

Платформа Радар

Руководство оператора

Версия 4.1.0

ООО «Пангео Радар»

Оглавление

1.	Общие си	Общие сведения о «Платформе Радар»11						
2.	Требования							
3.	Вход в пл	атформу						
4. Интерфейс платформы								
	4.1 Шаг	ка сайта						
	4.2 Пан	ель разделов						
	4.3 Уни	версальные таблицы						
	4.3.1	Настройка сортировки и фильтрации записей таблицы						
	4.3.2	Настройки отображения полей						
	4.4 Боко	овая панель						
	4.4.1	Поиск объектов в списке						
	4.4.2	Сортировка и фильтрация объектов в списке						
	4.4.3	Массовые действия						
	4.5 Пап	ки контента						
	4.6 Фор	мы работы с объектами						
	4.6.1	Шаблоны объектов						
	4.6.2	Визуализации						
5.	События							
	5.1 Оби	ие данные						
	5.1.1	График "Поток событий"						
	5.1.2	Топ-10 значений по выделенной области потока событий						
	5.1.2.1	Масштабирование графика потока событий						
	5.1.3	Список событий						
	5.2 Рабо	эта с фильтрами						
	5.2.1	Настройка запросов						
	5.2.1.1	Добавление запроса в условия фильтра						
	5.2.1.2	Сохранение конфигурации запроса						
	5.2.2	Настройка агрегации						
	5.2.2.1	Добавление агрегации						
	5.2.2.2	Добавление подагрегации						
	5.2.2.3	Сохранение агрегации						
	5.2.3	Работа с пресетами						
	5.2.3.1	Создание пресета						
	5.2.3.2	Применение пресета						
	5.2.3.3	Улаление пресета	48					
	5.2.4	История поиска	48					
	5.3 Pado	та с событиями						
	5.3.1	Созлание инцилента	50					
	532	Побавление события в инцилент	50 57					
	0.0.2	Acousteme coopting p miquident						

5.3.3	Поиск инцидента	
5.3.4	Экспорт списка событий	53
5.3.5	Вспомогательные инструменты для анализа событий	
5.3.5	5.1 Поиск событий	
5.3.5	5.2 Просмотр событий по сформированной агрегации	56
5.3.5	5.3 Настройка плотности отрисовки потока событий	56
5.3.5	5.4 Сортировка событий	
5.3.5	5.5 Настройка набора полей для табличного вида	
6. Инциде	енты ИБ	
6.1 Ин	нциденты	
6.1.1	Общие данные	
6.1.2	Создание инцидента	
6.1.3	Просмотр инцидента	
6.1.3	3.1 Общая информация об инциденте	
6.1.3	3.2 Информация об активе	
6.1.3	3.3 Информация о происшествиях	
613	3.4 История коммуникации	70
614	Назиацение инпилента	71
615	Изменение статуса инцидента	71
616	Лобавление комментария к инциленту	71
6.1.7	Редактирование инцидента	
6.1.8	т сдатирование пада доставния инцидента	
6.1.9	Удаление инцидента	
6.2 Ти	ипы инцидентов	
6.2.1	Общие сведения	
6.2.2	Просмотр и анализ типа инцидента	
6.2.3	Создание типа инцидента	
6.2.4	Редактирование типа инцидента	
6.2.5	Написать ответственному	
6.2.6	Дублирование типа инцидента	
6.2.7	Импорт типов инцидентов	
6.2.8	Экспорт типов инцидентов	
6.2.9	Экспорт типов инцидентов в CSV	
6.2.10	Удаление типа инцидента	
6.3 Гр	уппы инцидентов	
6.3.1	Просмотр группы инцидентов	
6.3.2	Создание группы инцидентов	
6.3.3	Редактирование группы инцидентов	
6.3.4	Назначение группы инцидентов пользователю	
6.3.5	Назначение группы инцидентов группе пользователей	
6.3.6	Дооавление инцидентов в группу	
6.3.7	массовое закрытие инцидентов через группу	
6.3.8	Открепление инцидентов от группы	

	6.3.9	Удаление группы инцидентов					
6.4	4 Про	Іроисшествия на отправку					
6.5 Доп		толнительные поля	83				
	6.5.1	Создание дополнительного поля					
6.5.2		Редактирование дополнительного поля					
6.5.3		Добавление дополнительного поля в инцидент					
	6.5.4	Просмотр значений дополнительного поля					
	6.5.5	Удаление дополнительного поля					
7.	Активы.						
7.1	L Акт	гивы					
	7.1.1	Общие данные					
	7.1.2	Просмотр и анализ актива	89				
	7.1.3	Создание актива					
	7.1.4	Редактирование актива					
	7.1.5	Добавление актива в группу					
	7.1.6	Написать ответственному					
	7.1.7	Удаление актива					
7.2	2 Гру	лпы активов					
	7.2.1	Создание группы активов					
	7.2.2	Просмотр группы активов					
	7.2.3	Редактирование группы активов					
	7.2.4	Настройка автоматического добавления актива в группу					
	7.2.5	Написать ответственному					
	7.2.6	Удаление группы активов					
7.3	B Hac	тройки идентификации активов					
	7.3.1	Создание стратегии идентификации активов	100				
	7.3.2	Редактирование стратегии идентификации активов	100				
	7.3.3	Удаление стратегии идентификации активов	100				
7.4	4 Сет	тевые интерфейсы	100				
	7.4.1	Просмотр сетевого интерфейса					
	7.4.2	Создание сетевого интерфейса					
	7.4.3	Редактирование сетевого интерфейса	103				
	7.4.4	Удаление сетевого интерфейса	103				
7.5	Б Рез	ультаты сканирования					
	7.5.1	Импорт результатов сканирования					
	7.5.2	Просмотр списка результатов сканирования	105				
	7.5.3	Просмотр результата сканирования	106				
	7.5.3.	1 Основная информация о результате сканирования	106				
	7.5.3.	2 Информация о просканированных хостах					
	7.5.4	Сравнение результатов сканирования					
	7.5.4	1 Создание инцидентов по результатам сравнения					
	7.5.4	2 Закрытие инцидентов по результатам сравнения					
	755	Изменение статуса результата сканирования	110				
7 F	, 5 Объ	наружение хостов					
	0.01		Construction and the second				

	7.7 Обнаружение сервисов							
	7.8	Сбор данных						
8.	Coor	гветст	вие ПО	115				
	8.1	Общи	ие сведения					
	8.2	Резул	ьтаты соответствия ПО					
	8.2.1	L	Запуск процесса проверки соответствия ПО					
	8.2.2	2	Просмотр информации о результате соответствия ПО					
	8.2.3	3	Удаление результатов соответствия ПО					
	8.3	Спис	ок ПО					
	8.3.1	L	Просмотр информации о ПО					
	8.3.2	2	Просмотр информации об активах, на которых установлено ПО					
	8.3.3	3	Редактирование записи о ПО					
	8.3.4	1	Удаление записи о ПО из платформы					
	8.4	Спис	ок групп ПО					
	8.4.1	L	Создание группы ПО					
	8.4.2	2	Просмотр группы ПО					
	8.4.3	3	Редактирование группы ПО					
	8.4.4	1	Удаление группы ПО					
	8.5	Прав	ила соответствия ПО					
	8.5.1	L	Создание правила соответствия ПО					
	8.5.2	2	Просмотр правила соответствия ПО					
	8.5.3		Редактирование правила соответствия ПО					
	8.5.4	1	Удаление правила соответствия ПО					
	8.6	Набо	ры правил соответствия ПО					
	8.6.1	L	Создание политики соответствия ПО					
	8.6.2	2	Просмотр политики соответствия ПО					
	8.6.3	3	Редактирование политики соответствия ПО					
	8.6.4	1	Удаление политики соответствия ПО					
9.	Корј	релято	p					
	9.1	Общи	ие данные					
	9.2	Прав	ила корреляции					
	9.2.1	L	Просмотр статистики работы правил					
	9	.2.1.1	Вкладка "Инциденты"					
	9	.2.1.2	Вкладка "Результаты"					
	9	.2.1.3	Вкладка "Лог изменений"					
	9	.2.1.4	Вкладка "Лог правила"					
	9	.2.1.5	Вкладка "Метрики"					
	9.2.2	2	Создание и настройка правила					
	9	.2.2.1	Создание правила с помощью визуального конструктора					
	9	.2.2.2	Создание правила с помощью скриптового языка Lua					
	9.2.3 I		Редактирование правила					
	9.2.4		Активация правила					
	9.2.5	5	- Перезапуск правила					

9.2.6	Б Дублирование правила	
9.2.7	7 Конвертирование правила в код Lua	
9.2.8	3 Импорт правил	
9.2.9	Э Экспорт правил	
9.2.1	10 Удаление правила	
9.2.1	11 Массовые действия над правилами	
9.2.1	12 Действия над результатами сработок правила	
9	0.2.12.1 Создание инцидента	159
9	0.2.12.2 Просмотр события	159
9.3	Пересылка событий	
9.3.1	l Общие данные	
9.3.2	2 Включение пересылки событий	
9.3.3	3 Просмотр фильтра для пересылки событий	
9.3.4	4 Создание фильтра для пересылки событий	
9.3.5	5 Редактирование фильтра для пересылки событий	
9.3.6	5 Дублирование фильтра для пересылки событий	
9.3.7	7 Импорт фильтров	
9.3.8	3 Экспорт фильтров	
9.3.9	Э Удаление фильтра	
9.4	Фильтры потока событий	
9.4.1	l Общие данные	
9.4.2	2 Просмотр фильтра потока событий	
9.4.3	3 Создание фильтра потока событий	
9.4.4	4 Редактирование фильтра потока событий	
9.4.5	5 Дублирование фильтра потока событий	
9.4.6	5 Импорт фильтров потока событий	
9.4.7	7 Экспорт фильтров потока событий	
9.4.8	3 Удаление фильтра потока событий	
9.5	Макросы	
9.5.1	l Общие данные	
9.5.2	2 Просмотр макроса	
9.5.3	3 Создание макроса	
9.5.4	4 Редактирование макроса	
9.5.5	5 Дублирование макроса	
9.5.6	5 Импорт макросов	
9.5.7	7 Экспорт макросов	
9.5.8	3 Удаление макроса	
9.6	Шаблоны алертов	
9.6.1	I Общие данные	
9.6.2	2 Просмотр шаблона "алерта"	
9.6.3	3 Создание шаблона "алерта"	
9.6.4	4 Редактирование шаблона "алерта"	
9.6.5	5 Дублирование шаблона "алерта"	
9.6.6	5 Удаление шаблона "алерта"	

9.7 L	Іаблоны группировки	
9.7.1	Общие данные	
9.7.2	Просмотр шаблона группировки	
9.7.3	Создание шаблона группировки	
9.7.4	Редактирование шаблона группировки	
9.7.5	Дублирование шаблона группировки	
9.7.6	Удаление шаблона группировки	
9.8 T	абличные списки	
9.8.1	Общие данные	
9.8.2	Создание табличного списка	
9.8.3	Работа с записями табличного списка	
9.8.4	Редактирование табличного списка	
9.8.5	Дублирование табличного списка	
9.8.6	Импорт табличных списков	
9.8.7	Экспорт табличных списков	
9.8.8	Удаление табличного списка	
9.8.9	Массовые действия над табличными списками	
9.9 P	етроспективная корреляция	
9.9.1	Общие данные	
9.9.2	Добавление задачи для ретроспективной корреляции	
9.9.3	Остановка задачи	
9.9.4	Перезапуск задачи	
9.9.5	Удаление задачи	
9.9.6	Массовые действия над задачами	
10. Парам	етры	189
10.1	Основные параметры	
10.2	Оповещения по задержкам	191
10.3	Черный список ID плагинов	193
10.4	Фоновые задачи	
10.5	Интеграции	195
10.6	Типы интеграций	196
10.7	Папки контента	196
10.8	Шаблоны	
11. Рабочі	1е столы	199
11.1	Общие данные	199
11.2	Создание рабочего стола	
11.3	Редактирование рабочего стола	
11.4	Управление виджетами	
11.4.1	Установка периода и обновление данных виджетов	
11.4.2	Добавление виджета на рабочий стол	
11.4.3	Переход к табличному представлению данных	
11.4.4	Редактирование виджета	
11.4.5	Копирование настроек виджета	
11.4.6	Изменение расположения виджета	
11.4.7	Изменение размера виджета	

11.4.8	Удаление виджета					
11.5	Копирование рабочего стола					
11.6	Создание отчета					
11.7	7 Удаление рабочего стола					
11.8	Grafana. Единицы измерения и временной диапазон					
12. Констр	руктор виджетов					
12.1	Особенности работы в конструкторе					
12.2	Конструктор запросов					
12.2.1	Добавление запроса					
12.2	2.1.1 Шаг 1. Выбор источника данных и датасета					
12.2	2.1.2 Шаг 2. Выбор периода формирования запроса					
12.2	2.1.3 Шаг З. Настройка набора полей					
12.2	2.1.4 Шаг 4. Условия фильтрации					
12.2	2.1.5 Шаг 5. Группировка и Сортировка					
12.2.2	Копирование запроса					
12.2.3	Дублирование запроса					
12.2.4	Удаление запроса					
12.3	Настройка внешнего вида виджета					
12.3.1	Основные настройки виджета					
12.3.2	Временной ряд					
12.3	3.2.1 Шаг 1. Настройка осей					
12.3	3.2.2 Шаг 2. Настройка визуализации					
12.3	3.2.3 Шаг З. Легенда					
12.3.3	Круговая диаграмма					
12.3.4	Таблица					
12.3.5	Текст					
12.3.6	Гистограмма					
12.3	3.6.1 Шаг 1. Настройка осей					
12.3	3.6.2 Шаг 2. Настройка визуализации					
12.3	3.6.3 Шаг З. Легенда					
12.3.7	Метрика					
12.3.8	Изображение					
12.4	Копирование виджета					
12.5	Предустановки					
13. Отчеть	51					
13.1	Общие данные					
13.2	Создание отчета					
13.3	Конструктор отчета					
13.3.1	Добавление страницы					
13.3.2	Выбор периода формирования данных виджетов					
13.3.3	Настройка наименования отчета в момент генерации					
13.3.4	Настройка страниц					

	13.3.4.1		Настройка верхнего колонтитула	
13.3.4.2		.4.2	Настройка нижнего колонтитула	
13.3.4.3		.4.3	Настройка стиля шрифта	
13	.3.5	Had	тройка виджетов	
	13.3	.5.1	Добавление виджета	246
	13 3	5.2	Релактирование вилжета	246
	13.3	53		247
	10.0			247
	12.2	.5.4	изменение расположения виджета	
	13.3	.5.5	изменение размера виджета	
10	13.3	.5.6	Удаление виджета	
13	.3.6	Изм	ленение порядка страниц	
13 A	.3.7	у да Настр	ление страницы	
13.4	11	Пастр	очка расписания генерации отчета	240
13 5	.4.1	Настр	ойка прав доступа к отцету	240
13.6		Импо	опка приз доступа к от тету	
13.7		Экспо	рт отчетов	
13.8		Удале	• ние отчета	
13.9		Архин	в отчетов	
14. Co	ообще	ения		
14.1		Созда	ние сообщения	
14.2		Просм	ютр сообщения	
14.3		Ответ	на сообщение	
14.4		Отмет	ить сообщения прочитанными	
14.5		Отмет	ить прочитанные сообщения как непрочитанные	
14.6		Экспо	рт сообщений	
14.7		Удале	ние сообщений	
15. Ilp	рофил	ть полі	530Вателя	
15.1		Измен	ение информации о своеи учетнои записи	
15.2		Полки		
15.4		Выхо	лиз всех сессий	258
15.5		Просм	иотр журнала изменений учетной записи	
15.6		Настр	ойка оповещений	
15.7		Просм	иотр истории действий в платформе	
16. Ин	нтегра	ации		
16.1		RT Pr	otect EDR	
16	.1.1	Обі	цие сведения	
	16.1	.1.1	Характеристики системы	
	16.1	.1.2	Активные действия	
	16.1	.1.3	Синхронизация инцидентов и активов	
	16.1	.1.4	Параметры типа интеграции RT Protect EDR	

16.1.2 EDF	действия	266
16.1.2.1	Создание EDR действия	267
16.1.2.2	Просмотр EDR действия	268
16.1.2.3	Редактирование EDR действия	270
16.1.2.4	Дублирование EDR действия	270
16.1.2.5	Изменение статуса EDR действия	270
16.1.2.6	Экспорт EDR действий	270
16.1.2.7	Импорт EDR действий	271
16.1.2.8	Удаление EDR действий	271
16.1.3 Hac	гройка интеграции RT Protect EDR	271
16.1.3.1	Шаг 1. Создание экземпляра интеграции с RT Protect EDR	271
16.1.3.2	Шаг 2. Настройка задачи синхронизации активов	273
16.1.3.3	Шаг З. Настройка активных действий для интеграции	274
16.1.3.4	Шаг 4. Активация интеграции	274
16.1.4 Рабо	эта с интеграцией RT Protect EDR	
16.1.4.2	Работа с правилами корреляции	278
16.1.4.3	Работа с активами	281
16.1.4.4	Работа с инцидентами	282
16.1.4.5	Просмотр журнала выполнения действий по интеграции	283
16.2 Kasper	sky Security Center	
16.2.1 Xap	актеристики системы	284
16.2.2 Hac	гройка интеграции	285
16.2.2.1	Шаг 1. Создание экземпляра интеграции с KSC	285
16.2.2.2	Шаг 2. Создание задачи по синхронизации активов	286
16.2.2.3	Шаг 3. Активация экземпляра интеграции с KSC	287
16.2.3 Рабо	эта с интеграцией	

1. Общие сведения о «Платформе Радар»

Специализированное программное обеспечение «Платформа Радар» (далее – СПО РАДАР, Платформа Радар, платформа) является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и предназначено для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности (далее – ИБ) с целью выявления инцидентов и организации реагирования на них.

Платформа обеспечивает решение следующих задач:

- сбор информации об активах, их учет и управление записями об активах;
- сбор событий ИБ от активов и/или от установленного на активах ПО;
- автоматическая обработка поступивших событий (нормализация, обогащение);
- загрузка и анализ результатов работы сканеров уязвимостей;
- корреляция событий, создание записей об инцидентах и управление ими;
- автоматизированный контроль реагирования на инциденты, контроль устранения;
- получение, обновление и использование информации об угрозах;
- ручной анализ событий ИБ при расследовании инцидентов;
- формирование отчетов, в том числе в графическом виде (рабочие столы).

СПО РАДАР имеет сертификат соответствия ФСТЭК России № 4210 от 05 февраля 2020 г. (переоформлен 22 марта 2022 г.), срок действия: пять лет.

2. Требования

Для работы с сервисом пользователю необходимы:

- Современный компьютер с операционной системой. Работа с сервисом возможна на следующих ОС:
 - Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
 - Apple Mac OS X: 10.6 (Snow Leopard) и выше;
 - Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux
 Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов
- Монитор с разрешением не менее 1920х1080.

Для работы с графическим интерфейсом **СПО Радар** на АРМ пользователя должен быть установлен один из следующих браузеров:

- Microsoft Edge;
- Google Chrome;
- Mozilla Firefox;
- Яндекс.Браузер.

3. Вход в платформу

Вход пользователей в Платформу Радар осуществляется через Web-браузер.

Для входа в платформу в браузере перейдите по адресу https://host:port//

Где:

- host IP-адрес или доменное имя устройства, на котором расположен сервер платформы;
- port порт, который задан для точки подключения.

Откроется окно «Вход» (см. «Рис. 1»).

ПАНГЕО РАДАР
Вход
Имя пользователя или E-mail
Пароль
Вход

Рис. 1 – Окно входа в платформу

Укажите имя пользователя и пароль в соответствующих полях и нажмите кнопку Войти.

При первой аутентификации **Платформа Радар** может потребовать от пользователя сменить пароль.

После входа в платформу откроется раздел «Рабочие столы», в котором отображаются интерактивные информационные панели с информацией о текущем состоянии безопасности. Подробнее см. раздел «<u>Рабочие столы</u>».

4. Интерфейс платформы

Интерфейс платформы состоит из шапки сайта, панели разделов, боковой панели, рабочей области и элементов управления

Рабочая область раздела имеет два варианта представления:

- через универсальные таблицы;
- через боковую панель и формы работы с объектами (просмотр, создание, редактирование).

По умолчанию все разделы открываются в табличном представлении (см. Рис. 2).

Панель разделов Шапка сайта Рабочая область (Ун					ъ (Универсальная	таблица	а) Эле	ементы упра I	вления-
📃 🏅 пангео 172.30.254.97 ~	∕ ⊓	равила корреляции				Лицензия ак	тивна до: 2027-11-16	 Документация 	() admin v
Рабочий стол	Пр	равила корреляции							
Q События									
③ Инциденты ~	V	Создать Удалить Удалить все Экс	портировать З	кспортироват	все Импортировать Переместит	ь в папку		Выбрано: (0 C @
СВ Активы		Название ↓↑	` Акти ↓↑	Ретр	Тип инцидента 🗸 🗍	Сраб 🥼	Обновлено	Создано 🥼	
_		Active Directory Group Enumeration With	Нет	Нет	MS-WIN-Обнаружение разрешен	-	2025-04-02 13:51:25	2025-03-14 16:42:16	◎ ⁄ ⊡ _
Соответствие ПО		AD - Многочисленные неуспешные	Нет	Нет	AD - Многочисленные неуспешн	-	2025-04-02 13:51:39	2024-11-28 09:41:10	◎ ⁄ ū —
% Коррелятор 🔷		Auditd - Добавление заданий в cron	Да	Нет	Добавление заданий в cron	0	2025-04-02 13:53:36	2024-05-30 16:11:31	◎ ⁄ ū
Правила корреляции		AuditD - Обнаружение сжатия данных	Да	Нет	Linux - Обнаружение сжатия	0	2025-04-02 13:51:08	2024-08-08 11:49:36	© 0 fi
Пересылка событий		AuditD - Обнаружено изменение в	Да	Нет	Linux - Обнаружено изменение в	0	2025-04-02 13:52:37	2024-08-08 11:49:39	◎ ⁄ Ē
Фильтры потока событий		AuditD - Обнаружено изменение	Да	Нет	Linux - Обнаружено изменение	0	2025-04-02 13:51:48	2024-08-08 11:49:36	© ∥ ⊡
Макросы		AuditD - Обнаружено изменение прав	Да	Нет	Linux - Обнаружено изменение	0	2025-04-02 13:50:19	2024-08-08 11:49:39	© 0 fi
Шаблоны алертов		AuditD - Обнаружено разделение файла	Да	Нет	Linux - Обнаружено разделение	0	2025-04-02 13:50:34	2024-08-08 11:49:40	© ∥ ⊡
Шаблоны группировки		AuditD - Обнаружено создание скрытой	Да	Нет	Linux - Обнаружено создание	0	2025-04-02 13:51:01	2024-08-08 11:49:36	© 0 🖞
Табличные списки		AuditD - Обнаружено удаление	Да	Нет	Linux - Обнаружение удаления	0	2025-03-12 07:05:35	2024-08-08 11:49:40	© ∥ ⊡
		AuditD - Обнаружен поиск паролей	Да	Нет	Linux - Обнаружен поиск паролей	0	2025-04-02 13:49:59	2024-08-08 11:49:36	© ∥ ⊡
Ретроспективная корре		AuditD - Остановлен сервис межсетевог	Да	Нет	Linux - Остановлен сервис	0	2025-04-02 13:52:21	2024-08-08 11:49:36	◎ ⁄ Ē
ж Источники 🗸 🗸		AuditD - Попытка передачи данных из	Да	Нет	Linux - Попытка передачи данны	0	2025-04-02 13:50:08	2024-08-08 11:49:41	• 1
🙌 Параметры 🗸 🗸		AuditD - Создан новый пользователь	Да	Нет	Linux - Создан новый пользователь	0	2025-04-08 11:22:04	2024-08-08 11:49:41	♥ Ø 1
🐵 Администрирование 🗸 🗸	<	1 2 3 4 5 6 7	··· 11 >	50 / страни	ца \vee				

Рис. 2 – Интерфейс Платформы Радар. Табличное представление

Для переключения с табличного представления раздела на боковую панель необходимо открыть объект на просмотр (кнопка ^(O) или по ссылке в колонке **Название**). Откроется представление раздела через боковую панель и форма просмотра выбранного объекта (см. «Рис. 3»).

Панель разделов Боковая	а панель Шапка сайта	Рабочая область	Элементы управления
📃 👹 пангео 172.30.254.138 🗸 Правила н	корреляции		⊙ База знаний @ admin ∨
© Рабочий стол	а с + Множественны	іе неудачные попытки входа	а Активное Перезалустить 🕑 Открыть редактор 🔅
 О Инциденты ✓ Инциденты ✓ Инциденты ✓ Изманене: 2024-09-05 Саяботсе: 1, Озибос 0 Соработсе: 1, Озибос 0 Соответствие ПО ✓ Необычное врем Не активнее (Ретрос. Жоррелятор ✓ Измоте: 0, Озибос 0 Сработо: 0, Озибос 0 	неудачные 5 14:27:19 ID: Создано: ия входа в си нективное 3 14:11:16 Organizations: 1 14	а5е6b264-455е-412а-933с-b176e6f2cbct 2024-07-10 12:16:49 2024-09-04 17:13:21 Активная версия от Lua скрият Мисжественные неудачные попытки вхо Тестовое правило для обработки событи Нет Да иб): Нет Нет жЯ: windows_eventlog	9 0 т 2024-09-04 17:13:21 Эда на одном узле под разными учетными записими ий windows
Шаблоны группировки Табличные списки	К Инциденты Результат	ъ Логизменений Логошибок Метр	C
Ретроспективная корре	Eps		
ж Источники	0.000000007		
₩ Параметры 🗸	0.000000005 - 0.0000000004 -		
Администрирование ч Добавить г	0.00000003 - 0.000000002 - 0.000000001 - 0.00 11 июл 11 июл	а 0946 11 июля 0953 11 июля 1000	11 work 1006 11 work 1013 11 work 1020 11 work 1025

Рис. 3 – Интерфейс Платформы Радар. Представление через боковую панель и формы объектов

4.1 Шапка сайта

Шапка сайта является единой для всех разделов платформы и содержит следующие элементы управления:

Кнопка	Действие
	показать/скрыть панель разделов
master 🗸	выбор инстанса
База знаний	доступ к базе знаний платформы
\bigotimes admin \checkmark	наименование текущей учетной записи и доступ к выходу из учетной записи

4.2 Панель разделов

Для каждого пользователя список разделов формируется индивидуально в соответствии с возможностями, выданными данному пользователю.

В интерфейсе доступны следующие разделы:

- События. Раздел предназначен для просмотра и анализа событий информационной безопасности.
- Инциденты ИБ. Раздел содержит следующие подразделы:
 - «Инциденты» расследование инцидентов информационной безопасности;

- «Типы инцидентов» сведения о уязвимостях, нарушениях политики, аномальной сетевой активности которые могут послужить основой для возникновения инцидента;
- «Группы инцидентов» управление группами инцидентов и массовые операции над инцидентами через группы;
- «Происшествия на отправку» отправка происшествий, выявленных в критической информационной инфраструктуре (КИИ) Российской Федерации, в национальный координационный центр по компьютерным инцидентам;
- «Дополнительные поля» настройка параметров дополнительной информации, которую можно добавить к инцидентам.
- Активы. Раздел содержит следующие подразделы:
 - «Активы» управление и анализ состояния активов;
 - «Группы активов» управление группами активов;
 - «Настройки идентификации активов» настройка сравнения отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в платформе;
 - «Сетевые интерфейсы» сведения о сетевых интерфейсах, обнаруженных у активов;
 - «Результаты сканирования» изучение данных по наличию уязвимостей, полученные сторонними сканерами уязвимости в ходе работы и импортированные в платформу;
 - «Обнаружение хостов» сканирование подсети, в результате которого может быть получен набор данных, достаточный для идентификации актива;
 - «Обнаружение сервисов» сбор данных о сервисах на выбранных активах;
 - «Сбор данных» сбор общих данных на выбранных активах.
- Соответствие ПО. Раздел содержит следующие подразделы:
 - «Результаты соответствия ПО» просмотр результатов всех текущих проверок соответствия ПО;
 - «Список ПО» перечень всего программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов;
 - «Список групп ПО» управление группами ПО;
 - «Наборы правил соответствия ПО» настройка политик для выполнения проверки соответствия ПО;
 - «Правила соответствия ПО» настройка регулярных выражений, по которым формируются политики для выполнения проверки соответствия ПО.
- Коррелятор. Раздел содержит следующие подразделы:
 - «Правила корреляции» управление правилами корреляции;
 - «Пересылка событий» управление фильтрами потока событий, которые применяются для отправки событий на другой экземпляр платформы;

- «Фильтры потока событий» управление фильтрами потока событий, которые применяются в правилах корреляции;
- «Макросы» управление модулями поведения для правил корреляции;
- «Шаблоны алертов» управление шаблонами "алертов";
- «Шаблоны группировки» управление шаблонами группировки событий;
- «Табличные списки» управление справочниками;
- «Ретроспективная корреляция» проведение ретроспективного анализа на основе данных хранимых в платформе
- Источники. Раздел содержит следующие подразделы:
 - «Источники» подключение и настройка источников событий информационной безопасности;
 - «Отладка источника» проверка работы правил разбора и обогащения для выбранного источника;
 - «Правила разбора» управление правилами разбора поступающих событий;
 - «Обогащение» управление правилами обогащения разобранных событий;
 - «Группы GROK» управление группами пользовательских GROK паттернов;
 - «Паттерны GROK» управление пользовательскими GROK паттернами;
 - «Поля события» настройка маппинга полей события, используемых в процессах разбора и нормализации;
 - «Агенты сбора» настройка агентов сбора событий от источников;
 - «Профили сбора» управление профилями сбора событий ИБ на выбранных агентах сбора.

Примечание: подробнее о работе с источниками событий ИБ, настройке лог-коллектора и правил разбора событий см. руководство «Работа с источниками событий ИБ».

- Параметры. Раздел содержит следующие подразделы:
 - «Основные параметры» настройка основных параметром Платформы Радар;
 - «Оповещения по задержкам» настройки автоматических оповещений по задержкам в обработке инцидентов операторами;
 - «Черный список ID плагинов» настройка списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы;
 - «Фоновые задачи» просмотр информации о запущенных задачах ретроспективной корреляции, синхронизации и отчетов;
 - «Интеграции». Управление экземплярами интеграций со сторонними системами;
 - «Типы интеграций». Просмотр доступных классов систем, с которым можно настроить интеграцию, а также переключение платформы в режим работы с соответствующим типом интеграции;

- «Папки контента». Управление папками для структурирования пользовательского контента;
- «Шаблоны». Управление шаблонами форм пользовательского контента.
- Сообщения. Раздел предназначен для просмотра и управления личными сообщениями, создаваемые в рамках работы с платформой, а также для обмена сообщениями с другими пользователями платформы.
- Профиль. Раздел предназначен для просмотра и управления своей учетной записью, оповещениями, а также для просмотра истории действий в платформе.
- Рабочие столы. Раздел предназначен для оперативного отслеживания данных о состоянии информационной безопасности с помощью интерактивных информационных панелей.
- Отчеты. Раздел предназначен для формирования отчетов о состоянии информационной безопасности.

4.3 Универсальные таблицы

Универсальные таблицы в платформе – это список объектов, представленных в табличном виде и имеющие единые элементы управления (см. «Рис. 4»).

≡	К ПАНГЕ РАДАР	° 172.30.254.138 ∨ ∣ Отчёты					 База знаний 	1 (2)) admin 🗸
â	Отч	іёты							
Q									
()	C	∇ Создать Удалить Удалить все Экс	портировать	Экспортировать все	Импортировать				Ô
		Название ↓↑	Создано	Создано 🕼			авило генерации		
⊊₿		Новый отчет	13:36:24 09.07.2024			*/1	5 * * * *		0
ů		Ежедневный отчет	14:10:51 19.07.2024			15	23 * * *		0
°P.+	<	1 > 10 / страница ~							
ж									
44									
0									

Рис. 4 -- Рабочая область. Таблицы

Элементы управления располагаются над таблицей и в общем случае состоят из следующих кнопок:

Кнопка	Действие
C	обновление данных
V	настройка сортировки и фильтрации записей таблицы
v	если у кнопки есть специальный значок, то это означает что к таблице применяется фильтр
Создать	создание записи/объекта в таблице

Кнопка	Действие					
Удалить	удаление выбранной записи/объекта из таблицы					
Удалить все	удаление всех показанных записей/объектов. Будут удалены все записи/объекты, попавшие под параметры сортировки и фильтрации					
Экспортировать	экспорт выбранной записи/объекта					
Экспортировать все	экспорт всех показанных записей/объектов. Будут выгружены в архив все записи/объекты, попавшие под параметры сортировки и фильтрации					
Экспортировать выбранные в csv	массовый экспорт выбранных записей/объектов в формат CSV					
Экспортировать в csv	экспорт всех показанных записей/объектов в формат CSV. Будут выгружены в файлы формата CSV все записи/объекты, попавшие под параметры сортировки и фильтрации					
Импортировать	импорт записей/объектов в таблицу					
Переместить в папку	переместить выбранные объекты в папку					
0	настройка столбцов таблицы					

В колонках таблицы могут располагаться следующие кнопки:

Кнопка	Действие
↓ ↑	выбор направления сортировки выбранной колонки
0	просмотр подробных сведений об объекте
Ø	изменение информации об объекте
间	удаление объекта

4.3.1 Настройка сортировки и фильтрации записей таблицы

Для поиска необходимого объекта по значениям полей и формирования списка может быть использован фильтр. Для настройки фильтра выполните следующие действия:

1. Нажмите на кнопку . Откроется блок для настройки сортировки и фильтрации (см. «Рис. 5»).

Фильтры На	азвание: ×	+				
Сортировка	ऻ Созд	ано ×	+			
Сбросить	Применит	ъ				
CV	Создать	Удалить	Удалить все	Экспортировать	Экспортировать все	Импортировать

Рис. 5 – Таблица. Блоки для настройки фильтров и сортировки

- 2. В блоке **Фильтры** нажмите кнопку «+» для добавления столбца, по которому будет выполняться фильтрация. Можно выполнить фильтрацию по значения нескольких столбцов.
- 3. В блоке **Сортировка** нажмите кнопку «+» для выбора столбца, по значениям которого будет задано направление сортировки (↓, ↑). Можно выполнить сортировку по значениям нескольких столбцов.
- 4. Нажмите кнопку **Применить**. При просмотре таблицы к ней будет автоматически применяться настроенный фильтр.
- 5. Если необходимо очистить параметры фильтра, то нажмите кнопку Сбросить.

4.3.2 Настройки отображения полей

Для изменения состава отображаемых полей (колонок таблицы) используйте кнопку При нажатии на кнопку откроется список, в котором можно выбрать поля для отображения (см. «Рис. 6»).

се поля	Отображаемые пол	ія	
Q Название поля	Q Название поля		
Название	Создано	$^{\sim}$ $^{\vee}$	×
	Правило генерации	~ ~	×

Рис. 6 – Настройки отображения полей

4.4 Боковая панель

В общем случае боковая панель предназначена для поиска, сортировки, фильтрации и выбора объекта, для вывода информации о нем в рабочей области (см. «Рис. 7»).



Рис. 7 – Боковая панель. Список объектов

На боковой панели доступны следующие элементы управления:

Кнопка	Действие
+	показать/скрыть панель разделов
\bigtriangledown	настройка сортировки и фильтров для поиска
	 включение возможности выбора объектов для выполнения над ними массовых операций и доступ к следующим действиям над объектами: импорт объектов; экспорт выбранных объектов; экспорт всех объектов удаление выбранных объектов; удаление всех объектов.
Нажатие ЛКМ по объекту	выбор объекта и вывод информации об объекте в рабочую область
Ø	настройка отображения боковой панели

4.4.1 Поиск объектов в списке

Для поиска объекта нажмите кнопку **7**, укажите значение или часть значения в поле **Текстовый поиск** и нажмите кнопку **Применить**. Будут выданы подходящие данные.

4.4.2 Сортировка и фильтрация объектов в списке

1. Нажмите кнопку **7**. Откроется блок для настройки сортировки и фильтрации объектов в списке (см. «Рис. 8»).

	+							
Текстовый поиск Q								
Фильтры								
О Ретроспективное ×								
С Активное × Название	: ×							
+								
Сортировка								
↓↑ Название ×								
↓ Активное ×								
+								
Сбросить Применить								

Рис. 8 – Боковая панель. Сортировка и фильтрация

- 2. Если для объекта доступна фильтрация по конкретным полям (для некоторых объектов фильтрация недоступна), то в блоке **Фильтрация** укажите необходимые значения полей.
- 3. В блоке Сортировка выполните следующие действия:
 - Добавьте поля, по которым должна выполняться сортировка
 - Выберите направление сортировки:
 - ↓ от последнего к первому;
 - 1 от первого к последнему.
- 4. Нажмите кнопку Применить.

Если необходимо очистить параметры сортировки и фильтрации, то нажмите кнопку **Сбросить**.

4.4.3 Массовые действия

Количество массовых операций, доступных над объектами в разделах платформы, может отличаться.

В общем случае над объектами доступны следующие массовые действия:

- Импортировать импорт объектов в платформу;
- Экспортировать экспорт выбранных объектов;
- Экспортировать все экспорт всех отфильтрованных объектов. Будут экспортированы все объекты, попавшие под параметры сортировки и фильтрации;
- Удалить удаление выбранных объектов;
- Удалить все удаление всех отфильтрованных объектов. Будут удалены все объекты, попавшие под параметры сортировки и фильтрации.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку и из выпадающего списка выберите пункт **Массовые действия**. Появятся флаги для выбора табличных списков (см. «Рис. 9»).



Рис. 9 – Массовые действия над табличными списками

- 2. Выберите объекты, установив соответствующие флаги.
- 3. Нажмите на соответствующую кнопку действия.

4. Завершите действие в открывшемся окне.

4.5 Папки контента

Для упрощения работы и структурирования пользовательского контента в платформе используется механизм **папок**.

Управление папками контента выполняется в разделе **Параметры** — «<u>Папки контента</u>».

Просмотр содержимого папок выполняется через боковую панель соответствующего раздела (см. «Рис. 10»).



Рис. 10 – Боковая панель. Папки контента

При просмотре содержимого папок доступны следующие элементы управления:

Кнопка	Действие
\$E / :=	выбрать элементы/отменить выбор элементов
↓ ↑	настройка сортировки и фильтров для поиска
ٹا <mark>ہ</mark>	включение/выключение режима каскадного выбора. Режим позволяет по клику на папку автоматически выбрать папки на всю глубину вложения. Режим по умолчанию включен

Отображение содержимого папок работает по следующему принципу:

- при клике на папку, в универсальной таблице отобразится содержимое выбранной папки;
- если папка является родительской, то при клике на папку раскрывается дерево дочерних папок;
- если установлены флаги для нескольких папок, в универсальной таблице отобразятся все объекты, содержащиеся в выбранных папках;
- если включен каскадный режим, то при клике на родительскую папку автоматически устанавливаются флаги на дочерние папки.

Для создания пользовательского контента в папке выполните следующие действия:

- 1. Перейдите в нужный раздел.
- 2. Начните процесс создания.
- 3. В поле Папка из выпадающего списка выберите нужную папку.

Для переноса пользовательского контента в папку выполните следующие действия:

- 1. Перейдите в нужный раздел.
- 2. Выберите нужные объекты, установив соответствующие флаги.
- 3. Нажмите кнопку Переместить в папку.
- 4. В открывшемся окне выберите папку и нажмите кнопку Переместить.

В версии 4.1.0 данный механизм доступен для следующего контента:

• Правила корреляции.

4.6 Формы работы с объектами

Основная работа пользователя с объектами осуществляется на странице **Форма работы с объектами**. Формы объектов могут быть следующих типов:

- Создание;
- Просмотр;
- Редактирование.

Форма работы с объектами имеет различный вид в зависимости от объекта и выполняемого действия (см. «Рис. 11»).

Выбранный объект Вид выбранного объекта Набор пол							ей объек	та Пан	нель действ	ий над	д объекто	M				
≡	Кангео Радар	172.30.254.138 🗸	∣Шаби	лоны алертов										 База знаний 	🛛 admir	i ~
â	Поиск		+ti :	Автомати	ческо	е создание і	инцидент	a				<u></u> 🗇 y	далить	Дублировать	Редактироват	ь
Q																
0	Автомат	тическое создан	ие	Уровень риска												
¢	Провери	ка времени опер	ации	0	1	2	3	4		5	6	7	8		9	10
ð				🗸 Создать инци	COSTST- MUNIMPOUT			Назначить инцидент пользователю			П Логировать первое и последнее событие			Логировать указанное число событий		
20													2			+
н				IP актива			FQDN актива	1		Hostname a	актива		МАС акт	тива		
ŧti				event.dns.type			elastic_key			action			action			
0				Шаблон												
				Описание												
			<													

Рис. 11 – Рабочая область. Форма объекта

В общем случает страница состоит из следующих элементов:

- Поля формы содержит поля для указания сведений и выполнения настроек объекта;
- Панель действий содержит кнопки для работы с объектами. Кнопки, которые не помещаются на панели действий, будут помещены в выпадающее меню, доступное по кнопке

Панель действий может содержать следующие элементы управления:

Кнопка	Тип формы объекта	Действие
Редактировать / 🔗	Просмотр	Изменение информации об объекте
Дублировать	Просмотр	Создание нового объекта на основе существующего
Назначить пользователю / 🞗	Просмотр	Выдача прав на работу с объектом выбранному пользователю
Назначить группе пользователей / 📿	Просмотр	Выдача прав на работу с объектом выбранной группе пользователей
Написать ответственному	Просмотр	Написать сообщение ответственному пользователю. История сообщений доступна в профиле пользователя
Добавить в группу	Просмотр	Добавление объекта в выбранную группу
Опубликовать	Просмотр	Публикация изменений на всех подчиненных инстансах
Сохранить	Создание / Редактирование	Сохранение сведений об объекте
Сбросить	Создание / Редактирование	Сброс введенных сведений об объекте
Создать	Создание	Создание объекта
\	Bce	Возврат на предыдущую страницу

4.6.1 Шаблоны объектов

Для упрощения создания/редактирования объектов в платформе используется механизм **шаблонов**.

Шаблон будет определять структуру данных, внешний вид и поведение форм создания/редактирования объектов.

Для создания шаблона выполните следующие действия:

- 1. Откройте необходимый объект на создание или редактирование.
- 2. Настройте поля формы.
- 3. Нажмите кнопку Сохранить как шаблон (располагается внизу формы).
- 4. Укажите название шаблона в открывшемся окне и нажмите кнопку Сохранить.
- 5. Шаблон будет сохранен в платформе. Информацию о шаблоне можно посмотреть в разделе **Параметры** → «Шаблоны».

Для использования шаблона выполните следующие действия:

- 1. Откройте форму необходимого объекта на создание или редактирование.
- 2. В поле **Использовать существующий шаблон** из выпадающего списка выберите заранее созданный шаблон.

3. Поля формы будут автоматически заполнены данными из шаблона.

В версии 4.1.0 данный механизм доступен для следующих объектов:

• Профили сбора.

4.6.2 Визуализации

Визуализации – это графики, виджеты, метрики и т.д. (см. «Рис. 12»).



Рис. 12 – Рабочая область. Визуализации

Визуализации имеют различные элементы управления, которые подробно расписаны в соответствующих разделах.

5. События

5.1 Общие данные

Платформа Радар предоставляет большое количество информации о событиях информационной безопасности и удобные инструменты по их анализу:

- просмотр потока событий в виде графика;
- просмотр выделенного фрагмента потока событий в виде круговой диаграммы, таблицы или гистограммы;
- просмотр детальной информации по каждому событию.

При рассмотрении событий пользователю предоставляется следующая информация:

- id уникальный идентификатор события;
- этап разбора события. Может принимать следующие значения: Событие нормализовано, Событие разобрано, Событие не разобрано;
- информация о полях события.

По результатам анализа событий платформа предоставляет следующие возможности:

- создание инцидента на основе анализа события;
- добавление события в существующий инцидент;
- быстрый переход к просмотру инцидента, в котором участвует событие.

Платформа предоставляет широкий набор инструментов для формирования списка событий:

- фильтрация по следующим параметрам: по периоду, по этапам разбора события, по запросам к конкретным полям события, по агрегациям;
- пресеты вы можете сохранить часто используемые условия фильтрации как пресет;
- поиск по значениям полей события;
- фильтрация по выбранным полям просматриваемого события;
- просмотр истории поиска с возможностью повторного применения ранее используемых условий фильтрации.

Для работы с событиями перейдите раздел События (см. «Рис. 13»).

≡	<mark>∦ пангес</mark> 172.30.254.82 ∨ Собы	© База энаний 🔘 admin 🗸
â	Фильтры Пресеты	С С История
Q	Автообновление данных	
0	Выкл 🗸 🖓	Поток событий, 15 апр. (05:07:23) - 15 апр. (06:07:23)
53	Период	보 아 됩
ð	Когда событие было зарегистрировано в системе	50
%	Последний час 📋	
н	Нормализованное событие	49
+11	Не важно 🗸	30
0	Запрос Сохраненные запросы >	
	Э Добавить запрос	
	A	
	Сохраненные агрегации >	
	Добавить агрегацию	▖▁▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋
		Событий: 2020, показано 1 - 20
		Ввести О. 🗄 Сортировка 🖉 Набор полей 🛩 Выбрать несколько
		jd: pZnbxtEXMTljuFwRTqowMjsjZrOxrWSQ Событие нормализовано
		@timestamp Q Q * 22.03.2024 13:21:17
	Сбросить	Показать больше 🗸

Рис. 13 – Страница "События"

Интерфейс раздела состоит из следующих блоков:

- график "Поток событий";
- топ-10 значений по выделенной области потока событий (опционально);
- список событий;
- фильтры настройка условий фильтрации потока событий;
- пресеты список сохраненных условий фильтрации.

5.1.1 График "Поток событий"

Блок представляет из себя график, в котором отображается плотность появления событий за период времени.

Пример потока событий приведен на «Рис. 14».



Рис. 14 – Страница "События". График "Поток событий"

В блоке доступны следующие элементы управления:

Кнопка	Действие
• История	просмотр истории поиска событий
5	просмотр предыдущего запроса из истории поиска событий
\sim	просмотр следующего запроса из истории поиска событий
По дням 🗸	выбор плотности отрисовки значений графика "Поток событий"
۶۶۰۰۰۹ ۱	инструмент "Прямоугольное выделение" - создает прямоугольную рамку вокруг области на графике потока событий, ограничивая ее по горизонтальным и вертикальным сторонам
€	инструмент "Выделение по горизонтали" - создает прямоугольную рамку вокруг области по оси X, при этом выделяя все значения по оси Y
[[]	режим "Массовое выделение" - позволяет прямоугольному и горизонтальному выделению создать рамку вокруг нескольких областей на графике потока событий

5.1.2 Топ-10 значений по выделенной области потока событий

В блоке отображаются первые 10 запросов о регистрации событий в платформе за выбранный период.

Блок появляется после выделения области на графике "Поток событий". Для выделения области на графике выполните следующие действия:

- 1. Сформируйте график "Поток событий" (см. раздел «<u>Работа с фильтрами</u>»).
- 2. Выберите инструмент для выделения:
 - []] прямоугольное выделение;
 - 🔂 выделение по горизонтали.
- 3. Нарисуйте выделение, перетаскивая инструмент по графику потока событий.

- 4. В блоке ниже будет отображаться статистика по выделенной области.
- 5. Для выделения нескольких областей на графике, включите режим "Массовое выделение" по кнопке .
- 6. Используйте инструмент «Масштабирование» для более точного выделения нужной области (см. раздел «<u>Масштабирование графика потока событий</u>»).







Рис. 15 – Страница "События". Блок "Топ-10"

В блоке отображается следующая информация:

- дата и время регистрации событий в платформе;
- количество событий в запросе о регистрации.

Информацию можно вывести следующими способами:

- столбчатая диаграмма (см. «Рис. 15»);
- таблица;
- круговая диаграмма (см. «Рис. 16»).





Для закрытия блока нажмите кнопку X.

5.1.2.1 Масштабирование графика потока событий

Для более подробной детализации графика потока событий используйте инструмент "Масштабирование" (см. «Рис. 17»).



Рис. 17 – Элементы управления масштабом

Инструмент позволяет менять масштаб следующим образом:

- изменение диапазона отображаемой области по оси X;
- перемещение выбранного диапазона по оси Х.

Для использования инструмента выполните следующие действия:

- 1. Наведите курсор на нужный элемент управления масштабом.
- 2. Зажмите ЛКМ.
- 3. Двигайте курсор в нужном направлении. Данные на графике будут автоматически изменяться.

5.1.3 Список событий

Блок располагается под графиком "Поток событий". В блоке отображается информация о событиях. Информация о событиях может отображаться двумя способами:

- в карточном виде (используется по умолчанию);
- в табличном виде.

Панель управления списком событий

Панель располагается над списком событий (см. «Рис. 18»).

Событие: 1076491, показано 1 - 20						
Ввести	Q	⊞	Сортировка	🖉 Набор полей	🛩 Выбрать несколько	:



На панели доступны следующие элементы управления:

Кнопка	Действие					
Поиск	поиск по значениям полей события					
⊞	включить табличный вид					
=	включить карточный вид					
Сортировка	настроить параметры сортировки событий в списке					
Набор полей	выбрать поля для отображения в таблице (только для табличного вида)					
Выбрать несколько	включение режима для массовых операций над событиями					
:	доступ к следующим действиям над событиями: – создать инцидент; – добавить в инцидент; – экспорт в CSV.					

Карточный вид

По умолчанию события отображаются в карточном виде (см. «Рис. 19»).

Событие: 1076491 , показано 1 - 2	20	
Ввести	Q	🗄 Сортировка 🖉 Набор полей 🛩 Выбрать несколько
_id: AAAAAGYdAYTbSK/i18IKLi/	AWig9wkp/W	Не разобрано Действия 🗸
@timestamp	$\oplus \bigcirc *$	15.04.2024 13:29:24
event.logsource.host	$\oplus \bigcirc *$	172.30.254.154:9992
Показать больше 🗸		
_id: AAAAAGYc/8axUVJh4jg7Qa	a6S/qZllbhE	Событие разобрано Действия 🗸
@timestamp	$\oplus \bigcirc *$	15.04.2024 13:21:37
event.logsource.host	$\oplus \bigcirc *$	172.30.254.154:9992
Показать больше 🗸		
_id: AAAAAGYc/8byinXTbtFLIG	cQ3cJts6lQ C	Событие нормализовано Действия 🗸
@timestamp	$\oplus \bigcirc *$	15.04.2024 13:21:37
event.logsource.host	$\oplus \bigcirc *$	172.30.254.154:9992
Показать больше 🗸		

Рис. 19 – Список событий в карточном виде

По кнопкам **Показать больше** / **Показать меньше** можно открыть/скрыть отображение всех полей события (см. «Рис. 20»).

_id: pZnbxtEXMTIjuFwRTqowMjsjZ	rOxrWSQ	Событие нормализовано		Действия 🗸
@timestamp	⊕	22.03.2024 13:21:17		
elastic_key	$\oplus \bigcirc *$	normalized		
fqdn	⊕	["MVV-4269", "2"]		
hostname	⊕	["MVV-4269"]		
id	⊕	pZnbxtEXMTIjuFwRTqowN	MjsjZrOxrWSQ	
initiator.host.internal	⊕	false		
initiator.host.test	⊕	testest		
initiator.host.test-ip	⊕	192.168.236.223		
ip	⊕	["192.168.236.223"]		
target.host.internal	⊕	false		
Показать меньше 🔨				

Рис. 20 – Просмотр карточки события

При просмотре событий в карточном виде доступны следующие элементы управления:

Кнопка	Действие				
Ð	установить фильтр "Равно". В параметры запроса фильтра добавится условие поиска событий по значению равным в указанном поле				
Q	установить фильтр "Не равно". В параметры запроса фильтра добавится условие поиска событий по всем значениям, кроме того, что указано в поле				
*	установить фильтр "Существует". В параметры запроса фильтра добавится условие поиска событий по всем событиям, в которых существует выбранное поле				
Действия 🗸	доступ к действию "Найти инцидент", в котором присутствует событие				

Табличный вид

Для переключения списка событий в табличный вид нажмите кнопку 🖽.

Пример табличного представления данных приведен на «Рис. 21».

