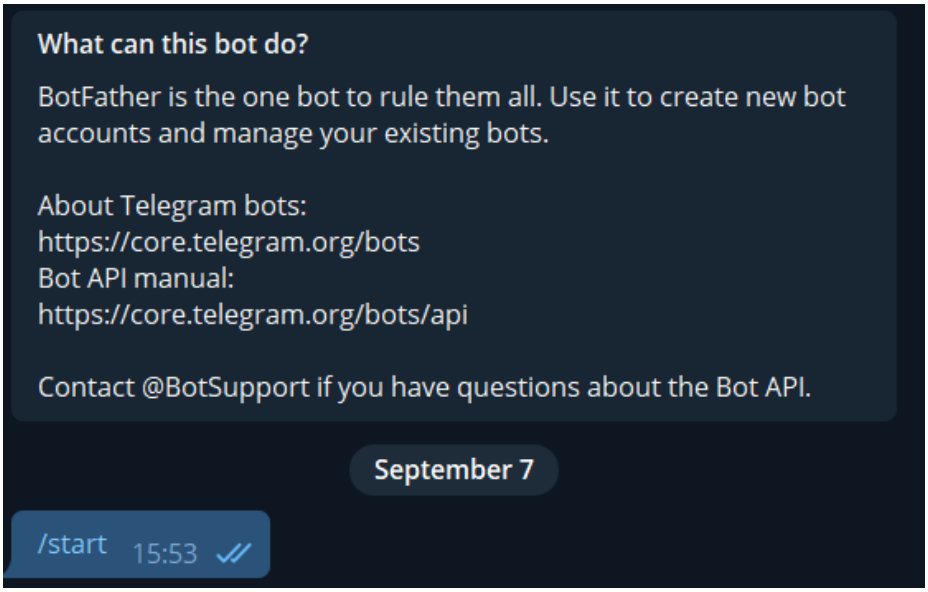
Отправка уведомления в телеграм-бот

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

Настройка Telegram

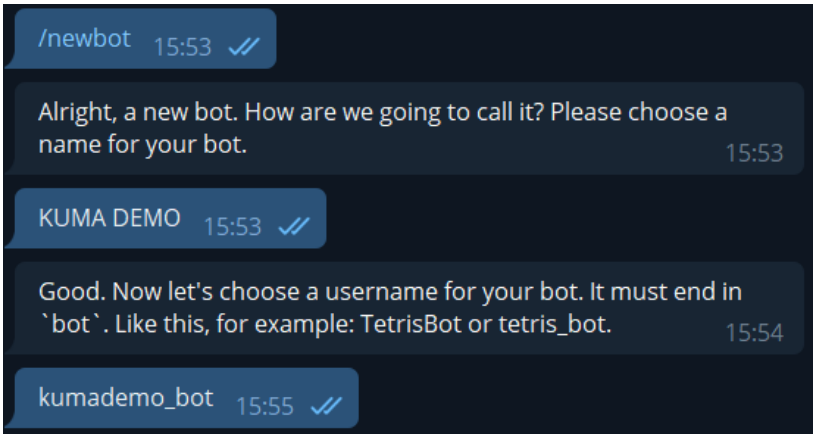
1. ? Telegram ??????? ????: https://t.me/BotFather

