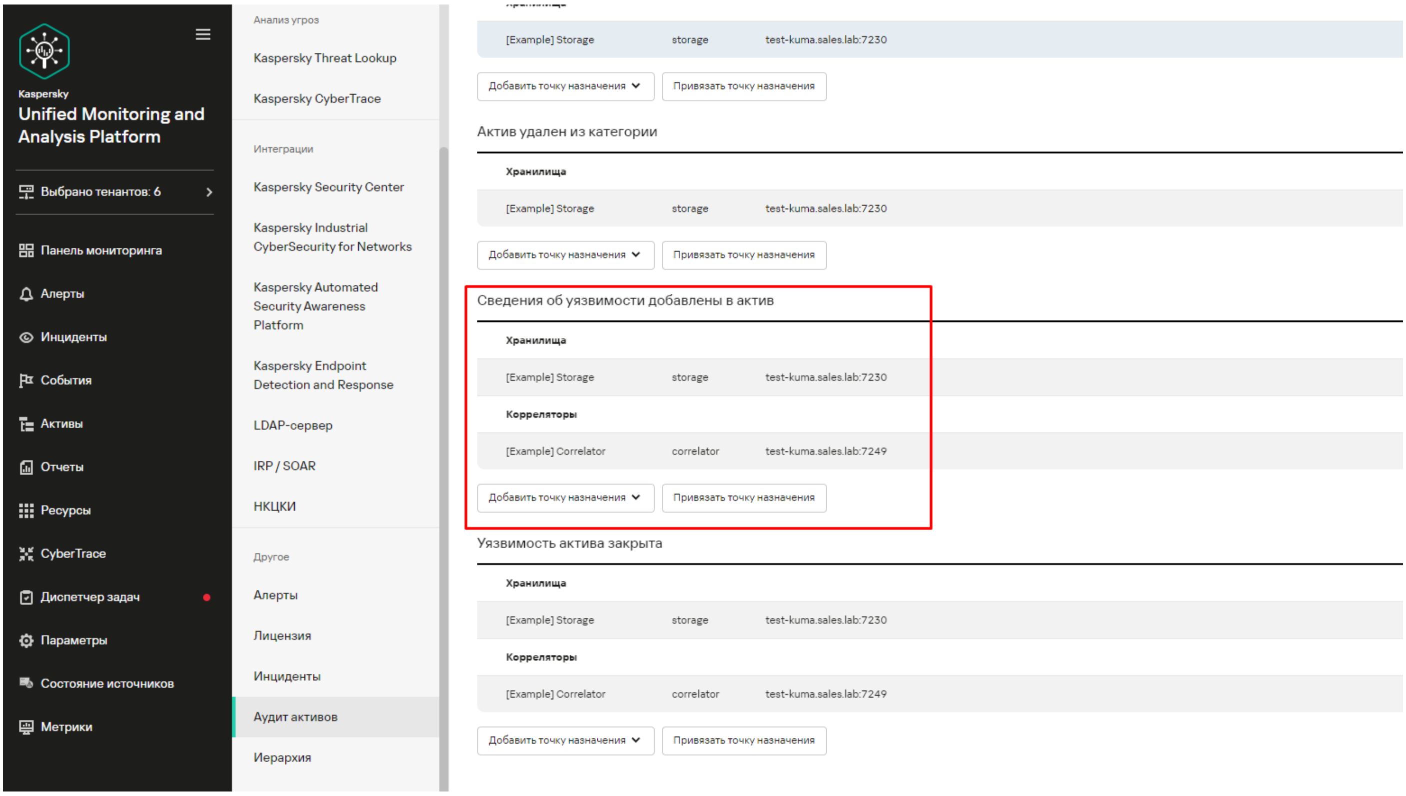
Аудит изменений по активам

> 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.com/KUMA/2.1/ru-RU/233948.htm

Аудит изменений по активам позволяет произволить корреляцию событий аудита по активам по изменеям данных ассета.

