?????? ? YARA-?????????? ? KATA

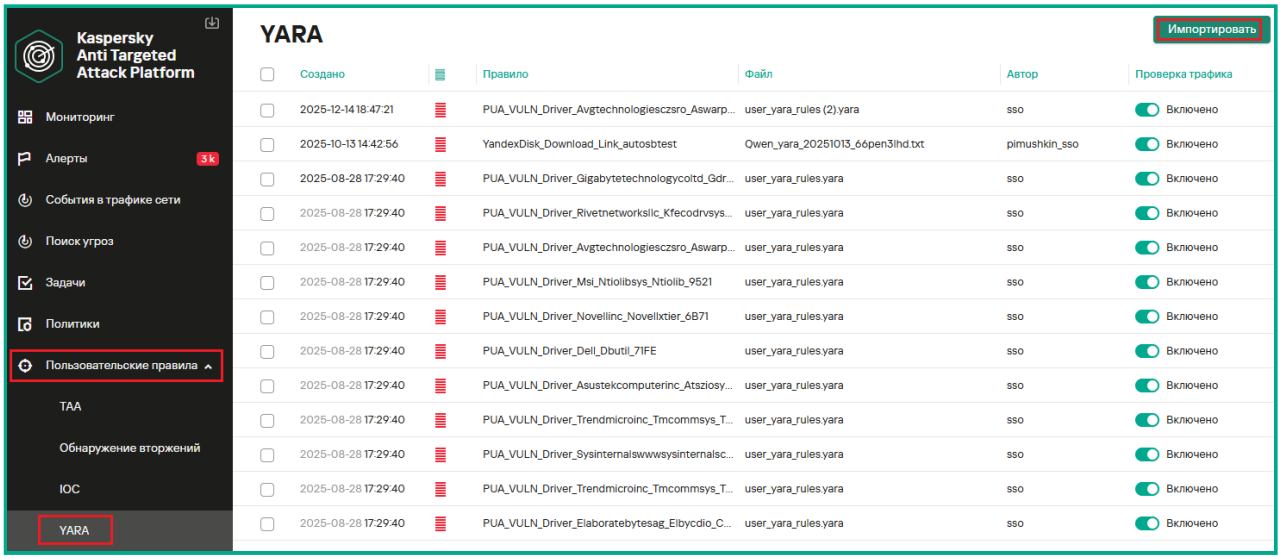
Вы можете загружать собственные YARA правила в KATA для проверки файлов и объектов, поступающих на Central Node, и для проверки хостов с компонентом Endpoint Agent.

> Только пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать, удалять, скачивать IOC-файлы, включать и отключать поиск по IOC-файлам и настраивать расписание поиска. Пользователи с ролью **Сотрудник службы безопасности** и **Аудитор** могут только просматривать список IOC-файлов и информацию о выбранном файле, а также экспортировать IOC-файлы на компьютер

?????????? YARA ??????

Для добавления новых правил YARA необходимо авторизоваться в интерфейсе KATA под УЗ с ролью **Старший сотрудник службы безопасности** и перейти в раздел **Пользовательские правила --> YARA** и нажать **Импортировать** и выбрать необходимое правило для импорта

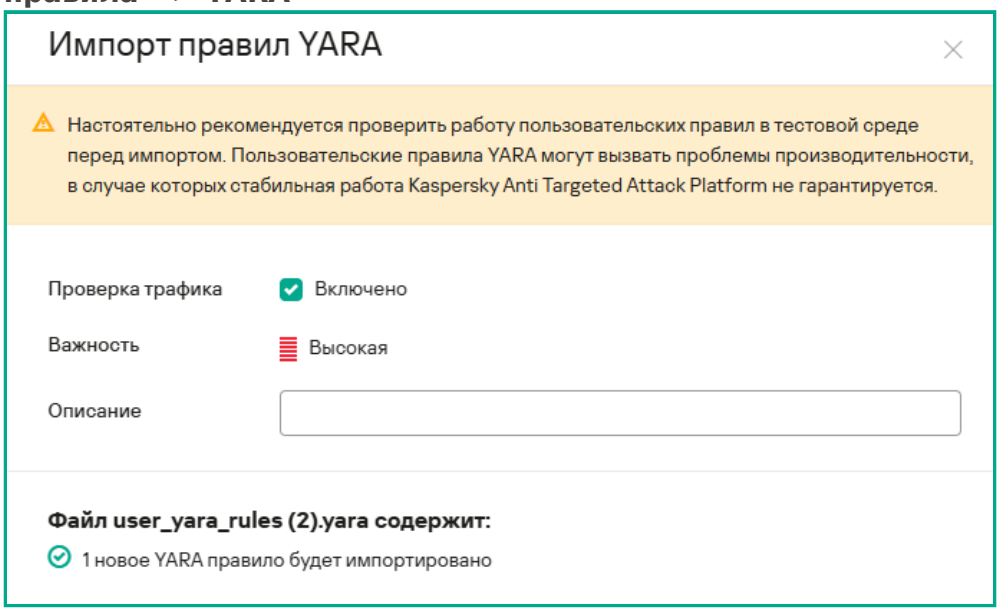
> Максимальный допустимый размер загружаемого файла – 20 МБ.



