Оценка покрытия матрицы MITRE ATT&CK

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

?????? ??????-??????? «???????? ??????? MITRE ATT&CK»: https://support.kaspersky.ru/kuma/4.0/272743

???? ?? ?????? ??????? ???????? ??????? MITRE ATT&CK (https://attack.mitre.org/) ?????????????? ?????????, ????????????? ? KUMA («???????????» ?/??? ???????????????), ????????? ????????? ????:

- ????????? ?????????? ?????? MITRE ?? ???????????? ??????????? MITRE ATT&CK ? ???????????? ?????????? ?????? MITRE ? KUMA.
- ????????? ??????? MITRE ? ???????? ??????????.
- ????????????? ??????? ?????????? ? MITRE ATT&CK Navigator.
- ? ?????????? ?? ??????? ????????? ??????? ???????? ??????? MITRE ATT&CK.

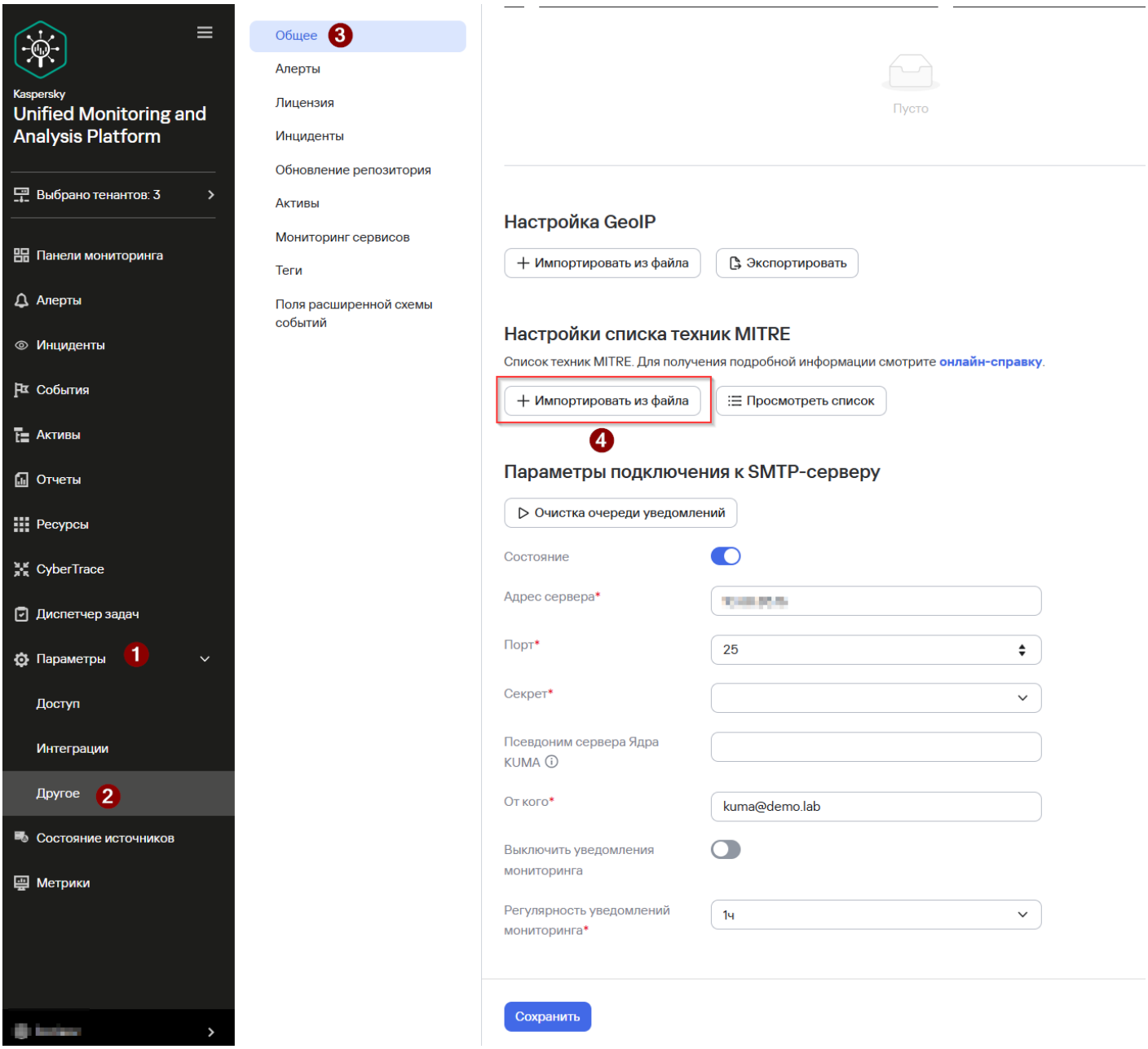
????????? ?????????? ?????? MITRE ????? ?? ???????????? ??????????? MITRE ATT&CK: https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json

KUMA ???????????? ?????? ?????? ?? ???????????? ?????? MITRE ATT&CK ?????? 14.1.

