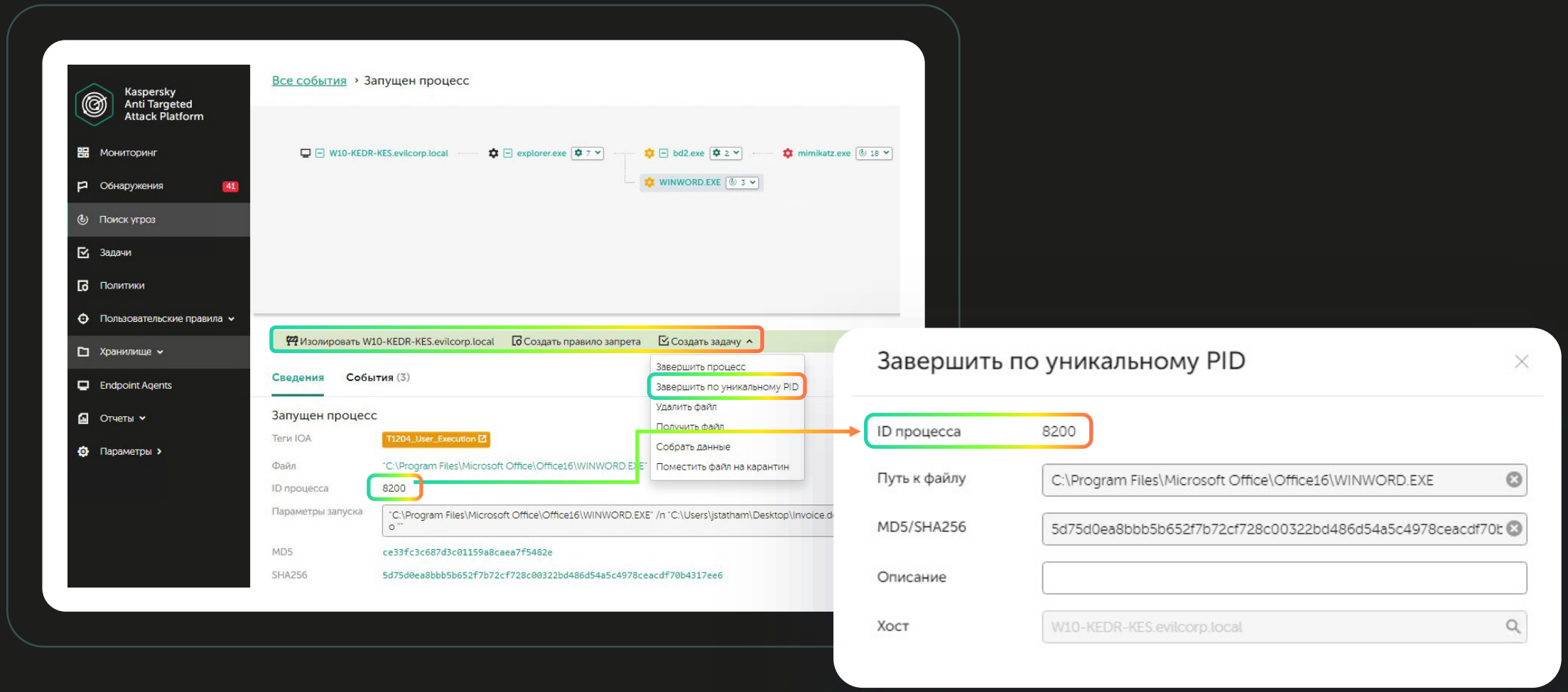
Схема централизованного реагирования на инциденты