2. ????????? ???????? `/start`

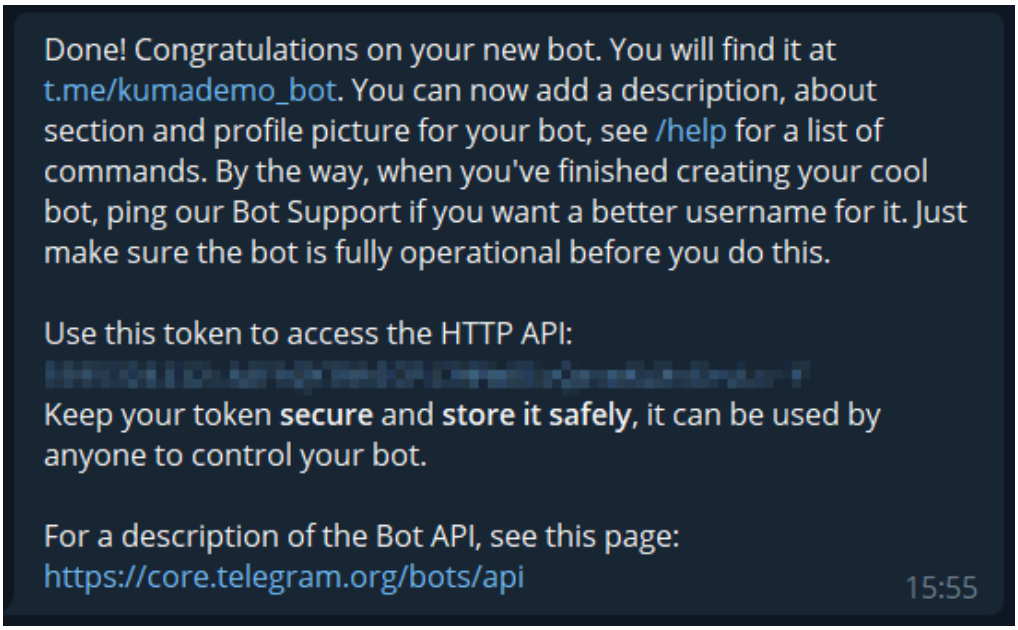


3. ??????? ?????? ???? ???????? `/newbot`

4. ?????? ???????? ??? ? ????? ???? (?????? ????????????? ?????? `bot`). ? ?????? ??????? ??? ???? "KUMA DEMO" ? ????? ???? "kumademo_bot".



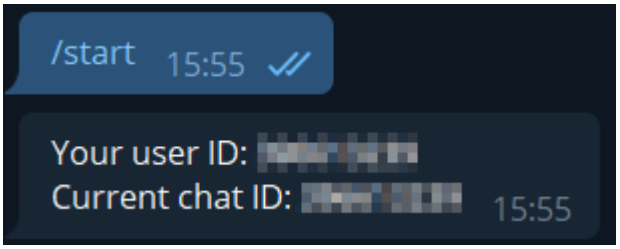
5. ?? ?????????? ???????? ????? ??? ????????? ? ???? ? ?????? ?? ????



6. ???? ?????????? ???????????? ???? ? ??????, ? ?? ? ?????? ??????????, ?? ?????????? ???????? ????????? ???????????. ??? ????? ?????? `/mybots`, ???????? ?????? ???? ?? ??????, ???????? Bot Settings, Group Privacy ? ???????? Turn off. ????? ????? ??? ?????? ?????????? ????????? ? ???????.

7. ????? ????????? ? ?????? ???? ?? ?????? ?????????? ?? BotFather ? ????????? ??????? /start ??? ??????? ????.

8. ??? ???????? ????????? ?????????? ???????????? ?????????? ?????? ?????? ? ?????, ? ????? ?????? chat_id ????? ????????????. ????? ?????? chat_id ???????????? ??????? ? ???? https://t.me/getmyid_bot ? ?????? ??????? `/start`. ?????????? ???????? chat_id ???????????? ? ?????????? ??? ???????? ????????? ?????



9. ????? ?????????? ????????? ????? ? ?????? ?????????? ?????? chat_id ???? ??????. ??? ????? ? ????????? ?????? ?????????? ?????????? ???? https://t.me/getmyid_bot ? ?? ??????? chat_id ?????? (? ???? Current chat ID), ??????? ???????????? ? ?????????? ??? ???????? ????????????. ????? ????????? id ???? ????? ??????? ?? ??????.

10. ?????? ????? ????????? ???????? ????????? ???? ?????? ? ?????? ???????? ???????:

```
https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test
```

????????? ?????? `<token>` ? `<chat_id>` ???????? ?????????? ?????. ? ?????????? ? ?????? ???? ??? ?????? (? ??????????? ?? ?????????? ???????) ?????? ????????? ???????????, ? ? ?????? ???????? JSON ?? ?????? ????????? ??????.



11. ????? ???????? ???????????????? ???? ????? ?????????? ? ????????? ???????? ???????????.

Скрипт уведомления

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

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

```
#!/bin/bash
set -eu
CHAT_ID=<chat_id ?? ?.8-9 ?????????? ???????>
TG_TOKEN=<token ?? ?.5 ?????????? ???????>
RULE=$1
TEXT="????????? ???????? ??????? <b>$RULE</b>"
curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML"
https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

? ??????, ???? ? ??????? ???????????? ???????????? ?????? ?????? ? ????????, ?????? ????? ????????????? ??????? ????? ??????-??????? ??? ??????? ? ????????

```
#!/bin/bash
set -eu
CHAT_ID=<chat_id ?? ?.8-9 ?????????? ???????>
TG_TOKEN=<token ?? ?.5 ?????????? ???????>
RULE=$1
TEXT="????????? ???????? ??????? <b>$RULE</b>"
PROXY=<????? ? ???? ??????-???????>
curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode
"parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

