

Работа с алертами

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

Официальная документация по данному разделу приведена в онлайн-справке на продукт: <https://support.kaspersky.ru/kuma/4.0/218046>

Алерт - это уведомление (оповещение), создаваемое в KUMA, при получении события или последовательности событий, которое приводит к срабатыванию правила корреляции.

KUMA автоматически присваивает уровень важности каждому алерту. Уровень важности отражает насколько критичны для безопасности действия/выполненные команды/запущенные процессы и файлы, обнаруженные в событии. Уровень важности зависит от уровня важности сработавшего правила корреляции и категории актива, который вовлечен в алерт.

Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Критический

Редактирование правила корреляции

Общие

Селекторы

Действия

Корреляторы

Название*	Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUM
Тенант*	Main
Тип*	standard
Группирующие поля* ⓘ	DeviceAction × SourceAddress × SourceUserName × EventOutcome ×
Время жизни контейнера, сек.*	60
Уникальные поля ⓘ	
Частота срабатываний ⓘ	0
Политика хранения базовых событий	all
Уровень важности	Высокий
Сортировать по	Timestamp

Изменить категорию



Название*	Windows 10
Родительская категория*	Main/Categorized assets
Тенант*	Main
Способ категоризации*	Активно
Уровень важности*	Низкий

В первую очередь следует обрабатывать алерты с более высоким уровнем важности. Значение уровня важности автоматически обновляется при получении новых корреляционных событий в результате срабатывания правил корреляции, но аналитик

также может задать уровень важности вручную. В этом случае уровень важности алерта больше не обновляется автоматически.

В разделе **Алерты** веб-интерфейса KUMA можно просматривать и обрабатывать алерты, зарегистрированные KUMA.

Жизненный цикл алертов

- KUMA создает алерт при срабатывании правила корреляции. Алерт именуется по породившему его правилу корреляции. Алерту присваивается статус **Новый**.
- Алерты в статусе **Новый** продолжают наполняться данными при последующих срабатываниях того же правила корреляции (если не используются правила сегментации). При изменении статуса алерта на любой другой, алерт больше не обновляется и, если правило корреляции срабатывает снова, создается новый алерт.

С помощью [правил сегментации](#) поток однотипных корреляционных событий можно разделять, создавая более одного алерта.

- Алерт назначается пользователю (аналитику) для дальнейшего расследования. Статус алерта меняется на **Назначен**.
- Аналитик выполняет одно из следующих действий:
 - Закрывает алерт как ложно положительный (статус алерта меняется на **Закрит**).
 - Реагирует на угрозу и закрывает алерт (статус алерта меняется на **Закрит**).
 - Создает на основе алерта инцидент (статус алерта меняется на **В инциденте**).

Наполнение алертов событиями

По умолчанию количество привязанных событий к алерту не может превышать 10 000. Когда количество событий привязанных к алерту достигает 10 000, создается новый алерт с таким же названием, но новым идентификатором. Идентификатор алерта можно просмотреть в деталях алерта. При необходимости вы можете изменить это значение в свойствах правила сегментации в поле **Количество корреляционных событий**. Правило сегментации при этом должно быть включено и привязано к правилам корреляции алертов тенанта.

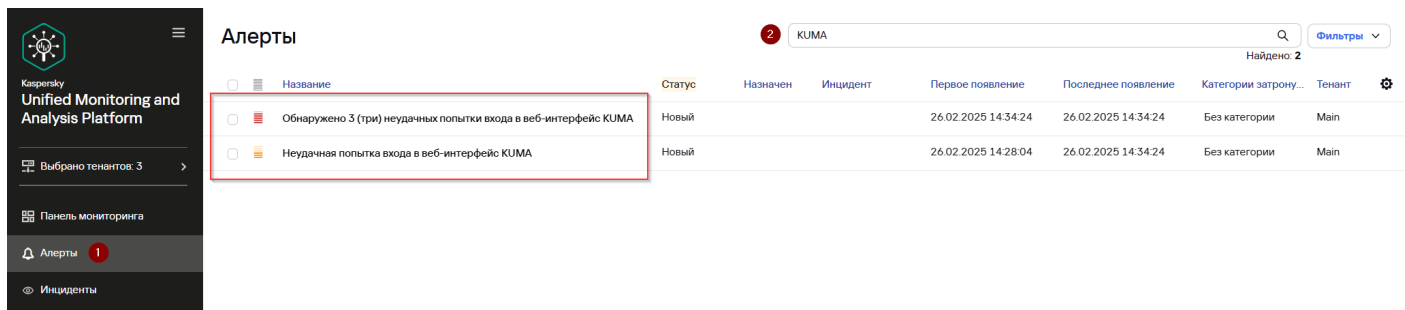
Поиск алертов

Чтобы выполнить поиск алертов:

- Перейдите в **Алерты**
- Введи в поле **Поиск** искомое имя алерта, например, «KUMA»

Пример алерта с именем «KUMA» будет доступен при создании правила типа [Simple](#) или [Standard](#).

- Убедитесь, что в таблице отображаются только алерты в названии, которых содержится слово "KUMA"



Алерты

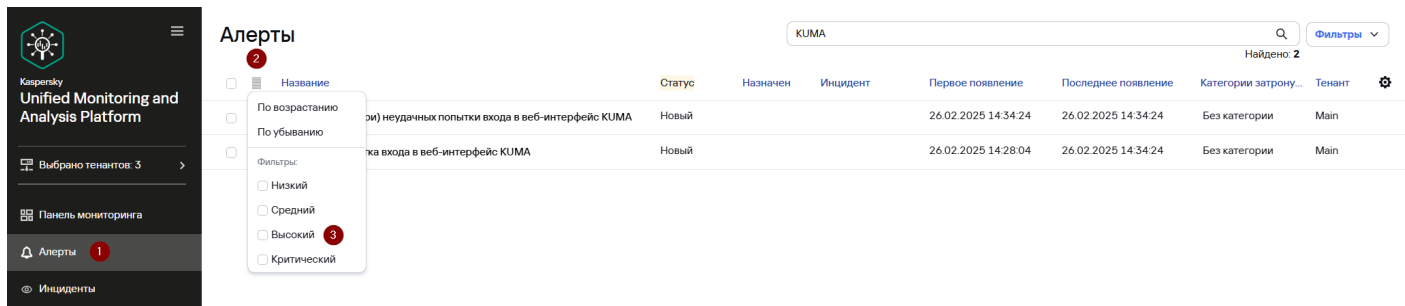
2 KUMA Найдено: 2

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затрону...	Тенант
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории	Main
Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории	Main

Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.
- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

При нажатии на заголовки столбцов вы можете просмотреть значения для фильтрации алертов. При фильтрации алертов по какому-либо параметру соответствующий заголовок таблицы алертов подсвечивается желтым цветом.



