



Как создавать правила для MaxPatrol SIEM, чтобы они точно работали



Кирилл Кирьянов

Старший специалист PT Expert Security Center



Антон Кутепов

Старший специалист PT Expert Security Center

ptsecurity.com

Если хотя бы однажды:

- Вы долго искали правило, которое написали где-то в блокноте или какой-либо SIEM-системе
- Не могли понять, кто и когда написал или изменил правило
- Много времени тратили на проверку работоспособности правила
- Испыывали трудности с доставкой контента в продукт
- Испыывали трудности с хранением различных версий одного и того же правила

Тогда этот вебинар для вас ;)

Процессы и инструменты

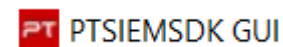


Элементы SDLC (заимствуем только последние три этапа):

- Этап 4: Создание или разработка продукта -> Создание правил
- Этап 5: Тестирование продукта -> Запуск тестов для правил
- Этап 6: Развертывание и сопровождение -> Создание установочного пакета с контентом

Инструментарий для разработки ПО:

- Использование системы контроля версий (Git)
- Использование единой среды разработки (IDE)



В будущем:

- Непрерывное тестирование и поставка результата (CI/CD)



Создание Git-репозитория из БД РТКВ

Подготовка репозитория

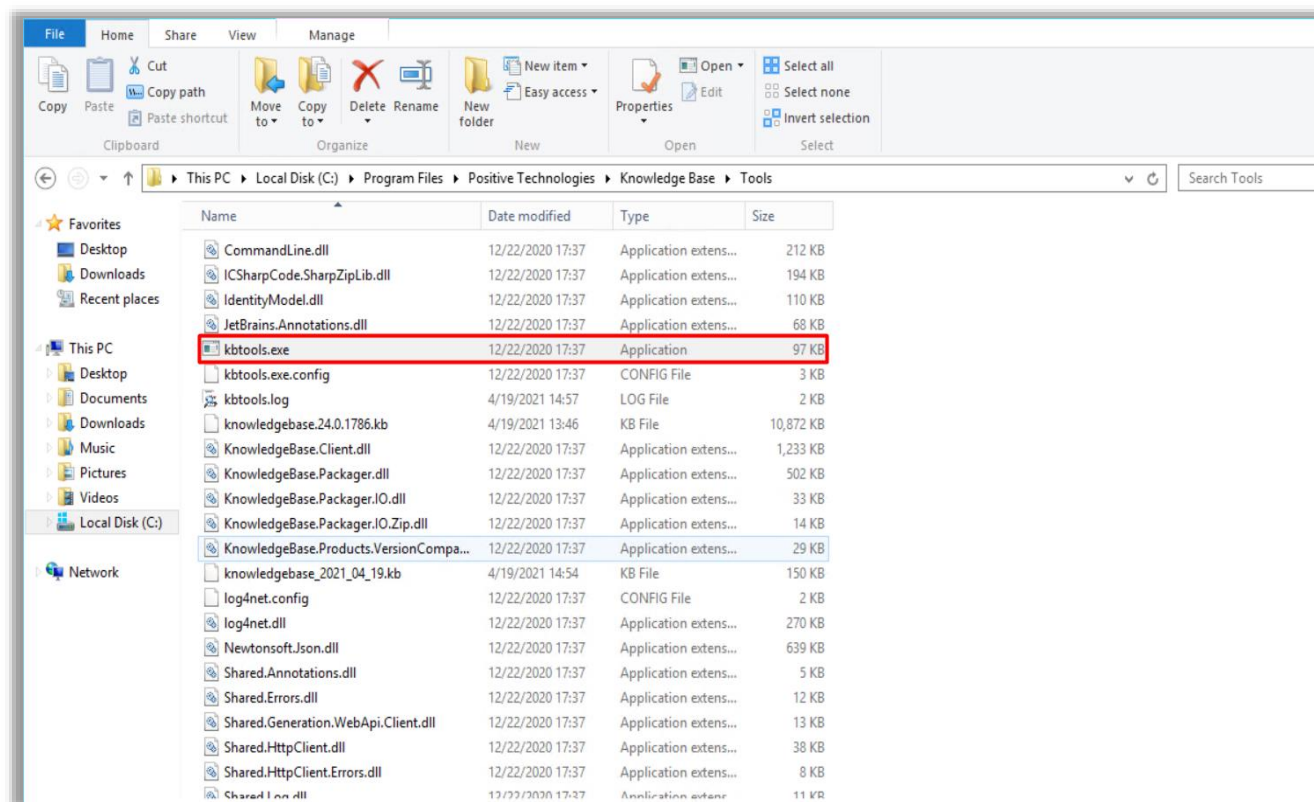


Основные этапы подготовки окружения:

- Скачать утилиту для конвертации пакетов *kbtools.exe*
- Конвертировать и выгрузить контент из MaxPatrol SIEM
- Создать Git-репозиторий и необходимые ветки
- Загрузить контент в систему контроля версий

Где взять утилиту для создания и распаковки пакетов KB?