Еще один вариант скрипта

??? ???? ??????? ???????, ????? ? ???????? ????????? ???????? ????????? ???? *"{{.Timestamp}} | {{.Name}} | {{.DeviceHostName}}"*:

```
#!/bin/bash

set -eu
```

```
CHAT_ID=<chat_id ?? ?.8-9 ??????????? ???????>
TG_TOKEN=<token ?? ?.5 ??????????? ???????>

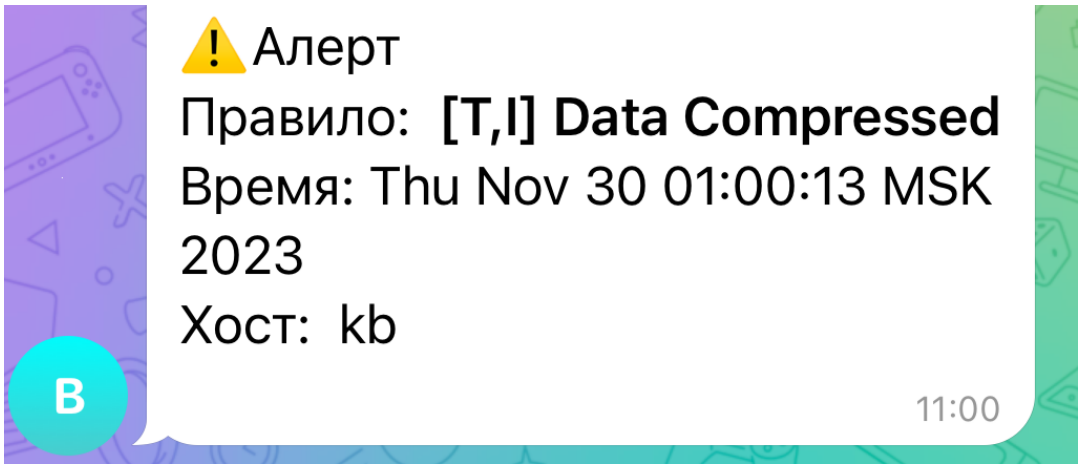
RULE=$1

# writing local log of arguments
echo $(date +"%d-%m-%Y %T.%3N") - $RULE >> /opt/kaspersky/kuma/correlator/0b9200ae-d5a9-41ce-bf7b-
c16814ed9524/scripts/bot.log

# escaping spec characters in argument except \s \|
RULE=$(echo $RULE | sed 's/[][\~`!@#$%^&*()=+{};:'"'"'"<>/?-]/\\&/g')

#try to beautify alert if arg is like "{{.Timestamp}} | {{.Name}} | {{.DeviceHostName}}"
{
    TIME=$(date -d @$(($(echo $RULE | cut -d "|" -f 1)/1000)))
    NAME=$(echo $RULE | cut -d "|" -f 2)
    HOST=$(echo $RULE | cut -d "|" -f 3)
    TEXT="??????? %0A???????: <b>$NAME</b> %0A?????: $TIME %0A????: $HOST"
} || {
#else if can't beautify
    TEXT="??????? %0A???????: <b>$NAME</b> %0"
}
    curl -XPOST
"https://api.telegram.org/bot$TG_TOKEN/sendMessage?chat_id=$CHAT_ID&text=$TEXT&parse_mode=html"
```

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



2. ????????? ?????? ? ????? ???????????, ???????????? ? ????????? ???????? ?????????? ?????????? ????? ????????-???

???? ??? ?????????? ???????

```
/opt/kaspersky/kuma/correlator/<id>/scripts/
```

`<id>` - ????????????? ????????????, ????? ????? ? ???-?????????? (??????)

3. ????????? ???????????? kuma ?????????? ????? ? ????? ????? ????? ?? ??????????

```
chown kuma:kuma /opt/kaspersky/kuma/correlator/<id>/scripts/bot.sh
chmod +x /opt/kaspersky/kuma/correlator/<id>/scripts/bot.sh
```

