

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Solar SUPRA



Оглавление

1.	ИСТОРИЯ ЗАДАЧ.....	3
2.	КОНТЕНТ.....	5
	2.1. ИМПОРТ	5
	2.2. СРАВНЕНИЕ	9
	2.3. ЭКСПОРТ	12
3.	ТАБЛИЧНЫЕ СПИСКИ.....	14
	3.1. ЭКСПОРТ ТС.....	14
	3.2. ИМПОРТ ТС	16
4.	ПАЙПЛАЙНЫ	18
	4.1. ИСТОРИЯ.....	18
	4.2. МОНИТОРИНГ	19

1. ИСТОРИЯ ЗАДАЧ

Раздел «История задач» позволяет просматривать информацию о задачах, созданных пользователем. Раздел содержит следующую информацию:

- историю по работе с сервисом — в табличном представлении отображаются все задачи, которые были когда-либо созданы в сервисе;
 - состояние задачи;
 - статус задачи;
 - результаты выполнения задачи;
 - параметры, с которыми запускалась задача;
- а также дает возможность скачать:
- логи выполнения задачи (хранятся 30 дней);
 - результаты выполнения задачи (хранятся от 7 до 30 дней в зависимости от типа результата):
 - 7 дней — для выгруженного контента;
 - 30 дней — для сравнительных отчетов.

Табличное представление содержит следующую информацию:

Параметр	Описание	Сортировка	Фильтрация
Переключатель «Мои задачи»	Позволяет посмотреть только задачи, созданные текущим пользователем. Если переключатель выключен, то отображаются все задачи всех пользователей, которые работают с сервисом		
Пользователь	Отображает email (он же логин) текущего пользователя	Да	Текстовый поиск по полному и частичному совпадению
Тип задачи	Отображает тип созданной задачи	Да	Фильтр с ограниченным списком значений
Дата создания	Отображает дату и время создания задачи в формате DD.MM.YYYY HH:MM:SS	Да	
Параметры	Отображает параметры запуска команды		Текстовый поиск по полному и частичному совпадению
Состояние задачи	Содержит список возможных значений: • created • progress • preparation • in queue • finished	Да	Фильтр с ограниченным списком значений
Статус	Отображает статус выполнения задачи. Список возможных значений: • success • warning	Да	Фильтр с ограниченным списком значений

	error		
Логи	Позволяет выгружать логи в процессе выполнения задачи. Архивов с логами может быть более одного. В этом случае отображается список архивов, доступных для скачивания		
Результаты	Позволяет выгружать результаты отработки процесса		

SUPRA

История задач

SIEM Core

Контент

ТС

Пайплайны

История

Расписание

Мониторинг

Настройки

Admin

Выйти

История задач

Мои задачи

Очистить фильтры

Пользователь	Тип задач	Дата создания ↓	Параметры	Состояние	Статус	Логи	Результат
Q	≡	Q	≡	≡	≡		
admin	Экспорт	18.11.2025 10:11:20	{"task_id":1076,"siem_address":"172.20.24.51"}	finished	success	↓	↓
admin	Экспорт	01.11.2025 13:00:15	{"task_id":868,"siem_address":"172.26.61.4"}	finished	success	↓	↓
admin	Экспорт	01.11.2025 12:59:45	{"task_id":867,"siem_address":"172.20.24.51"}	finished	success	↓	↓
admin	Импорт	06.10.2025 15:22:57	{"task_id":866,"src_siem_address":"172.20.24.51","dst_siem_address":"dev-allin01.rt-solar.local"}	finished	error	↓	↓
admin	Экспорт	15.08.2025 10:35:22	{"task_id":459,"siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Экспорт	15.08.2025 10:24:08	{"task_id":458,"siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Импорт TC	30.07.2025 15:01:52	{"task_id":367,"dst_siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Экспорт	28.07.2025 14:22:47	{"task_id":192,"siem_address":"10.80.45.5"}	finished	error	↓	↓
admin	Экспорт TC	28.07.2025 12:24:47	{"task_id":191,"siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Импорт TC	22.07.2025 13:49:44	{"task_id":18,"dst_siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Импорт TC	22.07.2025 13:32:49	{"task_id":17,"dst_siem_address":"10.80.45.5"}	finished	success	↓	↓
admin	Экспорт TC	22.07.2025 13:31:56	{"task_id":16,"siem_address":"10.80.45.5"}	finished	success	↓	↓

< 1 2 >

Всего строк: 23 15/стр. Перейти на страницу

Рисунок 1

Просмотр детализированной информации по задаче:

Детализированную информацию по задаче можно посмотреть в модальном окне «Детализация задачи», которое открывается по клику на строку табличного представления «История задач».

Окно с детализацией содержит ту же информацию, что и табличное представление, а также:

- полное описание параметров задачи;
- детальное описание ошибки для задач со статусом «Ошибка»;
- дает возможность скачать логи и результаты выполнения задачи из формы «Детализация задачи» (функционал идентичен тому, что реализован в табличном представлении);
- позволяет по кнопке «Повторить» еще раз запустить задачу с такими же параметрами.

Детализация задачи

Пользователь:

admin

Тип задачи:

Экспорт

Дата создания:

18.11.2025 10:11:20

Параметры:

```
{"id":8,"task_id":1076,"siem_type":"mp25","siem_address":"172.20.24.51","siem_login":"api_supra","siem_source_paths":["all"],"auth_type":"local","extend_log":false,"core_id":78,"selected_core_name":"1 Эталон (172.20.24.51)","recursive_extraction_required":true,"unpacking_required":true}
```

Статус:

success

Логи:

↓

Результаты:

↓

Повторить

Рисунок 2

2. КОНТЕНТ

Раздел «Контент» состоит из следующих подразделов:

- подраздел «Импорт»;
- подраздел «Сравнение»;
- подраздел «Экспорт».

2.1. ИМПОРТ

В этом подразделе пользователю доступны:

- Получение и отображение всех наборов установки (НУ) для заданных Source и Destination SIEM.
- Получение ресурсов для НУ (если пользователь включает отдельный переключатель).
- Поиск по дереву НУ: по имени НУ и/или ресурса.
- Выбор в дереве Source НУ для импорта.
- Выбор в дереве Destination пути, куда необходимо импортировать ресурсы.
- Работа с путями импорта.
- Создание деревьев.

Для того чтобы импортировать контент, пользователь указывает SIEM Core в области «Source» и в области «Destination».

The screenshot shows the SUPRA web application interface for the 'Import' section. On the left is a dark sidebar with navigation links: 'История задач', 'SIEM Core', 'Контент' (expanded), 'Экспорт', 'Сравнение', 'Импорт' (highlighted), 'ТС', 'Пайплайн', 'История', 'Расписание', 'Мониторинг', and 'Настройки'. The main area has a top status bar with 'Last task: импорт', a timestamp '12.05.2023 14:30:43', and a command line snippet. Below this are two panels: 'Source' and 'Destination'. The 'Source' panel has a radio button for 'SIEM' (selected) and a text field 'Название SIEM Core' with the value 'Core12345'. The 'Destination' panel has a checked checkbox for 'Ручной ввод' (Manual input) and several input fields: 'IP/hostname SIEM*' (10.200.28.34), 'Тип SIEM*' (MP25.1), 'Логин*' (jsoc-monitor), and 'Пароль*' (123459697). There are also radio buttons for 'Аутентификация: Доменная' (selected) and 'Локальная'. At the bottom right is a blue button labeled 'Получить набор установки' (Get installation set).