После выбора необходимого файла появится окно импорта, в котором:

- Можно включить проверку трафика, если вы хотите использовать импортированные правила при потоковой проверке объектов и данных, поступающих на Central Node;
- Добавить описание;
- Количество правил, которые могут быть успешно импортированы;
- Количество правил, которые не будут импортированы (если такие есть). Для каждого правила, которое не может быть импортировано, указывается его название.

После добавления правило отобразиться в новой записью в разделе **Пользовательские правила --> YARA**



Нажав на правило можно ознакомиться с содержанием правила, включить/выключить проверку, скачать или удалить данное правило



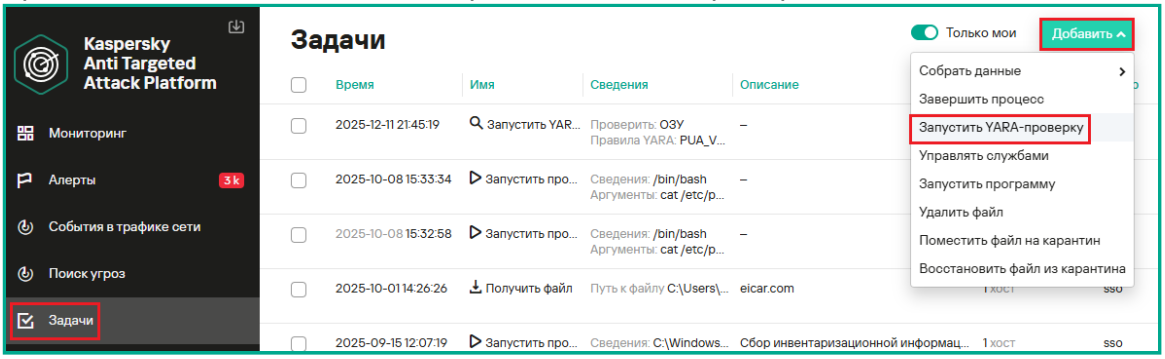
Также можно найти алерты связанные с выбранным правилом и создать задачу проверки по данному YARA-правилу нажав **Запустить YARA-проверку**

???????? ?????? YARA-????????

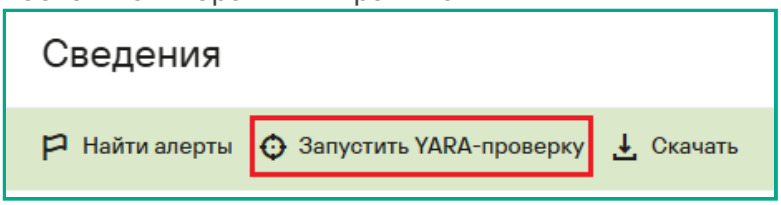
> Необходима лицензия, поддерживающая функционал KEDR Expert

При необходимости вы можете проверять хосты из раздела Endpoint Agent с помощью правил YARA. Для этого требуется создать задачу Запустить YARA-проверку. Вы можете создать задачу следующими способами:

- **В разделе Задачи.** В этом случае при создании задачи вам потребуется выбрать правила YARA, с помощью которых вы хотите проверить хосты;