< @timestamp	> < elastic_key	>	< id	>	Детали	
22 мар. 2024, 13:21:17	normalized		pZnbxtEXMTIjuFwRTqowMjsjZrOxrWSQ		0	:
22 мар. 2024, 13:21:16	normalized		AWFAttJjEOxkRjKOBxLvnRkTGyrNQtNF		0	:
22 мар. 2024, 13:21:15	normalized		PydbZAgCzAvYsZoaemPPWwTApFZexDqU		0	:
22 мар. 2024, 13:21:14	normalized		cLIxzLrfrZtYqIIQgYRJjgMSLHRamIQj		0	:
22 мар. 2024, 13:21:13	normalized		OVbRthxxDRTcxWPqWLHmBCdxvgLAmmpJ		0	:
22 мар. 2024, 13:21:12	normalized		faVggttVCckdKfzpKObAqWkUDuamtttO		0	:
22 мар. 2024, 13:21:11	normalized		zwflUfxzdqosUgbWaOCYXKVKUumRDFla		0	:
22 мар. 2024, 13:20:58	normalized		RccFGLEgclaUgouelXiEEtXafkhUcWMq		0	:

Рис. 21 – Список событий в табличном виде

Кнопки > / < , которые располагаются в заголовке столбцов, позволяют изменить порядок столбцов.

Кнопка ⁽²⁰⁾, которая располагается в графе "Детали", позволяет посмотреть детали события в карточном виде (см. «Рис. 22»).

<	@timestamp	> < event.lo	gsource.ho	$>$ < elastic_ke y >	< id	> <	initiator.host.intern al	> < initiator.host.t st	e > < initiator.host.test- ip >	Детали	
22 N 13:2	мар. 2024, 21:17			normalized	pZnbxtEXMTIjuFwRTqowMjsjZrO	rWSQ		testest	192.168.236.223	۵	:
22 N 13:2	мар. 2024, 21:16			normalized	AWFAttJjEOxkRjKOBxLvnRkTGyrN	IQtNF		testest	192.168.203.167	۵	:
22 N 13:2	мар. 2024, 21:15			normalized	PydbZAgCzAvYsZoaemPPWwTAp U	FZexDq		testest	192.168.36.98	٢	:
22 M 13:2	иар. 2024, 21:14			normalized	cLlxzLrfrZtYqIIQgYRJjgMSLHRam	IQj		testest	192.168.71.81	۵	:
22 N	иар. 2024,			normalized	OVbRthxxDRTcxWPqWLHmBCdx	vgLAm		testest	192.168.48.219	۵	:
											~
	_id: pZnbxtEXM	1TIjuFwRTqowMjsji	ZrOxrWSQ	Событие нормализовано						Действия	~
	@timestamp		€	22.03.2024 13:21:17							
	elastic_key		⊕	normalized							
	id		⊕	pZnbxtEXMTIjuFwRTqow	MjsjZrOxrWSQ						
	initiator.host.in	ternal	⊕	false							
	initiator.host.te	st	⊕	testest							
	initiator.host.te	st-ip	€ € *	192.168.236.223							
	fqdn	(€ Q * ⊕	["MVV-4269", "2"]							T

Рис. 22 – Список событий в табличном виде. Детали

Кнопка 🕀, которая располагается в блоке "Детали" (см. «Рис. 22»), позволяет добавить поле в набор столбцов таблицы.

Кнопка , которая располагается в конце строки, предоставляет доступ к действию "Найти инцидент" (подробнее см. раздел «<u>Поиск инцидента</u>»).

5.2 Работа с фильтрами

Настройка фильтра выполняется на вкладке "Фильтры" (см. «Рис. 23»).
Фильтры	Пресеты	
Автообнов	ление данных	
Выкл	\sim	۲°)
Период		
Когда событ зарегистрир	ие было овано в системе	
Последние	е 30 дней	Ë
Нормализо	ованное событие)
Не важно		~
Запрос	Сохраненные запро	осы > апрос
		<
Агрегация		
Сохраненны	е агрегации 🗦	
[Добавить агрег	ацию
	Сбросить	

Рис. 23 – Страница "События". Вкладка "Фильтры"

При работе с фильтрами доступны следующие элементы управления:

Кнопка	Действие	
	обновить список событий	
Ë	редактирование запроса/агрегации	
Добавить запрос	добавление запроса в условия фильтра	
Добавить агрегацию	добавление агрегаций в условия фильтра	
Ø	редактирование запроса/агрегации	
×	удаление запроса/агрегации	
Сбросить	очистить условия фильтра	

Для настройки условий фильтра выполните следующие действия:

- 1. В поле "Автообновление данных" из выпадающего списка выберите режим автоматического обновления данных. Доступные значения:
 - выключен;
 - по секундам: каждые 5, 10, 30 секунд;
 - по минутам: каждые 1, 5, 10, 30 минут.
- 2. В поле **Период** нажмите кнопку ^С. Откроется окно выбора временного диапазона.
- 3. В открывшемся окне выберите период и нажмите кнопку **Применить**. Доступные значения:
 - текущие: минута, час, день, месяц, год;
 - последние: минуты, часы, месяца, года;
 - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
- 4. В поле Нормализованное событие выберите этап разбора события:
 - событие нормализовано будут показаны только нормализованные события;
 - событие разобрано будут показаны только разобранные события;
 - событие не разобрано будут показаны только неразобранные события;
 - не важно будут показаны все события.
- 5. В поле **Запрос** добавьте необходимое количество запросов (см. раздел «<u>Настройка</u> <u>запросов</u>»).
- 6. В поле **Агрегация** добавьте необходимое количество агрегаций (см. раздел «<u>Настройка</u> <u>агрегации</u>»).
- 7. При необходимости вы можете сохранить условия фильтра как пресет (см. раздел «<u>Работа с</u> <u>пресетами</u>»).
- 8. Вы можете посмотреть журнал истории поиска и применить соответствующий фильтр из истории (см. раздел «<u>История поиска</u>»).

5.2.1 Настройка запросов

Настройка запросов включает в себя следующие процессы:

- 1. «Добавление запроса».
- 2. «Сохранение конфигурации запроса».

5.2.1.1 Добавление запроса в условия фильтра

Добавление запроса в условия фильтра можно выполнить тремя способами:

- Способ 1. Ручное добавление нового запроса.
- Способ 2. Добавление запроса из списка сохраненных.

• Способ 3. Добавление условий в запрос из полей события.

Все добавленные запросы отобразятся в соответствующем блоке (см. «Рис. 24»).

Запрос	Сохраненные з	апро	сы >
	🖹 Сохранить в	зыбор	о как
	🕀 Добави	ть за	прос
@timest 2024-03 22T13:2 03:00	<mark>атр НЕ</mark> равен 3- 1:17.998015077+	Ø	×
elastic_k	сеу существует	Ø	×
ір раве 192.168.	н 203.167	Ø	×
@timest 17121780	<mark>атр</mark> равен 000000	Ø	×

Рис. 24 – Вкладка "Фильтры". Список запросов

Способ 1. Ручное добавление нового запроса

1. На вкладке **Фильтры** в блоке **Запрос** нажмите кнопку **Добавить запрос**. Откроется окно "Добавить запрос" (см. «Рис. 25»).

Добавить запрос	×
Поле	
@timestamp	~
Действие	
равен	~
Значение	
2024-04-04	
	Сбросить Сохранить

Рис. 25 – Окно "Добавить запрос"

- 2. Укажите следующие данные:
 - из выпадающего списка выберите поле, по которому будет выполняться запрос;
 - в поле "Действие" из выпадающего списка выберите логический оператор;
 - в поле "Значение" укажите значение логического оператора.

- 3. Нажмите кнопку Сохранить.
- 4. Добавьте необходимое количество запросов.

Способ 2. Добавление запроса из списка сохраненных

Примечание. Подробнее о сохранении запроса см. раздел «Сохранение конфигурации запроса».

1. На вкладке **Фильтры** в блоке **Запрос** нажмите кнопку **Сохраненные запросы**. Откроется окно "Сохраненные запросы" (см. «Рис. 26»).

Сохраненные запросы			×
Категория *			
Выберите категор	олис		~
Источники	>	Microsoft Windows	
Поиск по IP	>		Сохранить

Рис. 26 – Окно "Сохраненные запросы"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимый запрос. Отобразится структура запроса (см. «Рис. 27»).



Рис. 27 – Окно "Сохраненные запросы". Структура запроса

3. Проверьте структуру запроса и нажмите кнопку Сохранить.

Способ 3. Добавление запросов по полям событий.

Если список событий уже сформирован, то вы можете добавить в запрос условия по выбранным полям конкретного события.

Для этого откройте карточку события и в соответствующем поле выберите нужное условие:

- для добавления в запрос условия "Равен" выберите поле и нажмите кнопку 🗨;
- для добавления в запрос условия "Не равен" выберите поле и нажмите кнопку $\heartsuit;$
- для добавления в запрос условия "Существует" выберите поле и нажмите кнопку *.

Пример, добавленных таких способом запросов, приведен на «Рис. 28».

Нормализованное событие				
Не важно 🗸	_id: pZnbxtEXMTIjuFwRTqow	MjsjZrOxrWSQ	Событие нормализовано	
2057000	@timestamp	⊕	22.03.2024 13:21:17	
Запрос Сохраненные запросы >	elastic_key	⊕	normalized	
	fqdn	€ € *	["MVV-4269", "2"]	
С дооавить запрос	hostname	€ € *	["MVV-4269"]	
@timestamp равен 🖉 🗙	id	€ € *	pZnbxtEXMTIjuFwRTqowN	ljsjZrOxrWSQ
2024-03- 22T13:21:17.998015077+ 03:00	initiator.host.internal	⊕	false	
	initiator.host.test	⊕	testest	
elastic_key существует 🖉 🗙 —————————————————————————————————	initiator.host.test-ip	€ € *	192.168.236.223	
Агрегация	ip	⊕	["192.168.236.223"]	
Сохраненные агрегации >	target.host.internal	$\oplus \ominus *$	false	
🕒 Добавить агрегацию	Показать меньше 🔨			



5.2.1.2 Сохранение конфигурации запроса

Настроенную конфигурацию запросов можно сохранить для дальнейшего использования.

Для этого выполните следующие действия:

- 1. Добавьте необходимое количество условий в запрос.
- 2. Нажмите кнопку **Сохранить выбор как**. Откроется окно "Сохранить запрос" (см. «Рис. 29»).

Сохранить запрос	×
Выберите категорию *	
Источники	~ +
Введите название *	
Windows Defender	
Windows Defender	

Рис. 29 – Окно "Сохранить запрос"

- 3. Укажите следующие данные:
 - в поле "Выберите категорию" из выпадающего списка выберите категорию, в которую будет сохранен запрос;
 - если вы еще не добавили ни одной категории, то нажмите кнопку «+», укажите название категории и сохраните изменения;
 - в поле "Введите название" укажите название запроса.
- 4. Нажмите кнопку Сохранить.

5.2.2 Настройка агрегации

Агрегация - функция группировки результатов поиска по выбранному полю.

Агрегацию можно выполнить по следующим функциям:

- min по минимальным значениям;
- max по максимальным значениям;
- sum по сумме всех значений;
- avg по среднему значению;
- stats вывод по функциям count, min, max, sum, avg;
- terms поиск нескольких значений в одном поле.

Для функции terms можно добавить подагрегации.

Результат поиска по агрегации будет выводиться в табличном виде вместо графика потока событий (см. «Рис. 30»).

	Агре	егация Поле и функция	г	1ода	грегация				
Фильтры Пресеты		@timestamp stats —							
Автообновление данных		count	min		max		avg	sum	
Выкл 🗸	2	2020	21.03.2024 15:45:08		22.03.2024 13:21:17		21.03.2024 16:56:58	3456279426358658	
Период		_id terms							
Когда событие было зарегистрировано в системе		_id	doc_count		elastic_key_terms		@timestamp_avg	_idterms	
Последние 2 месяца	5		1		elastic_key	doc_count	value	_id	doc_count
Нормализоранное событие		Abogowwy Rowinishwi Abraiegwcy wowwz		F	normalized	1	1711026709729	ADGgCMWyTKGMMsnMHA	DP\$iegwLyWdvV
Не важие					elastic_key	doc_count	value	_id	doc_count
Певажно		ADKCbBkQqpkUxpImbdxrucbpQAEGLLnO	1	L	error	1	1711026757794	ADKCbBkQqpkUxplmbdxru	bptQAEGLLnO
Запрос Сохраненные запросы	>				elastic_key	doc_count	value	_id	doc_count
🕀 Добавить запро		AFVeWLpkrededbQufeRekTOQWSigoQtK	1		normalized	1	1711025215595	AFVeWLpkrededbQufeRekT	OQWSigoQtK
A-more	Ť				elastic_key	doc_count	value	_id	doc_count
Сохраненные агрегации		AJXkJuOkvaYibjGgsxeROzmlLEjdqogq	1		normalized	1	1711025622258	AJXkJuOkvaYibjGgsxeROzn	nLEjdqogq
Сохранить выбор ка	к	AJddpwfpooGbRDYBbPrtvIAmuxIRbbGZ	1		elastic_key	doc_count	value	_id	doc_count
 Добавить агрегаци 	ю	Событий: 2020, показано 1 - 20							
@timestamp stats 🖉 🗙		Ввести					🔾 🗄 Сортировка	🖉 Набор полей 🛷 Выбра	ть несколько
_id terms 🖉 🗙		_id: pZnbxtEXMTljuFwRTqowMjsjZrOxrWSQ	Событие нормализованс	0					Действия 🗸
		@timestamp 🔍 Q 🛠	22.03.2024 13:21:17						
Сбросить		Показать больше 🗸							

Рис. 30 – Страница "События". Просмотр агрегаций

Настройка агрегации включает в себя следующие процессы:

- 1. «Добавление агрегации».
- 2. «Добавление подагрегации».
- 3. «Сохранение агрегации».

5.2.2.1 Добавление агрегации

Способ 1. Ручное добавление агрегации.

1. На вкладке **Фильтры** в блоке **Агрегация** нажмите кнопку **Добавить агрегацию**. Откроется окно "Добавить агрегацию" (см. «Рис. 31»).

Добавить агрегацию		×
Действие	Поле	
Stats ~	@timestamp	~
	Сброси	ть Сохранить

Рис. 31 – Окно "Добавить агрегацию"

- 2. Укажите следующие данные:
 - в поле "Действие" из выпадающего списка выберите функцию агрегации;
 - из выпадающего списка выберите поле, по которому будет выполняться функция агрегации.
- 3. Нажмите кнопку Сохранить.

4. Добавьте необходимое количество агрегаций.

Способ 2. Добавление агрегации из списка сохраненных

Примечание. Подробнее о сохранении агрегаций см. раздел «Сохранение агрегации».

1. На вкладке **Фильтры** в блоке **Агреграции** нажмите кнопку **Сохраненные агрегации**. Откроется окно "Сохраненные агрегации" (см. «Рис. 32»).

•		
атегория * Агрегация по ID и Timest	amp / Первая агрегация	~
Агрегация по ID >	Первая агрегация	
		Сохранить

Рис. 32 – Окно "Сохраненные агрегации"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимую агрегацию. Отобразятся параметры агрегации (см. «Рис. 33»).



Рис. 33 – Окно "Сохраненные агрегации". Структура агрегации

3. Проверьте структуру агрегации и нажмите кнопку Сохранить.

5.2.2.2 Добавление подагрегации

Вы можете добавить в агрегацию необходимое количество подагрегаций.

Чтобы добавить подагрегацию необходимо при добавлении/редактировании агрегации в поле "Действие" из выпадающего списка выбрать функцию terms. Откроется блок для добавления подагрегаций (см. «Рис. 34»).

lействие	Поле	
Terms	∽ _id	~
Ограничение количества		
10	- +	
Добавить подагрегацию		
_id terms		Ø ×
elastic_key terms		Ø×
@timestamp avg		Ø ×

Рис. 34 – Окно "Добавить агрегацию". Блок "Подагрегации"

Нажмите кнопку **Добавить подагрегацию**. Действия по добавлению подагрегации аналогичны действиям при добавлении агрегации.

При необходимости вы можете сделать подагрегацию многоуровневой, также указав при ее добавлении в поле "Действие" функцию terms.

Добавьте необходимое количество подагрегаций и нажмите кнопку Сохранить.

5.2.2.3 Сохранение агрегации

Настроенную агрегацию можно сохранить для дальнейшего использования.

Для этого выполните следующие действия:

- 1. Добавьте необходимое количество условий в агрегацию.
- 2. Нажмите кнопку **Сохранить выбор как**. Откроется окно "Сохранить агрегацию" (см. «Рис. 35»).

×
~ +
Отмена Сохранить

Рис. 35 – Окно "Сохранить агрегацию"

- 3. Укажите следующие данные:
 - в поле "Выберите категорию" из выпадающего списка выберите категорию, в которую будет сохранена агрегация;
 - если вы еще не добавили ни одной категории, то нажмите кнопку «+», укажите название категории и сохраните изменения;
 - в поле "Введите название" укажите название агрегации.
- 4. Нажмите кнопку Сохранить.

5.2.3 Работа с пресетами

Пресет – это сохраненные условия фильтрации, которые можно использовать как шаблон для формирования списка событий.

Работа с пресетами выполняется на вкладке "Пресеты" (см. «Рис. 37»).

Фильтры Пресеты
Только новые события
Дата создания: 18/04/2024 09:46
Применить Удалить
Не разобранные события
Дата создания: 18/04/2024 09:47
Применить Удалить
Нормализованные события
Дата создания: 18/04/2024 09:47
Применить Удалить
Создать пресет

Рис. 36 – Страница "События". Вкладка "Пресеты"

На вкладке отображается следующая информация:

- название пресета;
- дата создания пресета.

Работа с пресетами включает в себя следующие процессы:

- 1. «Создание пресета».
- 2. «Применение пресета».
- 3. «Удаление пресета».

5.2.3.1 Создание пресета

- 1. Настройте условия фильтра для получения списка событий.
- 2. Перейдите на вкладку "Пресеты".
- 3. Нажмите кнопку Создать пресет. Откроется окно "Создание пресета" (см. «Рис. 37»).

Создание пресета	×
Введите название * Разобранные событ	ия
Сохранить период	
Сохраняемые данные	
	Сбросить Сохранить

Рис. 37 – Окно "Создание пресета"

- 2. Укажите следующие данные:
 - в поле "Введите название" укажите название пресета;
 - установите флаг "Сохранить период" если необходимо сохранить данные о периоде формирования списка событий.
- 3. Нажмите кнопку Сохранить.

5.2.3.2 Применение пресета

- 1. Перейдите на вкладку "Пресеты".
- 2. Выберите пресет и нажмите кнопку Применить.
- 3. Будет сформирован список событий по сохраненному шаблону.

5.2.3.3 Удаление пресета

- 1. Перейдите на вкладку "Пресеты".
- 2. Выберите пресет и нажмите кнопку Удалить.
- 3. Пресет будет удален из списка.

5.2.4 История поиска

Платформа Радар ведет историю поиска событий.

Для ее просмотра нажмите кнопку ^{О История}. Отроется окно "История поиска" (см. «Рис. 38»).

История пои	ска		×
∨ Сегодня			
Время	Период	Запрос	
10:11	Последние 2 месяца	Нормализация: * Поле по оси X: @timestamp Правила: _id существует @timestamp равен 1712091600000	Применить
10:11	Последние 2 месяца	Нормализация: * Поле по оси X: @timestamp Правила: _id существует	Применить
> 17 апр. 2024			
> 16 апр. 2024			
> 15 апр. 2024			
			Закрыть

Рис. 38 – Окно "История поиска"

В окне отображается следующая информация:

- день формирования списка событий;
- время создания списка событий;
- период, за который был сформирован список событий;
- условия запроса, по которым был сформирован список событий.

Вы можете сформировать список событий из истории поиска. Для этого в соответствующей строке нажмите кнопку **Применить**.

5.3 Работа с событиями

Перед началом работы с событиями:

- 1. Ознакомьтесь с общими данными и интерфейсом раздела (см. раздел «Общие данные»).
- 2. Сформируйте список событий (см. раздел «<u>Работа с фильтрами</u>»).

Пример сформированного списка событий приведен на «Рис. 39».



Рис. 39 – Страница "События". Сформированный список событий

Работа с событиями включает в себя следующие процессы:

- 1. «Создание инцидента».
- 2. «Добавление в инцидент».
- 3. «Поиск инцидент».
- 4. «Экспорт списка событий».

При работе с событиями можно воспользоваться вспомогательными инструментами для анализа событий:

- поиск событий;
- просмотр событий по сформированной агрегации;
- настройка плотности отрисовки значений графика;
- сортировка событий;
- настройка набора полей для табличного вида.

Подробнее см. раздел «Вспомогательные инструменты для анализа событий».

5.3.1 Создание инцидента

Примечание. Подробнее об инцидентах см. раздел «Инциденты».

Платформа Радар позволяет создать инцидент на основе подозрительного события.

Для этого выполните следующие действия:

- 1. Включите режим для массовых операций над событиями нажав кнопку **Выбрать несколько**.
- 2. Выберите одно или несколько событий установив флаг в соответствующей карточке/строке таблицы.
- 3. Нажмите кнопку и из выпадающего списка выберите пункт "Создать инцидент". Откроется окно "Быстрое создание инцидента".
- 4. В поле "Тип инцидента" из выпадающего списка выберите тип инцидента. В окне отобразится полный набор полей для заполнения сведений о выбранном типе инцидента (см. «Рис. 40»).

Тип инцилента *	Aktur *
Подозрительная активность Р 🔾	Первый
Название инцидента *	Уровень риска
Подозрительная активность Power	4 -+
Правило корреляции *	
Правило корреляции * sshd: Превышено максимальное кол	ичество попыток аутентификации 🛛 🗸
Правило корреляции * sshd: Превышено максимальное кол Категория *	ичество попыток аутентификации 🔗
Правило корреляции * sshd: Превышено максимальное кол Категория * • Нарушение политики Сстевая	ичество попыток аутентификации — — я аномалия — Уязвимость
Правило корреляции * sshd: Превышено максимальное кол Категория * Нарушение политики Сстевая	ичество попыток аутентификации — я аномалия — Уязвимость

Рис. 40 – Окно "Быстрое создание инцидента"

- 5. В зависимости от выбранного типа инцидента значения полей будут предзаполнены соответствующей информацией. При необходимости измените следующие данные:
 - в поле **Актив** из выпадающего списка выберите техническое средство информационной системы, на котором произошел инцидент;
 - в поле Название инцидента укажите название инцидента;
 - в поле **Уровень риска** задайте уровень риска;

- в поле **Правило корреляции** из выпадающего списка выберите соответствующее правило корреляции;
- в поле **Категория** выберите категорию инцидента: нарушение политики, сетевая аномалия или уязвимость.
- 6. Нажмите кнопку Создать.

5.3.2 Добавление события в инцидент

Платформа Радар позволяет добавить событие или несколько событий в уже созданный инцидент.

Для этого выполните следующие действия:

- 1. Включите режим массовых операций над событиями нажав кнопку Выбрать несколько.
- 2. Выберите одно или несколько событий установив флаг в соответствующей карточке/строке таблицы.
- 3. Нажмите кнопку и из выпадающего списка выберите пункт "Добавить к инциденту". Откроется окно "Добавить события" (см. «Рис. 41»).

Травило корреляции *	
sshd: Превышено максимальное количество попыток аутенти	ификации 🗸
Зыберите инцидент *	
Подозрительная активность Powershell	\sim

Рис. 41 – Окно "Добавить события"

- 4. Укажите следующие данные:
 - в поле "Правило корреляции" из выпадающего списка выберите соответствующее правило корреляции;
 - в поле "Инцидент" выберите инцидент, в который будет добавлено событие.
- 5. Нажмите кнопку Добавить.

После успешного добавления события в инцидент платформа предложит вам открыть соответствующий инцидент.

5.3.3 Поиск инцидента

Для поиска инцидента, к которому относится событие, выполните следующие действия:

- 1. В зависимости от вида, в котором выполняется просмотр списка событий нажмите кнопку в теле события:
 - Действия 🗸 если включен карточный вид;
 - - если включен табличный вид.
- 2. Выберите пункт Найти инцидент. Откроется окно "Ссылки на инциденты" (см. «Рис. 42»).

Ссылки на инциденты	×
Антивирус – Обнаружено вредоносное ПО	
Рис. 42 – Список найденных инцидентов по событ	гию

3. Для открытия инцидента нажмите на нужную ссылку.

5.3.4 Экспорт списка событий

Платформа Радар позволяет выгрузить список событий в файл формата CSV. Для этого выполните следующие действия:

- 1. Сформируйте список событий.
- 2. Нажмите кнопку и из выпадающего списка выберите пункт Экспорт в CSV.
- 3. Укажите путь для сохранения файла.

Помимо экспорта сформированного списка событий, в платформе доступен экспорт событий в файлы формата CSV на всю глубину фильтрации:

- 1. Сформируйте список событий.
- 2. Нажмите кнопку и из выпадающего списка выберите пункт Экспортировать.

Экспорт событий в CSV		×
Максимальное количество экспортируемы	к событий	
179860		-+
Максимальное количество событий в файле	e	
9999		-+
Экспортировать все поля		
	Сбросить	Скачать в CSV

Рис. 43 – Окно "Экспорт событий в CSV"

- 3. Настройте в окне параметры экспорта:
 - Максимальное количество экспортируемых событий укажите количество событий, которое вы хотите экспортировать. В поле автоматически отображается максимальное число событий, выведенных по примененному фильтру;

Примечание: чем больше значение, тем дольше будет выполняться операция экспорта.

• **Максимальное количество событий в файле** – укажите максимальное количество событий, которое будет выгружено в один файл.

Примечание: чем больше значение, тем объемней будет файл. Ограничение: не более 100000 записей в один файл.

- Экспортировать все поля при необходимости включите экспорт всех полей события в файл. Если опция выключена, то будет выполнен экспорт только тех полей, которые настроены для отображения в табличном виде (см. раздел «Настройка набора полей для табличного вида»).
- 4. Нажмите кнопку **Скачать в CSV**. Начнется процесс экспорта, который может занять некоторое время. По ходу выполнения операции будут формироваться и автоматически скачиваться файлы с событиями. Файлы заполняются в соответствии с примененной фильтрацией: от первого события в списке к последнему.

5.3.5 Вспомогательные инструменты для анализа событий

5.3.5.1 Поиск событий

Примечание: начиная с версии 3.7.0 в Платформе Радар заменена поисковая система с **ElasticSearch** на **OpenSearch**. Платформа Радар позволяет искать конкретные события по значениям полей. При этом сохранилась возможность использовать в строке поиска <u>синтаксис</u> <u>строкового поиска Lucene</u>.

Для поиска событий укажите необходимое значение или выражение в строке поиска. Результаты поиска выводятся автоматически по мере заполнения поля.

Пример 1. Поиск всех событий, в которых поле elastic_key имеет значение "Разобрано" (см. «Рис. 44»).

Синтаксис elastic_key: (parsed).

elastic_key: (parsed)		Q 🗄	Сортировка	🖉 Набор полей	🛩 Выбрать несколько
id: AAAAAGYT2ItDRkTEh/iJdNk3	35NfcQJx1 Событие разобрано				Действия 🗸
@timestamp	€				
event.logsource.host	⊕ ⊝ ★ 172.30.254.155:9992				
elastic_key	⊕ ⊖ ∗ parsed				
epoch	⊕ ⊖ ★ 1712576651.792				
event.logsource.application	⊕ ⊖ ★ parsed				
event.logsource.input	⊕ ⊝ ★ 1514-microsoft_windows_even	itlog			
id: AAAAAGYT2IvCJ+3ZFfhcbyb	4gDKmc6CI Событие разобрано				Действия 🗸
@timestamp	€				
event.logsource.host	⊕ ⊝ ★ 172.30.254.155:9992				
elastic_key	⊕ ⊖ ∗ parsed				
epoch	⊕ ⊝ ★ 1712576651.792				
event.logsource.application	⊕ ⊖ ★ parsed				
event.logsource.input	\oplus \odot $*$ 1514-microsoft_windows_even	tlog			

Рис. 44 – Поиск всех событий, в которых поле elastic_key имеет значение "Разобрано"

Пример 2. Поиск всех событий, в которых поле elastic_key имеет значение отличное от "Разобрано" (см. «Рис. 45»).

Синтаксис: elastic_key: (NOT parsed)

stic_key: (NOT parsed)			П Сортировка Набор полей Выбрать несколь
I: AAAAAGYhIKExpLOT+iEEI	Uluk4y88tszW H	е разобрано	Действия
otimestamp	⊕ ⊝ *	18.04.2024 04:31:13	
vent.logsource.host		172.30.254.155:9992	
lastic_key		error	
rror	@ Q ★	Traceback (most recent call last): File " <frozen termite.daemon.worker="">", line 364, in _process_events File "<frozen termite.pipeline="">", line 69, in parse File "<frozen termite.parsers.json_parser="">", line 28, in parse rapidjson.JSONDeco member.</frozen></frozen></frozen>	termite.pipeline>", line 228, in execute File " <frozen deError: Parse error at offset 206: Missing a name for object</frozen
vent.logsource.input		1514-microsoft_windows_eventlog	
vent.uuid	$\odot \odot *$	AAAAAGYhIKExpLOT+iEEUluk4y88tszW	
	$\odot \odot *$	AAAAAGYhIKExpLOT+iEEUluk4y88tszW	
3W	@ @ *	{"rs_collector_hostname":"v-back-com-05";"rs_relay_fqdn":"172.30.254.169";"rs_relay_jp":"172.30.254.169";"rs_collector microsoft_windows_eventlog",	or_ts":"2024-04-18T16:31:13.073681+03:00","rs_module":"151
оказать меньше 🔨			
I: AAAAAGYhIKU5p4wUxuv	vLpyfJNklxZnsF	Событие нормализовано	Действия
otimestamp	€€*	18.04.2024 04:31:12	
vent.logsource.host	⊕	172.30.254.155:9992	
ction	€ € *	detect	
astic_key	⊕	normalized	
poch	• • *	1713447072.324	

Рис. 45 – Поиск всех событий, в которых поле elastic_key имеет значение отличное от "Разобрано"

Пример 3. Поиск по конкретному значению поля (см. «Рис. 46»).

AAAAAGYhJrxHuWzqY3i2p6n	nx31fkltnu	🔍 🗄 Сортировка 🖉 Набор полей	і 🛷 Выбрать несколько
id: AAAAAGYhJrxHuWzqY3i	2p6mx31fkltnu Событие нормализовано		Действия 🗸
@timestamp	€		
event.logsource.host	⊕		
Показать больше 🗸			
< 1 > 20 / страница	∃ ∽		

Рис. 46 – Поиск по конкретному значению

5.3.5.2 Просмотр событий по сформированной агрегации

Платформа Радар позволяет просматривать события, данные по которым были сформированы по результату агрегации.

Для этого настройте агрегации (см. раздел «<u>Добавление агрегации</u>») и нажмите на соответствующую ссылку в таблице результатов (см. «<u>Puc. 47</u>»).



Рис. 47 – Просмотр результатов агрегации

Произойдет переход на страницу "События", где в условиях фильтрации будет применен соответствующий запрос.

5.3.5.3 Настройка плотности отрисовки потока событий

При необходимости вы можете задать плотность отрисовки потока событий на графике. Доступны следующие значения:

- по годам;
- по месяцам;
- по дням;
- по часам: по три часа, по одному часу;
- по минутам: по тридцать минут, по десять минут, по одной минуте;

• по секундам.

Для изменения плотности отрисовки в правом верхнем углу графика "Поток событий" из выпадающего списка выберите необходимое значение (см. «Рис. 48»).



Рис. 48 – Настройка плотности отрисовки потока событий

5.3.5.4 Сортировка событий

Платформа позволяет сортировать порядок событий в списке по значениям выбранных полей.

Для этого нажмите кнопку **Сортировка**. Откроется окно настройки сортировки (см. «Рис. 49»).

Событий: 17, показано 1 - 17

вести		🔍 🗄 Сортирс	овка 🔗 Набор полей 🛷 🛛	Выбрать несколько
_id: AAAAAGX00CA5DZCnhl	b3gQ3HP0rBZp4Ef Событие нормализовано	Выбранные поля	× ^ []	Действия 🗸
		_id	× ^ 🗈	
@timestamp	⊕	Все поля		
event.logsource.host	⊕ ⊖ ★ 172.30.254.68:9992	Q Введите значение		
Показать больше 🗸		_index access		
_id: AAAAAGX0ODbT2qMnW	/YJVDmfq68/aS9wk Событие нормализовано	application.name.keyword createdTimeMs		Действия 🗸
@timestamp	€ € ★ 17.04.2024 11:28:36	elastic_key epoch		
event.logsource.host	⊕ ⊝ ★ 172.30.254.68:9992			
Показать больше 🗸				

Рис. 49 – Настройка сортировки списка событий

Для настройки сортировки воспользуйтесь следующими приемами:

- для выбора полей, по которым будет выполняться сортировка, установите флаги в соответствующих полях;
- сортировка выполняется в порядке добавления полей. Для изменения порядка сортировки используйте кнопки ^ / `;
- для полей, по которым выполняется сортировка, можно задать направление сортировки:
 - ↓ от последнего к первому;
 - 1 от первого к последнему.

5.3.5.5 Настройка набора полей для табличного вида

Для табличного вида списка событий вы можете настроить набор полей для отображения в таблице.

Для этого включите табличный вид по кнопке ^Ш и нажмите кнопку **Набор полей**. Откроется окно "Выбор набора полей" (см. «Рис. 50»).

Выбор набора полей	×
Q Введите название поля	
✓ @timestamp	^ v
✓ event.logsource.host	^ V
✓ elastic_key	^ V
✓ action	∧ ∨
_doc_count	
_id	
_index	
_source	
epoch	
error	
	Применить

Рис. 50 – Окно "Выбор набора полей"

В окне выполните следующие действия:

- 1. Выберите поля, информацию по которым необходимо отобразить в табличном виде, установив соответствующие флаги.
- 2. Настройте порядок столбцов таблицы с помощью кнопок ^ / `.
- 3. Нажмите кнопку Применить.

6. Инциденты ИБ

6.1 Инциденты

6.1.1 Общие данные

Платформа Радар предоставляет большой набор инструментов для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности с целью выявления инцидентов ИБ и организации реагирования на них.

Событие информационной безопасности (information security event) – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инструменты по анализу событий информационной безопасности подробно рассмотрены в разделе «События».

Инцидент информационной безопасности (information security incident) – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

При работе с инцидентами ИБ платформа автоматизирует ряд процессов:

- Оценку событий ИБ и принятие решения: является ли данное событие инцидентом ИБ.
- Оповещение о возникновении инцидента ИБ и назначение инцидента оператору.
- Исследование инцидента и принятие решения по результатам исследования.

Инцидент всегда относится к активу, на котором он выявлен. Значимость актива в инфраструктуре напрямую влияет на оценку угрозы инцидента. Для оценки угрозы инцидента можно использовать несколько параметров:

Срочность. Значение складывается из уровня "значимости" актива, на котором был выявлен инцидент и уровня риска, присвоенному инциденту. На параметр также влияет сетевая видимость актива и то, на сколько инцидент был просрочен.

Уровень риска. Цифровое обозначение уровня угрозы, присвоенному инциденту.

В платформе инцидент принадлежит к одной из трех категорий:

- нарушение политики это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности);
- сетевая аномалия актив проявляет сетевую активность, которую проявлять не должен;
- уязвимость у злоумышленника есть возможность получить контроль (полный или частичный) над активом.

Стадия обработки инцидента называется статус. В платформе используются следующие статусы инцидентов:

• ПР Новый – статус присваивается вне основного рабочего процесса, например для тестирования. Инцидент в данном статусе виден только в интерфейсе администратора;

- Новый статус присваивается, когда инцидент был создан вручную или автоматически;
- **Назначен** статус присваивается, когда инцидент передали в работу конкретному пользователю или группе пользователей;
- **В работе** статус присваивается, когда пользователь, на которого назначили инцидент, начал расследование инцидента;
- Запрошена информация обработка инцидента приостановлена, исполнителем была запрошена дополнительная информация;
- Ожидает проверки для исправления инцидента применены контрмеры, требуется проверка со стороны компетентного лица;
- Риск принят со стороны компетентного лица было принято решения отказаться от дальнейшего расследования инцидента;
- Закрыт работы по расследованию инцидента завершены;
- Недействительный инцидент был создан по ошибке, закрыт без разбора.

Процесс изменения стадии обработки инцидента приведен на «Рис. 51».



Рис. 51 – Процесс изменения статусов инцидентов

В платформе каждый инцидент всегда принадлежит к определенному типу инцидента. Типы инцидентов это сведения о уязвимости, нарушении политики, аномальной сетевой активности без привязки к активу (подробнее см. раздел «Типы инцидентов»).

Схожие инциденты можно объединить в группы, а их затем назначить пользователям. Это упрощает управление назначением инцидентов сотрудникам и позволяет выполнять массовые операции над инцидентами через группы (подробнее см. раздел «<u>Группы инцидентов</u>»).

Инциденты могут хранить любую дополнительную информацию, добавляемую к инцидентам как в процессе их создания правилами корреляции, так и в процессе расследования операторами (подробнее см. раздел «<u>Дополнительные поля</u>»).

Платформа Радар позволяет происшествия, критической отправлять выявленные в (КИИ) Российской информационной инфраструктуре Федерации, национальный В координационный центр по компьютерным инцидентам (подробнее см. раздел «Происшествия на отправку»).

Работа с инцидентами включает в себя следующие процессы:

- 1. «<u>Создание инцидента</u>».
- 2. «<u>Просмотр инцидента</u>».
- 3. «<u>Назначение инцидента</u>».
- 4. «Изменение статуса инцидента».
- 5. «Добавление комментария к инциденту».
- 6. «<u>Редактирование инцидента</u>».
- 7. «Просмотр истории изменения инцидента».
- 8. «<u>Удаление инцидента</u>».

Для работы с инцидентами ИБ перейдите в раздел **Инциденты** → **Инциденты** (см. «Рис. 52»).

≡ (С ПАНГЕС РАДАР	9 172.30.254.	138 ∨ Инци	іденты						④ База знаний	\bigcirc admin \checkmark
â	Инц	иденты									
Q											
0	∇	Создать У	/далить Удалить	все							C'
-0		Срочность	Уровень риска	Название	Статус	Актив	Создано	Тип инцидента	Обновлено	Группа инцидентов	
CD.		0.07	0.5	Множественные неудачные попытки	Ожидает проверки	localhost	14:28:52 05.09.2024	Множественные неудачные	13:48:42 09.09.2024	-	
đ		0.07	0.5	MS-WIN - Для учетной записи установле	В работе	localhost	14:37:16 05.09.2024	MS-WIN - Для учетной записи	10:56:31 09.09.2024	-	
2		0.82	8	Множественные неудачные попытки	Новый	stand-x.pgr.local	14:55:15 03.09.2024	Множественные неудачные	14:37:13 05.09.2024	-	
ж	<	1 > 1	I0 / страница ~								
#†4											
0											

Рис. 52 – Раздел "Инциденты"

В разделе отображается следующая информация об инцидентах:

- Срочность цветовое и цифровое обозначение срочности инцидента;
- Название наименование инцидента;
- Статус состояние инцидента;
- Создано дата и время создания инцидента;
- Уровень риска цифровое обозначение уровня угрозы, присвоенного инциденту;
- **ID** идентификатор инцидента;
- Тип инцидента наименование типа инцидента;
- Группа инцидентов наименование группы инцидентов, в которую входит инцидент;
- Актив наименование актива, на котором выявлен инцидент;
- **Последнее происшествие** дата и время последнего происшествия, зафиксированного по инциденту;
- Кол-во происшествий количество происшествий, зафиксированных в инциденте;
- Кол-во повторных открытий количество повторных открытий инцидента;
- Пользователь наименование пользователя, назначенного на разбор инцидента;
- **Группа пользователей** наименование группы пользователей, назначенной на разбор инцидента;

- Обновлено дата и время изменения информации об инциденте;
- Категория наименование категории, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость;
- Эксплуатируется удаленно признак, возможна ли удаленная эксплуатация уязвимости: да, нет;
- Результат анализа результат анализа инцидента.

6.1.2 Создание инцидента

Создание инцидента можно выполнить несколькими способами:

- 1. Вручную из раздела Инциденты.
- 2. При анализе событий ИБ (см. раздел «Создание инцидента»).
- 3. При анализе "сработок" правила корреляции (см. раздел «<u>Действия над результатами</u> <u>сработок правила</u>»).
- 4. Автоматически, по результатам работы следующих механизмов:
 - работы правил корреляции (см. раздел «<u>Правила корреляции</u>»);
 - при работе со сканером уязвимостей (см. раздел «<u>Начните процесс</u> удаления сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».
- 1. Подтвердите удаление в открывшемся окне.
- 2. Сетевой интерфейс будет удален из платформы.
 - Результаты сканирования»);
 - при контроле установленного программного обеспечения (см. раздел «<u>Наборы</u> <u>правил соответствия ПО</u>»).

Для создания инцидента вручную выполните следующие действия:

1. Перейдите в раздел **Инциденты** → **Инциденты** и нажмите кнопку **Создать**. Откроется форма "Создание инцидента" (см. «Рис. 53» и «Рис. 54»).

Создание инцидента		Сбросить	Создать
Тип инцидента	Актив		
Множественные неудачные попытки входа на одном узле 🔍	stand-x.pgr.local		\sim
Название инцидента	Уровень риска		
Множественные неудачные попытки входа на одном узле	2		- +
 Нарушение политики Сетевая аномалия Уязвимос Результат анализа () 	гь		
Внутреннее примечание			
Группа инцидентов			
Группа "Множественные неудачные попытки входа"			~

Рис. 53 – Создание инцидента. Общие сведения

Подробности по типу инцидента Сеодка
Один целевой узел сообщает о превышении установленного предела количества ошибок входа в систему под различными именами пользователя.
Описание
Обнаружено превышение установленного предела количества ошибок входа в систему с одного узла-источника под различными именами пользователей. Большое количество таких ошибок может указывать на попытку получения учетных данных пользователя в целевой системе методом подбора. Атака методом подбора предполагает поиск решения путем постоянного перебора множества возможных вариантов паролей расшифрованных ключей и т. д.
Последствия реализованной угрозы
Множественные оцибки аутентификации могут указывать на попытку взлома учетной записи. Риск будет зависеть от источника входа в систему. В случае успеха злоумышленника наиболее опасными являются следующие риски:
 Раскрытие информации: Уязвимость, которая может привести к раскрытию учетных данных жертвы. В результате киберпреступник может получить действительные учетные данные пользователя, а с их помощыс – доступ к конфиденциальной информации. Повышение привилютий: Злоумышленник, успешно воспользовавшийся этой уязвимостью, может запустить произвольный код от имени администратора. В этом случае он также получает возможность устанавливать программые, просматривать, изментых удалять данные, создавать новые учетные записи с полными праваим пользователя, по случае он также получает возможность устанавливать программые, просматривать, изменты и удалять данные, создавать новые учетные записи с полными подвателя. Удаленное выполнение кода: Эта уязвимость позволяет злоумышленнику получить доступ к чужому вычислительному устройству и вносить изменения, независимо от географического расположения этого
устройства. * Распространение вредоносного контента или спама, а также перенаправление доменов на страницы с вредоносным контентом и выдача себя за владельцев учетных записей с целью распространения фальшивог контента или вредоносных ссылок. * Сбор учетных данных для продажи третьим сторонам.
Рекомендации по устранению угрозы
 Изопируйте узел от сети. Просканируйте узел с помощью антивирусной программы на предмет наличия угроз и устраните их в случае выявления. Если узел-источник является внутренним узлом, проверьте его на предмет взлома. Если узел-источник является внешним узлом, проверьте политику брандмауара, чтобы убедиться, что доступ ко внутренним системам можно получить только с IP-адресов доверенных диапазонов.
Рекомендации по уменьшению риска
Профилактика угрозы эффективнее, чем устранение ее последствий. Далее приведен список основных рекомендаций по повышению безопасности системы:
* Используйте сложные пароли или требуйте их использования. * Определите «нормальное» количество неудачных попыток входа в систему. * Используйте тесты САРТСНА.
 Настройте задержку между попытками входа. Используйте контрольные вопросы.
 Actrustupy/pre_gayydpartophy/o ayrenrudpwsquwo. Используйте двухиранторную аугентификацию. Используйте несколько URL-заресов входа. Перехитрите ПО злоумышленнико (некоторые боты обучены распознавать ошибки, но в случае одновременных неудачных попыток входа в систему можно использовать перенаправление на разные страницы ошибок. Из-за этого злоумышленнику потребуется как минимум перейти на более продвинутое ПО).

- 2. Укажите на форме следующую информацию:
 - в поле **Тип инцидента** из выпадающего списка выберите тип, к которому относится инцидент. При выборе типа инцидента в поля формы будут автоматически добавлены данные из справочника "Типы инцидентов";
 - в поле **Актив** из выпадающего списка выберите устройство, на котором был обнаружен инцидент;
 - в поле Название инцидента укажите название инцидента;
 - в поле **Уровень риска** выберите цифровое обозначение уровня риска. Допустимые значения от 0 до 10;
 - в поле **Категория** выберите одну из категорий, в которую входит инцидент: нарушение политики, сетевая аномалия, уязвимость;
 - в случае, если сведения о происшествии инцидента планируется передать во внешнюю систему, то в поле **Результат анализа** необходимо указать соответствующие сведения (см. раздел «<u>Происшествия на отправку</u>»);
 - в поле Внутреннее примечание укажите дополнительные сведения об инциденте;
 - в поле **Группа инцидентов** из выпадающего списка выберите группу, в которую следует добавить инцидент (см. раздел «<u>Группы инцидентов</u>»).
- 3. При необходимости в блоке **Подробности по типу инцидента** актуализируйте информацию о типе инцидента.

Примечание: при изменении информации в данном блоке будет изменен соответствующий справочник в разделе «<u>Типы инцидентов</u>».

4. Нажмите кнопку Создать.

6.1.3 Просмотр инцидента

Для просмотра и анализа инцидента нажмите по ссылке с наименованием инцидента. Откроется форма просмотра инцидента (см. «Рис. 55»).

Просмотр инцидента				🛈 База знаний	0	admin
← ID:1			Статус: Назначен Н	азначить Редактир	овать] [:
Множественные неудачные попытки входа на различных хостах под различными учетными записями	Актив	ие: stand-x.pgr.local				
Обнаружено превышение установленного предела количества ошибок входа в систему нескольких целевых узлов с одного узла-источника под различными именами пользователей. Большое количество таких ошибок может указывать на попытку получения учетных данных пользователя в целевой истеме методом подбора. Атака мистодом подбора предполагает поиск решения путем постоянного перебора множества возможных вариантов паролей,	з Тип Группа	Host ККИ				
В Источник: Коррелятор Кол-во повторных открытий: 0 Кол-во повторных открытий: 0 Кол-во повторных открытий: 0 Дата создания 03.09.2024 14:55:15 Тип инцидента Множественные неудачные попытки входа на различных хостах под различным учетными записями Последнее происшествие - Группа инцидентов Группа "Множественные неудачные попытки входа" Назначено - Тип Нарушение политики Время повторного открытия - Показать меньше -						
Показать в событиях				Kauauau	С	, (Q
8c9c4f2d-8b37-442b-abdb-469cdc37216d		Нет	14:37:13 05.09.202	4 14:37:13 05.09.2024		İ
8f1debf8-3d19-4fbe-8740-1e25ffb033f5		Нет	14:55:14 03.09.2024	4 14:55:14 03.09.2024		± 4
1 > 10 / страница ~ История коммуникации 12 сент. 2024, 12:09:31 Инцидент взят в работу admin 12 сент. 2024, 12:09:48 Инцидент передан. Итоги в файле			Добави	гь комментарий 2 ком	ментар	∧ RN(
admin			2	024-09-12T12:06:48+03:	<u>)0_итог</u>	.pdf

Рис. 55 – Форма просмотра инцидента

На форме просмотра инцидента информация сгруппирована по следующим блокам:

- Общая информация об инциденте.
- Актив информация об активе, на котором обнаружен инцидент.
- Результат анализа информация о результатах анализа инцидента. Данный блок отображается если данное поле было заполнено при создании инцидента.
- Происшествия информация о происшествиях, из которых состоит инцидент.
- История коммуникации в рамках расследования инцидента.

6.1.3.1 Общая информация об инциденте

Пример блока с общей информации об инциденте приведен на «Рис. 56».

Множественные неудачные попытки входа на различных хостах под различными учетными записями

0	Обнаружено пр нескольких цел Большое колич пользователя в поиск решения расшифрованн	ревышение установленного предела количества ошибок входа в систему певых узлов с одного узла-источника под различными именами пользователей. нество таких ошибок может указывать на попытку получения учетных данных в целевой системе методом подбора. Атака методом подбора предполагает п путем постоянного перебора множества возможных вариантов паролей, ых ключей и т. д.
8	Источник: Кол-во повто Кол-во проис Правило кор	Коррелятор орных открытий: 0 сшествий: 2 реляции: identityRUle
Дата с	создания	03.09.2024 14:55:15
Тип ин	цидента	Множественные неудачные попытки входа на различных хостах под различными учетными записями
После проис	днее шествие	-
Группа	а инцидентов	Группа "Множественные неудачные попытки входа"
Назна	чено	-
Тип		Нарушение политики
Время повторного открытия		-
Показа	ать меньше 🔨	

Рис. 56 – Просмотр инцидента. Общая информация

В блоке отображается следующая информация:

- Название инцидента.
- Подробное описание инцидента.
- Цветовое и цифровое значение уровня риска.
- Источник механизм, с помощью которого был создан инцидент:
 - Коррелятор инцидент был создан на основе "сработки" правила корреляции;
 - Сканнер уязвимостей инцидент был создан в результате работы сканнера уязвимостей;
 - Если источник не указан, это означает что инцидент был создан вручную;
 - Контроль ПО инцидент был создан на основе "сработки" правила контроля установленного ПО.

Информация, отображаемая в блоке "Источник" формируется в зависимости от механизма, с помощью которого был создан инцидент и может содержать следующую информацию:

- Эксплуатируется удаленно (только для сканнера уязвимостей) признак удаленной эксплуатации, возможные значение: да, нет;
- Правило корреляции (только для коррелятора) наименование правила, по "сработке" которого был создан инцидент. По ссылке произойдет переход на форму просмотра правила;
- Количество повторных открытий инцидента;
- Количество происшествий, зарегистрированных в инциденте.
- Дата и время создания инцидента.
- Тип инцидента по ссылке произойдет переход на форму просмотра типа инцидента.
- Последнее происшествие дата и время последнего зарегистрированного происшествия.
- Информация о пользователях, которым назначен инцидент.
- Тип категория, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость.
- Дата и время повторного открытия.

6.1.3.2 Информация об активе

Пример блока с информацией об активе приведен на «Рис. 57».

Актие	}		
3	Название:	stand-x.pgr.local	
Тип		Host	
Группа		ККИ	

Рис. 57 -- Просмотр инцидента. Информация об активе

В блоке отображается следующая информация:

- Цветовое и цифровое обозначение "значимости" актива.
- Название актива. По ссылке произойдет переход на форму просмотра актива.
- Тип актива.
- Название группы, к которой принадлежит актив. По ссылке произойдет переход на форму просмотра группы активов.

6.1.3.3 Информация о происшествиях

Пример блока с информацией о происшествиях приведен на «Рис. 58».

Про	исшествия				
Пок	азать в событиях				C Ø
	ID	Отправлено в НКЦКИ	Начало активности	Конец активности	
	8c9c4f2d-8b37-442b-abdb-469cdc37216d	Нет	14:37:13 05.09.2024	14:37:13 05.09.2024	
	8f1debf8-3d19-4fbe-8740-1e25ffb033f5	Нет	14:55:14 03.09.2024	14:55:14 03.09.2024	
<	1 > 10 / страница ~				

Рис. 58 – Просмотр инцидента. Информация о происшествиях

В блоке отображается следующая информация:

- Уникальный идентификатор происшествия.
- Отправлено в НКЦКИ признак отправки происшествия в национальный координационный центр по компьютерным инцидентам (подробнее см. раздел «<u>Происшествия на отправку</u>»).
- Дата и время начала и конца активности происшествия.

Для просмотра деталей происшествия нажмите на кнопку . Произойдет переход в раздел **События** с автоматически сформированным фильтром для отображения происшествия на графике потока событий.

Для просмотра события, в котором было зарегистрировано происшествие, нажмите на кнопку 🖾. Откроется окно "Результат события" (см. «Рис. 59»).

Результат события	×
[{ "@timestamp": "2024-09-05T05:28:36.6214546Z", "action": "access",	
<pre>"elastic_key": "normalized", "event": { "auth": {</pre>	1
"protocol": { "name": "SMB" }	
<pre>}, "category": "share_operation", "description": "A network share object was added.",</pre>	
<pre>"logsource": { "application": "os", "name": "Microsoft Windows",</pre>	
"product": "windows", "subsystem": "system_operation", "vendor": "microsoft"	
<pre>}, "severity": "4", "subcategory": "share_created", "timeters", "age too offer you go for the set"</pre>	
"uuid": "1c6b5f0e-b34e-48c8-aba8-977fb093d27f" }, "id": "1c6b5f0e b34e-48c8-aba8-977fb093d27f"	
"initiator": { "session": { "id": "0x3a7"	
}, "user": { "domain": "DEMO".	
"id": "S-1-5-18", "name": "DEMO-SERVER2012\$"	
	Скопировать

Рис. 59 – Окно "Результат события"

Если инцидент был создан с помощью сканнера уязвимостей, то доступен просмотр данных об обнаруженной уязвимости. Для этого нажмите кнопку 🛆. Откроется окно "Данные по уязвимости" (см. «Рис. 60»).