Рисунок 3

Далее по кнопке «Получить набор установки» строятся деревья с наборами установки. При выборе НУ отображаются пути импорта по выбранным ресурсам.

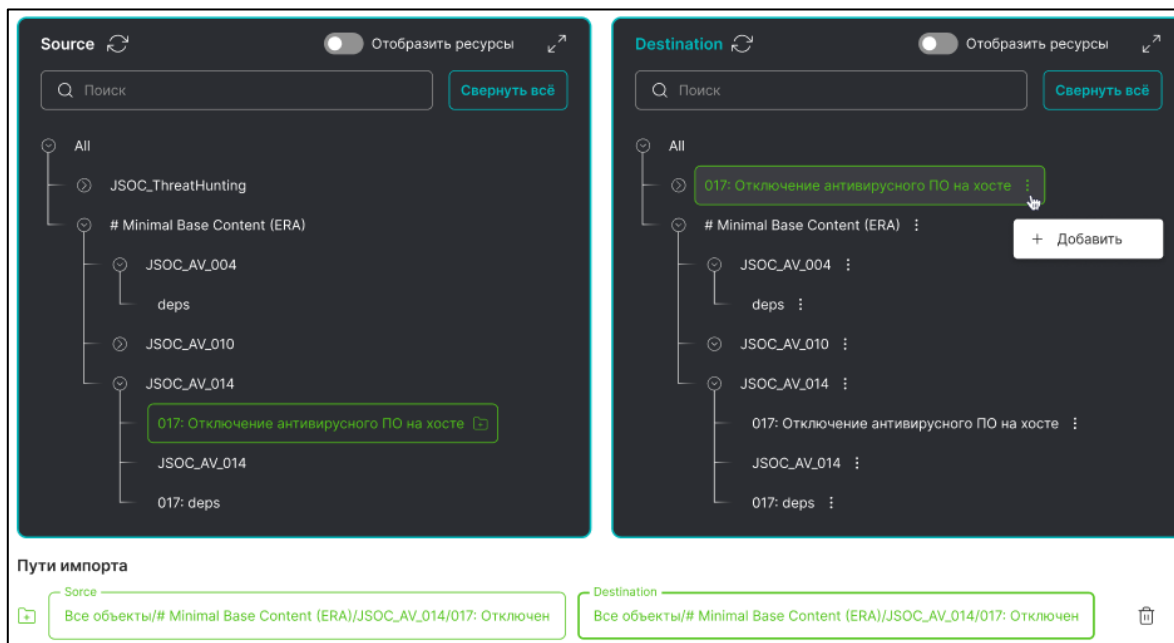


Рисунок 4

Затем пользователь выбирает параметры импорта:

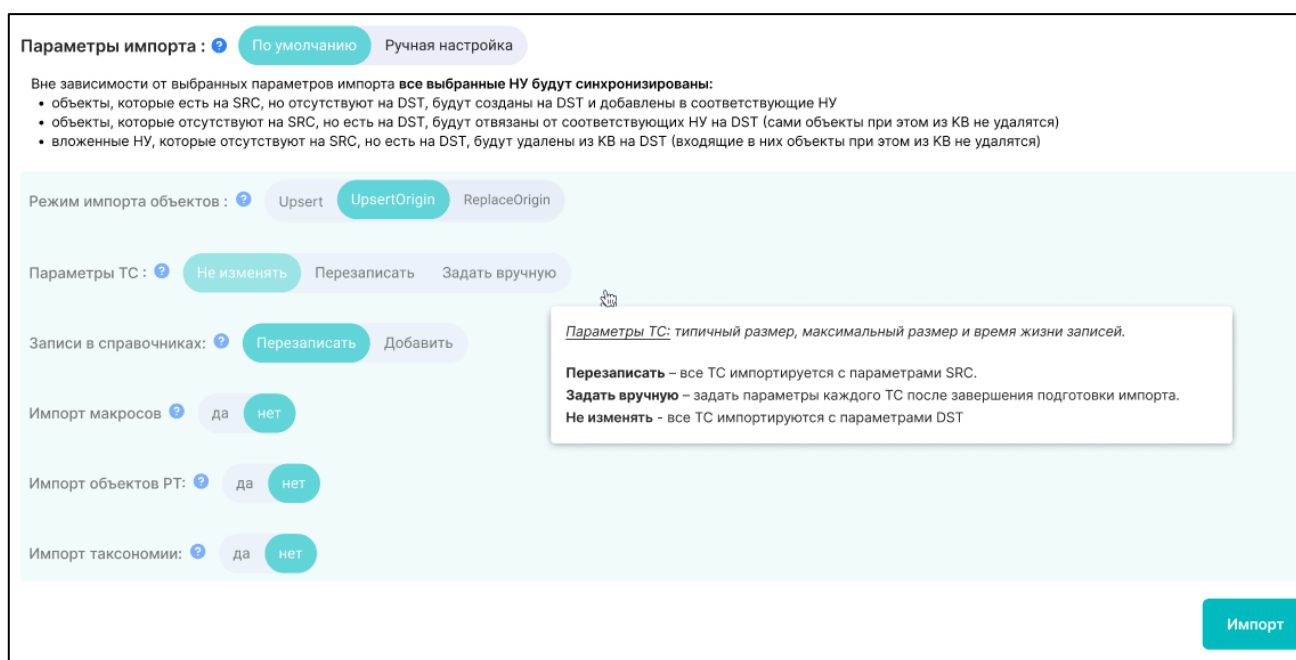


Рисунок 5

После нажатия кнопки «Импорт» открывается форма с подтверждением импорта выбранных НУ.