Скачать утилиту для конвертации можно с сервера MP SIEM по пути *C:\Program Files\Positive Technologies\Knowledge Base\Tools* (забираем полное содержимое папки)



Примеры использования утилиты kbtools.exe

Распаковка пакета KB (необходимо использовать полные пути до файлов):

```
C:\Webinars\kbtools
λ kbtools.exe unpack -s C:\Webinars\knowledgebase_2021_06_03.kb -o C:\Webinars\repo
Unpacking the knowledge base package into source format
Unpacking the knowledge base package into source format completed successfully
```

Сборка пакета KB:

```
C:\Webinars\kbtools
λ kbtools.exe pack -s C:\Webinars\repo -o C:\Webinars\repo.kb
Creating a knowledge base package
Search the Origins in the source content.
The Origins was found.
Search the Taxonomy in the source content.
The Taxonomy was found.
Search for event categories in the source content.
Event categories was found.
Search the Rules Filters in the source content.
Total found 40 Rules Filters
Search the Rule filter tags in the source content.
Rule filter tags was found.
```


Система контроля версий

Предлагается использовать open source платформу GitLab:



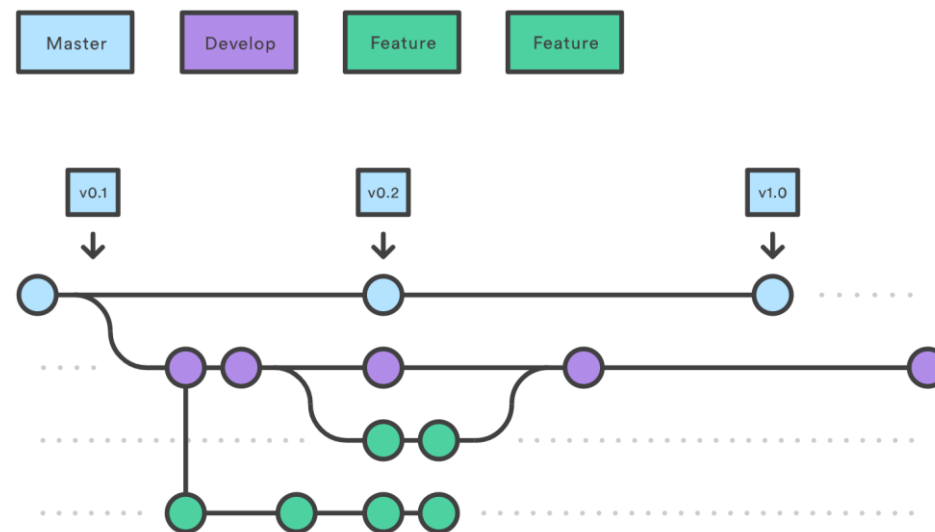
- Бесплатная Community версия
- Полный набор инструментов
 - Полноценный Git-сервер
 - Issue-трекер
 - Wiki
 - И многое другое ;)



Gitflow и ветвление

Следование стандартному Gitflow помогает содержать репозиторий в чистоте:

- Ветка «**master**» для релизов
- Ветка «**develop**» для текущей версии репозитория
- **Feature**-ветки для разработки функционала
- Название feature-веток удобно ассоциировать с задачами в треке (например feature/iss-123)




Запуск своего GitLab-сервера

Для быстрого развёртывания можно воспользоваться официальным docker-контейнером:

```
export GITLAB_HOME=/srv/gitlab
sudo docker run --detach \
  --hostname gitlab.example.com \
  --publish 443:443 --publish 80:80 --publish 22:22 \
  --name gitlab \
  --restart always \
  --volume $GITLAB_HOME/config:/etc/gitlab \
  --volume $GITLAB_HOME/logs:/var/log/gitlab \
  --volume $GITLAB_HOME/data:/var/opt/gitlab \
  gitlab/gitlab-ce:latest
```


<https://docs.gitlab.com/omnibus/docker/README.html>

GitLab

Projects ▾

Groups ▾


More ▾





+


Search or jump to...


Q














M MPSIEM_Custom_Co...

Project overview

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Issues0

Merge requests0

CI/CD

Security & Compliance

Operations

Packages & Registries

Analytics

Wiki

Snippets

Members

Collapse sidebar

mpsiem_content_dev > MPSIEM_Custom_Content > Repository

You pushed to **develop** just now

Create merge request


master ▾

mpsiem_custom_content / + ▾

History

Find file

Web IDE

 ▾

Clone ▾

Switch branch/tag

Search branches and tags


Q

Branches

develop

✓ master

49f25293



Last update

2 days ago

README.md

MPSIEM_Custom_Content

Custom MaxPatrol SIEM content

Конвертация и выгрузка контента из MP SIEM



Во время подготовки необходимо:

1. Экспортировать все объекты нужной БД из РТКВ в формате «Для импорта в другую Knowledge Base».
2. Преобразовать полученный архив в репозиторий на файловой системе при помощи утилиты *kbtools.exe*.
3. Экспортировать все объекты нужной БД из РТКВ в формате «Для установки в SIEM Lite».
4. Скопировать файлы *schema.json* и *correlation_defaults.json* из архива, полученного на шаге 3 в репозиторий из шага 2.

