Интеграция с Kaspersky MDR

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **??** ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.6/settings/16340

Интеграция с Kaspersky MDR

Описание интеграции

?????????? ? Kaspersky Managed Detection and Response ????????? ????????????? ????????????? ????????? ?? ??????? MDR ? KUMA. ?????? ???????????? ?????????? API MDR, ???????? ????? ????????? ? ??????? ?????????????? ????????? ? KUMA ????? API.

Предварительные требования

1. Сетевой доступ

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

mdr.kaspersky.com ?? ????? **TCP/443**.

2. Настройка пользователя и токена в KUMA

? KUMA ???????? ???????????? ? ????? **Младший аналитик**, ???????????? ????? ??? ????????????? ?? API ? ????????? ?????? ? ????????? ??????? API:

- `POST /events`
- `POST /incidents/create`
- `POST /incidents/comment`
- `POST /incidents/close`

3. Генерация токена в консоли MDR

1. ????????? ? **Параметры → API**.

2. ??????? **Добавить** ? ??????? **Имя соединения**.

> ??? ??? ????? ???????????? ??? ??? ???????????? ??? ???????? ??????????, ???????????? ? ????????, ????????? ????? ??????? ?? ???????? ? ???????????? ????????????.

4. ? ???? **Роль пользователя** ???????? ???? **Администратор MDR**.
5. ? ???? **Тенант** ???????? ??????, ????????? ???????? ?????????? ????????????? ? KUMA.

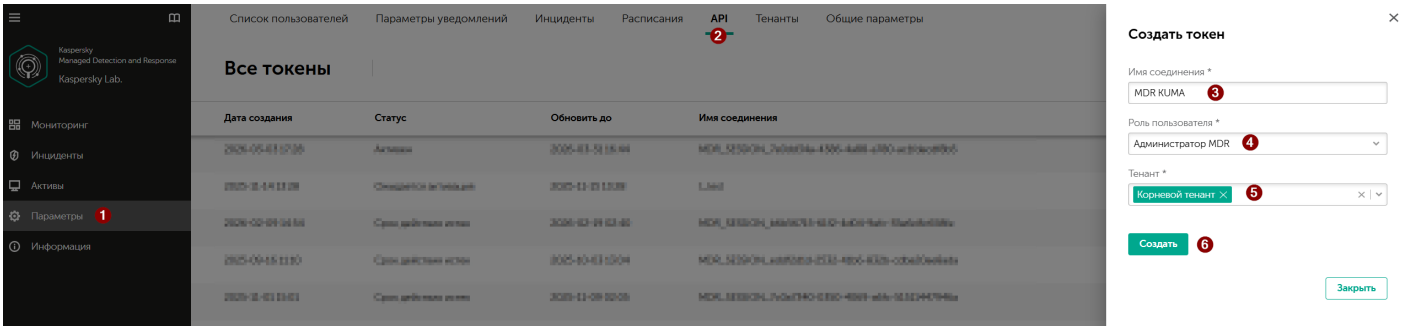
> ???? ??? ??????????, ???????????? ? ??????? MDR, ? ???? ?????? ???????????? ???????? — ??????? ? ???? ?????? ???????? «???????? ??????», ????? ?????? ?? ????????? ??? ?????????.

