

??????? ? YARA-???????????? ? КАТА

Вы можете загружать собственные YARA правила в КАТА 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 КАТА 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.

Создано	Правило	Файл	Автор	Проверка трафика
2025-12-14 18:47:21	PUA_VULN_Driver_Avgtechnologiesczsro_Aswarp...	user_yara_rules (2).yara	ss0	Включено
2025-10-13 14:42:56	YandexDisk_Download_Link_autosbtest	Owen_yara_20251013_66pen3lhd.txt	pimushkin_sso	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Gigabytetechnologycoltd_Gdr...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Rivetnetworksilic_Kfecodrvsys...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Avgtechnologiesczsro_Aswarp...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Msi_Ntiolibsys_Ntiolib_9521	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Novellinc_Novellxtier_6B71	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Dell_Dbutil_71FE	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Asustekcomputerinc_Atsziosy...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Trendmicroinc_Tmcommsys_T...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Sysinternalswwwsysinternalsc...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Trendmicroinc_Tmcommsys_T...	user_yara_rules.yara	ss0	Включено
2025-08-28 17:29:40	PUA_VULN_Driver_Elaboratebytesag_Elbyccio_C...	user_yara_rules.yara	ss0	Включено

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 отобразится в новой записью в разделе **Пользовательские правила --> YARA**

Импорт правил YARA ✕

⚠ Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила YARA могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется.

Проверка трафика Включено

Важность  Высокая

Описание

Файл user_yara_rules (2).yara содержит:

1 новое YARA правило будет импортировано

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

Сведения



Найти алерты Запустить YARA-проверку Скачать

Правило PUA_VULN_Driver_Msi_Ntiolibsys_Ntiolib_9521

Проверка трафика Включено

Важность Высокая

Описание

```
rule PUA_VULN_Driver_Msi_Ntiolibsys_Ntiolib_9521 {
  meta:
    description = "Detects vulnerable driver mentioned in LOLDrivers
    project using VersionInfo values from the PE header - NTIOLib.sys"
    author = "Florian Roth"
    reference = "https://github.com/magic sword-io/LOLDrivers"
    hash = "952199c28332bc90cf74530a77ee237967ed32b3c71322559c59f7a42187dc
    4"
    hash = "56a3c9ac137d862a85b4004f043d46542a1b61c6acb438098a9640469e2d80e
    7"
    hash = "85866e8c25d82c1ec91d7a8076c7d073cccf421cf57d9c83d80d63943a4edd9
    4"
    hash = "a9706e320179993dade519a83061477ace195daa1b788662825484813001f52
    6"
    hash = "ef86c4e5eedbc4f81cd864e8cd2f4a2a85ee4475b9a9ab698a4ae1cc71fbeb
    0"
    hash = "f088b2ba27dacd5c28f8ee428f1350dca4bc7c6606309c287c801b2e1da1a53
    d"
    hash = "18776682fcc0c6863147143759a8d4050a4115a8ede0136e49a7cf885c8a480
    5"
    hash = "50d5eaa168c077ce5b7f15b3f2c43bd2b86b07b1e926c1b332f8cb13bd2e079
    3"
    hash = "cd4a249c3ef65af285d0f8f30a8a96e83688486aab515836318a2559757a89b
    b"
    hash = "101402d4f5d1ae413ded499c78a5fcbbc7e3bae9b000d64c1dd64e3c48c3755
    8"
    hash = "c2a4ddcc9c3b339d752c48925d62fc4cc5adbf6fae8fedef74cdd47e88da01f
    8"
    hash = "d92eab70bcece4432258c9c9a914483a2267f6ab5ce2630048d3a99e8cb1b48
    2"
    hash = "a961f5939088238d76757669a9a81905e33f247c9c635b908daac146ae06349
    9"
    hash = "99f4994a0e5bd1bf6e3f637d3225c69ff4cd620557e23637533e7f18d7d6cba
    1"
    hash = "38fa0c663c8689048726666f1c5e019feaa9da8278f1df6ff62da33961891d2
    "
```