PT Knowledge Base

ESC_content

SIEM

Пакеты экспертизы

Пакеты

Все объекты

Базовый пакет

ESC

Наборы для установки

Все объекты

Вне наборов

Системное название, идентификатор

№...	С...	Идентификатор	Систем	Исходник	Папка
1	!	PT-NF-6269	25_Pro		Базовый пакет\normalization_formulas\Micro
2	!	PT-NF-6268	24_Clip	бновилось	Базовый пакет\normalization_formulas\Micro
3	!	PT-NF-6267	23_File		Базовый пакет\normalization_formulas\Micro
4	!	PT-NF-6266	22_DNS		Базовый пакет\normalization_formulas\Micro
5	!	PT-NF-6261	domain	группой	Базовый пакет\normalization_formulas\Syme
6	!	PT-NF-6260	WSS_re	IS отключе...	Базовый пакет\normalization_formulas\Syme
7	!	PT-NF-6259	WSS_de	е правильно	Базовый пакет\normalization_formulas\Syme
8	!	PT-NF-6258	Virus_definitions_are_missing	Не установлены описания вирусов	Базовый пакет\normalization_formulas\Syme
9	!	PT-NF-6257	update_install_on_client_en_ru	Обновления установлены	Базовый пакет\normalization_formulas\Syme
10	!	PT-NF-6256	Start_serving_as_GUP	Узел стал поставщиком обновлений групп	Базовый пакет\normalization_formulas\Syme
11	!	PT-NF-6255	SONAR_error	Ошибка SONAR	Базовый пакет\normalization_formulas\Syme
12	!	PT-NF-6254	Service_engine_start_failure	Не удалось запустить Service Engine	Базовый пакет\normalization_formulas\Syme
13	!	PT-NF-6253	Server_policy_import_fail	Не удалось импортировать политику сер...	Базовый пакет\normalization_formulas\Syme

Всего 6088 объектов, выбраны 0

Экспорт объектов

Объекты для экспорта

☒ Все объекты из Knowledge Base

☐ Объекты из набора для установки

Формат экспорта

☒ Для импорта в другую Knowledge Base

☐ Для установки в SIEM Lite

Экспортировать

Отмена

Обзор интерфейса PTSIEMSDK GUI

Утилита PTSIEMSDK GUI



PTSIEMSDK GUI — утилита, предназначенная для создания и отладки отдельных правил нормализации, агрегации, обогащения, корреляции и локализации, а также для отладки их совместной работы.

