

Реагирование на алерты и инциденты

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Одним из шагов расследования алерта или инцидента является реагирование, направленное на сдерживание (Containment) угрозы/злоумышленника или устранение (Eradication) угрозы.

Сдерживание (Containment)

Цель: Ограничить распространение угрозы/злоумышленника и минимизировать ущерб.

Примеры возможных действий:

- Изоляция зараженных систем/сетевых сегментов/хостов.
- Блокировка вредоносных IP-адресов или доменов.
- Временное отключение сервисов, если это необходимо.

Устранение (Eradication)

Цель: Полностью устранить причину инцидента.

Примеры возможных действий:

- Удаление вредоносного ПО или вредоносных скриптов.
- Закрывание уязвимостей, которые были использованы злоумышленниками.
- Обновление систем и приложений до актуальных версий.
- Смена скомпрометированных учетных данных (паролей, ключей).

За счет интеграции с другими решениями KUMA позволяет производить действия по реагированию:

- Реагирование через Kaspersky Security Center:
 - Запуск обновления антивирусных баз и модулей Kaspersky Endpoint Security для Windows или Linux;
 - Запуск задачи поиска вредоносного ПО.
- Реагирование через KEDR:

- Управление сетевой изоляцией активов.
- Управление правилами запрета (по хеш-сумме файла).
- Запуск программы.
- Реагирование через KICS for Networks:
 - Изменение статуса устройства на Разрешенное
 - Изменение статуса устройства на Неразрешенное
- Реагирование через Active Directory:
 - Добавление учетной записи в группу.
 - Удаление учетной записи из группы.
 - Сброс пароля учетной записи.
 - Блокировка учетной записи.
- Выполнение произвольного скрипта на сервере коррелятора KUMA.

Действия по реагированию могут запускаться вручную из веб-интерфейса KUMA или автоматически с помощью правил реагирования.

Статья онлайн-справки «Интеграция с другими решениями»

<https://support.kaspersky.ru/kuma/4.0/217927>

Статья KUMA Community «Реагирование» (доступны «кастомные» интеграции со сторонними решениями):

<https://kb.kuma-community.ru/books/integracii/chapter/reagirovanie>

Ниже рассмотрен пример ручного реагирования средствами Kaspersky Security Center.

Создание задач в Kaspersky Security Center

Предварительно выполните шаги по настройке интеграции с Kaspersky Security Center, описанные в Статье [Интеграция с Kaspersky Security Center](#).

Вы можете вручную или автоматически запускать на активах Kaspersky Security Center, импортированных в KUMA, задачу обновления антивирусных баз и модулей программы и задачу поиска вредоносного ПО. На активах должны быть установлены программы Kaspersky Endpoint Security для Windows или Linux.

Предварительно на стороне Kaspersky Security Center необходимо создать задачи обновления антивирусных баз и поиска вредоносного ПО.

Kaspersky Security Center Web Console

Чтобы создать задачу поиска вредоносного ПО:

- Выберите **Активы (Устройства) → Задачи**.
- В Списке задач нажмите на кнопку **Добавить**.
- Запустится мастер создания задачи.
- Настройте параметры задачи:
 - В раскрывающемся списке **Приложение** выберите используемое приложение Kaspersky Endpoint Security для Windows (в нашем примере 12.8.0).
 - В раскрывающемся списке **Тип задачи** выберите **Поиск вредоносного ПО**.
 - В поле **Название задачи** введите название создаваемой задачи. Важно в названии задачи указать префикс «**KUMA**». Задачи для Kaspersky Endpoint Security с данным префиксом в дальнейшем будут доступны в интерфейсе KUMA.
 - В блоке **Устройства, которым будет назначена задача** выберите **Задать адреса устройств вручную или импортировать из списка**.

