?????? ? IOC ? KATA

> Для работы с IOC необходима лицензия, поддерживающая функционал KEDR Expert

Индикатор IOC – это набор данных о вредоносном объекте или действии. **Kaspersky Anti Targeted Attack Platform** использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

При создании правил IOC рекомендуется:

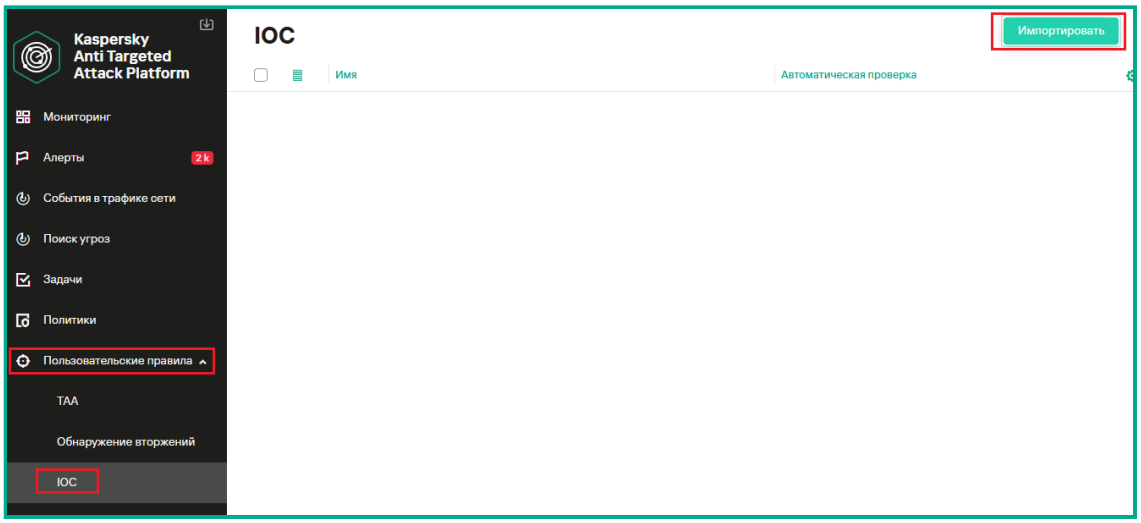
- Использовать OpenIOC Editor для создания пользовательских правил;
- Использовать поддерживаемые термины стандарта OpenIOC версии 1.1;
- Ознакомиться с требованиями и ограничениями применения IOC.