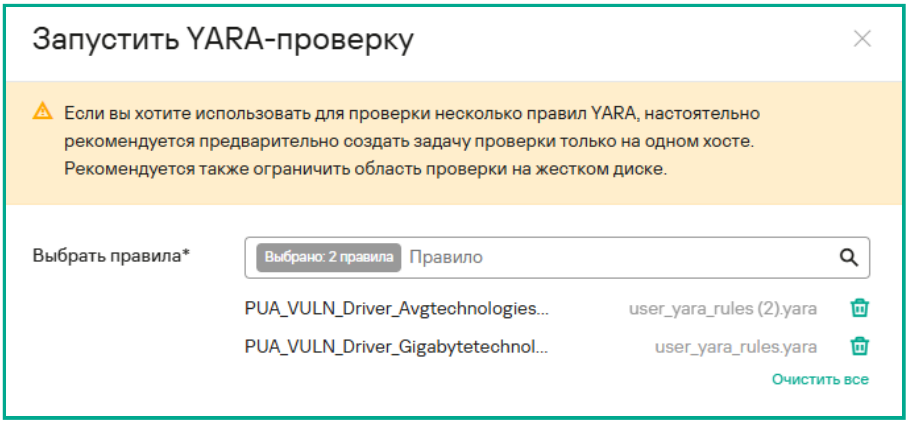


- **В разделе Пользовательские правила --> YARA**, выбрав необходимое правило и нажав **Запустить YARA-проверку** В этом случае создается задача для проверки хостов по выбранным правилам YARA.



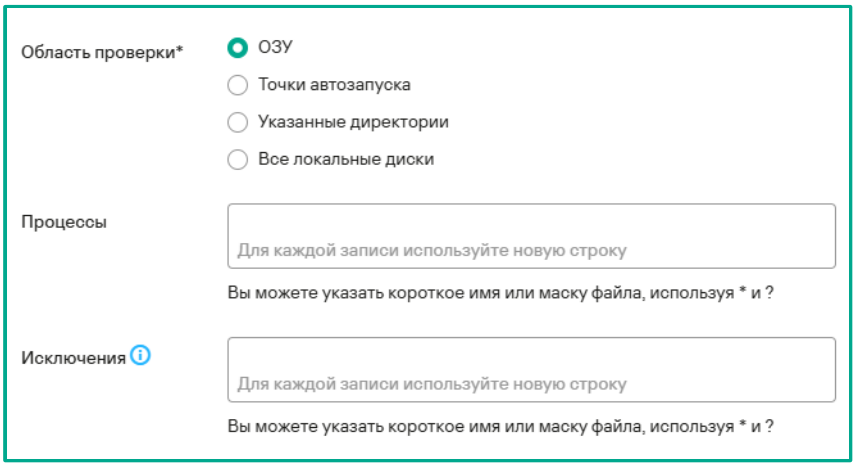
При использовании любого из способов откроется окно создания задачи.
В данном меню вы можете указать следующие параметры:

- Выбрать необходимые правила YARA для проверки. Можно выбрать сразу несколько;



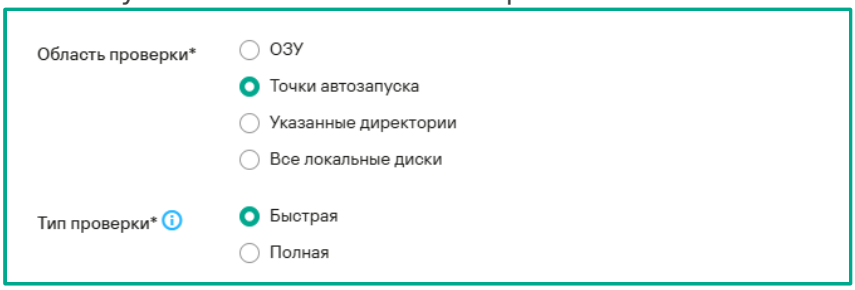
- Указать область проверки:

- **ОЗУ** - при необходимости проверить процессы, запущенные на момент выполнения задачи. Укажите необходимые короткие имена процессов или маску файлов, которые хотите проверить, а также исключения проверки при необходимости. Можно использовать маски * и ?;

