

Отправка уведомления в телеграм-бот со ссылкой на KATA и KUMA

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Данный сценарий рекомендуется использовать **только в демонстрационных целях!** Правило корреляции из данного сценария написано с широким фильтром и на боевой инсталляции может генерировать большое число алертов!

Настройка Telegram

Настройки Telegram-бота, а также инструкции по импорту скрипта на коррелятор приведены в соответствующей [статье](#)

Скрипт уведомления

Скрипт отправки уведомления выглядит следующим образом:

```
#!/bin/bash
set -eu
CHAT_ID=<id чата>
TG_TOKEN=<токен>
KUMA_ASSETS="https://<KUMA_ADDR>:7220/assets/all?asset="
TEXT="В KATA обнаружен TAA-детект <b>$1</b> на хосте <a href='$KUMA_ASSETS$3'>$2</a>.%0AАлерт KATA доступен по <a href='$4'>ссылке</a>"

curl --data-urlencode "chat_id=$CHAT_ID" --data "text=$TEXT" --data-urlencode "parse_mode=HTML"
https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

Для работы скрипта необходимо задать следующие параметры:

- CHAT_ID - id чата или группы с ботом вместо <id чата>
- TG_TOKEN - токен бота вместо <token>
- KUMA_ASSETS - указать адрес KUMA (FQDN или IP) вместо <KUMA_ADDR>

Поместите скрипт в папку коррелятора, уведомления о сработках которого необходимо отправлять через телеграм-бот

Настройка KUMA

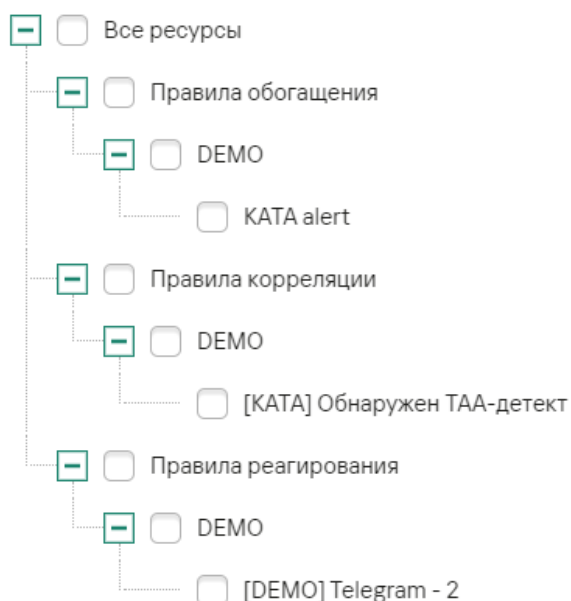
Для реализации предложенного сценария необходимо:

1. Импортировать в систему пакет ресурсов по [ссылке](#)

Состав и пароль от пакета ресурсов

Пароль для импорта: **Qwerty123!**

Состав пакета:



2. На коллекторе для сбора событий KATA применить правило обогащения из пакета **KATA alert** (или коробочный аналог **[OOTB] Kata Alert**)

3. На коррелятор привязать правило корреляции **[KATA] Обнаружен TAA-детект**

4. На коррелятор привязать правило реагирования **[DEMO] Telegram -2**

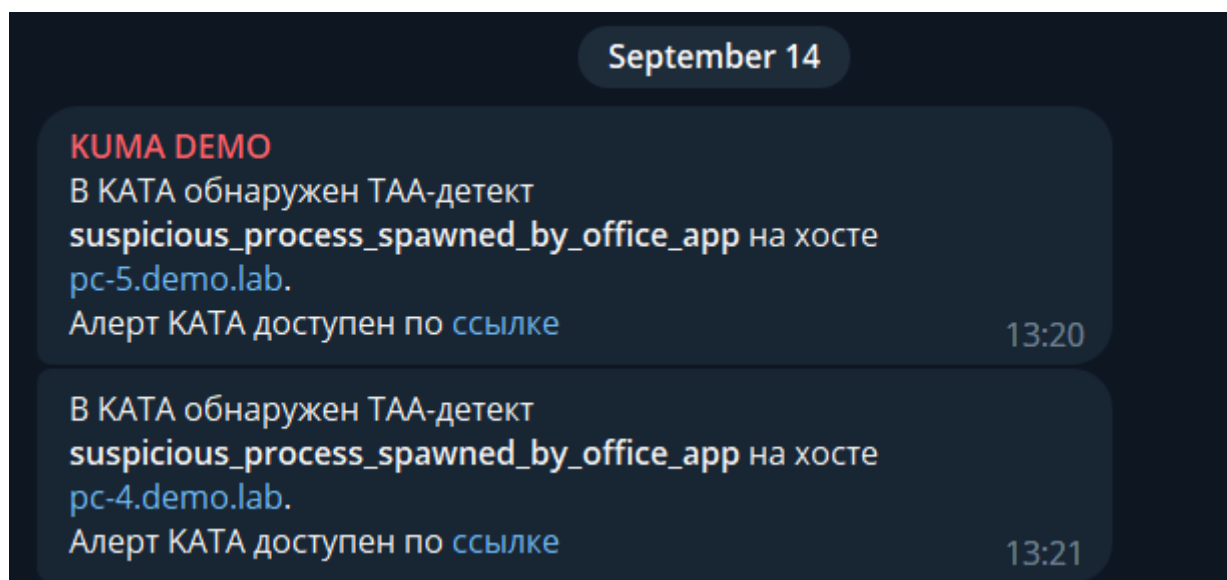
5. Выполнить обновление параметров сервисов коллектора и коррелятора.

Результат работы скрипта

1. Когда KATA возводит алерт по TAA-правилам, в KUMA срабатывает правило корреляции.
2. Корреляционное событие этого правила триггерит правило реагирования.
3. По правилу реагирования запускается скрипт отправки уведомлений в Телеграм.

Уведомление в телеграм содержит наименование TAA-детекта, FQDN-хоста, на котором была обнаружена активность (со ссылкой на активы KUMA), ссылку на соответствующий алерт в KATA.

Пример уведомления



Revision #4

Created 22 September 2023 14:24:14 by Koala

Updated 19 July 2024 14:37:44 by Koala