Параметры новой задачи

Приложение	Kaspersky Endpoint Security для Windows (12.8.0) 	1
Тип задачи	Поиск вредоносного ПО 	2
Название задачи	KUMA Поиск вредоносного ПО	3

Устройства, которым будет назначена задача 

☐ Назначить задачу группе администрирования

☒ Задать адреса устройств вручную или импортировать из списка 4

☐ Назначить задачу выборке устройств

- Нажмите на кнопку **Далее**.
- В окне **Область действия задачи** нажмите **Добавить устройства**. В окне справа **Добавить устройства** выберите **Выбрать устройства, обнаруженные в сети Сервером администрирования**. Для создания задачи можно указать любое устройство. KUMA будет передавать имена устройств, на которых нужно запустить задачу поиска вредоносного ПО.

KUMA Поиск вредоносного ПО

Общие

Результаты

Параметры

Параметры приложения

Расписание

История ревизий

Права доступа

Область проверки

+ Добавить

✕ Удалить

Области проверки	Статус	Дополнительно
☐ Моя почта	☐ Выключено	
☐ Память ядра	☐ Выключено	
☐ Запущенные процессы и объекты автозапуска	☐ Выключено	
☐ Загрузочные секторы	☐ Выключено	
☐ Системное резервное хранилище	☐ Выключено	
☐ Все съемные диски	☐ Выключено	
☐ Все сетевые диски	☐ Выключено	
☐ Все жесткие диски	☐ Выключено	
☐ Документы	☒ Включено	Включить вложенные папки

- Нажмите **Добавить** и затем **Далее**.
- В окне **Выбор учетной записи для запуска задачи** укажите **Учетная запись по умолчанию**. Нажмите **Далее**.
- Завершите работу мастера, нажав кнопку **Готово**.
- В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и укажите **Области проверки**. В рамках тестирования можно уменьшить область проверки. В дальнейшем эту настройку можно изменить.

KUMA Поиск вредоносного ПО

Общие

Результаты

Параметры

Параметры приложения

Расписание

История ревизий

Права доступа

Область проверки

+ Добавить

✕ Удалить

Области проверки	Статус	Дополнительно
☐ Моя почта	☐ Выключено	
☐ Память ядра	☐ Выключено	
☐ Запущенные процессы и объекты автозапуска	☐ Выключено	
☐ Загрузочные секторы	☐ Выключено	
☐ Системное резервное хранилище	☐ Выключено	
☐ Все съемные диски	☐ Выключено	
☐ Все сетевые диски	☐ Выключено	
☐ Все жесткие диски	☐ Выключено	
☐ Документы	☒ Включено	Включить вложенные папки

- В секции **Действие при обнаружении угрозы** снимите флажок **Выполнять только во время простоя компьютера**.

Действие при обнаружении угрозы

- ☒ Лечить. Удалять, если лечение невозможно
- ☐ Лечить. Информировать, если лечение невозможно
- ☐ Информировать
- ☐ Выполнять лечение активного заражения немедленно
В случае обнаружения активных угроз процедура лечения активного заражения будет запущена без запроса согласия пользователя.
По окончании процедуры компьютер может быть перезагружен.
- ☐ Проверять только новые и измененные файлы
Снижает время проверки
- ☐ Выполнять только во время простоя компьютера **1**

- Перейдите на вкладку **Расписание** и убедитесь, что для параметра **Запуск задачи** указано **Вручную**.

Расписание задачи

Запуск задачи

Вручную

1**Дополнительные параметры**

- ☐ Запускать пропущенные задачи
- ☐ Использовать автоматическое определение случайного интервала между запусками задачи
 - ☐ Использовать автоматическую случайную задержку запуска задачи в интервале

1

Минуты

- ☐ Включать устройства перед запуском задачи функцией Wake-on-LAN за
- ☐ Выключать устройства после выполнения задачи
- ☐ Остановить, если задача выполняется дольше

120

Минуты

- Нажмите **Сохранить**.

Задача поиска вредоносного ПО создана.

