

# Скоринг активов

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:

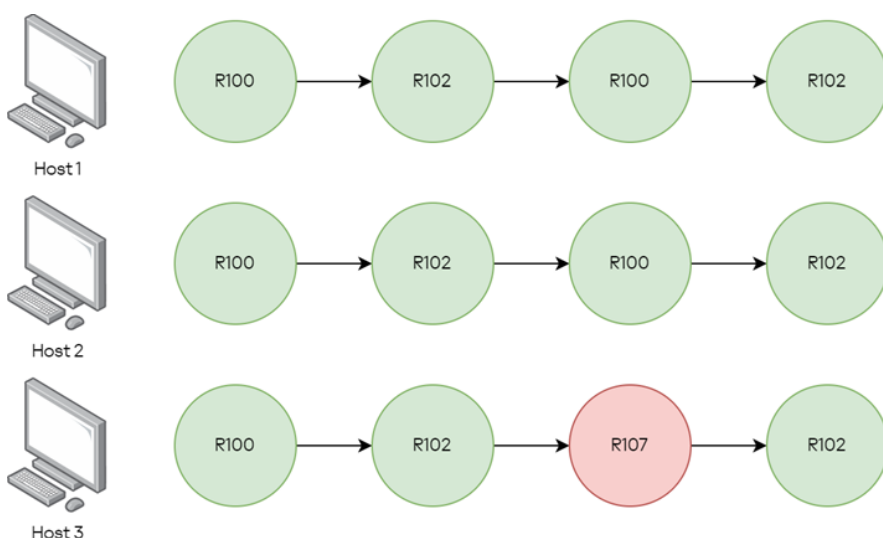
<https://support.kaspersky.ru/kuma/4.0/292782>

## Описание

**Скоринг активов** – это локальный сервис на базе машинного обучения, который обучается на сработавших правилах корреляции, анализирует типичные цепочки срабатываний в инфраструктуре и отслеживает отклонения.

Если на активе происходит нетипичная для инфраструктуры последовательность срабатываний, его рейтинг и статус повышаются, что перемещает его в более критичную категорию активов.

Таким образом, сервис помогает приоритезировать уже создаваемые алерты за счет анализа поведения хостов, вокруг которых эти алерты происходят. Кроме того, аналитик можно самостоятельно выбрать активы с высоким статусом аномальной активности и проанализировать события для поиска потенциальных угроз.



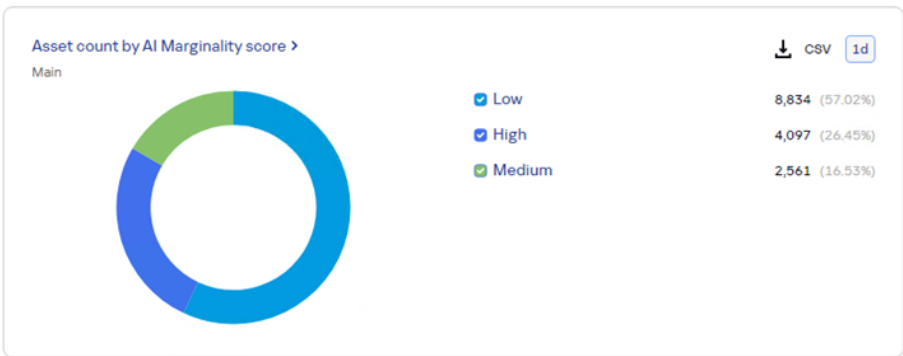
Сервис **Скоринг активов** получает из доступных кластеров хранения корреляционные

события, содержащие непустое поле Affected assets, выстраивает ожидаемую последовательность событий и обучает модель AI. На основании цепочки срабатываний корреляционных правил AI-сервис высчитывает, является ли такая последовательность срабатываний характерной в этой инфраструктуре. Нехарактерные паттерны повышают рейтинг актива.

По результатам расчетов сервиса **Скоринг активов** в карточке активов становится доступным для просмотра поле **AI-рейтинг** и **AI-Статус**. Рейтинг – это число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля **AI-Статус**: Low, Medium, High, Critical.

Dashboard

Updated 2024-11-30 18:06



После каждого перезапуска сервиса **Скоринг активов**, сервис заново обучает модель и выполняет переоценку рейтинга активов, указанных в событиях за сегодня. Активы со скорингом выглядят следующим образом:

И

+ Добавить условие

+ Добавить группу

Свернуть

Рейтинг AI > 0.25

| <input type="checkbox"/> | Название              | Полное доменное имя   | IP-адрес    | MAC-адрес         | Статус  | Рейтинг AI ↑       |
|--------------------------|-----------------------|-----------------------|-------------|-------------------|---------|--------------------|
| <input type="checkbox"/> | KESW                  | kesw.sales.lab        | 10.10.10.10 | 00:50:56:89:99:45 | Средний | 0.3333333333333333 |
| <input type="checkbox"/> | ksodk                 | ksodk                 | 10.10.10.10 |                   | Средний | 0.3636363636363636 |
| <input type="checkbox"/> | fd3c5a1db02c          | fd3c5a1db02c          |             |                   | Средний | 0.4                |
| <input type="checkbox"/> | dc-01.sales.lab       | dc-01.sales.lab       |             |                   | Средний | 0.4285714285714286 |
| <input type="checkbox"/> | xdr-ksc.demo.lab      | xdr-ksc.demo.lab      |             |                   | Средний | 0.4285714285714286 |
| <input type="checkbox"/> | wec.truecompany.local | wec.truecompany.local | 10.10.10.10 |                   | Высокий | 0.5714285714285714 |
| <input type="checkbox"/> | wec                   | wec                   | 10.10.10.10 |                   | Высокий | 0.5714285714285714 |

В директории, указанной в конфигурационном файле, хранятся события, которые сервиса **Скоринг активов** получил из кластеров хранения KUMA за указанное количество дней. Например, если в конфигурационном файле указано 12 дней (period\_for\_train\_days), сервис будет получать события за последние 12 дней. Самые давние события удаляются из

директории. В этой же директории будет храниться обученная модель.

Переобучение модели происходит в полночь по UTC. Переоценка рейтинга активов происходит раз в час для всех активов, которые были в событиях за сегодня по UTC.