Алерты

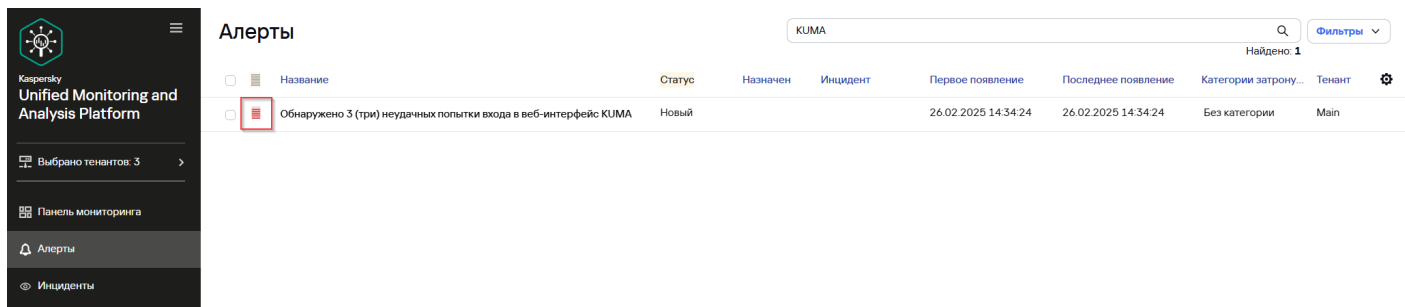
KUMA Найдено: 2

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затрону...	Тенант
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории	Main
Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории	Main

По возрастанию
По убыванию

Фильтры:

- ☐ Низкий
- ☐ Средний
- ☒ Высокий
- ☐ Критический



Алерты

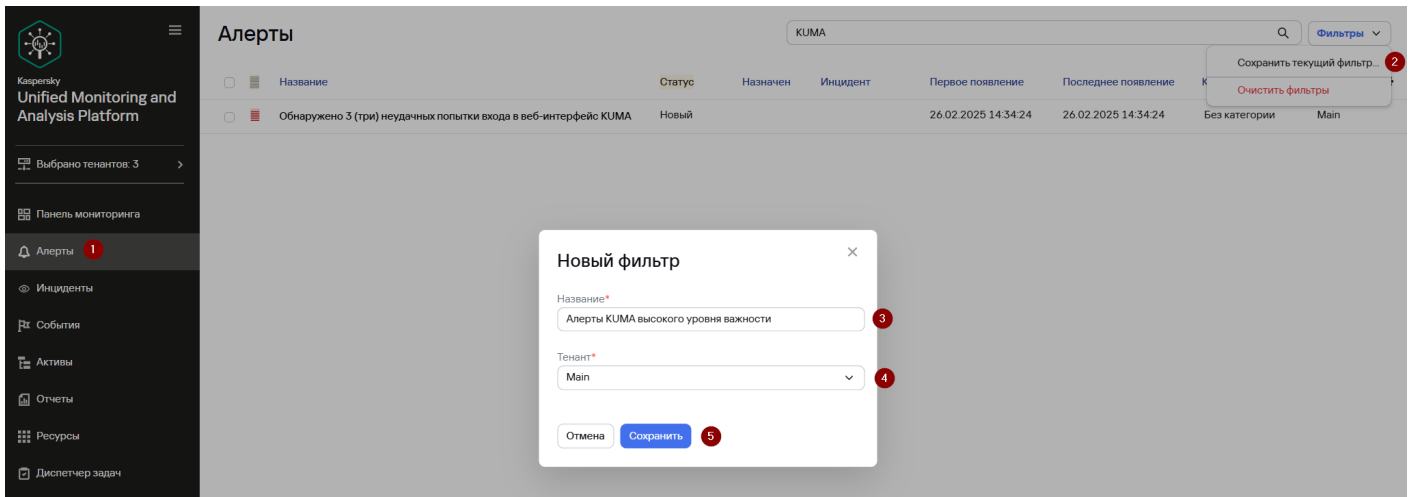
KUMA Найдено: 1

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затрону...	Тенант
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории	Main

Чтобы сохранить текущие параметры фильтрации алертов:

- В разделе **Алерты** откройте раскрывающийся список **Фильтры**.

- Выберите **Сохранить текущий фильтр**.
 - Появится поле для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
 - Введите название фильтра.
 - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.
- Фильтр сохранен.



Чтобы сбросить текущие настройки фильтра, откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтры**.

Просмотр информации об алерте

Для примера можно использовать уже сформированный алерт в KUMA (при наличии) или выполнить следующие действия для создания алерта:

- Убедитесь, что правила **R220_02_Сбор информации об учетных записях стандартными средствами Windows** и **R220_Сбор информации об учетных записях** привязаны к коррелятору. Для этого:
 - Перейдите в **Ресурсы** → **Активные сервисы**
 - Выберите сервис коррелятора
 - В окне **Редактирование коррелятора** перейдите на шаг **Корреляция**
 - В поле **Поиск** введите «220»
 - Убедитесь, что правила **R220_02_Сбор информации об учетных записях стандартными средствами Windows** и **R220_Сбор информации об учетных записях** присутствуют в списке.
 - Если правила отсутствуют в списке выполните привязку правил аналогично статьям [Простое правило \(simple\)](#) и [Стандартное правило \(standard\)](#).