Импорт справочника техника MITRE

????? ????????????? ?????? ?????? MITRE ATT&CK:

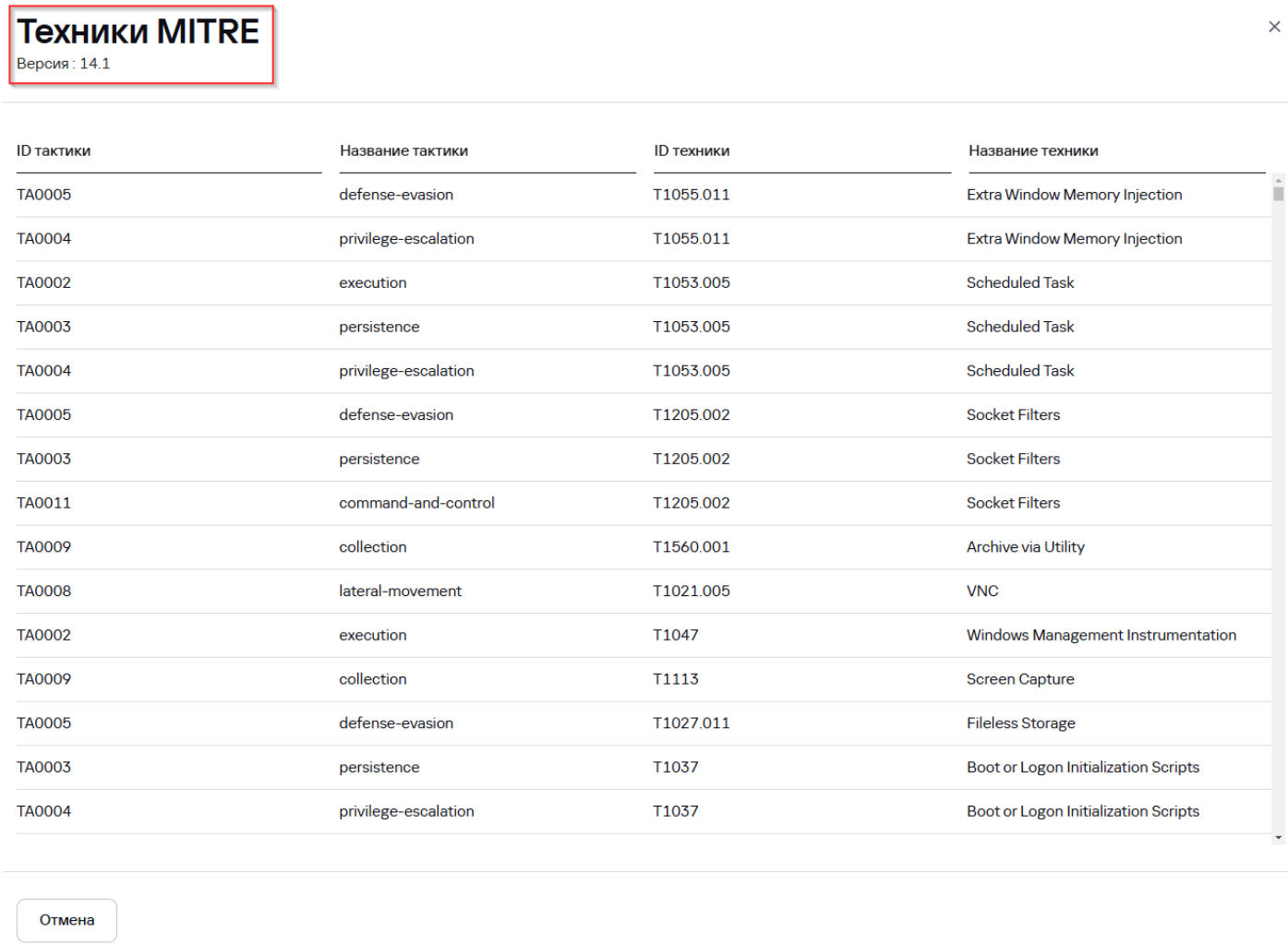
- ? ???-?????????? KUMA ????????? ? ?????? **Параметры** ? **Другое** ? **Общие**.
- ? ??????? **Настройки списка техник MITRE** ??????? ?? ?????? ????????????? ?? ?????.



