KATA/NDR 7.0

Информация, приведенная на данной странице, является разработкой команды presales и/или community KUMA и **HE** является официальной рекомендацией вендора.

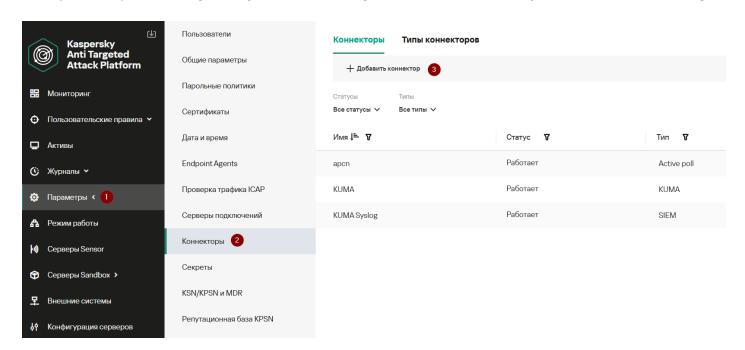
Данная инструкция предназначена строго для версии KATA/NDR **7.0**. Инструкция для предыдущих версии находится в соответствующем разделе базы знаний.

Данная способ позволяет собирать события **NDR**. Для сбора событий **КАТА** воспользуйтесь соответствующей инструкцией.

???????? 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



3. В открывшемся окне настроить параметры отправки событий в КUMA SIEM:

Тип коннектора: SIEM;

Имя коннектора: произвольное название, например, *KUMA Syslog*;

Адрес сервера: 127.0.0.1;

Узел размещения коннектора: выбрать нужный из выпадающего списка; **Пользователь программы**: выбрать нужного из выпадающего списка;

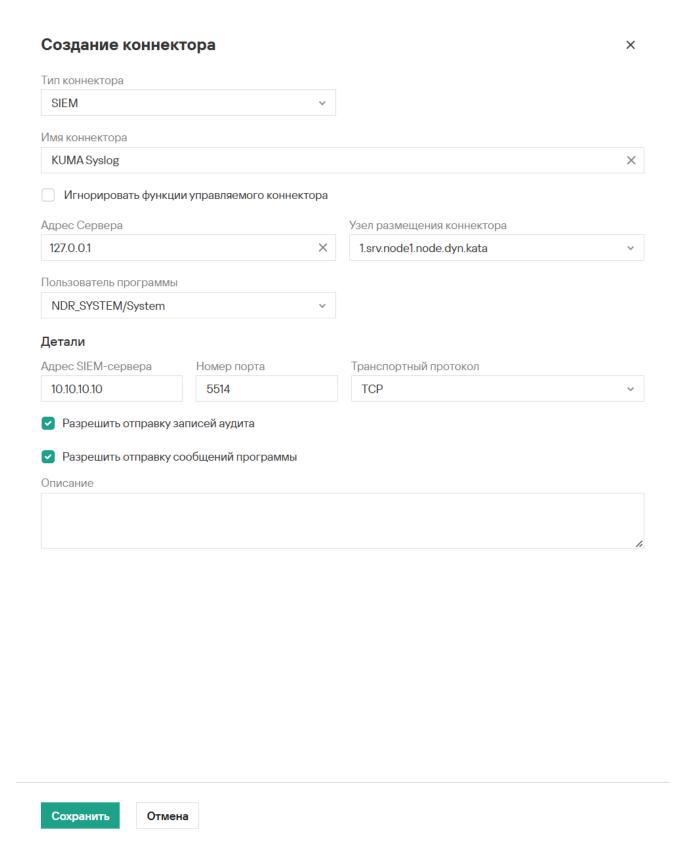
Адрес SIEM сервера: IP-адрес сервера коллектора KUMA;

Номер порта: порт коллектора KUMA; **Транспортный протокол**: TCP или UDP.

Разрешить отправку записей аудита: вкл, если требуется передача событий аудита

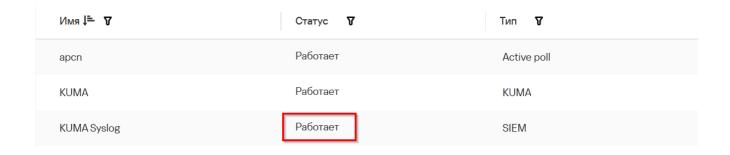
Разрешить отправку сообщений программы: вкл, если требуется передача сообщений

программы



3. По завершении заполнения необходимых полей нажать кнопку Сохранить.