ID	0e9a5757-82ef-4c9e-a9ca-0761215c039f
Начало активности	19 июля 2024, 05:47:40
Обновлено	19 июля 2024, 05:47:40
ld плагина	413501
Название плагина	Повреждение памяти, связанное с Internet Explorer
Порт	-1
Протокол	-1
Внешнее сканирование	true
Вектор CVSS	AV:N/AC:M/Au:N/C:C/I:C/A:C
Вектор временного CVSS	AV:N/AC:M/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C
Базовый CVSS	9.3
Временный CVSS	6.9
Фактор риска	Высокий
Дата изменения плагина	-
Дата публикации	2014-08-12T00:00:00Z
Дополнительные данные	-

Рис. 60 – Окно "Данные по уязвимости"

6.1.3.4 История коммуникации

Пример блока с информацией об истории коммуникации приведен на «Рис. 61».

История коммуни	кации	Добавить комментарий	2 комментария	
12 сент. 2024, 12:09:31 admin	Инцидент взять в работу			
12 сент. 2024, 12:09:48 admin	Инцидент передан. Итоги в файле	2024-09-12T12:06:	48+03:00_итог.pdf	

Рис. 61 -- Окно "Данные по уязвимости"

В блоке отображается следующая информация:

- Количество оставленных комментариев.
- Дата и время создания комментария.

- Содержание комментария.
- Список прикрепленных файлов.
- Пользователь, оставивший комментарий.

Для просмотра прикреплённых файлов нажмите на соответствующую ссылку.

6.1.4 Назначение инцидента

- 1. Перейдите на форму просмотра необходимого инцидента.
- 2. Нажмите на кнопку Назначить. Откроется окно "Назначить" (см. «Рис. 62»).

Назначить	×
Назначить пользователю Назначить группе	
admin	~
	Сохранить

Рис. 62 – Окно "Данные по уязвимости"

- 3. Выполните в окне следующие действия:
 - выберите способ назначения: конкретному пользователю или группе пользователей;
 - из выпадающего списка выберите пользователя или группу пользователей;
 - нажмите кнопку Сохранить.

6.1.5 Изменение статуса инцидента

- 1. Перейдите на форму просмотра необходимого инцидента.
- 2. Нажмите на кнопку с текущим статусом инцидента и из выпадающего списка выберите доступный статус. Описание и возможные изменения статусов приведены в разделе «Общая информация».

6.1.6 Добавление комментария к инциденту

- 1. Перейдите на форму просмотра необходимого инцидента.
- 2. В блоке **История коммуникации** нажмите на кнопку **Добавить комментарий**. Откроется окно "Добавить комментарий" (см. «Рис. 63»)

Добавить комментарий						
Комментарий						
Текст комментария	Текст комментария					
	Отмена	Прикрепить файл	Добавить			

Рис. 63 – Окно "Добавить комментарий"

- 3. Выполните в окне следующие действия:
 - в поле Комментарий укажите необходимые сведения.
 - при необходимости прикрепите файл. Для этого нажмите на кнопку **Прикрепить файл** и в открывшемся окне укажите путь к файлу.
 - нажмите кнопку Добавить.

6.1.7 Редактирование инцидента

- 1. Перейдите на форму просмотра необходимого инцидента и нажмите кнопку **Редактировать**.
- 2. Внесите необходимые изменения.
- 3. При необходимости добавьте дополнительные поля в инцидент (подробнее см. раздел «Дополнительные поляе поля»).
- 4. Сохраните изменения.

6.1.8 Просмотр истории изменения инцидента

Перейдите на форму просмотра необходимого инцидента, нажмите кнопку и из выпадающего списка выберите пункт **История изменений**. Откроется форма "История изменений" (см. «Рис. 64»).

История изменений	
Действие	Изменение
Время	12 сентября 2024, 12:02:22
Сервис	ui
Кем изменен	93adf94b-0f93-45d1-8b3c-a15a38399d49
Детали	Подробнее

Рис. 64 – История изменений"

На форме отображается следующая информация:

• Действие – тип действия, выполненного над инцидентом: создание, изменение и т.д.;
- Время дата и время выполнения действия над инцидентом;
- Сервис название сервиса, через который было выполнено изменение;
- Кем изменен уникальный идентификатор сервиса или пользователя, выполнившего изменение;
- Детали просмотр подробного журнала изменения инцидента.

6.1.9 Удаление инцидента

Удаление инцидента можно выполнить несколькими способами:

- Способ 1 из раздела Инциденты;
- Способ 2 из формы просмотра инцидента.

Способ 1:

- 1. Выберите один или несколько инцидентов, установив соответствующие флаги.
- 2. Нажмите кнопку Удалить.
- 3. Подтвердите удаление в открывшемся окне.
- 4. Для удаления всех инцидентов нажмите кнопку Удалить все.

Способ 2:

- 1. Перейдите на форму просмотра необходимого инцидента, нажмите кнопку ыпадающего списка выберите пункт **Удалить**.
- 2. Подтвердите удаление в открывшемся окне.

6.2 Типы инцидентов

6.2.1 Общие сведения

Типы инцидентов содержат сведения об угрозах, на основе которых создаются инциденты. В платформе каждый инцидент всегда принадлежит к определенному типу инцидента.

В платформе предоставляется большой набор предустановленных типов, но существует возможность добавлять, актуализировать и настраивать типы инцидентов самостоятельно.

Тип инцидента всегда принадлежит к одному из трех типов уязвимостей:

- нарушение политики это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности);
- сетевая аномалия актив проявляет сетевую активность, которую проявлять не должен;
- уязвимость у злоумышленника есть возможность получить контроль (полный или частичный) над активом.

Работа с типами инцидентов включает в себя следующие процессы:

- 1. «<u>Просмотр и анализ типа инцидента</u>».
- 2. «<u>Создание типа инцидента</u>».

- 3. «<u>Редактирование типа инцидента</u>».
- 4. «<u>Написать ответственному</u>».
- 5. «Дублирование типа инцидента».
- 6. «Дублирование типа инцидента
- 1. Откройте форму просмотра типа инцидента и нажмите кнопку Дублировать.
- 2. В открывшемся окне укажите наименование типа инцидента и нажмите кнопку Дублировать.
- 3. Будет создан новый тип инцидента на основе существующего.
- 7. Импорт типов инцидентов».
- 8. «<u>Экспорт типов инцидентов</u>».
- 9. «Экспорт типов инцидентов в CSV».
- 10. «<u>Удаление типа инцидента</u>».

Для работы с типами инцидентов перейдите в раздел **Инциденты** → **Типы инцидентов** (см. «Рис. 65»).

≡	ПАНГЕО Г	172.30.254.97	∨ ∣ Типы инцидентов		л	ицензия активна до: 2027-11-16 ① Документация	a \textcircled{a} admin \checkmark			
â	Типы	инциде	НТОВ							
Q	٩									
0	7	Создать Уда	алить Удалить все Экспортировать Экспортировать все Э	кспортировать выбранные в сsv	Экспортиро	вать в сsv Импортировать Выб	рано: 0 С 🕲			
c. 19		ID $ \uparrow $	Название ↓↑	Тип уязвимости	Оце ↓↑	Правила корреляции				
0 Q		109	Сетевые аномалии - Сканирование портов	Сетевая аномалия	0	Обнаружено сетевое сканирование портов, MS-WIN-FRWL - Сканирование с одного хоста по показать 10	© ÎI			
<i>%</i>		50	test	Нарушение политики	3	-	◎ ⁄⁄ ⑪			
×		161	Windows - Учётная запись была включена	Нарушение политики	5	Windows - Учётная запись была включена	© 11			
141		49	Windows - Системные журналы были очищены	Нарушение политики	9	-	© 0 fi			
ŶĬŎ		51	Отключение журналирования сервиса "UFW"	Нарушение политики	8	Linux - Отключение журналирования сервиса "UFW"	© 11			
0		52	Linux - Обнаружен поиск паролей	Сетевая аномалия	8	AuditD - Обнаружен поиск паролей	© 11			
		53	MS-WIN-Удаление подключений к сетевым ресурсам	Нарушение политики	6	MS-WIN_Sysmon_T1070.005_Удаление подключен	© <u>Ü</u>			
		54	Windows - Обнаружена атака с понижением версии	Нарушение политики	7	Windows - Обнаружена атака с понижением верси	© <u>Ü</u>			

Рис. 65 – Раздел "Типы инцидентов"

В разделе отображается следующая информация:

- ID идентификатор типа инцидента;
- Название наименование типа инцидента;
- Тип уязвимости наименование типа уязвимости, к которой относится угроза: нарушение политики, сетевая аномалия, уязвимость;
- Оценка риска цифровое обозначение уровня угрозы;
- **Правила корреляции** список правил корреляций, которые задействуют данный тип инцидента при "сработке". Если у типа инцидента выставлена связь с правилами корреляции, то его нельзя изменить.

Элементы управления универсальными таблицами описаны в разделе «Универсальные таблицы».

6.2.2 Просмотр и анализ типа инцидента

Для работы с типами инцидентов перейдите в раздел **Инциденты** → **Типы инцидентов**. Для просмотра типа инцидента выберите его из списка (см. «Рис. 66»).



Рис. 66 – Форма просмотра типа инцидента

В боковой панели отображается следующая информация о типах инцидентов:

- Оценка риска цветовое и цифровое обозначение уровня угрозы;
- Название типа инцидента;
- Уникальный идентификатор типа инцидента (короткая версия);
- Тип уязвимости наименование типа уязвимости, к которой относится угроза: нарушение политики, сетевая аномалия, уязвимость;
- Дата и время последнего изменения.

В рабочей области помимо информации, отображаемой в боковой панели, отображается следующая информация:

- Признак соответствия ПО: да, нет. Параметр определяет используется данный тип инцидентов для создания инцидентов при оценке соответствия ПО (подробнее см. «Руководство оператора 3.6.10» раздел «Оценка соответствия ПО»);
- Сводка краткое описание угрозы;
- Описание подробное описание угрозы;
- Последствия реализованной угрозы описание последствий, которые могут возникнуть, если угроза была реализована;

- Рекомендации по устранению угрозы описание действий, которые рекомендуется предпринять для устранения угрозы;
- Рекомендации по уменьшению риска список основных действий, которые рекомендуется предпринять для предотвращения реализации угрозы;
- Таблица со списком инцидентов, которые были созданы с признаком принадлежности к данному типу инцидента.

Элементы управления боковой панелью описаны в разделе «Боковая панель».

6.2.3 Создание типа инцидента

1. Начните процесс создания типа инцидента через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание типа инцидента" (см. «Рис. 67»).

Создание типа инцидента	Сбросить	Создать
Название *		
Новый тип инцидента. Уязвимость в поле "наименование поля"		
Тип уязвимости *		
Уязвимость		
Использовать для создания инцидентов при оценке соответствия ПО		
Сводка *		
BDU:2024-"номер": Уязвимость параметра "наименование поля" платформы раздельного хранения и управления данными, позволяющая нарушителю выполнять произвольные SQL-запросы к базе д	цанных	
Описание		
Точкой входа является URL /наименование сервиса/***, где *** задаёт сущности (удалось идентифицировать вхождение уязвимого параметра по крайней мере на страницах сущностей, где в парам поля для выгрузки данных.	terpe fields пер	редаются
Последствия реализованной угрозы		
Чтение информации из БД Чтение локальных файлов Исполнение кода на сервере Повышение призилетий		
Рекомендации по устранению угрозы *		
Обновиться до версии 3.7 и выше		
Рекомендации по уменьшению риска		
В качестве примера архитектурного решения для устранения уязвимости рекомендуется внедрение механизма предварительного получения полей из запрашиваемой таблицы с последующей свер запросе полями. При появлении нелегитимных сущностей запрос не должен исполняться, тем самым реализуется механизм фильтрации полей по белому списку.	жой с запраши	иваемыми в
Внутренняя заметка		
Информация для внутреннего пользования		
Оценка риска		
	-0	
υ I Z 3 4 5 6 7 8 Комментарий	Э	10
Дополнительная информация		

Рис. 67 – Форма "Создание типа инцидента"

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите название типа инцидента;
 - в поле **Тип уязвимости** из выпадающего списка выберите тип угрозы, к которой будет относится тип инцидента: нарушение политики, сетевая аномалия, уязвимость;
 - при необходимости использовать данный тип инцидентов для создания инцидентов при оценке соответствия ПО включите соответствующий переключатель;

Примечание: для создания инцидентов при оценке соответствия ПО требуется лишь один тип инцидента с данным признаком.

• в поле Сводка укажите краткое описание угрозы;

- в поле Описание укажите подробное описание угрозы;
- в поле **Последствия** укажите описание последствий, которые могут возникнуть, если угроза будет реализована;
- в поле **Рекомендации по устранению угрозы** укажите перечень действий, которые необходимо выполнить для устранения угрозы;
- в поле **Рекомендации по уменьшению риска** укажите перечень действий, которые необходимо предпринять для предотвращения возникновения угрозы;
- в поле **Внутренняя заметка** укажите дополнительные сведения, предназначенные для внутреннего использования;
- в поле Оценка риска задайте цифровое обозначение уровня угрозы;
- в поле Комментарий укажите дополнительные сведения.
- 3. Нажмите кнопку Создать.

6.2.4 Редактирование типа инцидента

- 1. Начните процесс редактирования типа инцидента через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

6.2.5 Написать ответственному

1. Откройте форму просмотра типа инцидента и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 68»).

×
~
Отправить

Рис. 68 – Окно "Новое сообщение"

- 2. Укажите в окне следующую информацию:
 - в поле **Получатель** из выпадающего списка выберите получателя сообщения;

- в поле Заголовок укажите тему сообщения;
- в поле Сообщение укажите текст сообщения.
- 3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя** → **Сообщения**.
- 4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку типа инцидента.

6.2.6 Дублирование типа инцидента

- 4. Откройте форму просмотра типа инцидента и нажмите кнопку Дублировать.
- 5. В открывшемся окне укажите наименование типа инцидента и нажмите кнопку **Дублировать**.
- 6. Будет создан новый тип инцидента на основе существующего.

6.2.7 Импорт типов инцидентов

- 1. Начните процесс импорта типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. В открывшемся окне укажите путь к архиву с данными.
- 3. Нажмите кнопку Открыть.

6.2.8 Экспорт типов инцидентов

- 1. Начните процесс экспорта типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. Будет сформирован архив с типами инцидентов в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

6.2.9 Экспорт типов инцидентов в CSV

- 1. Начните процесс экспорта в CSV типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. В открывшемся окне укажите путь для сохранения файла/файлов в формате .csv.

6.2.10 Удаление типа инцидента

- 1. Начните процесс удаления типа инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Тип инцидента будет удален из платформы.

6.3 Группы инцидентов

Группы инцидентов предназначены для упрощения исследования инцидентов сотрудниками. Схожие инциденты помещают в группы, а их затем назначают пользователям. Группа инцидентов может быть создана одним из следующих способов:

- вручную, через интерфейс платформы;
- автоматически, с использованием правила корреляции.

Работа с группами инцидентов включает в себя следующие процессы:

- 1. «<u>Просмотр группы инцидентов</u>».
- 2. «<u>Создание группы инцидентов</u>».
- 3. «Редактирование группы инцидентов».
- 4. «Назначение группы инцидентов пользователю».
- 5. «Назначение группы инцидентов группе пользователей».
- 6. «Добавление инцидентов в группу».
- 7. «Массовое закрытие инцидентов через группу».
- 8. «Открепление инцидентов от группы».
- 9. «<u>Удаление группы инцидентов</u>».

Для работы с группами инцидентов перейдите в раздел **Инциденты** → **Группы инцидентов** (см. «Рис. 69»).

≡	Кангес Радар	° 172.30.254.97 ∨ Группы инци	ентов		Лице	ензия активна до: 2027-11-16 	① Документация	$@$ admin \lor		
â	Гру	ипы инцидентов								
Q										
0	Фильтры +									
⊂8	Сортировка									
ð	Сбр	осить Применить								
*	7	Создать Удалить Удалить все					Выбрано: 0	C ©		
0.+		Название	Описание	Кол-во инцидентов 🥼	Пользователь	Группа пользователей 🥼	Обновлено 🕂			
ж		Windows инциденты	Группа, в которую помещаются	100	admin	users	2025-04-28 14:45:31	• 1		
ψ٩		Linux инциденты	-	20	admin	inventorization	2025-04-28 14:48:58	◎ ⁄ ⊡		
0		Прочие инциденты	-	0	-	-	2025-04-28 14:49:49	◎ ⁄ ⊡		
	< 1 > 50 / страница >									

Рис. 69 – Раздел "Группы инцидентов"

В разделе отображается следующая информация:

- Название наименование группы инцидентов;
- Описание описание группы инцидентов;
- Кол-во инцидентов количество инцидентов в группе;
- **Пользователь** наименование пользователя, которому по умолчанию будут назначаться инциденты, попадающие в данную группу;
- **Группа пользователей** наименование группы пользователей, которой по умолчанию назначаются инциденты, попадающие в данную группу;
- Обновлено дата и время обновления информации о группе инцидентов.

6.3.1 Просмотр группы инцидентов

Для просмотра группы инцидентов нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранной группы инцидентов (см. «Рис. 70»).

≡	Кангео 172.30.254.138 V Редак	тироват	ъ группу				 База знаний 	() adr	nin \sim
â	8 7 0 C +	← Γ _Ι	руппа "Множ	ественные неудачные попытки входа"			R 2 2	0	:
Q	Группа "Множественные								
0	Количество инцидентов: 2 Изменено: 2024-09-09 15:45:56	Описани							
⊊.ª	Группа "Ложные срабатывания"		а, оовединяющие все г						
D	Количество инцидентов: 2								
Ø	VISMENERO, 2024-05-05 17-13-30	Пользов	атель по умолчанию						
P.		admin							
×									
441		Группа г	пользователей по умол	танию					
		users							
Ø		Инцид	центы						
		∇	Открепить связанные	инциденты Закрыть инциденты				C	Ô
	0		Срочность	Название	Статус	Актив	Создано		
			0.82	Множественные неудачные попытки входа на одном узле под	Новый	localhost	15:46:51 09.09.2024		
			0.07	Множественные неудачные попытки входа на одном узле под	В работе	localhost	14:28:52 05.09.2024		
		<	1 > 10 / страны	ица ~					

Рис. 70 – Форма просмотра группы инцидентов

В боковой панели отображается следующая информация о группах инцидентов:

- Наименование группы инцидентов;
- Количество инцидентов в группе;
- Дата и время изменения информации о группе.

В рабочей области, помимо информации, отображаемой в боковой панели, отображается следующая информация:

- Описание описание группы инцидентов;
- Пользователь по умолчанию наименование пользователя, которому по умолчанию будут назначаться инциденты, попадающие в данную группу;
- **Группа по умолчанию** наименование группы пользователей, которой по умолчанию назначаются инциденты, попадающие в данную группу;
- Блок Инциденты содержит таблицу с информацией об инцидентах, входящих в группу:
 - Срочность цветовое и цифровое обозначение срочности инцидента;
 - Название наименование инцидента;
 - Статус состояние инцидента;
 - Создано дата и время создания инцидента;
 - Уровень риска цифровое обозначение уровня угрозы, присвоенного инциденту;
 - **ID** идентификатор инцидента;
 - Тип инцидента наименование типа инцидента;

- **Группа инцидентов** наименование группы инцидентов, в которую входит инцидент;
- Актив наименование актива, на котором выявлен инцидент;
- Последнее происшествие дата и время последнего происшествия, зафиксированного по инциденту;
- Кол-во происшествий количество происшествий, зафиксированных в инциденте;
- Кол-во повторных открытий количество повторных открытий инцидента;
- Пользователь наименование пользователя, назначенного на разбор инцидента;
- **Группа пользователей** наименование группы пользователей, назначенной на разбор инцидента;
- Обновлено дата и время изменения информации об инциденте;
- Категория наименование категории, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость;
- Эксплуатируется удаленно признак, возможна ли удаленная эксплуатация уязвимости: да, нет;
- Результат анализа результат анализа инцидента.

6.3.2 Создание группы инцидентов

1. Начните процесс создания группы инцидентов через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создать группу инцидентов" (см. «Рис. 71»).

Создать группу инцидентов	Сбросить	Создать
Название		
Ложные срабатывания		
Описание		
Сюда помещаются инциденты, признанные как "Ложное срабатывание"		
Пользователь по умолчанию		
admin		~
Группа пользователей по умолчанию		
users		~

Рис. 71 – Форма "Создать группу инцидентов"

2. Укажите на форме следующую информацию:

- в поле Название укажите название группы;
- в поле Описание укажите описание группы;
- в поле **Пользователь по умолчанию** выберите пользователя, которому по умолчанию будут назначаться все инциденты из группы;
- в поле **Группа пользователей** по умолчанию выберите группу пользователей, которым по умолчанию будут назначаться все инциденты из группы.
- 3. Нажмите кнопку Создать.

6.3.3 Редактирование группы инцидентов

- 1. Начните процесс редактирования группы инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

6.3.4 Назначение группы инцидентов пользователю

- 1. Откройте форму просмотра группы инцидентов и нажмите кнопку Q. Откроется окно "Назначение группы инцидентов".
- 2. В открывшемся окне из выпадающего списка выберите пользователя, которому необходимо назначить группу и нажмите кнопку **Применить**.

6.3.5 Назначение группы инцидентов группе пользователей

- 1. Откройте форму просмотра группы инцидентов и нажмите кнопку 🔍. Откроется окно "Назначение группы инцидентов".
- 2. В открывшемся окне из выпадающего списка выберите группу пользователей, которому необходимо назначить группу и нажмите кнопку **Применить**.

6.3.6 Добавление инцидентов в группу

Добавление инцидентов в группу может быть выполнено следующими способами:

- автоматически, по результатам "сработки" правил корреляции;
- вручную с формы создания/редактирования инцидента (см. раздел «Создание инцидента»).

6.3.7 Массовое закрытие инцидентов через группу

- 1. Откройте форму просмотра группы инцидентов.
- 2. В блоке Инциденты отметьте необходимые инциденты установив соответствующие флаги.
- 3. Нажмите кнопку **Закрыть инциденты** и подтвердите действие в открывшемся окне. Выбранные инциденты будут переведены в статус "Закрыт".

6.3.8 Открепление инцидентов от группы

1. Откройте форму просмотра группы инцидентов.

- 2. В блоке Инциденты отметьте необходимые инциденты установив соответствующие флаги.
- 3. Нажмите кнопку **Открепить связанные инциденты** и подтвердите действие в открывшемся окне. Выбранные инциденты больше не будут входить в данную группу.

6.3.9 Удаление группы инцидентов

- 1. Начните процесс удаления группы инцидентов через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Группа инцидентов будет удалена из платформы.

6.4 Происшествия на отправку

Внимание! Включение процесса отправки происшествий выполняется в старом интерфейсе. Начиная с версии 4.0.0 старый интерфейс более недоступен, а данная возможность находится на доработке. Вы можете выполнить данную операцию с инстанса, на котором установлена более ранняя версия.

6.5 Дополнительные поля

Платформа позволяет добавлять к инцидентам дополнительные поля, которые можно использовать для более полного описания инцидента.

Дополнительные поля могут быть созданы одним из следующих способов:

- вручную, через интерфейс платформы;
- автоматически, с использованием правила корреляции.

Работа с дополнительными полями включает в себя следующие процессы:

- 1. Создание дополнительного поля.
- 2. Редактирование информации о дополнительном поле.
- 3. Добавление дополнительного поля к инциденту.
- 4. Просмотр информации о дополнительном поле.
- 5. Удаление дополнительного поля.

Для работы с дополнительными полями перейдите в раздел **Инциденты** → **Дополнительные поля** (см. «Рис. 72»).

≡	ПАНГЕО РАДАР	172.30.254.138 ∨ Дополнител	ьные поля				 База знаний 	🔕 admin ~	/	
â	Допо	олнительные поля								
Q										
(1)	7	Создать Удалить Удалить все						C	3	
		Название	Ключ	Тип	Сортировка	Обновлено	Создано			
Ç.		Сырое событие	raw_event	JSON	1	17:25:16 10.09.2024	17:25:16 10.09.2024	© ∥ İİ		
ð		string	string	Строка	2	10:15:12 11.09.2024	10:15:12 11.09.2024	◎ ⁄ ⊡		
<i>%</i>		bool	bool	Логический	3	10:15:37 11.09.2024	10:15:37 11.09.2024	© ∥ 🗓		
ж		int	int	Целое число	0	10:16:04 11.09.2024	10:16:04 11.09.2024	© 🖉 🗓		
4 1 1	<	1 > 10 / страница ~								
Ø										

Рис. 72 – Раздел "Дополнительные поля"

В разделе отображается следующая информация:

- Название дополнительного поля. По ссылке произойдет переход на страницу просмотра дополнительного поля;
- Ключ уникальный ключ, идентифицирующий поле;
- Тип тип данных, указываемый в дополнительном поле:
 - логический;
 - JSON;
 - строка;
 - целое число;
 - действительное число;
 - дата.
- Сортировка порядок отображения дополнительных полей в карточке инцидента;
- Обновлено дата и время изменения информации о дополнительном поле;
- Создано дата и время создания дополнительного поля.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
Ø	редактирование информации о дополнительном поле
\odot	просмотр дополнительного поля
Ē	удаление записи из таблицы

6.5.1 Создание дополнительного поля

1. Нажмите на кнопку **Создать**. Откроется форма "Создание дополнительного поля" (см. «Рис. 73»).

 Создание дополнительного поля 	Очистить	Сохранить
Название		
Сырое событие		
Ключ		
raw_event		
Тип		
JSON		~
Сортировка		
1		- +
Тип JSON Сортировка 1		- +

Рис. 73 – Форма "Создание дополнительного поля"

- 2. Укажите на форме следующую информацию:
 - в поле **Название** укажите название дополнительного поля. Допускается указывать любое название поля на русском или английском языке;
 - в поле **Ключ** укажите уникальный ключ поля. Допускается указывать ключ только на английском языке. Указанный ключ должен быть уникальным в рамках платформы;
 - в поле **Тип** из выпадающего списка выберите тип данных, который будет указываться в поле;
 - в поле **Сортировка** выберите порядок отображения дополнительного поля в карточке инцидента.
- 3. Нажмите кнопку Сохранить.

6.5.2 Редактирование дополнительного поля

- 1. Выберите из списка необходимое дополнительное поле и нажмите кнопку 🖉.
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

6.5.3 Добавление дополнительного поля в инцидент

- 1. Перейдите в раздел **Инциденты** → **Инциденты**, выберите инцидент из списка и откройте его на просмотр.
- 2. Нажмите кнопку Редактировать. В блоке Дополнительные поля будет отображаться список доступных дополнительных полей.
- 3. Выберите дополнительное поле для добавления в инцидент и укажите в нем необходимую информацию.
- 4. Сохраните внесенные изменения.

6.5.4 Просмотр значений дополнительного поля

Открыть на просмотр дополнительное поле можно двумя способами:

- по ссылке по названию поля;
- по кнопке 🔘.

Откроется страница "Дополнительное поле <Наименование поля>" (см. «Рис. 74»).

← Дополнительное поле "Сырое событие"								
Значения дополнительного поля			C 🚳					
Инцидент	Значение	Дополнительное поле						
MS-WIN - непривилегированный доступ к общему сетевому ресурсу SMB	{ "Bookmark": " <bookmarklist>\r\n <bookmark <="" channel="Security" td=""><td>Сырое событие</td><td>回</td></bookmark></bookmarklist>	Сырое событие	回					
WEB - Обнаружена Log4ј инъекция	{ "Bookmark": " <bookmarklist>\r\n <bookmark <="" channel="Security" td=""><td>Сырое событие</td><td>包</td></bookmark></bookmarklist>	Сырое событие	包					
Множественные неудачные попытки входа на одном узле под разными учетными	{ "Bookmark": " <bookmarklist>\r\n <bookmark <="" channel="Security" td=""><td>Сырое событие</td><td>包</td></bookmark></bookmarklist>	Сырое событие	包					
Множественные неудачные попытки входа на различных хостах под различными	{ "Bookmark": " <bookmarklist>\r\n <bookmark <="" channel="Security" td=""><td>Сырое событие</td><td>包</td></bookmark></bookmarklist>	Сырое событие	包					
< 1 > 10 / страница ~								

Рис. 74 – Страница просмотра дополнительного поля"

На странице отображается следующая информация:

- Инцидент наименование инцидента, в котором добавлено дополнительное поле. По ссылке произойдет переход на форму просмотра инцидента;
- Значение информация, указанная в дополнительном поле;
- Наименование дополнительного поля.

При необходимости вы можете удалить значение дополнительного поля из выбранного инцидента. Для этого нажмите кнопку 🔟 в соответствующей строке.

6.5.5 Удаление дополнительного поля

Для удаления дополнительного поля нажмите кнопку 🔟 в соответствующей строке.

Для удаление всех записей нажмите кнопку **Удалить все**.

Для удаления конкретных записей таблицы установите нужные флаги и нажмите кнопку Удалить.

7. Активы

7.1 Активы

7.1.1 Общие данные

Актив: любое техническое средство информационной системы (устройство, подключенное к вычислительной сети, в том числе: сервер, рабочая станция, коммутационное устройство и т.п.), имеющее ценность для предприятия и подлежащее защите от киберугроз.

При отправке и получении данных активы генерируют траффик, который обрабатывается в платформе и на его основе в событиях информационной безопасности регистрируется информация о том, откуда исходит трафик и куда он направляется, например исходные и целевые IP-адреса, FQDN и прочая информация.

Тип сетевой видимости актива может принимать следующие значения:

- 1 актив напрямую подключен к сети Интернет;
- 2 актив располагается в демилитаризованной зоне (DMZ);
- 3 актив подключен к сети Интернет через Proxy-сервер;
- 4 актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайнсервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы;
- 5 актив не подключен к сети.

Сведения об активах в платформу могут быть добавлены следующими способами:

- при обнаружении/создании инцидента;
- по результатам работы сканера уязвимостей;
- по результатам работы сетевого сканера;
- добавлены вручную.

В случае, если у активов используются не статичные IP-адреса, то можно выполнить дополнительную настройку стратегии идентификации активов (подробнее см. раздел «<u>Настройки</u> идентификации активов»)

Уровень влияния актива на выполнение бизнес-процессов компании называется **Значимость**. В платформе значимость актива может принимать следующие значения:

- 1 ключевой. Данный актив обеспечивает функционирование бизнеса;
- 2 важный. Данный актив обеспечивает штатную работу компании;
- 3 некритичный. Данный актив не влияет на штатную работу компании;
- 4 распределенный. Данный актив находится в составе распределенной системы, которая не задействована в бизнес-процессах;
- 5 тестовый. Данный актив располагается в тестовой среде. Недоступность данного актива не влияет ни на бизнес-процессы, ни на штатную работу компании.

Активы можно объединить в группы, а затем их назначить ответственным. Это упрощает расследование связанных с активом инцидентов и позволяет выполнять проверку соответствия ПО для группы активов (подробнее см. раздел «<u>Группы активов</u>»).

Для подключения к сети и обмена данным используются сетевые интерфейсы, информация о которых и связанными с ними активами также содержится в платформе (подробнее см. раздел «<u>Сетевые интерфейсы</u>»).

Работа с активами включает в себя следующие процессы:

- 1. «<u>Просмотр и анализ актива</u>».
- 2. «<u>Создание актива</u>».
- 3. «<u>Редактирование актива</u>».
- 4. «Добавление актива в группу».
- 5. «<u>Написать ответственному</u>».
- 6. «<u>Удаление актива</u>».

Для работы с активами перейдите в раздел Активы → Активы (см. «Рис. 75»).

≡	<mark>радар</mark> радар	9 172.30.254.	97 ~ A	ктивы					Лицензия акти	вна до: 20	027-11-16	 Документация 	(admin	~
۵	Акт	гивы													
Q															
()	7	Создать	Удалить У	далить все	Экспортировать вы	бранные в сву Экспортиров	зать в сзу Объединить	Активация/деактивация	Установить зна	чение		Выбран	ю: 0	C	
cn.		Уров 🕼	Тип	1 Назван	иe Uî	Сетевые интерфейсы	Операционная	Группы активов	Распо 🕼	Обновл	ено 🎵	Создано	11		
D		0.82	Host	172.30	.254.107	172.30.254.107	Microsoft Windows 10 1709 - 1909	test	Москва	2025-04	4-28 16:36:40	2025-03-06 16:29	:31	◎ ⁄ ī	
*		0.29	Node	v-stand	I-07.pgr.local	ens18	-	test	-	2025-02	2-20 16:41:39	2025-02-20 16:41	:39	◎ ⁄ i	
ж	<	1 >	50 / страниц	la ∼											
496															
۵															

Рис. 75 – Раздел "Активы"

В разделе отображается следующая информация:

- Уровень риска цветовое и цифровое обозначение уровня риска актива;
- Тип типа актива: Host, Node;
- Название наименование актива;
- Сетевые интерфейсы наименование сетевого интерфейса актива;
- Операционная система наименование операционной системы, установленной на активе;
- Группы активов наименование групп активов, в которых состоит актив;
- Расположение геоданные актива;
- Открытые инциденты количество открытых инцидентов на активе
- **Риск принят** признак, принят ли потенциальный риск дальнейшей эксплуатации актива в текущем состоянии: да, нет;
- Закрытые инциденты количество закрытых инцидентов на активе;

- Обновлено дата и время изменения информации об активе;
- Создано дата и время создания записи об активе в платформе;
- Значимость актива уровень влияния актива на выполнение бизнес-процессов компании;
- Сетевая видимость тип сетевой видимости актива;
- **Группа ответственных** наименование группы пользователей, которым автоматически назначаются инциденты, выявленные на активе;
- **IP/MAC** IP и MAC-адрес актива.

7.1.2 Просмотр и анализ актива

Для просмотра актива нажмите кнопку В нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного актива (см. «Рис. 76»).

≡	Кангео 172.30.249.21 ∨ Просмо	отр актива							Лицензия активна до:	2025-08-16 🕕 База зн	каний Q admin ~			
â	8 7 Ø C +	← 10.14	14.98.106					Реда	ктировать 🗋 Добавить	в группу 🦪 Написать с	тветственному			
Q	10.200.68.90 Нозт © Основное							Сетевые интерфейсы						
	Штатный доступ в Интернет через Proxy	IP 10.144.98.106					Названи	ie	IP		MAC			
4 0	Ключевой Активный	FQDN	-				10.144	98.106	10.144.9	8.106				
đ	10.144.98.114	MAC	-						10.144.0	0.100				
×	Host ①	- OC												
0.0	Штатный доступ в интернет через Proxy	Группа ак	тива -				Програ	ммное обе	спечение					
н	Ключевой Активный	Тип актив	a Host				Microsoft	Office, версия	- 2007 SP3					
41	10.144.98.106	Располож	сение -				Kaspersky	Security Cente	ег, версия - 10.5.1781					
	Host ③	Ответств	енный -				Google Chrome, версия - 49.0.2623.112							
(i)	Proxy	Дата посл	еднего Не произведено				Показать больше 🗸							
	Ключевой Активный	Активен	Ла											
	10.200.4.17		-				Аппаратное обеспечение							
	Host ③ ③ zzz						network/dagter , deviceld: eng0/s18, name: 8254/0EW Glgabit Ethernet Controller (OEMU Virtual Machine), manufacturer: Intel Corporation, macAddress: 86:98:18:70:dc:be, ipv4: null, ipv6: null memory , capacity: 34350738388 processor , name: Common KVM processor, manufacturer: GenuineIntel, caption: , numberOfCores: , addressWidth:							
	Ключевой Активный													
	10.200.52.219													
	Host ③													
	Proxy													
	Ключевой Активный	Инцидент	ы											
											C			
		Срочность	Название	Статус	Актив	Создано		Уровень	Тип инцидента	Группа инцидентов	Обновлено			
		0.77	Множественные неудачные попытки	Назначен	stand-x.pgr.local	14:55:15 0	3.09.2024	8	Множественные	Группа "Множественные	12:10:09 12:09:2024			
		0.64	WEB - Обнаружена Log4j инъекция	В работе	stand-x.pgr.local	17:16:24 0	9.09.2024	7	WEB - Обнаружена Log4j	Группа "Ложные	09:52:40 11.09.2024			
		< 1	> 10 / страница ~											

Рис. 76 – Форма просмотра актива

В боковой панели отображается следующая информация об активах:

- Наименование актива;
- Тип актива;
- Расположение актива;
- Сетевая видимость актива;
- Значимость актива;
- Состояние актива.

В рабочей области отображается следующая информация об активах:

• В блоке Основное отображается основная информация об активе:

- IP;
- FQDN;
- MAC;
- OC;
- Группа актива;
- Тип актива;
- Расположение;
- Ответственный;
- Дата последнего сканирования;
- Состояние актива;
- В блоке **Сетевые интерфейсы** отображается информация о сетевых интерфейсах, входящих в актив:
 - Название;
 - IP;
 - MAC.
- В блоке **Программное обеспечение** отображается информация о списке ПО, установленном на активе;
- В блоке Аппаратное обеспечение отображается список аппаратного обеспечения актива;
- В блоке **Инциденты** отображается информация об инцидентах, выявленных на активе (подробнее см. раздел «<u>Инциденты</u>»).

7.1.3 Создание актива

1. Начните процесс создания актива через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание актива" (см. «Рис. 77»).

Создание актива	
Общее Название *	
Тестовый актив	
Активный	
Тип	
Тонкий клиент	
Значимость актива	
Некритичный	~
Сетевая видимость	
Штатный доступ в Интернет через Proxy	~
Группа ответственных ()	
users	~
Описание	
Тестовый актив для проверки работы сканера уязвимостей	1.
Расположение *	
г. Москва	
Ответственное лицо	
Сидоров	
Технический специалист	
Смирнов	
Сетевой интерфейс Выберите сетевой интерфейс	
127.0.0.253 127.0.0.253 ×	~
+ Создать новый	Создать

Рис. 77 – Форма "Создание актива"

- 2. Выполните на форме следующие действия:
 - в поле Название укажите наименование актива;
 - установите флаг Активный, если данный актив задействован в корпоративной сети;
 - в поле Тип укажите тип актива;
 - в поле Значимость актива из выпадающего списка выберите значимость актива;
 - в поле **Сетевая видимость** из выпадающего списка выберите сетевую видимость актива;
 - в поле **Группа ответственных** выберите группу пользователей, которой будут автоматически назначаться инциденты, выявленные на активе;
 - в поле Описание укажите описание актива;
 - в поле Расположение укажите расположение актива;
 - в поле Ответственное лицо укажите информацию о владельце актива;

- в поле Технический специалист укажите соответствующую информацию;
- в поле Сетевой интерфейс из выпадающего списка выберите сетевые интерфейсы, которые входят в состав актива. Если необходимого сетевого интерфейса нет в списке, то вы можете создать его вручную. Для этого нажмите кнопку Создать новый и укажите необходимую информацию (подробнее см. раздел «Сетевые интерфейсы»);
- 3. Нажмите кнопку Создать.

7.1.4 Редактирование актива

- 1. Начните процесс редактирования актива через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

7.1.5 Добавление актива в группу

- 1. Откройте форму просмотра актива и нажмите кнопку Добавить в группу.
- 2. В открывшемся окне из выпадающего списка выберите группу активов (подробнее см. раздел «<u>Группы активов</u>»), в которую необходимо добавить актив.
- 3. Нажмите кнопку Сохранить.

7.1.6 Написать ответственному

1. Откройте форму просмотра актива и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 78»).

×
~
Отправить

Рис. 78 – Окно "Новое сообщение"

2. Укажите в окне следующую информацию:

- в поле Получатель из выпадающего списка выберите получателя сообщения;
- в поле Заголовок укажите тему сообщения;
- в поле Сообщение укажите текст сообщения.
- 3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя** → **Сообщения**.
- 4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку актива.

7.1.7 Удаление актива

- 1. Начните процесс удаления актива через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Актив будет удален из платформы.

7.2 Группы активов

Для упрощения управления активами их можно поместить в группы.

Работа с группами активов включает в себя следующие процессы:

- 1. «<u>Создание группы активов</u>».
- 2. «<u>Просмотр группы активов</u>».
- 3. «<u>Редактирование группы активов</u>».
- 4. «Настройка автоматического добавления актива в группу».
- 5. «<u>Написать ответственному</u>».
- 6. «<u>Удаление группы активов</u>».

Для работы с группами активов перейдите в раздел **Активы → Группы активов** (см. «Рис. 79»).

≡	К панге Радар	° 172.30.254.138 ∨ Груг	пы активов						🛈 База знаний 🌘	g) admin v
â	Гру	ппы активов								
Q										
0	7	Создать Удалить Удалить	BCE							С 🎯
		Название	Регулярное выражение	Кол-во	Группа ответственных	Создано	Обновлено	кии	Маски подсетей	
CE I		кки		0	admin	14:04:15 11.09.2024	14:04:15 11.09.2024	Да		5
đ		Ключевые активы		0	admin	10:10:18 24.09.2024	10:10:18 24.09.2024	Нет		a
<i>%</i>		Проверка выражениия	(?=^.{4,253}\$)(^((?!-)[a-zA-ZO-9-]{1,63}(? -)_)+[a-z</th <th>0</th> <th>admin</th> <th>10:22:49 24.09.2024</th> <th>10:22:49 24.09.2024</th> <th>Нет</th> <th></th> <th>5</th>	0	admin	10:22:49 24.09.2024	10:22:49 24.09.2024	Нет		5
ж		Fully Qualified Domein Names	$(?!: \/\/) (?=.\{1,255\} \$) ((.\{1,63\} \.) \{1,127\} (?![0-9] * \$) [a-z$	0	admin	10:24:28 24.09.2024	10:24:28 24.09.2024	Нет		្រ
+t†		1 > 10 / страница ~								
٢										

Рис. 79 – Раздел "Группы активов"

В разделе отображается следующая информация о группах активов:

 Название – наименование группы активов. По ссылке произойдет переход на форму просмотра группы активов;

- **Регулярное выражение** стратегия автоматического добавления активов в группу по заданному регулярному выражению, применяемому к FQDN активов. Новые активы, чье FQDN отвечает заданному регулярному выражению, будут автоматически включаться в группу;
- Кол-во количество активов в группе;
- **Группа ответственных** группа пользователей, назначенная ответственными за данную группу активов;
- Создано дата и время создания группы активов;
- Обновлено дата и время последнего обновления группы активов;
- **Связанные группы пользователей** группы пользователей, связанные с конкретными активами из данной группы;
- КИИ признак того, относится ля группа активов к критической информационной инфраструктуре;
- **Маска подсетей** стратегия автоматического добавления активов в группу по заданной маске подсети. Новые активы, попадающие под указанную сетевую маску, будут автоматически включаться в группу.
- Кнопка **Запуск проверки соответствия ПО** (подробнее см. раздел «<u>Результаты</u> <u>соответствия ПО</u>»).

7.2.1 Создание группы активов

1. Нажмите кнопку **Создать**. Откроется форма "Создание группы активов" (см. «Рис. 80»).

← Создание группы актива	Сбросить Создат
Название	
Распределенные активы	
пастроики автоматического дооавления активов в группу 🕔 Маски подсетей в CIDR-нотации (например 192.168.0.0/24)	
+ Создать	
Регулярное выражение для FQDN	
Regex	
Справка по регулярным выражениям	
Группы пользователей	
Группа ответственных ()	
users	
Связанные группы пользователей	
admin \times inventorization \times	
D объекта	
534	
D субъекта	
45	
D системы	
55	
КИИ	
Этветственное лицо	
Смирнов	
Технический специалист	
Афанасьев	
Ассоциации	
Актив	
localhost ×	
Набор правил	
Выбрать	

Рис. 80 – Форма "Создание группы активов"

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите наименование группы активов;
 - в блоке Настройки автоматического добавления активов в группу настройте стратегию автоматического добавления активов в группу (см. раздел «<u>Настройка</u> автоматического добавления актива в группу»);
 - в блоке Группы пользователей укажите следующую информацию:
 - в поле **Группа ответственных** выберите группу, которой автоматически будут назначаться инциденты, выявленные на активах, входящих в данную группу активов;

- в поле **Связанные группы пользователей** укажите связанные группы пользователей;
- в случае, если группа активов относится к критической информационной инфраструктуре, то в полях ID объекта, ID субъекта, ID системы укажите соответствующие идентификаторы, которые указаны в протоколе интеграции с системой "ГосСОПКА", и установите флаг КИИ;
- в полях **Ответственное лицо** и **Технический специалист** укажите соответствующую информацию.
- в блоке Ассоциации укажите следующую информацию:
 - в поле **Актив** выберите активы, которые следует включить в группу, если необходимые активы уже добавлены в платформу;
 - в поле **Набор правил** выберите правила, по которым активы должны проверяться на соответствие ПО (см. раздел «<u>Создание правила соответствия</u> <u>ПО</u>»).
- 3. Нажмите кнопку Создать.

7.2.2 Просмотр группы активов

Для просмотра и анализа группы активов нажмите по ссылке с наименованием инцидента. Откроется форма просмотра группы активов (см. «Рис. 81»).

← Fully Qualif	ied Domain Names		Редактировать	Написать ответственному	
Основное					
Название	Fully Qualified Domain Nan	nes			
Маска подсети -					
Группа ответственны	Группа ответственных admin				
(тивы инциденты				C \$	
Уровень риска	Название	Обновлено	Создано		
0.77	localhost	14:55:13 03.09.2024	14:55:13 0	3.09.2024	
0.77	stand-x.pgr.local	14:55:15 03.09.2024	14:55:15 0	3.09.2024	

Рис. 81 – Форма просмотра группы активов

На форме просмотра группы отображается следующая информация:

- Основная информация группе: название, маска подсети, группа ответственных;
- Информация об активах, входящих в группу: уровень риска, название актива, дата и время обновления и создания актива;
- Информация об инцидентах, выявленных на активах (см. «Рис. 82»).

← Fully	Qualified Domain N	lames					Редактировать Написать от	гветственному
Основно	e							
Название	Fully Qualit	fied Domain Na	mes					
Маска поде	сети -							
Группа отв	етственных admin							
Активы И	нциденты							C
Срочность	Название	Статус	Актив	Создано	Уровень	Группа инцидентов	Тип инцидента	Обновлено
0.00	AuditD - Остановлен демо	Закрыт	localhost	16:32:09 12.09.2024	3	-	AuditD - Остановлен демон	11:08:01 13.09.2024
0.64	WEB - Обнаружена Log4j	В работе	stand-x.pgr.local	17:16:24 09.09.2024	7	Группа "Ложные срабатывания"	WEB - Обнаружена Log4j	09:52:40 11.09.2024
0.00	Множественные неудачны	Новый	localhost	15:46:51 09.09.2024	9	-	Множественные неудачные	09:53:12 11.09.2024
0.07	Множественные неудачны	В работе	localhost	14:28:52 05.09.2024	0.5	Группа "Множественные	Множественные неудачные	12:21:18 12.09.2024
0.00	MS-WIN	Новый	localhost	17:17:01 09.09.2024	0	Группа "Ложные срабатывания"	MS-WIN - непривилегированный	09:51:26 11.09.2024
0.07	MS-WIN - Для учетной	В работе	localhost	14:37:16 05.09.2024	0.5	-	MS-WIN - Для учетной записи	10:56:31 09.09.2024
0.77	Множественные неудачны	Назначен	stand-x.pgr.local	14:55:15 03.09.2024	8	Группа "Множественные	Множественные неудачные	12:10:09 12.09.2024
< 1	> 10 / страница <							

Рис. 82 – Форма просмотра группы активов. Таблица инциденты

7.2.3 Редактирование группы активов

- 1. Перейдите на форму просмотра необходимой группы активов и нажмите кнопку **Редактировать**.
- 2. Внесите необходимые изменения.
- 3. Сохраните изменения.

7.2.4 Настройка автоматического добавления актива в группу

Настройка стратегии автоматического добавления актива в группу выполняется на форме создания/редактирования группы активов в блоке **Настройки автоматического добавления активов в группу** (см. «Рис. 83»).





Стратегию можно настроить двумя способами:

- по маске подсети;
- по регулярному выражению для FQDN.

Выполните следующие действия:

- 1. В поле Маски подсетей в CIDR-нотации укажите маску подсети.
- 2. Используйте кнопки "+" и "-" для добавления/удаления масок подсетей.
- 3. В поле **Регулярное выражение для FQDN** укажите регулярное выражение.

7.2.5 Написать ответственному

1. Перейдите на форму просмотра группы активов и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 84»).

Новое сообщение	×
Получатель	
Выберите получателя	~
Заголовок	
Ввести	
Сообщение	
Выберите получателя	
	ĥ
	Отправить

Рис. 84 – Окно "Новое сообщение"

- 2. Укажите в окне следующую информацию:
 - в поле Получатель из выпадающего списка выберите получателя сообщения;
 - в поле Заголовок укажите тему сообщения;
 - в поле Сообщение укажите текст сообщения.
- 3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя** → **Сообщения**.
- 4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку группы активов.

7.2.6 Удаление группы активов

Удаление группы активов можно выполнить следующими способами:

- из раздела **Активы** → **Группы активов**;
- из формы просмотра группы активов.

Способ 1:

- 1. Перейдите в раздел Активы Группы активов.
- 2. Отметьте необходимые группы активов.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.
- 5. Для удаление всех групп активов нажмите кнопку Удалите все.

Способ 2:

- 1. Перейдите на форму просмотра группы активов, нажмите кнопку и из выпадающего списка выберите пункт **Удалить**.
- 2. Подтвердите удаление в открывшемся окне.

7.3 Настройки идентификации активов

Идентификация активов — это сравнение отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в платформе. По итогам сравнения либо создается запись о новом активе, либо обновляются записи о существующих активах.

Стратегию сравнения можно настроить по следующим идентификаторам:

- **FQDN** по полному доменному имени актива;
- МАС по Мас-адресу актива;
- **IP** по IP-адресу актива.

Работа со стратегиями идентификации активов включает в себя следующие процессы:

- 1. «Создание стратегии идентификации активов».
- 2. «Редактирование стратегии идентификации активов».
- 3. «Удаление стратегии идентификации активов».

Для работы со стратегиями идентификации активов перейдите в раздел **Активы** → **Настройки идентификации активов** (см. «Рис. 85»).

≡	Пангео 172.30.254.138 ∨ Настройки	и идентификации активов			① База знаний	I	\bigotimes admin \lor
ଜ	Настройки идентификаци	1 активов					
Q							
<u>(</u>)	Создать Удалить Удалить все						C Ø
-0	Имя	Диапазоны	Стратегия	Обновлено	Создано		
Ç0	strategy_1	192.168.0.0/24,192.168.1.0/24	IP	16:12:01 24.09.2024	16:12:01 24.09.2024	Ø	Ū
ð	strategy_2	192.168.0.0/24	FQDN	16:12:32 24.09.2024	16:12:32 24.09.2024	Ø	Ū
H:	< 1 > 10 / страница ~						
ж							
494							
Ø							

Рис. 85 – Раздел "Настройки идентификации активов"

В разделе отображается следующая информация о стратегиях идентификации активов:

- Имя наименование стратегии идентификации активов;
- Диапазоны диапазоны масок подсетей в CIDR-нотации;
- **Стратегия** идентификатор актива, по которому выполняется сравнение активов: FQDN, MAC, IP;
- Обновлено дата и время обновление стратегии;
- Создано дата и время создания стратегии.

7.3.1 Создание стратегии идентификации активов

1. Нажмите кнопку **Создать**. Откроется форма "Создание настройки идентификации активов" (см. «Рис. 86»).

 Создание настройки идентификации активов 	Очистить	Сохранить
Имя *		
strategy_3		
Диапазоны () 192.168.0.0/24 × +		
Стратегия *		
IP		~

Рис. 86 – Окно "Создание настройки идентификации активов"

- 2. Укажите на форме следующую информацию:
 - в поле Имя укажите уникальное наименование стратегии;
 - в поле **Диапазон** укажите диапазоны масок подсетей в CIDR-нотации;
 - в поле **Стратегия** из выпадающего списка выберите идентификатор, по которому будет выполняться сравнение атрибутов активов.
- 3. Нажмите кнопку Сохранить.