Если лицензию удалить, поля **AI-рейтинг** и **AI-Статус** будут скрыты из карточки актива. Если лицензию снова добавить, значения полей **AI-рейтинг** и **AI-Статус** снова будут отображаться.

Журналы сервиса хранятся в `/var/log/syslog`.

---

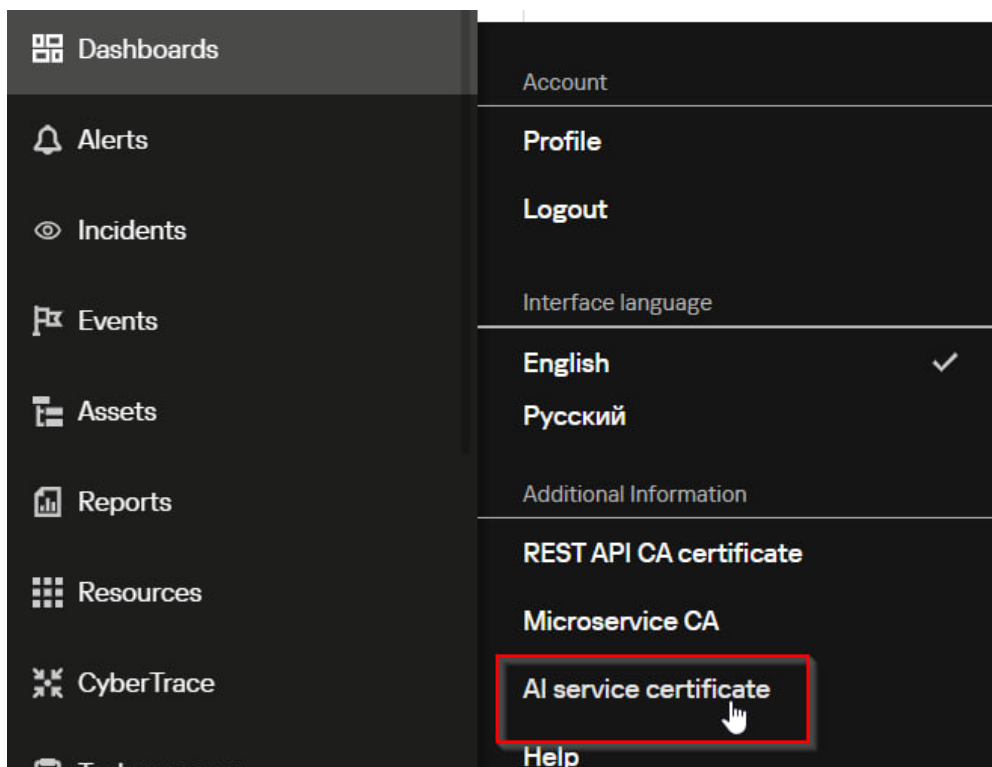
## Требуемые аппаратные ресурсы

4 vCPU, 12 GB RAM, 100 GB HDD

---

## Шаги по установке

- Скачайте архив: [ссылка](#). Архив содержит скрипты для установки и удаления сервиса, а также конфигурационный файл `config.yaml`.
- В конфигурационном файле `config.yaml` укажите порт, по которому сервис Ядра будет ожидать подключения от сервиса Скоринг активов. Например, в установке в отказоустойчивой конфигурации должен быть указан порт 7226. Для остальных параметров можно оставить значения по умолчанию.
- В веб-интерфейсе KUMA скачайте **AI service certificate** (в меню пользователя) и поместите его в `roles/mlservice/files`.



- Перейдите в директорию с файлами сервиса и из этой папки выполните команду:  
`bash ./install <путь к ИНВЕНТОРИ.yaml>`
- По умолчанию сервис устанавливается на хост с Ядром. Если вы хотите установить сервис на другой хост, укажите в конфигурационном файле `<hostname>:<port>` ядра KUMA в `kuma_address` и убедитесь в наличии сетевого доступа.
- Установщик генерирует необходимые сертификат и ключ в процессе установки и помещает их в директорию, указанные в конфигурационном файле, по умолчанию: `/opt/kaspersky/mlservice/`. Сертификат необходимо загрузить в KUMA. В веб-интерфейсе KUMA в разделе (появляется при наличии лицензии AI) **Параметры - Интеграции → AI-сервис** во вкладке **AI рейтинг и статус активов** заполните следующие поля:
  - В поле **URL** укажите **адрес и номер порта**, по которому Ядро будет ожидать подключения от AI-сервиса. Например, **:7226** (означает поднять порт на ядре 0.0.0.0:7226). Номер порта должен соответствовать указанному в конфигурационном файле.
  - В поле **Сертификат** в раскрывающемся списке выберите Создать и в открывшемся окне Создание сертификата укажите тип сертификата Certificate и загрузите сертификат из директории, указанной в конфигурационном файле, по умолчанию `/opt/kaspersky/mlservice/service.crt`.

Kaspersky Threat Lookup

Kaspersky CyberTrace

Kaspersky Security Center

KICS/KATA

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

IRP / SOAR

AI-сервисы

## AI-сервисы

AI-оценка и AI-статус активовKaspersky Investigation & Response AssistantОбнаружение атак DLL Hijacking

Состояние

☒

URL\*

:7226

Сертификат\*

ml\_service

Сразу после установки сервис будет пытаться в течение 15 минут подключиться к KUMA с интервалом в 1 минуту. Если сертификат не добавлен в веб-интерфейсе KUMA, подключение не будет выполнено и сервис остановится. В таком случае можно добавить сертификат и перезапустить сервис (`systemctl restart ml.service`), сервис Скоринг активов опять попытается подключиться к Ядру KUMA.

Сервис Скоринг активов установлен.