В результате в интерфейсе KATA/NDR созданный коннектор перейдет в состояние **Работает**.

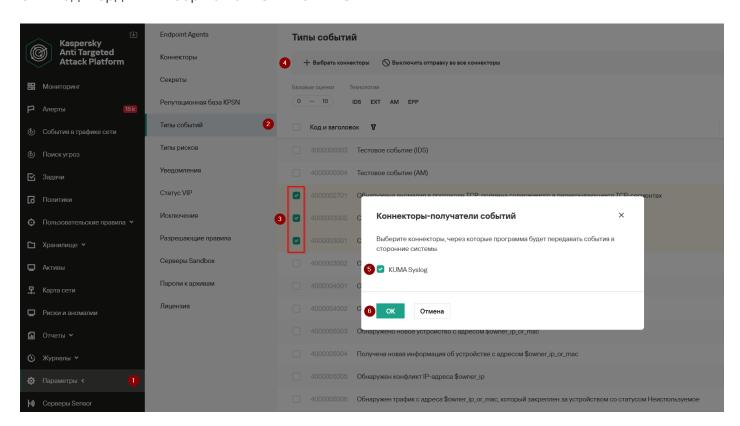


???????? ??????? ???????

По умолчанию события безопасности KATA/NDR не передаются ни в какие смежные системы, о чем свидетельствует колонка **Тип события** - **Не отправляются**. Поэтому, чтобы события безопасности передавать в другие системы необходимо определить перечень таких событий для каждой системы, для который мы настроили коннектор.

Для настройки отправки событий необходимо:

- 1. Войти в интерфейс KATA/NDR от имени пользователя Старший офицер безопасности
- 2. Перейти на вкладку Параметры Типы событий
- 3. Выбрать один или несколько типов событий, которые необходимо передавать
- 4. Нажать на кнопку Выбрать коннекторы
- 5. Установить флаг напротив тех систем, в которые необходимо предавать выбранные события
- 6. Подтвердить выбор нажатием кнопки ОК



После завершения настроек добавленные события будут отмечены флагом в колонке соответствующего коннектора



???????? KUMA

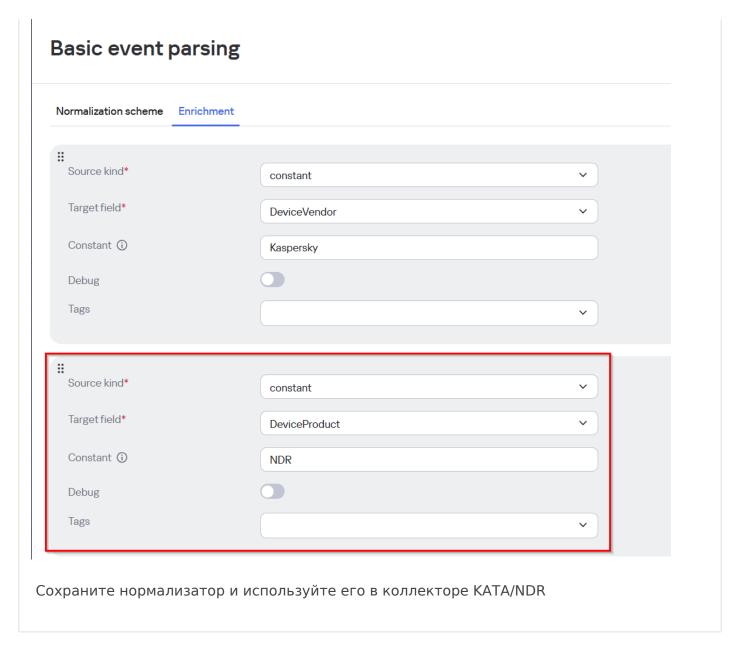
После того как параметры передачи событий настроены, требуется создать коллектор в вебинтерфейсе KUMA для событий KATA/NDR.

- 1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KATA/NDR. Также обязательно задайте в качестве разделителя **\0**.
- 2. На шаге Парсинг событий выберите соответствующий нормализатор

Какой нормализатор можно использовать

Сделайте копию коробочного нормализатора [OOTB] KICS4Net v3.x

В копии нормализатора, в главном парсере, на вкладке Обогащение измените значение константы для поля **DeviceProduct** на **NDR**



- 3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
 - Хранилище. Для отправки обработанных событий в хранилище.
 - Коррелятор. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

- 4. На шаге Проверка параметров нажмите Сохранить и создать сервис.
- 5. Скопируйте появившуюся команду для установки коллектора КИМА.