7.3.2 Редактирование стратегии идентификации активов

- 1. Выберите стратегию и нажмите кнопку 🖉.
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

7.3.3 Удаление стратегии идентификации активов

Удаление стратегии идентификации активов выполняется из раздела **Активы** – **Настройки** идентификации активов.

Для удаления стратегии, выберите необходимую запись в таблице и нажмите кнопку 🔟

Для удаления нескольких стратегий установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех записей таблицы нажмите кнопку Удалить все.

7.4 Сетевые интерфейсы

Платформа Радар собирает и хранит сведения о сетевых интерфейсах, обнаруженных у активов.

Работа с сетевыми интерфейсами автоматизирована и вносить изменения вручную может потребоваться в следующих случаях:

• если от сканера уязвимостей поступили неточные данные о сетевых интерфейсах;

• изменилась сетевая конфигурация в ходе эксплуатации актива. Если заранее известно в каком сетевом диапазоне динамичные адреса, то для диапазона можно настроить стратегию идентификации активов (см. «<u>Настройки идентификации активов</u>»).

Работа с сетевыми интерфейсами включает в себя следующие процессы:

- 1. «<u>Просмотр сетевого интерфейса</u>».
- 2. «Создание сетевого интерфейса».
- 3. «<u>Редактирование сетевого интерфейса</u>».
- 4. «Удаление сетевого интерфейса».

Для работы с сетевыми интерфейсами перейдите в раздел **Активы** → **Сетевые интерфейсы** (см. «Рис. 87»).

РАДАР	^{во} 172.30.254.97 ∨ Сетевые инт	ерфейсы			Лицензия акти	вна до: 2027-11-16 🕚 Докуми	ентация	8	admin 🗸	
Ce	тевые интерфейсы									
Филь	ьтры +									
Сорт	тировка ↓ Создано × +									
Сбр	росить Применить									
8	Создать Удалить Удалить все	Экспортировать выбранные в	ссу Экспортировать в ссу				Выбрано: 0	C	۲	
	Название	МАС-адрес	ПР-адрес U1	FQDN	Операционная	Актив 🗸 🕽	Обновлено			
	172.30.254.107	E6:C0:7E:AE:41:84	172.30.254.107	-	Microsoft Windows 10	172.30.254.107	2025-04-28	0	0 🗇	
	172.30.254.224	D2:96:C3:9F:9B:90	172.30.254.224	-	Microsoft Windows 10	172.30.254.224	2025-04-28	0	0 🗊	
	172.30.254.224 v-stand-03.pgr.local	D2:96:C3:9F:9B:90 26:0F:D1:76:A0:F9	172.30.254.224 172.30.254.93	- v-stand-03.pgr.local	Microsoft Windows 10 Oracle VM Server 3.4.2	172.30.254.224 v-stand-03.pgr.local	2025-04-28	0	0 10 0 10	
	172.30.254.224 v-stand-03.pgr.local v-stand-04.pgr.local	D2:96:C3:9F:9B:90 26:0F:D1:76:A0:F9 7A:D3:82:5A:50:E3	172.30.254.224 172.30.254.93 172.30.254.94	- v-stand-03.pgr.local v-stand-04.pgr.local	Microsoft Windows 10 Oracle VM Server 3.4.2	172.30.254.224 v-stand-03.pgr.local v-stand-04.pgr.local	2025-04-28 2025-04-28 2025-03-04	0		
	172.30.254.224 v-stand-03.pgr.local v-stand-04.pgr.local 172.30.254.1	D2:96:C3:9F:9B:90 26:0F:D1:76:A0:F9 7A:D3:82:5A:50:E3 52:FF:20:98:4D:50	172.30.254.224 172.30.254.93 172.30.254.94 172.30.254.94	- v-stand-03.pgr.local v-stand-04.pgr.local	Microsoft Windows 10 Oracle VM Server 3.4.2 - Linux 3.2 - 4.9	172.30.254.224 v-stand-03.pgr.local v-stand-04.pgr.local 172.30.254.1	2025-04-28 2025-04-28 2025-03-04 2025-04-28	© © ©		

Рис. 87 – Раздел "Сетевые интерфейсы"

В разделе отображается следующая информация:

- Название наименование сетевого интерфейса;
- МАС-адрес МАС-адрес сетевого интерфейса;
- **IP-адрес** IP-адрес сетевого интерфейса;
- **FQDN** FQDN актива, на котором установлен сетевой интерфейс;
- Операционная система наименование операционной системы, на которой работает актив;
- Актив наименование актива, на котором установлен сетевой интерфейс;
- Обновлено дата и время обновления информации о сетевом интерфейсе;
- Создано дата и время создания записи о сетевом интерфейсе в платформе.

7.4.1 Просмотр сетевого интерфейса

Для просмотра сетевого интерфейса нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного сетевого интерфейса (см. «Рис. 88»).

≡	Кангео 172.30.254.138 ∨ Проседание	осмотр сетевого инте	ерфейса	🛈 База знаний 🔘 admin 🗸
â	8 7 Ø C +	← 172.30.24	9.123	🖉 Редактировать 📃
Q (i)	172.30.249.109 IP: 172.30.249.1 MAC: 78:9a:18:b3:89:0b OC:	Общее		
Ç.	172.30.249.15	Название	172.30.249.123	
ð	IP: 172.30.249.15	МАС-адрес	86:98:18:7d:dc:be	
	MAC: de:dc:f4:5b:e3:e4 OC:	IP-адрес	172.30.249.123	
* <i>1</i> ?+	172.30.249.123	FQDN	-	
Ж	IP: 172.30.249.123 MAC: 86:98:18:7d:dc:be	Операционная система	Linux 2.6.32	
494	OC: Linux 2.6.32	Актив	172.30.249.123	
~	172.30.249.71			
\$	IP: 172.30.249.71			
	HINGS BUILER FLUUR 2-00			

Рис. 88 – Форма просмотра сетевого интерфейса

В боковой панели отображается следующая информация:

- Наименование сетевого интерфейса;
- ІР-адрес сетевого интерфейса;
- МАС-адрес сетевого интерфейса;
- Наименование операционной системы.

На форме просмотра отображается следующая информация:

- Название;
- MAC-адрес;
- IP-адрес;
- FQDN;
- Операционная система;
- Актив.

7.4.2 Создание сетевого интерфейса

1. Начните процесс создания сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание сетевого интерфейса" (см. «Рис. 89»).

← Создание сетевого интерфейса	Сбросить	Создать
Название *		
test		
MAC-adpec *		
de:dc:f4:5b:e3:e4		
IP-адрес *		
172.30.249.15		
FQDN * stand-x.pgr.local × +		
Операционная система		
Windows		
Активы		
172.30.249.15		\sim

Рис. 89 – Создание сетевого интерфейса

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите наименование сетевого интерфейса;
 - в поле **МАС-адрес** укажите Мас-адрес сетевого интерфейса;
 - в поле **IP-адрес** укажите IP-адрес сетевого интерфейса;
 - в поле **FQDN** укажите полное доменное имя сетевого интерфейса;
 - в поле **Операционная система** укажите ОС актива, на котором обнаружен сетевой интерфейс;
 - в поле Активы из выпадающего списка выберите актив, на котором обнаружен сетевой интерфейс.
- 3. Нажмите кнопку Создать.

7.4.3 Редактирование сетевого интерфейса

- 1. Начните процесс редактирования сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

7.4.4 Удаление сетевого интерфейса

- 3. Начните процесс удаления сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».
- 4. Подтвердите удаление в открывшемся окне.
- 5. Сетевой интерфейс будет удален из платформы.

7.5 Результаты сканирования

Под результатами сканирования понимаются данные по наличию уязвимостей, полученные сторонними сканерами уязвимости в ходе работы и импортированные в платформу.

Платформа Радар поддерживает импорт данных сканирования от следующих систем:

- REDCHECK;
- MaxPatrol;
- Nessus;
- OpenVAS.

Работа с результатами сканирования включает в себя следующие процессы:

- 1. «Импорт результатов сканирования».
- 2. «Просмотр списка результатов сканирования».
- 3. «Просмотр результата сканирования».
- 4. «Сравнение результатов сканирования».
- 5. «Изменение статуса результата сканирования».

7.5.1 Импорт результатов сканирования

1. Перейдите в раздел **Активы** → **Результаты сканирования** и нажмите кнопку **Создать**. Откроется форма "Результаты сканирования" (см. «Рис. 90»).

← Результаты сканирования	яния	Лицензия активна до: 20	062-11-07 ① Документация	(Q) admi	1
Тип сканирования		Загрузка файла			
redcheck		Выбрать файл			
Загруженные файлы Архивные отчеты		Запустить сканирование пос	сле загрузки		
Загруженные файлы Архиеные отчеты		Запустить сканирование пос Запустить пос запустить сканирование пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите пос запустите	сле загрузки	C	1
Загруженные файлы Архивные отчеты	Тип отчета	Запустить сканирование по Создано	сле загрузки Обновлено	C	\$
Загруженные файлы Архивные отчеты Г Имя файла 2024-08 С	Тип отчета redcheck	 Запустить сканирование пос Создано 11:06:07 29.08.2024 	сле загрузки Обновлено 11:06:07 29.08.2024	C.	6
Загруженные файлы Архивные отчеты	Tun orvera redcheck redcheck	 Запустить сканирование пос Создано 11:06:07 29.08.2024 18:39:49 12.09.2024 	сле загрузки Сле загрузки Собновлено 11:06:07 29.08.2024 18:39:49 12.09.2024	ج ح ا	\$ 0
Загруженные файлы Архивные отчеты Мяя файла 2024-08 2024-09-12T18:39:49+03:00_scan-rep.xml 2024-09-13T14:55:41+03:00_scan-rep.xml	Tun orvera redcheck redcheck redcheck	 Запустить сканирование пос Создано 11:06:07 29.08.2024 18:39:49 12.09.2024 14:55:41 13.09.2024 	сле загрузки Сле загрузки Сбновлено 11:06:07 29:08:2024 18:39:49 12:09:2024 14:55:41 13:09:2024	ج ج ج	\$ 0 0

Рис. 90 – Форма импорта результатов сканирования

- 2. Выполните на форме следующие действия:
 - в поле Тип сканирования из выпадающего списка выберите тип сканирования;
 - в поле Загрузка файла нажмите на кнопку Выбрать файл и в открывшемся окне укажите путь к файлу;
 - если необходимо запустить сканирование после загрузки файла, то установите соответствующий флаг.

- 3. Информация о загруженных файлах будет отображена на вкладке "Загруженные файлы", информация об обработанных результатах сканирования отображается на вкладке "Архивные отчеты".
- 4. Для импорта загруженного результата сканирования нажмите кнопку 🕑 в соответствующей строке.
- 5. Для скачивания загруженного результата сканирования нажмите кнопку 🖄.

7.5.2 Просмотр списка результатов сканирования

Для просмотра списка результатов сканирования перейдите в раздел **Активы** → **Результаты сканирования** (см. «Рис. 91»).

≡	K PALS	₽º 172.30.254.147 ∨ Pe	зультаты ска	нирования								ицензия активна до: 20	25-08-16 🕕 База ан	nambe 🔘 Kinana	
۵	Pe	зультаты сканир	ования												
Q															
0	V	Создать Удалить Уда	алить все											Выбрано: 0 С	۲
		Название		Импорт завершен	Обработано	Количество хостов	Ошибки	Важность: Общая (Новая)	Тип сканирования	Сканирование ПО	Импортировано	Начало	Конец сканирования	Цели	
9		для интеграции пример	Сравнить	Да	Нет	51	-	10278 (10276) 50693 (50692) 26628 (26628) 0 42137 (42137)	maxpatrol	Да	14:46:41 13.09.2024	18:32:26 13.05.2021	16:31:22 13.05.2021	10.144.86.166,10.1	۲
8		Example Report Name	Сравнить	Да	Нет	1		0 604 (402) 309 (296) 0 635 (515)	redcheck	Нет	14:55:43 13:09.2024				۲
38		Example Report Name	Сравнить	Да	2024-09	0		0 0 0	redcheck	Нет	18:39:49 12:09:2024				۲
ж		1 > 10 / страница													
45															
0															

Рис. 91 – Раздел "Результаты сканирования"

В разделе отображается следующая информация о результатах сканирования:

- **Название** наименование импортированного результата сканирования. По нажатию на ссылку произойдет переход к форме просмотра результата сканирования;
- Импорт завершен состояние успешности завершения импорта результата сканирования: да, нет;
- Обработано состояние обработки результата сканирования;
- Количество хостов количество хостов, обнаруженных в результате сканирования;
- Ошибки наличие ошибок в результатах сканирования;
- **Важность** отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS;
- Тип сканирования наименование сканнера уязвимости, который предоставил результаты сканирования;
- **Сканирование ПО** флаг выполнения сканирования программного обеспечения в результатах сканирования: да, нет;
- Импортировано дата и время импорта результатов сканирования в платформу;
- Начало сканирования дата и время начала сканирования;
- Конец сканирования дата и время окончания сканирования;
- **Цели** активы (IP-адреса), указанные в задаче сканирования. По наведению мыши на поле, в pop-up окне будет выведен полный список целей сканирования.

В разделе доступны следующие элементы управления:

Кнопка	Действие
Сравнить	сравнение результатов сканирования с существующими данными
\bigcirc	отметить результат сканирования как обработанный или необработанный

7.5.3 Просмотр результата сканирования

Для просмотра и анализа результата сканирования нажмите по ссылке с наименованием результата. Откроется форма просмотра результатов сканирования (см. «Рис. 92»).

	iora / laure										
Основное											
Тип сканирования:	maxpatrol										
Начало сканирования:	2021-05-13 18:3	2:26									
Конец сканирования:	2021-05-13 16:3	1:22									
Обработано:											
Импорт завершен:	Да										
Наличие уязвимостей:	Да										
Сканирование ПО:	Да										
Туть сканирования:	/opt/pangeorada	r/cruddy/imp	ports/maxpatrol/archive/2024-0	9-13T14:58:50+0	3:00_MP8_Audit	xml					
-айдено уязвимостей:	129736										
Количество хостов:	51										
Уязвимости по важности:	10278 (10276)	50693 (5069	26628 (26628) 0	42137 (42137)							
хосты с ошибкой 7											C
ты Хосты с ошибкой	IP	MAC	Количество уязвимостей	Важность 4	Важность 3	Важность 2	Важность 1	Важность О	Установле	Начало сканирования	С Конец сканирования
ты Хосты с ошибкой	IP 10.144.86.166	MAC	Количество уязвимостей 0	Важность 4 0	Важность 3 0	Важность 2 0	Важность 1 0	Важность 0	Установле 0	Начало сканирования 16:03:14 13.05.2021	С [*] Конец сканирования 16:31:22 13.05.2021
ты Хосты с ошибкой ОN	IP 10.144.86.166 10.144.87.122	MAC	Количество уязвимостей 0 0	Важность 4 0 0	Важность 3 0 0	Важность 2 0 0	Важность 1 0 0	Важность 0 0	Установле О О	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021
ты Хосты с ошибкой	IP 10.144.86.166 10.144.97.122 10.144.96.216	MAC	Количество уязвимостей 0 0	Важность 4 0 0 0	Важность 3 0 0 0	Важность 2 0 0 0	Важность 1 0 0 0	Важность 0 0 0	Установле 0 0 0	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021
ты Хосты с ошибкой	IP 10.144.86.166 10.144.87.122 10.144.96.216 10.144.87.131	MAC	Количество уязвимостей 0 0 0 0	Важность 4 0 0 0 0 0 0	Важность 3 0 0 0 0	Важность 2 0 0 0 0	Важность 1 0 0 0 0	Важность 0 0 0 0 0	Установле 0 0 0 0 0	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021
Хосты с ощибкой 2 ХОМ	IP 10.144.86.166 10.144.87.122 10.144.96.216 10.144.87.131 10.144.87.177	MAC	Количество уязвимостей 0 0 0 0 0	Важность 4 0 0 0 0 0 0 0 0	Важность 3 0 0 0 0 0	Важность 2 0 0 0 0 0 0 0 0 0 0 0 0	Важность 1 0 0 0 0 0	Важность 0 0 0 0 0 0	Установле 0 0 0 0 0 0	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021 16:59:44 13.05.2021
Thi Хосты с ощибкой 7 2DN	IP 10.144.86.166 10.144.87.122 10.144.96.216 10.144.87.131 10.144.87.177 10.200.70.148	MAC	Количество уязвимостей 0 0 0 0 0 0 0	Важность 4 0 0 0 0 0 0 0 0 0 0	Важность 3 0 0 0 0 0 0 0	Важность 2 0 0 0 0 0 0 0	Важность 1 0 0 0 0 0 0 0	Важность 0 0 0 0 0 0 0	Установле 0 0 0 0 0 0 0 0	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021 16:16:01 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021 16:59:44 13.05.2021 17:02:52 13.05.2021
ты Хосты с ощибкой ADN	IP 10.144.86.166 10.144.87.122 10.144.96.216 10.144.87.131 10.144.87.177 10.200.70.188	MAC	Количество уязвимостей 0 0 0 0 0 0 0 0 0 0	Важность 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 3 0 0 0 0 0 0 0 0 0	Важность 2 0 0 0 0 0 0 0 0 0 0	Важность 1 0 0 0 0 0 0 0 0 0 0	Важность 0 0 0 0 0 0 0 0 0 0	Установле 0 0 0 0 0 0 0 0 0 0	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021 16:16:01 13.05.2021 16:24:47 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021 16:59:44 13.05.2021 17:02:52 13.05.2021 16:49:42 13.05.2021
ты Хосты с ощибкой ADN	IP 10.144.86.166 10.144.87.122 10.144.96.216 10.144.87.131 10.144.87.131 10.144.87.177 10.200.70.182 10.200.70.182	MAC	Количество уязвимостей 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 3 0 0 0 0 0 0 0 0 0 0 0 0	Важность 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 1 0 0 0 0 0 0 0 0 0 0 0 0	Важность 0 0 0 0 0 0 0 0 0 0 0 0	Установле О О О О О О О О О О О О О	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021 16:16:01 13.05.2021 16:24:47 13.05.2021 16:25:10 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021 16:59:44 13.05.2021 16:59:24 13.05.2021 16:49:42 13.05.2021 16:55:22 13.05.2021
ты Хосты с ошибкой ADDN	IP 10.144.86.166 10.144.87.122 10.144.87.122 10.144.87.131 10.144.87.131 10.144.87.131 10.144.87.131 10.200.70.148 10.200.70.182 10.200.31.50 10.200.229.159	MAC	Количество уязвимостей 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Важность 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Установле О О О О О О О О О О О О О О О	Начало сканирования 16:03:14 13.05.2021 16:03:56 13.05.2021 16:07:13 13.05.2021 16:15:11 13.05.2021 16:16:01 13.05.2021 16:24:47 13.05.2021 16:25:10 13.05.2021 16:26:22 13.05.2021	С Конец сканирования 16:31:22 13.05.2021 16:48:04 13.05.2021 16:56:22 13.05.2021 17:00:01 13.05.2021 16:59:44 13.05.2021 16:59:24 13.05.2021 16:49:42 13.05.2021 16:55:22 13.05.2021

Рис. 92 – Форма просмотра результата сканирования

На форме просмотра результата сканирования информация сгруппирована по следующим блокам:

- Блок Основное основная информация о результате сканирования;
- Таблица Хосты/Хосты с ошибкой информация о просканированных хостах.

7.5.3.1 Основная информация о результате сканирования

Пример блока Основное приведен на «Рис. 93».

Основное	
Тип сканирования:	maxpatrol
Начало сканирования:	2021-05-13 18:32:26
Конец сканирования:	2021-05-13 16:31:22
Обработано:	
Импорт завершен:	Да
Наличие уязвимостей:	Да
Сканирование ПО:	Да
Путь сканирования:	/opt/pangeoradar/cruddy/imports/maxpatrol/archive/2024-09-13T14:58:50+03:00_MP8_Audit.xml
Найдено уязвимостей:	129736
Количество хостов:	51
Уязвимости по важности:	10278 (10276) 50693 (50692) 26628 (26628) 0 42137 (42137)

Рис. 93 – Форма просмотра результата сканирования. Блок "Основное"

В блоке отображается следующая информация:

- Тип сканирования наименование сканнера уязвимости, который предоставил результаты сканирования;
- Начало сканирования дата и время начала сканирования;
- Конец сканирования дата и время окончания сканирования;
- Обработано обработан ли результат сканирования оператором: Да, Нет;
- Импорт завершен завершен ли импорт результатов сканирования: Да, Нет;
- Наличие уязвимостей обнаружены ли уязвимости в ходе обработки результатов сканирования: Да, Нет;
- Сканирование ПО выполнялось ли сканирование ПО: Да, Нет;
- Путь сканирования путь к файлу с результатами сканирования;
- Найдено уязвимостей общее количество найденных уязвимостей;
- Количество хостов количество просканированных хостов;
- **Уязвимости по важности** количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS.

7.5.3.2 Информация о просканированных хостах

Информация о хостах отображается на следующих вкладках:

- "Хосты";
- "Хосты с ошибкой".

Пример таблицы приведен на «Рис. 94».

Хосты с ошибкой											C
FQDN	IP	MAC	Количество уязвимостей	Важность 4	Важность 3	Важность 2	Важность 1	Важность О	Установле	Начало сканирования	Конец сканирования
	10.144.86.166		0	0	0	0	0	0	0	16:03:14 13.05.2021	16:31:22 13.05.2021
	10.144.87.122		0	0	0	0	0	0	0	16:03:56 13.05.2021	16:48:04 13.05.2021
	10.144.96.216		0	0	0	0	0	0	0	16:07:13 13.05.2021	16:56:22 13.05.2021
	10.144.87.131		0	0	0	0	0	0	0	16:15:11 13.05.2021	17:00:01 13.05.2021
	10.144.87.177		0	0	0	0	0	0	0	16:16:01 13.05.2021	16:59:44 13.05.2021
cta-belav2.main.oao.rzd	10.200.70.148		0	0	0	0	0	0	0	16:24:47 13.05.2021	17:02:52 13.05.2021
cta-mileshnikov.main.oao.rzd	10.200.70.182		0	0	0	0	0	0	0	16:25:10 13.05.2021	16:49:42 13.05.2021
ctech-apolosov.main.oao.rzd	10.200.31.50		0	0	0	0	0	0	0	16:26:22 13.05.2021	16:55:22 13.05.2021
ctim-lukashkina.main.oao.rzd	10.200.229.159		0	0	0	0	0	0	0	16:30:38 13.05.2021	16:48:34 13.05.2021
ctlb-burenko.main.oao.rzd	10.222.9.145		0	0	0	0	0	0	0	16:31:37 13.05.2021	17:22:43 13.05.2021

Рис. 94 – Форма просмотра результата сканирования. Блок "Хосты"

В блоке отображается следующая информация:

- **FQDN** FQDN xocta;
- **IP** IP-адрес хоста;
- **MAC** MAC-адрес хоста;
- Количество уязвимостей количество уязвимостей, выявленных на хосте;
- **Важность** отображаются количественные результаты найденных уязвимостей, разделенные на группы важности от 0 до 4;
- Установленное ПО количество обнаруженного ПО на хосте;
- Начало сканирования дата и время начала сканирования;
- Конец сканирования дата и время окончания сканирования;
- Ошибка сканирования информация об ошибках (только для вкладки "Хосты с ошибкой").

7.5.4 Сравнение результатов сканирования

Для сравнения результатов сканирования с существующими данными перейдите в раздел **Активы** → **Результаты сканирования** и нажмите кнопку **Сравнить** в строке нужного результата сканирования.

Откроется форма сравнения результатов сканирования. Информация на форме разделена на три вкладки:

- "Новое" на вкладке отображаются новые уязвимости и предоставляется возможность на их основе создать инциденты;
- "Закрываемые" на вкладке отображаются уже обнаруженные уязвимости и предоставляется возможность закрыть соответствующие инциденты.;
- "Обработано" перечень обработанных уязвимостей.

Пример внешнего вида формы сравнения результатов сканирования приведен на «Рис. 95».
📃 👹 лантео 172.30.249.21 v Сравнение результатов сканирования с существующими данными Лицензия активна до: 2025-08-16 🛈 Документация 🛞 аdmin v										
Рабочий стол	Сравнение результа	тов сканирования с существуюц	цими данными							
Q События										
① Инциденты ~	🖓 Новое Закрываемые	Обработано								
с‼ Активы ^	Саписей: 2, показано 1 - 2									
Активы	Активы									
Группы активов	Название	Аутентифицированный	Статистик	ка важности	IP (MAC)					
Настройки идентификац	10.144.87.131	Ê 1/60 0/12		/483 0/0 0/1032	÷ 10.144.87.131					
Сетевые интерфейсы	10.144.76.106		0/344 1/1524 0	10.144.76.106						
Результаты сканирования	Уязвимости									
Обнаружение хостов	ID плагина Инци	адент / Тип инцидента	Название плагина	Сводка ІР ((МАС) Порт Протокол					
Обнаружение сервисов			0/344 1/1524 0/962 0/0	1						
Сбор данных	10.144.76.106		0/731	10.144.76.106 Nov	казать данные хоста \vee					
🗈 Соответствие ПО 🗸 🗸	100633 C MHO	кественные неудачные попытки входа на различных хост	гах под Выполнение произвольного кода 🗸	Выполнение						
% Коррелятор 🗸 🗸	разл	ичными учетными записями		произвольного кода						
¥ Источники 🗸			1/60 0/1218 0/483 0/0							
∦ ⊈ Параметры — ∽	10.144.87.131		0/1032	10.144.07.131	казать данные хоста					
 Администрирование ~ 	191057 C Множ	кественные неудачные попытки входа на различных хост ичными учетными записями	тах под Смешение типов 🗸	Смешение типов						
	< 1 > 10 / страница ~									

Рис. 95 – Форма сравнения результатов сканирования с существующими данными

Информация на форме разделена по двум таблицам: Активы и Уязвимости

В таблице Активы отображается следующая информация:

- Название наименование актива;
- **Аутентифицированный** аутентифицированный ли актив в платформе: да (зеленый замок), нет (красный замок);
- Статистика важности количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS;
- **IP (MAC)** IP или MAC-адрес актива.

В таблице Уязвимости информация об уязвимости сгруппирована в две строки:

• **Первая строка**. Отображается детальная информация об активе и статистике важности обнаруженных уязвимостей. Существует возможность показать подробные данные хоста при клике на соответствующую ссылку. Пример приведен на «Рис. 96».

10.200.68.90	315/315	2175/2175 936/936 0/0	1069 / 1069	10.200.68.90	Показать данные хоста \land
		IP	MAC	FQDN	OC
Просканированные хосты	£	10.200.68.90		czt-kalahnikova.main.oao.rzd	Microsoft Windows
Известные хосты		10.200.68.90			Microsoft Windows

Рис. 96 – Таблица "Уязвимости". Строка с информацией об активе

- Вторая строка. Отображается следующая информация:
 - **ID плагина** ID плагина, который обнаружил уязвимость;
 - Наименование инцидента/типа инцидента если по уязвимости уже существует инцидент, то отображается соответствующая информация;
 - Название плагина наименование плагина, выявившего уязвимость. По ссылке откроется детальная информация о плагине;
 - Сводка сводная информация об уязвимости.

Пример приведен на «Рис. 97».

= 🕻	PADAP	172.30.249.21 🗸	Сравнение результатов с	канирования с существующими данными		Лицензия активна до: 2025-08-16	🛈 Документация 🔘 admin
6	Уязвим	мости					
Q		ID плагина	Инцидент / Тип инцидента	Название плагина	Сводка	IP (MAC)	Порт Протокол
GB		10.200.68.90		315/315 2175/2175 936/936 0/0 1069/1069	10.200.68.90	Показать данные хоста 🖂	
۵		10006 +		Дата обновления антивирусных баз ^	Дата обновления ант	гивирусных баз	· ·
<i>7</i> 0	10	0.200.68.90					
ж Ф	Свод, Дата - Опис: Дата -	ка обновления антив ание угрозы обновления антив	ирусных баз ирусных баз		Вектор CVSS Нет данных CVSS Temporal Vector Нет данных CVSS Temporal Score Нет данных Фиктор риска Токи Дата изменения плагина Нет данных Дата изменения плагина Нет данных Дата изменения плагина Нет данных Дата изменения плагина Соки	сыых бөз <short_description></short_description> <description></description> >	how_to_fix/> <links></links>
	+Дог >	полнительная инфо	ормация		Рекомендации по устранению угрозь Нет данных		7

Рис. 97 – Таблица "Уязвимости". Строка с информацией о уязвимости

По результатам сравнения результатов сканирования с существующими данными доступны следующие действия:

- 1. «Создание инцидентов по результатам сравнения».
- 2. «Закрытие инцидентов по результатам сравнения».

7.5.4.1 Создание инцидентов по результатам сравнения

- 1. Откройте результаты сравнения и перейдите на вкладку "Новое".
- 2. Выберите уязвимости, установив соответствующие флаги.
- 3. Нажмите кнопку Создать инциденты. Откроется окно "Массовое создание инцидентов".
- 4. Проверьте в окне информацию о создаваемых инцидентах и подтвердите действие.

7.5.4.2 Закрытие инцидентов по результатам сравнения

- 1. Откройте результаты сравнения и перейдите на вкладку "Закрываемые".
- 2. Выберите уязвимости, установив соответствующие флаги.
- 3. Нажмите кнопку Закрытие инцидента. Откроется окно "Массовое закрытие инцидентов".
- 4. Проверьте в окне информацию о закрываемых инцидентах и подтвердите действие.

7.5.5 Изменение статуса результата сканирования

В Платформе Радар результаты сканирования могут находиться в следующих состояниях:

- Обработано результаты сканирования исследованы ответственным специалистом, выполнено сравнение с текущим состоянием активов.
- Не обработано результаты сканирования еще не были исследованы.

Для изменения статуса результата сканирования перейдите в раздел **Активы** → **Результаты сканирования** и нажмите кнопку в соответствующей строке. По наведении курсора мыши на кнопку отобразится информация о том, на какое состояние будет изменен результат сканирования.

7.6 Обнаружение хостов

Под обнаружением хостов подразумевается сканирование подсети, в результате которого может быть получен набор данных, достаточный для идентификации актива.

В результате сканирования может быть создана новая запись об активе или обновлена информация о существующем.

Для выполнения сканирования подсети перейдите в раздел **Активы** → **Обнаружение хостов** и выполните следующие действия:

- 1. В поле **IP** укажите IP-адрес подсети.
- 2. В поле Подсеть из выпадающего списка выберите подсеть.
- 3. Нажмите кнопку Сканировать.

По результатам сканирования будет выдан список обнаруженных хостов (см. «Рис. 98»).

≡	Пангео 172	2.30.249.21 🗸 Обнаружение хосто	В	Лицензия а	ктивна до: 2025-08-16	🛈 База знаний	\bigcirc admin \lor				
ഹ	Обнар	ужение хостов									
Q											
()	IP	Подсеть									
⊊₿	172.30	0.254.0 24 V CK	анировать								
ð											
<i>7</i> ?+	Импортир	овать					C 🔯				
Xr		HOST	IPv4	IPv6	MAC						
25		["v-stand-01.pgr.local"]	172.30.254.91		6A:2A:15:81:D8:9E						
411		["v-stand-03.pgr.local"]	172.30.254.93		7E:CC:68:9C:D9:33						
Ø		["v-stand-05.pgr.local"]	172.30.254.95		BC:24:11:3C:6A:CA						
	< 1	> 10 / страница >									

Рис. 98 – Раздел «Обнаружение хостов»

В списке отображается следующая информация:

- **HOST** наименование хоста;
- IPv4 IP-адрес хоста по четвертой версии протокола IP;
- IPv6 IP-адрес хоста по шестой версии протокола IP;
- МАС Мас-адрес хоста.

Для создания новых записей об активах или обновлении информации о существующих отметьте необходимые хосты и нажмите кнопку **Импортировать**.

7.7 Обнаружение сервисов

В Платформу Радар встроен механизм, который позволяет по запросу собирать данные о сервисах на выбранных активах.

Результатом сканирования является наполнение выбранных активов информацией об открытых портах и диагностике установленного ПО и ОС по открытым данным актива.

Для работы с механизмом по обнаружению сервисов перейдите в раздел Активы → Обнаружение сервисов.

Пример собранной информации об активах приведен на «Рис. 99».

ПАНГЕС РАДАР	⁰ 172.30.249.21 ∨	Обнаружени	е сервисов				л	ицензия активн	а до: 2025-08	3-16 🕕 Документация	🔘 admin
06	наружение	сервисов									
8	Сканировать сер	висы								Выбра	ано: 1 С 🕴
	Название	Операционная	Сетевые	Сервисы	Тип	Обновлено	Создано	Значимост	Сетевая	Группа ответственных	Уровень рисн
	Атктив с сетевым			PostgreSQL DB	Host	11:36:46 04.12.2024	11:36:46 04.12.2024	Некритичн	Нет		0
	111.111.111.11		111.111.111.11	nginx	Host	13:05:42 02.12.2024	13:05:42 02.12.2024	Ключевой	Штатный	9	0
	10.11.0.205		10.11.0.205	nginx	Host	11:53:17 28.11.2024	11:53:17 28.11.2024	Ключевой	Штатный		0
	172.30.254.97		172.30.254.97	nginx	Host	13:57:45 30.10.2024	13:57:45 30.10.2024	Ключевой	Штатный	-	0
	10.200.68.90	Microsoft Windows	10.200.68.90	nginx	Host	13:37:02 17.10.2024	15:02:02 13.09.2024	Ключевой	Штатный	users	0
2	10.144.98.114	Microsoft Windows	10.144.98.114	nginx	Host	15:01:58 13.09.2024	15:01:58 13.09.2024	Ключевой	Штатный		o
	10.144.98.106	Microsoft Windows	10.144.98.106		Host	15:01:54 13.09.2024	15:01:54 13.09.2024	Ключевой	Штатный	-	0
	10.200.4.17	Microsoft Windows	1.2.1.12 10.200.4.17		Host	15:53:55 17.09.2024	15:01:52 13.09.2024	Ключевой	Штатный	-	0
	10.200.52.219	Microsoft Windows	10.200.52.219	•	Host	15:01:50 13.09.2024	15:01:50 13.09.2024	Ключевой	Штатный		0
	10.200.85.19	Microsoft Windows	10.200.85.19	-	Host	15:01:47 13:09:2024	15:01:47 13.09.2024	Ключевой	Штатный	-	0

Рис. 99 – Раздел "Сбор данных"

В разделе отображается следующая информация:

- Название наименование актива;
- Операционная система наименование ОС, установленной на активе;
- Сетевые интерфейсы список сетевых интерфейсов актива;
- Сервисы список сервисов, обнаруженных на активе;
- Тип тип обнаруженного сервиса;
- Создано дата и время добавления информации об активе;
- Обновлено дата и время изменения информации об активе;
- Значимость актива уровень влияния актива на выполнение бизнес-процессов компании называется;
- Сетевая видимость тип сетевой видимости актива;
- **Группа ответственных** группа пользователей, ответственная за разбор инцидентов, выявленных на активе;
- Уровень риска цифровое обозначение уровня риска актива.

Для запуска процесса обнаружения сервисов выполните следующие действия:

- 1. Выберите активы, с которых необходимо собрать данные, установив соответствующие флаги.
- 2. Нажмите кнопку Сканировать сервисы.
- 3. Начнется процесс сбора данных с выбранных активов. Процесс может занять некоторое время.

7.8 Сбор данных

В **Платформу Радар** встроен механизм, который позволяет по запросу собирать данные с выбранных активов.

Сбор выполняется с помощью учетных записей для сбора данных (подробнее см. документ «Руководство администратора. Раздел Кластер»).

Результатом работы сбора данных является найденный список установленного аппаратного и программного обеспечения на активе.

Для работы с механизмом по сбору данных перейдите в раздел **Активы** → **Сбор данных**.

Пример собранной информации об активах приведен на «Рис. 100».

i i	ПАНГЕО РАДАР	172.30.249.21 🗸	Сбор данных							Пицензия активна до: 20	25-08-16 ① Документа	ция Q admin
	Сбо	ор данных										
	7	Собрать									B	ыбрано: 1 С
		Название	Тип	Сетевые	Аппаратное	Программное	Создано	Обновлено	Значимость актива	Сетевая видимость	Группа ответственных	Уровень риска
	~	Атктив с сетевым	Host		×	×	11:36:46 04.12.2024	11:36:46 04.12.2024	Некритичный	Нет подключения к	-	0
		111.111.111.11	Host	111.111.111.11	×	×	13:05:42 02.12.2024	13:05:42 02.12.2024	Ключевой	Штатный доступ в	-	0
		10.11.0.205	Host	10.11.0.205	×	×	11:53:17 28.11.2024	11:53:17 28.11.2024	Ключевой	Штатный доступ в	-	0
		172.30.254.97	Host	172.30.254.97	×	×	13:57:45 30.10.2024	13:57:45 30.10.2024	Ключевой	Штатный доступ в	-	0
		10.200.68.90	Host	10.200.68.90	×	×	15:02:02 13:09:2024	13:37:02 17.10.2024	Ключевой	Штатный доступ в	users	0
		10.144.98.114	Host	10.144.98.114	×	×	15:01:58 13.09.2024	15:01:58 13.09.2024	Ключевой	Штатный доступ в	-	0
		10.144.98.106	Host	10.144.98.106	×	×	15:01:54 13.09.2024	15:01:54 13.09.2024	Ключевой	Штатный доступ в	-	0
		10.200.4.17	Host	1.2.1.12 aaaa 10.200.4.17	×	×	15:01:52 13.09.2024	15:53:55 17.09.2024	Ключевой	Штатный доступ в	-	0
		10.200.52.219	Host	10.200.52.219	×	×	15:01:50 13.09.2024	15:01:50 13.09.2024	Ключевой	Штатный доступ в	-	0
		10.200.85.19	Host	10.200.85.19	×	×	15:01:47 13:09:2024	15:01:47 13:09:2024	Ключевой	Штатный доступ в	-	0

Рис. 100 – Раздел "Сбор данных"

В разделе отображается следующая информация:

- Название наименование актива;
- **Тип** тип актива;
- Сетевые интерфейсы список сетевых интерфейсов актива;
- Аппаратное обеспечение список аппаратного обеспечения актива;
- **Программное обеспечение** список программного обеспечения, установленного на активе;
- Создано дата и время добавления информации об активе;
- Обновлено дата и время изменения информации об активе;
- Значимость актива уровень влияния актива на выполнение бизнес-процессов компании называется;

- Сетевая видимость тип сетевой видимости актива;
- **Группа ответственных** группа пользователей, ответственная за разбор инцидентов, выявленных на активе;
- Уровень риска цифровое обозначение уровня риска актива.

Для сбора данных выполните следующие действия:

- 1. Выберите активы, с которых необходимо собрать данные, установив соответствующие флаги.
- 2. Нажмите кнопку Собрать данные. Откроется окно "Настройки" (см. «Рис. 101»).

Настройки	×
Протокол	
RPC	~
Учетная запись	
учетная запись	~
Иппаратное обеспечение	Программное обеспечение
	Собрать Закрыть

Рис. 101 – Окно "Настройки"

- 3. Укажите в окне следующую информацию:
 - в поле **Протокол** выберите сетевой протокол, по которому будет выполнено подключение и сбор данных с актива;
 - в поле **Учетная запись** выберите учетную запись, которая будет выполнять подключение к активу. Список доступных учетных записей формируется в зависимости от выбранного протокола;
 - при необходимости собирать информацию об аппаратном и программном обеспечении установите соответствующие флаги.
- 4. Нажмите кнопку **Собрать**. Начнется процесс сбора данных с выбранных активов. Процесс может занять некоторое время.

При возникновении ошибок при сборе данных обратитесь к документу «Руководство администратора. Раздел Возможные проблемы при эксплуатации платформы».

8. Соответствие ПО

8.1 Общие сведения

Платформа Радар позволяет настроить контроль установленного программного обеспечения. Контролируется ПО, которое устанавливается на активах. Контроль выполняется в соответствии с политиками контроля.

Политика контроля состоит из набора правил, которые могут отслеживать следующую информацию:

- отсутствие программного обеспечения на активе;
- наличие программного обеспечения на активе.

Политика контроля может быть применена к группе активов.

По результатам проверки соответствия ПО принимается одно из решений "Соответствует" или "Не соответствует".

Актив считается соответствующим политике, если все правила, входящие в политику контроля, дали положительный результат.

Группа активов считается соответствующей политике, если все активы группы соответствуют политике.

По результатам проверки соответствия политикам, платформа автоматически создает соответствующие инциденты ИБ при выполнении следующего условия: добавлен тип инцидента, у которого включена настройка **Использовать для создания инцидентов при оценке** соответствия ПО (см. раздел «Создание типа инцидента»).

Результаты проверки соответствия ПО заданным политикам контроля, отображаются в разделе «<u>Результаты соответствия ПО</u>».

Управление правилами контроля выполняется в разделе «Правила соответствия ПО».

Управление наборами правил контроля (политиками) выполняется в разделе «<u>Наборы правил</u> <u>соответствия ПО</u>».

В разделах «<u>Список ПО</u>» и «<u>Список групп ПО</u>» выполняется управление информацией о программном обеспечении, которое установлено на активах и объединение списка ПО в группы.

8.2 Результаты соответствия ПО

В разделе отображаются сводные результаты всех текущих проверок соответствия ПО.

Работа с результатами соответствия ПО включает в себя следующие процессы:

- 1. «Запуск процесса проверки соответствия ПО».
- 2. «Просмотр информации о результате соответствия ПО».
- 3. «Удаление результатов соответствия ПО».

Для работы с результатами проверок на соответствие ПО перейдите в раздел **Соответствие ПО** → **Результаты соответствия** (см. «Рис. 102»).

≡	Кангео 172 радар	2.30.254.155 🗸 Результаты соответствия ПО		Лиценз	ия активна до: 2024-12-25 ① Документация	🔘 admin ~						
â	Резуль	ататы соответствия ПО										
Q												
0	У	7 Удалить Удалить все										
		ID	Группа активов	Соответствует	Выполнено							
CI3		68a36d86-ec9c-4067-83af-a75870534389	Servers	Нет	12:18:50 06.10.2023	@ fi						
ð		84185d45-f8e7-4e3f-ac16-5fd60b2fb41c	Servers	Нет	12:49:51 04.10.2024	© 11						
H.		e45a1829-8262-4244-ad9b-3be6671da52b	Servers	Нет	12:50:29 04.10.2024	© 11						
×		edc94644-118d-4e44-832f-7b6c5472da58	Servers	Нет	11:21:55 02.11.2024	© 11						
		79fe0e3e-ce11-4442-85fe-a5c8220b8afc	Servers	Нет	11:21:57 02.11.2024	© 11						
414		e40579a6-9263-4195-b225-13cc91e68e7d	Servers	Нет	11:21:57 02.11.2024	© 11						
٢		39a6a63e-3c20-4d90-ac8f-81b09affc427	Servers	Нет	11:21:57 02.11.2024	© fi						
		6ec88f35-2401-42dd-a687-96c5670fbc01	Servers	Нет	11:21:59 02.11.2024	© 11						
		3af3de75-2052-4d83-a257-7bbb5f2197f2	Servers	Нет	11:22:00 02.11.2024	© fi						
		c3d08bef-212f-42fd-ae46-8a2b088811a6	Servers	Нет	11:22:00 02.11.2024	0						
	< 1	2 3 > 10 / страница ~										

Рис. 102 – Раздел "Результаты соответствия ПО"

В разделе отображается следующая информация о результатах проверки ПО:

- **ID** идентификатор проверки соответствия ПО. По ссылке произойдет переход на форму просмотра результата соответствия ПО;
- **Группа активов** наименование группы активов, по которой выполнялась проверка соответствия ПО. По ссылке произойдет переход на форму просмотра группы активов;
- Соответствует результат проведения проверки: соответствует или не соответствует группа активов заданной политике контроля;
- Выполнено дата и время выполнения проверки.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
0	просмотр детализации по проверке
Ū	удаление записи из таблицы

8.2.1 Запуск процесса проверки соответствия ПО

Для запуска процесса проверки соответствия ПО перейдите в раздел **Активы** → **Группы** активов и нажмите кнопку ^[2] (см. «Рис. 103»).

Группы активов										
Создать Удалить Удалить все										
	Название	Регулярное выражение	Кол-во активов	Группа ответственных						
	Servers	.*AD.*	256	admin 📮						
< 1 > 10 / страница > Запуск проверки соответствия ПО										

Рис. 103 – Раздел "Группы активов". Запуск проверки соответствия ПО

Будет создана задача на проведение проверки соответствия ПО, а ее результаты отобразятся в разделе **Соответствие ПО** → **Результаты соответствия**.

8.2.2 Просмотр информации о результате соответствия ПО

Для просмотра детализации о результате соответствия ПО нажмите кнопку ⁽¹⁾. Откроется форма "Результаты соответствия ПО" (см. «Рис. 104»).

≡	Пангео 172.30.254.1	55 🗸 Результаты соответствия ПО		Лицензия активна до: 2024-12-25 ① Докум	 ентация 🔘 admin ~
â	Результаты	соответствия ПО			
Q					
1	Группа активов : Servers				
⊊Ē	Соответствует: Нет Выполнено: 06.10.2023 12:18:50				
ð	A				
<i>7</i> ?+	АКТИВ	Соответствует (количество наборов правил кон	нтроля)	Не соответствует (количество наборов правил контроля)	Данные ПО
	DESKTOP-AD01	0		1	\checkmark
ж	DESKTOP-AD09	0		1	\checkmark
49J	DESKTOP-AD10	0		1	~
	DESKTOP-AD01	0		1	\checkmark
0	DESKTOP-AD02	0		1	~

Рис. 104 – Форма "Результаты соответствия ПО"

На форме отображается следующая информация:

- Группа активов наименование группы активов, по которой проводилась проверка соответствия;
- Соответствует все ли активы, входящие в группу, соответствуют политике: да, нет;
- Выполнено дата и время выполнения проверки;
- Информация об активах, входящих в группу:
 - Актив наименование актива;
 - Соответствует (количество наборов правил контроля) количество политик, которые дали положительный (соответствует) результат при проведении проверки соответствия ПО на данном активе;
 - Не соответствует (количество наборов правил контроля) количество политик, которые дали отрицательный (не соответствует) результат при проведении проверки соответствия ПО на данном активе;
 - **Данные ПО** наличие/отсутствие данных об установленном программном обеспечении на активе.

8.2.3 Удаление результатов соответствия ПО

Удаление результатов соответствия ПО можно выполнить следующими способами:

- удаление конкретного результата соответствия ПО;
- массовое удаление результатов соответствия ПО;
- удаление всех результатов соответствия ПО.

Способ 1. Удаление конкретного результата соответствия ПО:

- 1. Перейдите в раздел **Соответствие ПО Результаты соответствия ПО**.
- 2. В строке нужного результата соответствия ПО нажмите кнопку 🔟.
- 3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление результатов соответствия ПО:

- 1. Перейдите в раздел **Соответствие ПО Результаты соответствия ПО**.
- 2. Отметьте необходимые результаты соответствия ПО.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех результатов соответствия:

- 1. Перейдите в раздел **Соответствие ПО** → **Результаты соответствия ПО**.
- 2. Нажмите кнопку Удалите все.
- 3. Подтвердите удаление в открывшемся окне.

8.3 Список ПО

В платформе доступен перечень всего программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов.

Работа со списком ПО включает в себя следующие процессы:

- 1. «<u>Просмотр информации о ПО</u>».
- 2. «Просмотр информации об активах, на которых установлено ПО».
- 3. «<u>Редактирование записи о ПО</u>».
- 4. «Удаление записи о ПО из платформы».

Для работы со списком ПО перейдите в раздел Соответствие ПО → Список ПО (см. «Рис. 105»).

=	PADAP	172.30.254.155 ∨ Список ПО				Лицензия ак	чивна до: 2024-12-25	 Документация 	l 🔕 admin
â	Спи	сок ПО							
Q ()	7	Удалить Удалить все						Выбран	D: 0 C 🔘
		Название	Версия	Описание	Необработанная строка данных	Группа ПО	Создано	Активы	
¢0		7-Zip	9.25 alpha		7-Zip 9.25 alpha	7-Zip	10:44:23 06.10.2023	Активы	◎ ⁄ 前
D		7-Zip	9.15 beta		7-Zip 9.15 beta	7-Zip	10:44:00 06.10.2023	Активы	◎ ⁄ 前
<i>%</i>		Quartz.dll (DirectShow)	6.2.18362.1316		Quartz.dll (DirectShow)		10:43:16 06.10.2023	Активы	@ Ø Ē
×		Microsoft OneDrive	19.2.107.5		Microsoft OneDrive 19.2.107.5		10:43:16 06.10.2023	Активы	000
41		Microsoft OneDrive	20.143.716.3		Microsoft OneDrive 20.143.716.3	-	10:43:16 06.10.2023	Активы	• 1 1
0		Remote Desktop Connection Client	10.0		Remote Desktop Connection		10:43:16 06.10.2023	Активы	• 0 1
		Yandex Browser	19.3.2.177		Yandex Browser 19.3.2.177		10:43:16 06.10.2023	Активы	◎ ⁄ ₫
		Microsoft Common Controls (mscomctl.ocx)			Microsoft Common Controls		10:43:16 06.10.2023	Активы	• 1 1
		Network Configuration	Network Configuration		Network Configuration Network		10:43:16 06.10.2023	Активы	000
		Microsoft Windows Remote Access Connection	6.2		Microsoft Windows Remote		10:43:16 06.10.2023	Активы	◎ ⁄ ₫
		1 2 3 4 5 6 7 37	> 10 / страница ~						

Рис. 105 – Раздел "Список ПО"

В разделе отображается следующая информация о ПО:

- Название наименование ПО в платформе;
- Версия версия ПО;
- Описание дополнительные сведения о ПО;
- Необработанная строка данных данные, полученные напрямую от сканера уязвимостей;
- Группа ПО наименование группы, в которую входит ПО;
- Создано дата и время создания записи о ПО.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие	
Ø	изменение записи о ПО	
\odot	оосмотр детализации по проверке	
回	удаление записи о ПО	
Активы	просмотр списка активов, на которых установлено ПО	

8.3.1 Просмотр информации о ПО

Для просмотра информации о ПО нажмите кнопку ⁽²⁰⁾. Откроется форма "Данные ПО" (см. «Рис. 106»).

≡	ПАНГЕО 172.30.254.155	∨ ∣ Список ПО	Лицензия активна до: 2024-12-25	 Документация 	🔘 admin 🗸
â	← Данные П	O "Microsoft Silverlight"		🖻 Удалить	Редактировать
Q					
(i)	Название	Microsoft Silverlight			
Ç.	Описание	-			
ð	Операционная система	Microsoft Windows			
* <i>P</i> +	Версия	5.1.50918.0			
	Релиз	5.1.50918.0			
ж	Необработанная строка данных	Microsoft Silverlight 5.1.50918.0			
₩Ŷ	Группа ПО				
Ø					

Рис. 106 – Форма "Данные ПО"

На форме отображается следующая информация:

- Название наименование ПО в платформе;
- Описание дополнительные сведения о ПО;
- Операционная система наименование операционной системы, на которой работает ПО;
- Версия версия ПО;
- Релиз информация о технике сборки ПО (билде);
- Необработанная строка данных данные, полученные напрямую от сканера уязвимостей;

• Группа ПО – наименование группы, в которую входит ПО.

8.3.2 Просмотр информации об активах, на которых установлено ПО

Для просмотра информации об активах, на которых установлено ПО, нажмите кнопку **Активы**. Откроется страница "Просмотр актива", где в боковой панели будет сформирован список активов, на которых установлено ПО. Подробнее см. раздел «<u>Просмотр и анализ актива</u>».

8.3.3 Редактирование записи о ПО

1. Выберите нужное ПО и нажмите кнопку 🖉. Откроется форма "Редактирование ПО" (см. «Рис. 107»).

≡	Гангео 172.30.254.155 ∨ Список ПО	Лицензия активна до: 2024-12-25 $\ {\mathbb O}$ Документация $\ {\mathbb Q}$ admin \sim
â	← Редактирование "Microsoft Silverlight"	🛍 Удалить Сбросить Сохранить
Q		
0	Название *	
0	Microsoft Silverlight	
⊊₿	Описание	
ð	Описание	
<i>%</i>		
ж		
441		
٥		

Рис. 107 – Форма «Редактирование списка ПО»

- 2. В полях Название и Описание укажите или измените соответствующие данные.
- 3. Нажмите кнопку Сохранить.

8.3.4 Удаление записи о ПО из платформы

Удаление записи о ПО можно выполнить следующими способами:

- удаление конкретной записи о ПО;
- массовое удаление записей о ПО;
- удаление всех записей о ПО.

Способ 1. Удаление конкретной записи о ПО:

- 1. Перейдите в раздел Соответствие ПО Список ПО.
- 2. В строке нужной записи о ПО нажмите кнопку 🔟 или перейдите на форму просмотра необходимой записи и нажмите кнопку **Удалить**.
- 3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое записей о ПО:

1. Перейдите в раздел Соответствие ПО - Список ПО.