Для проверки, что Скоринг активов успешно запущен выполните команду `systemctl status ml.service` и проверьте наличие строки старта обучения модели (msg: "training started").

```
Jul 27 19:56:46 kuma.demo.lab ml.service.service[4081891]: {"level":"info","ts":"2026-07-27T19:56:46.146+0300","msg":"tracing exporter is disabled","service_name":"kuma ml"}
Jul 27 19:56:46 kuma.demo.lab ml.service.service[4081891]: {"level":"info","ts":"2026-07-27T19:56:46.146+0300","msg":"run service","service_name":"kuma ml","version":"0.1.54.28"}
Jul 27 19:57:46 kuma.demo.lab ml.service.service[4081891]: {"level":"info","ts":"2026-07-27T19:57:46.235+0300","logger":"app.(*Service).Start","msg":"training started","service_name":"kuma ml"}
```

## Use Case 1. Приоритизация алертов

В KUMA можно настроить проактивную категоризацию активов на основании значений полей «AI-рейтинг» и «AI-статус». Как только ИИ-сервис «Скоринг активов» присвоит активу рейтинг и статус, актив будет перемещен в категорию, соответствующую данному уровню нетипичной активности.

Уровень важности категории актива влияет на уровень важности алерта, с которым связан этот актив. Таким образом, итоговый уровень важности алерта будет выше, если на активе фиксируется аномально высокий уровень нетипичной активности и актив помещен в соответствующую категорию.

По умолчанию уровень важности алерта определяется сработавшим правилом корреляции.

Благодаря скорингу активов выполняется автоматическая приоритизация: алерты, связанные с активами с повышенным уровнем нетипичной активности, получают более высокий уровень важности и должны обрабатываться аналитиками в приоритетном

порядке. Помимо этого аналитики получают дополнительный контекст при расследовании алерта/инцидента, принимая во внимание текущий уровень нетипичной активности на активе.

Чтобы настроить проактивную категоризацию:

- Перейдите в раздел **Активы** веб-интерфейса KUMA.
- Выберите категорию **Main/Categorized assets** и нажмите **Добавить подкатегорию**.
- В окне **Добавить категорию** укажите:
  - В поле **Название** введите название категории - **AI-Статус**.
  - В поле **Родительская категория** укажите место категории в дереве категорий - **Categorized assets**.
  - В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию.
  - В раскрывающемся списке **Способ категоризации** выберите **Вручную**.
  - Назначьте уровень важности категории в раскрывающемся списке **Уровень важности** выберите **Низкий**.
- Нажмите **Сохранить**.

## Добавить категорию



|                         |                             |
|-------------------------|-----------------------------|
| Название*               | AI-Статус <b>1</b>          |
| Родительская категория* | Categorized assets <b>2</b> |
| Тенант*                 | Main                        |
| Способ категоризации*   | Вручную <b>3</b>            |
| Уровень важности        | Низкий <b>4</b>             |
| Описание                |                             |

Сохранить

Отмена

- Далее выберите созданную категорию выберите категорию **AI-Статус** и нажмите **Добавить подкатеорию**.
- Создайте подкатеорию Critical с параметрами, как на скриншоте ниже.

## Изменить категорию



|                             |                                                               |
|-----------------------------|---------------------------------------------------------------|
| Название*                   | <input type="text" value="Critical"/>                         |
| Родительская категория*     | <input type="text" value="AI-Статус"/>                        |
| Тенант*                     | <input type="text" value="Main"/>                             |
| Способ категоризации*       | <input type="text" value="Активно"/>                          |
| Уровень важности            | <input type="text" value="Критический"/>                      |
| Описание                    | <div>Активы с критическим уровнем нетипичной активности</div> |
| Регулярность категоризации* | <input type="text" value="1ч"/>                               |

### Условия

Если

AI-статус

=

Критический

x

Проверить условия

Сохранить

Отмена

- Повторите операцию для подкатегорий High, Medium и Low.

# Изменить категорию



Название\*

High

Родительская категория\*

AI-Статус

Тенант\*

Main

Способ категоризации\*

Активно

Уровень важности

Высокий

Описание

Активы с высоким уровнем нетипичной активности

Регулярность категоризации\*

1ч

## Условия

И

+ Добавить условие

+ Добавить группу

Если

AI-статус

=

Высокий

x

Проверить условия

Сохранить    Отмена

# Изменить категорию



Название\*

Medium

Родительская категория\*

AI-Статус

Тенант\*

Main

Способ категоризации\*

Активно

Уровень важности

Средний

Описание

Активы со средним уровнем нетипичной активности

Регулярность категоризации\*

1ч

Условия

И

+ Добавить условие

+ Добавить группу

Если

AI-статус

=

Средний

x

Проверить условия

## Изменить категорию



|                             |                                                          |
|-----------------------------|----------------------------------------------------------|
| Название*                   | <input type="text" value="Low"/>                         |
| Родительская категория*     | <input type="text" value="AI-Статус"/>                   |
| Тенант*                     | <input type="text" value="Main"/>                        |
| Способ категоризации*       | <input type="text" value="Активно"/>                     |
| Уровень важности            | <input type="text" value="Низкий"/>                      |
| Описание                    | <div>Активы с низким уровнем нетипичной активности</div> |
| Регулярность категоризации* | <input type="text" value="1ч"/>                          |

### Условия

Если

AI-статус

=

Низкий

×

Проверить условия

Сохранить

Отмена

- После создания категорий убедитесь, что в них присутствуют активы с соответствующим AI-статусом.

Kaspersky  
Unified Monitoring and  
Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События

Активы 1

Отчеты

Активы

Все активы

Все тенанты

Поиск...

Все тенанты

Main

Categorized assets

AI-Статус

Critical 2

High

Low

Medium

Address space

pc

+ Добавить актив

Удалить

Привязать к категории

Экспортировать CSV

Импортировать активы KSC

Импортировать атрибуты активов KSC

Переместить в группу KSC

| Название | Полное доменное имя | IP-адрес | Источник актива                           | MAC-адрес         | AI-статус   | AI-рейтинг | Последн   |
|----------|---------------------|----------|-------------------------------------------|-------------------|-------------|------------|-----------|
| PC-5     | pc-5.demo.lab       |          | KICS/KATA, Kaspersky Security Center, ... | 00:50:56:A8:9D:8C | Критический | 0.85       | 28.07.202 |

Всего 1 / Выбрано 0

Пример алерта без использования скоринга активов и активной категоризации

- [illegible]

- Итоговый уровень важности алерта **Высокий**, так как с алертом связан актив **РС-5**, на котором зафиксирован критический уровень нетипичной активности и который автоматически определен в категорию **AI-Статус/Critical**

