

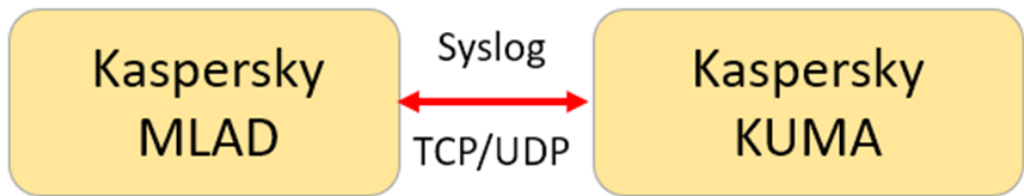
Kaspersky MLAD: ?????????? ? KUMA ?? Syslog

1. ?????????? ???????

?????? ?????????? ?????????? ?????????? ?????????? Kaspersky MLAD ??? ?????????? ? KUMA ?? ?????????? Syslog.

???? ?????? ?????????? – ?????????? ?????????? ?????????? ?????????????? ?? Kaspersky MLAD ? SIEM ?????????? ?? ?????????????? ?? ?????????????????? ?????????????? ? ?????????????????? ??????????.

???? ?????????????? ?????????????? ?????? ??????????????, ?????????????? ? ?????????????? ? ?????? ?????????????? ??????????????.



2. ?????????????? ???????

?????? ?????? ?????????????? ????????????? CEF-???????????? ? ????????? Kaspersky MLAD ?? ?????????? ?????????? ?????????????????? ? SIEM-?????????.

??? ?????? ?????????????? ? ???? ??????????????????, ?????? ? ?????????????? ?????????????, ?????? ? ?????????????? CEF-?????????????.

?????? ??? ?????????????? ?????????????????? ?????????????????? ?????????????????? ????????????? ?????????? ?????????? ?????????????????? ?????????????????? ?? Syslog-?????????, ?????????? ??? ?????????????? (TCP ??? UDP), ?????????? ?????? ? ???? Syslog-?????????. ???? ?? ?????????????? ?????????????????? ?????????????? TLS-?????????????, ?? ??? ?????????????? ?????? ?????????????? ?????????????/????????????? ???? ?????????? ? CA-????????????????? ??? ?????????????????? ?????????????? ??????????.

Kaspersky Machine Learning for Anomaly Detection

<<

Лицензирование

Пользователи

Роли

Права

Уведомления

Системные параметры

Активы

Русский

Системные параметры

ИмпортЭкспорт

Основные

Безопасность

Anomaly Detector

Keeper

Mail Notifier

Similar Anomaly

Stream Processor

Trainer

HTTP Connector

MQTT Connector

AMQP Connector

KICS Connector

CEF Connector

WebSocket Connector

Event Processor

Инциденты

Ведение журналов

Графики

Активы

Меню

Получать события для службы Event Processor

Отправлять зарегистрированные инциденты в SIEM-систему

Отправлять зарегистрированные события в SIEM-систему

IP-адрес для отправки событий и инцидентов в SIEM-систему

Порт для отправки событий и инцидентов в SIEM-систему

Отправлять журналы событий информационной безопасности на syslog-сервер

Транспортный протокол для отправки событий информационной безопасности на syslog-сервер

UDP

Адрес syslog-сервера для отправки событий информационной безопасности

192.168.100.99

Порт syslog-сервера для отправки событий информационной безопасности

5144

Использовать TLS-соединение

Использовать рекомендуемые параметры TLS-соединения

Сертификат сервера

+ Обзор

Закрытый ключ к сертификату сервера

+ Обзор

Сертификат CA для проверки подписи сертификата клиента

+ Обзор

Сертификат клиента

+ Обзор

Закрытый ключ к сертификату клиента

+ Обзор

Сертификат CA для проверки подписи сертификата сервера

+ Обзор

????? ?????? ?????????? ? ?????????? ?????, ?????? ? ???????, ?????? ? ??????? ????????????. ?????????? ??????? CEF connector, ??? ?????????????????? ??, ????? ?? ?????????? ??????????? ? ???????????.

