

KATA/NDR 7.0

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**. Инструкция для предыдущих версии находится в соответствующем разделе базы знаний.

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

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**

The screenshot displays the Kaspersky Anti Targeted Attack Platform (KATA) web console. The left sidebar contains the 'Параметры' (Parameters) menu, which is highlighted with a red badge '1'. The main content area shows the 'Коннекторы' (Connectors) section, also highlighted with a red badge '2'. A table lists the following connectors:

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

At the top of the 'Коннекторы' section, there is a '+ Добавить коннектор' button with a red badge '3'.

3. В открывшемся окне настроить параметры отправки событий в KUMA 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

Создание коннектора



Тип коннектора

Имя коннектора

☐ Игнорировать функции управляемого коннектора

Адрес Сервера

Узел размещения коннектора

Пользователь программы

Детали

Адрес SIEM-сервера

Номер порта

Транспортный протокол

☒ Разрешить отправку записей аудита

☒ Разрешить отправку сообщений программы

Описание

Сохранить

Отмена

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

В результате 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 отправки событий

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

<input type="checkbox"/> Код и заголовок ▾	Базовая о... ▾	Технология ▾	KUMA Syslog
✓ 4000002701 Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	3	IDS	✓
✓ 4000003000 Сработало правило из набора \$fileName (системный набор правил)	9	IDS	✓
✓ 4000003001 Сработало правило из набора \$fileName (пользовательский набор правил)	9	IDS	✓

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе 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**

Basic event parsing

Normalization scheme Enrichment

⋮

Source kind*

constant

▼

Target field*

DeviceVendor

▼

Constant ⓘ

Kaspersky

Debug

☒

Tags

▼

⋮

Source kind*

constant

▼

Target field*

DeviceProduct

▼

Constant ⓘ

NDR

Debug

☒

Tags

▼

Сохраните нормализатор и используйте его в коллекторе KATA/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 KUMA.

Revision #7

Created 25 December 2024 14:11:41 by Koala

Updated 12 February 2025 10:28:48 by Koala