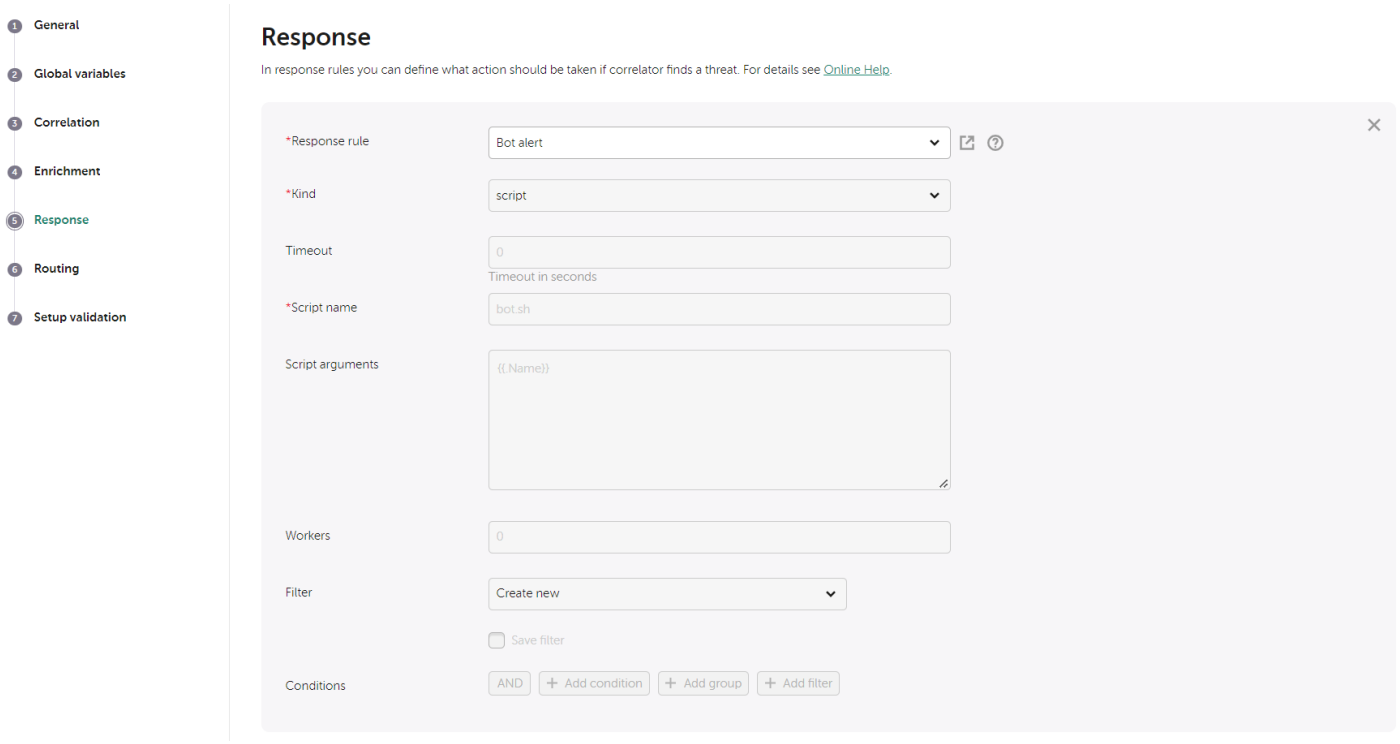
Настройка KUMA

1. ? ???-?????????? KUMA ????????? ?? ??????? **Resources**, ???????? **Response** ? ??????? ?? ?????? **Add Response**.

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

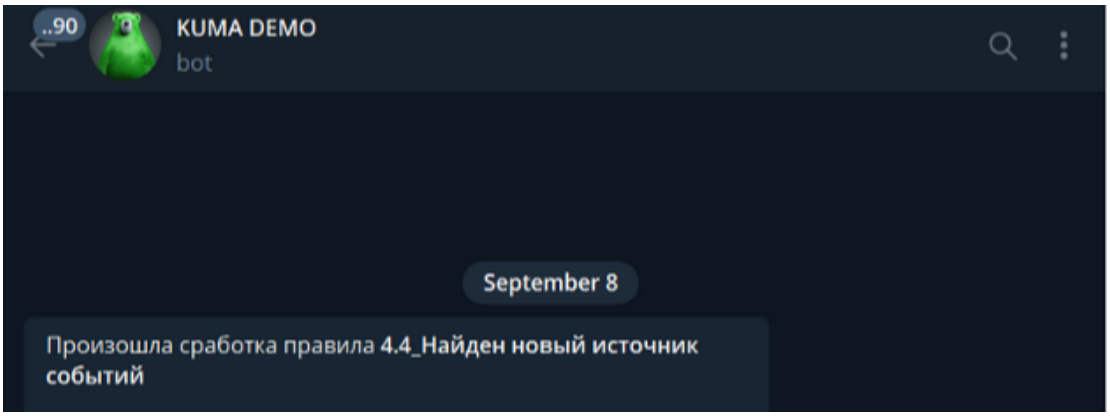
- ? ???? **Name** ??????? ??? ??????? ????????????.
- ??????? ??????.
- ? ???? **kind** ???????? **script**.
- ??????? ??? ??????? ? ???? **Script name**.
- ? ???????? ????????? ??????? **{{.Name}}** - ??? ? ???????? ????????? ?????????? ??????? ????? ???????????? ??? ??????????????? ???????.

3. ????? ????????? ? ????????? ???????????, ??????? ????? ????????? ???????????? ?? ??????? **Response** ??????? **Add** ? ?? ???????????? ?????? ???????? ????????? ????? ??????? ????????????.



4. ???????? ????????? ??????? ???????????

5. ????????? ?????? ??????? ??????????? ????



Revision #9
Created 2023-08-23 11:11:15 UTC by Koala
Updated 2024-07-19 14:37:44 UTC by Koala