- ? ???? ?????? ?????? ???????? ????????? ?????????? ?????? MITRE ATT&CK ? ??????? ?? ?????? **Открыть**.

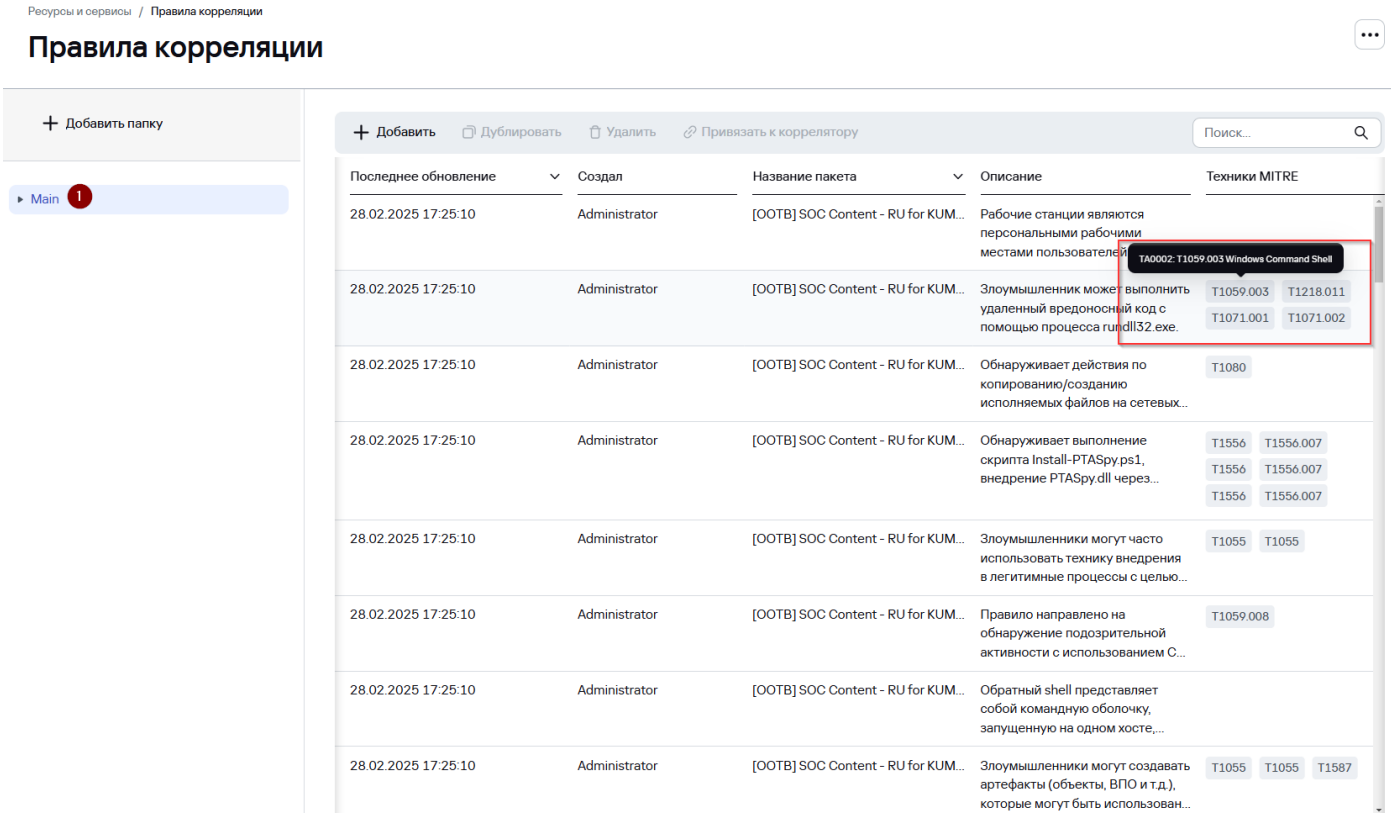
?????? ?????? MITRE ATT&CK ????? ???????????? ? KUMA. ?? ?????? ??????? ?????? ?????????????? ?????? ? ?????? ?????????? ?????? MITRE ATT&CK, ????? ?? ??????

Просмотреть список.



????? ????????? ??????????? ?????? ?????? MITRE ATT&CK ??? «??????????» ?????? ?????????? [OOTB] SOC Content - RU for KUMA 3.2:

- ????????? ? **Ресурсы** ? **Правила корреляции** ? ???????? ????? ????? **Main**.
- ?????????, ??? ? ??????? **Техники MITRE** ???????????? **ID Техники**.