The screenshot shows the 'Alerts' (Алерты) section of the 'Unified Monitoring and Analysis Platform'. The interface includes a sidebar with navigation options like 'Dashboard', 'Alerts', 'Incidents', and 'Events'. The main area displays a table of alerts. The table columns are: Name, Status, Assignee, Incident, First Occurrence, Last Occurrence, Category of affected assets, and Tenant. Two alerts are listed, both with a status of 'New' (Новый). The first alert is highlighted with a red box around the name and a red circle with the number 2. The second alert is also highlighted with a red box around the name and a red circle with the number 2. The category of affected assets for both alerts is 'Main/Categorized assets/All-Category/Critical'.

| Название                                                                   | Статус | Назначен | Инцидент | Первое появление    | Последнее появление | Категории затронутых активов                  | Тенант |
|----------------------------------------------------------------------------|--------|----------|----------|---------------------|---------------------|-----------------------------------------------|--------|
| R220_02_Сбор информации об учетных записях стандартными средствами Windows | Новый  |          |          | 28.07.2026 13:01:44 | 28.07.2026 13:01:44 | Main/Categorized assets/All-Category/Critical | Main   |
| R220_02_Сбор информации об учетных записях                                 | Новый  |          |          | 28.07.2026 13:01:44 | 28.07.2026 13:01:44 | Main/Categorized assets/All-Category/Critical | Main   |

- При этом сработавшее правило корреляции с уровнем важности **Средний**, но за счет критического уровня важности категории актива алерт получил более высокий приоритет.



Для настройки аудита активов:

- Перейдите в **Параметры → Другое → Активы** → вкладка **Аудит активов**.
- Нажмите **Добавить параметры для нового тенанта**.
- Выполните настройку параметров аудита активов, как на скриншоте ниже.

Аудит активов

Сбор событий аудита

Тенант\*

Main

Действия, в результате которых создаются события аудита активов

Актив добавлен в KUMA

Параметры актива изменены

Актив удален из KUMA

Актив добавлен в категорию

Актив удален из категории

Сведения об уязвимости добавлены в акт...

Уязвимость актива закрыта

Актив добавлен в категорию

+ Добавить

Привязать

Удалить

| <input type="checkbox"/> | Название          | Тип        | URL                |
|--------------------------|-------------------|------------|--------------------|
| <input type="checkbox"/> | [OOTB] Correlator | correlator | kuma.demo.lab:7231 |
| <input type="checkbox"/> | [OOTB] Storage    | storage    | kuma.demo.lab:7230 |

Актив удален из категории

+ Добавить

Привязать

Удалить

| <input type="checkbox"/> | Название          | Тип        | URL                |
|--------------------------|-------------------|------------|--------------------|
| <input type="checkbox"/> | [OOTB] Correlator | correlator | kuma.demo.lab:7231 |
| <input type="checkbox"/> | [OOTB] Storage    | storage    | kuma.demo.lab:7230 |

Сохранить

Отмена

Теперь при изменении категории актива, например, при переходе из категории High в Critical будет создано событие аудита активов.

Каперский

Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События 1

Активы

Отчеты

Ресурсы

СубетТраце

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Войти

События

SELECT FROM `events` WHERE DeviceCustomString1 ilike 'Main/Categorized assets/%' AND DeviceAction = 'asset added to category' AND EventOutcome = 'succeeded'

Нажмите Ctrl + Enter, чтобы выполнить запрос

Результаты запроса

TSV

| TenantID | Timestamp              | Name             | DeviceProduct | DeviceVendor |
|----------|------------------------|------------------|---------------|--------------|
| Main     | 28.07.2026 13:29:27164 | XDR-KSC          | KUMA          | Kaspersky    |
| Main     | 28.07.2026 13:29:27164 | XDR-DC           | KUMA          | Kaspersky    |
| Main     | 28.07.2026 13:29:27164 | XDR-DC           | KUMA          | Kaspersky    |
| Main     | 28.07.2026 13:29:27164 | PC-5             | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | Device 8747      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | Device 8749      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 |                  | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | Device 8750      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | Device 8748      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | pc-7demo lab     | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:38:00542 | WIN10ENT_NEW (3) | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:25:46085 | KUMA AIO         | KUMA          | Kaspersky    |
| Main     | 28.07.2026 12:25:46085 | DC-01            | KUMA          | Kaspersky    |
| Main     | 28.07.2026 11:53:57378 | Device 8747      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 11:53:57378 | Device 8746      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 11:53:57378 | Device 8739      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 11:53:57378 | Device 8744      | KUMA          | Kaspersky    |
| Main     | 28.07.2026 11:53:57375 | PC-7             | KUMA          | Kaspersky    |

Информация о событии

Копировать

Проанализировать с KIRA

Общий

Анализ KIRA

TenantID

Main

SpaceID

KUMA Default

Timestamp

28.07.2026 13:29:27164

Name

PC-5

EndTime

28.07.2026 13:29:27164

DeviceAction

asset added to category

DeviceAddress

DeviceAssetID

PC-5

DeviceEventCategory

Audit assets

DeviceHostName

pc-5.demo.lab

DeviceProduct

KUMA

DeviceTimeZone

+03:00

DeviceVendor

Kaspersky

SourceHostName

DeviceCustomString1

Main/Categorized assets/AI-Craney/Critical

DeviceCustomString1Label

category

DeviceCustomString2

active

DeviceCustomString2Label

categorization type

DeviceCustomString4

DeviceCustomString4Label

addresses

DeviceCustomString5

pc-5.demo.lab

DeviceCustomString5Label

fqdns

EventOutcome

succeeded

Priority

Низкий

Перемещение активов между категориями можно визуализировать с помощью виджетов. Для этого:

- Перейдите в **Панель мониторинга** и нажмите **Создать панель мониторинга**.
- Нажмите **Добавить параметры для нового тенанта**.
- В окне **Настройки макета** укажите параметры, как на скриншоте ниже, и нажмите **Применить**.

