

Импорт активов из KATA/NDR

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

Данная инструкция предназначена строго для версии KATA/NDR **7.0**.

Данная инструкция предназначена для импорта информации об активах, полученной KATA/NDR в KUMA.

Настройка KATA/NDR

Для настройки пересылки событий из KATA/NDR в SIEM KUMA необходимо выполнить следующие действия:

1. Перейти в веб-консоль KATA/NDR из-под учетной записи Администратора
2. Перейти в раздел **Параметры – Коннекторы** и нажать на кнопку **Добавить коннектор**

Имя	Статус	Тип
арсп	Работает	Active poll
KUMA	Работает	KUMA
KUMA Syslog	Работает	SIEM

3. В открывшемся окне настроить параметры интеграции с KUMA:

- Тип коннектора:** KUMA;
- Имя коннектора:** произвольное название, например, *KUMA*;
- Пароль доступа к сертификату коннектора:** задайте пароль для файла свертки;
- Пароль (повторно):** повторите введенный ранее пароль;
- Адрес сервера:** Адрес CN KATA/NDR;
- Узел размещения коннектора:** Адрес сервера в кластере KATA/NDR для размещения коллектора (в случае Single node будет совпадать с предыдущим пунктом);
- Пользователь программы:** выбрать нужного из выпадающего списка.

Создание коннектора

×

Тип коннектора

KUMA

▼

Имя коннектора

KUMA

×

Пароль доступа к сертификату коннектора

.....

👁

Пароль (повторно)

.....

👁

Адрес Сервера

10.0.0.1

×

Узел размещения коннектора

10.0.0.1

×

Пользователь программы

NDR_SYSTEM/System

▼

Описание

✎

3. По завершении заполнения необходимых полей нажать кнопку **Сохранить**.


В результате будет загружен архив, а также в интерфейсе KATA/NDR созданный коннектор перейдет в состояние **Работает**.

Имя ⚙	Статус ⚙	Тип ⚙
арсп	Работает	Active poll
KUMA	Работает	KUMA
KUMA Syslog	Работает	SIEM

Настройка KUMA

Перейдите в веб-интерфейс KUMA на вкладку Параметры - KICS/KATA и задайте параметры интеграции:

- Выключено:** галочка должна быть снята для работы интеграции;
- Тенант:** выберите необходимый тенант из выпадающего списка;
- Включить реагирование:** требуется для изменения статуса устройств;
- Файл свертки:** загрузите архив, полученный при настройке на стороне KATA/NDR;
- Пароль файла свертки:** укажите пароль от архива, заданный при настройке на стороне KATA/NDR;



Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

Доступ

Пользователи

Тенанты

Доменная аутентификация

Доступ к пространствам

Анализ угроз

Kaspersky Threat Lookup

Kaspersky CyberTrace

Интеграции

Kaspersky Security Center

KICS/KATA

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

IRP / SOAR

AI-сервис

НКЦКИ

Интеграция с KICS/KATA

IP-адрес сервера KICS/KATA: 10.10.10.10

Идентификатор коннектора KICS/KATA: 3

☐ Выключено

Интервал обновления в часах

3

⚠ Запланированное обновление: 25.12.2024 17:56:26

Тенант*

AntiAPT

☒ Включить реагирование

Файл свертки*

🔒

📄

Пароль файла свертки*

🔒

👁

Сохранить

По окончании настройки нажмите кнопку **Сохранить**.