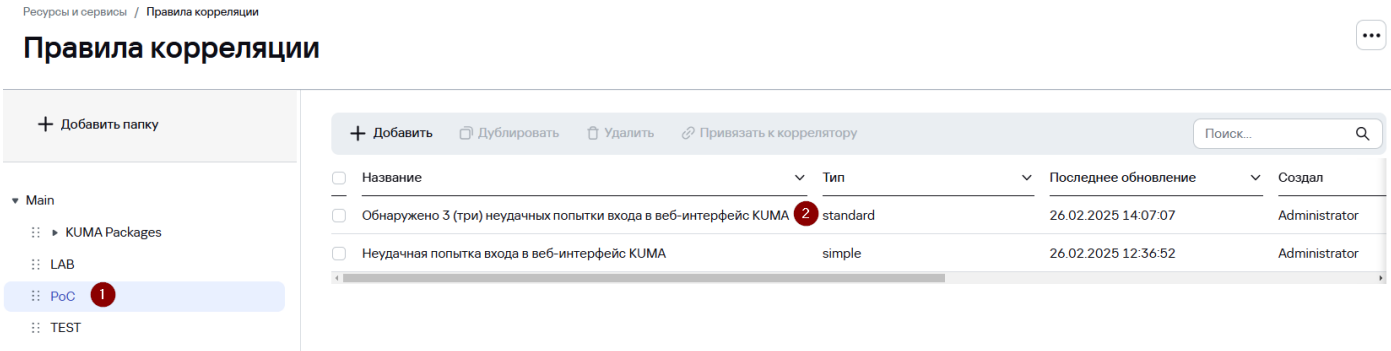


- ???? ??????? **Техники MITRE** ???????? ??????, ????????? ????????? ?????? ?????? **[OOTB] SOC Content - RU for KUMA 3.2** ?? ??????????? (??. ?????? ?????? ???????? ?? ???????????).

Привязка техник MITRE к правилам корреляции

????? ????????? ??????? MITRE ATT&CK ? ???????? ?????????? (?? ??????? ?????????? ??????? ?????????? ?? ??????? ???????? ??????? ????????? Standard):

- ? ???-?????????? KUMA ????????? ? ?????? **Ресурсы** ? **Правила корреляции**.
- ? ?????? ????? ???????? ????? ????????? ????? ??? ??????????????? ?????? ?????????? ? ???????? ???? ????????????? ??????? ??????????, ????? ?? ??? ??????? ??????????.