Импорт

Выбран режим импорта: `UpsertOrigin`

Source	Destination
<code>all/! Local SIEM Content</code>	<code>all/! Local SIEM Content</code>
<code>all/! Local SIEM Content/# Additional Info Content</code>	<code>all/! Local SIEM Content/# Additional Info Content</code>
<code>all/! Local SIEM Content/# Additional Info Content/AD_Export</code>	<code>all/! Local SIEM Content/# Additional Info Content/AD_Export</code>
<code>all/! Local SIEM Content/# Additional Info Content/AD_Export/For_AD_export_v5.3</code>	<code>all/! Local SIEM Content/# Additional Info Content/AD_Export/For_AD_export_v5.3</code>
<code>all/! Local SIEM Content/# Additional Info Content/AD_Export/SambaDC</code>	<code>all/! Local SIEM Content/# Additional Info Content/AD_Export/SambaDC</code>
<code>all/! Local SIEM Content/# Must Have Content</code>	<code>all/! Local SIEM Content/# Must Have Content</code>
<code>all/! Local SIEM Content/# Must Have Content/IT-HM-11: SystemHealth: Массовое срабатывание сценария DirectAlert</code>	<code>all/! Local SIEM Content/# Must Have Content/IT-HM-11: SystemHealth: Массовое срабатывание сценария DirectAlert</code>
<code>all/! Local SIEM Content/# Must Have Content/IT-HM-11: SystemHealth: Массовое срабатывание сценария DirectAlert/IT-HM-11: deps</code>	<code>all/! Local SIEM Content/# Must Have Content/IT-HM-11: SystemHealth: Массовое срабатывание сценария DirectAlert/IT-HM-11: deps</code>
<code>all/! Local SIEM Content/# Must Have Content/IT-HM-12: SystemHealth: Контроль массовой генерации инцидентов</code>	<code>all/! Local SIEM Content/# Must Have Content/IT-HM-12: SystemHealth: Контроль массовой генерации инцидентов</code>
<code>all/! Local SIEM Content/# Must Have Content/IT-HM-12: SystemHealth: Контроль массовой генерации инцидентов/deps</code>	<code>all/! Local SIEM Content/# Must Have Content/IT-HM-12: SystemHealth: Контроль массовой генерации инцидентов/deps</code>
<code>all/! Local SIEM Content/# Must Have Content/Must_Have_Content:deps</code>	<code>all/! Local SIEM Content/# Must Have Content/Must_Have_Content:deps</code>
<code>all/! Local SIEM Content/# Normalization</code>	<code>all/! Local SIEM Content/# Normalization</code>
<code>all/! Local SIEM Content/# Normalization/RedHat</code>	<code>all/! Local SIEM Content/# Normalization/RedHat</code>
<code>all/! Local SIEM Content/# Normalization/RedHat/FreeIPA</code>	<code>all/! Local SIEM Content/# Normalization/RedHat/FreeIPA</code>

Отменить Импорт

Рисунок 6

Если в настройках импорта пользователь выбрал:

- ручная настройка,
- в параметре «Параметры ТС» — значение «Задать вручную»,
- или в параметре «Записи в справочниках» — «Добавить»,

то открывается форма, демонстрирующая ход подготовительного этапа:

Подготовка данных для импорта контента

Выгрузка контента из SOURCE: `dev-alline.rt-solar.local`

in progress...

Выгрузка контента из DEST: `dev-alline.rt-solar.local`

in progress...

⚠ Импорт можно будет продолжить после завершения процедуры подготовки! Подготовка может занять до 30 минут.

Отменить

Рисунок 7

После успешного завершения подготовительного этапа открывается форма, предоставляющая возможность изменить параметры табличных списков.

Пользователь может изменить следующие параметры: типичный размер, максимальный размер и время жизни записей.

Чтобы внести изменение, необходимо кликнуть на ячейку в столбце Final в соответствующем параметре табличного списка. Синим цветом отображаются табличные списки, в которых были внесены изменения и их значения.

Изменение параметров TC

Столбцы Final отображают итоговые значения параметров, с которыми TC будут импортированы на DST. По умолчанию значения берутся из текущих значений DST, при их отсутствии – из SRC.

Какие TC отобразить:

☒ Все (500)

☐ Только с отличающимися параметрами (233)

☐ Только отсутствующие на DST (51)

☐ Только с отредактированными параметрами

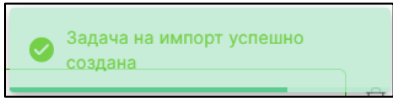
Наименование TC ↓	Типичный размер			Максимальный размер			Время жизни записей		
	Source ↓	Dest ↓	Final ↓	Source	Dest	Final	Source	Dest	Final
Q									
A_Customer_New_Users_1_day	10000	20000	20000	12000	22000	22000	86400	86400	86400
AB_Kaspersky_Host_Status_in	10000	-	10000	12000	-	22000	86400	-	86400
AC_Customer_New_Users_1_day	10000	20000	20000	12000	22000	22000	86400	86400	86400
AD_Kaspersky_Host_Status_in	10000	-	10000	12000	-	22000	86400	-	86400
AE_Customer_New_Users_1_day	10000	20000	20000	12000	22000	22000	86400	86400	86400
AV_Kaspersky_Host_Status_in	10000	-	10000	12000	-	22000	86400	-	86400
AV_New_Users_1_day	10000	20000	20000	12000	22000	22000	86400	86400	86400
AV_Kaspersky_Host_Status_in	10000	-	10000	12000	-	22000	86400	-	86400
AC_Customer_New_Users_1_day	10000	20000	20000	12000	22000	22000	86400	86400	86400
AV_Kaspersky_Host_Status_in	10000	-	10000	12000	-	22000	86400	-	86400

Отменить

Подтвердить

Рисунок 8

Далее после нажатия кнопки «Подтвердить» запускается задача на импорт контента.



Созданная задача отобразится в разделе «История задач».

2.2. СРАВНЕНИЕ

В разделе «Сравнение» отображается функционал для сравнения контента. В соответствующих областях пользователь указывает, какие контенты он хочет сравнить.

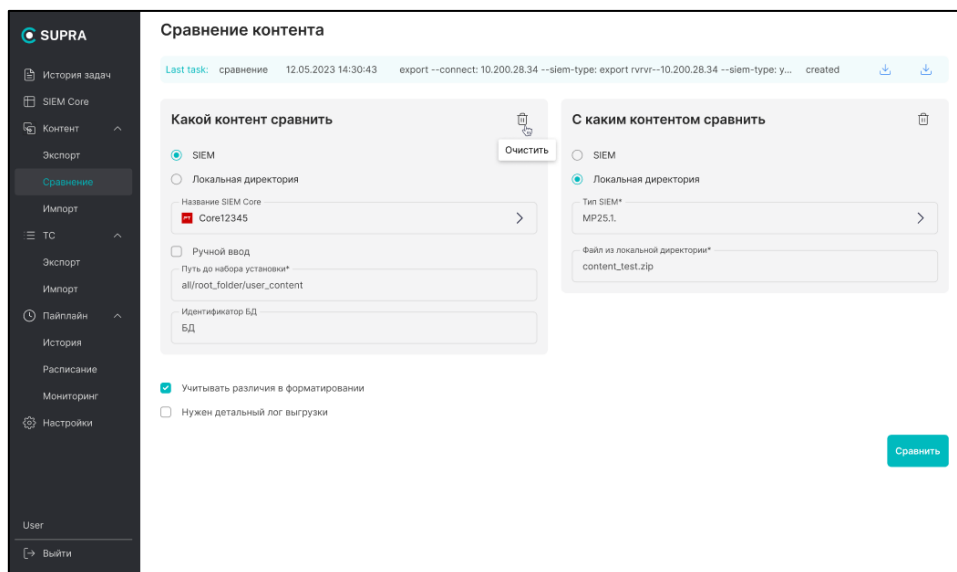


Рисунок 9

В области «Какой контент сравнить» и «С каким контентом сравнить» необходимо выбрать путь, откуда взять контент для сравнения:

- SIEM
- Локальная директория

При значении «Локальная директория» пользователю требуется выбрать:

- тип SIEM: при клике открывается выпадающий список из двух значений: MP или КУМА.
- файл из локальной директории: при клике открывается проводник с рабочим столом для выбора файла.