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

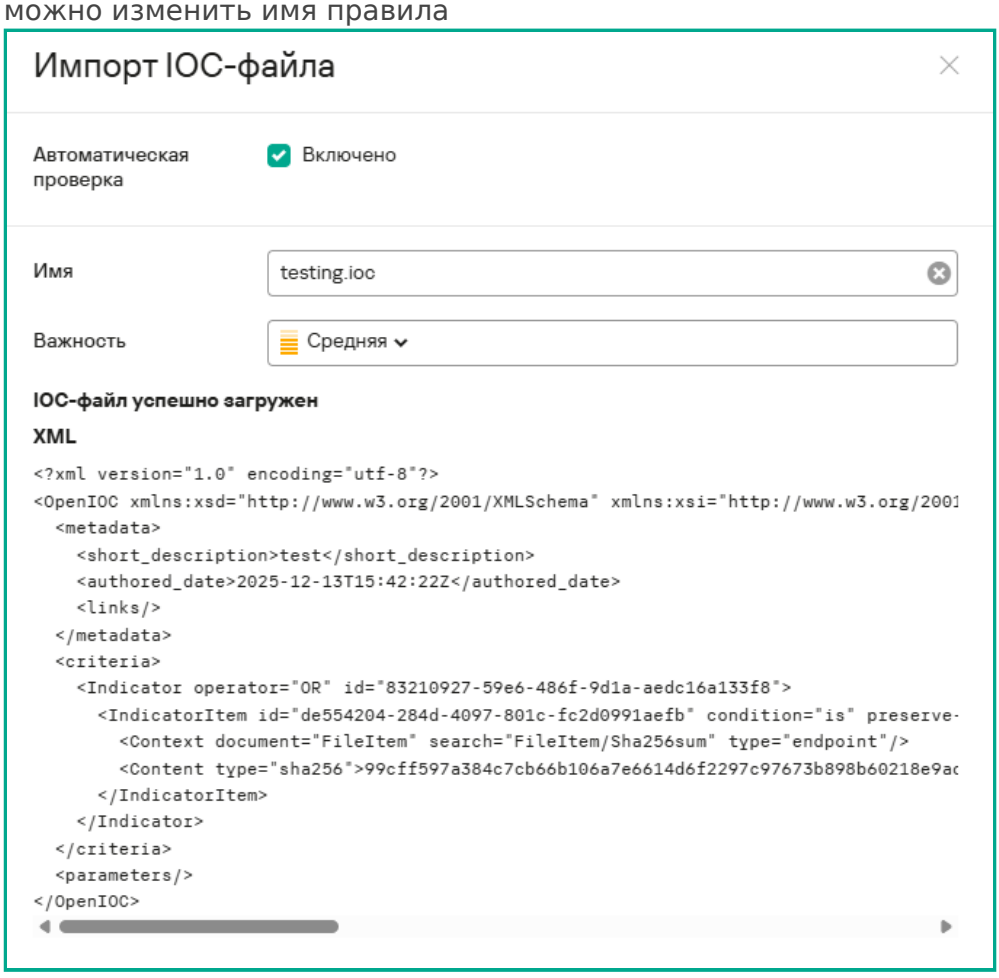
1. IOC-файл должен содержать поддерживаемые термины, список которых представлен ниже:
   - Для KES Windows
     - Область поиска IOC в реестре (при добавлении типа данных RegistryItem)
   - Для KES Linux
2. Только пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать, удалять, 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
3. Один IOC-файл может содержать только одно правило. Правило может быть любой сложности, строиться на условиях OR и AND

?????????? IOC-??????

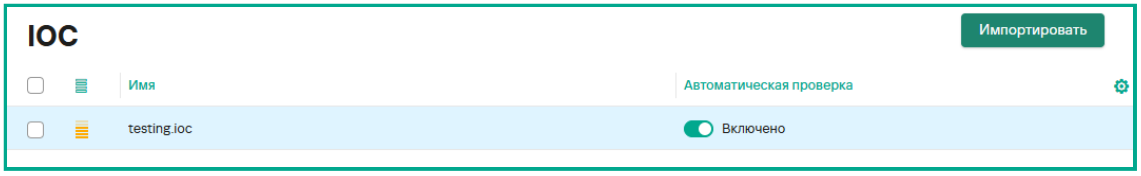
Для добавления нового IOC-правила необходимо авторизоваться в интерфейсе KATA под УЗ с ролью **Старший сотрудник службы безопасности** и перейти в раздел **Пользовательские правила --> IOC** и нажать **Импортировать** и выбрать необходимое правило для импорта



После выбора файла появится окно Импорта IOC-файла. Включите автоматическую проверку, укажите важность правила (низкая, средняя или высокая), при необходимости можно изменить имя правила



После этого правило отобразится новой записью в разделе **Пользовательские правила --> IOC**



При нажатии на правило появится меню сведений для данной записи. Здесь можно ознакомиться с содержанием правила и изменить его параметры: включить/выключить автоматическую проверку, изменить имя и важность.