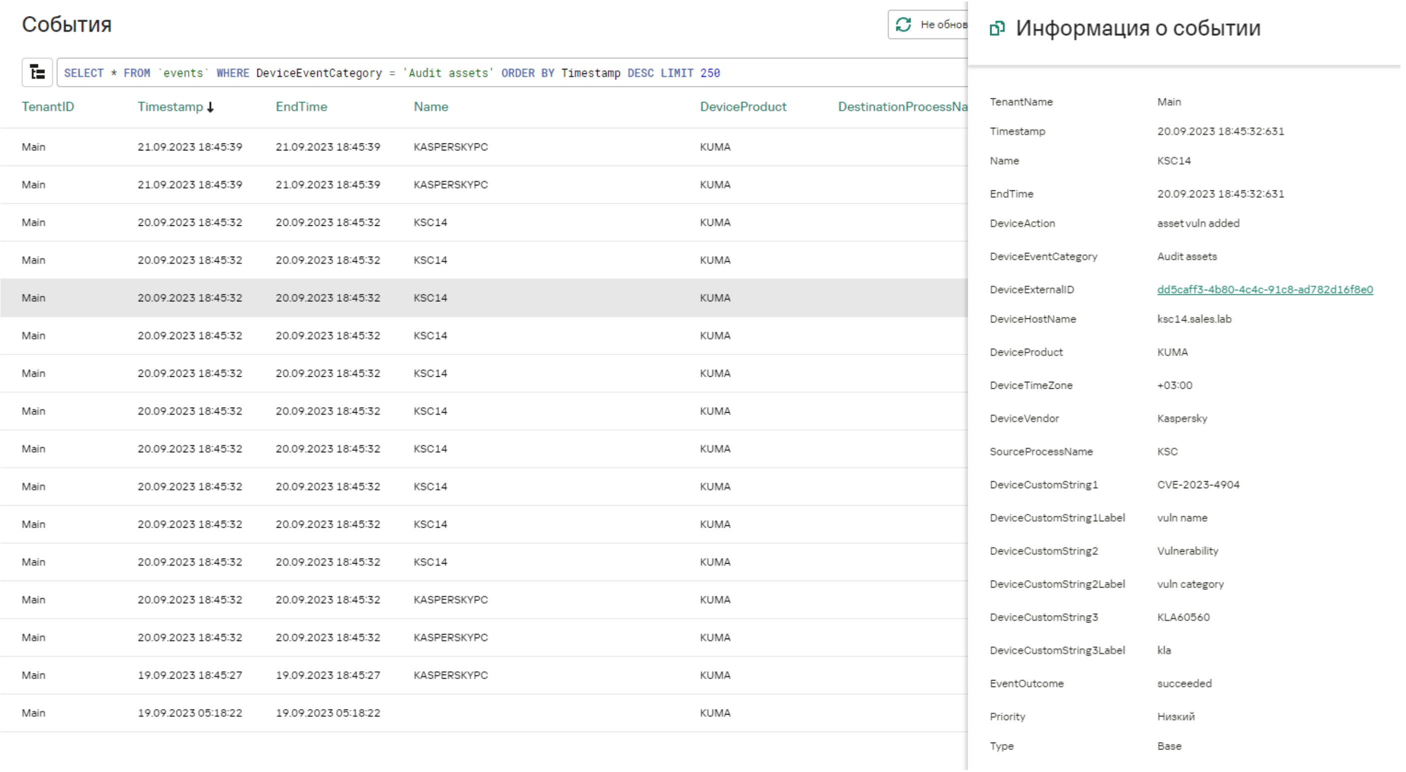
Перейдите в раздел **Параметры - Аудит активов** веб-интерфейсе KUMA. Щелкните (или добавьте) на тенант и выберите по каким параметрам вести аудит (чтобы производить корреляцию по изменениям необходимо добавить коррелятор):



> Событие формируется на каждое изменение: по одному событию на каждоеизменение (например, добавлено 5 уязвимостей - значит будет 5 событий аудитаассетов с типом "Добавление уязвимости ассета").

В событиях информацию можно найти следующим запросом:

```
SELECT * FROM `events` WHERE DeviceEventCategory = 'Audit assets' ORDER BY Timestamp DESC LIMIT 250
```



```
SELECT * FROM `events` WHERE DeviceEventCategory = 'Audit assets' ORDER BY Timestamp DESC LIMIT 250
```

TenantID	Timestamp ↓	EndTime	Name	DeviceProduct	DestinationProcessNa
Main	21.09.2023 18:45:39	21.09.2023 18:45:39	KASPERSKYPC	KUMA	
Main	21.09.2023 18:45:39	21.09.2023 18:45:39	KASPERSKYPC	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KASPERSKYPC	KUMA	
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KASPERSKYPC	KUMA	
Main	19.09.2023 18:45:27	19.09.2023 18:45:27	KASPERSKYPC	KUMA	
Main	19.09.2023 05:18:22	19.09.2023 05:18:22		KUMA	