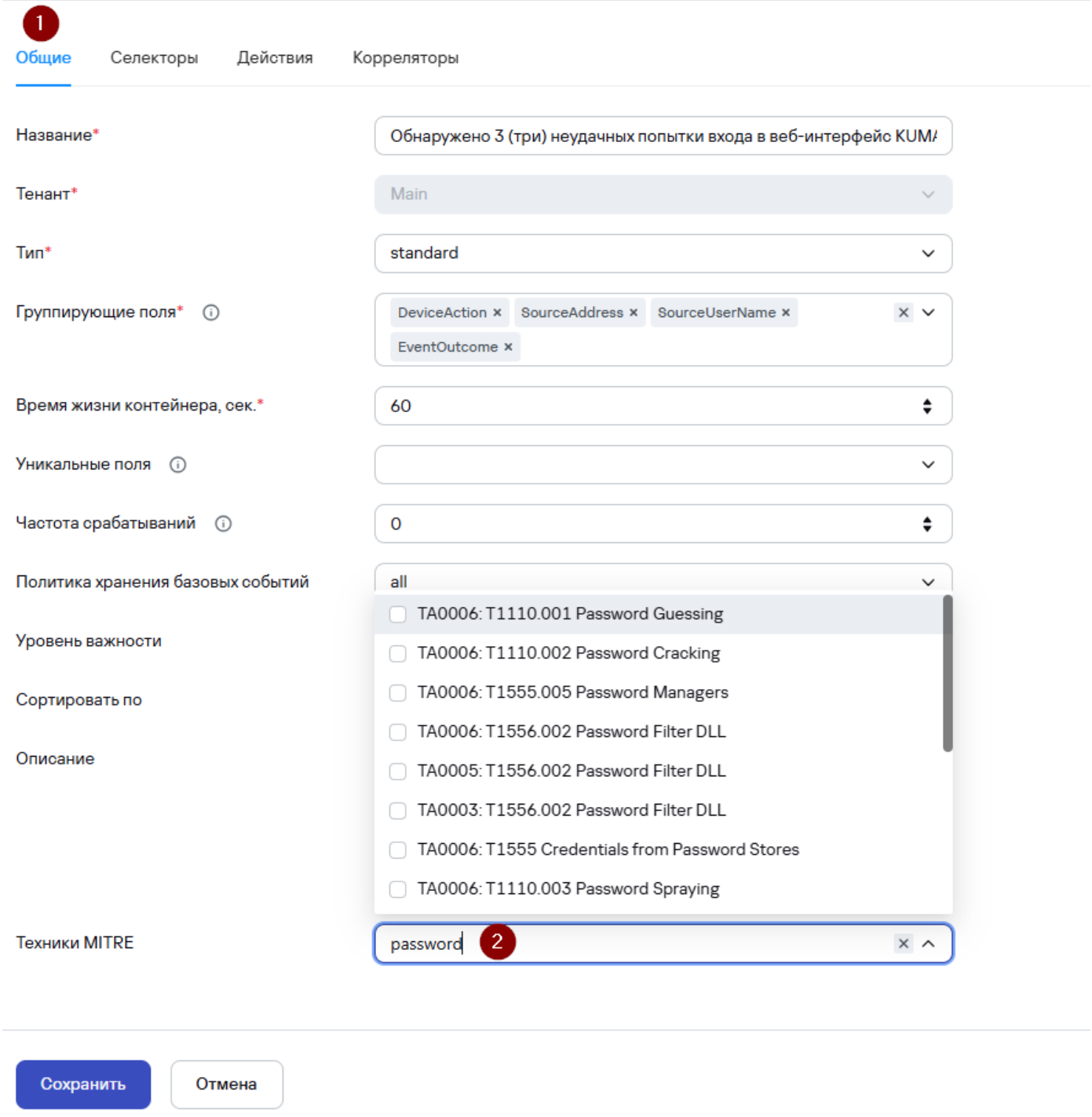


- ? ???? ????????????? ??????? ?????????? ?? ??????? **Общие** ??????? ?? ????

  Техники MITRE ????????? ?????? ????????? ??????.
- ??? ???????? ?????? ???????? ??????: ? ???? ????? ?????? ???????? ???????, ID ??????? ??? ???????. ??? ???????? ? ??????? ?????????? ???????? ???? ??? ????????? ?????? MITRE ATT&CK. ??? ??? ????????? ??????? ????????? ? ??????? Brute Force ? ???????????? ???????????? ??????? ????????? ?????? ??????? ? ???? ???-???????

  Password Guessing (https://attack.mitre.org/techniques/T1110/001/).

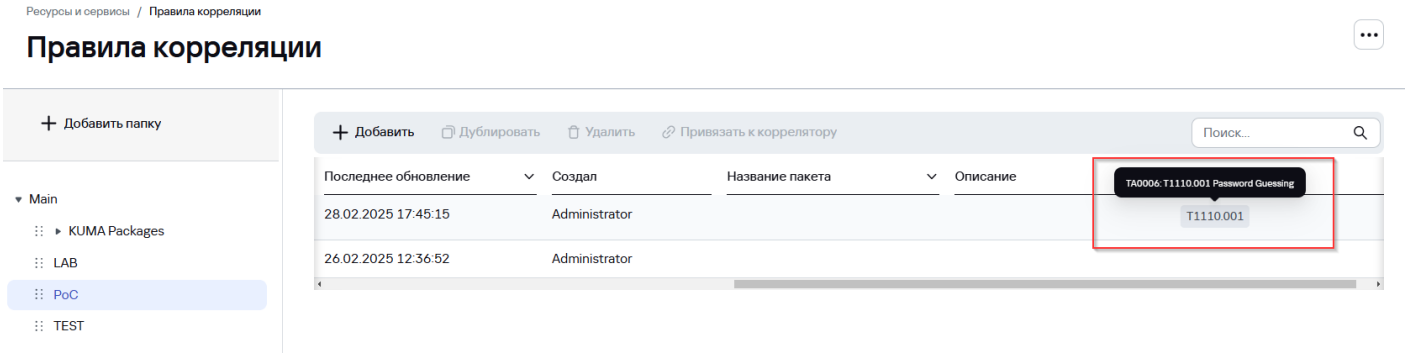
Редактирование правила корреляции



- ??????? ?? ?????? **Сохранить**.

??????? MITRE ATT&CK ????? ????????? ? ??????? ??????????. ?????????, ??? ? ???????