Удалить

Сохранить

Отмена

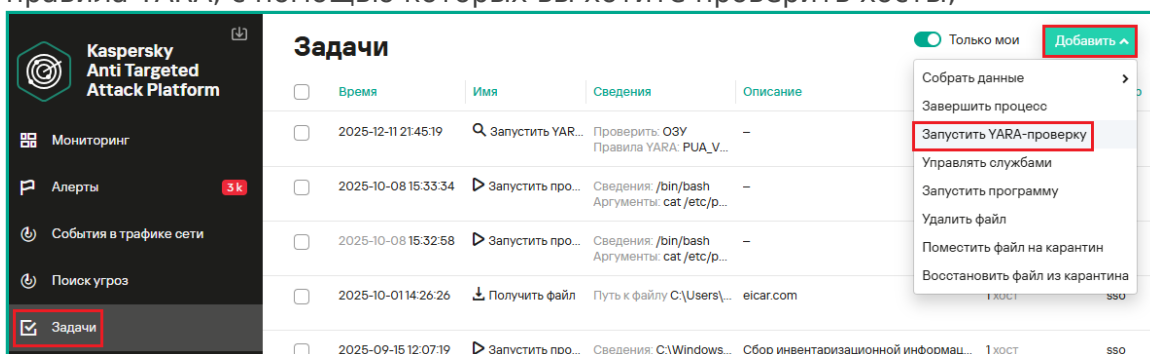
Также можно найти алерты связанные с выбранным правилом и создать задачу проверки по данному YARA-правилу нажав **Запустить YARA-проверку**

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

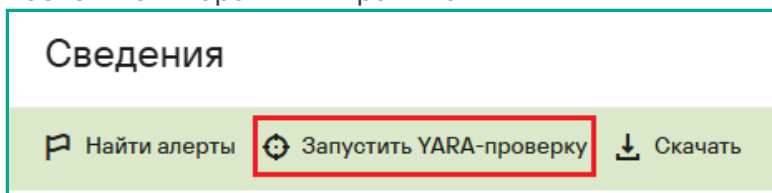
“ Необходима лицензия, поддерживающая функционал KEDR Expert

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;

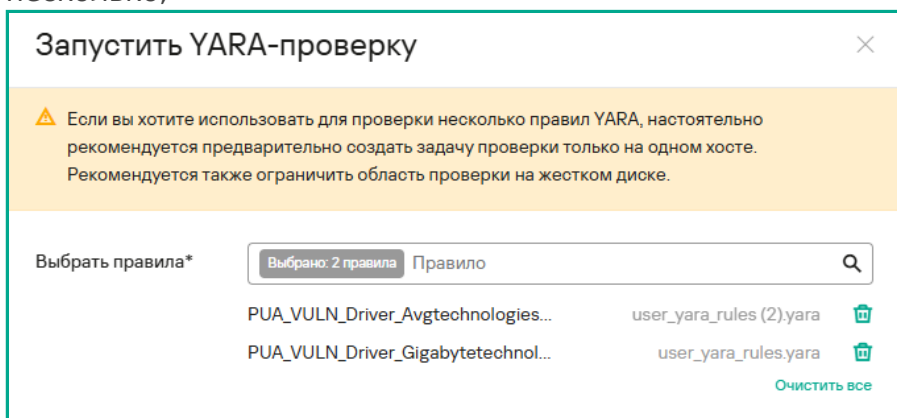


- **В разделе Пользовательские правила --> YARA,** выбрав необходимое правило и нажав **Запустить YARA-проверку** В этом случае создается задача для проверки хостов по выбранным правилам YARA.



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 ?;

Область проверки* ОЗУ
 Точки автозапуска
 Указанные директории
 Все локальные диски

Процессы
Вы можете указать короткое имя или маску файла, используя * и ?

Исключения ⓘ
Вы можете указать короткое имя или маску файла, используя * 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 СОМ-объектов. **Полная** - проверяются все точки автозапуска и связанные с ними файлы.


Область проверки* ОЗУ
 Точки автозапуска
 Указанные директории
 Все локальные диски

Тип проверки* ⓘ Быстрая
 Полная

- **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.

Область проверки* ОЗУ
 Точки автозапуска
 Указанные директории
 Все локальные диски

 Проверка всех дисков может создать повышенную нагрузку на хост.

Исключения 

Для каждой записи используйте новую строку

“ 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.

Запустить YARA-проверку ✕

⚠ Если вы хотите использовать для проверки несколько правил YARA, настоятельно рекомендуется предварительно создать задачу проверки только на одном хосте. Рекомендуется также ограничить область проверки на жестком диске.