- 2. Отметьте необходимые записи о ПО.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.

Способ З. Удаление всех записей о ПО:

- 1. Перейдите в раздел Соответствие ПО Список ПО.
- 2. Нажмите кнопку Удалите все.
- 3. Подтвердите удаление в открывшемся окне.

8.4 Список групп ПО

Для упрощения управления списком программного обеспечения, их можно объединить в группы.

Работа с группами ПО включает в себя следующие процессы:

- 1. «<u>Создание группы ПО</u>».
- 2. «<u>Просмотр группы ПО</u>».
- 3. «<u>Редактирование группы ПО</u>».
- 4. «<u>Удаление группы ПО</u>».

Для работы с группами ПО перейдите в раздел **Соответствие ПО** → **Список групп ПО** (см. «Рис. 108»).

≡	К пангео 172.3	30.254.155 🗸 Список групп	по	Лицензия активна	до: 2024-12-25 ①Дон	кументация 🔘 admin 🗸
â	Список	групп ПО				
Q						
(i)	ГСозд	ать Удалить Удалить все				Выбрано: 0 С
-0		Название	Добавить новые версии ПО	Описание	Создано	
Ç.		7-Zip	Нет		12:00:08 15.10.2024	© ∥ İİ
ð		string	Да	string	14:24:40 22.10.2024	◎ Ø 前
* <i>P</i> *		string	Да	string	14:24:44 22.10.2024	◎ Ø 前
ж		string	Да	string	14:24:47 22.10.2024	◎ ⁄ ₪
		string	Да	string	14:24:48 22.10.2024	◎ Ø 前
411		test	Нет		12:00:08 15.10.2024	◎ Ø 前
۵	< 1	> 10 / страница ~				

Рис. 108 – Раздел "Список групп ПО"

В разделе отображается следующая информация о группах ПО:

- Название наименование группы ПО;
- **Добавить новые версии ПО** будут ли в группу автоматически добавляться новые версии ПО: да, нет;
- Описание дополнительные сведения о группе;

• Создано – дата и время создания группы.

TT	~	~			
IInи	nanote $\mu_{a\pi}$	записями табли	ны лоступны	слелующие	элементы управления.
ripri	pubbic nug	Junichim 100/11	цы доступпы	следующие	sichemin ynpublicinn.

Кнопка	Действие
Ø	изменение записи о группе ПО
\odot	просмотр группы ПО
回	удаление записи о группе ПО

8.4.1 Создание группы ПО

1. Нажмите кнопку Создать. Откроется форма "Создание группы ПО" (см. «Рис. 109»).

← Создание группы ПО				Сбросить	Co	хранить
Название *						
Microsoft						
Описание						
Список ПО Microsoft						
Список ПО		Связан	ные ПО			
Q. Введите название ПО		Q Введ	ците название ПО			
🗹 Microsoft Silverlight (Версия: 5.1.50918.0)	0	Microso	ht Silverlight (Версия: 5.1.50918.0)		0	×
✓ Microsoft Pragmatic General Multicast (Версия: 6.2)	0	Microso	oft Pragmatic General Multicast (Версия: 6.2)		0	×
Quartz.dll (DirectShow) (Версия: 6.2.18362.1316)	0	Microso	oft Windows Remote Access Connection Manager (Версия: 6	5.2)	0	×
✓ Microsoft Windows Remote Access Connection Manager (Версия: 6.2)	0	Microso	oft OneDrive (Версия: 19.2.107.5)		0	×
✓ Microsoft OneDrive (Версия: 19.2.107.5)	0					
Microsoft OneDrive (Версия: 20.143.716.3)	0					
Remote Desktop Connection Client (Версия: 10.0)	0					

Рис. 109 – Форма "Создание группы ПО"

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите наименование группы ПО;
 - в поле Описание укажите описание группы ПО;
 - для автоматического добавления новых версий ПО в группу, установите переключатель **Добавить новые версии ПО** в положение **Включен**;
 - в блоке **Список ПО** выберите ПО, которое будет добавлено в группу. Для этого установите соответствующие флаги. Выбранное ПО будет отображено в блоке **Связанные ПО**.
- 3. Нажмите кнопку Сохранить.

8.4.2 Просмотр группы ПО

Для просмотра информации о группе ПО нажмите кнопку ⁽²⁰⁾. Откроется форма "Детали группы ПО" (см. «Рис. 110»).

≡	ПАНГЕО 172.30.254.155	∽ ∣ Список ПО	Лицензия активна до: 2024-12-25 🕕 Документация	🔘 admin 🗸
â	← Детали гру	ипы ПО "Microsoft"	面 Удалить	Редактировать
Q				
1	Название	Microsoft		
⊊!	Описание	Список ПО Microsoft		
ð	Добавить новые версии ПО	Да		
°P:+	Список ПО	Microsoft Silverlight (Версия: 5.1.50918.0), Microsoft Pragmatic General Multicast (Версия: 6.2), Microsoft Windows Remote Access Connection Manager (Версия: 6.2), Microsoft ОneDrive (Версия: 19.2.107.5)		
ж				
łţţ				
Ø				

Рис. 110 – Форма "Детали группы ПО"

На форме отображается следующая информация:

- Название наименование группы ПО;
- Описание дополнительные сведения о группе ПО;
- **Добавить новые версии ПО** будут ли в группу автоматически добавляться новые версии ПО: да, нет;
- Список ПО список ПО, добавленного в группу.

8.4.3 Редактирование группы ПО

- 1. Выберите нужную группу ПО и нажмите кнопку *О* или перейдите на форму просмотра необходимой группы ПО и нажмите кнопку **Редактировать**.
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

8.4.4 Удаление группы ПО

Удаление группы ПО можно выполнить следующими способами:

- удаление конкретной группы ПО;
- массовое удаление групп ПО;
- удаление всех групп ПО.

Способ 1. Удаление конкретной группы ПО:

- 1. Перейдите в раздел Соответствие ПО -> Список групп ПО.
- 2. В строке нужной группы ПО нажмите кнопку шили перейдите на форму просмотра необходимой группы ПО и нажмите кнопку **Удалить**.
- 3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление групп ПО:

- 1. Перейдите в раздел **Соответствие ПО Список групп ПО**.
- 2. Отметьте необходимые группы ПО.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех групп ПО:

- 1. Перейдите в раздел **Соответствие ПО Список групп ПО**.
- 2. Нажмите кнопку Удалите все.
- 3. Подтвердите удаление в открывшемся окне.

8.5 Правила соответствия ПО

Правило содержит регулярное выражение, по которому выполняется фильтрация списка ПО при выполнении проверки.

Работа с правилами соответствия ПО включает в себя следующие процессы:

- 1. «Создание правила соответствия ПО».
- 2. «<u>Просмотр правила соответствия ПО</u>».
- 3. «<u>Редактирование правила соответствия ПО</u>».
- 4. «Удаление правила соответствия ПО».

Для работы с правилами перейдите в раздел **Соответствие ПО** → **Правила соответствия ПО** (см. «Рис. 111»).

≡	радар 1	172.30.254.155 🗸 Правила соответст и	вия ПО		Лицензия активна до: 20	24-12-25 🛈 Документац	ия 🔕 admin 🗸
â	Прав	ила					
Q							
()	7	Создать Удалить Удалить все				E	Зыбрано: 0 С
		Название	Фильтр	Запись в черном	Создано	Обновлено	
ςΰ		Google Chrome	google & chrome & 9*	Нет	12:15:36 06.10.2023	12:15:36 06.10.2023	© ∥ ⊡
ð		TeamViewer	teamviewer (team & viewer)	Да	12:16:19 06.10.2023	12:16:19 06.10.2023	◎ ⁄ ⊡
"H:		7-Zip	7-Zip	Нет	11:00:51 12.11.2024	11:00:51 12.11.2024	◎ ⁄ ⊡
ж	< 1	> 10 / страница ~					
łti							
0							

Рис. 111- Раздел "Правила соответствия ПО"

В разделе отображается следующая информация о правилах:

- Название наименование правила;
- Фильтр регулярное выражение, по которому работает правило;
- Запись в черном списке отметка, что данного ПО не должно быть на активе;
- Создано –дата и время создания правила;

• Обновлено –дата и время изменения информации о правиле.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
\odot	просмотр правила
Ø	изменение правила
回	удаление правила

8.5.1 Создание правила соответствия ПО

1. Нажмите кнопку Создать. Откроется форма "Создание правила" (см. «Рис. 112»).

← Создание правила	Очистить	Сохранить
Название *		
7-Zip		
Фильтр		
7-Zip		
⑦ Показать справку		
Поиск проводится по текстовым данным, включающим наименование вендора, название продукта и версию.		
Проводится поиск одновременно по всем выражениям из запроса.		
Выражения могут объединяться операторами "&" (и) и " " (или).		
Отрицание выражения производится символом "!". Выражение ":*" отбирает любые непробельные символы .		
Выражения могут группироваться при помощи скобок.		
Пример 1: Проверка, что установлена версия Mozilla firefox 21 или 22, но не версия 21.3. mozilla & firefox & ((21:* 22:*) & !21.3)		
Пример 2: Установлен Libreoffice или Microsoft Office. (Microsoft & Office) Libreoffice		
Пример 3: Поиск Antivirus, Antispyware и Antispam, но не Antigen. Anti:* & !Antigen		
Пример 4: Поиск Photoshop или Gimp (adobe & photoshop) (gnu & gimp)		
Запись в черном списке		

Рис. 112 – Форма "Создание правила"

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите наименование правила;
 - в поле Фильтр укажите регулярное выражение, по которому будет проводиться поиск ПО. По кнопке Показать справку можно посмотреть подсказку по регулярным выражениям;
 - для поиска записей в черном списке включите соответствующий переключатель.
- 3. Нажмите кнопку Сохранить.

8.5.2 Просмотр правила соответствия ПО

Для просмотра правила соответствия ПО нажмите кнопку ^(O). Откроется форма просмотра правила (см. «Рис. 113»).

Google Chrom	Google Chrome		
Создано	12:15:36 06.10.2023		
Обновлено	12:15:36 06.10.2023		
Фильтр	google & chrome & 9*		
Запись в черном списке	Нет		
Наборы правил	Compliance		

Рис. 113 – Форма просмотра правила"

На форме отображается следующая информация:

- Создано дата и время создания правила;
- Обновлено дата и время изменения информации о правиле;
- Фильтр регулярное выражение, по которому работает правило;
- Запись в черном списке будет ли выполняться поиск ПО в черном списке: да, нет;
- Наборы правил список политик, которые используют правило.

8.5.3 Редактирование правила соответствия ПО

- 1. В строке нужного правила нажмите кнопку *о* или перейдите на форму просмотра правила и нажмите кнопку **Редактировать**.
- 2. Внесите необходимые изменения.
- 3. Сохраните изменения.

8.5.4 Удаление правила соответствия ПО

Удаление правила можно выполнить следующими способами:

- удаление конкретного правила;
- массовое удаление правил;
- удаление всех правил.

Способ 1. Удаление конкретного правила:

1. Перейдите в раздел **Соответствие ПО** → **Правила соответствия ПО**.

- 2. В строке нужного правила нажмите кнопку Ш или перейдите на форму просмотра правила и нажмите кнопку **Удалить**.
- 3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление правил:

- 1. Перейдите в раздел Соответствие ПО Правила соответствия ПО
- 2. Отметьте необходимые правила.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех правил:

- 1. Перейдите в раздел **Соответствие ПО** → **Правила соответствия ПО**.
- 2. Нажмите кнопку Удалите все.
- 3. Подтвердите удаление в открывшемся окне.

8.6 Наборы правил соответствия ПО

Наборы правил соответствия ПО это политики, с помощью которых выполняется проверка соответствия ПО.

Работа с политиками контроля соответствия ПО включает в себя следующие процессы:

- 1. «Создание политики соответствия ПО».
- 2. «<u>Просмотр политики соответствия ПО</u>».
- 3. «<u>Редактирование политики соответствия ПО</u>».
- 4. «<u>Удаление политики соответствия ПО</u>».

Для работы с политиками контроля перейдите в раздел **Соответствие ПО** → **Наборы правил соответствия ПО** (см. «Рис. 114»).

≡	👹 _{Радар} о 172.30.254.155 ∨ Наборы пран	зил соответствия ПО	Лицензия активна до: 2024-12-25 🤅	Документация 🔘 admin 🗸
â	Наборы правил соответсте	вия ПО		
Q				
()	Создать Удалить Удалить все			Выбрано: 0 С
- A	Название	Автоматическое создание инцидентов	Обновлено	
⊊₿	Compliance	Да	12:16:37 03.10.2024	© 🖉 🗓
ð	 1 > 10 / страница ∨ 			
₩.				
ж				
ŧţţ				
Ø				

Рис. 114 – Раздел "Наборы правил соответствия ПО"

В разделе отображается следующая информация о политиках:

• Название – наименование политики;

- Автоматическое создание инцидента будет ли автоматически создан инцидент по результатам проведения проверки соответствия ПО: да, нет;
- Обновлено дата и время обновления информации о политике.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
\odot	просмотр политики
Ø	изменение информации о политике
Ē	удаление политики

8.6.1 Создание политики соответствия ПО

1. Нажмите кнопку Создать. Откроется форма "Создать набор правил" (см. «Рис. 115»).

← Создать набор правил	Создать	Сбросить
Название *		
Compliance		
Автоматическое создание инцидентов		
Правила		
7-Zip × TeamViewer ×		~

Рис. 115 – Форма "Создать набор правил"

- 2. Укажите на форме следующую информацию:
 - в поле Название укажите наименование политики;
 - для автоматического создания инцидентов по результатам проведения проверки соответствия ПО, установите соответствующий переключатель в положение Включен.

Примечание: Также должен быть добавлен тип инцидента, у которого включена настройка **Использовать для создания инцидентов при оценке соответствия ПО** (см. раздел «Создание типа инцидента»).

- в поле Правила выберите правила, которые будут входить в политику.
- 3. Нажмите кнопку Создать.

8.6.2 Просмотр политики соответствия ПО

Для просмотра политики контроля соответствия ПО нажмите кнопку ^(O). Откроется форма просмотра политики (см. «Рис. 116»).

← Compliance				Удалить Редактировати	
<mark>Д</mark> етальная инфор	мация				
Название Compliance	9				
Автоматическое созда	ние инцидентов Да				
Правила					2
Название	Фильтр	Запись в черном	Создано	Обновлено	
Google Chrome	google & chrome & 9*	Нет	12:15:36 06.10.2023	12:15:36 06.10.2023	
TeamViewer	teamviewer (team & viewer)	Да	12:16:19 06.10.2023	12:16:19 06.10.2023	

Рис. 116 – Форма просмотра политики"

Информация на форме отображается в следующих блоках:

- Блок Детальная информация. В блоке отображается следующая информация:
 - Название наименование политики;
 - **Автоматическое создание инцидента** будет ли автоматически создан инцидент по результатам проведения проверки соответствия ПО: да, нет.
- Блок Правила. В блоке отображается информация о правилах, входящих в политику:
 - Название наименование правила;
 - Фильтр регулярное выражение, по которому работает правило;
 - Запись в черном списке отметка, что данного ПО не должно быть на активе;
 - Создано –дата и время создания правила;
 - Обновлено –дата и время изменения информации о правиле.

8.6.3 Редактирование политики соответствия ПО

- 1. В строке нужной политики нажмите кнопку \mathcal{O} или перейдите на форму просмотра политики и нажмите кнопку **Редактировать**.
- 2. Внесите необходимые изменения.
- 3. Сохраните изменения.

8.6.4 Удаление политики соответствия ПО

Удаление политики можно выполнить следующими способами:

- удаление конкретной политики;
- массовое удаление политик;
- удаление всех политик.

Способ 1. Удаление конкретной политики:

- 1. Перейдите в раздел **Соответствие ПО** → **Наборы правил соответствия ПО**
- 2. В строке нужной политики нажмите кнопку 🔟 или перейдите на форму просмотра политики и нажмите кнопку **Удалить**.
- 3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление политик:

- 1. Перейдите в раздел Соответствие ПО Наборы правил соответствия ПО
- 2. Отметьте необходимые политики.
- 3. Нажмите кнопку Удалить.
- 4. Подтвердите удаление в открывшемся окне.

Способ З. Удаление всех политик:

- 1. Перейдите в раздел Соответствие ПО Наборы правил соответствия ПО.
- 2. Нажмите кнопку Удалите все.
- 3. Подтвердите удаление в открывшемся окне.

9. Коррелятор

9.1 Общие данные

Коррелятор предназначен для выявления последовательностей в потоке событий, отфильтрованных с помощью фильтров потока событий и удовлетворяющих условиям, описанным в правиле корреляции.

Результатом работы коррелятора является так называемая "сработка" правила корреляции, на основании которой может быть создан инцидент и проведен анализ.

Условия для "сработок" правил корреляции задаются в разделе «Правила корреляции». В общем случае правила разрабатываются на скриптовом языке Lua, но **Платформа Радар** позволяет использовать визуальный конструктор для написания правил корреляции.

Правила делятся на два вида:

- линейные используются для реагирования на определенный вид события в одном экземпляре;
- с группировкой событий используется, когда необходимо провести корреляцию над сгруппированными по какому-либо принципу событиями.

Для обращения к справочникам используются табличные списки (см. раздел «<u>Табличные</u> <u>списки</u>»). Существуют следующие действия для работы с табличными списками:

- установить значение в табличном списке;
- удалить запись из табличного списка;
- очистка табличного списка.

Для настройки условий фильтраций, который будет применяться к потоку событий, используются фильтры потока событий (см. раздел «<u>Фильтры потока событий</u>»).

Существует возможность передавать поток событий на другой узел (например, выполнена множественная установка платформы на разных узлах), то вы можете настроить пересылку событий (см. раздел «<u>Пересылка событий</u>»).

Код правила корреляции может быть расширен с помощью макросов (см. раздел «<u>Макросы</u>»). Один и тот же макрос может быть использован во множестве правил.

Платформа Радар позволяет осуществлять ретроспективный анализ – проверку гипотез на основе исторических данных, хранимых в системе. Для осуществления ретроспективного анализа можно использовать как существующие правила корреляции, так и вновь созданные (см. раздел «<u>Ретроспективная корреляция</u>»).

9.2 Правила корреляции

Для работы с правилами корреляции перейдите в раздел **Коррелятор** → **Правила корреляции** (см. «Рис. 117»).

≡	👹 ^{пангео} 172.30.254.60 🗸 Правила ко	ррел	іяци	и					Лицензия активна до: 💈	2026-02-07 ①	Документация	🔘 admin 🗸
ନ ପ ଜ ଅ	C Eesnankor 579 D Eesnankor 579 D my 1 C D Rules 1+14 V D Linux_rules 14 V D Linux_rules 14 V D Linux_rules 14	1 4 0	Пра Рильт Сорти	авила корреляции гры Папка: Без папки +4 × - чровка ↑ Название × + осить Применить	÷							
۵			7	Создать Удалить Удалить в	се Экспортирова	Экспортировать все	Импортировать	Переместить в папку			Выбрано: 0	C @
25				Название	Активное	Ретроспективное	Ошибка 📗	Тип инцидента	Папка	Сработки	Ошибки	
ж				172.30.250.107	Да	Нет		Windows -Компиляция	my	5	0	• 0 0
414				AD Windows - BloodHound из	Нет	Нет	4	Разведка Active Directory	Без папки	0	0	• 0 1
65				AD Windows - SharpShares	Нет	Нет	-	Разведка Active Directory	Без папки	0	0	@ 0 fi
w				AD Windows - Выявление	Нет	Нет		AD Windows - Выявление доступа	Без папки	0	0	◎ ⁄ ₫
	6	2		AD Windows - Дамп учетных	Нет	Нет		AD Windows - Дамп учетных	Без папки	0	0	◎ Ø 前
				AD-Windows - Запрос аномальн	Нет	Нет	4	Запрос аномально длинного име	Без папки	0	0	• 0 •
				AD Windows - Запуск BloodHou	Нет	Нет	-	Разведка Active Directory	Без папки	0	0	© 0 🖻
				AD Windows - Обнаружена атак	Нет	Нет		AD Windows - Обнаружена атака	Без папки	0	0	• 2 6

Рис. 117 – Раздел "Правила корреляции". Представление через универсальную таблицу

В разделе отображается следующая информация:

- Название наименование правила корреляции;
- Активное признак активности правила: да, нет;
- Ретроспективное используется ли правило для ретроспективной корреляции: да, нет;
- Ошибка описание ошибки инициализации правила;
- Тип инцидента наименование типа инцидента, по которому работает правило;
- **Папка** наименование папки структуры контента, в которой находится правило. Подробнее о работе с папками см. раздел «<u>Папки контента</u>».
- Сработки количество "сработок" правила;
- Ошибки количество ошибок инициализации правила;
- Обновлено дата и время изменения информации о правиле;
- Создано дата и время создания правила;
- ID идентификатор правила.

Для переключения режима просмотра правил, нажмите по названию правила в соответствующей колонке или на кнопку ^(O) в нужной строке. Откроется представление правил через боковую панель, а выбранное правило откроется на просмотр (см. «Рис. 118»).



Рис. 118 – Раздел "Правила корреляции". Представление через боковую панель

Раздел состоит из следующих блоков:

- Список правил корреляции, в котором отображается следующая информация о правилах:
 - название правила;
 - состояние правила: активно, неактивно;
 - дата последнего изменения правила;
 - количество сработок;
 - количество ошибок.
- Основное, в котором отображается общая информация о выбранном правиле.
- Статистика работы правила, в котором отображается следующая информация:
 - "Инциденты" список инцидентов, созданных на основании сработавшего правила;
 - "Результаты" список "сработок" привила;
 - "Лог изменений" история изменения правила;
 - "Лог правила" журнал работы правила;
 - "Метрики" визуализация информации о "сработках" правила в виде графиков.

9.2.1 Просмотр статистики работы правил

9.2.1.1 Вкладка "Инциденты"

На вкладке отображается список инцидентов, созданных на основе "сработок" правил (см. «Рис. 119»).

Г	Создать	удалить Удалить	все	плетрики				C
	Срочность	Уровень риска	Название	Тип инцидента	Статус	Создано	Обновлено	Актив
	0.09	2	Перебор паролей	Перебор паролей	Новый	13:52:20 28.08.2024	13:52:20 28.08.2024	172.30.249.21
	0.07	0.5	Перебор паролей	Перебор паролей	В работе	13:13:54 25.07.2024	14:36:35 16.08.2024	localhost
	0.07	0.5	Suspicious DNS request	Suspicious DNS request	Закрыт	17:01:50 11.07.2024	14:11:27 14.08.2024	localhost
	0.07	0.5	Перебор хостов	Перебор хостов	Новый	14:01:57 16.07.2024	16:34:17 16.07.2024	localhost
<	1 >	10 / страница 🗸						



Полный набор информации, отображаемы в таблице:

- Срочность цифровое и цветовое обозначение оценки срочности реагирования на инцидент;
- Уровень риска цифровое и цветовое обозначение уровня угрозы;
- Название название обнаруженной угрозы. По ссылке произойдет переход к форме просмотра инцидента;
- Тип инцидента по ссылке произойдет переход к форме просмотра типа инцидента;
- Статус текущее состояние инцидента;
- Актив техническое средство информационной системы, на котором произошел инцидент. По ссылке произойдет переход к форме просмотра актива;
- Группа инцидентов название группы, к которой относится инцидент;
- ID идентификатор инцидента;
- Последнее происшествие дата и время последнего происшествия, зарегистрированного в инциденте;
- Кол-во происшествий количество происшествий в инциденте;
- Кол-во повторных открытий количество повторных открытий инцидента;
- Пользователь наименование ответственного пользователя;
- Группа пользователей наименование ответственной группы пользователей;
- Создано дата и время создания инцидента;
- Обновлено дата и время изменения информации об инциденте;
- Категория категория инцидента;
- Эксплуатируется удаленно признак удаленной эксплуатации, возможные значение: да, нет;
- Результат анализа результат анализа инцидента (по наведению мыши во всплывающем окне отобразится полное описание).

Подробнее о работе с инцидентами см. раздел «Инциденты».

9.2.1.2 Вкладка "Результаты"

На вкладке отображается список "сработок" правила корреляции (см. «Рис. 120»).

Инциден	гы Результаты Лог изменений Лог правила Метрики				
\ \ \ \ \ \	/далить Удалить все				C
	Инцидент	Актив	Риск	Произошло	
	-	-	5 (i)	12:35:59 28.08.2024	+ ◎ ඕ
	-	-	0.5 (i)	13:14:08 25.07.2024	+ ◎ ඕ
	-	-	0.5 (1)	13:13:58 25.07.2024	+ ◎ 団
	Перебор паролей	localhost	0.5 (i)	13:13:53 25.07.2024	◎ ¹
	Сбой активации лицензий	localhost	0.5 (i)	13:09:46 25.07.2024	◎ ¹
	Сбой активации лицензий	localhost	0.5 (i)	13:09:36 25.07.2024	◎ ¹
	Сбой активации лицензий	localhost	0.5 (i)	13:09:31 25.07.2024	◎ ¹
	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 (i)	16:34:16 16.07.2024	◎ ¹
	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 (1)	16:34:06 16.07.2024	◎ ¹
	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 (i)	16:34:01 16.07.2024	◎ ¹
< 1	2 3 4 5 6 7 … 14 > 10 / страниц	a 🗸			

Рис. 120 – Просмотр статистики работы правила. Вкладка "Результаты"

Π	ทน	работе нал	записями	таблины	лоступны	слелующ	ие элементы	vπi	равления.
тт	PEL	раооте пад	SallinChillin	таолицы	доступны	следуюш	LIC STUDIETIBI	ym	равления.

Кнопка	Действие
+	создание нового инцидента на основе "сработки" правила (см. раздел « <u>Создание</u> <u>инцидента</u> »)
\odot	просмотр событий, вызвавших "сработку" правила (см. раздел « <u>Просмотр</u> <u>события</u> »)
创	удаление записи из таблицы

В списке "сработок" правила корреляции отображается следующая информация:

- Инцидент наименование инцидента, созданного на основе "сработки" правила. По ссылке произойдет переход к форме просмотра инцидента;
- Актив название актива, на котором произошла "сработка". По ссылке произойдет переход к форме просмотра актива;
- Риск уровень угрозы;
- Произошло дата и время "сработки" правила.

9.2.1.3 Вкладка "Лог изменений"

На вкладке отображается журнал изменения правила (см. «Рис. 121»).

Инциденты	Результаты	Лог изменений	Лог правила Мет	оики			
v							C
Действие	Дата с	создания	Системное	Ken	изменен	Детали	
Изменение	10:45	19 12.12.2024	Нет	adn	nin	Показать детали	
Изменение	18:12:	42 11.12.2024	Нет	adn	nin	Показать детали	
Изменение	18:12	:06 11.12.2024	Нет	adn	nin	Показать детали	
	10 / страни	ица ~					



В журнале изменений отображается следующая информация:

- Действие тип действия, выполненного над правилом;
- Дата создания дата выполнения изменения;
- Системное признак того, было ли изменение выполнено платформой;
- Пользователь пользователь, выполнивший изменение.

По кнопке Показать детали можно посмотреть детальную информацию об изменении правила.

9.2.1.4 Вкладка "Лог правила"

На вкладке отображается журнал работы правила (см. «Рис. 122»).

Инциденты	Результаты Лог изменений Лог	правила Метрики	C
Функция	Дата	Сообщение	Уровень сообщения
init	12:16:16 17.03.2025	failed to unmarshal action: json: cannot unmarshal string into Go	0 Ошибка
	10 / страница ~		О Ошиока

Рис. 122 – Просмотр статистики работы правила. Вкладка "Лог ошибок"

В журнале отображается следующая информация:

- Функция наименование функции, по которой создано сообщение;
- Дата дата и время создания сообщения;
- Сообщение текст сообщения (при наведении мыши отобразится полное описание);
- Уровень сообщения наименование категории, к которой относится сообщение. Возможные значения: Отладка (debug), Информация (info), Предупреждение (warn), Ошибка (error).

9.2.1.5 Вкладка "Метрики"

На вкладке доступны следующие визуализации метрической информации о "сработке" правила:

• скорость потока событий (см. «Рис. 123»):

Eps						
0.00000007						8
0.00000006						
0.00000005						
0.00000004						
0.00000003					8	
0.00000002						
0.00000001						
0 о о о о 11 июля 09:33 11 и	ото ото ото ото ото ото ото ото ото ото	о о о о о 11 июля 09:53	о о о о о 11 июля 10:00 11 ин	оля 10:06 11 июля 10:13	11 июля 10:20	11 июля 10:26

Рис. 123 – Метрика "EPS"

• задействованная память (см. «Рис. 124»):

Память (мб)		
0.00025		
0.0002		4
0.00015		
0.0001		
0.00005		
0 с с 11 июля 09:31	иноля 09:38 11 июля 09:45 11 июля 09:51 11 июля 09:58 11 июля 10:05 11 июля 10:11 11 июля 10:18	11 июля 10:25 11 июля 10:31

Рис. 124 – Метрика "Память"

• количество накопленных событий в группе (см. «Рис. 125»):



Рис. 125 – Метрика "Количество накопленных событий в группе"

• время выполнения функции on_logline (см. «Рис. 126»).



Рис. 126 – Метрика "Время выполнения on_logline"

• время выполнения функции on_grouped (см. «Рис. 127»).



Рис. 127 – Метрика "Время выполнения on_grouped"

• количество ошибок, возникших во время "сработок" правила (см. «Рис. 128»).



Рис. 128 – Метрика "Количество ошибок"

9.2.2 Создание и настройка правила

Создание правила можно выполнить двумя способами:

- с использованием визуального конструктора при создании правила не используется скриптовый язык, само правило настраивается с помощью визуальных блоков. При необходимости вы всегда можете конвертировать подобное правило в скриптовый язык Lua (см. раздел «Конвертирование правила в код Lua»);
- помощью скриптового языка Lua это позволяет использовать весь доступный функционал при написании правила.

9.2.2.1 Создание правила с помощью визуального конструктора

1. Нажмите кнопку ⁺. Откроется окно "Добавить правило" (см. «Рис. 129»).

Создание правила	×
Название правила	
Новое правило	
Тип инцидента	
Множественные неудачные попытки входа на одном узл	те под разными \vee
Папка	
Rules	\sim
Автоматическое создание типа инцидента	
 Использовать визуальный конструктор 	
Создать	

Рис. 129 – Окно "Добавить правило"

- 2. Укажите в окне следующую информацию:
 - в поле Название правила укажите название правила;
 - в поле Тип инцидента из выпадающего списка выберите тип инцидента;
 - в поле **Папка** из выпадающего списка выберите папку, в которую следует поместить правило после создания;
 - если исполняемое правило не относится ни к одному из типов инцидента или необходимо создать новый тип инцидента, то установите флаг Автоматическое создание типа инцидента. При создании инцидента на основе "сработки" данного правила, будет создан новый тип инцидента, которому будет присвоено наименование правила.

Примечание: *если* опция включена, то убедитесь, что наименование правила корреляции не совпадает ни с одним наименованием типа инцидента.

- установите флаг Использовать визуальный конструктор;
- нажмите кнопку Создать.
- 3. Правило будет создано и автоматически откроется визуальный конструктор.
- 4. Выполните следующие шаги по настройке правила в визуальном конструкторе:
 - Шаг 1. Заполнение основной информации о правиле;
 - Шаг 2. Настройка фильтров потока;
 - Шаг З. Настройка алерта;
 - Шаг 4. Настройка группера;

- Шаг 5. Настройка условий;
- Шаг 6. Настройка действий;
- Шаг 7. Тестирование правила.

5. После выполнения всех шагов нажмите кнопку Сохранить.

9.2.2.1.1 Шаг 1. Заполнение основной информации о правиле

Заполнение основной информации о правиле выполняется на вкладке "Основное" (см. «Рис. 130»).

новое правило							🗊 Удалит	⊸ Сохран
овное Настройка фильтр	ов потока Наст	ройка алерта	Настройка групп	ера Конструктор условий	Действия	Тестирование	,	
Основное								
Название				Папка				
Новое правило				Rules				
ипинцидента								
Множественные неудачные	попытки входа на с	одном узле под р	разными учетными	записями		О. Автома	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание	попытки входа на с	одном узле под р Использовать	разными учетными	записями) Создать результат при срабо	отке правила	Q Автома	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание	попытки входа на с	одном узле под р Использовать	разными учетными	записями) Создать результат при срабо	отке правила	Q Автома	тическое созда	ние типа инциден
ингинцидента Множественные неудачные Сбор метрик — Ретрос Описание	попытки входа на с	одном узле под р Использовать	разными учетными	записями) Создать результат при срабо	отке правила	Q ABTOMA	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание Ограничения	попытки входа на с	одном узле под р	разными учетными	записями) Создать результат при срабо	отке правила	Q ABTOMA	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание Ограничения Максимальное количество ср	попытки входа на с	одном узле под р	разными учетными	записями) Создать результат при срабо За интервал (секунд)	отке правила	ABTOMA	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание Ограничения Максимальное количество ср 0	попытки входа на с	одном узле под р Использовать — +	разными учетными	записями Создать результат при срабо За интервал (секунд) О	отке правила	 Автома Автома Автома 	тическое созда	ние типа инциден
Множественные неудачные Сбор метрик Ретрос Описание Ограничения Максимальное количество ср 0 Максимальное значение памя	попытки входа на с	одном узле под р Использовать — +	разными учетными	записями Coздать результат при срабо За интервал (секунд) 0	отке правила	 Автома Автома Автома 	тическое созда	ние типа инциден

Рис. 130 – Настройка правила. Вкладка "Основное"

- при необходимости уточните сведения, указанные в полях **Название, Папка** и **Тип инцидента**;
- для активации сбора дополнительных метрик по данному правилу установите флаг **Сбор** метрик;
- установите флаг **Ретроспективное**, если необходимо провести ретроспективный анализ по данному правилу (подробнее см. раздел «<u>Ретроспективная корреляция</u>»);
- выберите вид правила: линейное или с группировкой событий, установив переключатель **Использовать группировку** в соответствующее положение. Переключатель отвечает за доступность вкладки "Настройки группера";
- если правило при своей "сработке" должно создавать результат, то нужно установить переключатель **Создавать результат при сработке правила**, при этом открывается доступ к настройкам "алерта" где можно указать данные, которые будут сохранены в результате "сработки";

Примечание: "алерт" это функция правила коррелятора, записывающая результат сработки.

- в поле Описание укажите дополнительные сведения о правиле;
- в блоке Ограничения установите необходимые ограничения:
 - в поле Максимальное количество сработок и в поле За интервал (секунд) укажите максимальное количество "сработок", которое будет регистрироваться за период времени;
 - в поле **Максимальное значение памяти (Мб)** укажите максимальный допустимый объем памяти, который может использовать правило.

Примечание: для снятия ограничений укажите "0".

9.2.2.1.2 Шаг 2. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «Рис. 131»).

← Новое правило				前 Удалить	✓ Co	охранить
Основное Настройка фильтров потока Настройка алерта	Настройки	группера	Конструктор услов	вий Действия	Тес	тирование
Все фильтры потока		Актив	ные фильтры			
Q Название фильтра потока		Q Has	вание фильтра потока	a		
Источник событий: windows	\odot	MS Wir	ndows Defender		0	×
MS Windows Defender	0					
Пересылка нормализованных событий	0					
Создание фильтра потока Название фильтра потока						
+ Сравнение						
Создать Сбросить						

Рис. 131 – Настройка правила. Вкладка "Настройка фильтров потока"

- в блоке **Все фильтры потока** выберите фильтры, которые необходимо добавить в правило. Список добавленных в правило фильтров будет отображаться в блоке **Активные фильтры**;
- для удобства настройки доступны следующие элементы управления:

- 🔘 просмотр подробной информации о выбранном фильтре;
- Х удаление фильтра из правила.

При необходимости можно создать новый фильтр потока в блоке **Создание фильтров потока**. Инструкция по созданию фильтров потока описана в разделе «<u>Фильтры потока событий</u>».

9.2.2.1.3 Шаг 3. Настройка алерта

Если вы на первом шаге выбрали поведение: **Создавать результат при сработке правила**, то необходимо выполнить настройку на вкладке "Настройки алерта" (см. «Рис. 132»).

Новое правило								🔟 Удалить	🗸 Сохрани
новное Настройка фильтро	в потока Настр	ройка алерта Наст	ройки группера Ко	энструктор условий	Действия	Тестирование			
Настройка алерта								Выбор шаблона	~
Уровень риска						0			
Создать инцидент		Назначить инциде	ент пользователю	Логирова	ать первое и посл	еднее событие	Логировать ука 2	занное число событи	й — +
IP актива		FQDN актива		Hostname ak	стива		МАС актива		
event.dns.type		elastic_key		action			action		
Техники Mitre									
T1584, T1584.006									
Шаблон									
Описание									
									,

Рис. 132 – Настройка правила. Вкладка "Настройка алерта"

- в поле **Уровень риска** выберите цифровое обозначение уровня риска, которое будет присвоено "сработке" правила;
- установите флаг **Создать инцидент** если необходимо автоматически создавать инцидент на основании "сработки" правила;
- установите флаг **Назначить инцидент пользователю** если необходимо автоматически назначать инцидент пользователю;
- выберите количество событий, которые необходимо записывать в журнал:
 - если вы хотите записывать только первое и последнее событие, то установите соответствующий флаг;
 - в обратном случае укажите необходимое значение в поле **Логировать указанное число событий**.
- в поле **IP актива** из выпадающего списка выберите поле, которое будет выступать в качестве IP-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **FQDN актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования домена актива. Поле может являться частью сводной таблицы событий;

- в поле **Hostname актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий;
- в поле **МАС актива** из выпадающего списка выберите поле, которое будет выступать в качестве МАС-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **Техники Mitre** укажите через запятую идентификаторы техник, используемых киберпреступниками, которые описаны в базе знаний компании Mitre (подробнее см. <u>Techniques Enterprise | MITRE ATT&CK®</u>);
- в поле Шаблон укажите дополнительную информацию об "алерте".

Если у вас подготовлен шаблон, то в поле **Выберите шаблон** выберите шаблон из выпадающего списка. Все поля на вкладке будут заполнены данными из шаблона. Инструкция по созданию шаблонов "алертов" описана в разделе «<u>Шаблоны алертов</u>».

9.2.2.1.4 Шаг 4. Настройка группера

Если вы на первом шаге выбрали вид правила **С группировкой событий**, то необходимо выполнить настройку на вкладке "Настройка группера" (см. «Рис. 133»).

овное Настройка фильтров потока Настройка алерта Настрой	ки группера Конструктор условий Действия	Тестирование
Настройки группера		Выбор шаблона 🗸 🗸
руппировать по		Агрегировать по
action 🛍 elastic_key 🛍		Выбрать 🗸 Заполнить из "Группировать по
^з азмер окна группировки		Порог количества событий для срабатывания
4 -+	Минуты	1 — + 🗹 Агрегировать только уникальные событи
Otimostamp	Формат времени	107-00 (707-00)
@timestamp	Формат времени RFC3339Nano 2006-01-02T15:04:05,999999999	+07:00 (Z07:00) ~
@timestamp Использовать цепочку	Формат времени RFC3339Nano 2006-01-02T15:04:05,999999999	+07:00 (Z07:00)
@timestamp О Использовать цепочку	Формат времени RFC3339Nano 2006-01-02T15:04:05.999999999	+07:00 (Z07:00) V
©timestamp Использовать цепочку :: и + сравнение	Формат времени RFC3339Nano 2006-01-02T15:04:05.999999999	+07:00 (Z07:00) ~
@timestamp Использовать цепочку іі и + Сравнение event.application равно значению в массиве event	Формат времени RFC3339Nano 2006-01-02T15:04:05,999999999	+07:00 (Z07:00)
@timestamp Использовать цепочку :: и + Сравнение event.application равно значению в массиве event :: количество событий 1 -+	Формат времени RFC3339Nano 2006-01-02T15:04:05.999999999 ичества событий ОС Отсутствует	+07:00 (Z07:00)
@timestamp Использовать цепочку іі и + Сравнение еvent.application равно значению в массиве event ії Количество событий 1 - + І Точное совладение ког	Формат времени RFC3339Nano 2006-01-02T15:04:05.9999999999 ичества событий Отсутствует	+07:00 (Z07:00)
() Использовать цепочку () Использовать цепочку () Использовать цепочку () Использовать цепочку () ()	Формат времени RFC3339Nano 2006-01-02T15:04:05.9999999999 ичества событий Отсутствует	+07:00 (Z07:00)

Рис. 133 – Настройка правила. Вкладка "Настройка группера"

- в поле **Группировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться группировка. Можно выполнять группировку по нескольким полям;
- в поле **Агрегировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться функция агрегации. Можно выполнить агрегацию по нескольким полям;
- в поле **Размер окна группировки** укажите временной интервал, в течение которого будет выполняться группировка событий;

- в поле **Порог количества событий для срабатывания** укажите количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- для агрегации только уникальных значений установите соответствующий флаг;
- в поле **Время события** из выпадающего списка выберите поле нормализованного события, по которому будет вычисляться время события;
- в поле **Формат времени** из выпадающего списка выберите формат времени события.

Платформа поддерживает возможность отслеживания и группировки подозрительных событий, следующих одно за другим (цепочки событий).

Для этого установите переключатель **Использовать цепочку** в положение "Включен" и выполните следующие действия:

1. Нажмите кнопку + Сравнение. Откроется окно "Настроить условие" (см. «Рис. 134»).

кция сравнения	
оверить наличие в массиве	
Строка Гип выражения	Массив Тип выражения
Значение из события 🗸	Массив строк \lor
Хлюч	Значение
event.alert ~	event - +
	event.anomaly (- +

Рис. 134– Окно "Настроить условие"

- 2. Укажите в окне "Настроить условие" следующую информацию:
 - В поле **Функция сравнения** из выпадающего списка выберите функцию **Проверить наличие в массиве**;
 - В блоке Строка настройте первую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Значение из события";
 - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет выявляться цепочка событий.
 - В блоке Массив настройте вторую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Массив строк";
 - в поле **Значение** укажите массив значений, по которым должно проверяться поле, указанное в поле **Ключ**.
 - В блоке **Результат** проверьте правильность заданного выражения;
 - Нажмите кнопку Сохранить.
- 3. Добавьте необходимое количество условий цепочки событий.
4. Настройте дополнительные параметры поведения для добавленных условий цепочки событий (см. «Рис. 135»):

	elastic_key равно знач	ению в массиве	56723123476		
::	Количество событий				×
	0			0-0-0-0-	

Рис. 135 – Параметры условий цепочки событий

- в поле **Количество событий** укажите минимальное количество найденных событий, подходящих под условие для "сработки" правила;
- для включения проверки строго соответствия количества событий установите флаг **Точное совпадение количества событий**;
- для отключения проверки по выбранному условия установите переключатель **Отсутствует** в положение "Включен".

Если у вас подготовлен шаблон, то в поле **Выберите шаблон** выберите шаблон из выпадающего списка. Все поля на вкладке будут заполнены данными из шаблона. Инструкция по созданию шаблонов группировки описана в разделе «Шаблоны группировки».

9.2.2.1.5 Шаг 5. Настройка условий

Настройка условий "сработки" правила выполняется на вкладке "Конструктор условий" (см. «Рис. 136»).

← Новое	е правило		🔟 Удалить 🗸 Сохранит			
Основное	Настройка фильтров потока	Настройка алерта	Настройки группера	Конструктор условий	Действия	Тестирование
• II M (+ Сравнение + Группа X значение из IP равно event.t значение из host+username с или + Сравнение + Группа ii elastic_key существует > ii elastic_key равно warning ii elastic_key равно error > hosname равно значению в м	accиве из 3 элемента	(ов) 🗙			

Рис. 136 – Настройка правила. Вкладка "Конструктор условий"

Конструктор представляет из себя набор условий в иерархическом виде.

Правило срабатывает, когда выполнены условия в соответствии с заданной логикой.

В условиях задается сравнение выбранного поля (в **первой** части условия) с указанным значением (во **второй** части условия).

В качестве значения для **первой** и **второй** части условия в общем случае можно указать следующие параметры:

- Значение из события выбор из списка полей нормализованного события;
- Значение из табличного списка выбор из полей существующего табличного списка;
- Количество записей в табличном списке выбор табличного списка из доступных, в котором будет подсчитано количество записей;
- Ручной ввод строки произвольное выражение;
- Целое число в значении указывается целое число;
- Дробное число в значении указывается дробное число;
- Логическое значение выбор из следующих вариантов: "ложь" или "истина";
- **IP** в значении указывается IP-адрес;
- CIDR в значении указывается IP-адрес в подсети, указанный в табличном списке;
- Дата указывается дата и время;
- Отсутствие значения значение для сравнения не указывается.

Примечание доступные параметры для **первой** и **второй** части условия формируются в зависимости от выбранной функции сравнения.

При настройке сравнения используются следующие функции:

• **Проверить равенство выражений** (оператор "*равно*") - проверяется полное равенство поля указанному значению. При равенстве поля указанному значению условие считается выполненным.

Для данной функции доступна возможность не учитывать регистр для строковых значений.

- Проверить наличие значения (оператор "*существует*") проверяется существование поля. При существовании поля условие считается выполненным.
- **Проверить значение в массиве** (оператор "*равно значению в массиве*") осуществляется поиск указанного значения поля в массиве. При успешном поиске условие считается выполненным.
- Элемент массива должен иметь подстроку (оператор "является подстрокой элемента массива") проверяется вхождение значения поля в строку в указанном массиве.
- Один элемент массива должен начинаться с подстроки (оператор "является префиксом элемента массива") проверяется вхождение значения поля в начало строки каждого элемента массива.
- Один элемент массива должен заканчиваться на подстроку (оператор "является суффиксом элемента массива") проверяется вхождение значения поля в конец строки каждого элемента массива.
- Поиск подстроки в строке (оператор "имеет подстроку") проверяется вхождение подстроки в выбранное поле.
- **Строка должна проходить regexp** (оператор "*npoxodum regexp*") проверяется проверка соответствия поля регулярному выражению.

- Первое значение больше второго (оператор "больше") сравнивается поле и указанное значение. Если поле больше значения, условие считается выполненным.
- Первое значение больше или равно второму (оператор "больше или равно") сравнивается поле и указанное значение. Если поле больше или равно значению, условие считается выполненным.
- Первое значение меньше второго (оператор "*меньше*") сравнивается поле и указанное значение. Если поле меньше значения, условие считается выполненным.
- Первое значение меньше или равно второму (оператор "*меньше или равно*") сравнивается поле и указанное значение. Если поле меньше или равно значению, условие считается выполненным.
- **Строка начинается с подстроки** (оператор "*начинается с*") проверяется наличие указанного значения в начале выбранного поля.
- Строка заканчивается на подстроку (оператор "заканчивается на") проверяется наличие указанного значения в конце выбранного поля.
- Поиск значения в табличном списке (оператор "*находит*") проверяется наличие указанного значения в выбранной колонке табличного списка.

Для данной функции доступна возможность не учитывать регистр для строковых значений.

- Поиск IP в табличном списке (оператор "*находит*") проверяется наличие указанного значения IP-адреса в выбранной колонке табличного списка.
- **Значение должно быть в диапазоне** (оператор "*находится между*") сравнивается поле и указанный диапазон значений. Если поле входит в диапазон, условие считается выполненным.

Для каждой функции можно включить отрицание: "не равно", "не существует" и т.д.

Созданные условия можно сгруппировать по следующим операторам:

- И группа условий выполняется и правило срабатывает, только если выполнены все условия в группе;
- ИЛИ группа условий выполняется и правило срабатывает, если хотя бы выполнено одно условие в группе;

На вкладке доступны следующие элементы управления:

Кнопка	Действие
+ Сравнение	добавление условия сравнения
+ Группа	добавление группы условий
Обернуть в группу	добавление условия сравнения в группу
::	изменение порядка условий сравнения
×	удаление условия сравнения из правила

Кнопка	Действие
Нажатие ЛКМ на оператор И, ИЛИ	настройка поведения для выбранной группы условий
Нажатие ЛКМ на строку условия	редактирование выбранного условия

Для добавления условия выполните следующие действия:

1. Нажмите на кнопку + ^{Сравнение}. Откроется окно "Настроить условие" (см. «Рис. 137»).

кция сравнения	
роверить равенство выражений 🗸	отрицание без учета регистра
Первое	Второе
Тип выражения	Тип выражения
Значение из события 🗸	Ручной ввод строки 🗸
Ключ	Значение
@timestamp	2023-01-31T08:28:36.6214546

Рис. 137 – Окно "Настроить условие". Пример "Проверить равенство выражений"

- 2. Выберите в окне функцию сравнения и тип выражения в соответствующих блоках. Будут сформированы поля в зависимости от выбранных значений.
- 3. В сформированных полях укажите соответствующую информацию.
- 4. Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг.
- 5. В блоке Результат проверьте правильность заданного выражения.
- 6. Нажмите кнопку Сохранить.
- 7. Добавьте необходимое количество условий в правило.

Для добавления группы условий выполните следующие действия:

1. Нажмите на кнопку + Группа. Откроется окно "Настроить условие" (см. «Рис. 138»).

Настроить условие	×
Оператор	
💿 и 🔷 или 🗌 отрицание	
Сбросить	Сохранить

Рис. 138 – Добавление группы. Окно "Настроить условие"

- 2. Выберите оператор.
- 3. Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг.
- 4. Нажмите кнопку Сохранить.

9.2.2.1.6 Шаг 6. Настройка действий

При необходимости вы можете настроить действия над табличными списками при "сработке" правила.

Доступны следующие действия:

- установить значение в табличном списке;
- удалить запись из табличного списка;
- очистка табличного списка.

Все действия выполняются последовательно.

В привило можно добавить неограниченное количество действий.

Настройка действий над табличными списками выполняется на вкладке "Действия" (см. «Рис. 139»).

← Ново	ре правило				问 Удалить	🗸 Сохранить
Основное	Настройка фильтров потока	Настройка алерта	Настройки группера	Конструктор условий	Действия	Тестирование
Установ	вка значения в табличном	списке 🗸 🖻				
Табличны	й список		TTL			
host+us	ername		0		-+	
Составно	й ключ					
host	💿 Значение 🔵	Поле события				
username	• Значение	Поле события				
Колонка			Значение			
host						
удален Табличны host	ие записи из таоличного й список	списка ^ 🗸 🔟				
Составно	й ключ					
host	🔵 Значение 🛛 🧿	Поле события				
Очистк	а табличного списка \land	Ū				
Табличны	й список					
IP						
Добавити	5					

Для добавления действия над табличным списком нажмите кнопку **Добавить** и укажите информацию в соответствии с выбранным действием:

- Установка значения в табличном списке:
 - в поле **Табличный список** из выпадающего списка выберите табличный список;
 - в поле **TTL** укажите размер окна времени отбора в миллисекундах. События старше указанного времени не будут отбираться для установки значения. Значение "0" - без ограничения;
 - в поле **Составной ключ** выберите способ формирования ключа: "*по значению*" или по "*полю события*";
 - в поле **Колонка** из выпадающего списка выберите колонку, в которую будет устанавливаться значение;
 - в поле **Значение** укажите значение, которое будет устанавливаться в соответствующую колонку табличного списка.
- Удаление записи из табличного списка:
 - в поле Табличный список выберите табличный список, из которого будут удаляться значения;
 - в поле **Составной ключ** укажите ключ, по которому будут удаляться значения.
- **Очистка табличного списка** -- в поле **Табличный список** выберите табличный список, который будет очищаться при "сработке" правила.

9.2.2.1.7 Шаг 7. Тестирование правила

При тестировании правил используется тестовый набор (массив), состоящий из "логлайнов". "Логлайн" это непосредственно само событие, представленное в формате JSON.

Тестирование правила выполняется на вкладке "Тестирование" (см. «Рис. 140»).