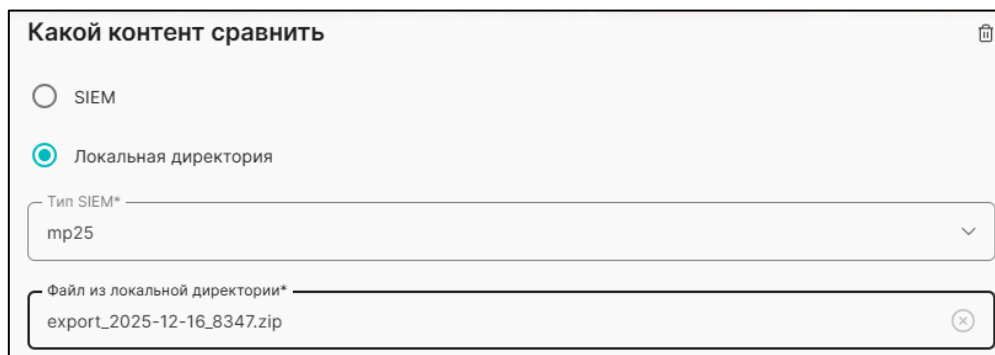


Рисунок 10

При значении SIEM в поле «Название SIEM Core» в выпадающем списке отобразится список SIEM Core для выбора:

Рисунок 11

Также данные о SIEM Core можно ввести вручную, если активировать чекбокс «Ручной ввод»:

Рисунок 12

После выбора SIEM Core в соответствующих полях пользователю потребуется ввести идентификатор БД и путь до НУ:

Рисунок 13

Можно активировать чекбокс «Установочная БД», тогда в процессе сравнения будет использоваться база данных с признаком «Установочная».

Путь до набора установки выбирается в дереве. Дерево наборов установки открывается при клике на область поля для ввода.

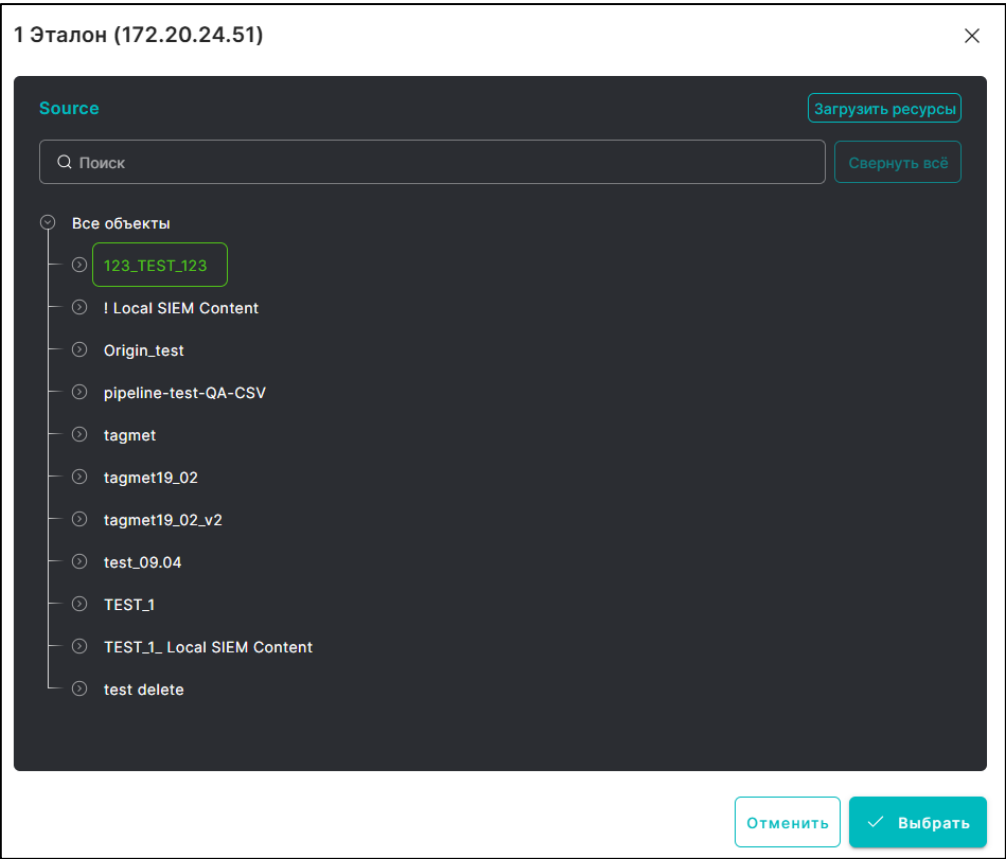


Рисунок 14

Выбранный набор установки отобразится зеленым цветом и появится в соответствующем поле:

Путь до набора установки*
all/! Local SIEM Content

. Аналогично требуется заполнить поля в области «С каким контентом сравнить».

☒ Учитывать незначительные отличия
☒ Нужен детальный лог выгрузки

Для процесса сравнения можно установить следующие параметры:
Если активен чекбокс «Учитывать незначительные отличия», то в этом случае не будет проведена проверка на различия в форматировании, все различия будут значимыми.
Если активен чекбокс «Нужен детальный лог выгрузки», то в файл с логами сохраняется детальная информация о выгрузке и сравнении файлов контента. Если параметр не задан, файл с детальными логами не формируется.
После того как выбран контент для сравнения и заданы параметры, необходимо запустить процесс сравнения

по кнопке **Сравнить**. Далее запустится задача на сравнение контента. Созданная задача отобразится в разделе «История задач».

✓ Задача на сравнение контента успешно создана

2.3. ЭКСПОРТ

В разделе «Экспорт» пользователь может экспортировать контент с выбранной SIEM Core.

Чтобы экспортировать контент, потребуется:

- Выбрать SIEM Core из выпадающего списка либо ввести данные о SIEM Core вручную.
- Указать идентификатор базы данных либо использовать установочную БД.
- Указать путь до набора установки.

Путь до набора установки выбирается в дереве. Дерево наборов установки открывается при клике на область поля для ввода.