Техники MITRE ???????????? **ID Техники.**

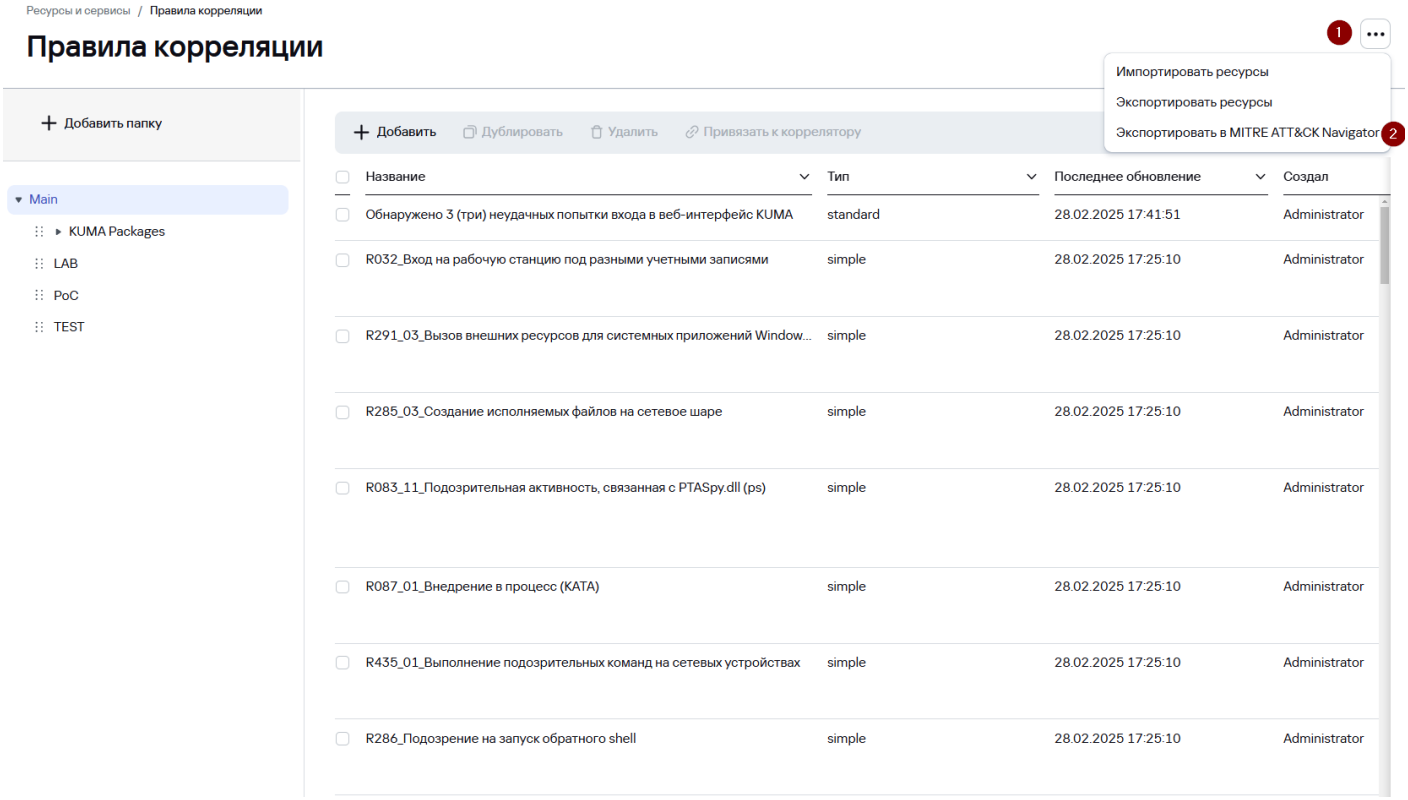


Экспорт правил корреляции в MITRE ATT&CK Navigator

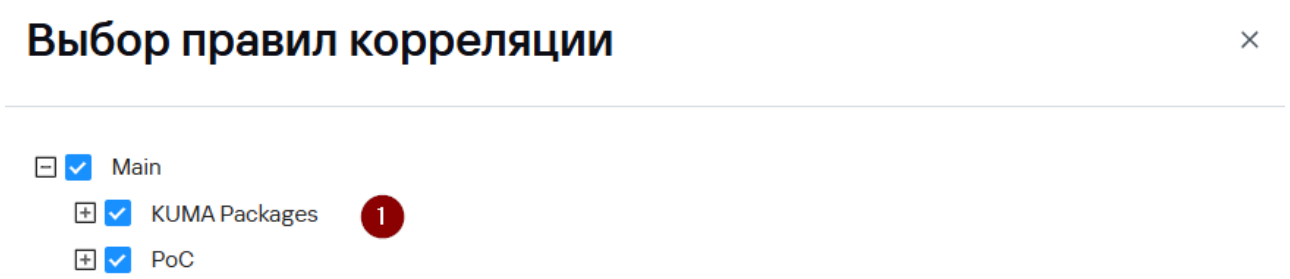
????? ??????? ???????? ??????? MITRE ATT&CK ?????????????? ?????????, ????????????? ? KUMA («???????????» ?/??? ??????????????????), ????????? ????????? ????:

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

- ? ???-?????????? KUMA ????????? ? ?????? **Ресурсы** ? **Правила корреляции.**
- ? ?????? ??????? ???? ??????? ?? ?????? .
- ? ?????????????? ?????? ??????? ?? ?????? **Экспортировать в MITRE ATT&CK Navigator**.

