

Интеграция по реагированию KUMA и KEDR

Настройки на KUMA

На стороне KUMA. Если мы не хотим делать отдельные интеграции разделенные по Тенантам (подходит для MSSP), а одну общую интеграцию с KEDR, то нужно убрать галочку **Распределенное решение**:

Интеграция с Kaspersky Endpoint Detection and Response по тенантам



☒ Распределенное решение



Для подтверждения параметров интеграции вам нужно принять запрос на подключение от Kaspersky Unified Monitoring and Analysis Platform в справке.


☐ Выключено

*Адрес сервера

*Порт

*Внешний ID  



*Секрет  






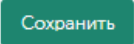
Задаем Адрес сервера и Порт, затем создаем Секрет для подключения к KEDR:

*Адрес сервера

*Порт

*Внешний ID  

*Секрет   


 Сохранить

Придумайте название Секрета и сгенерируйте закрытый ключ нажав на **значок Загрузки**.

Секрет

*Название

*Тип

*Файл сертификата 

*Закрытый ключ

Описание

Распакуйте архив, затем **загрузите Открытый ключ** (cert.pem) и **Закрытый ключ** (key.pem).

Секрет



*Название

*Тип

*Файл сертификата

*Закрытый ключ

Описание

Нажмите кнопку **Сохранить** для сохранения Секрета.

Затем снова на кнопку **Сохранить** для сохранения настроек Интеграции с KEDR.

Интеграция с Kaspersky Endpoint Detection and Response по тенантам

☐ Распределенное решение

Для подтверждения параметров интеграции вам нужно принять запрос на подключение от Kaspersky Unified Monitoring and Analysis Platform в веб-интерфейсе справки.

☐ Выключено

*Адрес сервера

*Порт

*Внешний ID

*Секрет

Сохранить

Настройки на KEDR

На стороне KEDR нужно залогиниться из под УЗ (с пролью администратора), по умолчанию это **Administrator**, перейти в раздел **Внешние системы**. Необходимо принять запрос от внешней системы (Внешний ID в настройках интеграции KUMA Должен совпадать с ID внешней системы в KEDR).

Мониторинг

Режим работы

Endpoint Agents

Отчеты

Параметры

Серверы Sensor

Серверы Sandbox

Внешние системы

Внешние системы

Отпечаток сертификата
Обрабатывать трафик с максимальным приоритетом

6F:8F:1C:63:4A:80:C3:3A:C6:63:3C:15:54:91:17:EB:95:CD:16:EC:C7:D3:54:78:DF:81:7B:0F:14:13:2D:C9

Включено

Список серверов

IP/Имя	Тип	Имя	ID	Отпечаток сертификата	Состояние	
10.68.85.15	Внешняя система	KWTS	c504e9f-0be8-491f-8a88-661d5193cf54	Отпечаток сертификата	Авторизован	Удалить
10.68.85.16	Почтовый сенсор "Лаборатории Касперского"	—		Отпечаток сертификата	Авторизован	Удалить
10.0.1.36	Внешняя система	KUMA	7c16eb14-5fa1-440c-9dad-dc82a0c85503	Отпечаток сертификата	Авторизован	Удалить
172.18.0.1	Внешняя система	KDS	e8295f19-43ca-4464-9b0d-a512f1d73067	Отпечаток сертификата	Авторизован	Удалить
10.0.1.70	Внешняя система	XDR	b39bab37-8238-11ee-b44d-76b6ebdc185b	Отпечаток сертификата	Авторизован	Удалить
10.0.1.70	Внешняя система	XDR-KUMA	f900719b-e635-4305-9e2b-0aceea70a52f	Отпечаток сертификата	Авторизован	Удалить
10.0.1.70	Внешняя система	System b39bab37-8238-11ee-b44d-76b6ebdc185b	b39bab37-8238-11ee-b44d-76b6ebdc185b	Отпечаток сертификата	Авторизован	Удалить
10.0.1.70	Внешняя система	System 2988edef-82e2-11ee-b44d-76b6ebdc185b	2988edef-82e2-11ee-b44d-76b6ebdc185b	Отпечаток сертификата	Авторизован	Удалить
10.0.1.70	Внешняя система	System e7e910cf-47b4-4e1e-ac83-8d43de3fa788	e7e910cf-47b4-4e1e-ac83-8d43de3fa788	Отпечаток сертификата	Ожидание	Принять Отклонить

Для удобства можно задать имя внешней системы в KEDR:

10.0.1.70

Внешняя система

System e7e910cf-47b4-4e1e-ac83-8d43de3fa788

e7e910cf-47b4-4e1e-ac83-8d43de3fa788

Интеграция завершена.

10.0.1.70

Внешняя система

TEST_KUMA

e7e910cf-47b4-4e1e-ac83-8d43de3fa788

Отпечаток сертификата

Авторизован

Удалить

Логирование работы с API на стороне CN (Central Node)

Зайти по ssh на сервер KATA/KEDR CN и выполнить команду:

```
[root@kata-cn-4 ~]# cat /var/log/kaspersky/apt-history/apt-history.log
2022-01-11 09:34:06.419690 info apt-history: EXTERNAL_SYSTEM=TEST_KUMA REQUEST_TIMESTAMP=2022-01-
```

11T09:34:06.418883: network isolation SET: host=14b22842-33d6-d3ef-3789-ef5108d6d411

rule={"autoTurnoffTimeoutInSec":180}

2022-01-11 09:36:15.200333 info apt-history: EXTERNAL_SYSTEM=TEST_KUMA REQUEST_TIMESTAMP=2022-01-

11T09:36:15.199826: network isolation DELETED: host=14b22842-33d6-d3ef-3789-ef5108d6d411

Revision #2

Created 29 November 2023 10:08:43 by Boris RZR

Updated 19 July 2024 14:37:44 by Koala