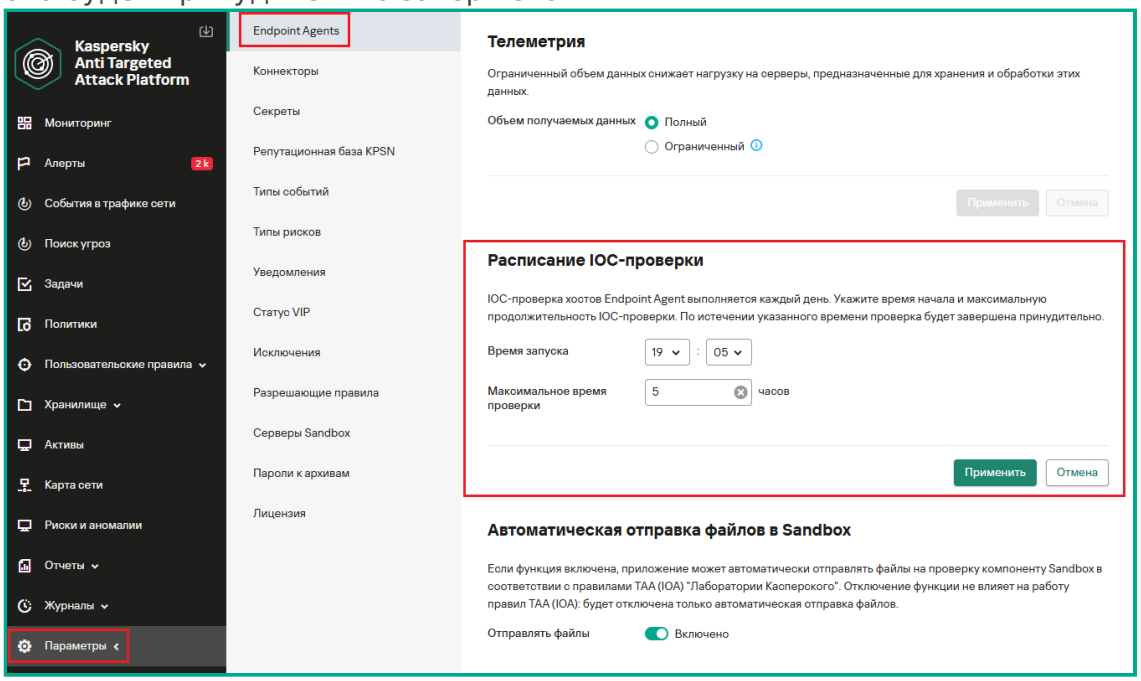
Также для удобства вы можете скачать выбранное правило, а также посмотреть события и алерты связанное с этим IOC-правилом.

При необходимость удалить правило воспользуйтесь соответствующей кнопкой внизу меню сведений IOC-правила


Сведения
Найти алерты
Найти события
Скачать
Автоматическая проверка
Включено
Имя
testing.ioc
Важность
Средняя
XML
<?xml version="1.0" encoding="utf-8"?>
<OpenIOC xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3
.org/2001/XMLSchema-instance" xmlns="http://openioc.org/schemas/OpenIOC_1.1"
id="e6a86b6c-2897-4c46-aee0-96d1e8404df2" last-modified="2025-12-13T15:42
:52Z" published-date="0001-01-01T00:00:00">
<metadata>
<short_description>test</short_description>
<authored_date>2025-12-13T15:42:22Z</authored_date>
<links/>
</metadata>
<criteria>
<Indicator operator="OR" id="83210927-59e6-486f-9d1a-aedc16a133f8">
<IndicatorItem id="de554204-284d-4097-801c-fc2d0991aefb" condition="is"
preserve-case="false" negate="false">
<Context document="FileItem" search="FileItem/Sha256sum" type="endpoint"
/>
<Content type="sha256"
>99cff597a384c7cb66b106a7e6614d6f2297c97673b898b60218e9acfbef6a54
</Content>
</IndicatorItem>
</Indicator>
</criteria>
<parameters/>
</OpenIOC>
Удалить
Сохранить
Отмена

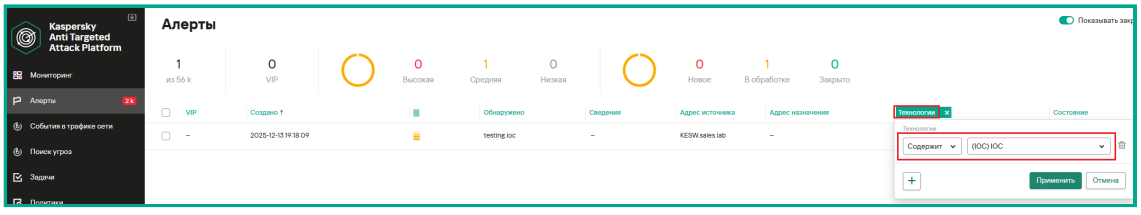
????????? ?????????????
???????? ?? IOC-????????