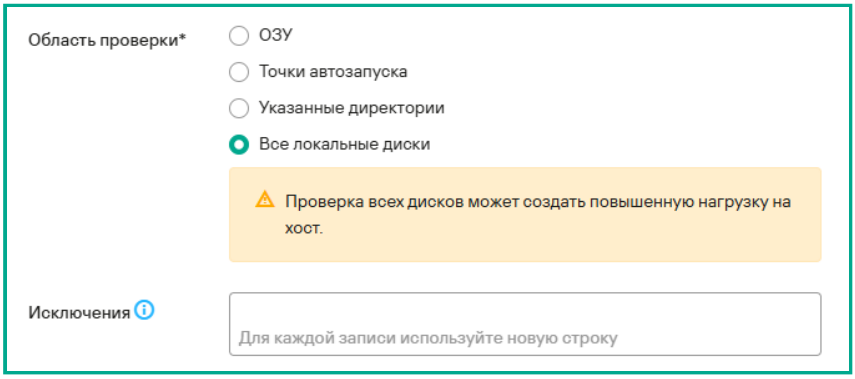


> Если поле **Процессы** не заполнено, приложение проверяет все процессы, запущенные на момент выполнения задачи, кроме процессов с PID ниже 10 и процессов, указанных в поле **Исключения**.

- **Точки автозапуска** - при необходимости проверить точки автозапуска, полученные в результате выполнения задачи **Собрать форензику**
  Для данной области задайте тип проверки. **Быстрая** - проверяются все точки автозапуска, кроме COM-объектов. **Полная** - проверяются все точки автозапуска и связанные с ними файлы.



- **Указанные директории** - при необходимости проверить файлы в указанной папке и во всех вложенных папках. Задайте путь вида C:<имя директории>\. Можно использовать маски * и ? для указания директории проверки и исключения;
- **Все локальные диски** - при необходимости проверить файлы, хранящиеся во всех папках локальных дисков. Можно использовать маски * и ? для указания директорий исключения.