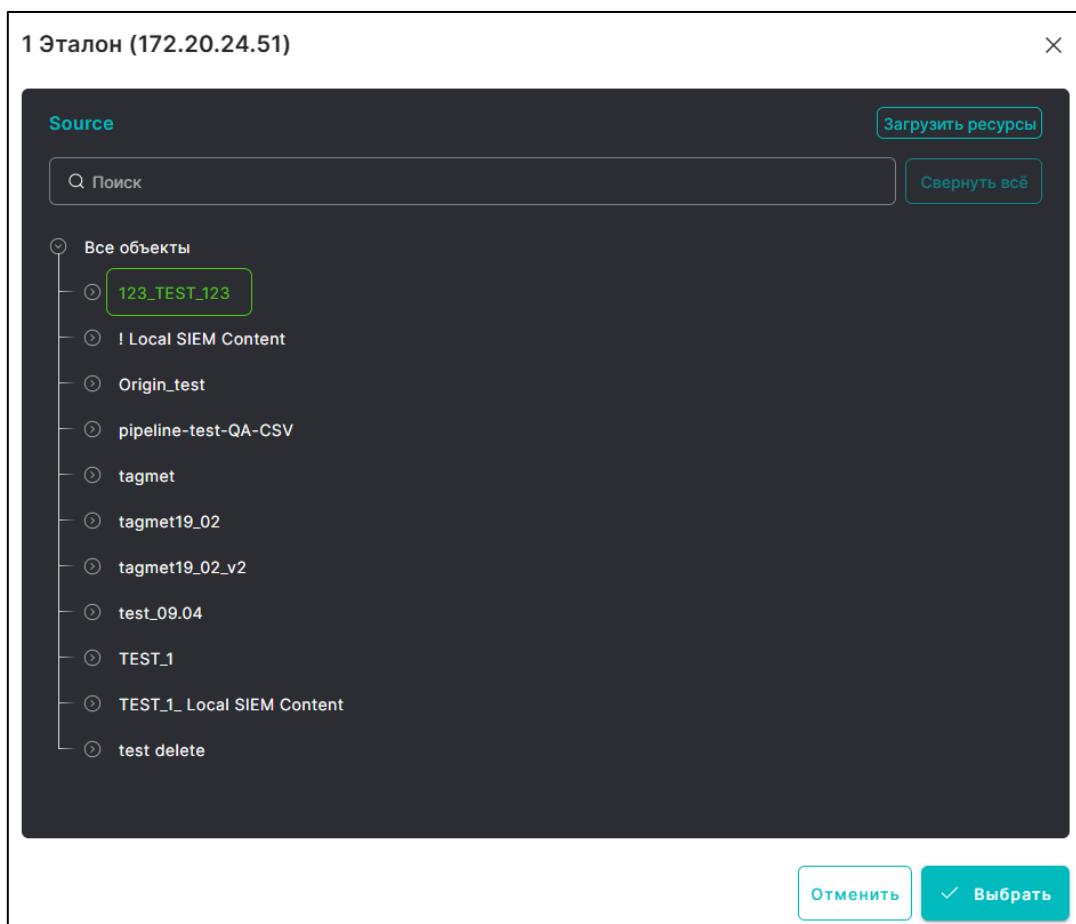


Рисунок 15

Выбранные наборы установки отображаются зеленым цветом и появляются в соответствующем поле:

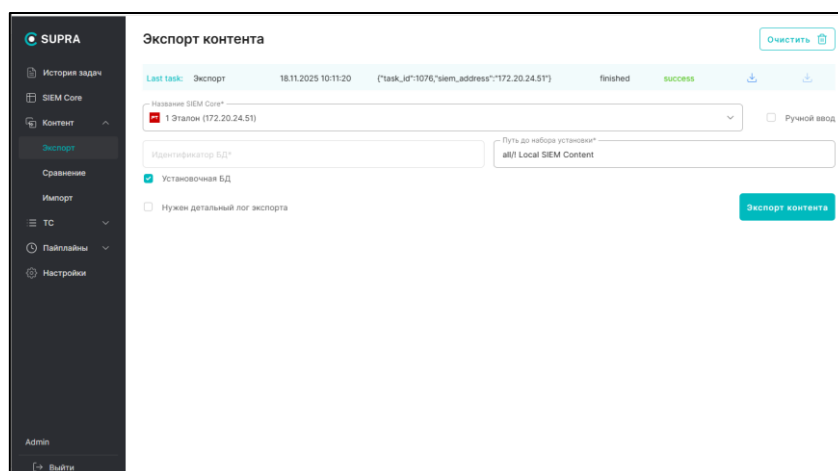


Рисунок 16

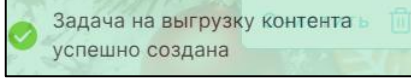


Для процесса экспорта можно установить следующий параметр:

Если активен чекбокс «Нужен детальный лог выгрузки», то в файл с логами сохраняется детальная информация о выгрузке и сравнении файлов контента. Если параметр не задан, файл с детальными логами не формируется.



После того как выбран контент для экспорта, необходимо запустить процесс по кнопке



Далее запустится задача на экспорт контента

Созданная задача отобразится в разделе «История задач».

3. ТАБЛИЧНЫЕ СПИСКИ

Раздел «Табличные списки» состоит из следующих подразделов:

- подраздел «Экспорт ТС»;
- подраздел «Импорт ТС».

3.1. ЭКСПОРТ ТС

В этом подразделе можно экспортировать табличные списки из выбранной SIEM Core. Для экспорта табличных списков следует совершить несколько шагов.

Прежде всего необходимо:

- Выбрать SIEM Core из выпадающего списка либо ввести данные о SIEM Core вручную.
- Кликнуть по кнопке **Посмотреть ТС**.



Рисунок 17

Если на SIEM Core было найдено более одного конвейера, то открывается форма с выбором конвейера. Можно выбрать только один конвейер.

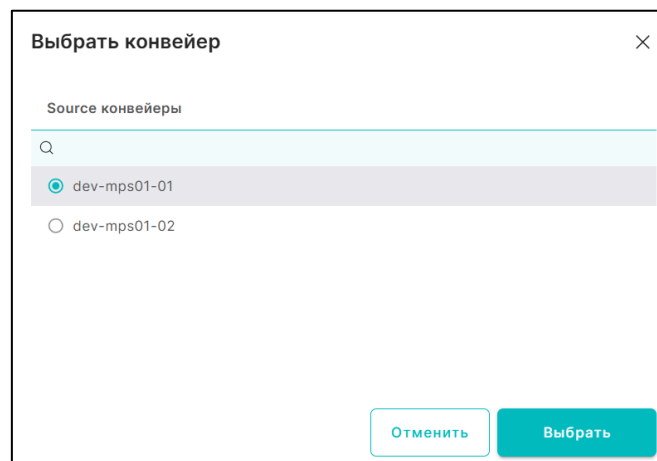


Рисунок 18

После выбора конвейера открывается форма с выбором табличных списков для экспорта:

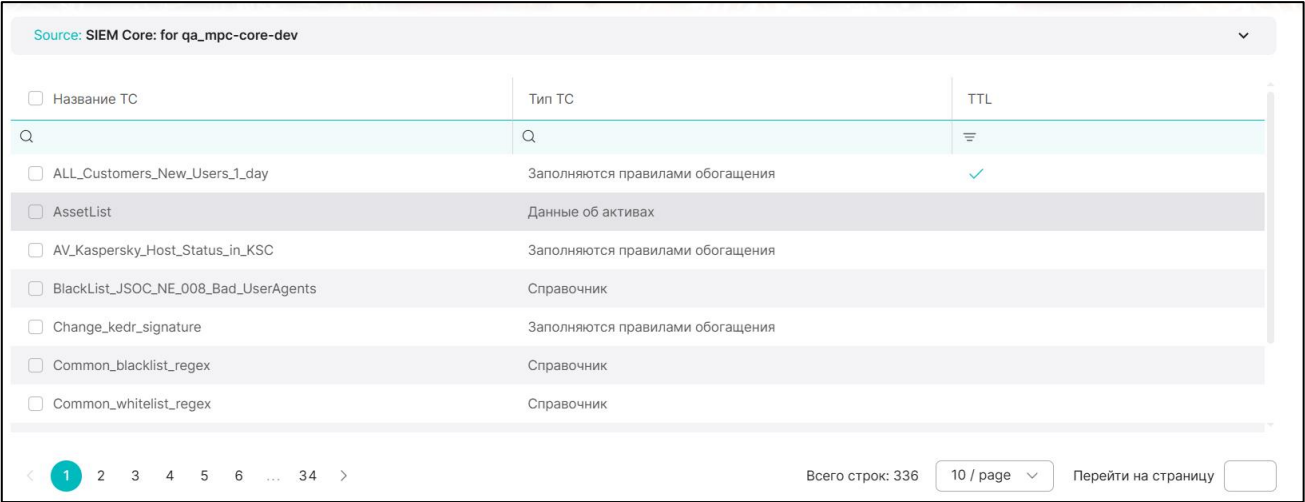
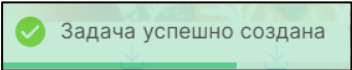