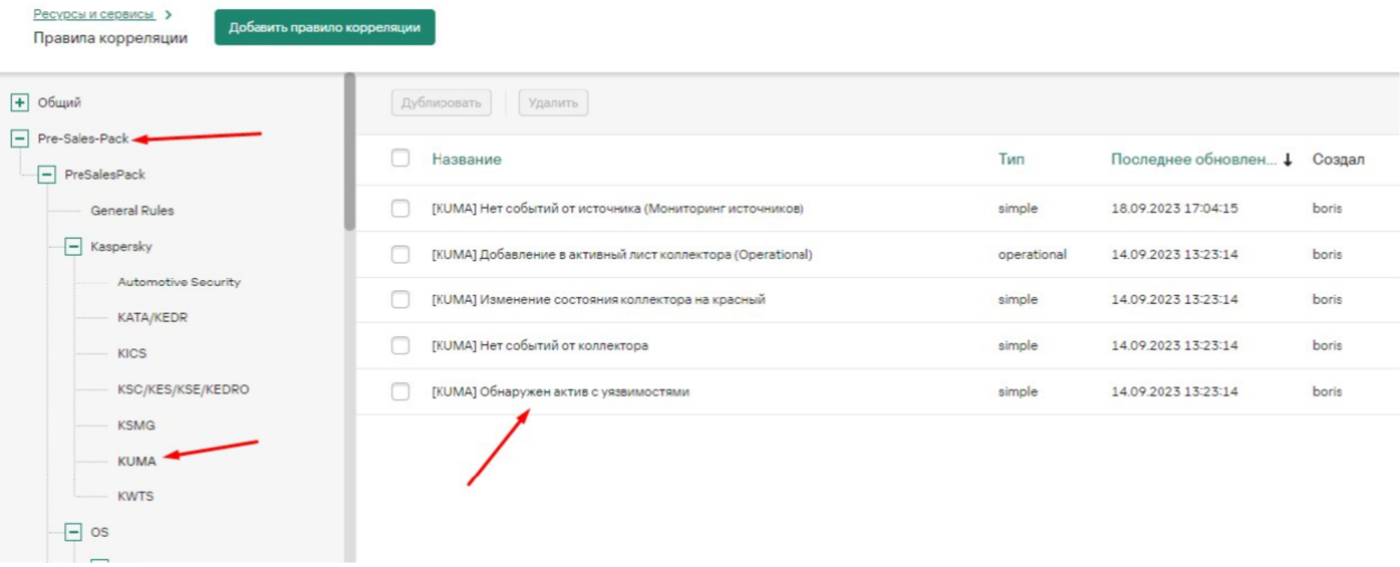
TenantName	Main
Timestamp	20.09.2023 18:45:32:631
Name	KSC14
EndTime	20.09.2023 18:45:32:631
DeviceAction	asset vuln added
DeviceEventCategory	Audit assets
DeviceExternalID	dd5caff3-4b80-4c4c-91c8-ad782d16f8e0
DeviceHostName	ksc14.sales.lab
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceProcessName	KSC
DeviceCustomString1	CVE-2023-4904
DeviceCustomString1Label	vuln name
DeviceCustomString2	Vulnerability
DeviceCustomString2Label	vuln category
DeviceCustomString3	KLA60560
DeviceCustomString3Label	kla
EventOutcome	succeeded
Priority	Низкий
Type	Base

Типы событий по которым ведется аудит:

- Ассет добавлен. Создание ассета любым способом: вручную через web-интерфейс KUMA, REST API, импорт KSC и тд.
- Ассет изменен. Изменены такие поля как: Name, IP address, Mac Address, FQDN, Operating system.
- Ассет удален. Ассет помечается как удаленный, если был удален вручную пользователем или если по нему не пришла информация из KSC по истечению срока в параметре TTL.
- Добавление уязвимости ассета. Пришла информация о новой уязвимости, ранее отсутствующей у ассета.
- Устранение уязвимости ассета. Уязвимость считается устраненной, если по ней отсутствует информация во всех источниках ассета. Информация об уязвимостях может приходить от разных источников. Считаем уязвимость устраненной, если со всех источников пришла информация об ее устранении.
- Ассет добавлен в категорию. Реативная категоризация (например, когда правило отправило ассет в определенную категорию) - фиксируется какое правило отправило и какая категория.

- Ассет удален из категории.

В наборе правил корреляции ПресейлПак есть пример правила корреляции по обнаружению новой уязвимости на Ассете по событию аудита в KUMA.



☐	Название	Тип	Последнее обновлен... ↓	Создал
☐	[KUMA] Нет событий от источника (Мониторинг источников)	simple	18.09.2023 17:04:15	boris
☐	[KUMA] Добавление в активный лист коллектора (Operational)	operational	14.09.2023 13:23:14	boris
☐	[KUMA] Изменение состояния коллектора на красный	simple	14.09.2023 13:23:14	boris
☐	[KUMA] Нет событий от коллектора	simple	14.09.2023 13:23:14	boris
☐	[KUMA] Обнаружен актив с уязвимостями	simple	14.09.2023 13:23:14	boris

---

Revision #5
Created 2 October 2023 12:49:26 by Boris Rzr
Updated 7 July 2024 07:42:08 by Koala