KSC CEF

> 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/KUMA/2.1/ru-RU/241235.htm

> Функция экспорта событий Kaspersky Security Center в SIEM-системы в формате CEF доступна при наличии лицензии Kaspersky Endpoint Security для бизнеса **Расширенный** или **выше**.

Настройка передачи событий KSC в формате CEF

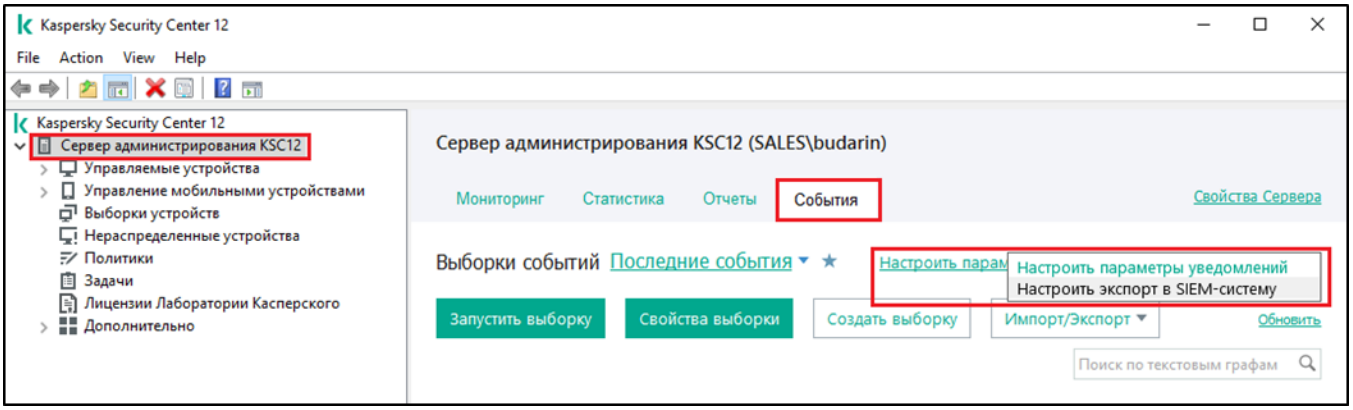
Чтобы настроить передачу событий от Сервера администрирования Kaspersky Security Center в SIEM-систему KUMA:

1. В дереве консоли Kaspersky Security Center выберите узел **Сервер администрирования**.

2. В рабочей области узла выберите вкладку **События**.