Рисунок 19

Табличный список можно выбрать, активировав чекбокс в соответствующей строке. Доступен множественный выбор и выбор всех табличных списков. Детальное описание формы представлено в таблице:

Параметр в интерфейсе	Функциональность	Описание
Столбец «TTL»	Фильтр, выпадающее поле с возможными значениями: - TTL установлен - TTL не установлен	При наведении на иконку отображается подсказка «Ограничено время жизни записей»
Столбец «Название TC»	Строка поиска по полному или частичному совпадению	В столбце отображаются наименования табличных списков
Столбец «Тип TC»	В столбце отображаются типы табличных списков. Возможные значения: - Справочник - Заполняются правилами корреляции - Заполняются правилами обогащения - Данные об активах - Репутационные списки	Строка поиска по полному или частичному совпадению
Чекбокс в строке каждого TC	Чекбокс по умолчанию не активен	При активации чекбокса в наименовании столбца выбираются все табличные списки

После выбора табличных списков появится кнопка . В каунтере указывается количество выбранных табличных списков. Процесс экспорта TC необходимо запустить по кнопке «Экспорт TC». Далее запустится задача на экспорт табличных списков . Созданная задача отобразится в разделе «История задач».

3.2. ИМПОРТ TC

В этом подразделе можно импортировать табличные списки из одной SIEM Core в другую.

Чтобы импортировать табличные списки, требуется:

- Указать SIEM Core в области «Source»:
 - выбрать SIEM Core из выпадающего списка либо ввести данные о SIEM Core вручную
 - загрузить файл из локальной директории. При клике открывается проводник с рабочим столом для выбора файла.
- Указать SIEM Core в области «Destination».
- Кликнуть по кнопке **Сопоставить TC**.

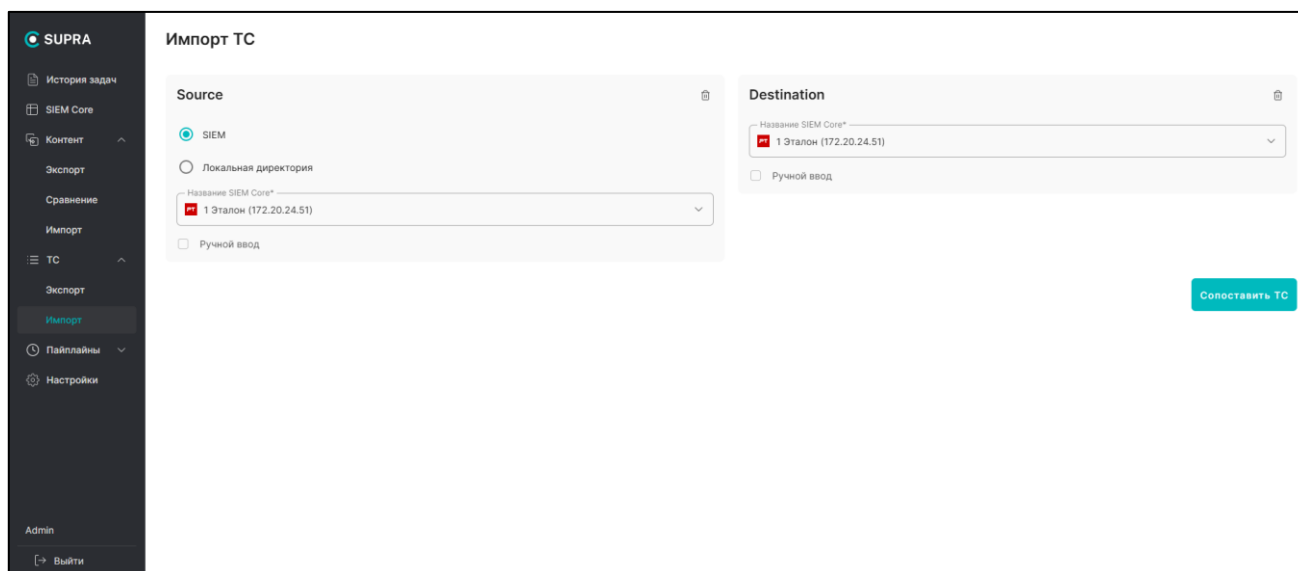


Рисунок 20

Если на указанных SIEM Core было найдено более одного конвейера, то открывается форма с выбором конвейера. В области Source можно выбрать только один конвейер, в области Dest доступен множественный выбор.

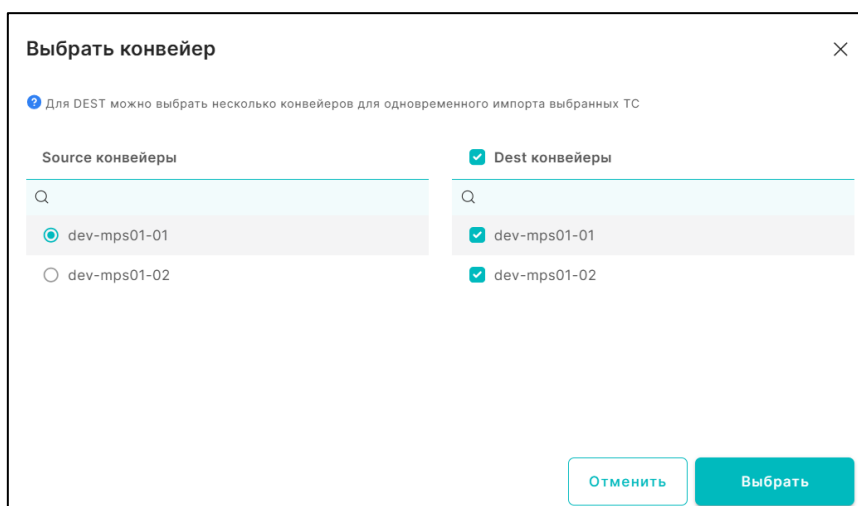


Рисунок 21

Далее открывается форма, в которой отображаются табличные списки. В форме отобразятся только те из них, которые совпадают по наименованию на всех конвейерах Source и Dest и соответствуют следующим типам табличных списков:

- Заполняются правилами корреляции.
- Заполняются правилами обогащения.