Далее создадим задачу обновления антивирусных баз и модулей.

Чтобы создать задачу обновления антивирусных баз и модулей:

- Выберите **Активы (Устройства) → Задачи**.
- В **Списке задач** нажмите на кнопку **Добавить**

- Запустится мастер создания задачи.
- Настройте параметры задачи:
 - В раскрывающемся списке **Приложение** выберите используемое приложение Kaspersky Endpoint Security для Windows (в нашем примере 12.8.0).
 - В раскрывающемся списке **Тип задачи** выберите **Обновление**.
 - В поле **Название задачи** введите название создаваемой задачи. Важно в названии задачи указать префикс «**KUMA**». Задачи для Kaspersky Endpoint Security с данным префиксом в дальнейшем будут доступны в интерфейсе KUMA.
 - В блоке **Устройства, которым будет назначена задача** выберите **Задать адреса устройств вручную или импортировать из списка**.

Параметры новой задачи

Приложение

Kaspersky Endpoint Security для Windows (12.8.0) ▼

1

Тип задачи

Обновление ▼

2

Название задачи

KUMA Обновление антивирусных баз и модулей

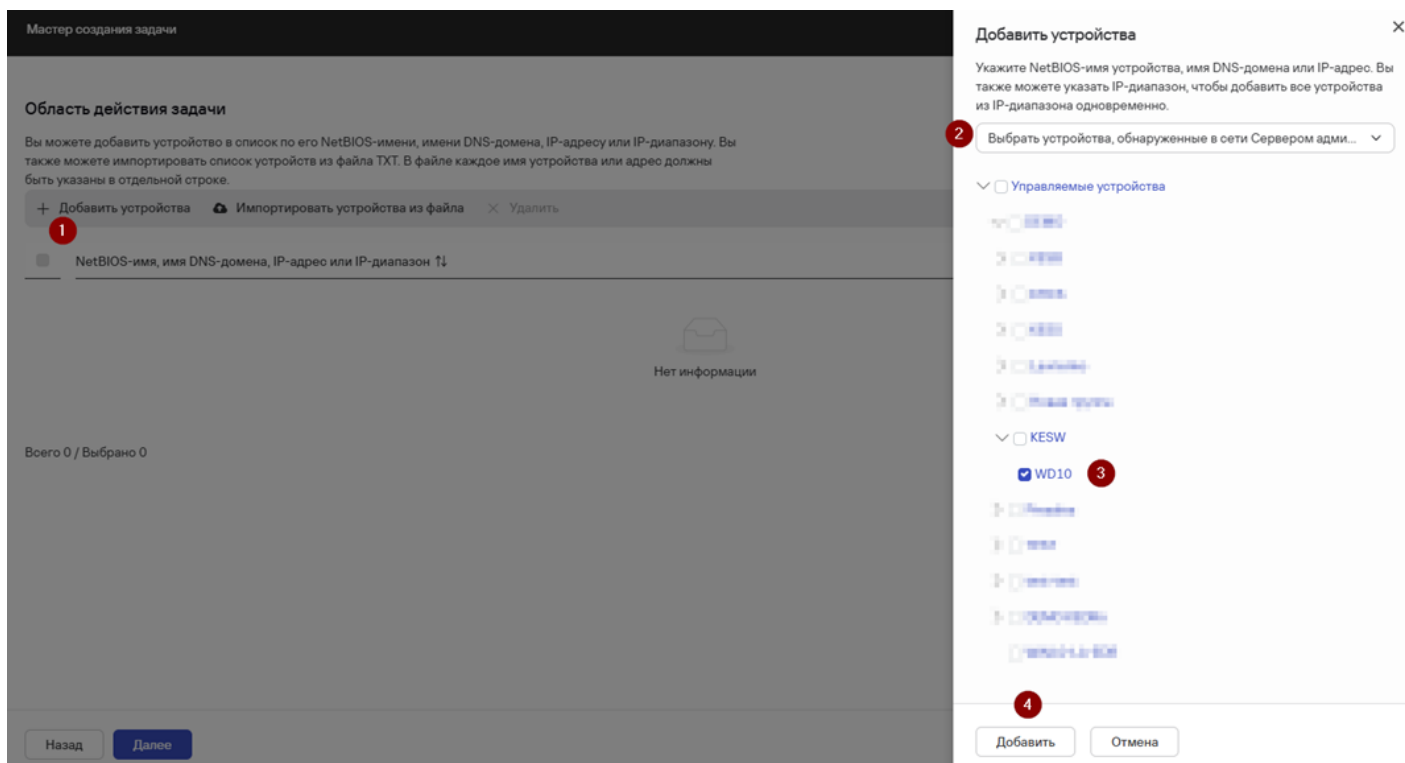
3

Устройства, которым будет назначена задача 

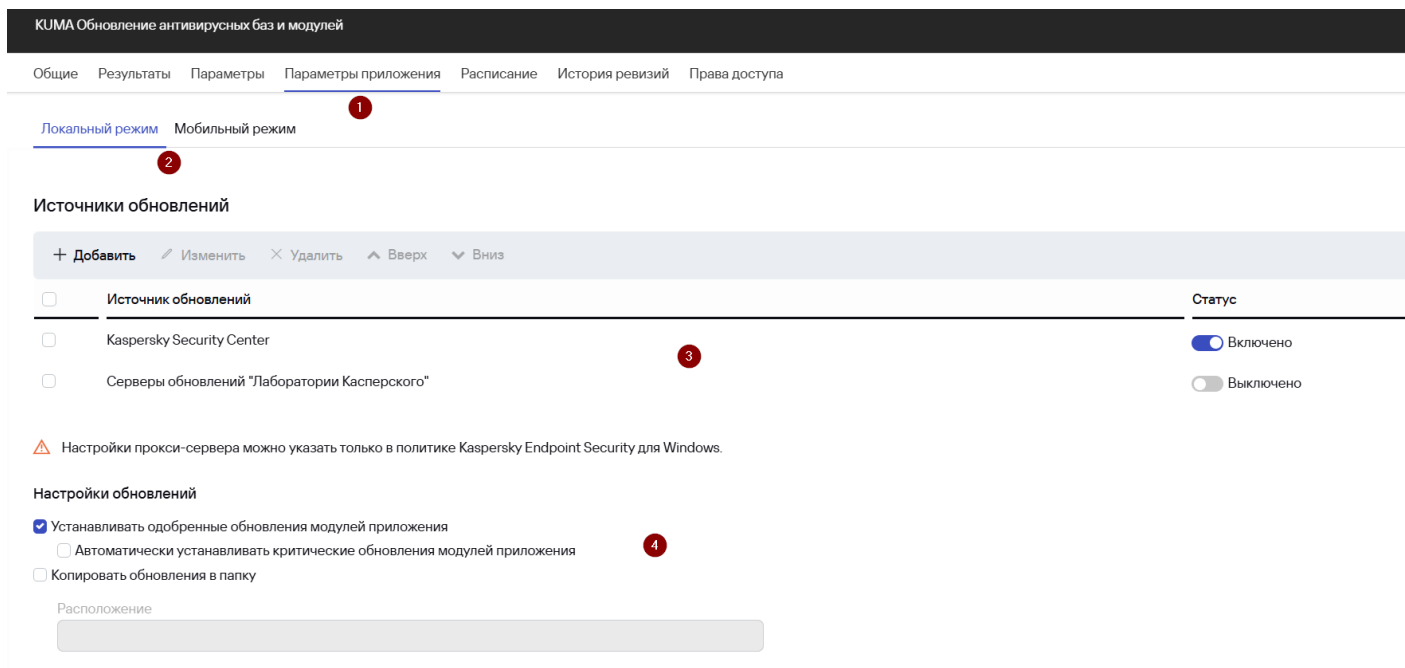
☐ Назначить задачу группе администрирования
 ☒ Задать адреса устройств вручную или импортировать из списка
 ☐ Назначить задачу выборке устройств