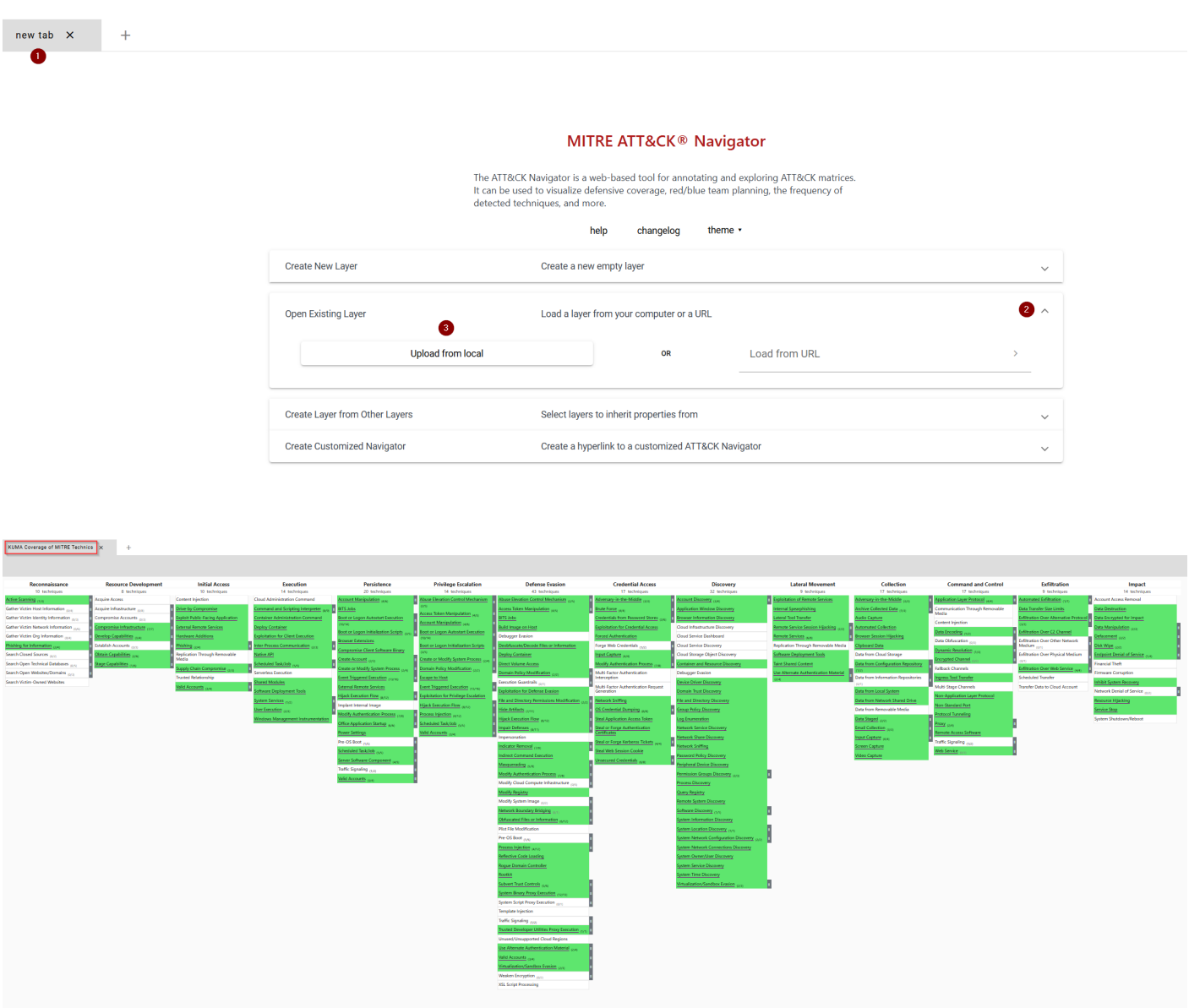


- ? ??????????? ???? ???????? ??????? ???????????, ??????? ?? ?????? ????????????? (???????? ??? ??? ?????? ???????? ????? ??????? ???????????).