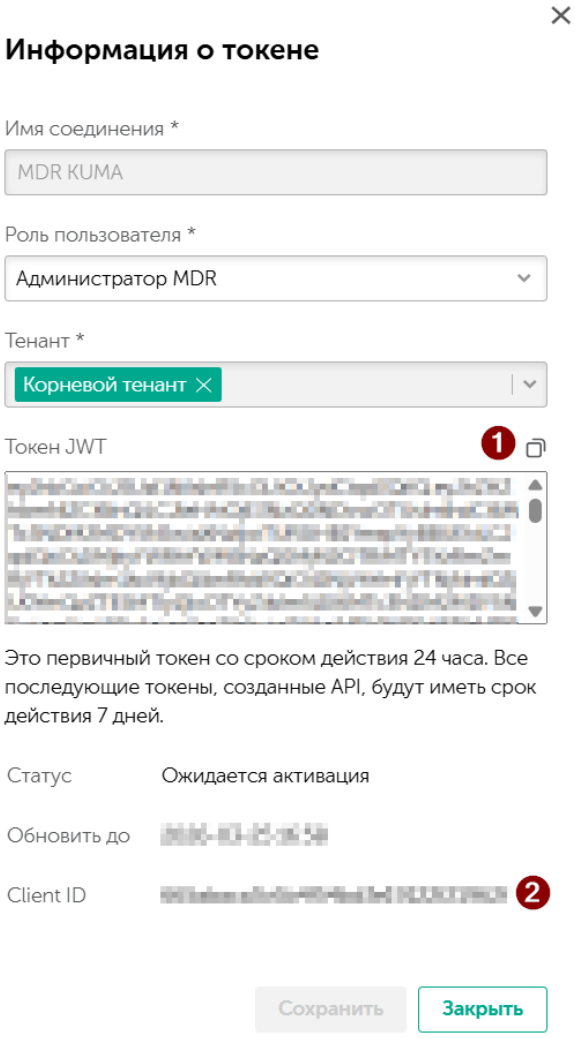
6. ??????? **Создать**.

? ?????????? ?? ????????:

- **JWT Token** (?? ?? `refresh_token`) — ??? ????????? ????? ?? ?????? ???????? 24 ???? . ?????? ????? ????????? ????????????, ????? ???????? ????? ???? `refresh_token` / `access_token`.
- **ClientID** — ????????????? ???????, ??????? ?????????? ????????? ??? ?????? ??????? ? API MDR.

????????? ??? ???????? — ??? ??????????? ?? ????? ?????????.





4. Загрузка репозитория

???????? ?????????? ??????????? MDR-integrations. ? ???????? ???????????? ?????:

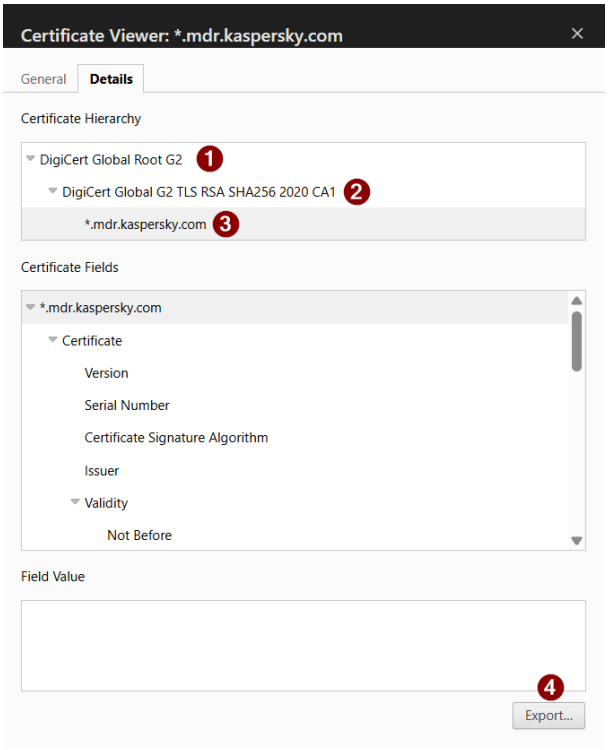
- ????????? ?????? ????? **mdr_integration** ????? ?????? https://download-directory.github.io/
- ??????????? ??????????? ???????? ?? ?????? KUMA:

```
git clone https://github.com/KUMA-Community/MDR-integrations.git
```

5. Получение цепочки сертификатов

????????? ?????????? ??????? ???????????? ??? **mdr.kaspersky.com** ? ??????? PEM. ??? ?????:

1. ???????? https://mdr.kaspersky.com ? ????????.
2. ??????????? ?????????? ? ??????????? ? ????????????? ??? ??????????? ??????? (??? ???????, 2–3 ?????).



4. ?????????? ?? ? ???? ???? ????????:

```
cat "DigiCert Global G2 TLS RSA SHA256 2020 CA1.crt" "DigiCert Global Root G2.crt" "_.mdr.kaspersky.crt" > mdr.pem
```

?????????? ???? `mdr.pem` ??????????? ?? ????? ?????????.