Общие

Глобальные переменные

Корреляция 1

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются алерты. Подробнее см. [в онлайн-справке](#).

+ Добавить 🔗 Привязать 🗑️ Удалить ⬆️ Поднять ⬆️ Опустить ⋮			220 2	🔍
☐ Правила корреляции	Тип	Действия		
☐ R220_03_Сбор информации о локальных учетных записях через PowerShell	simple	В дальнейшую обработку	В коррелятор	Не создавать алерт Обогащение событий
☐ R220_02_Сбор информации об учетных записях стандартными средствами Windows	simple	В дальнейшую обработку	В коррелятор	Не создавать алерт Обогащение событий
☐ R220_04_Сбор информации о доменных учетных записях через PowerShell (cmd)	simple	В дальнейшую обработку	В коррелятор	Не создавать алерт Обогащение событий
☐ R220_06_Поиск паролей в реестре	simple	В дальнейшую обработку	В коррелятор	Не создавать алерт Обогащение событий
☐ R220_Сбор информации об учетных записях	simple	В дальнейшую обработку	В коррелятор	Обогащение событий
☐ R220_07_Сбор информации об адресах электронной почты	simple	В дальнейшую обработку	В коррелятор	Не создавать алерт Обогащение событий

Найдено 8 / Выбрано 0

Сохранить

Отмена

- Убедитесь, что события Windows **A new process has been created (Event ID 4688)** поступают с тестовой рабочей станции. Для этого:
 - Перейдите в раздел **События**.
 - Укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE DeviceEventClassID = '4688' AND DeviceHostName = '<имя тестовой рабочей станции>' ORDER BY Timestamp DESC LIMIT 250
```

- Нажмите **Выполнить запрос**
- Убедитесь, что события **A new process has been created** отображаются в таблице событий.
- Если события **A new process has been created** отсутствуют в таблице событий выполните настройку сбора событий с EventID 4688 одним из [описанных способов](#).

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

События

Не обновлять

5m

Последние 5м

[OOTB] Storage (Main...

1 SELECT * FROM 'events' WHERE DeviceEventClassID = '4688' AND DeviceHostName = 'wd10.truecompany.local' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DeviceHostName	Name	DeviceEventClassID
Main	03.03.2025 19:25:57.763	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:24:38.107	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:24:37.091	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.862	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.862	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688
Main	03.03.2025 19:22:18.861	Microsoft	Windows	wd10.truecompany.local	A new process has been created.	4688

- На тестовой рабочей станции запустите командную строку и выполните команду `whoami` для отображения имени текущего пользователя.

Командная строка

```

Microsoft Windows [Version 10.0.19044.1288]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\i.ivanov>whoami
truecompany\i.ivanov