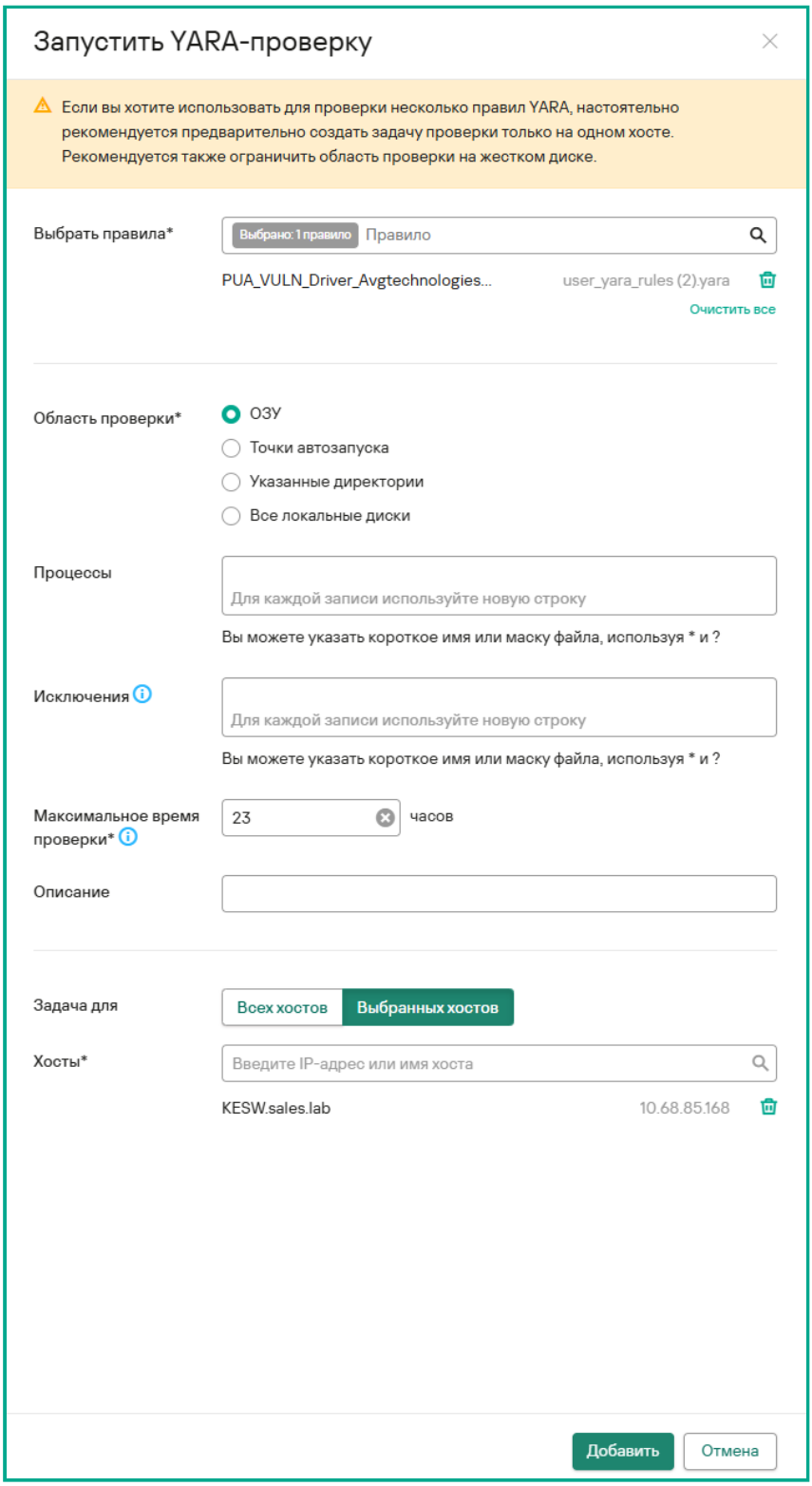


> Проверка всех локальных дисков может создать повышенную нагрузку на хост.

- Максимальное время проверки. В случае, если проверка не будет пройдена за указанный срок, то она будет принудительно завершена. В отчете о выполнении задачи указываются результаты, актуальные на момент завершения проверки.
- **Описание** – описание задачи. Поле необязательно для заполнения.
- **Задача для** – область применения задачи
  - **Всех хостов**, если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант;
  - **Выбранных серверов** - справа от названия параметра Серверы установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

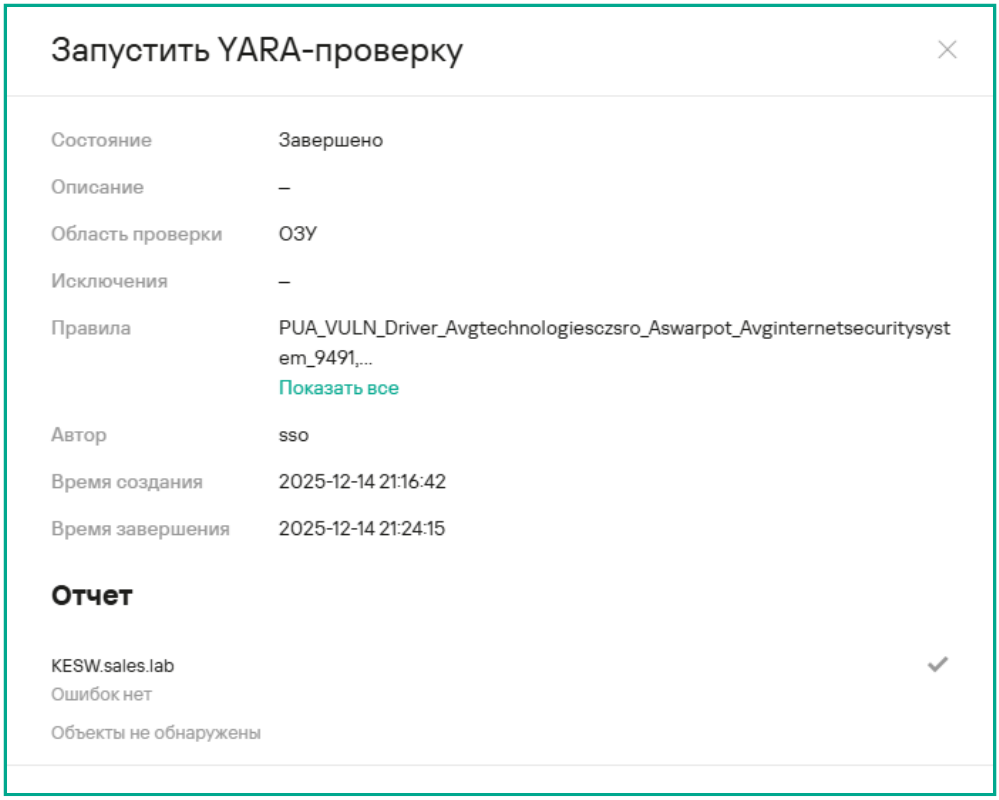
    > Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.