Настройка

Шаг 1. Размещение файлов на сервере

?????????? ????? **MDR-integrations-main.zip** ?? ?????? (??? ????????????? ??????????? — ?? ?????? Core) ? ?????????? ??? ? ????? `/opt`:

```
unzip MDR-integrations-main.zip -d /opt/
```

??????? ?????? ??????? ???????????:

```
mv /opt/MDR-integrations-main/mdr_integration /opt/
rm -rf /opt/MDR-integrations-main
```

Шаг 2. Создание файла конфигурации

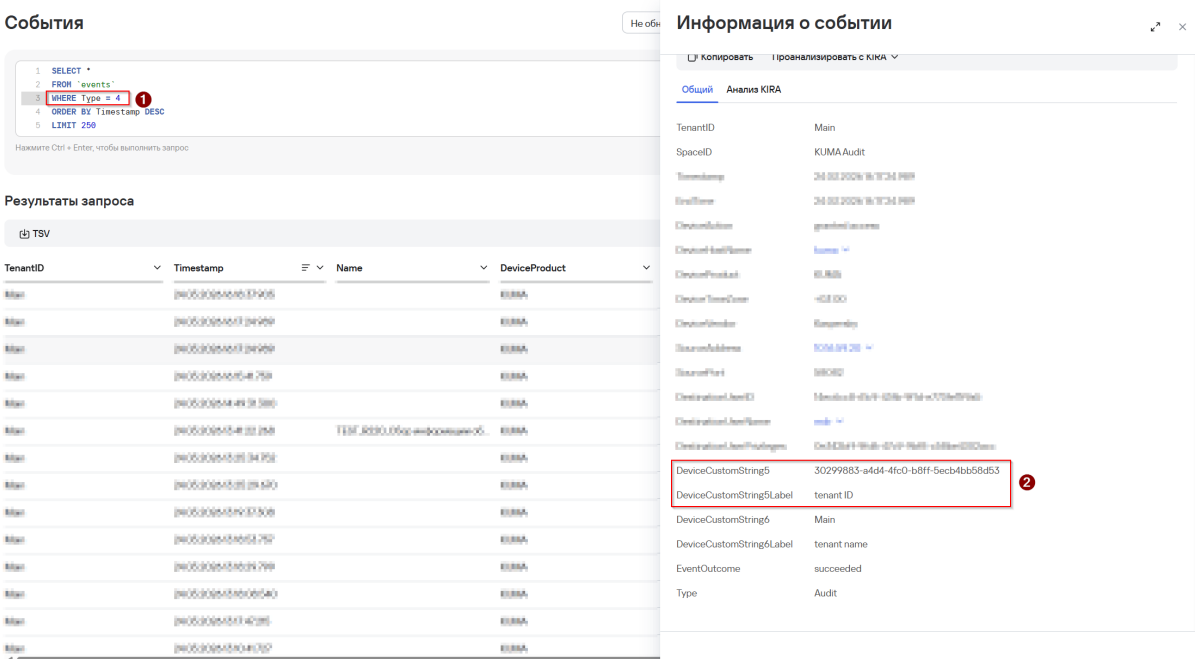
????????? ? ????? ? ????????????? ? ???????? ???? `config.yml` ?? ???????:

```
cd /opt/mdr_integration/conf
cp sample_config.yml config.yml
```

????????????? ???? `config.yml`:

- ? ?????? **General settings** ??????? `client_id` (???????? **ClientID** ?? ??????? MDR).
- ? ?????? **mdr_sync**:
  - ? ????? **modules** - **incident** ??? ????????? **enable** ??????? **true** ?????? **false**
  - ? ???? ?? ????? ??? ????????? **min_creation_time** ??????? ?????, ??????? ? ???????? ????????? ????????? ?????? ??????????
- ? ?????? **Modules settings → kuma** ???????:
  - `api_url` — FQDN ??? IP-????? ? ?????? API KUMA (?? ????????? ???? `7223`).
  - `api_token` — ?????, ?????????????? ??? ???????? ??????? ?????? ???????????? KUMA.
  - `tenant_id` — ????????????? ??????? KUMA, ? ??????? ????? ?????????? ?????????.

tenant_id ????? ???????? ?? ??????? ?????? KUMA.



