

РУКОВОДСТВО АДМИНИСТРАТОРА

Solar SUPRA



Оглавление

1. SIEM CORE	3
2. ПАЙПЛАЙНЫ	5
3. НАСТРОЙКИ	9
3.1. ВКЛАДКА «ТЕХНИЧЕСКИЕ ОКНА»	9
3.2. ВКЛАДКА «ЭТАЛОН»	9

1. SIEM CORE

Раздел «SIEM Core» позволяет оптимизировать выбор SIEM Core в формах сервиса путем предварительного заполнения данных по SIEM Core и последующему выбору нужного SIEM Core из списка.

Функционал расположен в левом боковом меню, в разделе «SIEM Core» и отображается в виде табличного представления. Описание табличного представления:

- название Core (текстовое поле, обязательно);
- тип SIEM (выбор из существующих типов, обязательно);
- vault-директория (текстовое поле, обязательно);
- ответственные (текстовое поле, необязательно);
- доступность мониторинга (признак участия SIEM Core в пайплайне автомониторинга);
- дата создания (добавляется системой автоматически, не редактируется);
- комментарии (необязательно).

Название Core	Тип SIEM	Vault директория	Ответственные	Доступность мониторинга	Дата создания ↓	Комментарии
EGISZ-FMBA	MP v.25	I432-MPC-01		✓	22.07.2025 16:00:50	
cs-siem-core	MP v.25	cs-siem-core		ИСКЛЮЧЕН	22.07.2025 16:00:50	
EGRN20	MP v.25	I143sec-mpc02		✓	22.07.2025 16:00:50	
Paul-Hartmann	MP v.25	yc-paul-mpc01		✓	22.07.2025 16:00:50	
SpbMetro	MP v.25	spbm-siem-core		✓	22.07.2025 16:00:50	
EGISZ-RCOD	MP v.25	soc-spb-mpc02		✓	22.07.2025 16:00:50	
CNP-AC-RF	MP v.25	dc1-is-siem-03		✓	22.07.2025 16:00:50	
1 Эталон (172.20.24.51)	MP v.25	msk-mpc-etln		✓	22.07.2025 16:00:50	
GEOP-1	MP v.25	I490-lb-siem-1.medvedko...		✓	22.07.2025 16:00:50	
dev-mpc01	MP v.25	dev-mpc01		ИСКЛЮЧЕН	22.07.2025 16:00:50	

Рисунок 1

Добавление новой SIEM Core происходит по кнопке «Добавить». Далее открывается поп-ап-форма «Создать SIEM Core». Необходимо внести данные в обязательные для заполнения поля.

Создать SIEM Core

Название Core*

Тип Siem*

Vault директория*

Ответственные

Комментарии

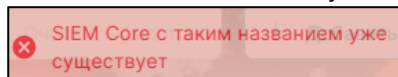
☐ Исключить из Мониторинга

Если чекбокс включен, то данная SIEM Core не участвует в процессе авто-мониторинга пайплайнами

Отменить Сохранить

Рисунок 2

Важно! Поле «Название Core» — уникальное. Если ввести уже существующее название, то отобразится



ошибка

После успешного сохранения данных созданная SIEM Core отобразится в списке SIEM Core в табличном представлении.

2. ПАЙПЛАЙНЫ

В разделе «Пайплайны» можно создать или отредактировать расписание запуска пайплайна мониторинга контента, посмотреть список существующего расписания.