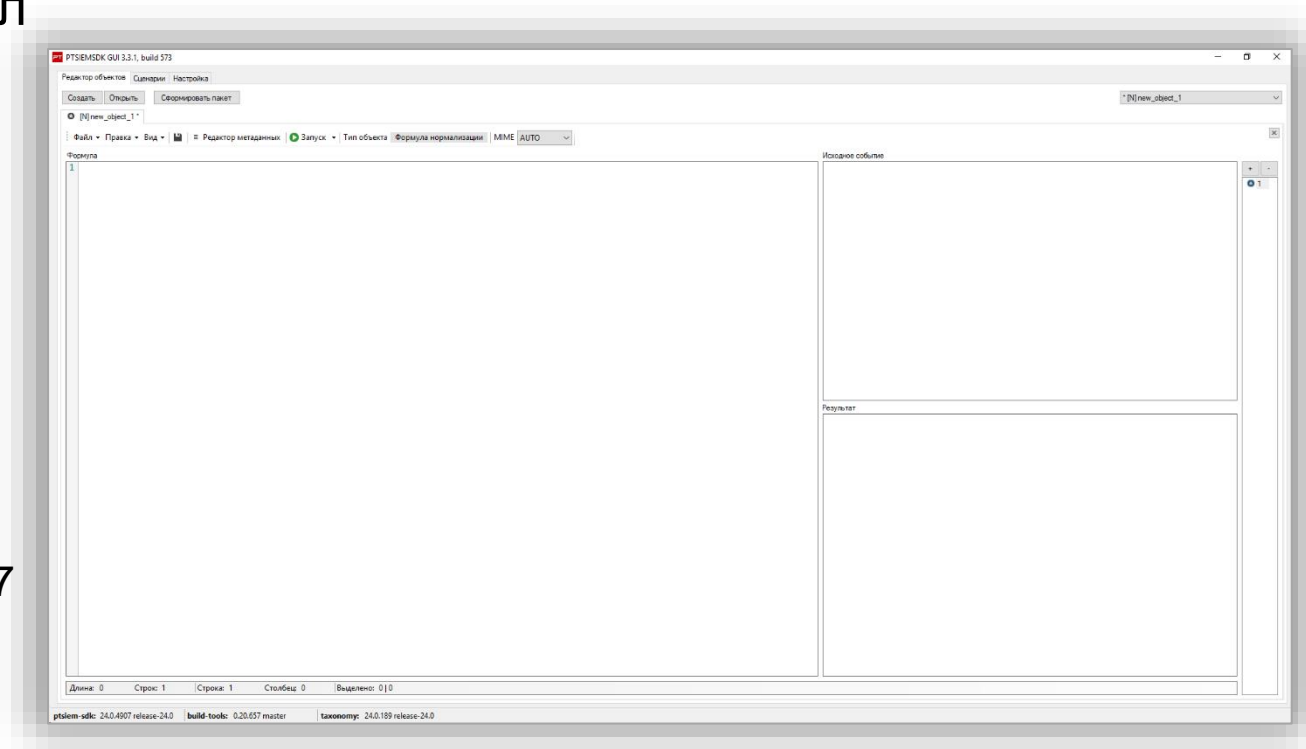
Программные требования

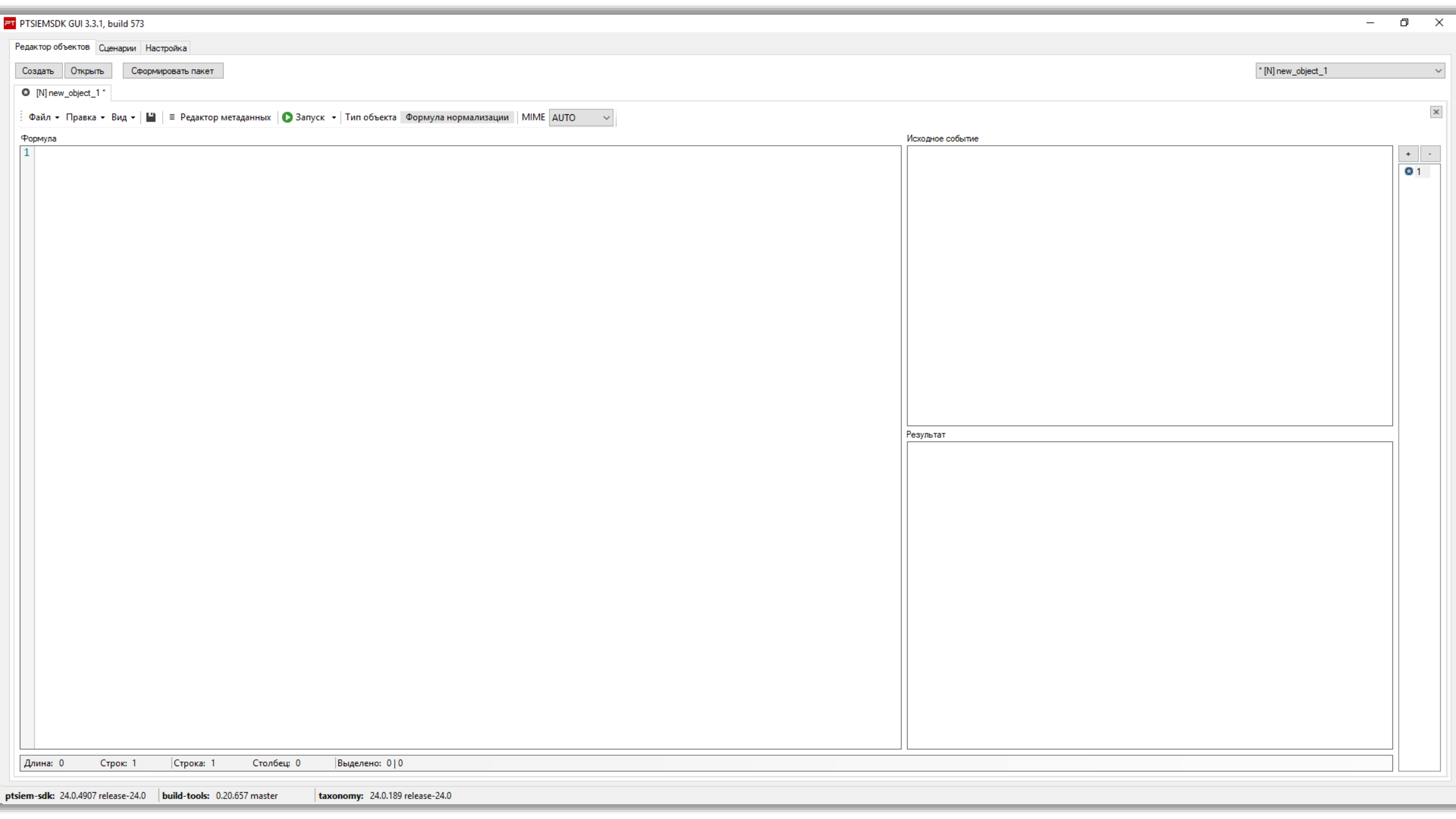
Поддерживается работа утилиты в Windows 10, 8.1, 7 и Windows Server 2019, 2016, 2012R2, 2008R2 с установленными обновлениями.

Для работы утилиты требуется следующее ПО:

- Microsoft .NET Framework v4.7.1
- Microsoft Visual C++ для Visual Studio 2015, 2017 и 2019 (x86)
- Microsoft Visual C++ для Visual Studio 2015, 2017 и 2019 (x64).

скачать ПО можно с сайта support.microsoft.com





Три основные вкладки

PT

PT PTSIEMSDK GUI 3.3.1, build 573

Редактор объектов | Сценарии | Настройка

Создать

Открыть

Сформировать пакет

✱ [N] new_object_1 *

⋮ Файл ▾ Правка ▾ Вид ▾ | 📁 | ≡ Редактор метаданных | 🎬 Запуск ▾ | Тип объекта | Формула нормализации | MIME | AUTO ▾

Настройка PTSIEMSDK GUI



Основные настройки:

- Пути (самый важный раздел)
- Интерфейс (цветовая схема, шрифты, язык и т.п.)
- Автоматическое сохранение сессии

Создание правила корреляции

Общий алгоритм

Подготовительная часть:

- идея для выявления (статья, твит, собственные исследования и т.п.)
- сбор информации и ссылок на источники

Создание правил корреляции:

- сбор сырых событий (эмуляция атаки, получение событий из MP SIEM и дальнейшая нормализация)
- написание тестов для проверки работоспособности правила (да, как в TDD, тесты до написания кода)
- написание кода правила корреляции
- создание локализации и описания правила
- загрузка изменений в систему контроля версий

Сбор сырых событий



Существует 2 основных способа сбора сырых событий:

Способ 1: Скопировать событие из Event Viewer (Web UI)

Способ 2: Собрать событие с помощью утилиты `export_data.exe` (подробно изложено в документации)

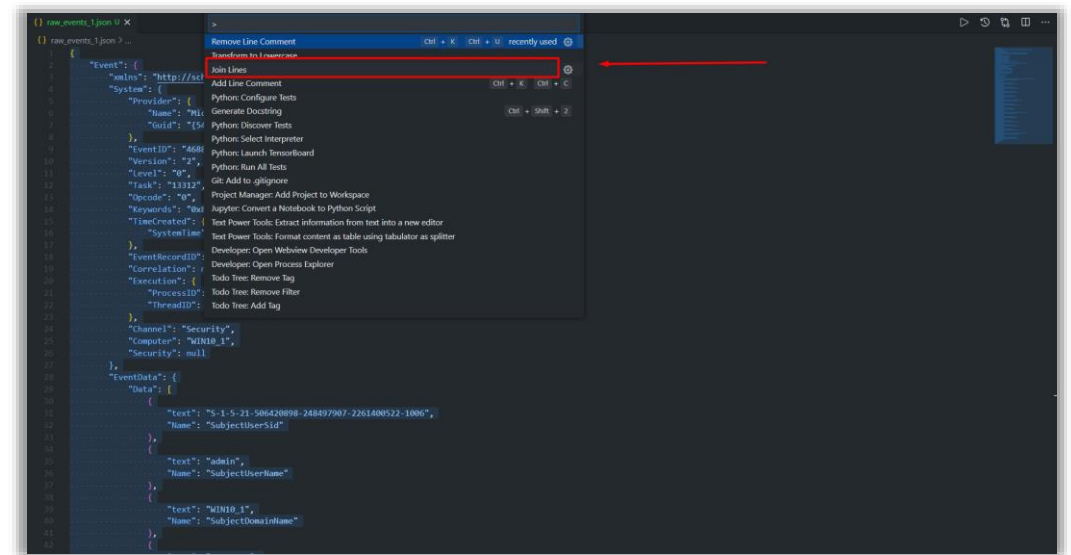
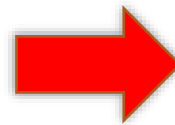
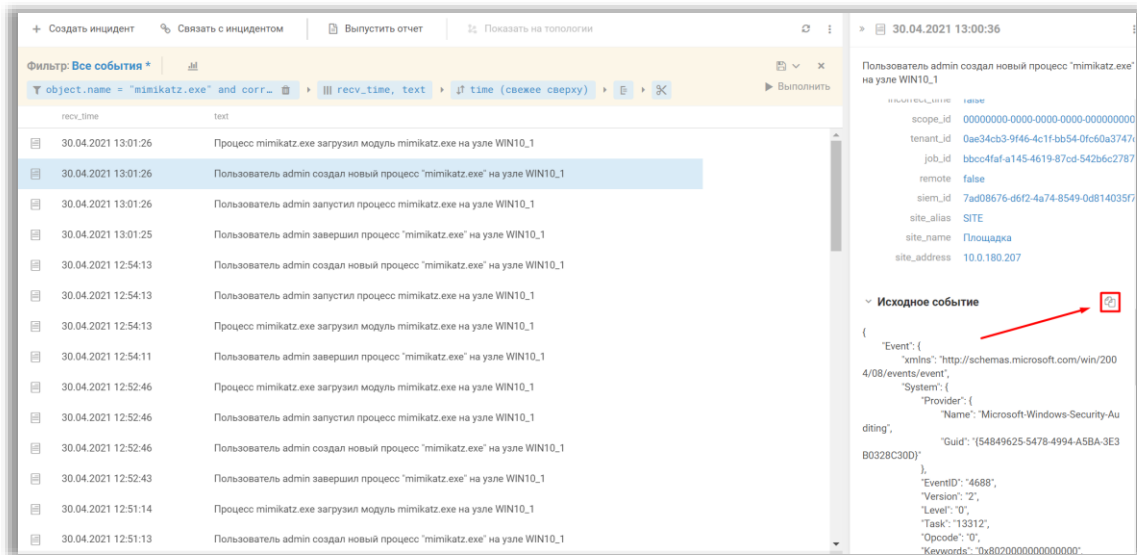
Примечание:

При выгрузке через UI полученное сырое событие нужно сохранить в папке «*test*» правила корреляции. Имя файла должно быть формата *raw_events_<N>.json*, где <N> — целое положительное число.