?????????????? ??? ?????? thehive

-

```
#thehive:
#    api_url: http://127.0.0.1:9000
#    api_key: jB79oI4ywUY1jBae5CdDmp4oyeuq0Dha
#    ssl_cert: /opt/mdr/conf/thehive.pem  # full path
#    modules:
#        incident:
#            enable: false
#            timeout: 60  # default 60
```

Шаг 3. Настройка токенов

?????? ?????????? ??? ????? ???????:

- **`.refresh_token`** — ??????????? ??????? ???? ???. ??? **JWT Token**, ?????????? ? ??????? MDR ?? ????? ?????????????? ??????????.
- **`.access_token`** — ????????? ??????? **не нужно**. ??? ??????? ?????? ????????????? ?????????? `refresh_token` ?? ???? `access_token` + ??????????? `refresh_token` ????? MDR API ? ?????????? ?? ? ?????. ? ?????????? ??????? ??????? `TokenUpdater` ????????? ? ????????? ?????? ?????? 10 ?????.

???????? ??? ????? (`.access_token` ?????? ???? ??????):

```
touch /opt/mdr_integration/conf/.refresh_token
touch /opt/mdr_integration/conf/.access_token
```

???????? JWT Token ?? ??????? MDR ? ???? `.refresh_token`:

```
echo -n '????????_?????_?????' > /opt/mdr_integration/conf/.refresh_token
```

> **Важно:** ? ????? ????? ?? ?????? ???? ??????? ????? ?????? (`\n`) — ????? ????????????? ?????????? ???????. ???? `-n` ? ??????? `echo` ????????????? ??? ??????????. ???? ?? ???????? ????? ???????, ????????? ? ??? ????????????? ??????? ?????? ????? ??????:
>
> ```
> # ????????? ??????? ??????? ????? ?????? (????????? "1" ????????, ??? ?? ????)
> wc -l /opt/mdr_integration/conf/.refresh_token
>
> # ???? ????? "1 .refresh_token" — ??????? ??????
> perl -p -i -e 'chomp if eof' /opt/mdr_integration/conf/.refresh_token
>
> # ????????? ???????? (?????? ???? ????? "0 .refresh_token")
> wc -l /opt/mdr_integration/conf/.refresh_token
> ```

Шаг 4. Указание начальной точки сбора инцидентов

? ????? `.last_check` ??????? ?????? ???????, ??????? ? ???????? ????? ???????? ?????????. ???????? ???????? ? ????????????? (Unix timestamp × 1000, 13 ????).

??? ????????? ??????? ???????? ??????????? ???????:

```
# ??????: ???????? timestamp ??? 1 ?????? 2024 00:00:00
date -d "2024-01-01 00:00:00" +%s000
```

???????? ?????????? ???????? ? ????:

```
echo -n '1704060000000' > /opt/mdr_integration/conf/.last_check
```

> ??? ???????????? ??????? ?????, ????????? ?? ????????? ?????????? ????????? ? MDR.

Шаг 5. Обновление сертификата

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

Предварительные требования:

```
cp /path/to/mdr.pem /opt/mdr_integration/conf/mdr.pem
```

Шаг 6. Редактирование скрипта main.py

????????????? ????????? ?????? ? ??????? main.py:

```
#from src.integration_thehive import TheHive

#the_hive = TheHive(config)

#process_the_hive = multiprocessing.Process(target = the_hive.run, args=(logging_queue,
process_logging_configurer))

#process_the_hive.start()
```