4

- Нажмите на кнопку **Далее**.
- В окне **Область действия задачи** нажмите **Добавить устройства**. В окне справа **Добавить устройства** выберите **Выбрать устройства, обнаруженные в сети Сервером администрирования**. Для создания задачи можно указать любое устройство. KUMA будет передавать имена устройств, на которых нужно запустить задачу обновления антивирусных баз.



- Нажмите **Добавить** и затем **Далее**.
- В окне **Выбор учетной записи для запуска задачи** укажите **Учетная запись по умолчанию**. Нажмите **Далее**.
- Завершите работу мастера, нажав кнопку **Готово**.
- В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и при необходимости отредактируйте **Источники обновлений** и **Настройки обновлений**.



- Перейдите на вкладку **Расписание** и убедитесь, что для параметра **Запуск задачи** указано **Вручную**.

Расписание задачи

Запуск задачи

Вручную

1

Дополнительные параметры

- ☐ Запускать пропущенные задачи
- ☐ Использовать автоматическое определение случайного интервала между запусками задачи
 - ☐ Использовать автоматическую случайную задержку запуска задачи в интервале

1

Минуты

- ☐ Включать устройства перед запуском задачи функцией Wake-on-LAN за
- ☐ Выключать устройства после выполнения задачи
- ☒ Остановить, если задача выполняется дольше

120

Минуты

- Нажмите **Сохранить**.

Задача обновления антивирусных баз и модулей создана.

Реагирование вручную средствами Kaspersky Security Center

Чтобы запустить реагирование средствами Kaspersky Security Center вручную:

- Перейдите в **Алерты** и выберите алерт, в рамках которого необходимо запустить действие по реагированию. В нашем примере это алерт **R220_Сбор информации об учетных записях** (см. статью [Работа с алертами](#))
- В карточке алерта в разделе **Связанные активы** выберите актив для запуска задачи.
- В появившемся окне **Информация об активе** нажмите **Запустить задачу**.

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты 1

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNetDomain: TRUECOMPANY, DeviceReceiptTime: 06.03.2025 14:28:19, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: 665d9a12-a35a-48dd-9930-dce06f608854, SourceNetDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867612-1129, DestinationAccountID: 6c578a24-f43d-412f-9fce-487ad639f77a, DestinationNetDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1e0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x1e78, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %N1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject login ID, FlexString2: 0x0

Связанные активы

Количество ↓	Актив	Категории
2	Название: wd10, IP-адрес: 10.68.85.92, Полное доменное имя: wd10.truecompany.local	Categorized assets/Критичные активы WIN10 2

Связанные пользователи

Количество ↓	Пользователь	Имя участника-пользователя (UPN)	Адрес электронной почты	Доме
1	Ivan Ivanov	I.Ivanov@truecompany.local	I.Ivanov@truecompany.local	truecoo

Журнал изменений

Комментарий

Время ↓	Пользователь	Действие
---------	--------------	----------

Информация об активе

Удалить

Изменить

Переместить в группу KSC

Запустить задачу 3

Название

wd10

Тенант

Main

Источник актива

Kaspersky Security Center, Создан вручную

Идентификатор

6c578a24-f43d-412f-9fce-487ad639f77a

Создано

20.02.2025 14:07:32

Последнее обновление

06.03.2025 06:58:03

IP-адрес

10.68.85.92

Владелец

Ivan Ivanov

Полное доменное имя

wd10.truecompany.local

MAC-адрес

88-E6-4F-8A-24-F4

Категория КИИ

Информационный ресурс не является объектом КИИ

Расширенный статус KSC

Антивирусные базы обновлялись слишком давно

- В раскрывающемся списке выберите **Реагирование KSC** и далее ранее созданную задачу **KUMA Обновление антивирусных баз и модулей** (перед запуском задачи KUMA Поиск вредоносного ПО выполним задачу обновления для получения наиболее актуальных сигнатур вредоносного ПО).