Данная проверка производится ежедневно для всех устройств раздела **"Endpoint Agents"** по IOC-правилам, для которых включён параметр **"Автоматическая проверка"**.
В разделе **Параметры --> Endpoint Agents** в блоке **"Расписание IOC-проверки"** укажите время запуска и максимальную длительность проверки. Нажмите **"Применить"** для сохранения параметров. В случае, если проверка не будет пройдена за указанный срок, то она будет принудительно завершена

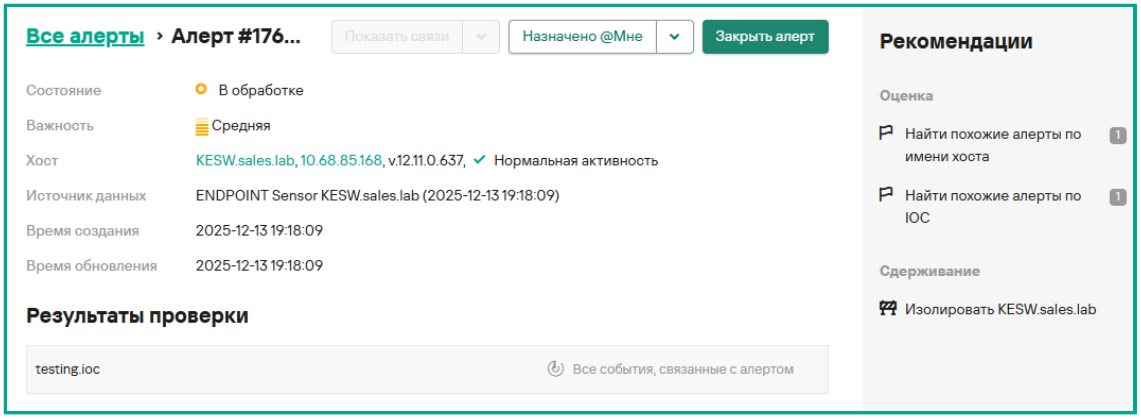


После выполнения проверки в указанное время в разделах **"Поиск угроз"** и **"Алерты"** могут появиться новые записи, в случае обнаружения IOC'ов из заданных правил.

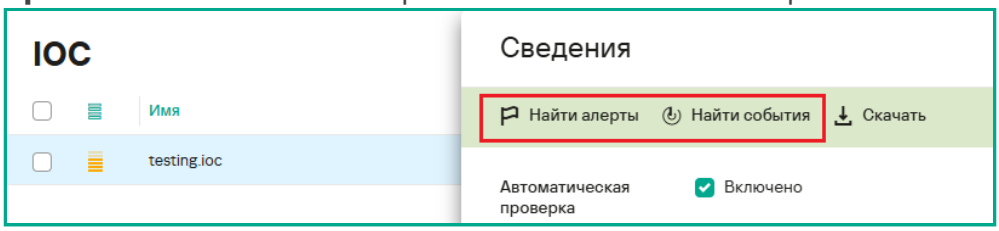
Для удобства поиска можно в разделе алерты задать фильтр для отображения записей связанных только с IOC-проверкой. Для этого в разделе **Алерты** нажмите на название столбца **Технологии**, выберите **IOC** из выпадающего списка и нажмите **Применить**



Для более детального ознакомления с алертом и применения действий нажмите на него (пустое пространство в строке алерта). В данном примере можно изолировать хост, на котором был обнаружен IOC