## Настройки макета



Название панели мониторинга\*

[AI] Скоринг активов

Тенант панели мониторинга\*

Main

Собирать данные из тенантов\*

Main

Временной интервал

7д now-7d

Интервал обновления

1 час

Теги

Описание

## Переменные

Вы можете использовать переменные для переопределения данных на виджетах или всей панели мониторинга по определенному значению или условию [Подробнее](#)

[Глобальные переменные](#)

[Локальные переменные](#)

+ Добавить

Удалить



Переменная

Используется в виджетах

Применить

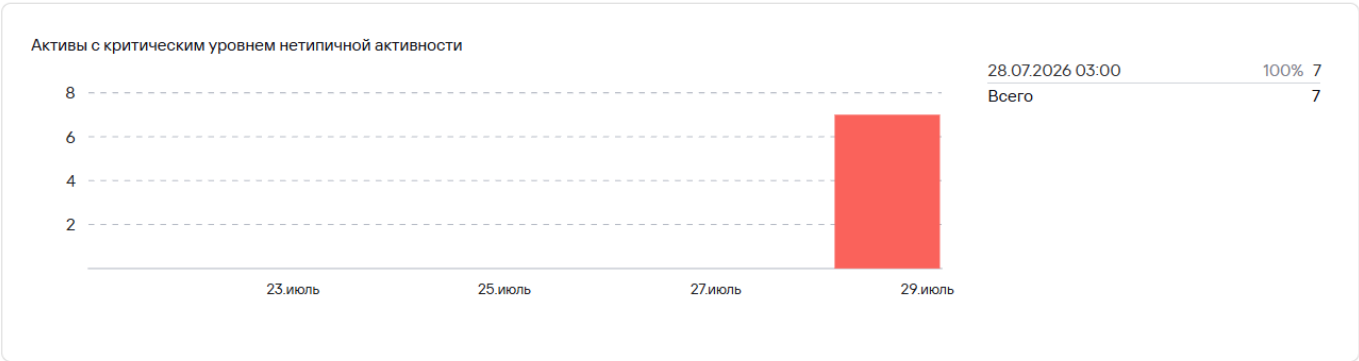
Отмена

- На новой панели мониторинга добавьте следующие виджеты:
  - "Коробочный" виджет **Активы по уровню AI важности** (**Добавить виджет → Активы → Активы по уровню AI важности**)
  - Виджеты (**Добавить виджет → События**) на основе событий:
    - **Активы с критическим уровнем нетипичной активности**

Редактирование виджета



Общие Действия Оси Внешний вид



Обновить предпросмотр

Название\*Активы с критическим уровнем нетипичной активности

ГрафикКалендарная диаграмма

Вид временной диаграммыСтолбчатая диаграмма

ТенантКак на макете

ПериодКак на макете

Показывать данные за предыдущий период ⓘ☐

Доступные переменные >

События

Хранилище\*KUMA Default(Stor...

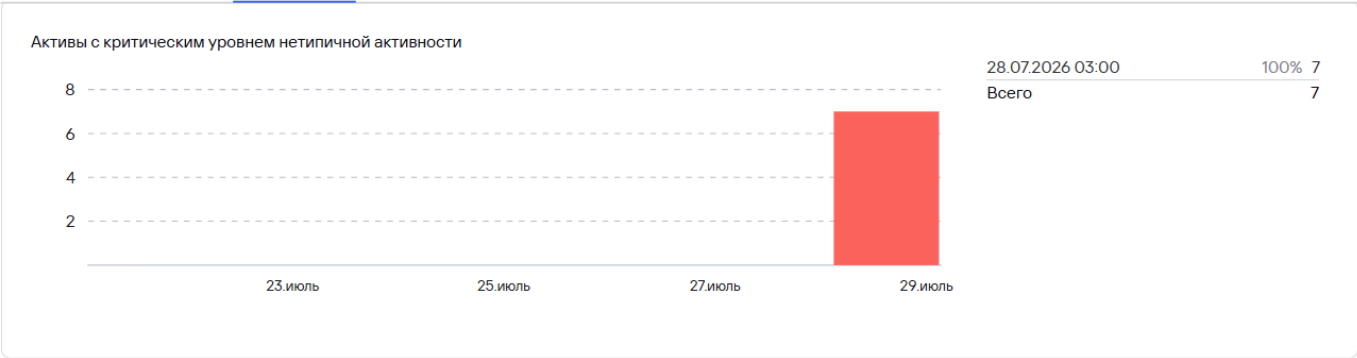
SQL-запрос

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp),
'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Cratic/Critical' AND DeviceAction =
'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit
assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

# Редактирование виджета



Общие Действия Оси Внешний вид



Обновить предпросмотр

Описание

Легенда ☒

Пустые значения в легенде ☐

Итоговые значения ☒

Отображать проценты в легенде ☒

Горизонтальный ☐

Цвет Градиент

Цвет

красный

Длительность отрезков периода

24 часа

Регрессия

не выбрано

Линейная

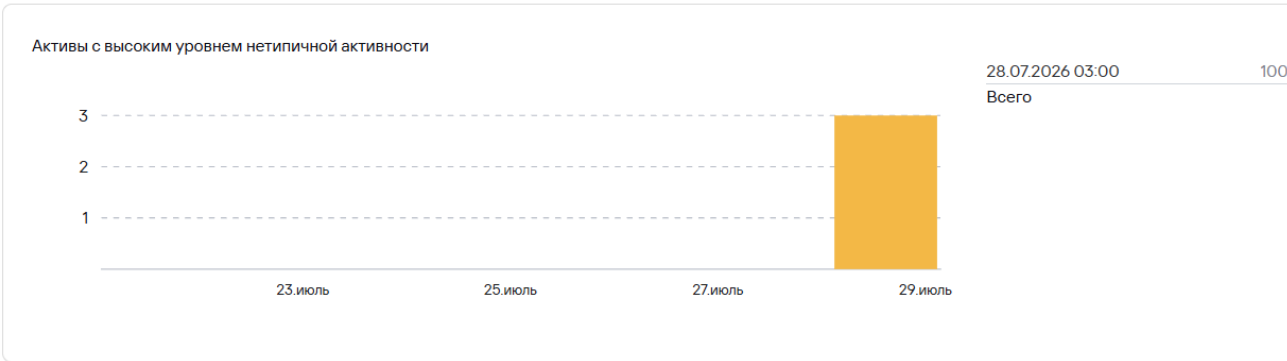
LOESS

Сохранить Отмена

- Активы с высоким уровнем нетипичной активности

# Редактирование виджета

Общие Действия Оси Внешний вид



Обновить предпросмотр

Название\*

Активы с высоким уровнем нетипичной активности

График

Календарная диаграмма

Вид временной диаграммы

Столбчатая диаграмма

Тенант

Как на макете

Период

Как на макете

Показывать данные за предыдущий период ⓘ

☐

Доступные переменные >

События

Хранилище\*

KUMA Default(Stor...

