

KATA

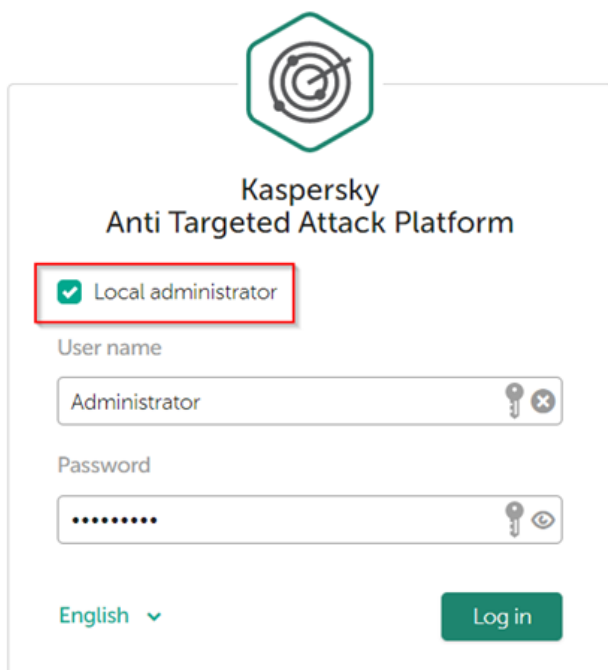
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/240690.htm>

Настройка KATA

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

1. Перейти в веб-консоль центрального узла Kaspersky Anti Targeted Attack из-под учетной записи Администратора, предварительно отметив параметр **Local administrator**



Kaspersky
Anti Targeted Attack Platform

☒ Local administrator

User name
Administrator

Password
.....

English ▾ Log in

2. Перейти в раздел **Settings – SIEM System** и настроить параметры отправки событий в KUMA SIEM:

Host/IP: ip или fqdn адрес коллектора KUMA

Port: порт коллектора KUMA

Protocol: TCP или UDP

Host ID: напр., kata-cn

Heartbeat: интервал в минутах

Kaspersky Anti Targeted Attack Platform

Dashboard

Operation mode

Endpoint Agents

Reports

Settings

Sensor servers

Sandbox servers

External systems

Users

General settings

Certificates

Date and time

Endpoint Agents

KSN/KPSN and MDR

KPSN reputation database

Notifications

SIEM system

Network settings

Passwords for archives

License

SIEM system Integration

Data to send

- ☒ Activity log
- ☒ Alerts

Host/IP* 10.68.85.125

Port* 5150

Protocol TCP

Host ID KATA 4.0

The server with this ID will be shown as the source of the alert in the SIEM system log

Heartbeat 1 minutes

TLS encryption Disabled

Apply Cancel

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Kaspersky Anti Targeted Attack Platform.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KATA.
2. На шаге **Парсинг** событий выберите нормализатор **[ООТВ] KATA**.
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.

Полезные ссылки

Настройка получения событий KATA/EDR (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/240690.htm>

Revision #6
Created 11 August 2023 08:15:42 by Koala
Updated 26 November 2024 12:49:49 by Koala