

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

?? KICS for Networks (???????

4.3 ? 4.5) ? KUMA

Настройка интеграции выполняется в два этапа: сначала создается и настраивается коллектор в KUMA, затем создается коннектор в KICS for Networks.

Настройка KUMA

1. Перейдите в раздел «Ресурсы» и откройте вкладку «Коллекторы».

Название картинки

1. Нажмите кнопку «+ Создать».

Название картинки

1. В открывшемся окне укажите название коллектора. Рекомендуется использовать наименование продукта, тип подключения и порт (например, KICS_for_Networks_TCP\5160), чтобы в дальнейшем легко идентифицировать коллектор.

Название картинки

1. На вкладке «Транспорт» укажите тип соединения (протокол) и порт, который будет использоваться для приема событий от источника.

Название картинки

1. На вкладке «Парсинг событий» - «Настройки парсинга» выберите соответствующий нормализатор для обработки входящих событий.

Название картинки

1. На вкладке «Маршрутизация» добавьте ранее созданные коррелятор и хранилище. Подробнее о разворачивании этих компонентов см. в [Справке по KUMA](#).

Название картинки

1. На вкладке «Проверка параметров» нажмите кнопку «Сохранить и создать сервис».

Название картинки

1. После создания коллектора скопируйте сгенерированную команду и выполните её в терминале сервера KUMA с правами администратора для разворачивания сервиса.

Название картинки

Настройка KICS for Networks

1. Перейдите в раздел «Параметры» - «Коннекторы» и нажмите кнопку «+ Добавить коннектор».
2. В карточке нового коннектора заполните поля:
 - Тип коннектора: SIEM.
 - Имя коннектора: Произвольное наименование.
 - Адрес сервера: IP-адрес узла, на котором развернут сервер KICS for Networks.

- Узел размещения коннектора: Server.
- Пользователь программы: Учетная запись администратора KICS for Networks.
- Адрес SIEM-сервера: IP-адрес узла, на котором развернут сервер KUMA.
- Номер порта: Порт, указанный при настройке коллектора KUMA (см. п. 4 раздела «Настройка KUMA»).
- Транспортный протокол: Протокол, указанный при настройке коллектора KUMA (см. п. 4 раздела «Настройка KUMA»).

Название картинки

1. Нажмите кнопку «Сохранить».
2. Убедитесь, что в свойствах созданного коннектора параметры имеют следующие значения:
 - Включен: Да.
 - Статус: Работает.

Название картинкиЕсли значения отличаются, проверьте выполненные настройки и перезапустите коннектор (выполните последовательность «Выключить» - «Включить»).

3. Перейдите в раздел «Параметры» - «Типы событий». Выберите типы событий, которые необходимо передавать в KUMA, и активируйте для них отправку через созданный коннектор.

Название картинки

Проверка передачи событий

1. В интерфейсе KUMA перейдите в раздел «События» и выполните опрос источников.

Название картинки

2. Убедитесь в наличии события об успешной аутентификации коннектора, которое должно появиться в момент его создания в KICS for Networks.

Название картинки

1. Воспроизведите событие безопасности, например, запустите тестовый вирус на узле, который интегрирован с KICS for Networks.

Название картинки

1. Убедитесь, что сработал модуль постоянной защиты KICS for Nodes (детектирование события на стороне источника).

Название картинки

1. В интерфейсе KUMA снова перейдите в раздел «События» и выполните опрос.

Название картинки

1. Убедитесь, что воспроизведенное событие безопасности успешно доставлено и отображается в KUMA.

Название картинки

Revision #6

Created 16 February 2026 13:34:50 by Alexey Panyukhin

Updated 26 June 2026 11:59:09 by Alexander Somonov