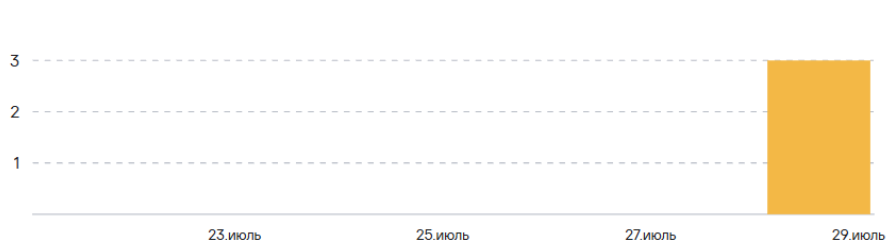
SQL-запрос:

```
SELECT count(ID) AS `metric`,
formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Cratic/High' AND DeviceAction
= 'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory =
'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

# Редактирование виджета

Общие Действия Оси Внешний вид

Активы с высоким уровнем нетипичной активности



28.07.2026 03:00 100% 3  
Всего 3

Обновить предпросмотр

Описание

Легенда ☒

Пустые значения в легенде ☐

Итоговые значения ☒

Отображать проценты в легенде ☒

Горизонтальный ☐

Цвет Градиент

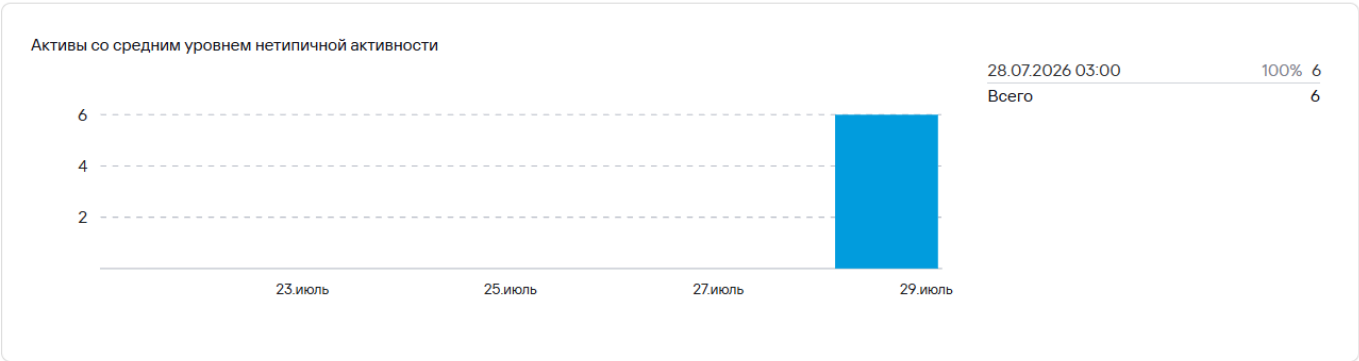
Цвет желтый

Длительность отрезков периода 24 часа

Регрессия не выбрано Линейная LOESS

Сохранить Отмена

Активы с средним уровнем нетипичной активности



Обновить предпросмотр

Название\*

Активы со средним уровнем нетипичной активности

График

Календарная диаграмма

Вид временной диаграммы

Столбчатая диаграмма

Тенант

Как на макете

Период

Как на макете

Показывать данные за предыдущий период ⓘ

☐

Доступные переменные >

События

Хранилище\*

KUMA Default(Stor...

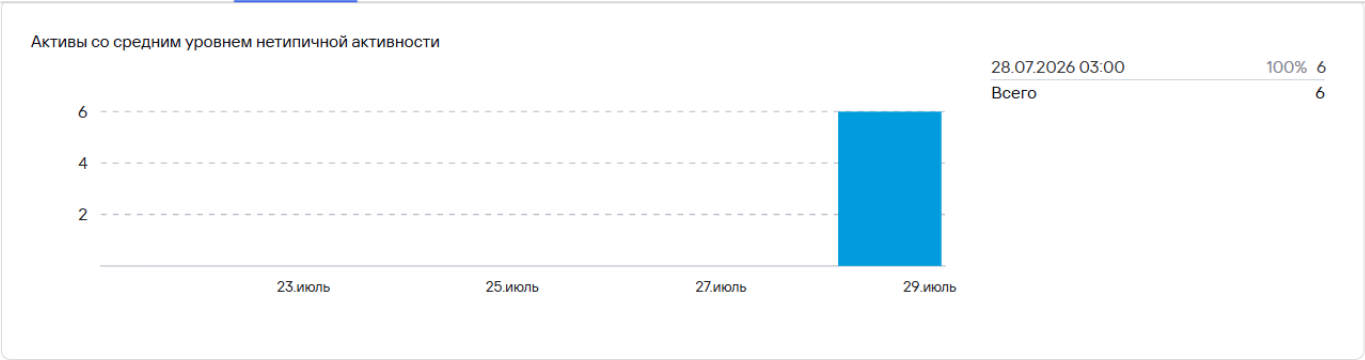
SQL-запрос:

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp),
'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Cratic/Medium' AND DeviceAction =
'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit
assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

# Редактирование виджета



Общие Действия Оси Внешний вид



Обновить предпросмотр

Описание

Легенда ☒

Пустые значения в легенде ☐

Итоговые значения ☒

Отображать проценты в легенде ☒

Горизонтальный ☐

Цвет Градиент

Цвет

синий

Длительность отрезков периода

24 часа

Регрессия

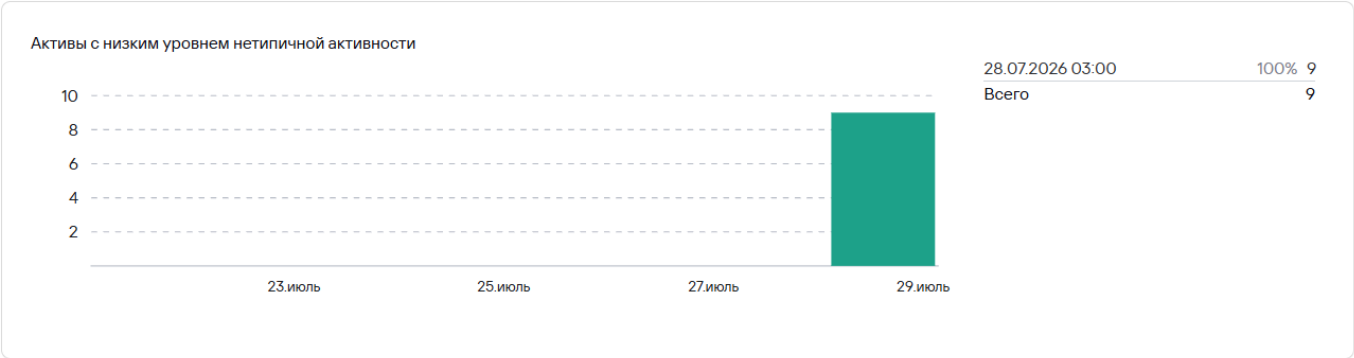
не выбрано

Линейная

LOESS

Сохранить Отмена

Активы с низким уровнем нетипичной активности



Обновить предпросмотр

Название\*Активы с низким уровнем нетипичной активности

ГрафикКалендарная диаграмма

Вид временной диаграммыСтолбчатая диаграмма

ТенантКак на макете

ПериодКак на макете

Показывать данные за предыдущий период ⓘ☐

Доступные переменные >

События

Хранилище\*KUMA Default(Stor...

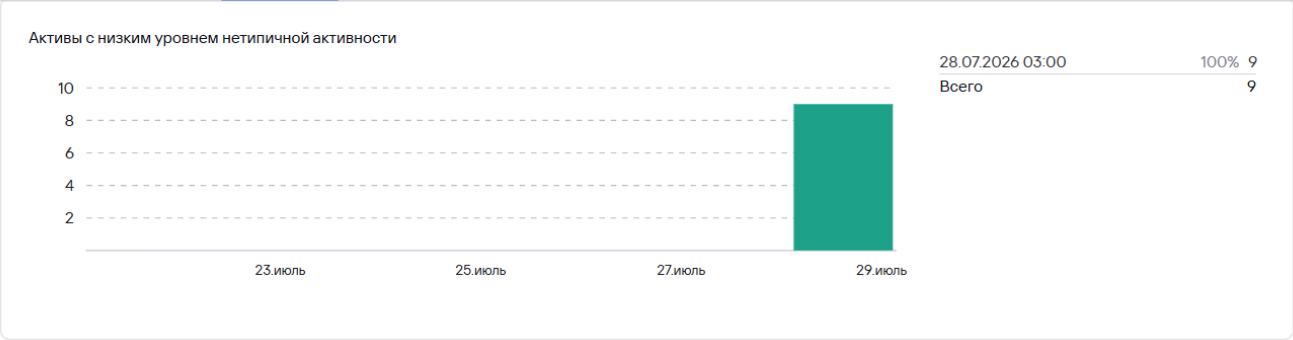
SQL-запрос:

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp),
'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Cratic/Low' AND DeviceAction = 'asset
added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

Редактирование виджета



Общие Действия Оси Внешний вид



Обновить предпросмотр

Описание

Легенда



Пустые значения в легенде



Итоговые значения



Отображать проценты в легенде



Горизонтальный



Цвет Градиент

Цвет

зеленый

Длительность отрезков периода

24 часа

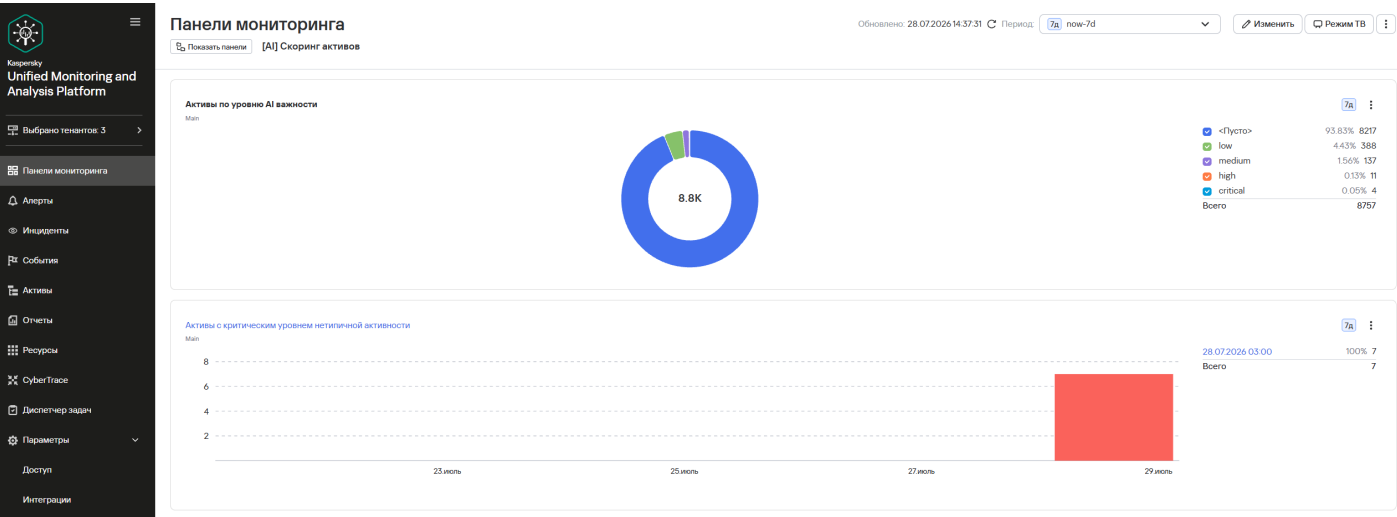
Регрессия

не выбрано Линейная LOESS

Сохранить

Отмена

Виджеты для мониторинга перемещений активов между категориями настроены. При нажатии на дату в легенде виджета будет выполнен переход в раздел **События** для просмотра событий аудита активов и определения какие активы были перемещены в категорию.



Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События

События

Не обновлять28.07.2026 03:00:00 - 29.07...KUMA DefaultStorage

1 SELECT \* FROM `events` WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Статус/Critical' AND DeviceAction = 'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit assets' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TSV