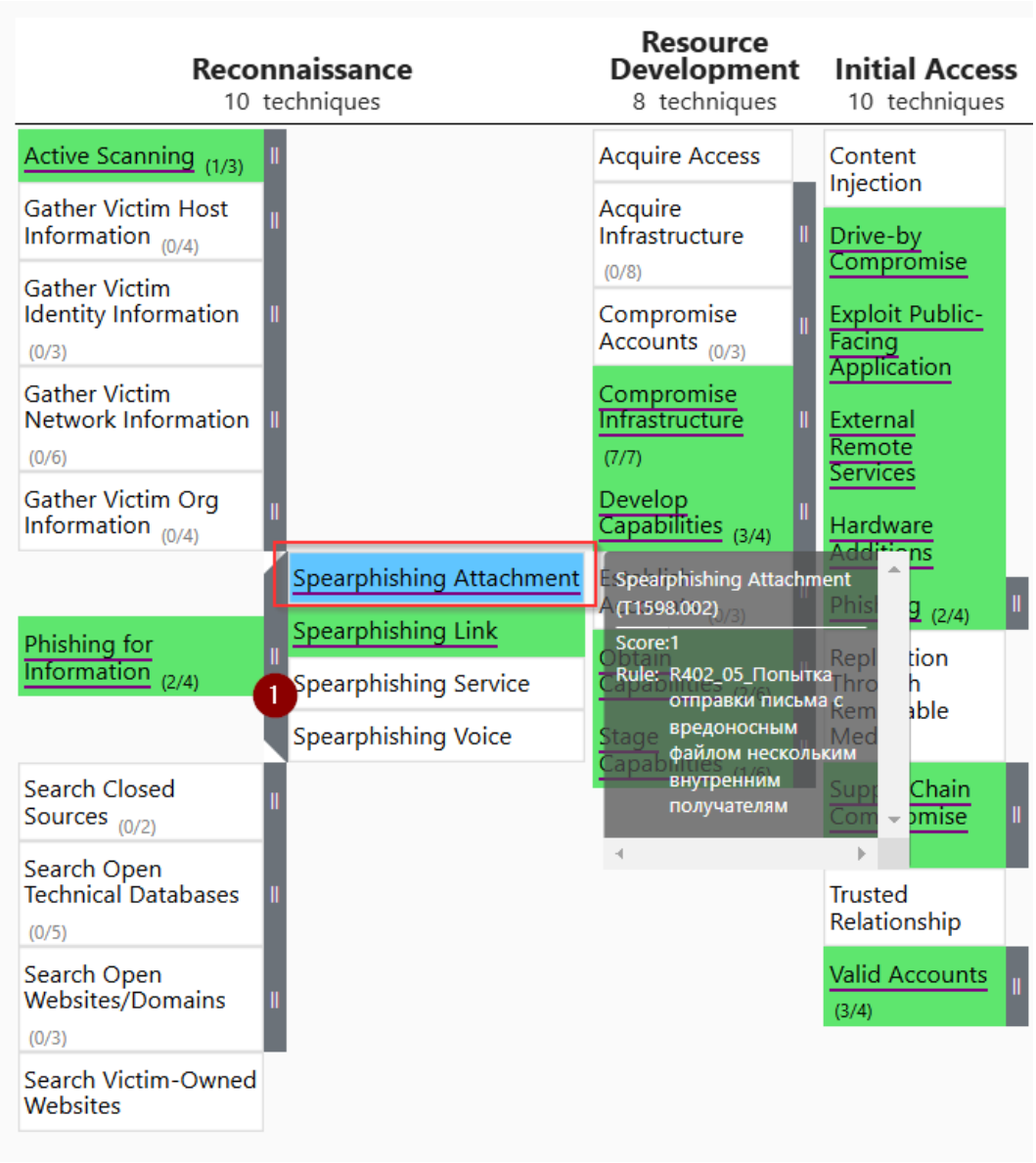


??????? ?? ?????? **OK**.

- ???? ? ???????????????? ????????? ????? ???????? ?? ??? ????????? ? ??????? json.
- ????????? ???? ? ?????? ??????????? ? MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) ??? ?????? ???????? ??????? MITRE ATT&CK.


new tab
1
MITRE ATT&CK® Navigator
The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices.
It can be used to visualize defensive coverage, red/blue team planning, the frequency of
detected techniques, and more.
help
changelog
theme
Create New Layer
Create a new empty layer
Open Existing Layer
Load a layer from your computer or a URL
2
3
Upload from local
OR
Load from URL
Create Layer from Other Layers
Select layers to inherit properties from
Create Customized Navigator
Create a hyperlink to a customized ATT&CK Navigator

? ?????????? ????? ?????????? ???????? MITRE ATT&CK. ??? ????????? ??????? ?? ?????????? ??????? ??? ???-??????? ????? ??????????, ??????????? ?? ???????.



Revision #2

Created 2026-08-07 16:55:38 UTC by Dmitry Borisov

Updated 2026-08-07 17:21:00 UTC by Dmitry Borisov