Выберите задачу

✓ KUMA Обновление антивирусных баз и модулей 1

KUMA Поиск вредоносного ПО

- Нажмите **Запустить**.

Задача обновления на выбранном активе запущена.
Чтобы убедиться, что задача была запущена и завершена успешно перейдите в раздел **События** и выполните следующий поисковый запрос:

```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA Обновление антивирусных баз и модулей' AND DeviceEventClassID = 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

Kaspersky
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События 1

Активы

События

Не обновлять
5m
Последние 5м
[OOTB] Storage (Main...

1
SELECT * FROM 'events' WHERE FlexString2 = 'KUMA Обновление антивирусных баз и модулей' AND DeviceEventClassID = 'KLPRCL_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DestinationHostName	DeviceEventClassID	Name	FlexString2
Main	06.03.2025 15:46:59.316	Kaspersky	KSC	WD10	KLPRCL_TaskState	Завершена успешно	KUMA Обновление антивирусных баз и модулей
Main	06.03.2025 15:45:59.034	Kaspersky	KSC	WD10	KLPRCL_TaskState	Выполняется	KUMA Обновление антивирусных баз и модулей

Также статус выполнения задачи можно посмотреть в консоли Kaspersky Security Center или непосредственно в интерфейсе приложения Kaspersky Endpoint Security.

Результат Последние события, на 06.03.2025 16:09:02

Обновить Удалить Экспортировать в файл Назначить категорию История ревизий Исключить из Адаптивного контроля аномалий

Событие произошло	Устройство	Событие	Описание	Группа
06.03.2025 15:58:24	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:58:24	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:58:24	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:58:24	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:58:24	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:56	WD10	Завершена успешно		KES
06.03.2025 15:49:53	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:53	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:53	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:53	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:53	«Сервер администрирования»	Аудит: окончание от Касперского	Выполнение "task.kumad" ...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:53	WD10	Выбран источник обновлений	Геттообъекты: Выбор из...	KES
06.03.2025 15:49:18	WD10	Выполняется		KES

Свойства события

Название задачи
KUMA Обновление антивирусных баз и модулей

Перейти к задаче

Завершена успешно

06.03.2025 15:49:56

KESW

WD10

Приложение
Kaspersky Endpoint Security для Windows (12.8.0)

Версия
12.8.0.505

Событие зарегистрировано 06.03.2025 15:50:03

Далее запустите ранее созданную задачу KUMA Поиск вредоносного ПО:

- Перейдите в **Алерты** и выберите алерт, в рамках которого необходимо запустить действие по реагированию. В нашем примере это алерт **R220_Сбор информации об учетных записях**.
- В карточке алерта в разделе **Связанные активы** выберите актив для запуска задачи.
- В появившемся окне **Информация об активе** нажмите **Запустить задачу**.



Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты 1

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Security-Audit, DeviceEventLastID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNetDomain: TRUECOMPANY, DeviceReceiptTime: 06.03.2025 14:28:19, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48dd-9930-d0e06f608854, SourceNetDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceHostID: 6-15-21-1404947508-1637455289-128886, 7512-1129, DestinationLastID: 6c578a24-f43d-412f-9fce-487ad639f77a, DestinationNetDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, ObjectIdType: SecurityLog, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: MandatoryLabel, DeviceCustomString3: 0x1a40, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x1c78, DeviceCustomString5Label: New Process ID, DeviceCustomString6: %N1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject logon ID, FlexString2: 0x0

Информация об активе

Удалить

Изменить

Переместить в группу KSC

Запустить задачу 3

Название

wd10

Тенант

Main

Источник актива

Kaspersky Security Center, Создан вручную

Идентификатор

6c578a24-f43d-412f-9fce-487ad639f77a

Создан

20.02.2025 14:07:32

Последнее обновление

06.03.2025 06:58:03

IP-адрес

10.68.85.92

Владелец

Ivan Ivanov

Полное доменное имя

wd10.truecompany.local

MAC-адрес

88-e1-2b-4a-87-f7-3f

Категория КИИ

Информационный ресурс не является объектом КИИ

Расширенный статус KSC

Антивирусные базы обновлялись слишком давно

Связанные активы

Количество ↓	Актив	Категория
2	Название: wd10, IP-адрес: 10.68.85.92, Полное доменное имя: wd10.truecompany.local	Categorized assets/Критичные активы WIN10 2

Связанные пользователи

Количество ↓	Пользователь	Имя участника-пользователя (UPN)	Адрес электронной почты	Домашний компьютер
1	Ivan Ivanov	I.Ivanov@truecompany.local	I.Ivanov@truecompany.local	trueco

Журнал изменений

Комментарий

Время ↓	Пользователь	Действие
---------	--------------	----------

- В раскрывающемся списке выберите **Реагирование КС** и далее ранее созданную задачу **КУМА Поиск вредоносного ПО**.
- Нажмите **Запустить**.

Выберите задачу

- ✓ KUMA Поиск вредоносного ПО 1

Задача поиска вредоносного ПО на выбранном активе запущена.

Чтобы убедиться, что задача завершена успешно перейдите в раздел **События** и выполните следующий поисковый запрос:

