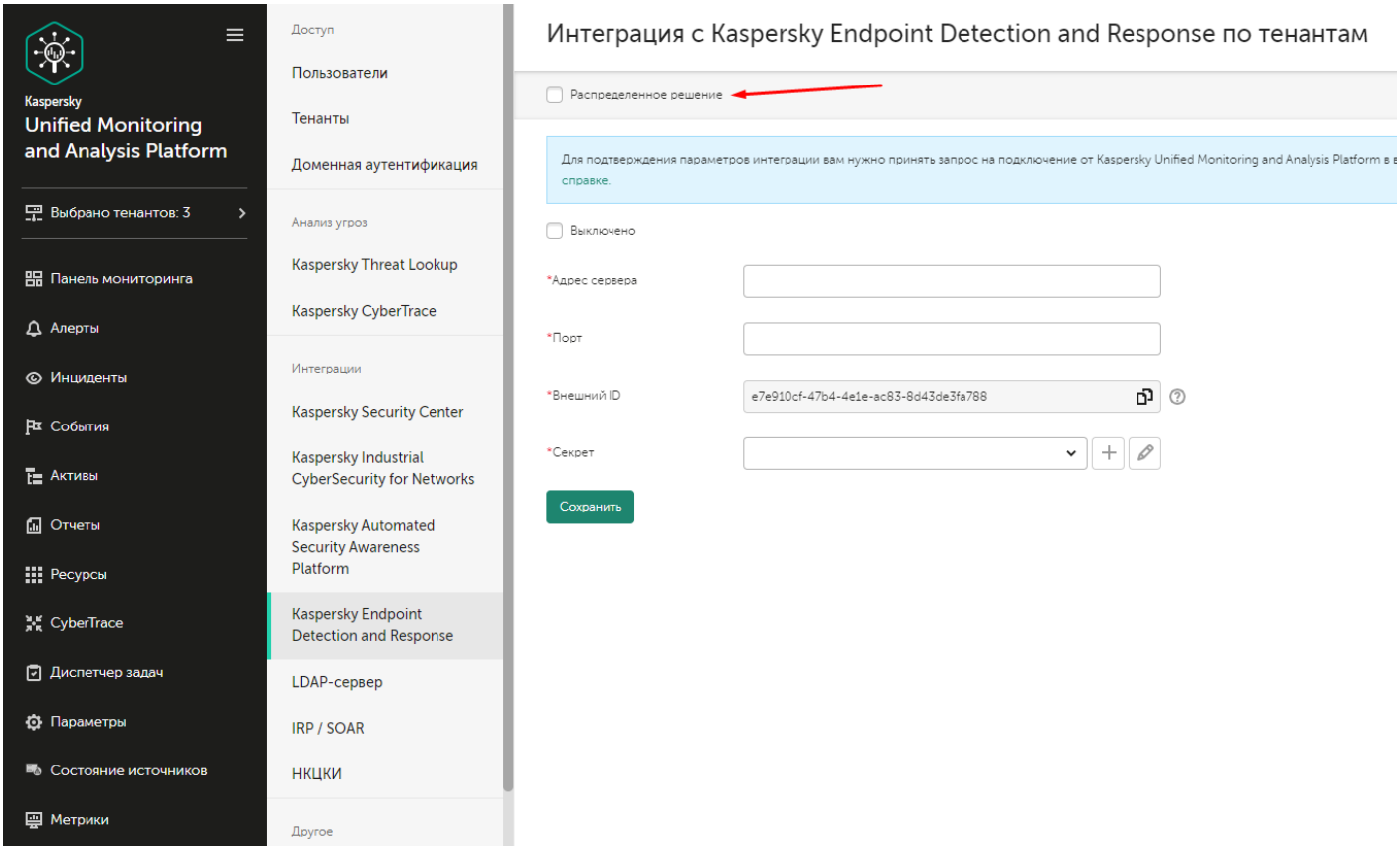
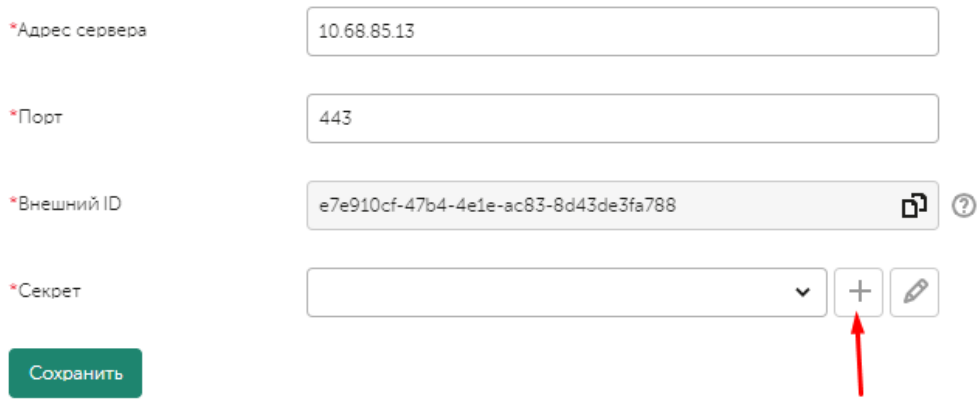
Интеграция по реагированию KUMA и KEDR