C:\Users\i.ivanov>

```

- В веб-интерфейсе KUMA перейдите в раздел **Алерты** и убедитесь, что алерт **R220_Сбор информации об учетных записях** появился в таблице алертов.

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Алерты

Поиск...

Филтры

Найдено: 4

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов	Тенант
R220_Сбор информации об учетных записях	Новый			03.03.2025 19:52:34	03.03.2025 19:52:34	Many/Categorized assets/Критичные активы WPN10	Main
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории	Main
Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории	Main
KWTS Detection	В инциденте		KWTS Detection	01.08.2024 12:30:58	01.08.2024 12:30:58	Без категории	Main

Чтобы просмотреть информацию об алерте:

- Перейдите в раздел **Алерты**.
- Нажмите на название алерта, информацию о котором вы хотите просмотреть. В нашем примере это алерт **R220_Сбор информации об учетных записях**.
- Откроется окно с информацией об алерте. В верхней части окна с информацией об алерте расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. В этом окне можно обработать алерт: изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент (подробнее см. Раздел Обработка алертов).

Корпоративная Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты

R220_Сбор информации об учетных записях Новый

Уровень важности:

Высокий

 Назначить:

Не назначено

Закрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции: Низкий

Первое появление: 04.03.2025 13:44:38

Тенант: Main

Наивысшая важность категории активов: Критический

Последнее появление: 04.03.2025 13:44:38

Правило корреляции: [R220_Сбор информации об учетных записях](#)

Идентификатор алерта: 326df6d-667a-4236-9b1e-4210463b5201

Связанные события

Скачать события

Найти в событиях

Время ↓	Информация о событии	Тенант
04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY.LOCAL\jlapov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: jlapov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-1436-412f-9f6e-487a6d39f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNTDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceProcessID: e65df912-a35a-48d1-9930-d0e04608854, SourceNTDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288667512-1129, DestinationAssetID: 6c578a24-1436-412f-9f6e-487a6d39f77a, DestinationNTDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, OffsetType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomStringLabel: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x1376, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %N%1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject login ID, FlexString2: 0x0	Main

Всего: 1

Раздел Информация об алерте

Этот раздел позволяет просмотреть основную информацию об алерте. Он содержит следующие данные:

- **Уровень важности правила корреляции** – уровень важности правила корреляции, в результате срабатывания которого создан алерт.
- **Наивысшая важность категории активов** – самый высокий уровень важности категории активов из тех, которые принадлежат связанным с этим алертом активам. Если с алертом связано несколько активов, отображается наибольшее значение.
- **Привязан к инциденту** – если алерт привязан к инциденту, то отображаются название и статус алерта. Если алерт не привязан к инциденту, поле не заполнено.
- **Первое появление** – дата и время создания первого корреляционного события, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события, приведшего к созданию или обновлению алерта.
- **Идентификатор алерта** – уникальный идентификатор алерта в KUMA.
- **Тенант** – название тенанта, которому принадлежит алерт.
- **Правило корреляции** – название правила корреляции, в результате срабатывания которого создан алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.

Коррелятор

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты >

R220_Сбор информации об учетных записях Новый

Уровень важности: Высокий Назначить: Не назначено Закрыть алерт Создать инцидент Привязать

Информация об алерте

Уровень важности правила корреляции
Низкий

Первое появление
04.03.2025 13:44:38

Тенант
Main

Наивысшая важность категории активов
Критический

Последнее появление
04.03.2025 13:44:38

Правило корреляции
[R220_Сбор информации об учетных записях](#)

Идентификатор алерта
326df6d-667a-4236-9b1e-4210463b5201

Связанные события

Скачать события Найти в событиях

Время ↓	Информация о событии	Тенант
> 04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY.LOCAL\jlapov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: jlapov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-1434-412f-9f6e-487a6d39f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNTDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48d1-9930-d0e04608854, SourceNTDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867512-1129, DestinationAssetID: 6c578a24-1434-412f-9f6e-487a6d39f77a, DestinationNTDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, OldFileTypes: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x1376, DeviceCustomString5Label: New Process ID, DeviceCustomString6: %N1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject login ID, FlexString2: 0x0	Main

Всего: 1

Раздел Связанные события

Этот раздел содержит таблицу событий, относящихся к алерту. Если нажать на значок  рядом с корреляционным событием, отобразятся базовые события, которые стали триггером срабатывания правила корреляции.

Базовое событие.

Корреляционное событие.

Событие, которое было получено от источника и было нормализовано.

При обнаружении события или последовательности событий, удовлетворяющих условиям правила корреляции, коррелятор создает корреляционное событие.

В нашем примере используется «вложенное» правило корреляции **R220_02_Сбор информации об учетных записях стандартными средствами Windows**, срабатывание которого приводит к срабатыванию вышестоящего (обобщающего) правила **R220_Сбор информации об учетных записях**. Поэтому при нажатии на значок  отображается сначала еще одно корреляционное событие (результат срабатывания **R220_02_Сбор информации об учетных записях стандартными средствами Windows**), а уже затем отображается базовое событие.