Также можно выбрать конкретное IOC-правило из списка в разделе **Пользовательские правила --> IOC** и посмотреть связанные с ним алерты или события

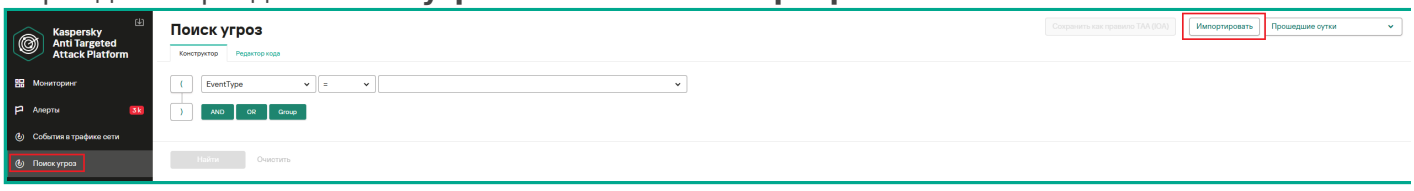


???????? TAA (IOA) ??????? ?? ?????? IOC ? ????? ?? ????????

Для IOC можно создать правило TAA (IOA) для поиска по базе событий раздела **Поиск угроз** и формирования алертов.

> При создании IOC-файла ознакомьтесь со **списком IOC-терминов**, которые можно использовать для поиска событий в разделе **Поиск угроз**

Авторизуйтесь под учётной записью с ролью **Старший сотрудник службы безопасности**. Перейдите в раздел **Поиск угроз** и нажмите **Импортировать**



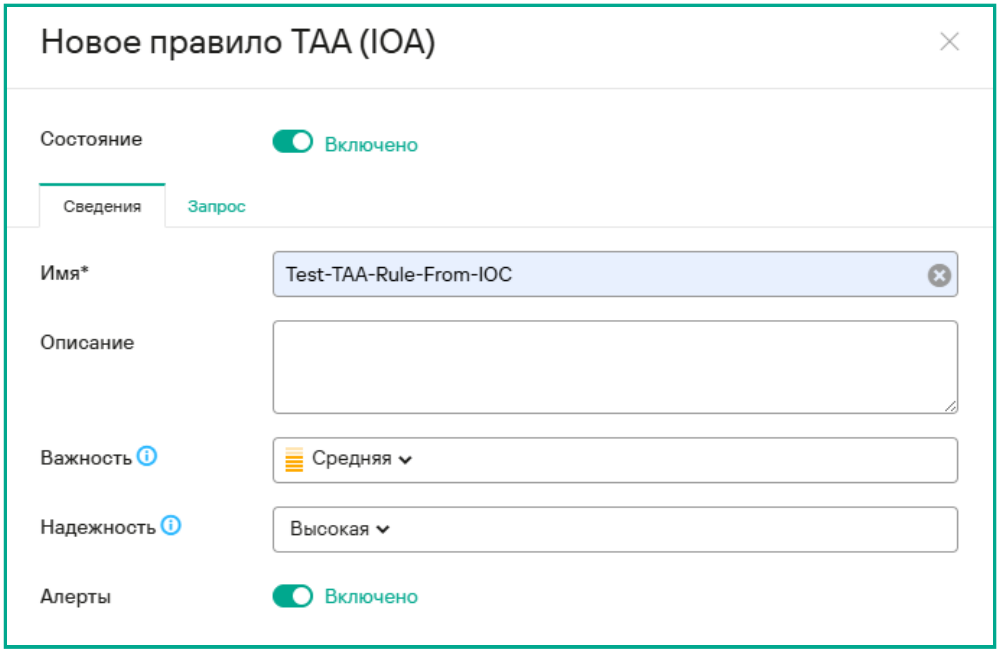
Поля из IOC будут перенесены в конструктор. При необходимости вы можете внести изменения и добавить новые поля. После чего нажмите Сохранить как правило TAA (IOA).