Выбрать правила* Выбрано: 1 правило Правило

PUA_VULN_Driver_Avgtechnologies... user_yara_rules (2).yara

[Очистить все](#)

Область проверки* ОЗУ
 Точки автозапуска
 Указанные директории
 Все локальные диски

Процессы
Для каждой записи используйте новую строку
Вы можете указать короткое имя или маску файла, используя * и ?

Исключения
Для каждой записи используйте новую строку
Вы можете указать короткое имя или маску файла, используя * и ?

Максимальное время проверки* часов

Описание

Задача для Всех хостов Выбранных хостов

Хосты*
Введите IP-адрес или имя хоста

KESW.sales.lab 10.68.85.168

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

Нажав на созданную задачу можно ознакомиться с результатом её выполнения

Запустить YARA-проверку

Состояние: Завершено

Описание: –

Область проверки: ОЗУ

Исключения: –

Правила: PUA_VULN_Driver_Avgtechnologiescszro_Aswarpot_Avginternetsecuritysystem_9491,...

Автор: sso

Время создания: 2025-12-14 21:16:42

Время завершения: 2025-12-14 21:24:15

Отчет

KESW.sales.lab ✓

Ошибок нет

Объекты не обнаружены

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

Просматривать алерты связанные с YARA правилами можно двумя способами:

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

Сведения

Найти алерты Запустить YARA-проверку Скачать

Правило
PUA_VULN_Driver_Gigabytetechnologycoltd_Gdrvsys_Gigabytesoftwaredriver_81AA

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

Алерты

56 k Всего 1 VIP 42 k Высокая 506 Средняя 13 k Низкая 4 k Новое

VIP	Создано ↑	Обнаружено	Сведения	Адрес ист...	Адрес назначения	Технологии
<input type="checkbox"/>	2025-12-14 21:30:54	IP-спуфинг	Обнаружен-спуфинг			Содержит (YARA) YARA
<input type="checkbox"/>	2025-12-14 21:28:14	IP-спуфинг	Обнаружен-спуфинг			

Кнопки: Применить, Отмена

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

Алерты Показывать закрытые алерты

7 из 56 k | 1 VIP | 7 Высокая | 0 Средняя | 0 Низкая

<input type="checkbox"/>	VIP	Создано ↑	Обнаружено	Сведения	Адрес ...	Адрес назнач...	Технологии
<input type="checkbox"/>	-	2025-11-18 15:20:46	Yara:disable_antivirus	Объект: Wireshark-4.4.3-x64.exe	KSVLA.sales.lab	-	YARA
<input type="checkbox"/>	-	2025-11-18 15:09:33	Yara:disable_antivirus	Объект: ksc_15_15.2.0.442_NetAgent_ru.zip	KSVLA.sales.lab	-	YARA

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

Все алерты > **Алерт #126036** ☆ Показать связи Назначить @Мне Закрыть алерт

Состояние: Новое
 Важность: Высокая
 Хост: KSVLA.sales.lab, 10.68.85.41
 Время создания: 2025-11-18 15:20:46
 Время обновления: 2025-11-18 15:21:37

Информация об объекте

"Wireshark-4.4.3-x64.exe" 83 МБ MD5 SHA256
 ре_exe
[Найти на Kaspersky TIP](#) [Создать правило запрета](#) [Скачать](#)

Результаты проверки

Wireshark-4.4.3-x64.exe//U...15.4.0.exe//Uninstall.exe 63 КБ MD5
 Подписано: Tomasz Mof
 AM Не выполнялась
 SB Не выполнялась
 YARA Yaradisable_antivirus
[Создать правило запрета](#) [Найти на Kaspersky TIP](#)

Журнал изменений

[Добавить](#)

2025-11-18 15:21:30	Система	Группа Группа по умолчанию
2025-11-18 15:21:30	Система	Состояние Новое

[Предоставить данные об алерте в "Лабораторию Касперского"](#)

Рекомендации

Оценка

[Найти похожие алерты](#) 8

[Найти похожие EPP-события](#) 0

Содержание

[Изолировать KSVLA.sales.lab](#)

Раследование

[Найти похожие события](#) 0

Revision #4

Created 15 December 2025 17:26:33 by Сергей

Updated 6 February 2026 11:00:25 by Кирилл