  - **Выбранных хостов**, если вы хотите выполнить задачу на выбранных хостах, перечислите эти хосты в соответствующем поле.



После указания необходимых параметров нажмите **Добавить** для запуска задачи

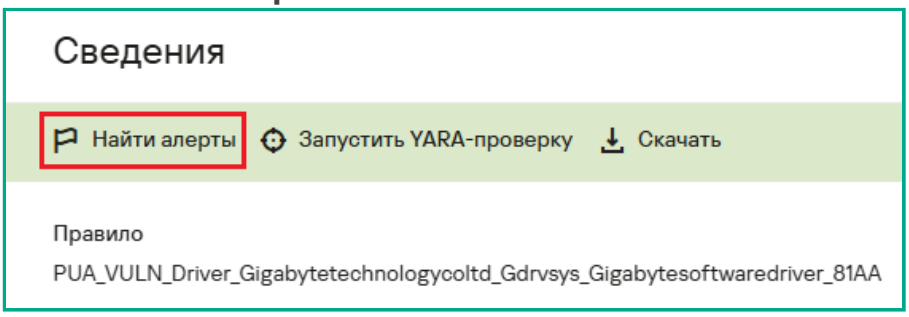
Нажав на созданную задачу можно ознакомиться с результатом её выполнения



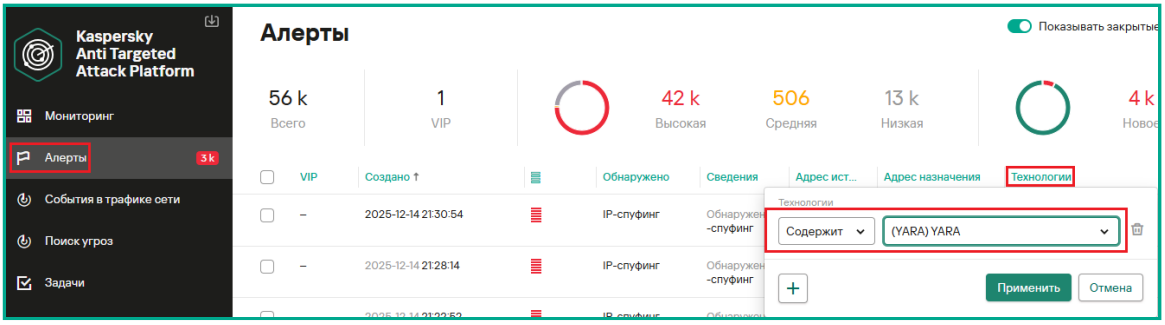
???????? ???????

Просматривать алерты связанные с YARA правилами можно двумя способами:

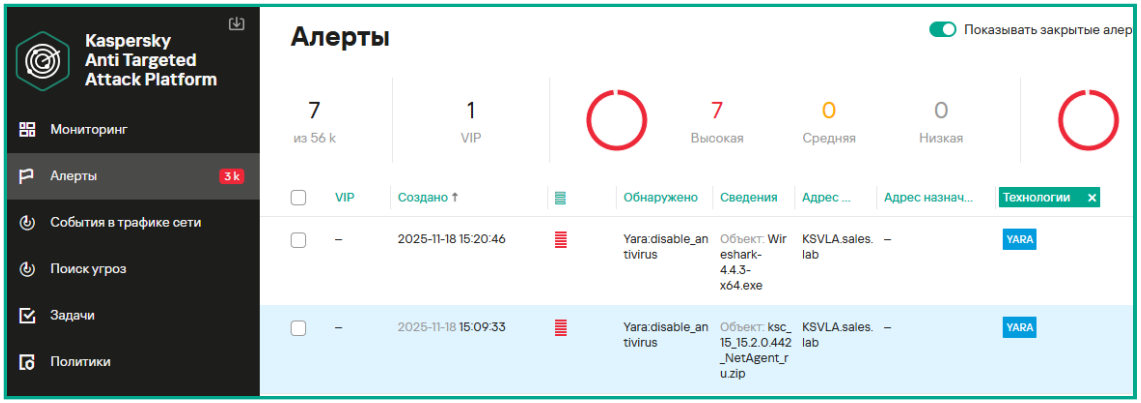
- Выбрав необходимое правило в разделе **Пользовательские правила --> YARA** и нажав **Найти алерты**