Связанные события

4	5	Время ↓	Информация о событии	Тенант
1		04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY\LOCAL\j.ivanov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: j.ivanov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-f43d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNTDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48dd-9930-dce06f608854, SourceNTDomain: TRUECOMPANY\LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867512-1129, DestinationAssetID: 6c578a24-f43d-412f-9fce-487ad639f77a, DestinationNTDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-O-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x137c, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject logon ID, FlexString2: 0x0	Main
			Корреляционное событие, созданное в результате срабатывания правила R220_Сбор информации об учетных записях	
2		04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY\LOCAL\j.ivanov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: j.ivanov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-f43d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNTDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48dd-9930-dce06f608854, SourceNTDomain: TRUECOMPANY\LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867512-1129, DestinationAssetID: 6c578a24-f43d-412f-9fce-487ad639f77a, DestinationNTDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-O-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x137c, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject logon ID, FlexString2: 0x0	Main
			Корреляционное событие, созданное в результате срабатывания правила R220_Сбор информации об учетных записях стандартными средствами Windows	
3		04.03.2025 13:44:37	EndTime: 04.03.2025 13:48:04, DeviceAssetID: 6c578a24-f43d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNTDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, DeviceVendor: Microsoft	Main
			Базовое событие (событие запуска утилиты whoami), ставшее триггером для срабатывания правила корреляции R220_Сбор информации об учетных записях стандартными средствами Windows	
		Найти в событиях 1		Main
		Найти в событиях 1		Main

Всего: 1

+

Добавить

📄

Дублировать

🗑️

Удалить

🔗

Привязать к коррелятору

220

При выборе события в таблице открывается область деталей, содержащая информацию о выбранном событии.

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Связанные события

Время ↓	Информация о событии	Тенант
04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY.LOCAL\ivanov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: Ivanov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-143d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNtDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimezone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48dd-9930-dce06f608854, SourceNtDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867512-1129, DestinationAssetID: 6c578a24-143d-412f-9fce-487ad639f77a, DestinationNtDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x137c, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %%1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject logon ID, FlexString2: 0x0	Main
04.03.2025 13:44:38	Message: Пользователь TRUECOMPANY.LOCAL\ivanov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: Ivanov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-143d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNtDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimezone: +03:00, EventOutcome: Audit Success, SourceAccountID: e65d9a12-a35a-48dd-9930-dce06f608854, SourceNtDomain: TRUECOMPANY.LOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: S-1-5-21-1404947558-1637455289-1288867512-1129, DestinationAssetID: 6c578a24-143d-412f-9fce-487ad639f77a, DestinationNtDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: S-1-0-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x1ef0, DeviceCustomString3Label: Process ID, DeviceCustomString4: whoami, DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x137c, DeviceCustomString5Label: New Process Id, DeviceCustomString6: %%1936, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x1a83f2, FlexString1Label: Subject logon ID, FlexString2: 0x0	Main
04.03.2025 13:44:37	EndTime: 04.03.2025 13:48:04, DeviceAssetID: 6c578a24-143d-412f-9fce-487ad639f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNtDomain: TRUECOMPANY, DeviceProduct: Windows, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimezone: +03:00, DeviceVendor: Microsoft	Main
	Найти в событиях 1	Main
	Найти в событиях 1	Main

Информация о корреляционном событии

TenantName	Main
Timestamp	04.03.2025 13:44:38:450
Name	R220_Сбор информации об учетных записях
StartTime	04.03.2025 13:44:38:448
EndTime	04.03.2025 13:44:38:448
Message	Пользователь TRUECOMPANY.LOCAL\ivanov на хосте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях
DeviceAssetID	wd10
DeviceAssetKSHostID	30bd0007-ce02-4b76-9fae-cc6c2e1b68f8
DeviceAssetKSCInstanceID	d93ef913-cb8c-4035-8798-8d9123441d2d
DeviceEventCategory	Microsoft-Windows-Security-Auditing
DeviceEventClassID	4688
DeviceHostName	wd10.truecompany.local
DeviceNtDomain	TRUECOMPANY
DeviceProduct	KUMA
DeviceReceiptTime	04.03.2025 13:48:04:290
DeviceTimezone	+03:00
DeviceVendor	Kaspersky
SourceAccountID	Ivan.Ivanov
SourceNtDomain	TRUECOMPANY.LOCAL
SourceProcessName	C:\Windows\System32\cmd.exe
SourceUserID	S-1-5-21-1404947558-1637455289-1288867512-1129
SourceUserName	Ivanov
DestinationAssetID	wd10

Информация о корреляционном событии

DestinationHostName	wd10.truecompany.local
DestinationNtDomain	-
DestinationProcessName	C:\Windows\System32\whoami.exe
DestinationUserID	S-1-0-0
DestinationUserName	-
DeviceCustomString1	S-1-16-8192
DeviceCustomString1Label	Mandatory Label
DeviceCustomString3	0x1ef0
DeviceCustomString3Label	Process ID
DeviceCustomString4	whoami