Способ 1

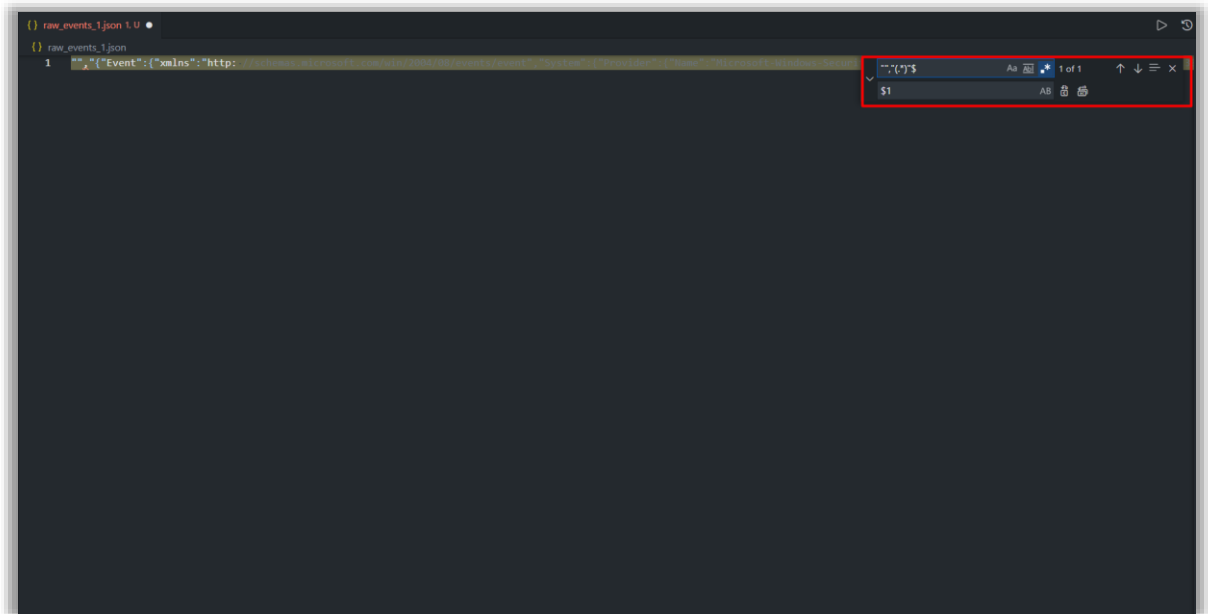
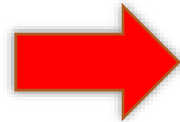
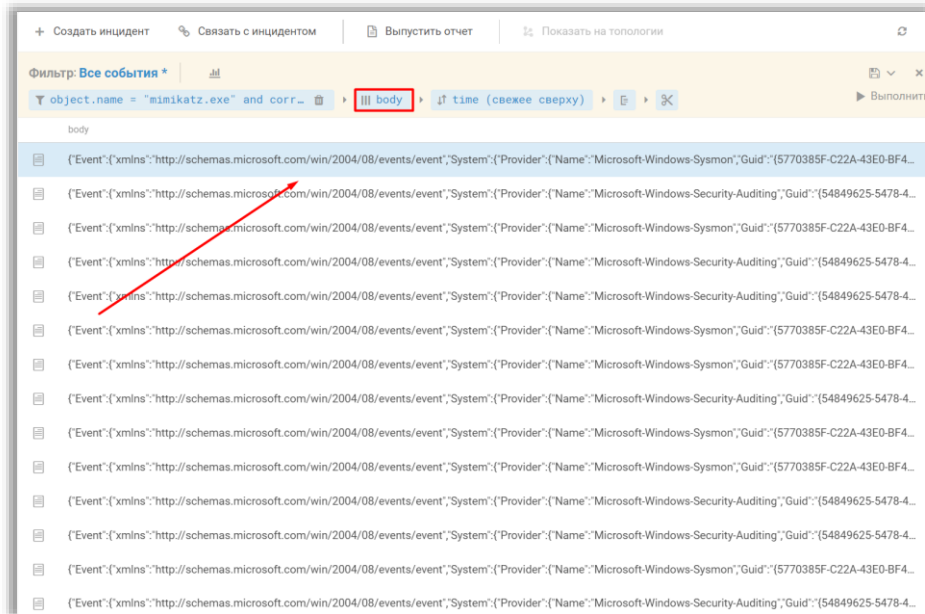
PT

1. Выбрать в Event Viewer нужное событие, скопировать его через иконку и вставить в текстовый редактор
2. В текстовом редакторе преобразовать в строку



Способ 2

1. Выбрать нужные события в Event Viewer и оставить только поле «body» в разделе выбора колонок для отображения. Далее скопировать через Ctrl+C и вставить в текстовый редактор
2. В текстовом редакторе удалить ненужные символы в начале (кавычки и запятая) и конце строки (кавычки) или воспользоваться регулярным выражением `"", "(.*)"`



Тесты



The screenshot displays the YARA Editor application window, which is divided into several panes.

Top Bar: Contains tabs for "Редактор объектов" (Object Editor), "Сценарии" (Scripts), and "Настройка" (Settings). Below these are buttons for "Создать" (Create), "Открыть" (Open), and "Сформировать пакет" (Generate Package).

Main Menu: Includes "Файл" (File), "Правка" (Edit), "Вид" (View), and a dropdown menu currently set to "Запуск" (Run). Other options visible are "Тип объекта" (Object Type) and "Правило корреляции" (Correlation Rule).

Left Pane (Rule Editor): Displays the YARA rule code for "ESC_Service_logon_from_VPN_network". The rule includes queries for VPN networks, user connections, and logon events, followed by a complex correlation logic block and a final action block.