| TenantID | Timestamp              | Name    | DeviceAction            | DeviceCustomString1                        | EventOutcome |
|----------|------------------------|---------|-------------------------|--------------------------------------------|--------------|
| Main     | 28.07.2026 13:29:27164 | XDR-KSC | asset added to category | Main/Categorized assets/AI-Статус/Critical | succeeded    |
| Main     | 28.07.2026 13:29:27164 | XDR-DC  | asset added to category | Main/Categorized assets/AI-Статус/Critical | succeeded    |
| Main     | 28.07.2026 13:29:27164 | PC-5    | asset added to category | Main/Categorized assets/AI-Статус/Critical | succeeded    |

Дополнительно можно настроить аналогичный шаблон отчета и правила корреляции для создания алертов в случае перемещения активов в заданную категорию, например, в категорию Critical.

# Use Case 3. Проактивный поиск угроз

Для активов с критическим или высоким уровнем нетипичной активности аналитик может вручную исследовать алерты и события с этих активов в поисках признаков вредоносной активности и проработки гипотез.

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

Активы 1

Отчеты

Ресурсы

CyberTrace

Активы

Все активы

Все тенанты

Поиск...

Все тенанты

Main

Categorized assets

AI-Статус

Critical 2

High

Low

Medium

Address space

Application

Assets from KSC

Assets from NDR

Поиск...

+ Добавить активУдалитьПривязать к категорииЭкспортировать CSVИмпортировать активы KSCИмпортировать атрибуты активов KSCПереместить в группу KSC

| Название | Полное доменное имя     | IP-адрес | Источник актива                         | MAC-адрес         | AI-статус   | AI-рейтинг         | Последне  |
|----------|-------------------------|----------|-----------------------------------------|-------------------|-------------|--------------------|-----------|
| XDR-DC   | xdr-dc, xdr-dc.demo.lab |          | KICS/KATA, Kaspersky Security Center    | 00:50:56:A8:73:7C | Критический | 0.8809523809523809 | 28.07.202 |
| XDR-KSC  | xdr-ksc.demo.lab        |          | Kaspersky Security Center               | 00:50:56:A8:EAE6  | Критический | 0.8095238095238095 | 28.07.202 |
| PC-5     | pc-5.demo.lab           |          | KICS/KATA, Kaspersky Security Center... | 00:50:56:A8:9D:8C | Критический | 0.8809523809523809 | 28.07.202 |

Всего 3 / Выбрано 0

# Информация об активе



|                                              |                     |
|----------------------------------------------|---------------------|
| Статус антивирусной защиты почтовых серверов | Неизвестно          |
| Статус защиты данных от утечек               | Неизвестно          |
| Статус Endpoint Sensor                       | Неизвестно          |
| Последнее обновление информации              | 28.07.2026 12:26:07 |
| Последнее обновление защиты                  | 26.01.2026 08:57:54 |
| Время начала последней сессии                | 26.01.2026 10:54:26 |

Настраиваемые поля >

Категории >

Уязвимости Kaspersky Security Center >

Информация о программном обеспечении >

Информация об оборудовании >

Оборудование KICS/KATA >

Связанные алерты ⓘ

Найти связанные алерты ▾

Критический: 2  
Новый: 2