DeviceCustomString4Label	Command Line
DeviceCustomString5	0x137c
DeviceCustomString5Label	New Process Id
DeviceCustomString6	%%1936
DeviceCustomString6Label	Token Elevation Type
CorrelationRule	R220_Сбор информации об учетных записях
Service	[OOTB] Correlator
BaseEventCount	1
EventOutcome	Audit Success
ExternalID	R220

Кнопка **Найти в событиях** справа от заголовка раздела используется для перехода к расследованию алерта.

Подробнее про расследование алерта:

<https://support.kaspersky.ru/kuma/4.0/217847>

Пример расследования инцидента с помощью KUMA:

<https://support.kaspersky.ru/kuma/4.0/245892>

С помощью кнопки **Скачать события** вы можете скачать информацию о связанных событиях в виде файла в формате CSV (в кодировке UTF-8).

Раздел Связанные активы

Этот раздел содержит таблицу активов, связанных с алертом. Информация об активах поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные активы. Активы можно сортировать по столбцам **Количество** и **Актив**.

Связанные активы

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

Всего: 1

При нажатии на название актива открывается окно **Информация об активе**, в котором можно посмотреть владельца актива, состояние защиты (статусы KSC), информацию о ПО, аппаратном обеспечении и уязвимостях (опционально).

DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNetDomain: TRUECOMPANY, DeviceProduct: Windows, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, DeviceVendor: Microsoft

Найти в событиях 1	Main
Найти в событиях 1	Main

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

Связанные пользователи

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

Журнал изменений

Комментарий

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

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

04.03.2025 06:55:22

IP-адрес

10.68.85.92

Владелец

Ivan Ivanov

Полное доменное имя

wd10.truecompany.local

MAC-адрес

08:00:2b:01:02:03

Категория КИИ

Информационный ресурс не является объектом КИИ

Информация об активе



Удалить

Изменить

Переместить в группу KSC

Запустить задачу

Категория КИИ

Информационный ресурс не является объектом КИИ

Расширенный статус KSC

Антивирусные базы обновлялись слишком давно

Идентификатор расширенного статуса KSC

Критический

С помощью кнопки **Скачать активы** вы можете скачать информацию о связанных активах в виде файла в формате CSV (в кодировке UTF-8).

Раздел Связанные пользователи

Этот раздел содержит таблицу пользователей, относящихся к алерту. Информация о пользователях поступает из событий, связанных с алертом. С помощью поля **Поиск пользователей** можно искать нужных пользователей. Пользователей можно сортировать по столбцам **Количество**, **Пользователь**, **User principal name** (Основное имя пользователя) и **Адрес электронной почты**.

Связанные пользователи

Скачать пользователей

Поиск пользователей...

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

Всего: 1

При нажатии на имя пользователя открывается окно **Информация об учетной записи**, в котором можно посмотреть данные учетной записи: в каких группах состоит учетная запись, UAC, контактные данные, местонахождение пользователя и другие атрибуты, которые были импортировать из MS Active Directory.

DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNetDomain: TRUECOMPANY, DeviceProduct: Windows, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, DeviceVendor: Microsoft

Найти в событиях 1

Найти в событиях 1

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

Связанные пользователи

Количество ↓	Пользователь	Имя участника-пользователя (UPN)	Адрес электронной почты	Домен
1	Ivan Ivanov	i.ivanov@truecompany.local	i.ivanov@truecompany.local	truecompany.local

Журнал изменений

Комментарий

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

Информация об учетной записи

Реагирование через Active Directory

Информация об учетной записи

Данные о курсах ASAP

Display name

ivan ivanov

Common Name

ivan ivanov

Distinguished name

cn=ivan ivanov,cn=users,dc=truecompany,dc=local

User logon name

i.ivanov

Имя участника-пользователя (UPN)

i.ivanov@truecompany.local

Member Of

{ cn=hr,cn=users,dc=truecompany,dc=local }

User account control

512

Mail

i.ivanov@truecompany.local

Дополнительная информация

Physical delivery office name

1-2-3

Telephone number

77777

С помощью кнопки **Скачать пользователей** вы можете скачать информацию о связанных пользователях в виде файла в формате CSV (в кодировке UTF-8).

Раздел Журнал изменений

Этот раздел содержит записи об изменениях, которые пользователи внесли в алерт. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии. Комментарии можно сортировать по столбцу **Время**.

Например, назначьте алерт пользователю **Administrator**. Статус алерта изменится с **Новый** на **Назначен**.

Кaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Алерты >

R220_Сбор информации об учетных записях Новый

Уровень важности: Высокий

Назначить: Не назначено

Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции

Низкий

Наивысшая важность категории активов

Критический

Идентификатор алерта

326dff6d-667a-4236-9b1e-4210463b5201

Первое появление

04.03.2025 13:44:38

Последнее появление

04.03.2025 13:44:38

Правило корреляции

[R220_Сбор информации об учетных записях](#)

Мне

Administrator

Уровень важности:



Высокий



Назначить:

Administrator



Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции

Низкий

Первое появление

04.03.2025 13:44:38

Тенант

Main

Наивысшая важность категории активов

Критический

Последнее появление

04.03.2025 13:56:13

Правило корреляции

[R220_Сбор информации об учетных записях](#)

Идентификатор алерта

326dff6d-667a-4236-9b1e-
4210463b5201

Убедитесь, что в разделе **Журнал изменений** появилась запись о назначении алерта пользователю **Administrator**.

Журнал изменений

Комментарий

Добавить

Время ↓	Пользователь	Действие
04.03.2025 14:48:44	Administrator	Назначить: Administrator

Всего: 1

При необходимости в поле **Комментарий** вы можете внести комментарий к алерту и нажать **Добавить**, чтобы сохранить его.