Right Pane (Test Results): Shows the output of running the rule against a sample event. It lists the tables used ("ESC_VPN_networks", "ESC_Service_Name"), the detected event details (logon from 8.8.8.8), and the resulting JSON output for the "Logon" event.

Status Bar: At the bottom, it shows file information: "ptsiem-sdsc: 24.0.7464 release-24.0", build tools version "0.20.680 master", and taxonomy version "24.0.189 release-24.0".

Написание кода правила корреляции

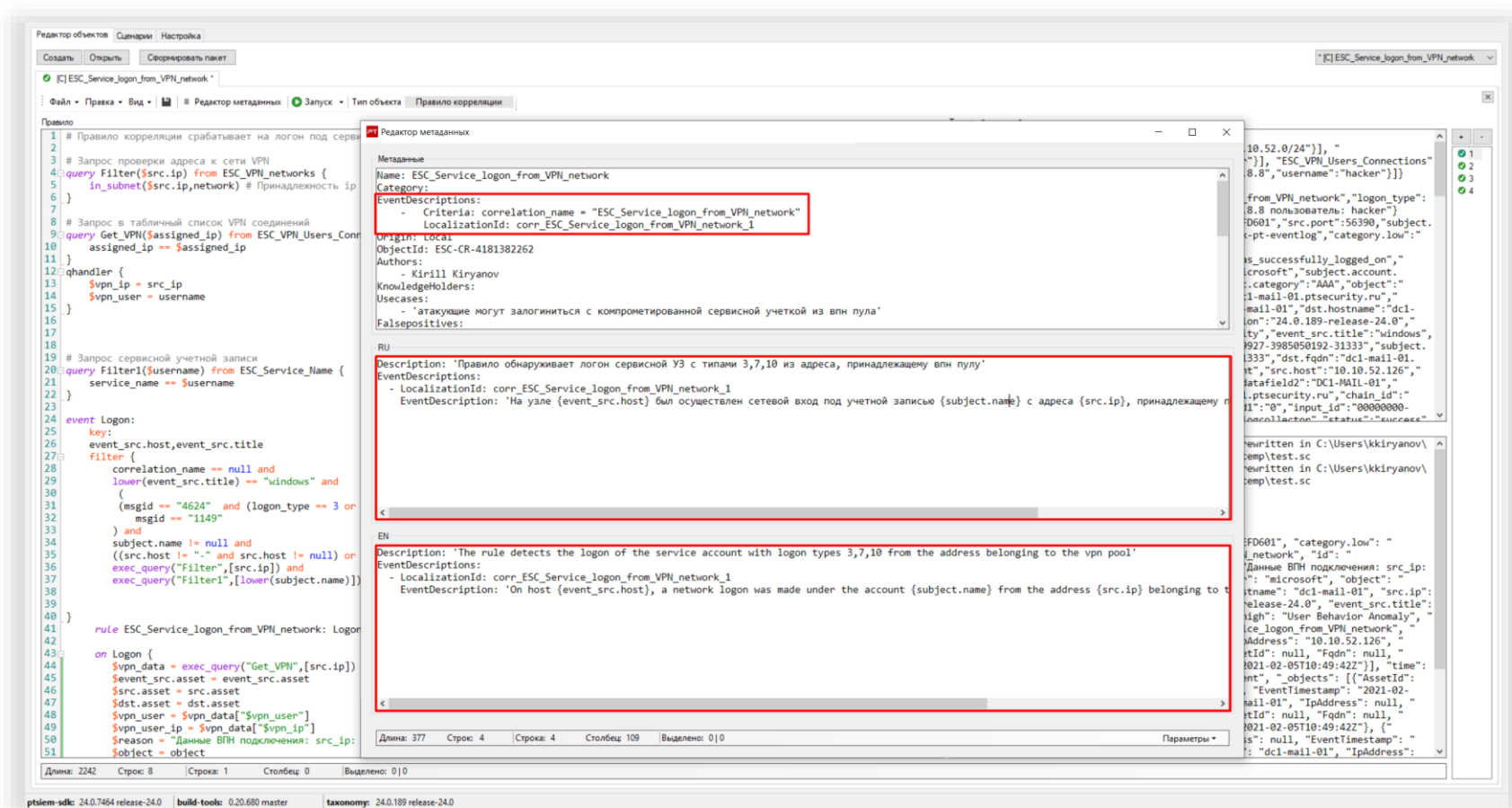
PT

После того как мы написали тесты, можем приступить к созданию кода правила корреляции