Kaspersky Machine Learning for Anomaly Detection

<<

Информационная панель

Мониторинг

История

Временной срез

Процессор событий

Инциденты

Модели

Пресеты

Службы

Источники данных

Службы

Обработка данных

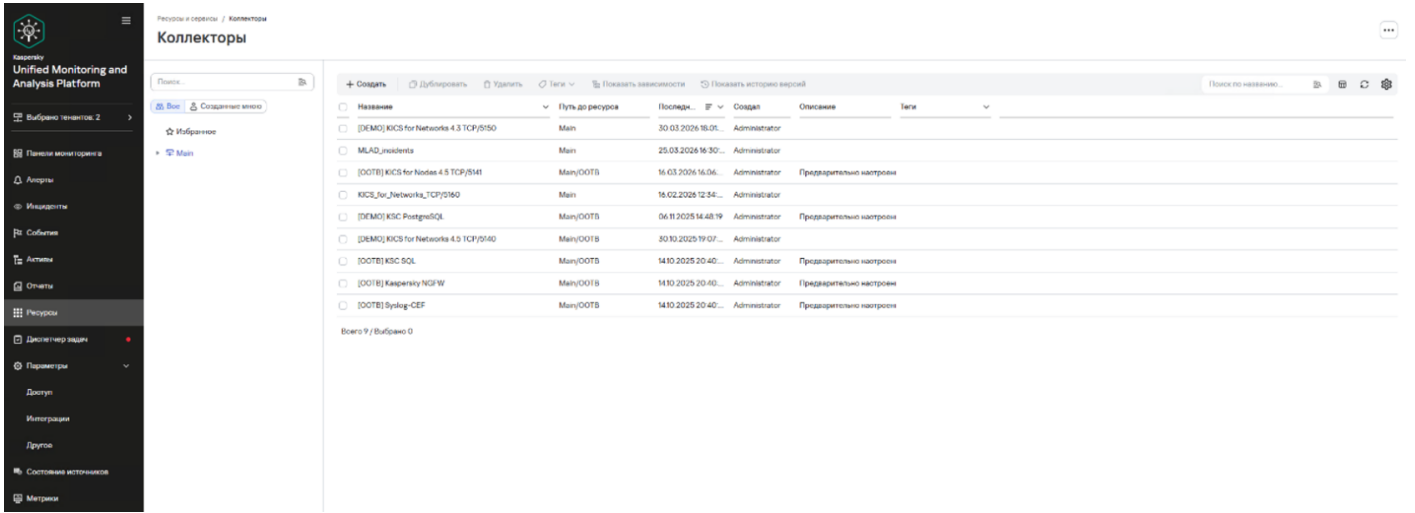
Основные

Коннекторы

Другие

Имя	Статус	Действия
HTTP Connector	Запущена	▶ Запустить □ Остановить ⌂ Перезапустить
AMQP Connector	Остановлена	▶ Запустить □ Остановить ⌂ Перезапустить
KICS-3.0 Connector	Остановлена	▶ Запустить □ Остановить ⌂ Перезапустить
MQTT Connector	Остановлена	▶ Запустить □ Остановить ⌂ Перезапустить
CEF Connector	Запущена	▶ Запустить □ Остановить ⌂ Перезапустить
WebSocket Connector	Остановлена	▶ Запустить □ Остановить ⌂ Перезапустить

?? ?????? ??????????? ?? ?????????? MLAD ???????????.
? KUMA ??????????? ? ??????? ??????????, ?????? ??????????????.



?????? ???????? KUMA ?????? ??? [OOTB] Syslog
CEF. ?????????? ?????? ?? ??????? ?????????? ?????????????? ? ??????????? ? ??? ????????????.
?????????? ?????????????? ?????????????????? ??????????? ?? ?????????? ??????????????.

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор	Создать
Тип* ?	udp
URL* ?	:5144
Auditd	
Разделитель	

????????? ??? ???????????, ??????????? ? ????, ?? ?????????? KUMA ?????? ??????????? ?????????????? ?? Syslog.
?????????????, ??? ?????????????? ??????????????? ? MLAD ?????????????? ? ??????????????? ? ??????? ??????????.

????????????? ?????????????? ?????????? ?? ??????? ?? ?????? ?????????????? Syslog. ?? ?????????? ?????????? ?????????? ??
????????? ??????????????, ??? ?????? ?????????????? ?????????? Syslog, ??????????????? ?? MLAD. ??? ?????? ???
????????????????????????? ?????????????? ?????????? ?????????????????????????? ???????. ?????????? ??????????? ? ?????????????? ??????????
????????? ? ?????????????????????? ?? KUMA, ? ? ?????????? ?????????????? ?? ??????????????????????,

?????? ?????????????????? ??????????????? ??? ?????????? ??????? ?????????????????? ??????? ???????????
????????????????????????????? ??????????.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.

Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

??? ????? ?????????? ?????????? ?????????????? ???????? (????? sudo) ?? ?????? ? KUMA.

Создание коллектора



- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.

Подробнее см. [в онлайн-справке](#).