← Необычное врем	мя входа в систему			🖻 Удалить	🗸 Сохранить
Основное Настройка фильтро	ов потока Настройка алерта	Настройки группера Ко	нструктор условий Действия	Тестирование	
Временное окно 1m	Задержка отправки 100 — +	Задержка группера 0 — -	÷	Код правила Показать код	
Тестовый набор данны	Запустить тест			Ошибки Ошибок нет	
Jorлаин { "@timestamp": 1720603009 hostname": "localhost" } }} Добавить логлайн в тестовь	Логлайн { "@ilmestamp": 1/20603009001, "event": { "field": "test" }, "target": { "host": { "ip": "127.0.0.1", "fqdn": "', hostmame": "localhost" })} Добавить логлайн в тестовый набор			Jor 1. etc. agg total: 2 for hash key	
 {"@timestamp":1720522980 {"rs_collector_hostname":"v 	0904,"event":{"field":"test"),"target":{" v-stand-09","rs_relay_fqdn":"172.30.25	nost":{"ip":"127.0.0.1","fqdn":"","ha i4.106","rs_relay_ip":"172.30.254.	ostname":"localhost"}}} ③ 💼 106";"rs_collector_ts" ③ 💼	Результаты сработки	

Рис. 140 – Настройка правила. Вкладка "Тестирование"

Для проведения тестирования выполните следующие действия:

- 1. Укажите на вкладке следующую информацию:
 - в поле Временное окно укажите размер временного окна выполнения правила корреляции;

- в поле Задержка отправки укажите время задержки отправки событий;
- в поле Задержка группера укажите время задержки работы группера;
- все значения задаются в миллисекундах.
- 2. Нажмите кнопку Запустить тест. Будут сформированы результаты проверки правила:
 - в блоке Код правила можно посмотреть код правила;
 - в блоке Ошибки будет выведен список выявленных ошибок;
 - в блок Лог отображается журнал выполнения тестирования;
 - в блоке Результаты сработки будет выведен список "сработок" правила.
- 3. При необходимости вы можете сформировать тестовый набор данных, который будет подаваться на вход правилу корреляции при выполнении тестирования. Для этого в блоке **Тестовый набор данных** укажите логлайн и нажмите кнопку **Добавить логлайн в тестовый набор**. Для управления логлайнами используйте следующие элементы управления:
 - 💿 просмотр подробной информации о выбранном логлайне;
 - 🔟 удаление логлайна из тестового набора данных.

9.2.2.2 Создание правила с помощью скриптового языка Lua

1. Нажмите кнопку +. Откроется окно "Добавить правило" (см. «Рис. 141»).

Создание правила	×
Название правила	
Новое правило	
Тип инцидента	
Множественные неудачные попытки входа на одном уз	зле под разными \vee
Папка	
Rules	~
Автоматическое создание типа инцидента	
Использовать визуальный конструктор	
Создать	

Рис. 141 – Окно "Добавить правило"

- 2. Укажите в окне следующую информацию:
 - в поле Название правила укажите название правила;
 - в поле Тип инцидента из выпадающего списка выберите тип инцидента;

- в поле **Папка** из выпадающего списка выберите папку, в которую следует поместить правило после создания;
- если исполняемое правило не относится ни к одному из типов инцидента или необходимо создать новый тип инцидента, то установите флаг Автоматическое создание типа инцидента. При создании инцидента на основе "сработки" данного правила, будет создан новый тип инцидента, которому будет присвоено наименование правила.

Примечание: если опция включена, то убедитесь, что наименование правила корреляции не совпадает ни с одним наименованием типа инцидента.

- не устанавливайте флаг Использовать визуальный конструктор;
- нажмите кнопку Создать.
- 3. Правило будет создано и автоматически откроется визуальный конструктор для настройки.
- 4. Выполните следующие шаги по настройке правила в визуальном конструкторе:
 - Шаг 1. Заполнение основной информации о правиле;
 - Шаг 2. Настройка фильтров потока;
 - Шаг З. Настройка кода правила;
 - Шаг 4. Настройка макросов;
 - Шаг 5. Тестирование работы правила.
- 5. После выполнения всех шагов нажмите кнопку Сохранить.

9.2.2.2.1 Шаг 1. Заполнение основной информации о правиле

Заполнение основной информации о правиле выполняется на вкладке "Основное" (см. «Рис. 142»).

			🔟 Удалить 🗸 Сохранить
ное Настройка фильтров пото	ка Код правила Макро	сы Тестирование	
сновное			
ізвание		Папка	
ювое правило		Rules	
п инцидента			
Иножественные неудачные попытк	ки входа на одном узле под разн	ными учетными записями	Автоматическое создание типа инцидента
Сбор метрик Ретроспектив	ное		
исание			
			<i>k</i>
граничения			
аксимальное количество сработок		За интервал (секунд)	
)	- +	0	-+
аксимальное значение памяти (Мб))		

Рис. 142 – Настройка правила на скриптовом языке Lua. Вкладка "Основное"

Укажите на вкладке следующую информацию:

- при необходимости уточните сведения, указанные в полях Название и Тип инцидента;
- в полях **Ограничение кол-во сработок в сек** и **Ограничение памяти (Мб)** установите необходимые ограничения;
- для активации сбора дополнительных метрик по данному правилу установите флаг Сбор метрик;
- установите флаг **Ретроспективное**, если необходимо провести ретроспективный анализ по данному правилу (подробнее см. раздел «<u>Ретроспективная корреляция</u>»);
- в поле Описание укажите дополнительные сведения о правиле;
- в блоке Ограничения установите необходимые ограничения:
 - в поле Максимальное количество сработок и в поле За интервал (секунд) укажите максимальное количество "сработок", которое будет регистрироваться за период времени;
 - в поле **Максимальное значение памяти (Мб)** укажите максимальный допустимый объем памяти, который может использовать правило.

Примечание: для снятия ограничений укажите "0".

9.2.2.2.2 Шаг 2. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «Рис. 143»).

новное Настройка фильтров потока Код	правила Макросы	Тестирование	
Все фильтры потока		Активные фильтры	
Q Название фильтра потока		Q Название фильтра потока	
Источник событий: windows	0	Источник событий: windows	© X
MS Windows Defender	0		
Пересылка нормализованных событий	Ø		
Создание фильтра потока			
Название фильтра потока			
+ Сравнение			

Рис. 143 – Настройка правила на скриптовом языке Lua. Вкладка "Настройка фильтров потока"

Укажите на вкладке следующую информацию:

- в блоке **Все фильтры потока** выберите фильтры, которые необходимо добавить в правило. Список добавленных в правило фильтров будет отображаться в блоке **Активные фильтры**;
- для удобства настройки доступны следующие элементы управления:
 - 🔘 просмотр подробной информации о выбранном фильтре;
 - Х удаление фильтра из правила.

При необходимости можно создать новый фильтр потока в блоке **Создание фильтров потока**. Инструкция по созданию фильтров потока описана в разделе «<u>Фильтры потока событий</u>».

9.2.2.3 Шаг 3. Настройка кода правила

На данном шаге выполняются основные настройки правила с помощью скриптового языка Lua.

Для настройки кода правила перейдите на вкладку "Код правила" и укажите соответствующий код (см. «Рис. 144»).

← №	К Множественные неудачные попытки входа					🔟 Удалить	🗸 Сохранить
Основно	be	Настройка фильтров потока	Код правила	Макросы	Тестирование		
1	loca	l detection windows = "1s"					
2	loca	l create incident = false					
3	loca	l assign to customer = false					
4	loca	l risk_score = 2					
5	loca	<pre>l grouped_by = {"initiator.ip"</pre>	, "initiator.f	qdn"}			
6	loca	<pre>l aggregated_by = {"target.ip"</pre>	, "target.port	"}			
7	loca	l grouped_time_field = "" -					
8	loca	l template = ""					
9							
10	func	tion on_logline(logline)					
11		grouper1:feed(logline)					
12	1.	end					
13	ena						
14	func	tion on grouped(grouped)					
15	Tunc	log("agg_total: "grouped)	rogatodData ag	areasted tota	" for bash koy "	grouped key)	
17		iog(agg totalgrouped.agg	regateubata.ag	gi egateu, tota	L. TOF Hash Key	grouped.key)	
18		if grouned aggregatedData aggr	egated total >	= 5 then			
19		п Біопрептаврі свассарасатаврі	cguccu.cocur y	- 5 chen			
20		alert({					
21		template = template,					
22		risk level = 2.5,					
23		asset ip = "127.0.0.1"	,				
24		asset_hostname = "loca	lhost",				
25		asset_fqdn = "localhos	t.pgr.local",				
26		asset_mac = "",					
27		create_incident = fals	e,				
28		assign_to_customer = f	alse,				
29		logs = grouped.aggrega	tedData.loglin	es,			
30		<pre>meta = {},</pre>					
31		trim_logs = 2,					
20		1)					

Рис. 144 – Настройка правила на скриптовом языке Lua. Вкладка "Код правила"

9.2.2.4 Шаг 4. Настройка макросов

При необходимости использовать один и тот же код в разных правилах корреляции, можно подключить соответствующий макрос

Подключение макросов выполняется на вкладке "Макросы" (см. «Рис. 145»).

← Множественные неудачные попытки вхо	рда
Основное Настройка фильтров потока Код правила Макросы	Тестирование
Все макросы	Активные макросы
Q Название макроса	Q Название макроса
Statistical Control of Control	© Logline X
• Новый	
Logline	
 function on_logline(logline) logline:raw() get raw logline (string) loglin:get("path") get value (string, number) for path 	I from logline
<pre>5 for i=1,20 do 6 logline:get("initiator.fqdn" tostring(i))</pre>	
7 end	
<pre>9 if logline:get("initiator.fqdn") == "pgr.local" then</pre>	
10 grouper1:feed(logline)	
11 end	
13 end	

Рис. 145 – Настройка правила на скриптовом языке Lua. Вкладка "Макросы"

Укажите на вкладке следующую информацию:

- в блоке **Все макросы** выберите макросы, которые необходимо добавить в правило. Список добавленных в правило макросов будет отображаться в блоке **Активные макросы**;
- для удобства настройки доступны следующие элементы управления:
 - 💿 просмотр подробной информации о выбранном макросе;
 - Х удаление макроса из правила.

Инструкция по созданию макросов описана в разделе «Макросы».

9.2.2.5 Шаг 5. Тестирование работы правила

При тестировании правил используется тестовый набор (массив), состоящий из "логлайнов". "Логлайн" это непосредственно само событие, представленное в формате JSON.

Тестирование правила выполняется на вкладке "Тестирование" (см. «Рис. 146»).

← Множественные неудачные попытки входа								
Основное Настройка фильтров потока Код правила Макросы Тестирование								
Временное окно Задержка отправки Задержка группера 1m 100 - + 0 - +		Ошибки Ошибок нет						
Запустить тест		Лог						
Тестовый набор данны: Логлайн	x	 во аду клас 2 тог пакт кеу Результаты сработки 						
Добавить логлайн в тестовы 1. ("@timestamp":1720603009	א אפולסף ווו אפולסף 2001,"event":{"field":"test"),"target":{"host":("ip":"127.0.01","fiqdn":"","hostname":"localhost")}} @ 🙆							

Рис. 146 – Настройка правила на скриптовом языке Lua. Вкладка "Тестирование"

Для проведения тестирования выполните следующие действия:

- 1. Укажите на вкладке следующую информацию:
 - в поле **Временное окно** укажите размер временного окна выполнения правила корреляции;
 - в поле Задержка отправки укажите время задержки отправки событий;
 - в поле Задержка группера укажите время задержки работы группера;
 - все значения задаются в миллисекундах
- 2. Нажмите кнопку Запустить тест. Будут сформированы результаты проверки правила:
 - в блоке Ошибки будет выведен список выявленных ошибок;
 - в блок Лог отображается журнал выполнения тестирования;
 - в блоке **Результаты сработки** будет выведен список "сработок" правила.
- 3. При необходимости вы можете сформировать тестовый набор данных, который будет подаваться на вход правилу корреляции при выполнении тестирования. Для этого в блоке **Тестовый набор данных** укажите логлайн и нажмите кнопку **Добавить логлайн в тестовый набор**. Для управления логлайнами используйте следующие элементы управления:
 - 🔘 просмотр подробной информации о выбранном логлайне;
 - 🔟 удаление логлайна из тестового набора данных.

9.2.3 Редактирование правила

- 1. Выберите из списка необходимое правило и нажмите кнопку Открыть редактор
- 2. В зависимости от типа редактируемого правила (с использованием визуального редактора или без) внесите необходимые изменения на соответствующие вкладки.
- 3. Нажмите кнопку Сохранить.

9.2.4 Активация правила

- 1. Выберите из списка необходимое правило и установите переключатель положение **Активное**.
- 2. Если в правиле были допущены ошибки, то платформа выдаст соответствующее предупреждение.
- 3. После активации правило включится в работу на потоке событий используя указанные фильтры. Если при инициализации правила произойдет какая-либо ошибка, то правило будет автоматически деактивировано.

9.2.5 Перезапуск правила

- 1. Выберите из списка необходимое правило и нажмите кнопку
- 2. Подтвердите перезапуск в открывшемся окне.
- 3. Правило будет перезапущено.

9.2.6 Дублирование правила

1. Выберите из списка необходимое правило, нажмите кнопку списка выберите пункт **Дублировать**. Откроется окно "Дублировать правило" (см. «Рис. 147»).

Дублировать правило		×
Название правила		
Необычное время входа в систему - Дубль		
	Сбросить	Дублировать

Рис. 147 – Окно "Дублировать правило"

- 2. Укажите в окне наименование правила.
- 3. Нажмите кнопку Дублировать.

9.2.7 Конвертирование правила в код Lua

При необходимости **Платформа Радар** позволяет конвертировать правила, созданные с помощью визуального конструктора, в скриптовой язык Lua.

Внимание! обратное конвертирование из Lua в визуальный режим не поддерживается, рекомендуется перед конвертированием продублировать правило (сделать резервную копию).

- 1. Выберите из списка правило, которое было создано с помощью визуального конструктора.
- 2. Нажмите кнопку *и* из выпадающего списка выберите пункт **Конвертировать в Lua**.
- 3. Подтвердите конвертацию в открывшемся окне.

9.2.8 Импорт правил

- 1. Нажмите на кнопку 🗹 и из выпадающего списка выберите пункт Импортировать.
- 2. В открывшемся окне укажите путь к архиву с правилами.
- 3. Нажмите кнопку Открыть.

9.2.9 Экспорт правил

- 1. Нажмите на кнопку и из выпадающего списка выберите пункт Экспортировать все.
- 2. Будет сформирован архив с правилами корреляции в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

9.2.10 Удаление правила

Удаление правила можно выполнить двумя способами.

Способ 1:

1. Выберите из списка необходимое правило, нажмите кнопку *и* из выпадающего списка выберите пункт **Удалить**.

🗓 Удалить

- 2. Подтвердите удаление в открывшемся окне.
- 3. Правило будет удалено из платформы.

Способ 2:

- 1. Выберите из списка необходимое правило, нажмите кнопку
- 2. В окне редактирования правила нажмите кнопку
- 3. Подтвердите удаление в открывшемся окне.
- 4. Правило будет удалено из платформы.

9.2.11 Массовые действия над правилами

Над правилами доступны следующие массовые действия:

- Экспортировать экспорт выбранных правил;
- Удалить удаление выбранных правил;
- Удалить все удаление всех правил.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку . Откроется список массовых операций и флаги для выбора правил (см. «Рис. 148»).



Рис. 148 – Массовые действия над правилами

- 2. Выберите правила корреляции.
- 3. Нажмите на соответствующую кнопку.
- 4. Завершите действие в открывшемся окне.

9.2.12 Действия над результатами сработок правила

9.2.12.1 Создание инцидента

- 1. Выберите из списка необходимое правило.
- 2. Перейдите на вкладку "Результаты".
- 3. Выберите из списка необходимую "сработку" правила и нажмите кнопку +.
- 4. Будет создан инцидент на основании "сработки" правила.

9.2.12.2 Просмотр события

- 1. Выберите из списка необходимое правило.
- 2. Перейдите на вкладку "Результаты".
- 3. Выберите из списка необходимую "сработку" правила и нажмите кнопку **Показать событие**. Откроется страница просмотра события (см. «Рис. 149»).



Рис. 149 – Просмотр события

4. Для просмотра события в разделе **Просмотр событий** нажмите кнопку (20), а для просмотра всех событий нажмите кнопку **Просмотреть все**. Откроется поток событий, который будет сформирован по соответствующему запросу.

Фильтры Пресеты							О Остория
Автообновление данных							
Выкл 🗸 🖓		Поток событий, 5 сент. (15:09:24)	- 5 сент. (15:09:24)				По месяцам — — — —
Период							其 은 恒
Когда событие было зарегистрировано в системе		2					
Последние 3 года 📋							
Нормализованное событие							
Не важно \lor							
Запрос Сохраненные запросы > ☐ Сохранить выбор как ④ Добавить запрос		1					
еvent.uuid один из	8						
Агрегация Сохраненные агрегации >		0 2022	Июл	2023	Июл	2024	Июл
🕀 Добавить агрегацию		Ú.					¢
		Топ 10 طி Столбчатая диаграмма					×

Рис. 150 – Просмотр потока событий по соответствующему запросу

9.3 Пересылка событий

9.3.1 Общие данные

Если **Платформа радар** работает в режиме мультиарендности, то вы можете настроить пересылку событий с одного экземпляра платформы на другой.

При включенной пересылке все события будут отправляться на другой узел.

За пересылку отвечает фильтр потока событий, не связанный с правилом корреляции. Подобный фильтр создается в разделе **Коррелятор** → **Пересылка событий** (см. «Рис. 151»).

≡).254.97 🗸 Пересылка со	бытий		Ли	цензия акти	ивна до: 2027-11-16	④ Документация	(admi	in 🗸
â	Пересы	лка событий								
Q										
(j)	Г Созда	ать Удалить Удалить все Эко	спортировать Экс	портировать все	Импортировать			Выбрано: 0	C	Ø
-T		Название фильтра	↓ ↑	Создано			Обновлено			
40		Cisco IOS		2025-04-29 11:3	6:34		2025-04-29 11:36:34		© 0	۵
ů		Нормализованные события		2025-04-29 11:3	8:03		2025-04-29 11:38:03		• 0	Û
₩.	< 1	> 50 / страница ~								
ж										
441										
Ø										

Рис. 151 – Раздел "Пересылка событий"

В разделе отображается следующая информация:

- Название фильтра наименование фильтра для пересылки событий;
- Создано дата и время создания фильтра;
- Обновлено дата и время обновления фильтра.

9.3.2 Включение пересылки событий

- 1. В веб-интерфейсе платформы перейдите в раздел **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**.
- 2. Включите пересылку событий. Для этого в древовидном списке параметров сервисов выберите **FlowBalancer** → **Head** и установите параметр **Пересылать события** в значение true, а в поле **Ip LogProxy** укажите IP-адрес узла, на который необходимо пересылать события (см. «Рис. 152»).

^{дантео} 172.30.249.21 ∨ Управление конфигурацией		Лицензия активна до: 2025-08-16 🕕 Документация
Уалы системы Управление конфигурацией АРІ ключи Учетня	е записи для сбора данных Планировщик задач Скрипты Управление мультиарендностью	
писок свойств конфигураций		Записать конфигурацию
> EventAnt - FlowBalancer (1)	Head > Пересылать события Пересылать события Бересылать события	История изменений
Интервал коммита событий (с)	true faise	~ 2024-12-10 10:26:56
FlowBalancer. Commitinterval		Пользователь: admin 1 изм. Обновление
Уровень логирования RowBilancer.LogLevel	Сбросить Сохранить	Уровень логирования ClusterAgentLogLevel
V Head 2	Переопределение параметров узлов	ctano: info
Ip LogProxy FlowBatancer.Head.lp	Ysen: master ~	✓ 2024-12-06 15:14:53 Пользователь: admin 1 изм. Обновление
ID события для номализованных событий LogProxy	Имя параметра:	Стандартный запуск/режим отладки
FlowBalancer.Head.Messageld	Выбрать 🗸	Cerberus.Mode 6ыло: release
ID события для разобраных событий LogProxy FlowBatancer.Head.MessageldParsed	Добавить	 2024-12-06 15:14:18
Nopt LogProxy FlowBalancetHead.Port	Сбросить Сохранить	Пользователь: admin 1 изм. Обновление
Пересылать события		IP адрес сервиса Cerberus.lp
FlowBalancer.Head.Used		было: 127.0.0.3 стало: 127.0.0.1
Использовать TLS шифрование FlowBatencer.Head.UseSSL		· 2024-12-06 15:14:10
> Frontend		Пользователь: admin 1 изм. Обновление
> sender Grafana		Cerberus.lp 6uno: 127.02
KafkaExporter		стало: 127.0.0.3
> Kafka		2024-12-06 15:13:56

Рис. 152 – Управление конфигурацией сервиса FlowBalancer

- 3. При необходимости переопределите следующие параметры: Порт LogProxy, ID события для нормализованных событий LogProxy, ID события для разобранных событий LogProxy. Подробнее о настройке сервиса **Log-proxy** см. раздел документ «Работа с источниками событий ИБ».
- 4. После внесения изменений нажмите кнопку Записать конфигурацию.
- 5. Перейдите в раздел **Коррелятор** → **Пересылка событий** и создайте фильтр для пересылки событий с необходимыми параметрами (см. раздел «<u>Создание фильтра для пересылки</u> <u>событий</u>»).

Проверка работы пересылки событий:

- 1. Включите пересылку событий.
- 2. Перейдите в раздел **Коррелятор** → **Пересылка событий** и создайте фильтр со следующими параметрами (см. «Рис. 153»):
 - Функция сравнения -- "Проверить равенство выражений";
 - Тип выражения -- "Значение из события" и "Ручной ввод строки" соответственно;
 - Ключ -- "elastic_key";
 - **Значение** -- "normalized".

Настроить условие	×
Функция сравнения	
Проверить равенство выражений 🗸	отрицание
Первое Тип выражения Значение из события	Второе Тип выражения Ручной ввод строки
Ключ elastic_key	Значение normalized
Результат: elastic_key равно normalized	Сбросить Сохранить

Рис. 153 – Настройка фильтра для пересылки нормализованных событий

- 3. Включите поток событий на основной узел.
- 4. На удаленном (дополнительном) узле перейдите в раздел **Просмотр событий** и удостоверьтесь, что пришедшие нормализованные события изначально отправлялись на основной узел.

9.3.3 Просмотр фильтра для пересылки событий

Для просмотра фильтра для пересылки событий нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название фильтра**. Откроется представление через боковую панель и форма просмотра выбранного фильтра (см. «Рис. 154»).



Рис. 154 – Форма просмотра фильтра для пересылки событий

В боковой панели отображается следующая информация:

- название фильтра для пересылки событий;
- количество событий, попавших под условия фильтра;
- количество отброшенных событий;
- дата и время изменения информации о фильтре.

В рабочей области отображаются условия фильтрации. Условия могут принимать следующие значения:

- равно для условия выполняется функция проверки равенства выражений;
- равно значению в массиве для условия выполняется функция проверки наличия значения в массиве данных;
- имеет подстроку для условия выполняется функция поиска подстроки в строке;
- оператор "не" означает что выполняется отрицание при выполнении функции: "не равно", "не равно значению в массиве", "не имеет подстроку".

9.3.4 Создание фильтра для пересылки событий

1. Начните процесс создания фильтра через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание фильтра потока" (см. «Рис. 155»).

≡	Каралар 172.30.254.138 ∨ Пере	есылка событий	$()$ База знаний (Q) admin \vee
â	8 7° 🗹 C +	 Создание фильтра потока 	Сбросить Создать
Q	Cisco IOS		
(i)	Изменено: 2024-09-05 16:07:37	Название фильтра	
0	Пересылка событий Windows	Пересылка нормализованных событий	
⊊Ē	Изменено: 2024-09-05 16:04:56		
¢		+ Сравнение :: elastic key равно normalized ×	
<i>7</i> ÷			
X			
494			
Ø			

Рис. 155 – Форма "Создание фильтра для пересылки событий"

2. В поле **Название** укажите название фильтра и добавьте условие для сравнения нажав на кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 156»).

нкция сравнения	
роверить равенство выражений — — — — — — — — — — — — — — — — — — —	отрицание
Первое	Второе
Тип выражения	Тип выражения
Значение из события 🗸	Ручной ввод строки
Ключ	Значение
elastic_key	normalized

Рис. 156 – Окно "Настроить условие"

- 3. Укажите в окне "Настроить условие" следующую информацию:
 - В поле Функция сравнения из выпадающего списка выберите функцию сравнения:
 - "Проверить равенство выражений";
 - "Проверить наличие в массиве";
 - "Поиск подстроки в строке".
 - Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг;
 - В блоке **Первое** настройте первую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Значение из события";
 - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет происходить фильтрация.
 - В блоке Второе настройте вторую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Ручной ввод строки";
 - в поле Значение укажите значение, по которому должно проверяться поле указанное в поле Ключ. Если выбрана функция "Проверить наличие в массиве", то укажите массив значений.
 - В блоке **Результат** проверьте правильность заданного выражения.
 - Нажмите кнопку Сохранить.
- 4. Добавьте необходимое количество условий в фильтр для пересылки событий.
- 5. Нажмите кнопку Сохранить.

9.3.5 Редактирование фильтра для пересылки событий

1. Начните процесс редактирования фильтра через «универсальные таблицы» или инструмент «боковая панель».

- 2. Внесите необходимые изменения:
 - для добавления нового условия нажмите кнопку + Сравнение;
 - для изменения условия нажмите по строке выбранного условия;
 - для изменения порядка условий используйте кнопку ;
 - для удаления условия из фильтра используйте кнопку X.
- 3. Нажмите кнопку Сохранить.

9.3.6 Дублирование фильтра для пересылки событий

1. Откройте фильтр на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать фильтр потока событий" (см. «Рис. 157»).

Дублировать фильтр потока собы	гий	×
Название фильтра потока событий		
Пересылка нормализованных событий - Ду	бль	
	Сбросить	Дублировать

Рис. 157 - Окно "Дублировать фильтр потока событий"

- 2. Укажите в окне наименование фильтра.
- 3. Нажмите кнопку Дублировать.

9.3.7 Импорт фильтров

- 1. Начните процесс импорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
- 2. В открывшемся окне укажите путь к архиву с фильтрами.
- 3. Нажмите кнопку Открыть.

9.3.8 Экспорт фильтров

- 1. Начните процесс экспорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
- 2. Будет сформирован архив с фильтрами в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

9.3.9 Удаление фильтра

- 1. Начните процесс удаления фильтра через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Фильтр будет удален из платформы.

9.4 Фильтры потока событий

9.4.1 Общие данные

Фильтры отвечают за фильтрацию потока событий по заданным условиям.

Для работы с фильтрами перейдите в раздел **Коррелятор** → **Фильтры потока событий** (см. «Рис. 158»).

≡	Пангео 172.3	0.254.97 🗸 🕴 Фильтры потока событий	Лицензия активна до: 2027	- 11-16 ① Документация	\bigotimes admin \lor
â	Фильтр	ы потока событий			
Q					
(1)		ать Удалить Удалить все Экспортировать Экспортирова	ать все Импортировать	Выбрано: С	C @
<u>ط</u> ٩		Название фильтра	Создано	Обновлено	
40		add_and_remove	2023-04-19 18:27:18	2025-03-07 17:42:59	◎ Ø 前
Ĵ		antivirus (all events)	2023-10-03 14:30:05	2025-03-07 17:42:54	◎ ⁄ 前
%		Antivirus (detect)	2023-10-03 13:12:26	2025-04-02 13:52:01	◎ ⁄ أأ
Ж		antivirus (detect/delete/clean/quarantine)	2023-04-18 17:24:57	2025-03-07 17:42:58	◎ ⁄⁄ أأ
441		antivirus_protection	2024-01-25 12:16:04	2025-04-02 13:51:47	◎ ⁄ أأ
		auditd - command_execution	2023-09-19 17:12:33	2025-04-02 13:53:36	◎ ⁄ 前
Ø		auditd_download_and_bash	2024-07-30 13:49:53	2025-04-02 13:52:27	◎ ⁄ 前
		auditd - execve	2024-07-23 14:14:45	2025-04-02 13:52:16	◎ ⁄ أأ
	< 1	2 3 4 5 > 50 / страница ~			

Рис. 158 – Раздел "Фильтры потока событий"

В разделе отображается следующая информация:

- Название фильтра наименование фильтра потока событий;
- Создано дата и время создания фильтра;
- Обновлено дата и время обновления фильтра.

9.4.2 Просмотр фильтра потока событий

Для просмотра фильтра потока событий нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название фильтра**. Откроется представление через боковую панель и форма просмотра выбранного фильтра (см. «Рис. 159»).

≡	Кангео 172.30.254.138 ∨ Филь	гры потока событий		 База знаний 	🔕 admin 🗸
â	8 7 Ø C +	windows_eventlog	🔟 Удалить	Дублировать	Редактировать
Q	Событий: 0 (0 EPS); Отброшено: 100 % Изменено: 2024-01-12 12:54:59	Связанные правила			
(j)	MS-WIN-DEF virus detect	errorRule			
Ç.	Событий: 0 (0 EPS); Отброшено: 100 % Изменено: 2023-11-22 12:08:54	identityRUle			
ð	windows_eventlog	События Windows			
<i>%</i>	Событий: 39 (0 EPS); Отброшено: 0 % Изменено: 2024-09-04 17:05:19	event logsource product равно windows			
3K	MS-WIN-user_unlock				
~	Событий: 0 (0 EPS); Отброшено: 100 % Изменено: 2024-02-12 00:08:49				
ŧţţ	Communication_teredo				
Ø	Событий: 0 (0 EPS); Отброшено: 100 % Изменено: 2024-03-27 12:17:05				

Рис. 159 – Форма просмотра фильтра потока событий

В боковой панели отображается следующая информация о фильтрах:

- наименование фильтра;
- количество событий, попавших под условия фильтра;
- количество отброшенных событий;
- дата и время последнего изменения фильтра.

В рабочей области отображается следующая информация о выбранном фильтре:

- список правил корреляции, в которых используется фильтр потока событий;
- список условий, заданных для фильтра. Условия могут принимать следующие значения:
 - равно для условия выполняется функция проверки равенства выражений;
 - равно значению в массиве для условия выполняется функция проверки наличия значения в массиве данных;
 - имеет подстроку для условия выполняется функция поиска подстроки в строке;
 - оператор "не" означает что выполняется отрицание при выполнении функции: "не равно", "не равно значению в массиве", "не имеет подстроку".

9.4.3 Создание фильтра потока событий

1. Начните процесс создания фильтра через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создание фильтра потока" (см. «Рис. 160»).

← Создание фильтра потока	Сбросить	Создать
Название		
MS Windows Defender		
+ Сравнение ::: event.logsource.name равно windows-defender × ::: event.logsource.vendor равно microsoft × ::: observer.event.id равно значению в массиве из 4 элемента(ов) × ::: event.logsource.product не имеет подстроку wondows 11 ×		

Рис. 160 – Окно "Создание фильтра потока"

2. В поле **Название** укажите название фильтра и добавьте условие для сравнения нажав на кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 161»).

нкция сравнения	
роверить равенство выражений 🗸	отрицание
Первое	Второе
Тип выражения	Тип выражения
Значение из события 🗸	Ручной ввод строки 🗸
Ключ	Значение
event.logsource.name	windows-defender

Рис. 161 – Окно "Настроить условие"

- 3. Укажите в окне "Настроить условие" следующую информацию:
 - В поле **Функция сравнения** из выпадающего списка выберите функцию сравнения:
 - "Проверить равенство выражений";
 - "Проверить наличие в массиве";
 - "Поиск подстроки в строке".
 - Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг;
 - В блоке **Первое** настройте первую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Значение из события";
 - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет происходить фильтрация.
 - В блоке Второе настройте вторую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Ручной ввод строки";

- в поле Значение укажите значение, по которому должно проверяться поле, указанное в поле Ключ. Если выбрана функция "Проверить наличие в массиве", то укажите массив значений.
- В блоке **Результат** проверьте правильность заданного выражения.
- Нажмите кнопку Сохранить.
- 4. Добавьте необходимое количество условий в фильтр потока событий.
- 5. Нажмите кнопку Сохранить.

9.4.4 Редактирование фильтра потока событий

- 1. Начните процесс редактирования фильтра через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения:
 - для добавления нового условия нажмите кнопку + Сравнение;
 - для изменения условия нажмите по строке выбранного условия;
 - для изменения порядка условий используйте кнопку ;;
 - для удаления условия из фильтра используйте кнопку X.
- 3. Нажмите кнопку Сохранить.

9.4.5 Дублирование фильтра потока событий

1. Откройте фильтр на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать фильтр потока событий" (см. «Рис. 162»).



Рис. 162 – Окно "Дублировать фильтр потока событий"

- 2. Укажите в окне наименование фильтра.
- 3. Нажмите кнопку Дублировать.

9.4.6 Импорт фильтров потока событий

- 1. Начните процесс импорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
- 2. В открывшемся окне укажите путь к архиву с фильтрами.
- 3. Нажмите кнопку Открыть.

9.4.7 Экспорт фильтров потока событий

- 1. Начните процесс экспорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
- 2. Будет сформирован архив с фильтрами в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

9.4.8 Удаление фильтра потока событий

- 1. Начните процесс удаления фильтра через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Фильтр будет удален из платформы.

9.5 Макросы

9.5.1 Общие данные

Макросы – это подключаемые общие модули к правилам корреляции, которые могут содержать, как и переменные, так и расширять функционал с помощью функций.

Если вы хотите установить для разных правил модуль с одинаковым поведением, то подключите соответствующий макрос к правилам.

Макросы, как и правила корреляции, разрабатываются на скриптовом языке Lua.

Для работы с макросами перейдите в раздел **Коррелятор** → **Макросы** (см. «Рис. 163»).

≡	Радар 172.30	0.254.97 ∨ ∣ Макросы		Лицензия	я активна до: 2027-11-16 🕕 Документация	8	admin \checkmark						
â	Макрос	ы											
Q													
0	Фильтры +												
đ	Сортировка	Сортировка 1 Название × +											
-	Сбросить Применить												
ů	Г Созда	ать Удалить Удалить все Экспортировать Экспорт	ировать все Импортировать		Выбрано:	0 C	۵						
%		Название ↓↑	Создано		Обновлено 🗸								
ж		Logline	2025-04-29 14:22:37		2025-04-29 14:22:37	© (夕 茴						
49J		Windows logs	2025-04-29 14:23:32		2025-04-29 14:23:32	© (2 前						
Ø	< 1	>											

Рис. 163 – Раздел "Макросы"

В разделе отображается следующая информация:

- Название наименование макроса;
- Создано дата и время создания макроса;
- Обновлено дата и время обновления макроса.

9.5.2 Просмотр макроса

Для просмотра макроса нажмите кнопку В нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного макроса (см. «Рис. 164»).

	<mark>₩ радар</mark> 172.30.254.138 ∨ Мак	росы		⑤ База знаний	\mid (Q) admin \vee
ھ م	8 7 0 C +	Logline	🖻 Удалить	Дублировать	Редактировать
1	Logline Изменено: 12.07.2024 15:59:02	<pre>1 function on_logline(logline) 2 logline:raw() get raw logline (string) 3 loglin:get("path") get value (string, number) for path from logline 4</pre>			
ð	Новый Изменено: 12.07.2024 15:59:16	<pre>5 for i=1,20 do 6 logline:get("initiator.fqdn" tostring(i)) 7 end 8</pre>			
**		9 if logine:get('initiator.tqdn') == "pgr.local" then 10 grouper1:feed(logline) 11 end 12 13 end			÷
4 1 4					
۵					

Рис. 164 – Форма просмотра макроса

В боковой панели отображается следующая информация о макросах:

- наименование макроса;
- дата и время последнего изменения макроса.

В рабочей области отображается тело макроса.

9.5.3 Создание макроса

1. Начните процесс создания макроса через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создание макроса" (см. «Рис. 165»).

← Co	оздание макроса	Сбросить Сохранить					
Название							
Logline							
1	function on_logline(logline)						
2	logline:raw() get raw logline (string)						
3	loglin:get("path") get value (string, number) for path from logline						
4							
5	for i=1,20 do						
6	<pre>logline:get("initiator.fqdn" tostring(i))</pre>						
7	end						
8							
9	if logline:get("initiator.fqdn") == "pgr.local" then						
10	grouper1:feed(logline)						
11	end						
12							
13	end						



2. Укажите в окне название и код макроса.

3. Нажмите кнопку Сохранить.

9.5.4 Редактирование макроса

- 1. Начните процесс редактирования макроса через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

9.5.5 Дублирование макроса

1. Откройте макрос на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать макрос" (см. «Рис. 166»).

Сбросить Дублировать

Рис. 166 – Окно "Дублировать макрос"

- 2. Укажите в окне наименование макроса.
- 3. Нажмите кнопку Дублировать.

9.5.6 Импорт макросов

- 1. Начните процесс импорта макросов через «универсальные таблицы» или инструмент «боковая панель».
- 2. В открывшемся окне укажите путь к архиву с макросами.
- 3. Нажмите кнопку Открыть.

9.5.7 Экспорт макросов

- 1. Начните процесс экспорта макросов через «универсальные таблицы» или инструмент «боковая панель».
- 2. Будет сформирован архив с макросами в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

9.5.8 Удаление макроса

- 1. Начните процесс удаления макроса через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Макрос будет удален из платформы.

9.6 Шаблоны алертов

9.6.1 Общие данные

При настройке правила корреляции вы можете использовать заранее подготовленные шаблоны "алертов", в которых можно настроить следующее поведение при сработке правила:

- присвоение уровня риска;
- автоматическое создание инцидента;
- автоматическое назначение инцидента пользователю.

Для работы с шаблонами "алертов" перейдите в раздел **Коррелятор** → **Шаблоны алертов** и выберите шаблон из списка (см. «Рис. 167»).

≡	🏅 радар 172.30.254.97 🗸 Шаблоны алерт	ия активна до: 2027-11-16	🛛 🛈 Документация 📔	(Q) admin ~									
â	Шаблоны алертов	Шаблоны алертов											
Q													
Ū	Фильтры +												
đ	Сортировка												
	Сбросить Применить												
۵	Создать Удалить Удалить все							Выбрано:	0 0 0				
*	Название	† Уровень риска 👫	FQDN	Hostname	IP	MAC	Обновлено	Создано					
ж	Авто создание инцидента	3	-	-	elastic_key	-	2025-04-29 14:50:35	2025-04-09 14:04:45	© / 11				
498	Anept no elastic_key	3	@timestamp	elastic_key	action	elastic_key	2025-04-29 14:50:03	2025-04-09 14:04:38	© Ø û				
0	< 1 > 50 / страница >												

Рис. 167 – Раздел "Шаблоны алертов"

В разделе отображается следующая информация:

- Название наименование шаблона "алерта";
- Уровень риска цифровое обозначение уровня угрозы, которое будет присвоено инциденту в результате "сработки" правила;
- **FQDN** поле события, которое будет определяться как FQDN актива;
- **Hostname** поле события, которое будет определяться как Hostname актива;
- **IP** поле события, которое будет определяться как IP-адрес актива;
- МАС поле события, которое будет определяться как МАС-адрес актива;
- Обновлено дата и время изменения информации о шаблоне;
- Создано дата и время создания шаблона.

9.6.2 Просмотр шаблона "алерта"

Для просмотра шаблона нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного шаблона (см. «Рис. 168»).

≡	👹 ранеео 172.30.254.138 ∨ Шан	блоны алертов								⑤ База знаний	🔘 admin ~
â	8 7 Ø C +	Авто создани	е инцидента					Û	Удалить	Дублировать	Редактировать
Q	Авто создание инцидента										
0	Изменено: 2024-09-06 09:53:45	Уровень риска									
¢0	Проверка времени операции Изменено: 2024-09-06 09:54:43	0 1	2	3	4	5	6	7	े 8		9 10
ð		🗸 Создать инцидент		Назначить инци	идент пользователю	Ло	гировать первое и пос	леднее событие	Логиров	ать указанное чис	ло событий
%									2		-+
×		IP актива		FQDN актива		Hostn	ame актива		МАС акт	ива	
+14		elastic_key		action		~ ever	nt.application.risk		@time:	stamp	
۵	0	Техники Mitre									

Рис. 168 –Форма просмотра шаблона «алерта»

В боковой панели отображается следующая информация о шаблонах:

- наименование шаблона;
- дата и время последнего изменения шаблона.

В рабочей области отображается структура данных и внешний вид шаблона.

9.6.3 Создание шаблона "алерта"

1. Начните процесс создания шаблона через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создать шаблон" (см. «Рис. 169»).

← Создат	ь шаблон										Создать		
Название шаблона	а												
Авто назначение	9												
Уровень риска													
0	0 1	2	3	4	5		6	° 7	° 8	9	10		
Создать инцидент			🛃 Назначить инцидент пользователю			Логировать первое и последнее событие			Логировать указанное число событий				
									2		- +		
IP актива			FQDN актива			Hostname актив	а		МАС актива				
action		~	elastic_key		\sim	event.packet		~	@timestamp		~		
Техники Mitre													
T1548, T1548.00	1												
Шаблон													
Авто назначение	9												
											le		

Рис. 169 – Окно "Создать шаблон"

- 2. Укажите в окне следующую информацию:
 - в поле Название шаблона укажите название шаблона "алерта";

- в поле **Уровень риска** выберите цифровое обозначение уровня риска, которое будет присвоено "сработке" правила;
- установите флаг Создать инцидент если необходимо автоматически создавать инцидент на основании "сработки" правила;
- установите флаг Назначить инцидент пользователю если необходимо автоматически назначать инцидент пользователю;
- выберите количество событий, которые необходимо записывать в журнал:
 - если вы хотите записывать только первое и последнее событие, то установите соответствующий флаг;
 - в обратном случае укажите необходимое значение в поле **Логировать** указанное число событий.
- в поле **IP актива** из выпадающего списка выберите поле, которое будет выступать в качестве IP-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **FQDN актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования домена актива. Поле может являться частью сводной таблицы событий;
- в поле **Hostname актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий;
- в поле **МАС актива** из выпадающего списка выберите поле, которое будет выступать в качестве МАС-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **Техники Mitre** укажите через запятую идентификаторы техник, используемых киберпреступниками, которые описаны в базе знаний компании Mitre (подробнее см. <u>Techniques Enterprise | MITRE ATT&CK®</u>);
- в поле Шаблон укажите дополнительную информацию об "алерте".
- 3. Нажмите кнопку Создать.

9.6.4 Редактирование шаблона "алерта"

- 1. Начните процесс редактирования шаблона через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

9.6.5 Дублирование шаблона "алерта"

1. Откройте шаблон на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать шаблон алерта" (см. «Рис. 170»).

Дублировать шаблон алерта	×
Название шаблона	
Проверка времени операции - Дубль	
	Сбросить Дублировать

Рис. 170 – Окно "Дублировать шаблон алерта"

- 2. Укажите в окне наименование шаблона.
- 3. Нажмите кнопку Дублировать.

9.6.6 Удаление шаблона "алерта"

- 1. Начните процесс удаления шаблона через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Шаблон алерта будет удален из платформы.

9.7 Шаблоны группировки

9.7.1 Общие данные

При настройке правила корреляции вы можете использовать заранее подготовленные шаблоны группировки событий.

Группировка выполняется по выбранному полю нормализованного события.

Платформа поддерживает возможность отслеживания и группировки подозрительных событий, следующих одно за другим (цепочки событий).

Для работы с шаблонами группировки перейдите в раздел **Коррелятор** → **Шаблоны группировки** (см. «Рис. 171»).

≡	К ПАНГЕ РАДАР	° 1	72.30.254.97 🗸 Шаблоны группиро	вки	Лицензия активна до: 2	2027-11	-16 🛈 Документация	I	8	admin \vee				
۵	Ша	Шаблоны группировки												
Q														
0	Филь	Фильтры +												
Сортировка († Название × +														
	Сбр	оси	гь Применить											
Ð	∇	Создать Удалить Удалить все									٢			
<i>%</i>			Название	Размер окна группировки	Порог количества событий для	Обновлено		Создано						
ж			Группировка по дате	5	1	2025-04-29 17:27:37		2025-04-29 17:27:24		0 0) 🗇			
494			Шаблон с цепочкой	5	1	2025-04-17 14:31:10		2025-04-17 14:31:10		00	, 🗊			
0	<	1	> 50 / страница ~											

Рис. 171 – Раздел "Шаблоны группировки"

В разделе отображается следующая информация:

- Название наименование шаблона группировки;
- Размер окна группировки временной интервал, в течение которого будет выполняться группировка событий;
- Порог количества событий для срабатывания количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- Обновлено дата и время изменения информации о шаблоне;
- Создано дата и время создания шаблона.

9.7.2 Просмотр шаблона группировки

Для просмотра шаблона нажмите кнопку ^(O) в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного шаблона (см. «Рис. 172»).

≡	<mark>₿ пантео</mark> 172.30.254.138 ∨ Ша	абло	ны группировки				🛈 База знаний	🔘 admin ~
â	8700+		Группировка по времени			🗇 Удали	ть Дублировать	Редактировать
Q	Группировка по времени							
0	Изменено: 2024-09-06 10:15:11		Название шаблона					
	Агрегация по идентификатору		Группировка по времени					
¢.	Изменено: 2024-09-06 10:15:52		Группировать по		Агрегировать по			
6			action 🗎		action 🗎			
<i>%</i>		0	Размер окна группировки		Порог количества событий для срабатывания			
н			5 -+	Минуты 🗸	1 -+	Агрегировать т	олько уникальные собы	RNJ
494 F								
			Время события	Формат времени				
۲			@timestamp ~	RFC3339Nano 2006-01-02T15:04:05.999	3999+07:00 (Z07:00)			
			Использовать цепочку					

Рис. 172 – Форма просмотра шаблона группировки

В боковой панели отображается следующая информация о шаблонах:

- наименование шаблона;
- дата и время последнего изменения шаблона.

В рабочей области отображается структура данных и внешний вид шаблона.

9.7.3 Создание шаблона группировки

1. Начните процесс создания шаблона через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создать шаблон" (см. «Рис. 173»).

Создать шаблон			Создать	
Название шаблона				
Группировка по ключу				
Группировать по		Агрегировать по		
elastic_key 🛱		error 🗇 event 🛱		
Размер окна группировки		Порог количества событий для срабатывания		
5 -+	Минуты	1 -+	Агрегировать только уникальные события	
Врамя события	Формат времени			
@timestamp	RFC3339Nano 2006-01-02T15:04:05.999999999	9+07:00 (Z07:00)		

Рис. 173 – Форма "Создать шаблон"

2. Укажите в окне следующую информацию:

- в поле Название шаблона укажите название шаблона группировки;
- в поле **Группировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться группировка. Можно выполнять группировку по нескольким полям;
- в поле **Агрегировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться функция агрегации. Можно выполнить агрегацию по нескольким полям;
- в поле **Размер окна группировки** укажите временной интервал, в течение которого будет выполняться группировка событий;
- в поле **Порог количества событий для срабатывания** укажите количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- для агрегации только уникальных значений установите соответствующий флаг;
- в поле **Время события** из выпадающего списка выберите поле нормализованного события, по которому будет вычисляться время события;
- в поле **Формат времени** из выпадающего списка выберите формат времени события.
- 3. При необходимости настройте цепочку событий. Для этого установите соответствующий переключатель в положение "Включен" и добавьте условия для цепочки событий нажав на кнопку + **Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 174»).

нкция сравнения		
роверить наличие в массиве — ~		
Строка	Массив	
Тип выражения	Тип выражения	
Значение из события 🗸	Массив строк	\sim
Ключ	Значение	
event.alert \lor	event	- +
	event.anomaly	- +

Рис. 174 – Окно "Настроить условие"

- 4. Укажите в окне "Настроить условие" следующую информацию:
 - В поле Функция сравнения из выпадающего списка выберите функцию Проверить наличие в массиве;
 - В блоке Строка настройте первую часть выражения:
 - в поле Тип выражения выберите необходимый тип выражения, например "Значение из события";

- в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет выявляться цепочка событий.
- В блоке Массив настройте вторую часть выражения:
 - в поле **Тип выражения** выберите необходимый тип выражения, например "Массив строк";
 - в поле **Значение** укажите массив значений, по которым должно проверяться поле, указанное в поле **Ключ**.
- В блоке **Результат** проверьте правильность заданного выражения;
- Нажмите кнопку Сохранить.
- 5. Добавьте необходимое количество условий цепочки событий.
- 6. Настройте дополнительные параметры поведения для добавленных условий цепочки событий (см. «Рис. 175»):

	elastic_key равно значению в мас	сиве 56723123476	
÷	Количество событий		2
	2 -+	Точное совпадение количества событий Отсутствует	

Рис. 175 – Параметры условий цепочки событий

- в поле **Количество событий** укажите минимальное количество найденных событий, подходящих под условие для "сработки" правила;
- для включения проверки строго соответствия количества событий установите флаг **Точное совпадение количества событий**;
- для отключения проверки по выбранному условия установите переключатель **Отсутствует** в положение "Включен".
- 7. Нажмите кнопку Создать.

9.7.4 Редактирование шаблона группировки

- 1. Начните процесс редактирования шаблона через «универсальные таблицы» или инструмент «боковая панель».
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

9.7.5 Дублирование шаблона группировки

1. Откройте шаблон на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать шаблон группировки" (см. «Рис. 176»).

Дублировать шаблон группировки		×
Название шаблона		
Группировка по ключу - Дубль		
	Сбросить	Дублировать

Рис. 176 – Окно "Дублировать шаблон группировки"

- 2. Укажите в окне наименование шаблона.
- 3. Нажмите кнопку Дублировать.

9.7.6 Удаление шаблона группировки

- 1. Начните процесс удаления шаблона через «универсальные таблицы» или инструмент «боковая панель».
- 2. Подтвердите удаление в открывшемся окне.
- 3. Шаблон группировки будет удален из платформы.

9.8 Табличные списки

9.8.1 Общие данные

Табличные списки (Rapid Value Store), являются видом активного хранилища -- автоматически изменяемого, в зависимости от условий.

Табличные списки могут использоваться для следующих целей:

- для обращения к справочным данным;
- для дополнительной фильтрации при работе с обогащением из таких источников как: Active Directory, Активы;
- для добавления идентификаторов активов и пользователей в "карантин", для исключения повторных "сработок" правил до решения инцидента;
- для реализации механизма "черных" и "белых" списков.

Хранилища могут быть созданы вручную и автоматически. Автоматическое создание хранилища включает в себя следующие способы:

- посредством обработки событий от источника "Kaspersky-SecurityCenter-db-host-activity" и правила "AV_KES_Hosts with old bases and without workable antivirus";
- посредством исполнения скриптов, получающих информацию из Active Directory активов Платформы.

Табличные списки поддерживают следующие типы полей:

- string указывается строка;
- integer указывается целое число;
- bigint указывается целое число произвольной точности;
- double указывается целое или дробное число с двойной точностью;
- ІР указывается ІР-адрес,
- CIDR указывается IP-адрес подсети.

При написании правил корреляции для их вызова в коде правила необходимо использовать функцию RVS.

Для работы с табличными списками перейдите в раздел **Коррелятор** → **Табличные списки** и выберите хранилище из списка (см. «Рис. 177»).

≡	👹 ^{пангео} 172.30.254.138 ∨ Табл	ичный спис	сок		() Ба	за знаний 🔘 admin 🗸
â	8 7 Ø C +	local-ı	networks		🗓 Удалить Дубли	ровать Редактировать
Q	whitelist_account_sids Записей: 0					
()	Пример заполнения хранилища target.user.id, target.host.ip,	РД	обавить запись Удалить Удалить все	Экспортировать все	Импортировать	C 🚳
-0	customer domain		_id	_ttl	₽ net	
40	# Пример: FQDN, IP, is_dc_RODC,		10.0.0/8	-	10.0.0/8	7 D D
ð	Hostname		172.16.0.0/12	-	172.16.0.0/12	🖉 🗇 💼
12:	local-networks Записей: 3		192.168.0.0/16	-	192.168.0.0/16	n 🖉 n 🗇 n 🗇 🔿 n 🗇 n n n n n n n n n n n n n n n n n
ж	DNS-servers Записей: 0 Список DNS серверов	< 1	> 10 / страница ~			
441	cred dump files path					
ത	['\\mimidrv';'\\Isass','\\minidump\\minidum					
0	Domain controllers Записей: 0					
	Список контроллеров домена Пример: FQDN, IP, is_dc_RODC,					
	blacklisted service Записей: 22 Описание: "evil_service_pattern"					

Рис. 177 – Раздел "Табличные списки"

Набор отображаемых данных формируется в зависимости от настроек выбранного табличного списка.

Значком *Р* отмечены поля, которые являются "ключами" для формирования уникального идентификатора записи (поле _id). По этому идентификатору правила будут обращаться к нужной записи из табличного списка. Признак "ключа" указывается для поля на этапе создания табличного списка. Необходимо соблюдать уникальность поля _id.

9.8.2 Создание табличного списка

1. Нажмите кнопку **Создать табличный список**. Откроется окно "Создание табличного списка" (см. «Рис. 178»).

laobanno				
host+username				
Описание				
Подсчет обращени	ий с определенного хоста, ко	нкретны	м пользо	вателем
Схема данных				
Название	Тип		Ключ	
host	string	\sim		Удалить
Название	Тип		Ключ	
username	string	\sim		Удалить
Название	Тип		Ключ	
· · · · • •	integer	~		Удалить

Рис. 178 – Окно "Создание табличного списка"

- 2. Укажите в окне следующую информацию:
 - в поле Название укажите название табличного списка;
 - в поле Описание укажите дополнительные сведения о табличном списке;
 - в блоке Схема данных настройте поля табличного списка:
 - в поле **Название** укажите название поля схемы данных;
 - в поле **Тип** из выпадающего списка выберите тип поля: string, integer, bigint, double, IP, CIDR;
 - в поле **Ключ** при необходимости установите признак "ключ". Ключ служит для формирования уникального идентификатора записи табличного списка;
 - добавьте необходимое количество полей в схему данных табличного списка.
 Для этого нажмите кнопку **Добавить**.
- 3. Нажмите кнопку Сохранить.

