

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 произвести корреляцию событий аудита по активам по изменениям 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):

The screenshot displays the KUMA web interface. On the left is a dark sidebar with the Kaspersky logo and navigation menu items: 'Выбрано тенантов: 6', 'Панель мониторинга', 'Алерты', 'Инциденты', 'События', 'Активы', 'Отчеты', 'Ресурсы', 'CyberTrace', 'Диспетчер задач', 'Параметры', 'Состояние источников', and 'Метрики'. The main panel shows the 'Параметры - Аудит активов' configuration page. It features a table of assets with columns for name, type, and ID. Below the table, there are sections for 'Хранилища' (Storage) and 'Корреляторы' (Correlators). A red box highlights the 'Корреляторы' section, which contains a table with columns for name, type, and ID, and buttons for 'Добавить точку назначения' and 'Привязать точку назначения'. The 'Корреляторы' table has one entry: '[Example] Correlator', 'correlator', 'test-kuma.sales.lab:7249'.

Событие формируется на каждое изменение: по одному событию на каждое изменение (например, добавлено 5 уязвимостей - значит будет 5 событий аудита ассетов 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
```

События						Информация о событии	
TenantID	Timestamp ↓	EndTime	Name	DeviceProduct	DestinationProcessName	TenantName	Main
Main	21.09.2023 18:45:39	21.09.2023 18:45:39	KASPERSKYPC	KUMA		Timestamp	20.09.2023 18:45:32:631
Main	21.09.2023 18:45:39	21.09.2023 18:45:39	KASPERSKYPC	KUMA		Name	KSC14
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		EndTime	20.09.2023 18:45:32:631
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceAction	asset vuln added
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceEventCategory	Audit assets
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceExternalID	dd5caff3-4b80-4c4c-91c8-ad782d16f8e0
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceHostName	ksc14.sales.lab
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceProduct	KUMA
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceTimeZone	+03:00
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceVendor	Kaspersky
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		SourceProcessName	KSC
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceCustomString1	CVE-2023-4904
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceCustomString1Label	vuln name
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceCustomString2	Vulnerability
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KSC14	KUMA		DeviceCustomString2Label	vuln category
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KASPERSKYPC	KUMA		DeviceCustomString3	KLA60560
Main	20.09.2023 18:45:32	20.09.2023 18:45:32	KASPERSKYPC	KUMA		DeviceCustomString3Label	kla
Main	19.09.2023 18:45:27	19.09.2023 18:45:27	KASPERSKYPC	KUMA		EventOutcome	succeeded
Main	19.09.2023 05:18:22	19.09.2023 05:18:22		KUMA		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.

Ресурсы и сервисы > Правила корреляции [Добавить правило корреляции](#)

<input type="checkbox"/>	Название	Тип	Последнее обновлен... ↓	Создал
<input type="checkbox"/>	[KUMA] Нет событий от источника (Мониторинг источников)	simple	18.09.2023 17:04:15	boris
<input type="checkbox"/>	[KUMA] Добавление в активный лист коллектора (Operational)	operational	14.09.2023 13:23:14	boris
<input type="checkbox"/>	[KUMA] Изменение состояния коллектора на красный	simple	14.09.2023 13:23:14	boris
<input type="checkbox"/>	[KUMA] Нет событий от коллектора	simple	14.09.2023 13:23:14	boris
<input type="checkbox"/>	[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