Сервисы, использующие этот коллектор

Тип	Название
коллектор	[DEMO] Syslog-CEF-MLAD - копия

Сохранить и перезапустить сервисы Сохранить и обновить параметры сервисов

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-ics.demo.lab:7210 --id fafac7f2-c213-4097-ad84-c4c8ef5f3649 --api.port 7240 --install
```

???? ??????? ?? ? ??????????, ?? ????? ?????????? ?????????? ?????????? ?? ???????

????????? ?????????? ? ??????? ??????? ?????????? ? ?????????????? ?????????.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).
Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.
Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

Сервисы, использующие этот коллектор

Тип	Название
коллектор	[OOTB] Syslog-CEF

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

????????? ? ?????? ????????? ????????? ? ??????????, ??? ??? ?????? ??????????? Syslog
?????????.

Ресурсы и сервисы / Сервисы

Сервисы

+

Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

Смотреть раздачи

Скопировать

Копировать идентификатор

Поиск

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
Вкл	Коллектор	KICS_for_Networks_TCP/S160	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7237	3 часа 11 минуты 33...	16.02.2026 12...
Вкл	Коллектор	MLAD_incidents	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7238	3 часа 11 минуты 36...	23.03.2026 11...
Вкл	Коллектор	[DEMO] KICS for Networks 4.3 TCP/S150	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7236	3 часа 11 минуты 34...	30.10.2025 16...
Вкл	Коллектор	[DEMO] KICS for Networks 4.5 TCP/S140	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7232	3 часа 11 минуты 37...	14.10.2025 20...
Вкл	Коллектор	[DEMO] KSC PostgreSQL	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7233	3 часа 11 минуты 35...	14.10.2025 20...
Вкл	Коллектор	[OOTB] KICS for Nodes 4.5 TCP/S141	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7234	3 часа 11 минуты 37...	14.10.2025 20...
Вкл	Коллектор	[OOTB] Syslog-CEF	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7235	3 часа 11 минуты 33...	14.10.2025 20...
Вкл	Ядро	core-1	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7210	3 часа 11 минуты 43...	14.10.2025 20...
Вкл	Коррелятор	[OOTB] Correlator	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7231	3 часа 11 минуты 35...	14.10.2025 20...
Вкл	Метрики	metrics	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7227		14.10.2025 20...
Вкл	Хранилище	[OOTB] Storage	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7230	3 часа 11 минуты 30...	14.10.2025 20...

????????? ? MLAD ? ????????????? ??????-???????? ?????????? ?????????, ?????????, ????????? ? ?????
????????? ? ?????????.

????? ?????????? ???? ?????????? ?????? ? KUMA ? ????????? ??????? ????????? ? ??????????.

Ресурсы и сервисы / Сервисы

Сервисы

+

Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

Смотреть раздачи

Скопировать

Копировать идентификатор

Поиск

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
Вкл	Коллектор	KICS_for_Networks_TCP/S160	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7237	3 часа 13 минуты 12...	16.02.2026 12...
Вкл	Коллектор	MLAD_incidents	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7238	3 часа 13 минуты 16...	23.03.2026 11...
Вкл	Коллектор	[DEMO] KICS for Networks 4.3 TCP/S150	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7236	3 часа 13 минуты 13...	30.10.2025 16...
Вкл	Коллектор	[DEMO] KICS for Networks 4.5 TCP/S140	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7232	3 часа 13 минуты 15...	14.10.2025 20...
Вкл	Коллектор	[KUMA] KSC PostgreSQL	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7233	3 часа 13 минуты 14...	14.10.2025 20...
Вкл	Коллектор	[OOTB] KICS for Nodes 4.5 TCP/S141	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7234	3 часа 13 минуты 16...	14.10.2025 20...
Вкл	Коллектор	[OOTB] Syslog-CEF	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7235	3 часа 13 минуты 12...	14.10.2025 20...
Вкл	Ядро	core-1	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7210	3 часа 13 минуты 21...	14.10.2025 20...
Вкл	Коррелятор	[OOTB] Correlator	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7231	3 часа 13 минуты 14...	14.10.2025 20...
Вкл	Метрики	metrics	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7227		14.10.2025 20...
Вкл	Хранилище	[OOTB] Storage	4.0.2.13	Main	kuma-ics.demo.lab	192.168.100.99	7230	3 часа 13 минуты 9...	14.10.2025 20...

C????????? ?????????? SQL-????????. ?? ????????? ? ?????? ????????? ?????????????? ?? MLAD.

Картина

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Аварии

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Составные источники

Метрики

События

Не обновлять

15 now-24h

RUSSIA-AUTOCOTTE-Storage

SELECT * FROM "events" WHERE ServiceID = 'a23ca3ff-9a52-4825-a7f9-ee4b0226a2ef' ORDER BY Timestamp DESC LIMIT 250

Настроить SQL-запрос, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TBV

TenantID	Timestamp	Name	DeviceProduct	DeviceVendor	DestinationAddress	DestinationUsername	DeviceEventClassID	DeviceAddress	AggregationRuleID
Main	10.04.2026 16:35:42.322							192.168.100.98	
Main	10.04.2026 16:35:40.681							192.168.100.98	
Main	10.04.2026 16:21:34.183							192.168.100.98	
Main	10.04.2026 16:21:33.839							192.168.100.98	
Main	10.04.2026 16:18:09.406							192.168.100.98	
Main	10.04.2026 16:18:07.112							192.168.100.98	
Main	10.04.2026 16:13:22.448							192.168.100.98	
Main	10.04.2026 16:13:22.184							192.168.100.98	
Main	10.04.2026 15:59:20.581							192.168.100.98	
Main	10.04.2026 15:59:09.110							192.168.100.98	

Revision #3

Created 10 April 2026 13:57:30 by Эльдар Юсуфов

Updated 23 October 2026 11:20:47 by Эльдар Юсуфов