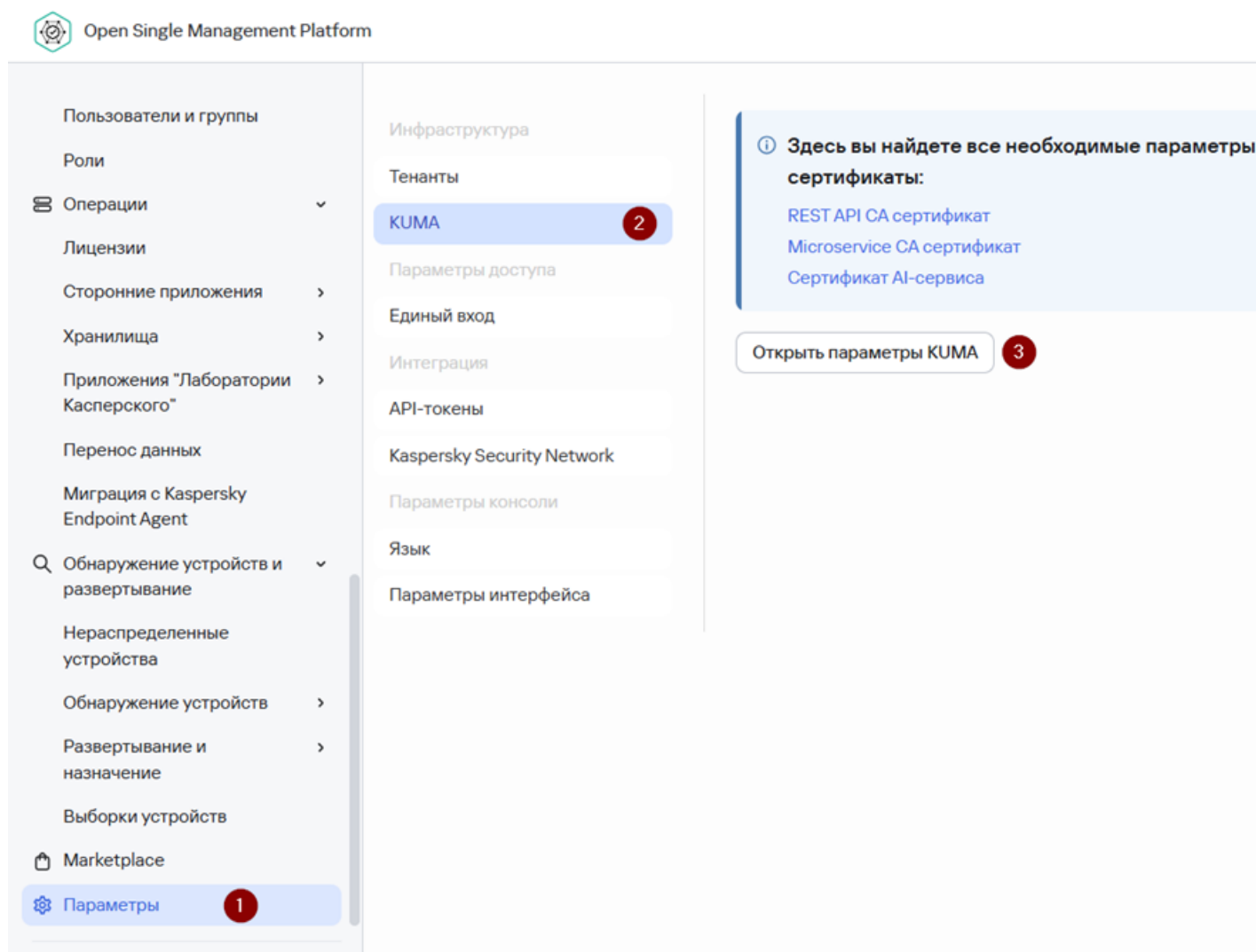


Интеграция с KIRA и 3rd party LLM

Интеграция с KIRA (LLM)

KIRA (Kaspersky Investigation & Response Assistant) поддерживает режим **Custom**, позволяющий подключаться к любому OpenAI-совместимому API-эндпоинту, включая локальный экземпляр Ollama.