Настройки на KUMA

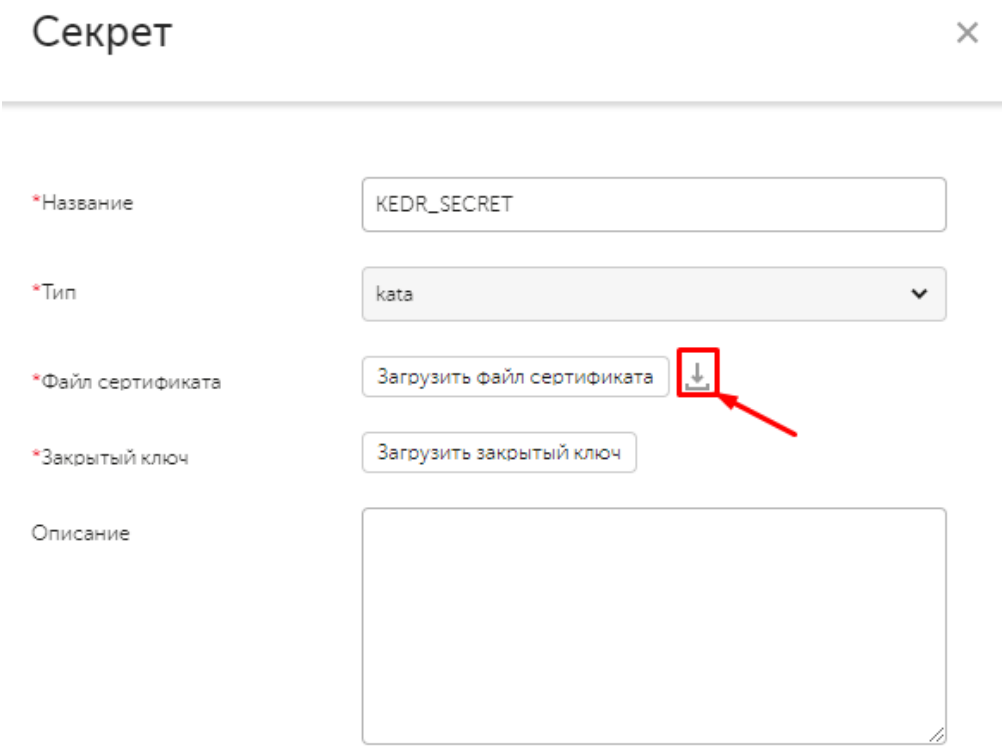
На стороне KUMA. Если мы не хотим делать отдельные интеграции разделенные по Тенантам (подходит для MSSP), а одну общую интеграцию с KEDR, то нужно убрать галочку **Распределенное решение**:



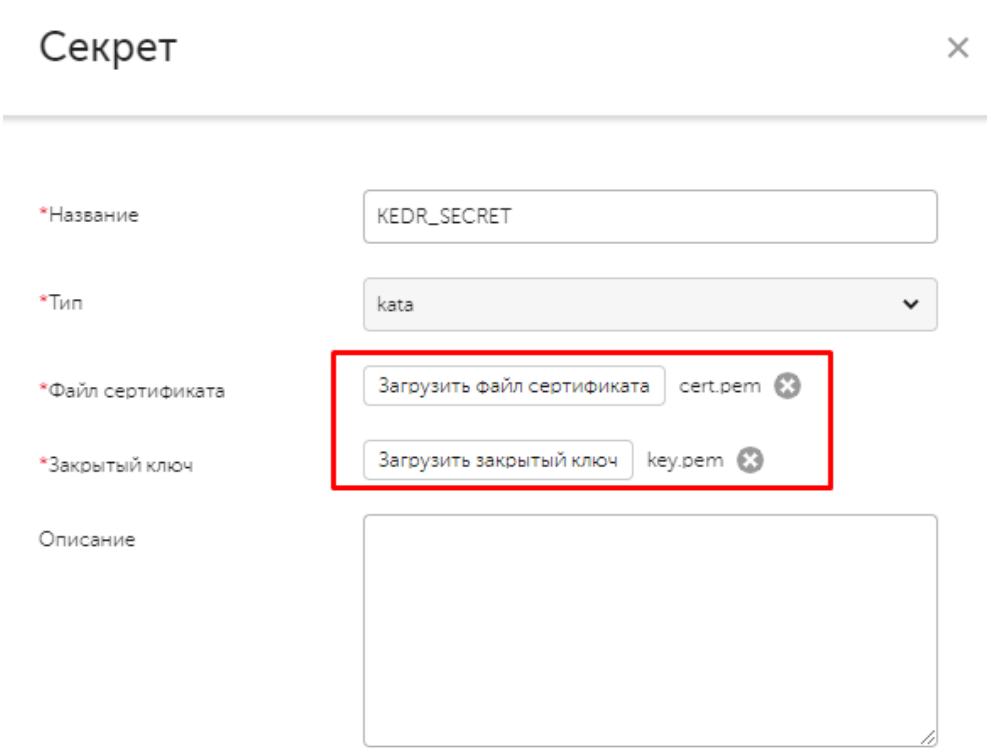
Задаем Адрес сервера и Порт, затем создаем Секрет для подключения к KEDR:



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

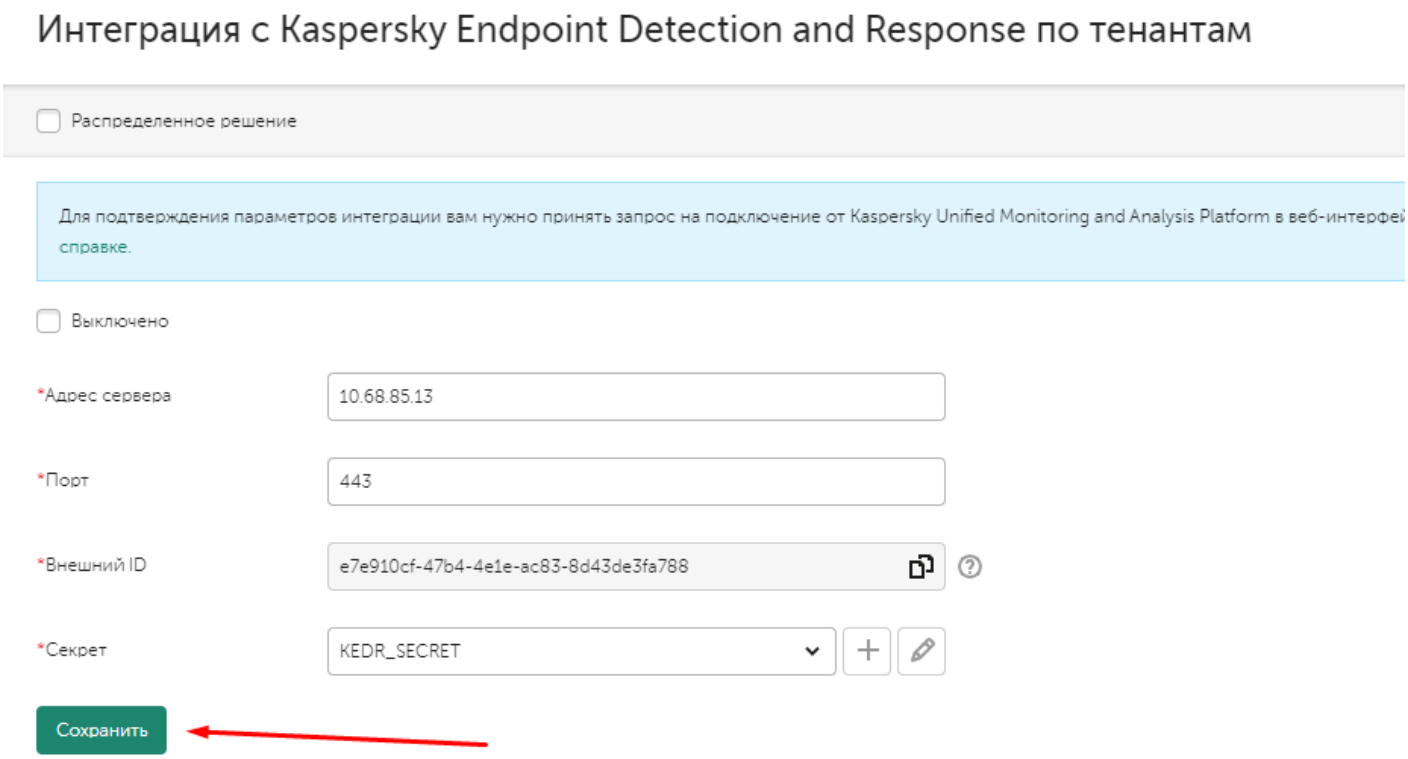


Распакуйте архив, затем **загрузите Открытый ключ** (cert.pem) и **Закрытый ключ** (key.pem).