Обработка алертов

Вы можете изменить уровень важности алерта, назначить алерт пользователю, закрыть алерт или создать на основе алерта **инцидент**.

В терминах Лаборатории Касперского **инцидент** — это подтвержденный алерт (другими словами, подтвержденная угроза информационной безопасности). Инцидент может объединять несколько алертов, например, в рамках расследования аналитик обнаружил первичное заражение и боковое перемещение и привязал эти алерты к одному инциденту.

Чтобы обработать алерт:

- Выберите необходимый алерт одним из следующих способов:
 - В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть. Откроется окно алерта, в верхней его части

расположена панель инструментов.



Каперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты >
R220_Сбор информации об учетных записях Новый

Уровень важности: Высокий

Назначить: Не назначено

Закрывать алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции: Низкий

Первое появление: 04.03.2025 13:44:38

Тенант: Main

Наименьшая важность категории активов: Критический

Последнее появление: 04.03.2025 13:44:38

Правило корреляции: [R220_Сбор информации об учетных записях](#)

Идентификатор алерта: 326df6d-667a-4236-9b1e-4210463b5201

Связанные события

Скачать события

Найти в событиях

Время ↓	Информация о событии	Тенант
04.03.2025 13:44:38	Message: Пользователь TRUECOMPANYLOCAL\ivanov на ксте wd10.truecompany.local выполнил команду "whoami" для получения данных об учетных записях. DeviceHostName: wd10.truecompany.local, SourceUserName: ivanov, DestinationHostName: wd10.truecompany.local, DestinationUserName: -, DeviceAssetID: 6c578a24-f43d-412f-9f6e-487a6539f77a, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: wd10.truecompany.local, DeviceNetDomain: TRUECOMPANY, DeviceReceiptTime: 04.03.2025 13:48:04, DeviceTimeZone: +03:00, EventOutcome: Audit Success, SourceAccountID: a65d9a12-a35a-48d9-9930-dce06f608854, SourceNetDomain: TRUECOMPANYLOCAL, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserID: 9-1-9-21-1404947558-1a37455289-1288867512-1129, DestinationAssetID: 6c578a24-f43d-412f-9f6e-487a6539f77a, DestinationNetDomain: -, DestinationProcessName: C:\Windows\System32\whoami.exe, DestinationUserID: 9-1-0-0, DeviceFileType: Security log, DeviceCustomString1: 9-1-16-8192, DeviceCustomStringLabel: Mandatory Label, DeviceCustomString3: 0x1e0, DeviceCustomStringLabel: Process ID, DeviceCustomString4: whoami, DeviceCustomStringLabel: Command Line, DeviceCustomString5: 0x1376, DeviceCustomStringLabel: New Process Id, DeviceCustomString6: 9b1936, DeviceCustomStringLabel: Token Elevation Type, FlexString1: 0x1a83f2, FlexStringLabel: Subject login ID, FlexString2: 0x0	Main

Всего: 1

- В разделе **Алерты** веб-интерфейса KUMA установите флажок рядом с требуемым алертом (можно выбрать более одного алерта). В нижней части окна отобразится панель инструментов.



Каперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты 1

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты

Поиск...

Найдено: 4

Фильтры

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов
☒ R220_Сбор информации об учетных записях	Назначен	Administrator		04.03.2025 13:44:38	04.03.2025 13:56:13	Main/Categorized assets/Критичные активы WIN10
☐ Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории
☐ Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории
☐ KWTS Detection	В инциденте		KWTS Detection	01.08.2024 12:30:58	01.08.2024 12:30:58	Без категории

Выбрано: 1

Уровень важности: Высокий

Назначить: Administrator

Закрывать алерт

Создать инцидент

Привязать

Алерты со статусом **Закрыт** не могут быть выбраны для обработки.

- Измените уровень важности алерта с помощью раскрывающегося списка Уровень важности:
 - Низкий.
 - Средний.

- Высокий.
- Критический.

В нашем примере измените **Уровень важности** с **Высокий** на **Критический**.

Алерты

Поиск... Найдено: 4 Фильтры

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов
☒ R220_Сбор информации об учетных записях	Назначен	Administrator		04.03.2025 13:44:38	04.03.2025 13:56:13	Main/Categorized assets/Критические активы WIN10
☐ Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории
☐ Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории
☐ KWTS Detection	В инциденте		KWTS Detection	01.08.2024 12:30:58	01.08.2024 12:30:58	Без категории

Выбрано: 1 Уровень важности: **Высокий** Назначить: Administrator Закрыть алерт Создать инцидент Привязать

- Алерт можно назначить пользователю для дальнейшего анализа. Ранее в Разделе **Просмотр информации об алерте** мы уже назначили алерт пользователю **Administrator**. Статус алерта в таком случае изменяется на **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.
- Если алерт признан ложным срабатыванием или расследование алерта завершено закройте алерт. Для этого:
 - Нажмите **Закрыть алерт** (это можно сделать в карточке алерта или в таблице алертов, выбрав соответствующий алерт, как на скриншоте выше).
 - В появившемся окне подтверждения укажите причину закрытия алерта:
 - **Отработан**. Это означает, что было проведено расследование алерта и приняты необходимые меры по устранению угрозы безопасности.
 - **Неверные данные**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности.
 - **Неверное правило корреляции**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции.
 - Нажмите **ОК**.



Касперский
Unified Monitoring and
Analysis Platform

Выбрано tenants: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты

Поиск...

Найдено: 4

Фильтры

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов
☒ R220_Сбор информации об учетных записях	Назначен	Administrator		04.03.2025 13:44:38	04.03.2025 13:56:13	Main/Categorized assets/Критичные активы WIN10
☐ Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории
☐ Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории
☐ KWTS Detection				2024 12:30:58	01.08.2024 12:30:58	Без категории

Выбрано: 1 Уровень важности: Критический Назначить: Administrator