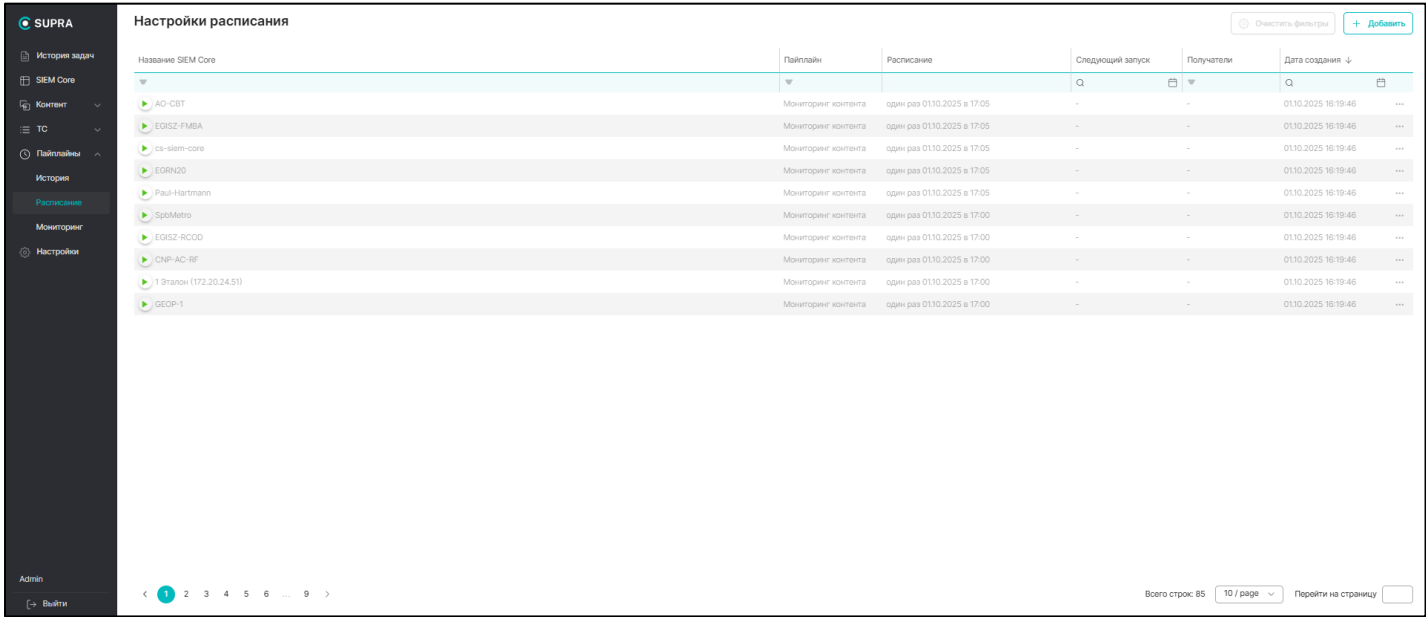
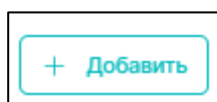


Рисунок 3

Детальное описание формы представлено в таблице:

Параметр	Описание	Сортировка	Фильтрация	Поиск	Комментарий
Кнопка «Запустить немедленно»	Кнопка «Запустить пайплайн сейчас» дает возможность немедленного запуска пайплайна мониторинга из раздела с настройкой расписания				Кнопка активна всегда, для активных и неактивных ов
Название SIEM Core	Наименование SIEM Core, по которой было задано расписание для мониторинга контента	Да	Выпадающий список всех SIEM Core	Да	
Пайплайн	Тип пайплайна. Возможное значение: Мониторинг контента	Да	Выпадающий список	Да	
Расписание	Информация о заданном расписании. Отображает, как часто и в какое время будет запущен пайплайн мониторинга контента	Нет	Нет	Нет	

Следующий запуск	Дата и время следующего запуска в соответствии с расписанием в формате DD.MM.YYYY HH:MM:SS	Да	Да	Да	
Получатели	Электронный адрес ответственного за SIEM Core	Да	Выпадающий список	Да	
Дата создания	Дата и время создания в формате DD.MM.YYYY HH:MM:SS	Да	Да	Да	
Панель «Действия»	В строке расположена панель, отображающая список доступных действий: • активировать расписание • деактивировать расписание • удалить расписание				



Добавление нового а происходит по кнопке «Расписание».

Расписание

Пайплайн*

Отменить

Сохранить

Рисунок 4

Далее нужно установить тип пайплайна: «Мониторинг контента», после чего откроются дополнительные поля для заполнения, они обязательные.

Расписание

Пайплайн*

Мониторинг контента

Название SIEM Core*

Отправить оповещения ответственным за SIEM Core

Дополнительно отправлять оповещение

Дата начала (MSK)

Время начала (MSK)

Как повторять

Один раз

Ежедневно

Еженедельно

Ежемесячно

Нет даты запуска

Отменить

Сохранить

Рисунок 5

Детальное описание формы представлено в таблице:

Поле	
Пайплайн* Мониторинг контента	
Название SIEM Core* Core12345	
Отправить оповещения ответственным за SIEM Core e.kantyshev@rt-solar.ru, a.paramonov@rt-solar.ru, b.smirnov@rt-solar.ru	
Дополнительно отправлять оповещение	
Дата начала (MSK)* 21.10.2023	

W: RT-SOLAR.RU

SOLAR

7

Время начала (MSK)* 14:00	
До какой даты повторять (MSK) Последний повтор пайплайна будет выполнен в указанную дату	
Как повторять Один раз Ежедневно Еженедельно Ежемесячно Пайплайн будет автоматически запущен один раз 21.10.2023 в 14:00	
Как повторять Один раз Ежедневно Еженедельно Ежемесячно Пайплайн будет автоматически запускаться каждый день в 14:00	
Как повторять Один раз Ежедневно Еженедельно Ежемесячно Дни повтора Пн Вт Ср Чт Пт Сб Вс	
Как повторять Один раз Ежедневно Еженедельно Ежемесячно числа каждого месяца каждый 1ый день недели каждого месяца	

После успешного сохранения данных созданное расписание отобразится в списке расписаний в табличном представлении.