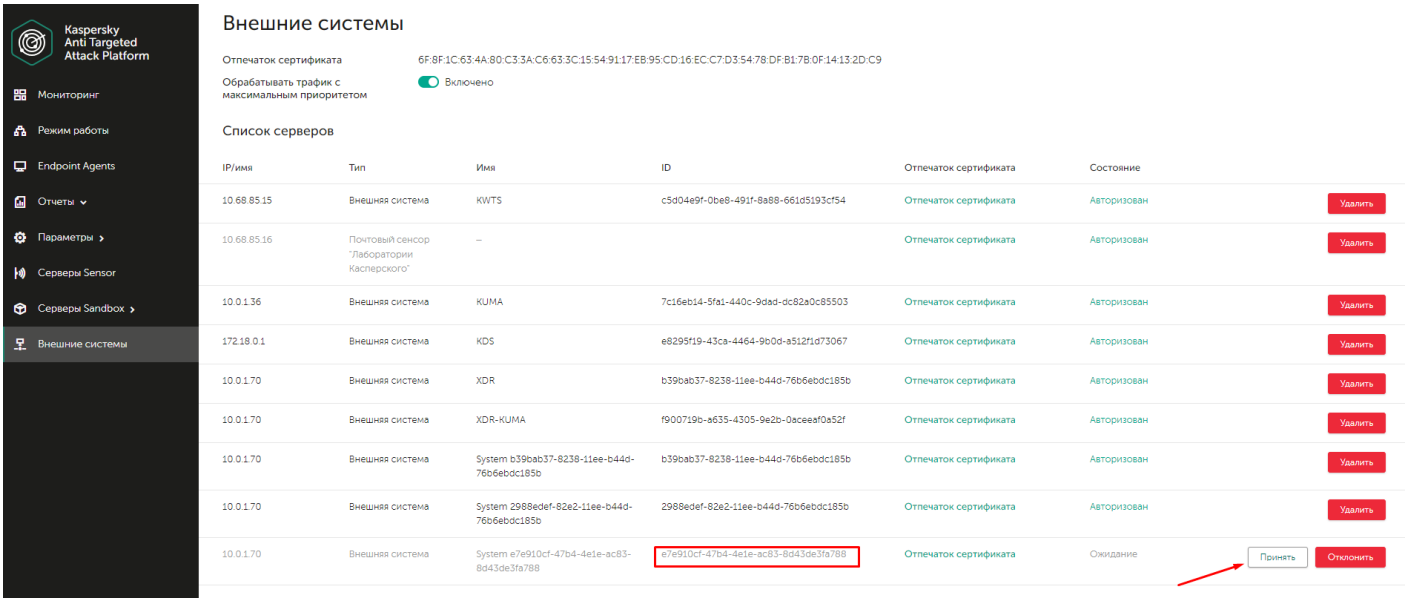
Нажмите кнопку **Сохранить** для сохранения Секрета.

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

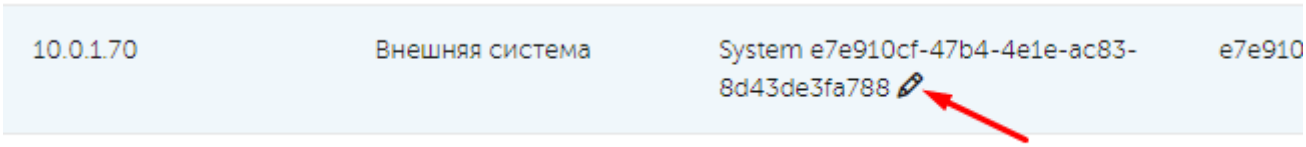


Настройки на KEDR

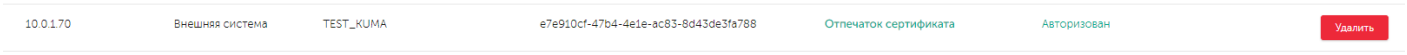
На стороне KEDR нужно залогинться из под УЗ (с пролью администратора), по умолчанию это **Administrator**, перейти в раздел **Внешние системы**. Необходимо принять запрос от внешней системы (Внешний ID в настройках интеграции KUMA Должен совпадать с ID внешней системы в KEDR).



Для удобства можно задать имя внешней системы в KEDR:



Интеграция завершена.



> Для работы кнопки реагирования KEDR: Полное доменное имя (FQDN) актива в KUMA должно совпадать со значением Хост в Активах KEDR (вход от Администраторской УЗ)

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 #3
Created 2023-11-29 10:08:43 UTC by Boris Rzr
Updated 2025-08-05 13:37:21 UTC by Boris Rzr