Закрывать алерт Создать инцидент Привязать

Вы уверены, что хотите закрыть алерт?

Выберите причину закрытия алерта:

☒ Отработан

☐ Неверные данные

☐ Неверное правило корреляции

Отмена

OK

- Статус алерта будет изменен на **Закрыт**. Алерты с таким статусом не обновляются новыми корреляционными событиями и отображаются в таблице алертов, только если в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого алерта или назначить его другому пользователю невозможно.



Касперский
Unified Monitoring and
Analysis Platform

Выбрано tenants: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты

Поиск...

Найдено: 3

Фильтры

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов
☐ Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Новый			26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории
☐ Неудачная попытка входа в веб-интерфейс KUMA	Назначен			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории
☐ KWTS Detection	В инциденте		KWTS Detection	01.08.2024 12:30:58	01.08.2024 12:30:58	Без категории

Статус

Фильтры:

☒ Новый

☒ Назначен

☐ Закрыт

☒ В инциденте

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты 1

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Инциденты >

Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA

Назначить: Не назначено

Сохранить

Отмена

Описание

Связанные алерты

Связанные активы

Связанные пользователи

Журнал изменений

Интеграция с НКЦКИ

Описание

Создан 05.03.2025 17:28:50

Название* Обнаружено 3 (три) неудачных попы

Тенант* Main

Статус Открыт

Уровень важности* Высокий

Категории затронутых активов Без категории

Появление первого события 26.02.2025 14:34:24

Появление последнего события 26.02.2025 14:34:24

Категория инцидента

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты 1

События

Инциденты

Поиск...

Создать инцидент

Выбрать фильтр

Найдено: 1

Название	Назначен	Создан	Тенант	Статус	Количество алертов	Уровень важности	Тип инцидента
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Administrator	05.03.2025 17:44:02	Main	Назначен	1	Высокий	Неудачные попытки авторизации

Касперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты 1

Инциденты

События

Алерты

Поиск...

Фильтры

Найдено: 2

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категории затронутых активов
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	В инциденте	Administrator	Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	26.02.2025 14:34:24	26.02.2025 14:34:24	Без категории
Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	26.02.2025 14:34:24	Без категории

Подробнее про работу с инцидентами:

<https://support.kaspersky.ru/kuma/4.0/220213>

Уведомления об алертах

При создании и назначении алертов по электронной почте рассылаются стандартные уведомления KUMA. Предварительно необходимо настроить подключение к SMTP-серверу

организации, а также установить флажок **Получать уведомления по почте** в карточке пользователя.

Чтобы настроить подключение к SMTP-серверу:

- Перейдите в раздел **Параметры → Общие**.
- В секции **Параметры подключения к SMTP-серверу** укажите необходимые параметры:
 - **Адрес сервера** – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
 - **Порт** – порт подключения к почтовому серверу.
 - **От кого** – адрес электронной почты отправителя сообщения. Например, kuma-aio@truecompany.local.
 - (Опционально) Если при подключении к почтовому серверу необходимо пройти аутентификацию в поле **Секрет** выберите или создайте секрет типа credentials, в котором будут указаны учетные данные для подключения к SMTP-серверу.
- Нажмите **Сохранить**.

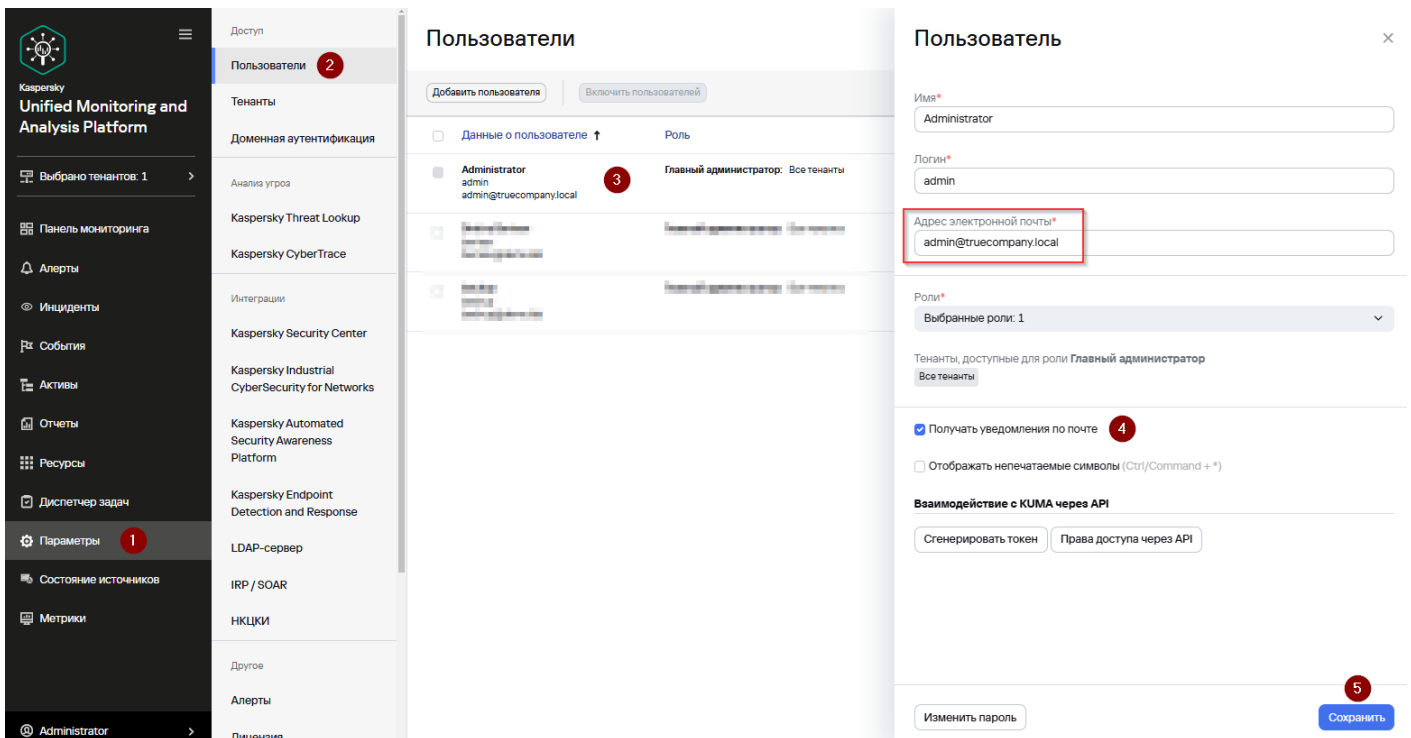
Соединение с SMTP-сервером настроено.

The screenshot displays the Kaspersky EDR management console. On the left, a sidebar menu includes 'События', 'Активы', 'Отчеты', 'Ресурсы', 'Диспетчер задач', 'Параметры' (marked with a red circle 1), 'Состояние источников', and 'Метрики'. The 'Параметры' section is expanded, showing a list of settings: 'LDAP-сервер', 'IRP / SOAR', 'НКЦКИ', 'Другое', 'Алерты', 'Лицензия', 'Инциденты', 'Аудит активов', 'Обновление репозитория', 'Активы', 'Мониторинг сервисов', and 'Общие' (marked with a red circle 2). The main panel is titled 'Параметры подключения к SMTP-серверу'. It contains the following fields and controls: a 'Выключено' toggle switch; 'Адрес сервера*' (marked with a red circle 3); 'Порт*' (marked with a red circle 4) set to 25; 'Секрет' field with a dropdown and a '+' icon; 'Псевдоним сервера Ядра ① KUMA'; 'От кого*' (marked with a red circle 5) set to kuma-aio@truecompany.local; a 'Выключить уведомления мониторинга' toggle switch; 'Регулярность уведомлений мониторинга*' set to 'Не повторять'; and a 'Сохранить' button (marked with a red circle 6).

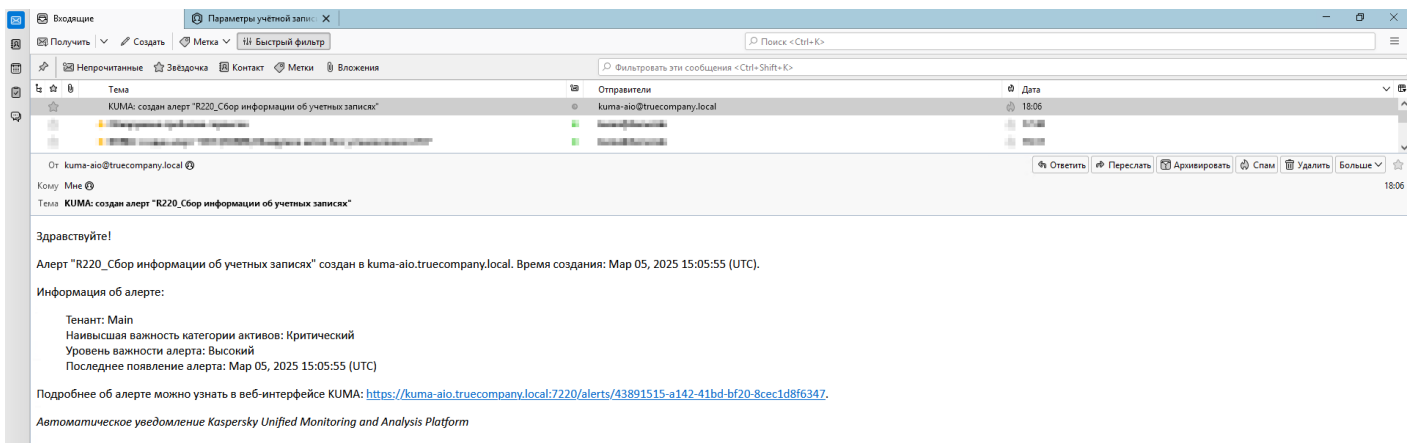
Для того, чтобы пользователи смогли получать сообщения электронной почты от KUMA также необходимо в карточке пользователей установить флажок **Получать уведомления по почте**. Для этого:

- Перейдите в раздел **Параметры → Пользователи**.
- Нажмите на пользователя, для которого необходимо настроить получение уведомлений.

- В появившемся окне справа **Пользователи** установите флажок **Получать уведомления по почте**.
- Нажмите **Сохранить**.



Сгенерируйте тестовый алерт (см. **Раздел Просмотр информации об алерте**). Убедитесь, что на почтовый ящик пользователя пришло почтовое сообщение с уведомлением о созданном алерте.



Вместо стандартных уведомлений KUMA о создании алертов (как на скриншоте выше) можно рассылать уведомления на основании пользовательских шаблонов. Подробнее: <https://support.kaspersky.ru/kuma/4.0/233518>

Также в KUMA поддерживается отправка уведомлений в Telegram: Статья онлайн-справки «Отправка уведомлений в Telegram»: <https://support.kaspersky.ru/kuma/4.0/258846>

Community-скрипт с расширенными возможностями уведомлений и управления через Telegram:

https://github.com/KUMA-Community/kuma_telebot

Revision #4

Created 2026-08-10 13:48:47 UTC by Dmitry Borisov

Updated 2026-08-11 14:19:02 UTC by Dmitry Borisov