Высокий: 8  
Новый: 3, Закрыт: 5

Средний: 1  
Новый: 1

1

Найти в алертах

Отмена

Удалить

При нажатии на **Найти в алертах** будет выполнен переход в раздел **Алерты** и автоматически применен фильтр по активу для отображения только тех алертов, в которых фигурирует выбранный актив.

Касперский  
Unified Monitoring and  
Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты 1

Инциденты

События

Активы

Отчеты

Ресурсы

СубетПаве

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Алерты

2 PC-5

Поиск...

Найдено: 11

Фильтры

| <input type="checkbox"/>            | Название                                                                   | Статус            | Назначен | Инцидент | Первое появление    | Последнее появление | Категории затронутых активов                                                                                                                                                                                                       | Тенант |  |
|-------------------------------------|----------------------------------------------------------------------------|-------------------|----------|----------|---------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--|
| <input type="checkbox"/>            | R424_Подозрительные параметры входа в систему                              | Новый             |          |          | 20.07.2026 14:02:33 | 28.07.2026 14:44:01 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Server<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC        | Main   |  |
| <input type="checkbox"/>            | R424_01_Новая сессия пользователя с назначением подозрительных привилегий  | Новый             |          |          | 15.07.2026 06:02:29 | 28.07.2026 14:44:01 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Server<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC        | Main   |  |
| <input type="checkbox"/>            | R001_Учетная запись была добавлена в группу подозрительным пользователем   | Новый             |          |          | 19.07.2026 00:46:27 | 28.07.2026 14:14:30 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Server<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC        | Main   |  |
| <input checked="" type="checkbox"/> | R220_Сбор информации об учетных записях                                    | Закрыт, обработан |          |          | 28.07.2026 13:16:29 | 28.07.2026 13:16:29 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC<br>Main/Categorized assets/Address space/IO 0.0.0/8 | Main   |  |
| <input type="checkbox"/>            | R220_02_Сбор информации об учетных записях стандартными средствами Windows | Новый             |          |          | 28.07.2026 13:16:29 | 28.07.2026 13:16:29 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC<br>Main/Categorized assets/Address space/IO 0.0.0/8 | Main   |  |
| <input checked="" type="checkbox"/> | R220_Сбор информации об учетных записях                                    | Закрыт, обработан |          |          | 28.07.2026 13:01:44 | 28.07.2026 13:01:44 | Main/Categorized assets/AI-Cranyy/Critical<br>Main/Categorized assets/OS/Windows Desktop<br>Main/Categorized assets/Vulnerabilities<br>Main/Categorized assets/Assets from KSC                                                     | Main   |  |