9.8.3 Работа с записями табличного списка

Над записями табличного списка доступны следующие операции:

- Добавление записи.
- Редактирование записи.
- Дублирование записи.
- Экспорт записей.
- Импорт записей.
- Удаление записей.
- Массовые операции над записями.

Добавление записи выполняется следующим способом:

1. Выберите табличный список и нажмите кнопку **Добавить запись**. Откроется окно "Создание записи" (см. «Рис. 179»).

Создание записи		×
_ttl		
Выбрать дату и время		
host		
host1		
username		
username1		
count		
0		
	Отмена	Сохранить

Рис. 179 – Окно "Создание записи"

- 2. Окно "Создание записи" формируется в зависимости от настроенной схемы данных табличного списка. Укажите в окне соответствующие данные.
- 3. В поле **ttl** укажите дату, до наступления которой запись табличного списка будет действительна;
- 4. Нажмите кнопку Сохранить.

9.8.4 Редактирование табличного списка

- 1. Выберите из списка необходимый табличный список и нажмите кнопку Редактировать.
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

9.8.5 Дублирование табличного списка

1. Выберите из списка необходимый табличный список и нажмите кнопку **Дублировать**. Откроется окно "Дублирование табличного списка" (см. «Рис. 180»).

host+username-ду	бль			
Описание				
Подсчет обращен	ий с определенного хоста, ко	нкретнь	ІМ ПОЛЬЗОІ	зателем
Схема данных				
Название	Тип		Ключ	
host	string	~		Удалить
Название	Тип		Ключ	
username	string	~		Удалить
Название	Тип		Ключ	
	integer	\sim		Удалить

Рис. 180 – Окно "Дублирование табличного списка"

- 2. Укажите в окне наименование табличного списка.
- 3. Нажмите кнопку Сохранить.

9.8.6 Импорт табличных списков

- 1. Нажмите на кнопку 🗹 и из выпадающего списка выберите пункт Импортировать.
- 2. В открывшемся окне укажите путь к архиву с табличными списками.
- 3. Нажмите кнопку Открыть.

9.8.7 Экспорт табличных списков

- 1. Нажмите на кнопку и из выпадающего списка выберите пункт Экспортировать все.
- 2. Будет сформирован архив с табличными списками в формате .zip.
- 3. Нажмите кнопку Скачать и укажите путь для сохранения архива.

9.8.8 Удаление табличного списка

- 1. Выберите из списка необходимый табличный список и в рабочей области нажмите кнопку **Удалить**.
- 2. Подтвердите удаление в открывшемся окне.
- 3. Табличный список будет удален из платформы.

9.8.9 Массовые действия над табличными списками

Над табличными списками доступны следующие массовые действия:

- Экспортировать экспорт выбранных табличных списков;
- Удалить удаление выбранных табличных списков;
- Удалить все удаление всех табличных списков.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку . Откроется список массовых операций и флаги для выбора табличных списков (см. «Рис. 181»).



Рис. 181 – Массовые действия над табличными списками

- 2. Выберите табличные списки.
- 3. Нажмите на соответствующую кнопку действия.
- 4. Завершите действие в открывшемся окне.

9.9 Ретроспективная корреляция

9.9.1 Общие данные

Платформа Радар позволяет осуществлять повторную корреляцию по сохраненным ранее событиям потока.

Ретроспективную корреляцию событий можно использовать в следующих случаях:

- для проверки гипотез по добавлению новых правил корреляции;
- для проверки событий после обновления данных табличных списков;
- для проверки событий по правилам, работа которых была приостановлена.

Для перевода правила в режим ретроспективного анализа необходимо выполнить следующие условия:

- правило должно быть "активно";
- для правила выставлен признак "Ретроспективное".

Для выполнения ретроспективной корреляции необходимо создать задачу с одним из правил, подходящих для проведения анализа.

Для управления задачами для ретроспективной корреляции перейдите в раздел **Коррелятор** → **Ретроспективная корреляция** (см. «Рис. 182»).

≡	Кангео Радар	172.30.254.13	≋∨ ∣ Ретро	спективная корреляция					 База знаний 	🔕 admin 🗸
â	Ретр	оспекти	вная корре	еляция						
Q										
0	7	Добавить зада	ачу Остановить	Перезапустить Удалить Удалит	ъвсе					C Ø
		Название	Статус	Правило корреляции	Период с	Период по	Индекс	Выполнено	Обновлено	
⊊‼		Задача 2	В очереди	anotherOneForMEMORYERROR	12:24:32 06.09.2024	12:24:32 06.09.2024	_2	0	12:26:06 06.09.2024	■ <i>Ĉ</i> 🖻
ð		Задача 1	Остановлено	anotherOneForMEMORYERROR	12:22:43 06.09.2024	12:22:43 06.09.2024	_1	0	12:26:02 06.09.2024	■ 2 値
%	<	1 > 10	/ страница 🗸							
¥										
494										
Ø										

Рис. 182 – Раздел "Ретроспективная корреляция"

В разделе отображается следующая информация:

- Название название задачи ретроспективной корреляции;
- Статус текущее состояние задачи:
 - Остановлено;
 - В очереди;
 - Ошибка;
 - Выполняется.
- Период с и Период по период выполнения задачи;
- Правило корреляции наименование правила корреляции, по которому выполняется задача. По ссылке открывается форма просмотра правила;
- Индекс индексы событий, по которым проводится анализ;
- Выполнено количество выполнений задачи.

9.9.2 Добавление задачи для ретроспективной корреляции

1. Нажмите кнопку Добавить задачу. Откроется окно "Создать задачу" (см. «Рис. 183»).

Название				
Задача З				
Травило корреляции				
anotherOneForMEMORYER	ROR			\sim
Период				
2024-09-06 12:35:50	\rightarrow	2024-09-06 12:35	5:50	
Индекс				
*3 *4				

Рис. 183 – Окно "Создать задачу"

- 2. Укажите в окне следующую информацию:
 - в поле Название укажите название задачи;
 - в поле **Правило** из выпадающего списка выберите правило для ретроспективного анализа;
 - в поле **Период** укажите период выполнения задачи;
 - в поле **Индекс** укажите индексы событий, по которым будет выполняться задача (поддерживается wildcard символ "*").
- 3. Нажмите кнопку Создать.

9.9.3 Остановка задачи

- 1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку .
- 2. Выполнение задачи будет остановлено.

9.9.4 Перезапуск задачи

- 1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку $\overline{\sim}$.
- 2. Выполнение задачи будет заново запушено.

9.9.5 Удаление задачи

- 1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку 🔟.
- 2. Задача будет удалена.

9.9.6 Массовые действия над задачами

Над задачами доступны следующие массовые действия:

- Остановить остановка выполнения выбранных задач;
- Перезапустить повторный запуск выбранных задач;
- Удалить удаление выбранных задач;
- Удалить все удаление всех задач.

Для выполнения массового действия выполните следующие шаги:

- 1. Отметьте в таблице необходимые задачи, установив соответствующие флаги.
- 2. Нажмите на соответствующую кнопку действия.
- 3. Завершите действие в открывшемся окне.

10. Параметры

В разделе выполняется управление следующими параметрами Платформы Радар:

- «<u>Основные параметры</u>». Настройка общих параметров **Платформы Радар**.
- «<u>Оповещения по задержкам</u>». Настройка автоматических оповещений по задержкам в обработке инцидентов, формируемых **Платформой Радар**.
- «<u>Черный список ID плагинов</u>». Настройка списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы.
- «<u>Фоновые задачи</u>». Просмотр информации о фоновых задачах, запущенных в **Платформе Радар**.
- «Интеграции». Управление экземплярами интеграций со сторонними системами.
- «<u>Типы интеграций</u>». Просмотр доступных классов систем, с которым можно настроить интеграцию, а также переключение платформы в режим работы с соответствующим типом интеграции.
- «<u>Папки контента</u>». Управление папками для структурирования пользовательского контента.
- «Шаблоны». Управление шаблонами форм пользовательского контента.

10.1 Основные параметры

Для выполнения настройки основных параметров **Платформы Радар** перейдите в раздел **Параметры** → **Основные параметры** (см. «Рис. 184»).

■ Кангес 172.30.254.155 ∨	Основные параметры	Лицензия активна до: 2024-12-25 💿 Документация 🔘 admin 🗸
Рабочий стол	Основное Оповещения по задержкам Черный список ID плагинов	Сохранить
Q События		
О Инциденты ~	Общее	Создание инцидентов
ς₿ Активы ∨	Название клиента	
🗈 Соответствие ПО 🗸 🗸	Название клиента	Автоматически создавать инциденты при импорте результатов сканирования
🗱 Коррелятор 🗸 🗸	Риск принят: количество дней по умолчанию	Минимальный уровень важности для открытия инцидента
ж Источники 🗸	90 - + Принятие риска инцидента установит это значение в качестве срока по-умоличнио (парамето "Принять по"). Чтобы оставить	
нараметры ∧	принотня ракай индерства разволят это электельно и общати с учени то учение по раконо породения разволять уколо значение для Принять до" пустым, укажите значение 0. Расположение	
Основные параметры	Москва 🗃	Автоматическое создание происшествий и переоткрытие инцидентов
Оповещения по задерж	Группа пользователей по-умолчанию для инцидентов, связанных с активами, без определенного "ответственного пользователя"	Создавать новый инцидент для повторных происшествий, если инцидент закрыт
Черный список ID плаги	Users	Создавать новый инцидент Переоткрывать инцидент
Фоновые задачи	Стратегия илентификации активов по-умолианию	Минимальный уровень писка для повтопного открытия иншилентов
🕲 Администрирование 🗸	IP O MAC O FQDN	 Высокий Средний Низкий Отсутствует
	Conservue DODH	
	Coshagehve PQDN	Статус повторно открытых инцидентов
	 включает сопладение по имени хоста ичали), где выорана стратегии идентификации FQDN. Внимание! Если имя хоста опраделено в нескольких доменах, совпадение по PQDN не проверяется т.к. мы не знаем какой домен правильных 	о новыи 💿 назначен

Рис. 184 – Раздел "Основные параметры"

Раздел содержит следующие блоки:

- Общие настройка значений по умолчанию для различных параметров платформы;
- Создание инцидентов настройка автоматического создания инцидентов;

• Автоматическое создание происшествий и переоткрытие инцидентов – настройка поведения платформы при возникновении повторных происшествий.

После внесения любых изменений, для того чтобы они вступили в силу, необходимо нажать кнопку **Сохранить**.

Общие

Для настройки значений по умолчанию выполните следующие действия:

- в поле **Название клиента** укажите наименование организации, в которой установлена **Платформа Радар**;
- в поле **Риск принят: количество дней по умолчанию** укажите количество дней, по истечении которых будет принят риск инцидента. Значение будет автоматически добавлено в поле инцидента **Принять до**. Чтобы оставить значение поля **Принять до** пустым, укажите значение 0;
- в поле **Расположение** укажите город, в котором располагается организация;
- в поле **Группа пользователей по умолчанию** выберите из списка группу пользователей, которая будет назначаться по умолчанию для инцидентов, связанных с активами без назначенного "ответственного пользователя";
- в поле **Стратегия идентификации активов по умолчанию** выберите одну из стратегий (IP, FQDN, MAC), которая будет применена при идентификации активов, в случае если актив не попал ни под одну, настроенную пользователем, стратегию;
- если выбрана стратегия идентификации по FQDN, то выберите поведение платформы: включать или не включать совпадение по имени хоста (PQDN).

Внимание! Если имя хоста определено в нескольких доменах, совпадение по PQDN не проверяется.

Создание инцидентов

- при необходимости включите автоматическое создание инцидентов при импорте результатов сканирования, установив соответствующий флаг;
- установите минимальный уровень важности для открытия инцидента.

Автоматическое создание происшествий и переоткрытие инцидентов

Выберите поведение платформы при возникновении повторных происшествий в закрытом инциденте:

- Создавать новый инцидент;
- Переоткрывать инцидент. В этом случае необходимо указать следующие параметры:
 - выберите минимальный уровень риска для повторного открытия инцидента: высокий, средний, низкий, отсутствует;
 - выберите статус повторно открытых инцидентов: новый, назначен.

10.2 Оповещения по задержкам

Для выполнения настройки автоматических оповещений по задержкам в обработке инцидентов операторами, перейдите в раздел **Параметры** → **Оповещения по задержкам** (см. «Рис. 185»).

Concer Texterement on taggenesis		ржкам	Лицензи	я активна до: 2024-12-25 🕕 Документация 🔘
Vicene picca Vicene picca <td< th=""><th>Основное Оповещения по задержкам Чер</th><th>ный список ID плагинов</th><th></th><th>Сохра</th></td<>	Основное Оповещения по задержкам Чер	ный список ID плагинов		Сохра
Hopvanuo Hopvanuo <td< th=""><th>Уровень риска Высокий</th><th>Уровень риска Средний Настроить</th><th>Уровень риска Низкий</th><th>Уровень риска Отсутствует Настроит</th></td<>	Уровень риска Высокий	Уровень риска Средний Настроить	Уровень риска Низкий	Уровень риска Отсутствует Настроит
небольшая задержая небольшая задержая небольшая задержая небольшая задержая небольшая задержая 3 задержая 28 задержая 3адержая 3адержая 3адержая 3адержая 3адержая 3адержая 3адержая 3адержая 3адержая 0 задержая 3адержая 0 задержая 3адержая 0 задержая 0 содан 202012-002313:30 0 0 0 0 0 содан 202012-002313:30 0 0 содан 202012-002313:30 0 0 содан 202012-002313:30 0 0 содан 202012-002313:30	Нормально 3	Нормально 5	Нормально 28	Нормально 84
Здерхка Sdeрхка Sdeрxкa Sdeрхка Sdeрхка <	Небольшая задержка 5	Небольшая задержка 28	Небольшая задержка 84	Небольшая задержка О
Содан 2020-12-09 231330 Codan 2020-12-09 231330 Codan 2020-12-09 231330 Codan	Задержка 10	Задержка 56	Задержка 168	Задержка О
Онновлен 2020*12:09:23:13:30 Онновлен 2024*11*08 13:01:21 Настройка оповещений 0 Отправлять оповещений 0 Отправлять оповещение одножди после достижения последнего показателя времени удержания, отправлять оповещение через 0 5 дней 0 Для индидентов с риском "Чизкий", после достижения последнего показателя времени удержания, отправлять оповещение через 0 5 дней 0 Для индидентов с риском "Чизкий", после достижения последнего показателя времени удержания, отправлять оповещение через 0 5 дней 0 Для индидентов с риском "Чизкий", после достижения последнего показателя времени удержания, отправлять оповещение регулярно • • Через 0 5 дней 0 • • Отправлять слосефдений раз в недело • • • Оповещение об изменении времени удержания инцидента от "Небольшой задержои" до "Задержои" • через 0 5 дней • • • отправлять слосефцения • • •	Создан 2020-12-09 23:13:30	Создан 2020-12-09 23-13:30	Создан 2020-12-09 23:13:30	Создан 2020-12-09-23:13:30
Отгравить опоещение при каждом изменении времени обработки Отравить опоещение при каждом изменении времени удержания последнего показателя времени удержания, отправлять оповещение Porynapho Vepes © 5 дней © Для инцидентов с риском "Средней", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Средней", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Средней", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение perynapho Vepes © 5 дней © Для инцидентов с риском "Thaskid", после достижения последнего показателя времени удержания, отправлять оповещение Vepes © 5 дней © Отправлять группу сообщения рав в недено Vepes © 5 дней © Отправлять последнего показателя времени удержания, отправлять оповещение Vepes © 5 дней © Отправлять проперани удержания, отправлять оповещение Vepes © 5 дней © Отправлять последнего показателя времени удержания, отправлять оповещение Vepes © 5 дней © Отправлять пруппу сообщения рав в недело	Настройка оповещений 🕕		Тексты оповещений	
 Отправить оповещение единохды после достижения последнего показателя времени удержания. Чрев О править оповещение единохды после достижения последнего показателя времени удержания, отправлять оповещение Чрев О преми О Для ницидентов с риском "Быский", после достижения последнего показателя времени удержания, отправлять оповещение Чрев О преми О Для ницидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение Чрев О преми О Для ницидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение Чрев О преми О Канкий после достижения последнего показателя времени удержания, отправлять оповещение Чрев О пинкий, после достижения последнего показателя времени удержания, отправлять оповещение Чрев О пинкий после достижения последнего показателя времени удержания, отправлять оповещение Черев О пинкий после достижения последнего показателя времени удержания, отправлять оповещение Черев О пинкении времени удержания инцидента от "Небольшой задержки" до "Небольшой задержки" до "Небольшой задержки" Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки" Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки" Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки" Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки" Текст сообщения рак в неделю О тправлять групту сообщений раз в неделю 				
"через Гдень	Отправлять оповещение при каждом изменении време	ни обработки	Общий текст, отправляемый в каждом оповещении	
ратуприю Через 5 дней 6 Для нацидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение рагупарно Через 5 дней 0 Для нацидентов с риском "Тизикий", после достижения последнего показателя времени удержания, отправлять оповещение через 5 дней 0 Для нацидентов с риском "Тизикий", после достижения последнего показателя времени удержания, отправлять оповещение через 5 дней 0 Для нацидентов с риском "Тизикий", после достижения последнего показателя времени удержания, отправлять оповещение через 5 дней 0 Для нацидентов с риском "Тизикий", после достижения последнего показателя времени удержания, отправлять оповещение через 5 дней 0 О отправлять труппу сообщения раз в недело	Отправлять оповещение при каждом изменении время Отправить оповещение единожды после достижения г	ни обработки юследнего показателя времени удержания	Общий текст, отправляемый в каждом оповещении	
Оля ницидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение Уля ницидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение Уля ницидентов с риском "Тизийи", после достижения последнего показателя времени удержания, отправлять оповещение Через S 5 дней Оправлять тосле достижения последнего показателя времени удержания, отправлять оповещение через S 5 дней Оправлять тосле достижения последнего показателя времени удержания, отправлять оповещение через S 5 дней Оправлять тосле достижения последнего показателя времени удержания, отправлять оповещение через S 5 дней Оправлять тосле достижения последнего показателя времени удержания, отправлять оповещение через S 5 дней О 7 О птравлять тосле достижения последнего показателя времени удержания, отправлять оповещение через S 5 дней О 7 О птравлять тосле достижения последнего показателя времени удержания, отправлять оповещение С поравлять труппу сообщения раз в недело	Оттравлять оповещение при каждом изменении времи Оттравить оповещение единожды после достижения г Чера О 1день О Дляницидентов с риском "Высокий", после достижения	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять опозещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от *	Задержки" до "Недопустимого"
Через S дней O Для ичидидентов с риском "Чизкий", после достижения последнего показателя времени удержания, отправлять оповещение регулярно Через S дней O Для ичидидентов с риском "Отслутствует", после достижения последнего показателя времени удержания, отправлять оповещение регулярно Через S дней O Отправлять групту сообщений раз в неделю	Оттравлять оповещение при каждом изменении время Оттравить опсвещение единожды после достижения г Чераз О 1 день О Для инцидентов с риском "Высский", после достижени регуприо Чераз О 5 дней О	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от *	Задержки" до "Недопустимого"
регулярно Через 🕞 5 дней 🕜 Для инцидентов с риском "Отсутствует", после достижения последнего показателя времени удержания, отправлять оповещение регулярно Через 🕞 5 дней 🚱 Отправлять групту сообщения раз в неделю	Оттравлять оповещение при каждом изменении времи Оттравить оповещение единожды после достижения г Через О 1 день О Для нечиднетов с риском "Высокий", после достижени регулярно Через Бдней О Для нечиднетов с риском "Средний", после достижени регулярно	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение я последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от * Текст сообщения об изменении времени удержания инцидента от т	Задержки" до "Недопустимого" Небольшой задержки"
Для иницидентов с риском "Отсутствует", после достижения последнего показателя времени удержания, отправлять оповещение регулярис. Через ⊙ 5 дней ⊙ Отправлять группу сообщений раз в неделю	Отправлять оповещение при каждом изменении времи З Отправить оповещение единожды после достижения г Через ○ 1день ○ З Для инцидентов с риском "Высский", после достижени регуприю Через ○ 5дней ○ Для инцидентов с риском "Средний", после достижения регуприю Через ○ 5дней ○ З Для инцидентов с риском "Средний", после достижения регуприю Через ○ 5дней ○ З Для инцидентов с риском "Инакий", после достижения	ни обработки последнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение я последнего показателя времени удержания, отправлять оповещение последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от "	Задержки" до "Надопустимого" Чебольшой задержки" до "Задержки"
Отправлять группу сообщений раз в неделю	 Оттравлять оповещение при каждом изменении время Оттравить опсеещение единохды после достижения г Чераз О 1 день О Для нацидентов с риском "Высский", после достижени регуприю Для нацидентов с риском "Средний", после достижени регуприю Через О 5 дней О Для нацидентов с риском "Средний", после достижени через 5 дней О Для нацидентов с риском "Накий", после достижения через 5 дней О Для нацидентов с риском "Накий", после достижения через 5 дней О Для нацидентов с риском "Накий", после достижения через 5 дней О 	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение я последнего показателя времени удержания, отправлять оповещение последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от "	Задержки" до "Надопустимого" Небольшой задержки" до "Задержки" Чормального" до "Небольшой задержки"
Ortipasivitie (pyring Cocoupting pase response)	Оттравлять оповещение при каждом изменении времи З Оттравить оповещение единожды после достижения п Через ○ 1 день ○ З Для нецицентов с риском "Высокий", после достижения регулярно Через ○ 5 дней ○ Для нецицентов с риском "Средний", после достижения регулярно Через ○ 5 дней ○ З Для нецидентов с риском "Назмий", после достижения регулярно Через ○ 5 дней ○ З для нецидентов с риском "Отсутствует", после достижения регулярно меся ○ 5 лией ○	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение последнего показателя времени удержания, отправлять оповещение ения последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от "	Задержки" до "Недопустимого" Небольшой задержки" до "Задержки" Нормального" до "Небольшой задержки"
	 Оттравлять оповещение при каждом изменении время Оттравить оповещение единожды после достижения г Через ○ 1 день ○ Для нецидентов с риском "Высокий", после достижения регулярно через ○ 5 дней ○ Для нецидентов с риском "Средний", после достижения регулярно через ○ 5 дней ○ Для нецидентов с риском "Какий", после достижения регулярно через ○ 5 дней ○ Для нецидентов с риском "Какий", после достижения регулярно через ○ 5 дней ○ Для нецидентов с риском "Отсутствует", после достижения регулярно через ○ 5 дней ○ 	ни обработки юследнего показателя времени удержания я последнего показателя времени удержания, отправлять оповещение последнего показателя времени удержания, отправлять оповещение ения последнего показателя времени удержания, отправлять оповещение	Общий текст, отправляемый в каждом оповещении Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от " Текст сообщения об изменении времени удержания инцидента от "	Задержки" до "Недопустимого" Небольшой задержки" до "Задержки" Нормального" до "Небольшой задержки"

Рис. 185 – Раздел "Оповещения по задержкам"

Раздел содержит следующие блоки:

- Блок настроек временных отсечек для оповещений;
- Блок настройки режимов отправки оповещений;
- Блок настройки текстов для оповещений.

Блок настроек временных отсечек для оповещений

Для каждого уровня риска (высокий, средний, низкий, отсутствует) можно настроить 3 контрольных отсечки по времени разбора инцидента:

- Нормально время, в пределах которого разбор инцидентов считается штатным (в днях);
- **Небольшая задержка** время, в пределах которого разбор считается выполненным с небольшой задержкой (в днях);
- Задержка время, в пределах которого разбор инцидентов считается выполненным с задержкой (в днях).

При превышении последнего порога, указанного в поле "Задержка", время разбора инцидентов считается недопустимым.

Для настройки времени контрольных отсечек выполните следующие действия:

1. Выберите уровень риска, для которого будет выполнена настройка и в соответствующем блоке нажмите кнопку **Настроить**. Откроется окно "Редактирование уровня риска" (см. «Рис. 186»).

я риска: Высокий	×
	- +
	- +
	- +
Отмена	Сохранить
	ия риска: Высокий

Рис. 186 – Окно "Редактирование уровня риска"

- 2. В полях **Нормально, Небольшая задержка**, **Задержка** укажите необходимое количество дней.
- 3. Нажмите кнопку Сохранить.

Блок настройки режимов отправки оповещений

В Платформе Радар возможно настроить следующие режимы отправки оповещений:

- Отправлять оповещения при каждом изменении времени обработки при активации опции оповещение будет отправляться при прохождении каждой временной отсечки, указанной для разбора инцидента.
- Отправлять оповещение единожды через <...> дн., после достижения последнего показателя времени удержания при активации опции оповещение будет отправляться после прохождения последней сконфигурированной временной отсечки.
- Для инцидентов с риском "Высокий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания – при активации опции оповещение для инцидентов с высоким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- Для инцидентов с риском "Средний" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания – при активации опции оповещение для инцидентов со средним риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- Для инцидентов с риском "Низкий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания – при активации опции оповещение для инцидентов с низким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- Для инцидентов с риском "Отсутствует" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания при активации

опции оповещение для инцидентов с отсутствующим риском будет отправляться после прохождения последней сконфигурированной временной отсечки.

• **Отправлять группу сообщений раз в неделю. День недели** <...> – при активации опции все накопившиеся оповещения будут отправляться единожды в указанный день.

Блок настройки текстов для оповещений

Для оповещений по задержкам в обработке инцидентов можно настроить следующий текст:

- Общий текст, отправляемый в каждом оповещении;
- Текст сообщения об изменении времени удержания инцидента от "Задержки" до "Недопустимого"*;
- Текст сообщения об изменении времени удержания инцидента от "Небольшой задержки" до "Задержки";
- Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки".

10.3 Черный список ID плагинов

Для настройки списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы, перейдите в раздел **Параметры** → **Черный список ID плагинов** (см. «Рис. 187»).

Пангео 172.30.2	54.147 ~	Черный список ID плагинов			Лицензия активна до: 2062-11-07	🛈 Документация 🔘 admin ~
Рабочий стол		Основное Оповещения по заде	ержкам Черный список ID плагин	ов		Добавить плагин в ЧС
Q События						
① Инциденты	~	Плагина: 2 , показано 1 - 2				
с≘ Активы	~	Поиск по ID плагина				🔍 🛹 Выбрать несколько Џ По ID
Соответствие ПО	~	ID плагина	Причина	Создан	Обновлен	
🚀 Коррелятор	~	7	Не поддерживается	13.11.2024 05:09:26	13.11.2024 05:09:26	:
Ж Источники	<u> </u>	4	Не актуален	13.11.2024 05:09:15	13.11.2024 05:09:15	:
	Ť	< 1 > 10 ~				
## Параметры	~					
Администрирование	~					

Рис. 187 – Раздел "Черный список ID плагинов"

В разделе отображается следующая информация:

- **ІD плагина** идентификатор плагина;
- Причина описание причины добавления плагина в черный список;
- Создан дата и время создания записи о добавлении плагина в черный список;
- Обновлен дата и время обновления записи о добавлении плагина в черный список;

Для добавления плагина в черный список выполните следующие действия:

1. Нажмите кнопку **Добавить плагин в ЧС**. Откроется окно добавления плагина в ЧС (см. «Рис. 188»).

Добавление записи в ЧС		×
ID плагина		
0		- +
Причина		
		4
	Отмена	Сохранить

Рис. 188 – Добавление плагина в ЧС"

- 2. Укажите в окне следующую информацию:
 - в поле **ID** укажите идентификатор плагина;
 - в поле Причина укажите причину добавления плагина в черный список.
- 3. Нажмите кнопку Сохранить.

10.4 Фоновые задачи

В разделе отображается информация о запущенных задачах ретроспективной корреляции, синхронизации и отчетов.

Для просмотра информации о фоновых задачах, запущенных в **Платформе Радар** перейдите в раздел **Параметры** → **Фоновые задачи** (см. «Рис. 189»).

	249.21 🗸	Фоновые задачи	Лиценз	ия активна до: 2025-08-16	③ Документация	nin 🗸
Рабочий стол		Фоновые задачи				
Q События						
④ Инциденты	~	∇	C	0		
		Название	Результат	Начало	Завершено	
С. Активы	~	sync_	Ошибка	14:41:43 15.08.2024	-	
Соответствие ПО	~	sync_logmuleGoModule	Завершено	17:15:17 20.08.2024	17:15:17 20.08.2024	
🚀 Коррелятор	~	< 1 > 10 / страница ~				
ж Источники	~					
₩ Параметры	^					
Основные параметры						
Оповещения по задер	ж					
Черный список ID пла	ги					
Фоновые задачи						
Администрирование	~					

Рис. 189 – Раздел "Фоновые задачи"

В разделе отображается следующая информация:

- Название наименование задачи;
- Результат описание результата выполнения задачи (контекст зависит от задачи);
- Начало дата и время запуска задачи;
- Завершено дата и время завершения задачи.

10.5 Интеграции

Платформа Радар позволяет добавлять интеграции со сторонними системами.

Различные классы систем, с которым можно настроить интеграцию, называются в платформе **Типами интеграций**. Для каждого типа поддерживаемой системы может быть одновременно настроено несколько интеграций.

Интеграции могут находится в следующих состояниях:

- Активно по интеграции выполняется взаимодействие со сторонней системой;
- Неактивно по интеграции не выполняется взаимодействие со сторонней системой.

В платформе поддерживаются следующие типы интеграций:

- «<u>RT Protect EDR</u>» система обнаружения целенаправленных атак и сложных угроз;
- «<u>Kaspersky Security Center</u>» универсальная консоль централизованного управления различными решениями, продуктами и сервисами, которые обеспечивают информационную безопасность корпоративной ИТ-инфраструктуры.

Примечание: Процессы работы с различными типами интеграций рассмотрены в соответствующих разделах.

Все действия над интеграциями выполняются в разделе **Параметры** → **Интеграции** (см. «Рис. 190»).

Пангес 172.30.252.105	∨ ∣ Интеграции			Лицензия активна д	ю: 2026-04-30 🕕 Документаці	ия 🔕 admin ~	
Рабочий стол	Интеграции						
Q. События							
① Инциденты ~	Создать Удалить Удалить Удалить все Экспортировать в су Экспортировать в су Выбр						
-0.4	Тип интеграции	Название интеграции	Статус	Создано	Обновлено		
	RT Protect EDR	RT Protect EDR	💽 Активно	19:14:34 12.03.2025	12:09:00 19.03.2025	◎ / 前	
Соответствие ПО	RT Protect EDR	RT Protect EDR.Hosoe	Неактивно	19:14:34 12.03.2025	12:09:00 19.03.2025	© 0 fi	
🗱 Коррелятор 🗸 🗸	< 1 > 10 / страница ~						
ж Источники 🗸							
🙌 Параметры 🔷							
Основные параметры							
Оповещения по задерж							
Черный список ID плаги							
Фоновые задачи							
Интеграции							
EDR действия							
Типы интеграций							
Администрирование							

Рис. 190 – Раздел "Интеграции"

В разделе отображается следующая информация:

- Тип интеграции наименование типа интеграции, к которой относится интеграция;
- Название интеграции;
- Статус состояние интеграции: Активно, Неактивно;
- Создано дата и время создания интеграции;
- Обновлено дата и время обновления информации об интеграции.

В разделе используются стандартные элементы управления, которые доступны через «универсальные таблицы» или инструмент «боковая панель».

10.6 Типы интеграций

Для просмотра поддерживаемых в платформе типов интеграций перейдите в раздел **Параметры** → **Типы интеграций** (см. «Рис. 191»).

📃 👹 пангео 172.30.2	252.105	∨ Типы интеграций		Лицензия активна до: 2026-04-30	🛈 Документация	\bigotimes admin \lor
Рабочий стол		Типы интеграций				
Q События						
Онциденты	~	∇				C Ø
с‼ Активы	~	Название	↓↑ c	Статус		
Соответствие ПО	~	RT Protect EDR		О Активно		0
% Коррелятор	~	Kaspersky Security Center		Активно		0
ж Источники	~	< 1 > 50 / страница ~				
∦ ‡ Параметры	~					
Администрирование	~					

Рис. 191 – Раздел "Типы интеграций"

В разделе отображается наименование сторонних систем, с которыми в платформе можно настроить интеграцию.

Тип интеграции может находится в следующих состояниях:

- Активно платформа переведена в режим взаимодействия с данным типом интеграции. В этом режиме могут быть изменены элементы интерфейса платформы и появятся дополнительные функции для поддержки интеграции;
- Неактивно в данном состоянии платформа не поддерживает дополнительные функции необходимые для работы интеграций, настроенных для данного типа.

Для включения поддержки типа интеграции в платформе переведите соответствующий переключатель в состояние **Активно**.

Для просмотра подробной информации о типе интеграции нажмите кнопку 🔘.

Примечание: Подробная информация о каждом типе интеграции рассмотрена в соответствующих разделах.

10.7 Папки контента

Общие принципы работы с содержимом папок описано в разделе (см. раздел **Интерфейс** → «<u>Папки контента</u>»).

Для работы с папками перейдите в раздел **Параметры** → **Папки контента** (см. «Рис. 192»).

	Ξ 👹 ^{панкео} 172.30.254.60 ∨ Папки контента л				Лицен	зия активна до: 2026-02-07	 Документация 	\bigcirc admin \vee	
â	Папк	и контента							
Q	a								
()	Создат	удалить Экспортировать выбран	ные в csv Экспорт	ировать в csv Переместить в	папку			Выбрано	o: 0 C' 🕲
-M		Название	Правила 🥼	Создано	Обновлено		Родительская папка	Кем создано	
-0		my	1	2001-01-01 02:30:17	2001-01-01 02:30:17		-	admin	© 0 🖞
đ		Без папки	594	2025-04-22 15:00:15	2025-04-22 15:00:15		-	admin	0
<i>%</i>		Rules	94	2001-01-01 02:30:17	2001-01-01 02:30:17		-	admin	◎ ⁄ Ē
×		Linux_rules	90	2001-01-01 02:30:17	2001-01-01 02:30:17		Rules	admin	© / fi
491		Linux_rules для тестов	4	2001-01-01 02:30:17	2001-01-01 02:30:17		Linux_rules	admin	◎ Ø Ĥ
114		Windows_rules	0	2001-01-01 02:30:17	2001-01-01 02:30:17		Rules	admin	◎ ⁄ îi
Ø									

Рис. 192 – Раздел "Папки контента"

В разделе отображается следующая информация:

- Название наименование папки. Смещение наименования папки означает вложенность данной папки относительно папки выше по списку;
- Правила количество правил, помещенных в папку;
- Создано дата и время создания папки;
- Обновлено дата и время обновления информации о папке;
- Кем создано наименование пользователя, создавшего папку.

Примечание: В каталоге "Без папки" содержится неструктурированный контент. Данный каталог является системным и не может быть удален.

В разделе используются стандартные элементы управления, которые доступны через «универсальные таблицы».

10.8 Шаблоны

Общие принципы работы с шаблонами описаны в разделе **Интерфейс** → «Шаблоны объектов».

Управление шаблонами выполняется в разделе **Параметры** → Шаблоны (см. «Рис. 193»).

≡	радар 17	2.30.254.97 ∨ Шаблоны			Лицензия активна р	40: 2027-1 1	1-16 🛈 Документация 🔘 а	idmin \checkmark
â	Шабло	оны						
Q								
(i)	۲ У	цалить Удалить все Экспортиро	вать Экспортировать все Э	кспортировать выбранные в csv	Экспортировать в csv	Импортиро	овать Выбрано: 0 С*	©
-®		Название ↓↑	Сущность	Тип шаблона 🗸 🎼	Создано		Обновлено	
-ro		kafka_test_preset	Профиль сбора	Редактирование	2025-04-11 11:03:39		2025-04-11 11:03:39	Û
ů		eventlog_test	Профиль сбора	Редактирование	2025-04-11 1 1 :31:49		2025-04-11 11:31:49	创
₩.		udp_input_preset	Профиль сбора	Редактирование	2025-04-11 11:47:20		2025-04-11 11:47:20	Û
ж		tcp_input_preset_1	Профиль сбора	Редактирование	2025-04-11 14:48:06		2025-04-11 14:48:06	Ū
491		mseven6_52	Профиль сбора	Редактирование	2025-04-14 12:23:25		2025-04-14 12:23:25	Û
		local_eventlog	Профиль сбора	Редактирование	2025-04-14 12:41:10		2025-04-14 12:41:10	Ū
Ø		tcp_input_2520 Cisco-ASA	Профиль сбора	Редактирование	2025-04-14 13:50:18		2025-04-14 13:50:18	Ū
		smb_52	Профиль сбора	Редактирование	2025-04-14 15:44:22		2025-04-14 15:44:22	ŵ

Рис. 193 – Раздел "Шаблоны"

В разделе отображается следующая информация о шаблонах:

- Название наименование шаблона;
- Сущность тип пользовательского контента, для которого настроен шаблон;
- Тип шаблона тип формы, для которой настроен шаблон: создание или редактирование;
- Создано дата и время создания шаблона;
- Обновлено дата и время обновления информации о шаблоне.

11. Рабочие столы

11.1 Общие данные

Рабочие столы – это интерактивные информационные панели, которые отображают данные о состоянии информационной безопасности.

Отображение информации выполняется с помощью следующих типов виджетов:

- временной ряд;
- круговая диаграмма;
- таблица;
- текст;
- гистограмма;
- метрика;
- изображение.

Подробнее о каждом типе виджета вы можете ознакомиться в разделе «<u>Конструктор виджетов</u>». Работа с рабочими столами включают в себя следующие процессы:

- 1. Создание рабочего стола.
- 2. <u>Редактирование рабочего стола</u>.
- 3. Управление виджетами.
- 4. Копирование рабочего стола.
- 5. Создание отчета.
- 6. Удаление рабочего стола.

Для работы с рабочими столами перейдите в новый интерфейс, откройте раздел **Администрирование — Рабочие столы** и выберите рабочий стол из списка.

Внешний вид рабочего стола формируется в зависимости от выставленной пользователем конфигурации виджетов.

Пример интерфейса раздела представлен на «Рис. 194».



Рис. 194 – Интерфейс раздела "Рабочие столы"

Раздел состоит из следующих блоков:

- Список рабочих столов, в котором отображается информация о доступных рабочих столах:
 - название рабочего стола;
 - количество виджетов, добавленных на рабочий стол.
- Рабочая область, в которой отображается информация о выбранном рабочем столе:
 - название рабочего стола;
 - идентификатор рабочего стола;
 - информация о виджетах, добавленных на рабочий стол: заголовок, описание и содержимое виджета (см. «Рис. 195»);
 - режим автообновления рабочего стола;
 - период времени, за который формируется информация для рабочего стола.

Пример отображения информации о виджете приведен на «Рис. 195».



Рис. 195 – Пример виджета

На странице доступны следующие элементы управления рабочим столом:

Кнопка	Действие			
Создать рабочий стол	создание нового рабочего стола			
C	копирование ссылки на рабочий стол			
Ç.	обновление отображаемой информации			
Ë	выбор временного диапазона для формирования данных			
+ Добавить виджет	создание виджета в конструкторе			
:	доступ к следующим действиям над рабочим столом: – редактирование; – создание копии; – создание отчета; – удаление.			

При наведении мыши на виджет, становятся доступны следующие элементы управления виджетом:

Кнопка	Действие
Ċ	переход в соответствующий раздел платформы к табличному представлению данных
¢ [‡] →	перемещение виджета по рабочему столу
	доступ к следующим действиям над виджетом: – редактирование; – удаление; – копирование настроек.

11.2 Создание рабочего стола

Перейдите

В

Администрирование – Рабочие раздел Создать рабочий стол

столы

И

нажмите

кнопку

Создание рабочего стола	×
Название	
Сегодняшние события	
Период	
Сегодня	Ë
	Создать

Рис. 196 – Окно "Создание рабочего стола"

Выполните следующие действия:

- 1. В поле "Название" укажите название рабочего стола.
- 2. В поле "Период" из выпадающего списка выберите период, по которому будут выводиться данные на рабочий стол.
- 3. Нажмите кнопку Создать.

После создания рабочего стола рекомендуется выполнить следующие действия:

- настроить права доступа пользователей к рабочему столу (подробнее см. раздел «<u>Редактирование рабочего стола</u>»);
- настроить вывод данных, добавив необходимое количество виджетов (подробнее см. раздел «Управление виджетами»).

11.3 Редактирование рабочего стола

Выберите нужный рабочий стол. Нажмите кнопку 🛄 и из выпадающего списка выберите пункт **Редактировать**.

Откроется страница редактирования рабочего стола (см. «Рис. 197»).

егодняшние события 🔗 21c17a2d-21e1-4da6-b74f-f0abbabaa9b5		Назад
Название		
Сегодняшние события		
Период		
Сегодня		
Пользователи		
Выбрать		\sim
Группы пользователей		
Выбрать		~
	Сбросить	Сохранить

Рис. 197 – Страница редактирования рабочего стола

При необходимости измените данные о рабочем столе и нажмите кнопку Сохранить.

Настроить права доступа пользователей к рабочему можно следующими способами:

- в поле "Пользователи" из выпадающего списка выберите пользователей, которым будет доступен рабочий стол;
- в поле "Группы пользователей" из выпадающего списка выберите группы пользователей, которым будет доступен рабочий стол.

11.4 Управление виджетами

При открытии рабочего стола, данные выводятся в соответствии с заданными параметрами. Все данные визуализируются на рабочем столе с помощью виджетов. Настройка виджетов выполняется в специальном конструкторе (см. раздел «Конструктор виджетов»).

При работе с виджетами выполняются следующие процессы:

- 1. Установка периода и обновление данных виджета.
- 2. Добавление виджета на рабочий стол.
- 3. Переход к табличному представлению данных.
- 4. Редактирование виджета.
- 5. Копирование виджета.
- 6. Изменение расположения виджета.
- 7. Изменение размера виджета.
- 8. Удаление виджета.

11.4.1 Установка периода и обновление данных виджетов

При необходимости вы можете временно изменить период формирования данных, выставленный по умолчанию для рабочего стола.

Для этого выполните следующие действия:

- 1. Нажмите кнопку 🛱 . Откроется окно выбора временного диапазона.
- 2. Выберите период. Доступные значения:
 - за все время;
 - текущие: минута, час, день, месяц, год;
 - последние: минуты, часы, месяца, года;
 - период можно указать вручную в соответствующих полях. Поддерживается формат дат из «Grafana. Единицы измерения и временной диапазон».
- 3. Нажмите кнопку Применить.

Для обновления отображаемых данных нажмите кнопку 🗟.

Для того, чтобы информация по новым данным автоматически обновлялась, необходимо из выпадающего списка выбрать режим автообновления. Доступны следующие режимы: без автообновления, 1 сек, 30 сек, 1 мин, 5 мин.

11.4.2 Добавление виджета на рабочий стол

Для добавления виджета на рабочий стол выполните следующие действия:

- 1. Выберите нужный рабочий стол и нажмите кнопку + Добавить виджет
- 2. Выполните настройку виджета в конструкторе (подробнее см. раздел «<u>Конструктор</u> <u>виджетов</u>»).
- 3. Добавьте необходимое количество виджетов на рабочий стол.

11.4.3 Переход к табличному представлению данных

Платформа позволяет перейти к табличному представлению данных выбранного виджета.

Переход выполняется на соответствующую страницу в зависимости от настроек поля **Датасет** в конструкторе (подробнее см. раздел «<u>Конструктор виджетов</u>»). Например, если используется датасет "Инциденты", то переход будет в раздел **Инциденты** с уже сформированной таблицей по параметрам фильтра из виджета.

Для перехода к табличному представлению данных выберите нужный виджет и нажмите кнопку \mathcal{O} .

11.4.4 Редактирование виджета

Для редактирования виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.

- 2. Нажмите кнопку : и из выпадающего списка выберите пункт Редактировать.
- 3. Выполните настройку виджета в конструкторе (подробнее см. раздел «<u>Конструктор</u> <u>виджетов</u>»).

11.4.5 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

- 1. Перейдите на рабочий стол и выберите виджет.
- 2. Нажмите кнопку и из выпадающего списка выберите пункт Копировать настройки.
- 3. Затем вы можете передать настройки другому пользователю, или создать новый виджет на основе скопированного.

Чтобы применить скопированные настройки необходимо начать процесс создания или редактирования виджета. Для применения скопированных настроек нажмите кнопку в конструкторе виджетов (подробнее см. раздел «Конструктор виджетов»).

11.4.6 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

- 1. Перейдите на рабочий стол и выберите виджет.
- 2. Нажмите и удерживайте кнопку 🍄
- 3. Перемещайте мышку в нужном направлении.
- 4. Отпустите кнопку после перемещения.

11.4.7 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

- 1. Перейдите на рабочий стол и выберите виджет.
- 2. Нажмите и удерживайте правый нижний угол виджета (см. «Рис. 198»).

Количество	о новых
4	1

Рис. 198 – Кнопка изменения размера виджета

- 3. Перемещайте мышку в нужном направлении.
- 4. Отпустите правый нижний угол после перемещения.

11.4.8 Удаление виджета

Для удаления виджета с рабочего стола выполните следующие действия:

- 1. Перейдите на рабочий стол и выберите виджет.
- 2. Нажмите кнопку и из выпадающего списка выберите пункт Удалить.
- 3. Подтвердите удаление в открывшемся окне. Виджет будет удален с рабочего стола.

11.5 Копирование рабочего стола

Платформа Радар позволяет создавать рабочие столы на основе существующих. Для этого выберите нужный рабочий стол. Нажмите кнопку и из выпадающего списка выберите пункт **Создать копию**. Будет создан рабочий стол с аналогичными параметрами.

11.6 Создание отчета

Платформа Радар позволяет формировать отчеты, которые предоставляют наглядные данные, чтобы помочь вам оценить эффективность и производительность платформы.

Отчет можно сформировать в том числе и на основе данных, выведенных на рабочий стол.

Для этого выберите нужный рабочий стол и выполните следующие действия:

1. Нажмите кнопку и из выпадающего списка выберите пункт **Создать отчет**. Откроется окно "Создание отчета" (см. «Рис. 199»).

Создать отчёт		×
Название отчёта		
Отчет по основному рабочему столу		
Период		
Последние 2 месяца		Ë
	Отмена	Сохранить
	OTMena	Сохранить

Рис. 199 – Окно "Создать отчет"

- 2. Укажите следующие данные:
 - в поле "Название отчета" укажите название отчета;
 - в поле "Период" из выпадающего списка выберите период формирования отчета.
- 3. Нажмите кнопку Сохранить. Откроется страница с отчетом (см. «Рис. 200»).



Рис. 200 – Страница с отчетом

Дальнейшие действия над отчетом выполняются в разделе «Отчеты».

11.7 Удаление рабочего стола

Выберите нужный рабочий стол, нажмите кнопку *и* из выпадающего списка выберите пункт **Удалить**. Подтвердите удаление в открывшемся окне.

11.8 Grafana. Единицы измерения и временной диапазон

Grafana поддерживает следующие единицы измерения временного диапазона:

- s (секунды);
- m (минуты);
- h (часы);
- d (дни);
- w (недели);
- М (месяцы);
- у (годы).

Оператор минус позволяет сделать шаг назад во времени относительно выбранного значения текущей даты и времени, или значения **now**. Если необходимо отобразить полный период единицы измерения (день, неделю, месяц и т.д.), необходимо добавить «/<единица измерения времени>» в конце.

В таблице приведены примеры временных диапазонов:

Пример относительного диапазона	От	До
Последние 5 минут	now-5m	now
Прошедший день	now/d	now
На этой недели	now/w	now/w
Пока что на этой недели	now/w	now
В этом месяце	now/M	now/M
Пока что в этом месяце	now/M	now
Предыдущий месяц	now-1M/M	now-1M/M
Пока что в этом году	now/y	now

12. Конструктор виджетов

Платформа Радар позволяет визуализировать данные с помощью виджетов. Виджеты применяются при работе с данными в разделах **Рабочие столы** и **Отчеты**.

Перейти в конструктор виджетов можно несколькими способами:

- Способ 1. Из раздела Рабочие столы начать процесс добавления или редактирования виджета;
- Способ 2. Из раздела Отчеты начать процесс редактирования виджета.

Внешний вид конструктора виджетов приведен на «Рис. 201».

Отмена Сохранить 🖺 🗇 🗉			Режим отладки 🔵	Последние 2 месяца	Ĉ.	🖹 Гистограмма 🗸
Виджет с распределением открыты 1 0.8 0.6 0.4	ых инцидентов по критичности					 Основные настройки Показывать заголовок Заголовок Виджет с распределением открытых инцидентов по кр. Описание Вести
0.2 0 ,		3				 Легенда Сверху Снизу Скрыто Настройки визуализации
Основное Период Не выбран период () Набор полей () Полько уникальные значения Поле ()	Алиас ()					 Ш Линия ₫ Колонка Стек Стек Цветовая схема Roma
incident_id v status v risk_Jevel v		f Ū f Ū f Ū				> Настройка осей

Рис. 201 – Страница "Конструктор виджетов"

Конструктор состоит из следующих блоков:

- панель действий;
- режим визуализации/Режим отладки;
- конструктор запросов;
- настройка визуализации виджета, которая включает:
 - выбор типа виджета;
 - основные настройки;
 - настройку внешнего вида виджета.

Панель действий

Блок располагается вверху страницы конструктора виджетов (см. «Рис. 202»).



Рис. 202 – Конструктор виджетов. Блок "Панель действий"

С

На панели действий доступны следующие элементы управления:

Кнопка	Действие
Отмена	отмена изменений и возврат на предыдущую страницу
Сохранить	сохранение информации о виджете
Ê	вставить скопированные настройки виджета
ð	скопировать настройки
	переход к управлению предустановками настроек виджета
Режим отладки	включение/выключение режима отладки. При включенном режиме будут показаны данные, возвращаемые из источника
Ë	выбор периода формирования данных виджета
7.2	обновление отображаемой информации

Режим визуализации/Режим отладки

Блок располагается по центру конструктора. Переключение между режимами выполняется с помощью переключателя **Режим отладки**. В режиме визуализации можно посмотреть то, как виджет будет выглядеть на рабочем столе или странице отчета (см. «Рис. 203»).



Рис. 203 – Конструктор виджетов. Блок "Режим визуализации"

В режиме отладки можно посмотреть корректность работы написанных запросов (см. «Рис. 204»).

Отмена Сохранить 🖹 🗗 🗉 Режим от	ладки 🔵 Последние 30 дней 🛱 🖯
Запрос А Запрос В	
date	test
2024-04-03T15:55:14+03:00	32
2024-04-03T15:56:14+03:00	32
2024-04-03T15:57:14+03:00	33
2024-04-03T15:58:14+03:00	33
2024-04-03T15:59:14+03:00	46
2024-04-03T16:00:14+03:00	33
2024-04-03T16:01:14+03:00	33
2024-04-03T16:02:14+03:00	33
2024-04-03T16:03:14+03:00	32

Рис. 204 – Конструктор виджетов. Блок "Режим отладки"

Конструктор запросов

Блок располагается под режимом визуализации	і/отладки	(см. «	Рис. 2	<mark>05</mark> »)).
---	-----------	--------	--------	--------------------	----

🗄 🗦 Запрос А 🖉			:
III 🗸 Запрос В 🖉			
Источник данных	Датасет 🕕		
Метрики системы	Общие метрики		
Период			
Последний час 🛛 🛈			
Набор полей 🕕			
Поле 🕦	Алиас 🕕		
go_goroutines ~	test	f	
Дата 🗸		f	
+ Добавить			
Условия фильтрации 🕕			
+ Добавить			
+ Добавить запрос			

Рис. 205 – Конструктор виджетов. Блок "Конструктор запросов"

В конструкторе запросов доступны следующие элементы управления запросами:

Кнопка	Действие
+ Добавить запрос	добавление запроса
::	изменение расположения запроса
Ø	изменение наименования запроса
:	доступ к следующим действиям над запросом: – скопировать настройки; – вставить настройки; – дублировать; – удалить.
+ Добавить	добавление параметра
Ū	удаление параметра из запроса
F	добавление агрегацию в запрос
£	синий индикатор обозначает что к запросу добавлена агрегация. При повторном клике можно ее изменить

Настройка внешнего вида виджета

Блок располагается в правой части страницы конструктора и формируется в зависимости от выбранного виджета (см. «Рис. 206»).