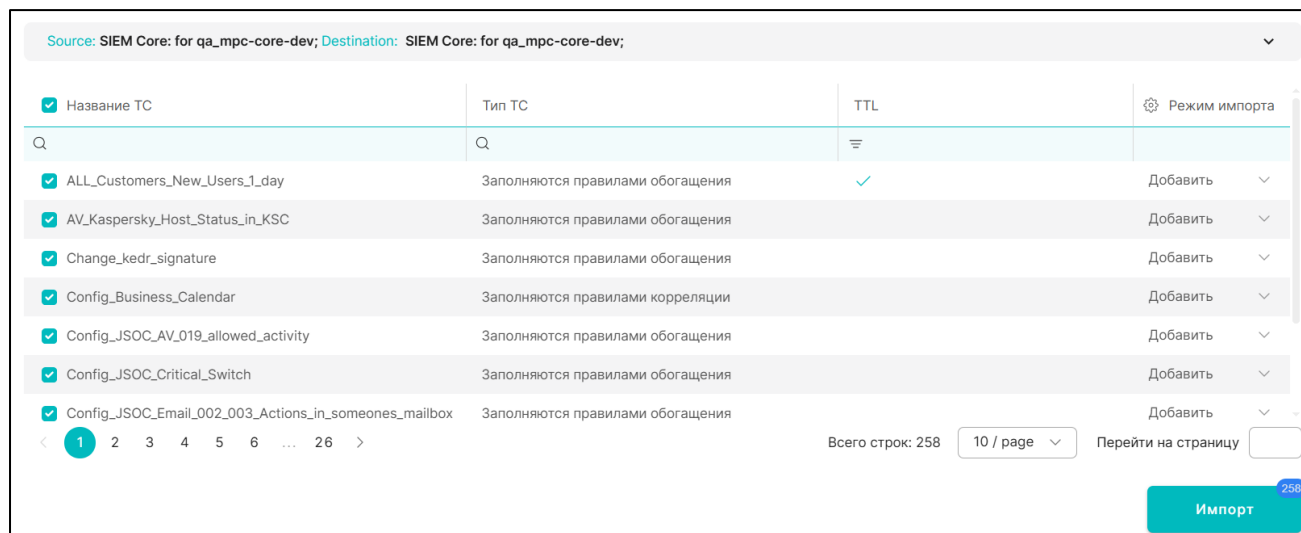


Рисунок 22

Далее следует установить режим импорта в соответствующем столбце «Режим импорта».

Он может устанавливаться и применяться многократно при выборе всех или нескольких объектов в таблице и последующем установлении режима импорта.

Возможные режимы импорта:

- **Добавить.** В этом режиме в табличный список добавляются те строки, которые есть в Source, но их нет Dest.

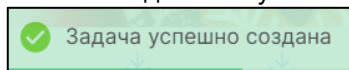
- **Перезаписать.** В этом режиме удаляются все строки внутри табличного списка на Dest, полностью импортируются строки из табличного списка из Source.

Табличный список можно выбрать, активировав чекбокс в соответствующей строке. Доступен множественный выбор и выбор всех табличных списков.

После выбора табличных списков появится кнопка



В каунтере указывается количество выбранных табличных списков. Процесс импорта ТС необходимо запустить по кнопке «Импорт». Далее



запустится задача на импорт табличных списков

Созданная задача отобразится в разделе «История задач».

4. ПАЙПЛАЙНЫ

4.1. ИСТОРИЯ

История задач

SIEM Core

Контент

Экспорт

Сравнение

Импорт

ТС

Экспорт

Импорт

Пайплайны

История

Расписание

Мониторинг

Настройки

Admin

Выйти

История пайплайнов

Очистить фильтры

ID	Пайплайн	Название SIEM Core	Дата по расписанию	Дата начала	Дата завершения	Состояние	Статус
d0eb939e-aa16-45ae-9caa-bb3fe91b2f38	Мониторинг контента	1 Эталон (172.20.24.51)	19.11.2025 14:59:37	19.11.2025 14:59:38	19.11.2025 15:17:07	finished	warning
681a66b3-da94-47a2-b4b7-edaa9eca8e80	Мониторинг контента	OTCpharm	19.11.2025 12:57:43	19.11.2025 12:57:44	19.11.2025 13:18:15	finished	success
881212b6-cc69-4856-94ce-ctbfc29bd3a7	Мониторинг контента	1 Эталон (172.20.24.51)	19.11.2025 12:57:30	19.11.2025 12:57:31	19.11.2025 13:21:44	finished	warning
ed9ec452-4a52-4822-b3e2-7995fe13fd84	Мониторинг контента	1 Эталон (172.20.24.51)	17.11.2025 18:12:19	17.11.2025 18:12:20	17.11.2025 18:30:21	finished	warning
4f2acdab-8a35-4762-8cca-fc7ff2803231	Мониторинг контента	OTCpharm	17.11.2025 18:12:14	17.11.2025 18:12:15	17.11.2025 18:27:31	finished	success
e5c4a92d-f255-4eb5-9e3a-171efe15119c	Мониторинг контента	1 Эталон (172.20.24.51)	17.11.2025 13:09:45	17.11.2025 13:09:46	17.11.2025 13:29:18	finished	warning
481fea8e-6cc0-4c40-a0ee-b8c987b9840d	Мониторинг контента	OTCpharm	17.11.2025 13:09:35	17.11.2025 13:09:37	17.11.2025 13:25:54	finished	success
01b75661-5be1-451b-bf50-cf777bea4d87	Мониторинг контента	GEOP-2	14.11.2025 15:05:06	14.11.2025 16:40:15	14.11.2025 16:40:48	finished	error
c6a17a93-5695-42fe-9cb1-845f8a978ce3	Мониторинг контента	СКДЕGКurch	14.11.2025 15:05:06	14.11.2025 16:39:46	14.11.2025 16:55:26	finished	success
5b836abd-b397-487d-a5f2-9918860fa6e6	Мониторинг контента	СКДЕGM9	14.11.2025 15:05:06	14.11.2025 16:39:26	14.11.2025 16:55:03	finished	success

1 2 3 4 5 ... 73

Всего строк: 728 10 / page Перейти на страницу

Параметр	Описание	Фильтрация	Поиск
ID	Уникальный идентификатор пайплайна мониторинга в формате GUID		Поиск по полному или частичному совпадению
Пайплайн	Тип пайплайна. Возможные значения: - Мониторинг контента - Обновление эталона	Выпадающий список	В столбце отображаются наименования табличных списков
Название SIEM Core	Наименование SIEM Core, по которой проводился мониторинг контента	Выпадающий список со всеми SIEM Core, которые есть в сервисе	Строка поиска по полному или частичному совпадению
Дата старта	Дата и время старта пайплайна по заданному планировщику в формате DD.MM.YYYY HH:MM: SS	Числовой фильтр	Поиск по полному или частичному совпадению
Дата завершения	Дата и время завершения пайплайна в формате DD.MM.YYYY HH:MM: SS	Числовой фильтр	Поиск по полному или частичному совпадению
Состояние	Состояние выполнения пайплайна. Возможные значения: - Created - Progress - In queue - Finished	Фильтр с ограниченным списком значений	
Статус	Статус выполнения пайплайна. Возможные значения: Success	Фильтр с ограниченным списком значений	

W: RT-SOLAR.RU

18

	- Warning - Error		
Логи	Возможность выгрузки логов по процессу выполнения пайплайна. Иконка выгрузки становится активной, если: - задача имеет статус «Success», «Warning» и «Error» (если получилось сформировать файл) - срок хранения файла не превышен (файл хранится 30 дней)		
Результаты	Возможность выгрузки результатов выполнения пайплайнов мониторинга контента. Иконка выгрузки становится активной, если: - задача имеет статус «Success» и нет ошибок - срок хранения файла не превышен (файл хранится 7 дней)		