3. НАСТРОЙКИ

В разделе «Настройки» расположен функционал по управлению работой сервиса. Администраторам предоставляется возможность:

- Поставить выполнение всех задач на паузу.
- Обновить в хранилище эталонный контент.

3.1. ВКЛАДКА «ТЕХНИЧЕСКИЕ ОКНА»



По кнопке администратор может поставить работу сервиса на паузу. Состояние задач и пайплайнов изменится на «in queue» (в очереди). После снятия паузы работа сервиса возобновится, статус задач и пайплайнов изменится.

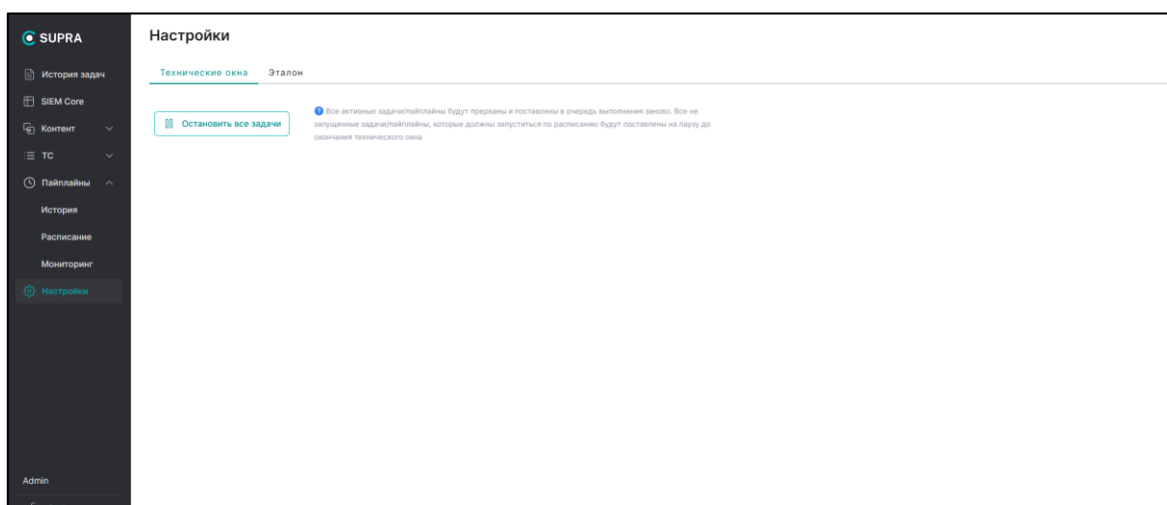
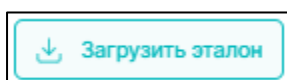


Рисунок 6

3.2. ВКЛАДКА «ЭТАЛОН»



По кнопке администратор может загрузить эталонный контент и обновить его в хранилище. Допустимый формат для загрузки — zip. Также в форме отображается дата и время последней успешной загрузки и логин пользователя, загрузившего эталон.

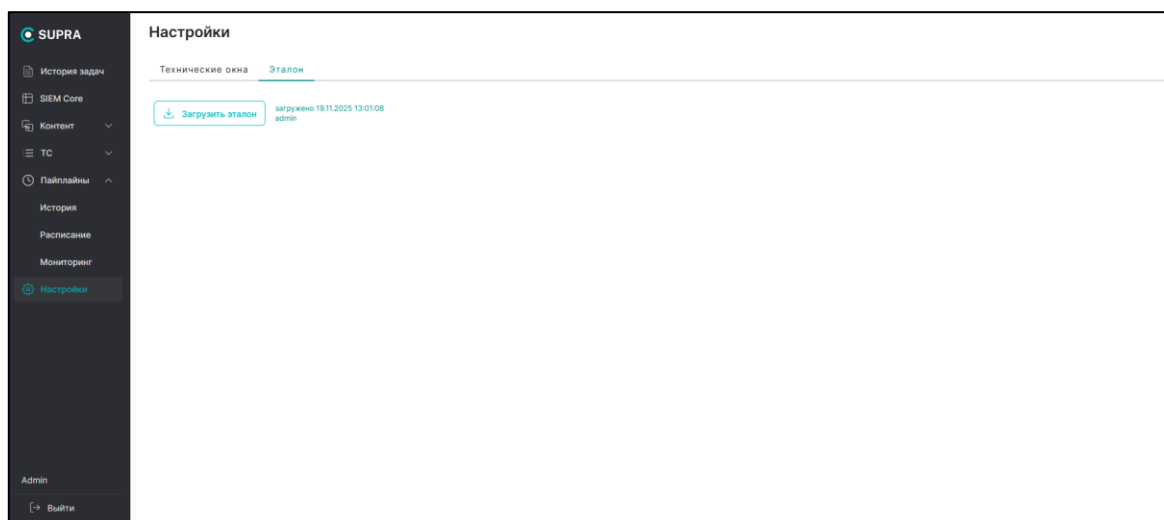


Рисунок 7