> Также вы можете сразу выполнить поиск по событиям выбрав необходимый временной период в верхнем правом углу и нажав **Найти**

В появившемся окне добавления TAA (IOA) правила укажите:

- **Состояние**. Переведите переключатель в активное положение для работы правила
- **Имя правила**. (Нельзя использовать пробелы)
- **Описание** при необходимости
- **Важность**. Выберете из выпадающего списка низкая, средняя или высокая
- **Надёжность**. Выставите уровень надёжности в зависимости от вероятности ложных срабатываний
- **Алерты**. Возможность создания алертов из обнаруженных событий
  На вкладке **Запрос** вы сможете ознакомиться с содержанием правила.

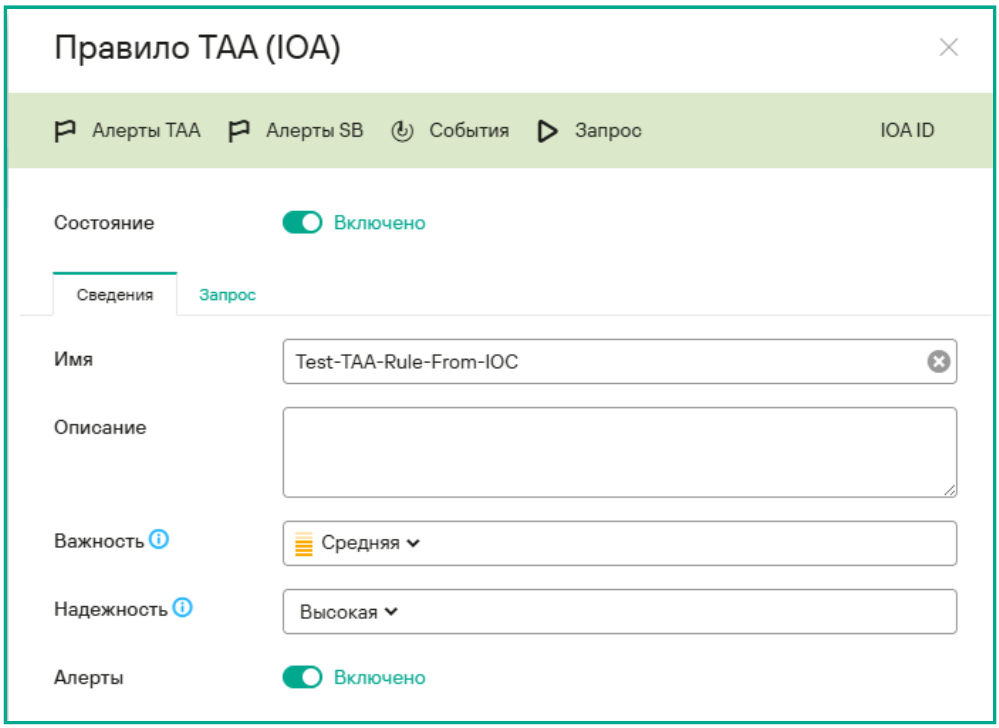
После внесения необходимых параметров сохраните правило



В разделе **Пользовательские правила --> TAA** нажмите на созданное правило. Здесь можно отредактировать заданные ранее параметры, удалить правило, а также:

- Показать алерты связанные с данным правилом. Для этого нажмите **Алерты TAA** для запуска соответствующей выборки алертов.
- Показать алерты компонента **Sandbox** связанные с данным правилом. Для этого нажмите **Алерты SB** для запуска соответствующей выборки алертов.

- Показать события для данного правила. Для этого нажмите **События**. Запустит выборку в разделе **Поиск угроз** по IOAId (указан в верхнем правом углу правила)
- Выполнить поиск событий по полям правила. Для этого нажмите **Запуск**. Запустит выборку в разделе **Поиск угроз**



Revision #10
Created 15 December 2025 14:39:27 by Сергей
Updated 6 February 2026 11:00:11 by Кирилл