Просмотр детализированной информации по пайплайну:

Детализация пайплайна

ID:

63fc65d5-a30c-4f40-9373-13bf4bfe15f5

Пайплайн:

Мониторинг контента

Название SIEM Core

1 Эталон (172.20.24.51)

Дата по расписанию:

12.11.2025 12:23:48

Дата начала:

12.11.2025 12:23:50

Дата завершения:

12.11.2025 12:24:24

Статус:

success

Логи:

Результаты:

МОНИТОРИНГ

SUPRA

История задач

SIRM Core

Коммент

TC

Платформы

История

Расширение

Мониторинг

Настройки

Результаты мониторинга

Дата обновления эталона 19.11.2025 13:01:08

В процентах

Очистить фильтры

Статус	Название SEM Core	Дата получения контента SEM Core	Дата успешного выполнения	Всего сценариев	Актуальных сценариев	Неактуальных сценариев	Кастом сценариев	Всего NU	Актуальных NU	Неактуальных NU	Кастом NU	Всего объектов	Актуальных объектов	Неактуальных объектов	Кастом объектов	Результаты
▲	1 Эталон (172.20.24.51)	19.11.2025 15:13:58 ▲	19.11.2025 15:17:07	0	0	0	0	443	442	1	0	11782	11781	0	1	
●	OTCpharm	19.11.2025 13:13:33 ▲	19.11.2025 13:18:19	99	90	33	16	344	268	72	4	11520	11251	144	129	
●	OKDEOKurch	14.11.2025 16:48:47 ▲	14.11.2025 16:55:26	88	0	75	13	376	46	312	18	3628	549	0	3079	
●	OKDEQMB	14.11.2025 16:48:21 ▲	14.11.2025 16:55:03	92	0	76	16	374	46	312	16	3780	549	0	3231	
●	POB-Vietnams	14.11.2025 16:45:59 ▲	14.11.2025 16:50:34	21	0	21	0	424	174	246	4	11679	10670	938	71	
●	EGBNIO-NZ	14.11.2025 16:42:17 ▲	14.11.2025 16:49:14	64	0	41	23	126	7	37	82	4772	549	0	4223	
●	GEOP-MeuJust	14.11.2025 16:39:46 ▲	14.11.2025 16:47:28	76	0	63	13	23	2	7	14	2918	545	0	2373	
●	RTLabs	14.11.2025 16:38:21 ▲	14.11.2025 16:46:42	56	0	51	5	154	7	134	13	3578	549	0	3029	
●	AO-CBT	14.11.2025 16:40:15 ▲	14.11.2025 16:45:44	64	10	42	12	425	224	197	4	11734	10871	790	83	
●	OKDEQOstap	14.11.2025 16:36:35 ▲	14.11.2025 16:45:28	88	0	75	13	374	46	312	16	3361	549	0	2812	

Admin

1

2

3

4

5

6

7

Всего строк: 6810 / pageПерейти на страницу

Параметр	Описание	Фильтрация	Поиск
Статус	Статус выполнения пайплайна. Список возможных значений: - Success - Error	Выпадающий список	Да
Название SIEM Core	Наименование SIEM Core, по которой проводился мониторинг контента	Выпадающий список со всеми SIEM Core, которые есть в сервисе	Да
Дата получения контента SIEM Core	Дата и время, когда сервис последний раз выгрузил контент с SIEM Core, в формате DD.MM.YYYY HH:MM: SS	Числовой фильтр	Да
Дата успешного выполнения	Дата и время завершения пайплайна в формате DD.MM.YYYY HH:MM: SS	Числовой фильтр	Да
Время сценариев	Суммарное количество уникальных идентификаторов сценариев из всех TC JSOC_Core_CustomerKB, со всех конвейеров SIEM Core	Числовой фильтр	Да
Актуальные сценарии	Суммарное количество уникальных сценариев из TC JSOC_Core_CustomerKB, для которых на SIEM Core есть все НУ (должны быть в соответствии с файлом scenarios_mapping.csv), и все сценарии актуальные	Числовой фильтр	Да
Неактуальные сценарии	Суммарное количество уникальных сценариев из TC JSOC_Core_CustomerKB, для которых на SIEM Core есть все НУ (должны быть в соответствии с файлом scenarios_mapping.csv), включая хотя бы один неактуальный сценарий (и нет кастома)	Числовой фильтр	Да
Кастом сценариев	Все остальные случаи при сравнении сценариев	Числовой фильтр	Да
Всего НУ	Суммарное кол-во НУ, выгруженных с SIEM Core (на основании deployment_sets.yaml)	Числовой фильтр	Да
Актуальные НУ	Суммарное количество НУ, которые есть на эталоне и содержат точно такой же набор объектов, которые совпадают по содержимому с эталоном	Числовой фильтр	Да

Неактуальные НУ	Суммарное кол-во НУ, которые есть на эталоне и содержат точно такой же набор объектов, но хотя бы один объект, выгруженный SIEM Core, отличается содержимым от эталона	Числовой фильтр	Да
Кастом НУ	Все остальные НУ, кроме установочных	Числовой фильтр	Да
Всего объектов	Суммарное количество объектов, выгруженных с SIEM Core	Числовой фильтр	Да
Актуальные объекты	Суммарное количество объектов, выгруженных SIEM Core, которые есть на эталоне, и они идентичны	Числовой фильтр	Да
Неактуальные объекты	Суммарное количество объектов, выгруженных с SIEM Core, которые есть на эталоне, но они не идентичны	Числовой фильтр	Да
Кастом объектов	Суммарное количество объектов, которые есть на SIEM Core, но их нет на эталоне	Числовой фильтр	Да
Результаты	Возможность выгрузки результатов выполнения пайплайна мониторинга контента		

Функциональные возможности в разделе «Результаты мониторинга»:

🕒 Дата обновления эталона 17.03.25 12:25	
🔍 В процентах	
📄	
📂	
⚙️ Очистить фильтры	

Просмотр детализированной информации о результатах мониторинга

Детализация результатов

✕

▶

Запустить пайплайн сейчас

Название SIEM Core:

Lyudmila_test_core

Дата получения контента SIEM Core:

23.11.2025 16:24:00

Дата успешного выполнения:

23.11.2025 16:25:07

Статус:

success

Результаты:

📄

Файлы не найдены

⚠️ контент просрочен (дата выгрузки больше 14 дней)

Статистика по наборам установок:

Общее количество: 444

Количество актуальных: 434

Количество неактуальных: 9

Количество кастомизированных: 1

Статистика по сценариям:

Общее количество: 32

Количество актуальных: 27

Количество неактуальных: 4

Количество кастомизированных: 1

Статистика по объектам:

Общее количество: 11782

Количество актуальных: 11769

Количество неактуальных: 3

Количество кастомизированных: 10

Оповещение:

Отправлено: 23.11.2025 16:25:08

Получатели:

i.vatagina@rt-solar.ru

e.mikhaylov@rt-solar.ru

a.bacherova@rt-solar.ru