The screenshot displays the PT rule editor interface. The main window shows the rule code for a correlation rule named "ESC_Service_logon_from_VPN_network". The code is written in a YAML-like syntax and includes several sections: a rule definition, a query to filter logon events, and a handler to process the logon events. The rule is designed to trigger on logon events from VPN networks and to correlate them with other logon events. The test scenario on the right shows a sequence of events that trigger the rule, including a logon event from a VPN network and a subsequent logon event from a different source. The test results show that the rule successfully correlated the two logon events.

```
1 # Правило корреляции срабатывает на логон под сервисной учетной записью из сетей vpn
2
3 # Запрос проверки адреса к сети VPN
4 query Filter($src_ip) from ESC_VPN_networks {
5   in_subnet($src_ip, network) # Принадлежность ip адреса к маске
6 }
7
8 # Запрос в табличный список VPN соединений
9 query Get_VPN($assigned_ip) from ESC_VPN_Users_Connections {
10   assigned_ip == $assigned_ip
11 }
12
13 handler {
14   $vpn_ip = src_ip
15   $vpn_user = username
16 }
17
18 # Запрос сервисной учетной записи
19 query Filter1($username) from ESC_Service_Name {
20   service_name == $username
21 }
22
23
24 event Logon:
25   key:
26     event_src.host, event_src.title
27   filter {
28     correlation_name == null and
29     lower(event_src.title) == "windows" and
30     (msgid == "4624" and (logon_type == 3 or logon_type == 10 or logon_type == 7)) or
31     msgid == "1149"
32   ) and
33   subject.name != null and
34   ((src.host != "-" and src.host != null) or (src.ip != "-" and src.ip != null)) and
35   exec_query("Filter", [src_ip]) and
36   exec_query("Filter1", [lower(subject.name)])
37
38
39
40 }
41
42 rule ESC_Service_logon_from_VPN_network: Logon
43
44 on Logon {
45   $vpn_data = exec_query("Get_VPN", [src_ip])
46   $event_src.asset = event_src.asset
47   $src.asset = src.asset
48   $dst.asset = dst.asset
49   $vpn_user = $vpn_data["$vpn_user"]
50   $vpn_ip = $vpn_data["$vpn_ip"]
51   $reason = "Данные VPN подключения: src_ip: " + $vpn_ip + " пользователь: " + $vpn_user
52   $object = object
```

Написание локализации и описания



Проверка правила локализации

PT

The screenshot shows the 'Просмотр событий' (Event Viewer) window. The left pane displays a list of events under the 'RU_EVENTS' tab. The right pane shows the details of a selected event, including a JSON representation of the event data.

Event Details:

- Subject:** srv-service с адреса 172.16.222.55, принадлежащему пулу VPN, с типом 3. Данные ВПН
- Action:** login
- Object:** system
- Status:** success
- Rule:** ESC_Service_logon_from_VPN_network
- Category (generic):** Anomaly
- Category (high):** User Behavior Anomaly
- Category (low):** Detection
- Correlation Name:** ESC_Service_logon_from_VPN_network
- Correlation Type:** event
- Count:** 1
- Datafield1:** 0
- Datafield2:** DC3-W16
- Datafield6:** Network
- Datafield8:** Kerberos
- Event Src Host:** DC3-W16.testlab.esc
- Event Src Hostname:** DC3-W16
- Event Src Title:** windows
- Event Src Vendor:** microsoft
- ID:** ESC_Service_logon_from_VPN_network
- Importance:** high
- Logon Type:** 3
- Reason:** Данные ВПН подключения: src_ip: 8.8.8.8 пользователь: weak_pwd_user
- Src IP:** 172.16.222.55
- Subevents:** [00000000-0000-0000-0000-000000000001]
- Subevents Time:** [2021-06-02T11:24:17Z]
- Subject Domain:** testlab.esc
- Subject Name:** srv-service
- Time:** 2021-06-02T11:24:17Z
- UUID:** d8c2a597-3934-4a0b-8ead-7e6abc4846e8

Footer: Событие: 1 / 1 | Предупреждения: Отсутствует точка в конце строки

Отправка изменений на сервер



```
C:\Webinars\mpsiem_content (develop)
λ git add *

C:\Webinars\mpsiem_content (develop)
λ git commit -m "Добавили модульные тесты к правилу ESC_Service_logon_from_VPN_network"
[develop 9181d5f0] Добавили модульные тесты к правилу ESC_Service_logon_from_VPN_network
11 files changed, 153 insertions(+), 122 deletions(-)
create mode 100644 packages/esc/correlation_rules/ESC_Service_logon_from_VPN_network/tests/raw_events_1.json
create mode 100644 packages/esc/correlation_rules/ESC_Service_logon_from_VPN_network/tests/raw_events_2.json
create mode 100644 packages/esc/correlation_rules/ESC_Service_logon_from_VPN_network/tests/raw_events_3.json
create mode 100644 packages/esc/correlation_rules/ESC_Service_logon_from_VPN_network/tests/test_1.sc
create mode 100644 packages/esc/correlation_rules/ESC_Service_logon_from_VPN_network/tests/test_2.sc

C:\Webinars\mpsiem_content (develop)
λ git push origin develop
Enumerating objects: 31, done.
Counting objects: 100% (31/31), done.
Delta compression using up to 8 threads
Compressing objects: 100% (19/19), done.
Writing objects: 100% (19/19), 9.46 KiB | 484.00 KiB/s, done.
Total 19 (delta 8), reused 0 (delta 0), pack-reused 0
remote:
remote: To create a merge request for develop, visit:
remote:   http://gitlab.local/root/mpsiem_content/-/merge_requests/new?merge_request%5Bsource_branch%5D=develop
remote:
To 127.0.0.1:root/mpsiem_content.git
48e1d0da..9181d5f0  develop -> develop
```


Демонстрация

Заключение

- Использование системы контроля версий для своего контента значительно упрощает процесс управления изменениями
- Создание тестов позволяет быстрее разрабатывать правила и эмулировать атаки, избавляет от необходимости повторного выполнения реальных действий
- При помощи PTSIEMSDK GUI можно проверять правила локализации без необходимости эмулировать атаку заново