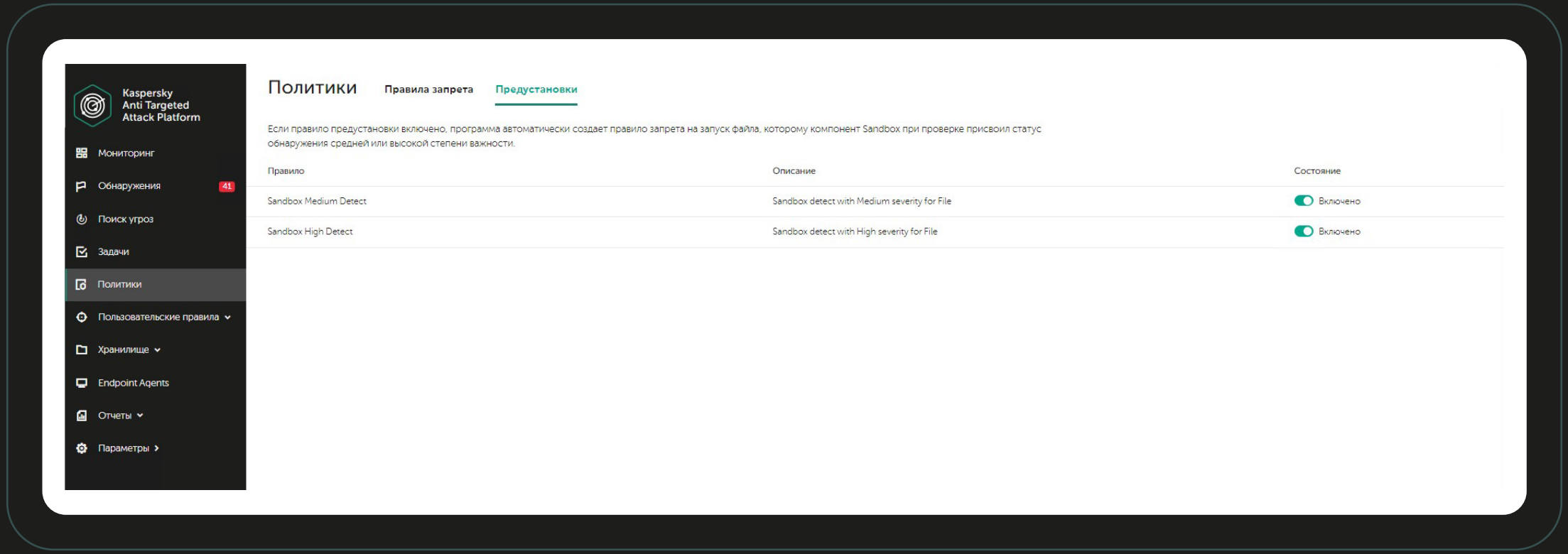
Изоляция скомпрометированного хоста



Завершение процесса с конкретным Process ID



Автоматическое создание правил блокировки запуска файла



Автоматическое создание правил блокировки запуска файла
на защищаемых хостах при получения вердикта от Sandbox

Администрирование и интеграция

В рамках управления системой доступны следующие возможности:

1. Поддержка режима multitenancy (возможность создания иерархической структуры серверов)
2. Ролевая модель доступа (Администратор, Старший офицер безопасности, Офицер безопасности, Аудитор)
3. Аудит действий пользователей
4. Мониторинг работоспособности системы (виджеты, SNMP, syslog, почтовые уведомления)
5. Поддержка отказоустойчивого режима работы системы за счет развертывания кластера серверов

В решении KATA доступны следующие возможности:

Интеграция с SIEM

Отправка данных об обнаружениях по протоколу Syslog

Интеграция с SIEM

Отправка телеметрии по API с Endpoint Agent для анализа

Интеграция с Kaspersky (Private) Security Network

API для отправки сведений

об обнаружениях во внешнюю систему

API для проверки объектов

в KATA Platform с возвратом результатов сканирования

Интеграция с сервисом Managed Detection and Response

Ключевые преимущества

Ключевые преимущества

Уникальный стек технологий

Собственный Antimalware Engine

Глобальная репутационная база KSN

Интеграция с Threat Lookup

Встроенный инструментарий для написания YARA правил

Targeted Attack Analyzer

CloudML для проверки APK файлов

Низкие системные требования

Требует на 30% меньше серверных ресурсов чем аналогичные отечественные решения

Масштабируемость

Отказоустойчивость всех компонентов системы

Легкое горизонтальное и вертикальное масштабирование

Развертывание неограниченного количества песочниц в рамках одной лицензии KATA и KEDR Expert

Автоматические и ручные сценарии реагирования

Автоматическое реагирование на почтовом и веб-трафике

Корреляция событий на сети и хостах

Создание правил автоматического запрета запуска исполняемых файлов по вердикту песочницы

Отправка объектов на исследование в песочницу в ручном режиме или по API

Спасибо!