1. В веб-консоли XDR перейдите в **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Интеграции** → **AI сервисы**.



2. Откройте вкладку **Kaspersky Investigation & Response Assistant**. Включите переключатель **Состояние**, чтобы активировать KIRA, и установите **Режим** в значение **Custom**.

Параметры

Доступ

Профиль

Тенанты

Доступ к пространствам

Анализ угроз

Kaspersky CyberTrace

Интеграции

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

AI-сервисы

Другое

Общее

Лицензия

Параметры обновления

Мониторинг сервисов

Теги

Поля расширенной схемы событий

AI-сервисы

AI-рейтинг и AI-статус активовKaspersky Investigation & Response AssistantОбнаружение атак DLL Hijacking

Состояние

Режим

Базовый URL-адрес

API ключ

Модель

Максимальный размер промпта

Дополнительные настройки

Прокси-сервер

Язык ответа

Подключение

KIRA

Сохранить

3. Заполните параметры подключения в зависимости от выбранного бэкенда. Пример:

Параметр	OpenAI (cloud)	Локальный DeepSeek через Ollama
Базовый URL-адрес	https://api.openai.com/v1	http://kuma-services.abc.lab:11434/v1
API ключ	Секрет с ключом OpenAI	Любая непустая строка (например, ollama)
Модель	gpt-4o / gpt-4.1	deepseek-r1:7b

Максимальный размер промта	400000	32000 (лимит контекста модели)
Язык ответа	Russian	English

Примечание. Ollama предоставляет OpenAI-совместимый API по пути /v1 — интеграция KIRA в KUMA работает без дополнительных адаптеров.

- При необходимости загрузите JSON-файл **Дополнительные настройки**, чтобы переопределить параметры модели (temperature, top_p и т. д.).
- Нажмите **Сохранить**. KUMA предложит **принять лицензионное соглашение KIRA** — принятие обязательно для включения функции.
- Нажмите **Проверить подключение**, чтобы убедиться, что KUMA имеет доступ к LLM-эндпоинту. Зелёный статус подтверждает работоспособность интеграции.
- После сохранения и принятия соглашения на страницах алертов и инцидентов станет доступна кнопка **KIRA**. Нажмите её, чтобы запустить AI-анализ сработавшего правила корреляции или таймлайна инцидента.

Детали алерта

Алерт 61143

В инциденте

AI-анализ 1

Изменить

Изменить статус

Назначить

Выбрать плейбук

Связать с инцидентом

Удалить связь с инцидентом

Создать инцидент

Анализ с помощью KIRA 2

Оставшиеся токены: 10 000 000

Подробнее

Наблюдаемые объекты

Активы

Файлы

Похожие закрытые алерты

Похожие инциденты

История

Комментарии

Сводная информация

Аналитик

Имя

Тенант

Активы

Зарегистрировано

Время обновления

Первое событие

Последнее событие

Не назначен

exploit_detected_windows

Main

Пользователей: 0; устройств: 1

06.08.2026 12:24:37

06.08.2026 12:25:07

06.08.2026 12:24:35

06.08.2026 12:24:35

Связанный с

Важность

Правила корреляции

IOA-правила

Технология

Тактика MITRE

Техника MITRE

Источники обнаружений

ID инцидента 1703

Same host asset any of ["XDR-KSC"]

Связан автоматически

Высокий

[OOTB] EDR IOA alert

exploit_detected_windows

IOA

TA0002: Execution

T1203: Exploitation for Client Execution

XDR-KSC

4. Если во внутренней инфраструктуре развёрнута локальная LLM, её также можно интегрировать с XDR. Настройка локальной LLM аналогична настройке любой коммерческой.

Состояние	☒
Режим ⓘ	KSN Custom
Базовый URL *	http://192.168.1.54:11434/v1
Ключ API *	Local-LLM
Модель *	phi3:latest
Максимальная длина запроса * ⓘ	400000
Дополнительные настройки ⓘ	Загрузить JSON-файл
Прокси-сервер	
Язык ответа	Русский English
Соединение	Проверить соединение
KIRA	Лицензионное соглашение (статус: принято)

Revision #6

Created 2026-08-05 07:22:25 UTC by Koala

Updated 2026-08-18 10:22:53 UTC by Koala