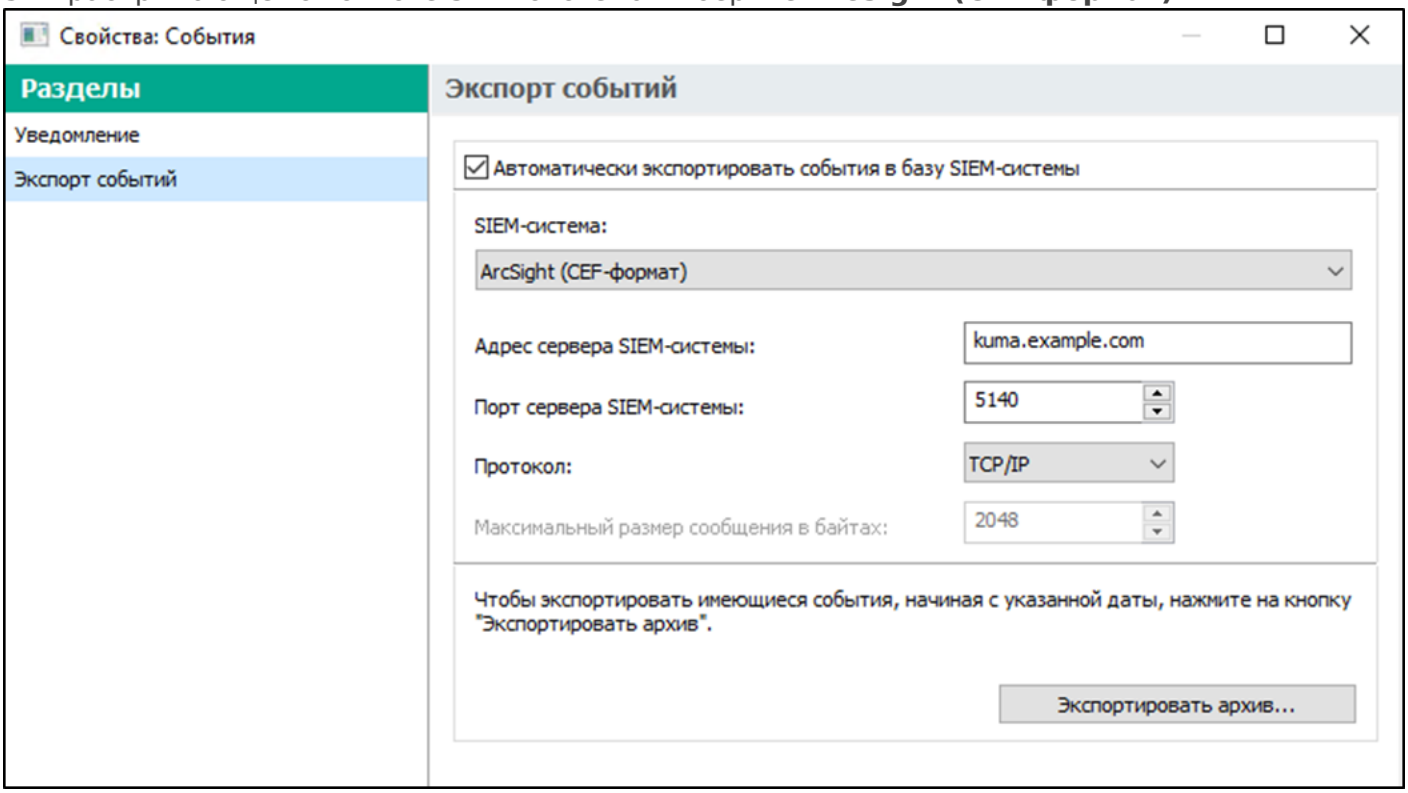
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите **Настроить экспорт в SIEM-систему**.

Откроется окно **Свойства**: **События**.



4. Установите флажок **Автоматически экспортировать события в базу SIEM-системы**.

5. В раскрывающемся списке SIEM-система выберите **ArcSight (CEF-формат)**.



6. Укажите адрес сервера SIEM-системы KUMA и порт для подключения к серверу в соответствующих полях.

По кнопке **Экспортировать архив** Kaspersky Security Center экспортирует уже созданные события в базу SIEM-системы KUMA с указанной даты. По умолчанию Kaspersky Security Center экспортирует события с текущей даты.

7. Нажмите на кнопку **OK**.

Настройка коллектора KUMA

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коллекторы**.

2. В списке коллекторов найдите коллектор с нормализатором **[OOTB] KSC** и откройте его для редактирования.

Что делать, если ресурс не доступен для редактирования

Начиная с версии KUMA 2.1 OOTB ресурсы недоступны для редактирования. В таком случае необходимо скопировать OOTB-ресурс и произвести редактирование в копии этого ресурса.

> Важно! При копировании OOTB ресурса, копируется и становится доступным для редактирования только сам ресурс. Связанные ресурсы нужно копировать и привязывать отдельно.

3. На шаге **Транспорт** в поле **URL** укажите порт, по которому коллектор будет получать события Kaspersky Security Center.

4. Порт должен совпадать с портом сервера SIEM-системы KUMA, указанным в настройках на стороне KSC.

5. На шаге Парсинг событий проверьте, что выбран нормализатор **[OOTB] KSC**.

6. 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.

7. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

8. Скопируйте появившуюся команду для установки коллектора KUMA.

Revision #14
Created 9 August 2023 10:57:36 by Admin
Updated 7 July 2024 08:56:23 by Koala