```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA Поиск вредоносного ПО' AND DeviceEventClassID = 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События 1

Активы

События

Не обновлять 5m Последние 5m [OOTB] Storage (Main...

1 SELECT * FROM 'events' WHERE FlexString2 = 'KUMA Поиск вредоносного ПО' AND DeviceEventClassID = 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DestinationHostName	DeviceEventClassID	Name	FlexString2
Main	06.03.2025 15:51:59.897	Kaspersky	KSC	WD10	KLPRCI_TaskState	Завершена успешно	KUMA Поиск вредоносного ПО
Main	06.03.2025 15:51:59.897	Kaspersky	KSC	WD10	KLPRCI_TaskState	Выполняется	KUMA Поиск вредоносного ПО

Также статус выполнения задачи можно посмотреть в консоли Kaspersky Security Center или непосредственно в интерфейсе приложения Kaspersky Endpoint Security.

Результат Последние события, на 06.03.2025 16:09:02

Обновить Удалить Экспортировать в файл Назначить категорию История ревизий Исключить из Адаптивного контроля аномалий

Событие произошло	Устройство	Событие	Описание	Группа
06.03.2025 15:56:14	«Сервер администрирования»	Аудит: включенный сервер	Получены данные "Task State"	KES
06.03.2025 15:56:14	«Сервер администрирования»	Аудит: включенный в сеть	Получены данные "Task State"	KES
06.03.2025 15:55:58	«Сервер администрирования»	Аудит: включенный сервер	Получены данные "Task State"	KES
06.03.2025 15:55:58	«Сервер администрирования»	Аудит: включенный в сеть	Получены данные "Task State"	KES
06.03.2025 15:55:43	«Сервер администрирования»	Аудит: включенный сервер	Получены данные "Task State"	KES
06.03.2025 15:55:43	«Сервер администрирования»	Аудит: включенный в сеть	Получены данные "Task State"	KES
06.03.2025 15:55:27	WD10	Завершена успешно		KES
06.03.2025 15:55:27	WD10	Выполняется		KES

Свойства события

Название задачи
KUMA Поиск вредоносного ПО

Перейти к задаче
Завершена успешно

06.03.2025 15:55:27
KESW
WD10

Приложение
Kaspersky Endpoint Security для Windows (12.8.0)

Версия
12.8.0.505

Событие зарегистрировано 06.03.2025 15:55:33

Запускать ручную реагирование средствами Kaspersky Security Center также можно из раздела **Активы**, выбрав соответствующий актив из списка, или из карточки **События**, нажав на имя актива в поле ***AssetID**.