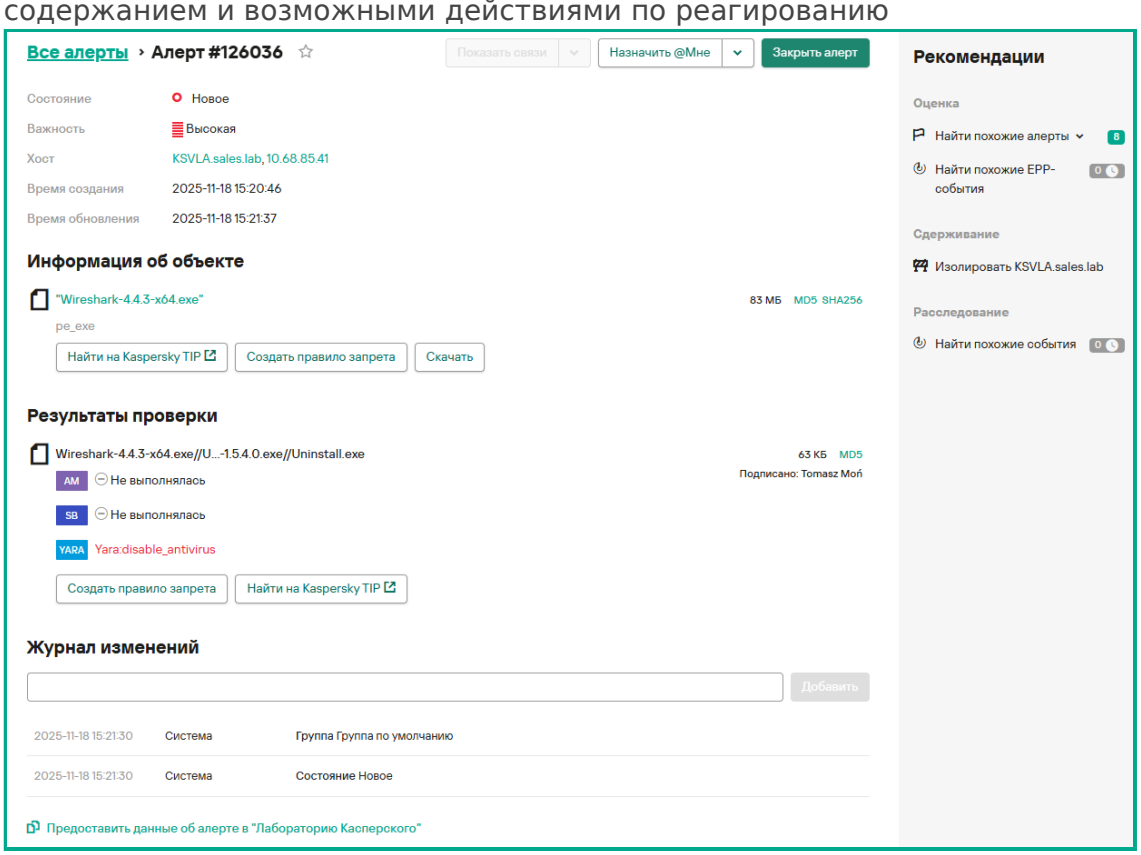
- Перейти в раздел **Алерты** и задать соответствующий фильтр на столбец **Технологии**



При использовании любого из способов будет использоваться раздел **Алерты**.



Нажав на алерт (свободное пространство в строке) можно подробнее ознакомиться с его содержанием и возможными действиями по реагированию



Revision #4
Created 15 December 2025 17:26:33 by Сергей
Updated 6 February 2026 11:00:25 by Кирилл