Шаг 7. Проверка работоспособности

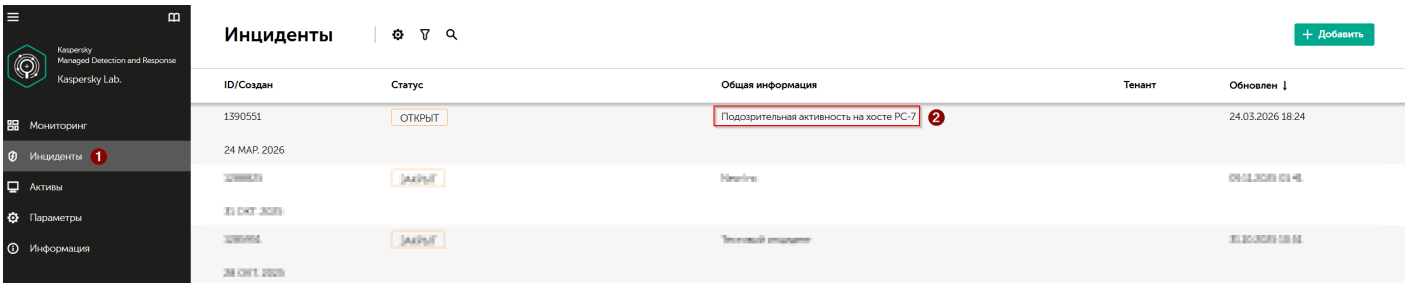
????????? ? ????? ?? ???????? ? ????????? ???:

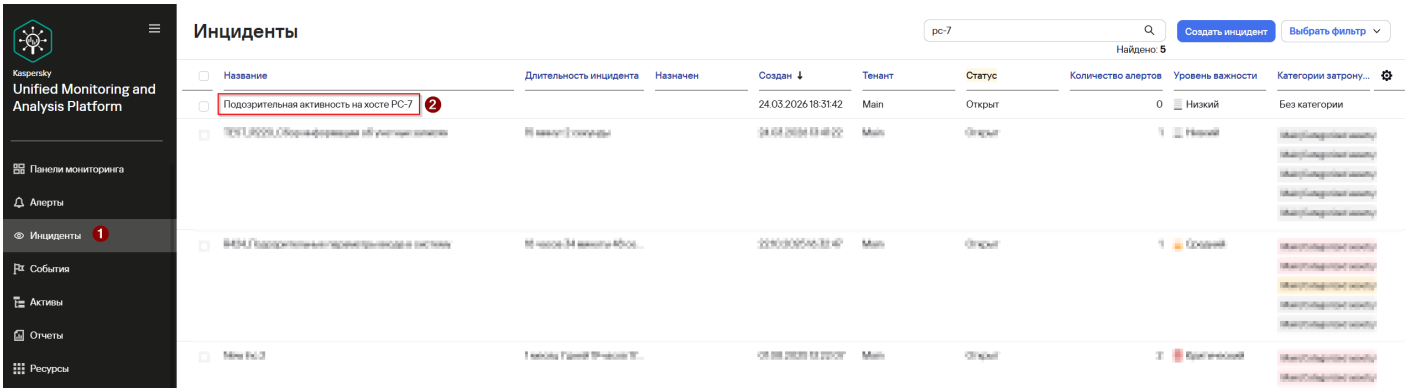
```
cd /opt/mdr_integration
python3 ./main.py
```

???? ??? ??????? ??????? ? ??????? ?????????? ?????? (????? ????????????? ? ?????????? ???????????), ?????? ?????????? ???????? ?????????. ??? ?????? ??????? ???????????? ?:

```
/opt/mdr_integration/log/app.log
```

?????????, ??? ????????? ?? ??????? MDR, ????????? ??????? ? ???????, ?????????? ? `.last_check`, ????????? ? KUMA.





????? ???????? ?????????? ?????? (`Ctrl+C`).

Шаг 7. Запуск в фоновом режиме

????????? ?????? ? ????:

```
nohup python3 /opt/mdr_integration/main.py &
```

? ???????? ???????????? ?? ?????? ????????? ?????? ??? ?????????? ? MDR, ??? ??????. ? ????? ?????? ??? 8 ????? ??????????.

Шаг 8. Автозапуск после перезагрузки

????????? ????????????? ?????? ??????? ????? cron:

```
sudo crontab -e
```

???????? ??????:

```
@reboot sleep 300 && python3 /opt/mdr_integration/main.py &
```

> ???????? sleep 300 (5 ?????) ??????????, ????? ?????? kuma-core ????? ?????????? ?? ?????? ?????? ???????.

Revision #10
Created 2026-03-24 13:00:37 UTC by Dmitry Borisov
Updated 2026-11-05 09:09:53 UTC by Dmitry Borisov