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы 1

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Активы

Все активы

Выбранные тенанты: Все

Все тенанты

Main

Categorized assets

Address space

Business impact

Infrastructure

KATA servers

Critical Assets

Location

Org chart

Критичные активы WIN10

Активы без категории

wd10

Название	Полное доменное имя	IP-адрес	Источник актива
wd10	wd10.truecompany.local	10.68.85.92	Kaspersky Security Cent

Информация об активе

Удалить Изменить Переместить в группу KSC Запустить задачу

Название
wd10

Тенант
Main

Источник актива
Kaspersky Security Center, Создан вручную

Идентификатор
6c578a24-f43d-412f-9fce-487ad639f77a

Создано
20.02.2025 14:07:32

Последнее обновление
06.03.2025 06:58:03

IP-адрес
10.68.85.92

Владелец
Ivan Ivanov

Полное доменное имя
wd10.truecompany.local

MAC-адрес
0800 541F 1F1F

Категория КИИ
Информационный ресурс не является объектом КИИ

Отмена

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События 1

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

События

1 SELECT * FROM `events` WHERE DeviceEventClassID = '4624' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct
Main	06.03.2025 15:00:16:907	Microsoft	Windows
Main	06.03.2025 15:00:14:882	Microsoft	Windows
Main	06.03.2025 15:00:13:852	Microsoft	Windows
Main	06.03.2025 15:00:12:836	Microsoft	Windows
Main	06.03.2025 15:00:12:836	Microsoft	Windows
Main	06.03.2025 15:00:11:831	Microsoft	Windows
Main	06.03.2025 15:00:11:831	Microsoft	Windows
Main	06.03.2025 15:00:10:823	Microsoft	Windows
Main	06.03.2025 15:00:08:796	Microsoft	Windows
Main	06.03.2025 15:00:08:796	Microsoft	Windows
Main	06.03.2025 15:00:08:795	Microsoft	Windows
Main	06.03.2025 15:00:07:776	Microsoft	Windows
Main	06.03.2025 15:00:07:774	Microsoft	Windows
Main	06.03.2025 14:59:46:511	Microsoft	Windows
Main	06.03.2025 14:59:46:510	Microsoft	Windows
Main	06.03.2025 14:59:46:510	Microsoft	Windows

Информация о событии

Копировать

TenantID	Main
Timestamp	06.03.2025 15:00:14:882
Name	An account was successfully logged on.
EndTime	06.03.2025 15:03:47:471
DeviceAssetID	wd10
DeviceEventCategory	Microsoft-Windows-Security-Auditing
DeviceEventClassID	4624
DeviceHostName	wd10.truecompany.local
DeviceNtDomain	TRUECOMPANY
DeviceProduct	Windows
DeviceReceiptTime	06.03.2025 15:03:47:471
DeviceTimeZone	+03:00
DeviceVendor	Microsoft
SourceNtDomain	TRUECOMPANY.LOCAL
SourceProcessName	Advapi
SourceUserID	S-1-5-18
SourceUserName	wd10\$
DestinationAssetID	wd10
DestinationHostName	Информация об активе
DestinationNtDomain	Найти похожие события
DestinationProcessName	C:\Windows\System32\services.exe
DestinationUserID	S-1-5-18

Статья онлайн-справки «Автоматический запуск задач Kaspersky Security Center»:
<https://support.kaspersky.ru/kuma/4.0/218008>

Revision #3
Created 2026-08-12 11:17:46 UTC by Dmitry Borisov
Updated 2026-08-12 12:56:29 UTC by Dmitry Borisov