🗠 Временной ряд 🗸 🗸	🕗 Круговая диаграмма 🗸	В Гистограмма ∨
> Основные настройки	> Основные настройки	> Основные настройки
> Легенда	> Легенда	> Легенда
> Настройки визуализации	> Настройки визуализации	> Настройки визуализации
> Настройка осей	> Настройка осей	> Настройка осей
🗉 Таблица 🗸	Аа Текст 🗸	🖾 Изображение 🗸
> Основные настройки	> Основные настройки	> Основные настройки
> Настройки колонок	> Текст	> Настройки визуализации
Метрика		
> Основные настройки		
> Настройки метрики		
> Настройки тренда		

Рис. 206 – Конструктор виджетов. Блок "Настройка внешнего вида виджета"

12.1 Особенности работы в конструкторе

Каждый виджет обладает своим уникальным способом визуализации данных и имеет ряд персональных настроек.

По типу запросов виджеты делятся на виджеты с серией запросов и на виджеты без серии запросов (простые):

- Для следующих типов виджетов можно задать серию запросов:
 - временной ряд;
 - гистограмма;
 - круговая диаграмма;
 - метрика;
 - таблица.
- Для следующих типов виджетов нельзя задать серию запросов:
 - текст;
 - изображение.

Стандартный процесс настройки виджета может выглядеть следующим образом:

- 1. Выберите тип виджета из выпадающего списка.
- 2. Укажите "Основные настройки виджета".
- 3. Если для виджета доступна настройка серии запросов, то включите Режим отладки.
- 4. Настройте запрос или серию запросов.
- 5. Обновите отображаемую информацию и проверьте работу запросов в Режиме отладки.
- 6. Удостоверьтесь что все настроенные запросы работают корректно.
- 7. Для настройки параметров визуализации отключите Режим отладки.
- 8. Укажите настройки визуализации серии запросов.
- 9. Удостоверьтесь что визуализация данных в виджете работает корректно.
- 10. Сохраните изменения нажав соответствующую кнопку.

12.2 Конструктор запросов

Управление запросами включает в себя следующие процессы:

- 1. Добавление запроса.
- 2. Дублирование запроса.
- 3. Копирование параметров запроса.
- 4. Удаление запроса.

12.2.1 Добавление запроса

Примечание: перед началом процесса добавления запроса рекомендуется включить **Режим отладки**. После изменения запроса рекомендуется обновлять данные с помощью кнопки \mathfrak{C} для проверки корректности запроса.

Для начала процесса добавления запроса нажмите кнопку + Добавить запрос

При необходимости вы можете изменить наименование запроса нажав кнопку

Добавление запроса можно условно разделить на несколько шагов:

- Шаг 1. Выбор источника данных и датасета.
- Шаг 2. Настройка периода формирования запроса.
- Шаг 3. Добавление набора полей, информация по которым будет обрабатываться запросом.
- Шаг 4. Настройка условий фильтрации выбранных полей.
- Шаг 5. Настройка группировки и сортировки выбранных полей.

12.2.1.1 Шаг 1. Выбор источника данных и датасета

На данном шаге необходимо выбрать источник данных, информация из которого будет обрабатываться запросом, и соответствующий набор данных - датасет (см. «Рис. 207»).

🗄 🗸 Запрос А 🖉	:
Источник данных	Датасет 🕕
Метрики системы	Кафка 🗸
Период Последний час × (i)	

Рис. 207 – Конструктор запросов. Выбор источника данных, датасета и периода

Соответствие источников данных и датасетов приведено в таблице:

Источник данных	Датасет
Основное	Инциденты
События	 Все; Нормализованные; Обработанные; Ошибки.
Метрики системы	 Менеджер кластера; Кафка; Коллектор логов; Коррелятор; Общие метрики; Хранилище событий; Коллектор метрик; Rsyslog.

Источник данных	Датасет
Табличные списки	Датасет формируется на основе данных, созданных пользователем при работе с табличными списками

12.2.1.2 Шаг 2. Выбор периода формирования запроса

Примечание: период, указанный для запроса, всегда имеет приоритет над периодом, указанным для рабочего стола или отчета.

Для изменения периода формирования запроса (см. «Рис. 207») выполните следующие действия:

- 1. Нажмите на соответствующее поле. Откроется окно выбора временного диапазона.
- 2. Выберите период. Доступные значения:
 - за все время;
 - текущие: минута, час, день, месяц, год;
 - последние: минуты, часы, месяца, года;
 - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
- 3. Нажмите кнопку Применить.

12.2.1.3 Шаг 3. Настройка набора полей

На данном шаге вы добавляете в запрос конкретные поля из выбранного датасета. Для каждого поля при необходимости можно задать **Алиас** и **Агрегацию**.

Алиас - это ключ, по которому можно определить выбранное поле при настройке визуализации виджета. Если вам необходимо чтобы визуализация строилась по одинаковым полям, но из разных запросов, то задайте этим полям одинаковый Алиас.

Агрегация - возможность выбрать функцию группировки результатов, которые будут выводиться при построении визуализации. Набор параметров агрегации для каждого поля является уникальным. Например, если вам необходимо чтобы по одной из шкал временного ряда, значения указывались по минутам, то задайте для поля с типом "Дата" соответствующую агрегацию. При отсутствии группировки агрегируются все результаты выбранного поля. Агрегацию можно выполнить по следующим функциям:

- count по любым значениям;
- min по минимальным значениям;
- max по максимальным значениям;
- sum по сумме всех значений;
- avg по среднему значению;
- interval по интервалу (минуты, часы и.д.).

Для настройки набора полей выполните следующие действия:

- 1. Если вы хотите, чтобы в запросе отображались только уникальные значения полей, то включите переключатель **Только уникальные значения**.
- 2. Нажмите кнопку + Добавить
- 3. Появятся параметры для настройки поля (см. «Рис. 208»).

Набор полей 🛈			
О Только уникальные значения			
Поле	Алиас		
Идентификатор происшествия \vee	cnt	f	Ū
Статус \lor		f	Ū
+ Добавить			

Рис. 208 – Конструктор запросов. Набор полей

- 4. Выберите необходимое поле датасета из выпадающего списка.
- 5. При необходимости укажите алиас.
- 6. При необходимости задайте агрегацию. Для этого нажмите на кнопку добавления агрегации. Откроется окно "Настройки поля" (см. «Рис. 209»).

Настройки поля		×
Аггрегация	Параметры	
interval	∨ По часам	~
Только уникальные значения	🔲 Использовать для периода	

Рис. 209 – Окно "Настройки поля"

- 7. Укажите в окне следующие данные:
 - в поле "Агрегация" из выпадающего списка выберите функцию группировки результатов запроса;
 - в поле "Параметры" из выпадающего списка выберите параметры функции;
 - если необходимо выполнять агрегацию только по уникальным значениям, то установите соответствующий флаг;
 - если необходимо чтобы агрегация применялась только в рамках заданного периода, то установите флаг **Использовать для периода** (только для полей с типом date).
- 8. Добавьте необходимое количество полей.
12.2.1.4 Шаг 4. Условия фильтрации

После добавления полей в запрос при необходимости можно указать точную фильтрацию для каждого поля, участвующего в запросе. Для добавления условия фильтрации выполните следующие действия:

1. Нажмите кнопку <u>+ Добавить</u>. Появятся параметры для настройки условия фильтрации (см. «Рис. 210»).

Набор полей 🛈		
О Только уникальные значения		
Поле	Алиас 🛈	
Уровень риска 🗸	test	F
Дата создания инцидента 🗸 🗸		f
+ Добавить		
Условия фильтрации 🕕		
Поле	Оператор	Значение
Уровень риска	ие равно 🗸	0 -+ Ū
Дата создания инцидента	не больше 🗸	2024-04-01
+ Добавить		

Рис. 210 – Конструктор запросов. Условия фильтрации

- 2. Выберите поле из выпадающего списка, по которому вы хотите настроить фильтрацию.
- 3. Выберите логический оператор.
- 4. Укажите значение оператора.
- 5. Добавьте фильтрацию по всем необходимым полям.

12.2.1.5 Шаг 5. Группировка и Сортировка

Примечание: данный шаг недоступен для полей из источника данных Метрики системы.

Группировка используется для объединения результатов по настроенным функциям агрегаций. Например, если вы хотите получить результаты по уровню риска инцидента и дате создания инцидента и при этом выставили агрегацию для поля "Уровень риска" в count, то вам необходимо будет выполнить группировку по полю "Дата создания". В результате вы получите группировку всех инцидентов с одинаковым уровнем риска по датам.

Для настройки нажмите кнопку <u>+ Добавить</u> и выберите поле, по которому вы хотите выполнить группировку (см. «Рис. 211»).

Поле	Алиас 🕕	
Уровень риска	✓	f
Дата создания инцидента	 ✓ 	f
+ Добавить		
Условия фильтрации 🛈		
+ Добавить		
Группировка 🕕		
Поле		
Дата создания инцидента	 ✓ □ 	
+ Добавить		
Сортировка 🕕		
+ Добавить		
Лимит 🕦	Оффсет 🕦	
-+	- +	

Рис. 211 – Конструктор виджетов. Группировка и сортировка

Сортировка настраивает порядок отображения результатов запроса: **asc/desc**. Для сортировки можно настроить следующие параметры:

- Лимит сколько элементов возвращать в запросе;
- Оффсет сколько элементов пропустить.

Для настройки сортировки выполните следующие действия:

- 1. Нажмите кнопку <u>+ Добавить</u>. Появятся параметры для настройки сортировки (см. «Рис. 211»).
- 2. Выберите поле из выпадающего списка, по которому вы хотите настроить сортировку.
- 3. Выберите направление сортировки: asc/desc.
- 4. В поле "Лимит" укажите значение лимита.
- 5. В поле "Оффсет" укажите значение оффсета.

12.2.2 Копирование запроса

Вы можете скопировать параметры запроса и передать их другому пользователю. Для этого выберите нужный запрос, нажмите кнопку и из выпадающего списка выберите пункт **Скопировать настройки**. Настройки будут скопированы в буфер обмена.

Для того чтобы применить скопированные настройки выберите нужный запрос, нажмите кнопку и из выпадающего списка выберите пункт **Вставить настройки**. Настройки из буфера обмена будут применены к запросу.

12.2.3 Дублирование запроса

Вы можете создать новый запрос на основе существующего. Для этого выберите нужный запрос,

нажмите кнопку и из выпадающего списка выберите пункт **Дублировать**. В списке запросов появится дубликат запроса.

12.2.4 Удаление запроса

Для удаления запроса выберите нужный запрос, нажмите кнопку *и* и из выпадающего списка выберите пункт **Удалить**.

12.3 Настройка внешнего вида виджета

Примечание: настройку внешнего вида виджета рекомендуется выполнять после настройки серии запросов и в режиме визуализации (переведите переключатель **Режим отладки** в состояние "выключен").

Настройку внешнего вида виджета условно можно разделить на следующие действия:

- выбор типа виджета из выпадающего списка;
- установка основных настроек виджета;
- персональная настройка выбранного типа виджета.

12.3.1 Основные настройки виджета

Блок "Основные настройки" является общим для всех типов виджетов (см. «Рис. 212»).

✓ Основные настройки	Ĉ
Показывать заголовок	
Заголовок	
Гистограмма	
Описание	
Распределение уровня угрозы по времени	

Рис. 212 – Основные настройки виджетов

В блоке доступны следующие настройки:

- Флаг "Показывать заголовок" включение/выключение отображения наименования виджета на рабочем столе/отчете;
- Заголовок наименование виджета;
- Описание дополнительная информация о виджете.

Пример отображения основных настроек приведен на «Рис. 213»



Содержимое виджета

Рис. 213 – Отображение основных настроек на виджете

12.3.2 Временной ряд

Виджет отображает график с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 214».



Рис. 214 – Виджет "Временной ряд"

Настройка внешнего вида виджета включает в себя следующие шаги:

- Шаг 1. Настройка осей для отображения графика.
- Шаг 2. Настройка визуализации результатов запроса.
- Шаг З. Настройка легенды.

Пример настроек приведен на «Рис. 215».

Последние 15 минут 📋 🖯	🗠 Временной ряд 🗸
	 > Основные настройки Улегенда
	Сверху Снизу Скрыто
	 ✓ Настройки визуализации Стиль Линия Колонка Стек Ω
17:05 17:10 17:15	Стиль Линейный
	 Скругленный Шаг - сначала
	🗌 Шаг - сконца
	Показывать точки Да Нет У Настройка осей Поле для оси Х. ()
	date ~
	Поле для оси Ү 🕕
	cnt 🗸

Рис. 215 – Виджет "Временной ряд". Настройки

12.3.2.1 Шаг 1. Настройка осей

Примечание: значения полей, которые доступны для выбора при настройке данного шага, формируются на основе данных, указанных в запросе (подробнее см. раздел «<u>Добавление</u> <u>запроса</u>»).

Настройка позволяет выбрать значения полей для оси Х и для оси Ү, по которым будет строиться график.

Для настройки осей выполните следующие действия:

- 1. Из выпадающего списка выберите поле для оси Х.
- 2. Из выпадающего списка выберите поле для оси Ү.
- 3. Проверьте отображение осей на виджете.

12.3.2.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать один из двух стилей графика:

- линия;
- колонка.

При выборе стиля "Линия" доступна возможность настроить дополнительные параметры:

- Внешний вид линий на графике:
 - линейный;
 - скругленный;
 - шаг с начала;
 - шаг с конца.
- Включение/выключение отображения точек.

Примеры визуализации графика приведены на «Рис. 216».



Рис. 216 – Примеры визуализации настроек виджета "Временной ряд"

Стек - настройка отвечает за группировку колонок или линий. Если вы настроили несколько запросов для виджета, то для удобства отображения мы можете установить флаг **Стек**.

Если в параметрах различных серий запросов используются разный набор полей, то чтобы объединить их необходимо ввести одинаковое название для каждого **Алиас** (подробнее см. раздел «<u>Добавление запроса</u>»). Для объединения полей при визуализации необходимо в параметрах блока "Настройка осей" указать **Алиас**.

Пример отображения с включенным и выключенным стеком приведен на «Рис. 217».





Рис. 217 – Пример визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

- 1. Выберите стиль: линия или колонка.
- 2. При необходимости включите стек, установив соответствующий флаг.
- 3. Если выбран стиль линия, то выберите ее тип: линейный, скругленный, шаг с начала, шаг с конца.
- 4. При необходимости включите отображение точек, включив соответствующий переключатель.

12.3.2.3 Шаг З. Легенда

Настройка отвечает за выбор способа отображения легенды на графике. Выберите место отображения легенды: сверху, снизу или не отображать.

12.3.3 Круговая диаграмма

Виджет отображает группировку по выбранным параметрам с процентным распределением. Пример визуализации приведен на «Рис. 218».



Рис. 218 – Виджет "Круговая диаграмма"

Пример настроек приведен на «Рис. 219».

🖉 Кругова	ая диаграмма	\sim
> Основны	е настройки	
\vee Легенда		۲°
Сверху	Снизу Скрыто	
\vee Настрой	ки визуализации	٦° ک
Отображать	проценты	
Отображать 🔽	значения	
\vee Настрой	ка осей	Ĉ
Стратегия о	бработки некорректных значений	
• Использ	овать значения по-умолчанию	
🕖 Игнорир	оовать	
Поле по оси	X 🕕	
cnt		\sim
Поле по оси	Y (1)	

Рис. 219 – Виджет "Круговая диаграмма". Настройки

Для настройки внешнего вида виджета выполните следующие действия:

1. В блоке "Настройка осей" укажите следующие данные:

- выберите стратегию обработки некорректных значений: игнорировать или использовать по умолчанию;
- из выпадающего списка выберите поле для оси Х;
- из выпадающего списка выберите поле для оси Ү.
- 2. В блоке "Настройка визуализации" при необходимости включите отображение следующих данных:
 - проценты по выбранным полям;
 - значения по выбранным полям.
- 3. В блоке "Легенда" выберите место расположения легенды.

Примечание: значения полей, которые доступны для выбора при настройке в блоке "Настройка осей", формируются на основе данных, указанных в запросе (подробнее см. раздел «<u>Добавление</u> <u>запроса</u>»).





Рис. 220 – Примеры визуализации настроек виджета "Круговая диаграмма"

12.3.4 Таблица

Виджет отображает выбранные показатели в табличном варианте. Пример визуализации приведен на «Рис. 221».

таблица с топ-5 активов (или групп активов) по открыты	м инцидентам
Наименование актива	Количество
DESKTOP-AD02	2
DESKTOP-AD03	1
DESKTOP-AD04	2
DESKTOP-AD05	1
DESKTOP-AD09	1

Рис. 221 – Виджет "Таблица"

Пример блока "Настройки" приведен на «Рис. 222».

⊟ Ta	аблица	\sim
> Ocr	ювные настройки	
\sim Hac	тройки колонок	٢,٢
		创
key	date	~
label	Дата	
Сгр	уппировать значения	
::		Ū
key	go_goroutines	~
label	Количество потоков	
🗹 Сгр	уппировать значения	
+ д	обавить	
Страте О Ис	гия обработки некорректных значений пользовать значения по-умолчанию	
🔾 Иг	норировать	

Рис. 222 – Виджет "Таблица". Настройки

Для настройки внешнего вида виджета выполните следующие действия:

- 1. Для добавления колонок в таблицу нажмите кнопку + Добавить. Добавьте необходимое количество колонок.
- 2. В поле "key" из выпадающего списка выберите поле или алиас из набора полей запроса, значения которого будут отображаться в колонке.

- 3. В поле "label" укажите наименование колонки, которое будет отображаться в виджете.
- 4. При необходимости установите флаг "Сгруппировать значения" для объединения результатов запроса по выбранному полю в одну ячейку таблицы.
- 5. Выберите стратегию обработки некорректных значений: игнорировать или использовать по умолчанию.

Примечание: значения полей, которые доступны для выбора при настройке колонок таблицы, формируются на основе данных, указанных в запросе (подробнее см. раздел «<u>Добавление</u> <u>запроса</u>»).

Примеры визуализации настроек приведены на «Рис. 223».

Значения сгруппированы		Без группировки	
Дата	Количество потоков	Дата	Количество потоков
2024-04-05T08:09:07+03:00		2024-04-05T08:09:07+	03:00 34
2024-04-05T08:10:07+03:00	34	2024-04-05T08:10:07+	03:00 34
2024-04-05T08:11:07+03:00		2024-04-05T08:11:07+	03:00 34
2024-04-05T08:12:07+03:00	25	2024-04-05T08:12:07+	03:00 35
2024-04-05T08:13:07+03:00	35	2024-04-05T08:13:07+	03:00 35
2024-04-05T08:14:07+03:00	34	2024-04-05T08:14:07+	03:00 34
2024-04-05T08:15:07+03:00	35	2024-04-05T08:15:07+	03:00 35
2024-04-05T08:16:07+03:00	34	2024-04-05T08:16:07+	03:00 34
2024-04-05T08:17:07+03:00	49	2024-04-05T08:17:07+	03:00 49

Рис. 223 – Примеры визуализации настроек виджета "Таблица"

12.3.5 Текст

Примечание: данный тип виджета не поддерживает серию запросов.

Виджет отображает текст, указанный пользователем.

Пример визуализации приведен на «Рис. 224».

Ежедневная проверка 🕕	¢‡→	:
Памятка при работе с рабочим столом:		
 Сначала проверь поток событий. Затем выяви угрозы. Составь топ -5 угроз по критичности Создай и распечатай отчет. Свяжись по телефону с руководителем по номеру 0511. Доложи об угрозах. 		

Рис. 224 – Виджет "Текст"

Пример настроек приведен на «Рис. 225».

Aa Tekct	
 Основные настройки 	
Іоказывать заголовок	
Заголовок	
Ежедневная проверка	
Описание	
Виджет для описания ежедневных пр	оверок
∽ Текст	
∽ Текст (онтент	
 Текст Контент Памятка при работе с рабочим столо 	м:
 Текст Контент Памятка при работе с рабочим столо Сначала проверь поток событий. 	м:
 Текст Контент Памятка при работе с рабочим столо 1. Сначала проверь поток событий. 2. Затем выяви угрозы. 	м:
 Текст Контент Памятка при работе с рабочим столо 1. Сначала проверь поток событий. 2. Затем выяви угрозы. 3. Составь топ -5 угроз по критичнос 4. Созгавь и распециатай отцет. 	м: ти
 Текст Контент Памятка при работе с рабочим столо Сначала проверь поток событий. Затем выяви угрозы. Составь топ -5 угроз по критичнос Создай и распечатай отчет. Свяжись по телефону с руководите 	м: ти елем по номеру

Рис. 225 – Виджет "Текст". Настройки

Для настройки виджета в блоке "Текст" укажите необходимую информацию.

12.3.6 Гистограмма

Виджет отображает столбчатую диаграмму с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 226».



Рис. 226 – Виджет "Гистограмма"

Настройка внешнего вида виджета включает в себя следующие шаги:

- Шаг 1. Настройка осей для отображения графика.
- Шаг 2. Настройка визуализации результатов запроса.
- Шаг З. Настройка легенды.

Пример настроек приведен на «Рис. 227».

Последние 6 месяцев	ĉ	🖻 Гистограмма 🗸
7.3		 ► Тистограмма Настройки визуализации Стиль Линия Колонка Стек ① Цветовая схема Walden ✓ Настройка осей Настройка осей Настройка оси Х Поле ① risk_level Кастомный диапазон ① ✓ Использовать значения не входящие в диапазоон Диапазон + Добавить Настройка оси Y
		Поле () спт ~ Поле для группировки ()
		Выбрать ~

Рис. 227 – Виджет "Гистограмма". Настройки

12.3.6.1 Шаг 1. Настройка осей

Примечание: значения полей, которые доступны для выбора при настройке шага, формируются на основе данных, указанных в запросе (подробнее см. раздел «<u>Добавление запроса</u>»).

Настройка позволяет выбрать значения полей для оси Х и для оси Ү, по которым будет строиться график.

Для настройки осей выполните следующие действия:

- 1. Из выпадающего списка выберите поле для оси Х.
- 2. Если вы хотите задать конкретный диапазон по оси X, по которому будут визуализироваться результаты запроса, то установите флаг "Кастомный диапазон". Появятся поля для настройки диапазона:
 - нажмите кнопку + Добавить
 - укажите диапазон в соответствующем поле;
 - если вы хотите использовать значения, не входящие в диапазон, то установите соответствующий флаг.
- 3. Из выпадающего списка выберите поле для оси Ү.
- 4. Проверьте отображение осей на виджете.

12.3.6.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать следующие параметры:

- стиль диаграммы: линия или колонка;
- включить или выключить стек;
- выбрать цветовую схему диаграммы.

При выборе стиля "Линия" доступна возможность настроить дополнительные параметры:

- Внешний вид линий на диаграмме:
 - линейный;
 - скругленный;
 - шаг с начала;
 - шаг с конца.
- Включение/выключение отображения точек.

Примеры визуализации графика приведены на «Рис. 228».



Рис. 228 – Примеры визуализации настроек виджета "Гистаграмма".

Стек - настройка отвечает за группировку колонок или линий. Если вы настроили несколько запросов для виджета, то для удобства отображения мы можете установить флаг **Стек**.

Если в параметрах различных серий запросов используются разный набор полей, то чтобы объединить их необходимо ввести одинаковое название для каждого **Алиас** (подробнее см. раздел «<u>Добавление запроса</u>»). Для объединения полей при визуализации необходимо в параметрах блока "Настройка осей" указать **Алиас**.

Пример отображения с включенным и выключенным стеком приведен на «Рис. 229».



Рис. 229 – Примеры визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

- 1. Выберите стиль: линия или колонка.
- 2. При необходимости включите стек, установив соответствующий флаг.
- 3. Если выбран стиль линия, то выберите ее тип: линейный, скругленный, шаг с начала, шаг с конца.
- 4. Выберите цветовую схему.

12.3.6.3 Шаг З. Легенда

Настройка отвечает за выбор способа отображения легенды на графике. Выберите место отображения легенды: сверху, снизу или не отображать.

12.3.7 Метрика

Виджет отображает тренд изменения выбранного показателя за период времени. Пример внешнего вида приведен на «Рис. 230».



Рис. 230 – Виджет "Метрика"

Пример настроек приведен на «Рис. 231».

🗠 Метрика	\sim
> Основные настройки	
imes Настройки метрики	Ĉ
Использовать значение из поля	
go_goroutines	~
Серия с данными	
А	~
imes Настройки тренда	Ĉ
Включить отображение тренда	
~	
Инвертировать тренл	
Инвертировать тренд	
Инвертировать тренд Поле со значениями	
Инвертировать тренд Поле со значениями go_goroutines	~
Инвертировать тренд Поле со значениями go_goroutines Серия с данными	~
Инвертировать тренд Поле со значениями go_goroutines Серия с данными А	~
Инвертировать тренд Поле со значениями go_goroutines Серия с данными А Серия для прогнозирования	~
Инвертировать тренд Поле со значениями go_goroutines Серия с данными А Серия для прогнозирования В	

Рис. 231 – Виджет "Метрика". Настройки

Для настройки виджета выполните следующие действия:

- 1. В блоке "Настройки метрики" укажите следующие данные:
 - в поле "Использовать значение из поля" выберите поле, значение из которого будет использоваться при подсчете метрики;
 - в поле "Серия с данными" из выпадающего списка выберите запрос.
- 2. В блоке "Настройки тренда" укажите следующие данные:
 - для отображения тренда на виджете установите соответствующий флаг;
 - для изменения направления отображения тренда установите флаг "Инвертировать тренд";
 - в полях "Поле со значениями" и "Серия с данными" выберите запрос и поле, значение из которого будет использоваться для отображения численной части метрики;
 - в поле "Серия для прогнозирования" выберите запрос, по которому будет отображаться изменение тренда.

Примечание: значения полей, которые доступны для выбора при настройке в блоках "Настройки метрики" и "Настройки тренда", формируются на основе данных указанных в запросе (подробнее см. раздел «<u>Добавление запроса</u>»).

Примеры визуализации виджета приведены на «Рис. 232».

Метрика с трендом	Метрика - Инвертированный тренд	Метрика
37 1	37↓	37

Рис. 232 – Примеры визуализации настроек виджета "Метрика"

12.3.8 Изображение

Виджет отображает изображение, загруженное пользователем.

Пример внешнего вида представлен на «Рис. 233».

	K 11	lan.									•
	Mag	идочты								(per s	(and a second second second second second second second second second second second second second second second
		Logica e	-		20.000	• 🖬			fearers and the	an I dama a ta iy	par tana senye
Платформа							_		_		
Радар						in vie	850 TM	19.00 110	 1100 000	n arter	
- Ключевое жено жффективного SOC		10 ×	nai ()		- 0 - 1		171 0 1701 0 10	means () man	 NUMBER OF	erite inter	entrati ()
		0				0.0.000		retire 12 critican	 		
Скачать презентацию	0	•	-	•	-		M We beautypeter		 		
	- D	•	-	•	-	-	-		 		8
		-							 10.00		

Рис. 233 – Виджет "Изображение"

Пример настроек приведен на «Рис. 234».

🖾 Изобрах	кение	
> Основные	настройки	
✓ Настройк	и визуализации	
Соответствие	э сторон	
Вписать	Растянуть	
Изображение	9	
Выб	ерите или перетащите изображение .png, .jpg, .jpeg	

Рис. 234 – Виджет "Изображение". Настройки

Для настройки виджета выполните следующие действия:

- 1. Выберите соответствие сторон: вписать изображение или растянуть изображение.
- 2. Загрузите изображение с помощью стандартного механизма выбора и загрузки изображения на сайт.

12.4 Копирование виджета

Вы можете скопировать параметры виджета и передать их другому пользователю или создать новый виджет на основе существующего.

Есть несколько способов для копирования параметров:

- Способ 1. В конструкторе виджетов нажмите кнопку . Настройки виджета будут скопированы в буфер обмена.
- Способ 2. Перейдите в раздел Администрирование → Рабочие столы, выберите виджет, нажмите кнопку и из выпадающего списка выберите пункт Копировать настройки.
- Способ 3. Перейдите в раздел Администрирование → Отчеты, выберите виджет, нажмите кнопку и из выпадающего списка выберите пункт Копировать настройки.

Для того чтобы применить скопированные настройки откройте конструктор виджетов и нажмите кнопку 🗐.

12.5 Предустановки

Предустановки используются для быстрой настройки виджетов на основе шаблона.

Вы можете добавить собственные шаблоны настроек виджетов в список предустановок.

В открывшемся окне "Предустановки" (см. «Рис. 235») выберите предустановку и нажмите кнопку </

Предустановки	×
Q Введите значение	
Тарлица	🗸 Ш
Гистограмма	
Метрика	✓ ÎI
Временной ряд	
Круговая диаграмма	
Текст	
	Создать новую

Рис. 235 – Окно "Предустановки"

Для создания предустановки выполните следующие действия:

- 1. Настройте запросы и визуализацию виджета.
- 2. Нажмите кнопку Ш и в открывшемся окне "Предустановки" (см. «Рис. 235») нажмите кнопку Создать новую.
- 3. В открывшемся окне укажите название предустановки.
- 4. Нажмите кнопку Создать.

13. Отчеты

13.1 Общие данные

Платформа Радар позволяет формировать отчеты, которые предоставляют наглядные данные, чтобы помочь вам оценить эффективность и производительность платформы.

Отображение информации выполняется с помощью следующих типов виджетов:

- временной ряд;
- круговая диаграмма;
- таблица;
- текст;
- гистограмма;
- метрика;
- изображение.

Подробнее о каждом типе виджета вы можете ознакомиться в разделе «Конструктор виджетов».

Работа с отчетами включают в себя следующие процессы:

- 1. «<u>Создание отчета</u>».
- 2. «<u>Конструктор отчета</u>».
- 3. «Настройка расписания генерации отчета».
- 4. «<u>Настройка прав доступа к отчету</u>».
- 5. «<u>Импорт отчетов</u>».
- 6. «<u>Экспорт отчетов</u>».
- 7. «<u>Удаление отчета</u>».

В разделе «<u>Архив отчетов</u>» выполняется работа с архивом сгенерированных отчетов.

Для работы с отчетами перейдите в новый интерфейс и откройте раздел Администрирование → Отчеты (см. «Рис. 236»).

≡	К плигео 172.30.254.138 ∨ Отчёты © База знаний @ аdr						admin \checkmark		
ଜ	Отчёты								
Q									
1	С Создать Удалить Удалить все Экспортировать Экспортировать все Импортировать			Импортировать			Ô		
-8	Название Создано				Правило генерации				
С∎ Новый отчет		13:36:24 09.07.2024		*/15 * * * *		0			
ů			Ежедневный отчет	t 14:10:51 19.07.2024		15 23 * * *		0	
<i>%</i> :	2 10 / страница ~								
ж									
494									
@									

Рис. 236 – Раздел "Отчеты"

В разделе отображается следующая информация:

- Название наименование отчета;
- Создано дата и время создания отчета;
- Правило генерации расписание автоматической генерации отчета.

13.2 Создание отчета

Перейдите в раздел Администрирование --- Отчеты и нажмите кнопку Создать.

Откроется окно "Создать отчет" (см. «Рис. 237»).

Создать отчёт	×
Название	
Ежемесячный отчет	
	Создать

Рис. 237 – Окно "Создать отчет"

Выполните в окне следующие действия:

- 1. В поле "Название" укажите название отчета.
- 2. Нажмите кнопку Создать.
- 3. Будет создан отчет и произойдет переход в конструктор отчета (см. «Рис. 238»).

â	Hasag 🔟 Ō 였 🕃 😚 100% ~	Новый отчет		Настройки Виджеты
Q			កា	> Основное
()			Ð	> Верхний колонтитул
ςΞ				> Нижний колонтитул
đ			Ω	> Стили
₩.				
х				
411				
Ø				

Рис. 238 – Страница "Конструктор отчета"

13.3 Конструктор отчета

Примечание: при настройке отчета все изменения автоматически сохраняются.

Настройка отчета выполняется на странице "Конструктор отчета" (см. «Рис. 239»).



Рис. 239 – Интерфейс страницы "Конструктор отчета"

Страницу можно открыть следующими способами:

- перейти в раздел Администрирование → Отчеты, выбрать нужный отчет из списка и нажать кнопку 🖉 в соответствующей строке;
- выполнить процесс создания отчета. После создания отчета страница "Конструктор отчета" откроется автоматически.

Внешний вид отчета формируется в зависимости от выставленной пользователем конфигурации настроек страниц отчета и виджетов.

Конструктор состоит из следующих блоков:

- панель действий, где располагаются элементы управления;
- рабочая область, где располагаются страницы отчета, на которых отображаются виджеты;
- настройка страниц, где выполняется настройка внешнего вида страниц отчета.

Панель действий

Блок располагается вверху конструктора (см. «Рис. 240»).



Рис. 240 – Страница "Конструктор отчета". Блок "Панель действий"

На панели действий доступны следующие элементы управления:

Кнопка	Действие
Назад	возвращение к списку отчетов
Ū	удаление отчета
Ō	настройка расписания генерации отчетов
<u>A</u>	настройка прав доступа пользователей к отчету
₽	экспорт отчета в файл формата .pdf
9	просмотр списка сгенерированных по расписанию отчетов
100% ~	изменение масштаба отображения страниц отчета

Рабочая область

Пример внешнего вида блока приведен на «Рис. 241».



Рис. 241 – Страница "Конструктор отчета". Блок "Рабочая область"

В рабочей области доступны следующие элементы управления:

Кнопка	Действие
回	удаление страницы из отчета
+	добавление страницы в отчет
$\hat{\nabla}$	перемещение страницы вниз. После действия текущая страница поменяется местами со следующей страницей
仑	перемещение страницы вверх. После действия текущая страница поменяется местами с предыдущей страницей

При наведении курсора на виджет становятся доступны следующие элементы управления:

Кнопка	Действие
	доступ к следующим действиям над виджетом: – редактирование; – удаление; – копирование настроек.
5	изменение размера виджета

Настройка страниц

Блок состоит из двух вкладок:

- Настройки настройки страниц отчета, включающие в себя:
 - Основное настройка периода и правила генерации наименования отчета;
 - Верхний колонтитул настройка текста и изображения на верхнем колонтитуле;
 - Нижний колонтитул настройка текста, нумерации страниц и отображения даты на нижнем колонтитуле;

+ Добавить страницу

- Стили настройка используемых шрифтов.
- Виджеты список доступных типов виджетов, которые можно добавить на страницу отчета.

Настройка отчета состоит из следующих процессов:

- 1. Добавление страницы.
- 2. Выбор периода формирования данных виджетов.
- 3. Настройка наименования отчета в момент генерации.
- 4. Настройка страниц, которая включает в себя:
 - настройку верхнего колонтитула;
 - настройку нижнего колонтитула;
 - настройку стиля шрифтов.
- 5. Настройка виджетов, которая включает в себя:
 - добавление виджета на страницу отчета;
 - редактирование виджета;
 - копирование настроек виджета;
 - изменение размера виджета;
 - изменение расположения виджета;
 - удаление виджета.
- 6. Изменение порядка страниц.
- 7. Удаление страницы.

13.3.1 Добавление страницы

На страницах можно расположить виджеты для отображения данных.

Добавление страниц в отчет выполняется следующим образом:

- если в отчете нет страниц, то нажмите кнопку
- если в отчете уже есть страницы, то нажмите кнопку 🗠

Добавьте необходимое количество страниц в отчет.

13.3.2 Выбор периода формирования данных виджетов

Выбор периода формирования данных виджетов выполняется в блоке **Настройки** → **Основное** (см. «Рис. 242»).

	Настройки Виджеты	
	∨ Основное	Ĉ
	Период	
	Последние 30 минут	Ë
Быстрый фильтр	Временной диапазон	
> Текущие	От *	
> Минуты	now-30m	Ë
> Часы	До *	
	now	Ë
> Дни		. (
> Месяца	Поддерживается формат даты и	13 Grafana
	Пр	именить

Рис. 242 – Выбор периода формирования данных виджетов

Для настройки периода выполните следующие действия:

- 1. В поле **Период** нажмите кнопку ¹. Откроется окно выбора временного диапазона (см. «Рис. 242»).
- 2. Выберите период. Доступные значения:
 - текущие: минута, час, день, месяц, год;
 - последние: минуты, часы, месяца, года;
 - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
- 3. Нажмите кнопку Применить.

13.3.3 Настройка наименования отчета в момент генерации

Вы можете настроить расписание генерации отчета (подробнее см. раздел «<u>Настройка расписания</u> <u>генерации отчета</u>»).

В момент генерации, отчету присваивается наименование в соответствии с настроенным правилом.

Настройка правила выполняется в блоке **Настройки** → **Основное**. В поле "Маска для генерации названия" укажите необходимую маску (см. «Рис. 243»).

Настройки	Виджеты	
✓ Основное		Ç,
Период		
Последние	30 минут	Ë
Маска для ге	нерации названия	1
##NAME##,	##DAY##, ##MON	TH##, ##YE/

Рис. 243 – Настройка маски для генерации названия

Доступные значения:

- ##NAME## название отчета;
- *##*ID*##* идентификатор отчета;
- ##MINUTE## минута в момент генерации;
- ##HOUR## час в момент генерации;
- ##DAY## день в момент генерации;
- ##MONTH## месяц в момент генерации;
- ##YEAR## год в момент генерации.

13.3.4 Настройка страниц

13.3.4.1 Настройка верхнего колонтитула

При необходимости вы можете настроить отображение заголовка и изображение в верхнем колонтитуле.

Настройка выполняется в блоке **Настройки** → **Верхний колонтитул** (см. «Рис. 244»).

зображение Заголовок			Настройки Виджеты		
Послед	ние 30 дней		□ ● ①	 > Основное > Верхний колонтитул С[*] Показывать верхний колонтитул 	
Гистограмма 2 1.5 1 0.5 0 1.1.1.1 5.9	Круговая 1 8.6	диаграмма	Ŷ	 Показывать на всех страницах Заголовок Последние 30 дней Изображение 	
Метрика с трендом	Последний час 50↓	^{Метрика}			
Временной ряд	-O- A -O- B			Удалить > Нижний колонтитул > Стили	

Рис. 244 – Настройка верхнего колонтитула

Для настройки верхнего колонтитула выполните следующие действия:

- 1. Для отображения верхнего колонтитула установите флаг "Показывать верхний колонтитул".
- 2. Для отображения верхнего колонтитула на всех страницах отчета установите флаг "Показывать на всех страницах".
- 3. В поле "Заголовок" укажите заголовок отчета.
- 4. В поле "Изображение" загрузите изображение с помощью стандартного механизма выбора и загрузки изображения на сайт.

13.3.4.2 Настройка нижнего колонтитула

Для многостраничных отчетов вы можете настроить отображение нумерации страниц, даты и текста в нижнем колонтитуле.

Настройка выполняется в блоке Настройки → Нижний колонтитул (см. «Рис. 245»).

Метрика с трендом	Последний час	Метрика	
			> Верхний колонтитул
50 ↑	50↓	50	✓ Нижний колонтитул
			Показывать нижний колонтитул
Временной ряд			Показывать на первой странице
	- O- A - O- B		
60			
30			Показывать дату
20			
20 10 15:45 15:50 15:55	16:00 16:05 16:10 16:15 16:20	16:25 16:30 16:35 16:40	
10 10 15:45 15:50 15:55	16:00 16:05 16:10 16:15 16:20	16:25 16:30 16:35 16:40	Текст
20 10 15:45 15:50 15:55	16:00 16:05 16:10 16:15 16:20	16:25 16:30 16:35 16:40	Текст Конфиденциально

Рис. 245 – Настройка нижнего колонтитула

Для настройки нижнего колонтитула выполните следующие действия:

- 1. Для отображения нижнего колонтитула установите флаг "Показывать нижний колонтитул".
- 2. Для отображения нижнего колонтитула на первой странице отчета установите флаг "Показывать на первой странице".
- 3. Для отображения нумерации страниц установите флаг "Показать номер страницы".
- 4. Для отображения даты генерации отчета установите флаг "Показывать дату".
- 5. В поле "Текст" укажите необходимый текст.

13.3.4.3 Настройка стиля шрифта

Вы можете настроить стиль шрифта, отображаемый в виджетах.

Настройка выполняется в блоке Настройки - Стили.

Для выбора стиля шрифта в поле "Используемый шрифт" из выпадающего списка выберите шрифт.

При необходимости вы можете загрузить собственный стиль шрифта. Для этого нажмите кнопку **Загрузить** и укажите путь к файлу со стилем шрифта.

13.3.5 Настройка виджетов

Данные, формируемые для отчета, отображаются с помощью виджетов. Настройка виджетов включат в себя следующие процессы:

- 1. Добавление виджета на страницу отчета.
- 2. Редактирование виджета.
- 3. Копирование настроек виджета.

- 4. Изменение расположения виджета.
- 5. Изменение размера виджета
- 6. Удаление виджета.

13.3.5.1 Добавление виджета

Добавление виджета на страницу отчета выполняется из вкладки Виджеты (см. «Рис. 246»).



Рис. 246 – Страница "Конструктор отчета". Вкладка "Виджеты"

Для добавления виджета на страницу отчета выполните следующие действия:

- 1. Наведите курсор мыши на нужный виджет и зажмите ЛКМ.
- 2. Перетащите виджет на страницу отчета. Место, на котором можно расположить виджет, будет подсвечено.
- 3. Отпустите ЛКМ.
- 4. Добавьте необходимое количество виджетов в отчет.

13.3.5.2 Редактирование виджета

Для редактирования виджета выполните следующие действия:

- 1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
- 2. Нажмите кнопку : и из выпадающего списка выберите пункт Редактировать.

3. Выполните настройку виджета в конструкторе (подробнее см. раздел «<u>Конструктор</u> виджетов»).

13.3.5.3 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

- 1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
- 2. Нажмите кнопку и из выпадающего списка выберите пункт Копировать настройки.
- 3. Затем вы можете передать настройки другому пользователю, или создать новый виджет на основе скопированного.

Чтобы применить скопированные настройки необходимо начать процесс редактирования виджета.

Для применения скопированных настроек нажмите кнопку 🗐 в конструкторе виджетов (подробнее см. раздел «<u>Конструктор виджетов</u>»).

13.3.5.4 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

- 1. Перейдите на страницу "Конструктор отчета" и наведите курсор мыши на нужный виджет. Курсор мыши примет следующий вид: 😳.
- 2. Зажмите ЛКМ и перемещайте мышку в нужном направлении.
- 3. Отпустите ЛКМ после перемещения.

13.3.5.5 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

- 1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
- 2. Нажмите и удерживайте кнопку 🍾 в правом нижнем углу виджета.
- 3. Перемещайте мышку в нужном направлении.
- 4. Отпустите кнопку после перемещения.

13.3.5.6 Удаление виджета

Для удаления виджета со страницы отчета выполните следующие действия:

- 1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
- 2. Нажмите кнопку : и из выпадающего списка выберите пункт Удалить.
- 3. Подтвердите удаление в открывшемся окне. Виджет будет удален со страницы отчета.

13.3.6 Изменение порядка страниц

Если у вас многостраничный отчет, то при необходимости вы можете изменить порядок страниц.

Для перемещения страницы вниз, выберите нужную страницу и нажмите кнопку abla. Выбранная страница поменяется местами со следующей страницей.

Для перемещения страницы вверх, выберите нужную страницу и нажмите кнопку **1**. Выбранная страница поменяется местами с предыдущей страницей.

13.3.7 Удаление страницы

Для удаления страницы из отчета, выберите нужную страницу и нажмите кнопку 🔟.

13.4 Настройка расписания генерации отчета

Работа с генерацией отчетов по расписанию проходит по следующему сценарию:

- 1. Настройка расписания генерации отчета пользователем.
- 2. Автоматическая генерация отчета по расписанию с сохранением отчетов в архив.
- 3. Просмотр архива пользователем и экспорт выбранных отчетов в виде файлов.

Для настройки расписания генерации отчета выполните следующие действия:

1. Настройте отчет и нажмите кнопку 🕐. Откроется окно "Планировщик" (см. «Рис. 247»).

Планировщик		×
Cron выражение		
* 0-11 * * *		
	Удалить задачу	Сохранить

Рис. 247 – Окно "Планировщик"

- 2. Укажите в окне Стоп выражение.
- 3. Нажмите кнопку Сохранить. Будет создана задача планировщика.

Для удаления задачи планировщика необходимо выбрать отчет, для которого настроено расписание, нажать кнопку \overline{O} и в открывшемся окне нажать кнопку **Удалить задачу**.

13.4.1 Просмотр истории генерации отчета

Для просмотра архива по отчету перейдите на страницу "Конструктор отчета" и нажмите кнопку ⁽¹⁾. Откроется окно "Список отчетов" (см. «Рис. 248»).

Название	Создан	Действия
Отчет 1	11.04.2024 13:26:44	↓
Отчет 1	11.04.2024 13:26:44	*
Отчет 1	11.04.2024 13:26:44	↓
Отчет 1	11.04.2024 13:26:44	↓
Отчет 1	11.04.2024 13:26:44	↓

Рис. 248 – Окно "Список отчетов"

В окне отображается следующая информация:

- Название название отчета;
- Создан дата и время генерации отчета.

Для экспорта отчета нажмите кнопку 🔄.

Для просмотра истории генерации по всем отчетам нажмите кнопку **Посмотреть больше** (подробнее см. раздел «<u>Архив отчетов</u>»).

13.5 Настройка прав доступа к отчету

Перейдите на страницу "Конструктор отчета" и нажмите кнопку 🔍. Откроется окно "Редактирование прав" (см. «Рис. 249»).

\sim
~
Сбросить Сохранить

Рис. 249 – Окно "Редактирование прав"

Настройте права доступа одним из следующих способов:

- в поле "Пользователи" из выпадающего списка выберите пользователей, которым будет доступен отчет;
- в поле "Группы пользователей" из выпадающего списка выберите группы пользователей, которым будет доступен отчет.

13.6 Импорт отчетов

Для импорта отчетов выполните следующие действия:

- 1. Перейдите в раздел Администрирование Отчеты.
- 2. Нажмите кнопку Импортировать.
- 3. В открывшемся окне укажите путь к архиву с отчетами.
- 4. Нажмите кнопку Открыть.

13.7 Экспорт отчетов

Выполнить экспорт отчетов можно двумя способами:

- экспорт в файл формата .pdf;
- экспорт в архив.

Способ 1. Экспорт в файл формата .pdf

- 1. Перейдите на страницу "Конструктор отчета".
- 2. Настройте отчет и нажмите кнопку 💽.
- 3. В открывшемся окне укажите путь для сохранения отчета.
- 4. Отчет будет сохранен в файл формата .pdf.

Способ 2. Экспорт в архив

Для экспорта одного или нескольких отчетов в архив формата .zip выполните следующие действия:

- 1. Перейдите в раздел Администрирование Отчеты.
- 2. Установите флаги напротив нужных отчетов.
- 3. Нажмите кнопку Экспортировать.
- 4. Будет сформирован архив с отчетами в формате .zip.
- 5. Нажмите кнопку Скачать и укажите путь для сохранения архива.

Для экспорта всех отчетов, отображаемых в таблице, нажмите кнопку Экспортировать все.

13.8 Удаление отчета

Удаление отчета можно выполнить следующими способами:

- Из конструктора отчетов. Перейдите на страницу "Конструктор отчета" и нажмите кнопку 🔟. Подтвердите удаление в открывшемся окне.
- Из таблицы "Отчеты". Перейдите в раздел **Администрирование** → **Отчеты**, выберите нужный отчет из списка и нажмите кнопку 🔟 в соответствующей строке;
- Массовое удаление отчетов:

- перейдите в раздел **Администрирование** → **Отчеты**, установите флаги напротив нужных отчетов и нажмите кнопку **Удалить**.
- для удаления всех отчетов, отображаемых в таблице, нажмите кнопку Удалить все.

13.9 Архив отчетов

Отчеты, сгенерированные по расписанию, помещаются в архив (подробнее см. раздел «<u>Настройка</u> <u>расписания генерации отчета</u>»). Для просмотра истории генерации по всем отчетам перейдите в раздел **Администрирование** → **Архив отчетов** (см. «Рис. 250»).

≡	ПАНГЕ РАДАР	° 172.30.254.64 ∨	Архив отчётов		(ī) E	база знаний	\bigotimes admin \vee
â	Ар	кив отчётов					
Q	Отчёт						
(i)	Дата создания						
Ç.		Название	Создан		Действия		
ð		Отчет 1	11.04.2024 13:22:56		↓		
R		Отчет 1	11.04.2024 13:22:56		↓		
		Отчет 1	11.04.2024 13:22:56		↓		
âk.		Отчет 1	11.04.2024 13:22:56		↓		
441		Отчет 1	11.04.2024 13:22:56		↓		
Ø					<		20 / страница $\scriptstyle{\smallsetminus}$

Рис. 250 – Раздел "Архив отчетов"

В разделе отображается следующая информация:

- Название название отчета;
- Создан дата и время генерации отчета.

Для формирования списка отчетов выполните следующие действия:

- 1. В поле "Отчет" из выпадающего списка выберите отчет.
- 2. Выберите направление сортировки:
 - ↓ от последнего к первому;
 - 1 от первого к последнему.

Для экспорта отчетов выполните следующие действия:

- 1. Отметьте отчеты, которые необходимо экспортировать, установив флаг в соответствующей строке.
- 2. Нажмите кнопку 🛃.
- 3. В открывшемся окне укажите путь для сохранения отчетов.

14. Сообщения

Платформа Радар поддерживает обмен сообщений между пользователями платформы.

Например, при изменении информации об инцидентах или активах можно **написать ответственному**. Сообщения, отправленные подобным образом, отображаются в разделе **Сообщения**. Доступна возможность написать другому пользователю, из данного раздела.

Работа с сообщениями включает в себя следующие процессы:

- «<u>Создание сообщения</u>»;
- «<u>Просмотр сообщения</u>»;
- «<u>Ответ на сообщение</u>»;
- «<u>Отметить сообщения прочитанными</u>»;
- «<u>Отметить прочитанные сообщения как непрочитанные</u>»;
- «<u>Экспорт сообщений</u>»;
- «<u>Удаление сообщений</u>».

Для работы с сообщениями нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Сообщения**. Откроется страница "Сообщения" (см. «Рис. 251»).

≡	👹 пангео 172.30.249.21 ∨ Сообщения Лицензия активна до: 2025-08-16 ① Документация 🔘 admin [®] ∨				
ଜ	Сообщения				
Q					
()	Новые сообщения Прочитанные Исходящие				
Ç.	Новое сообщение Прочитать выбранные Прочитать все Удалить Удалить все Экспортировать в сsv Выбрано: 0 С				
ð	Дата создания От кого Тема Актив Инцидент Тип инцидента				
*8.	14:29:21 13.12.2024 admin from asset alert Уязвимость переполнения буфера Уязвимость переполнени 👁 🖻				
0.	< 1 > 20 / страница ~				
ж					
łŶ↓					
Ø					

Рис. 251 – Раздел "Сообщения"

Примечание: если есть непрочитанные сообщения, то рядом с учетной записью появится индикатор **•**.

Сообщения в разделе разделены по следующим вкладкам:

- Новые сообщения список новых сообщений;
- Прочитанные список прочитанных сообщений;
- Исходящие список исходящих сообщений.

На вкладках отображается следующая информация:

• Дата создания – дата и время создания сообщения;
- От кого/Кому адресант/адресат сообщения;
- Тема тема сообщения;
- Актив наименование актива, при изменении информации о котором было создано сообщение. По ссылке откроется страница просмотра актива;
- **Инцидент** наименование инцидента, при изменении информации о котором было создано сообщение. По ссылке откроется страница просмотра инцидента;
- Тип инцидента наименование типа инцидента. По ссылке откроется страница просмотра типа инцидента.

14.1 Создание сообщения

1. Нажмите кнопку Новое сообщение. Откроется окно "Новое сообщение" (см. «Рис. 252»)

Новое сообщение		×
Кому		
userf		\checkmark
Тема		
Тема сообщения		
Сообщение		
Текст сообщения		
		li
	Отмена	Отправить

Рис. 252 – Окно "Новое сообщение"

- 2. Укажите в окне следующую информацию:
 - в поле Кому из выпадающего списка выберите адресата сообщения;
 - в поле Тема укажите тему сообщения;
 - в поле Сообщение укажите текст сообщения.
- 3. Нажмите кнопку Отправить.

14.2 Просмотр сообщения

1. В строке нужного сообщения нажмите кнопку ^(C). Откроется окно "Просмотр сообщения" (см. «Рис. 253»).

Просмотр сос	бщения	×
От кого	admin	
Кому	admin	
Тема	from asset	
Сообщение	from asset	
		Закрыть Ответить

Рис. 253 – Окно "Просмотр сообщения"

2. Если сообщение было просмотрено из вкладки "Новые сообщения", то оно сменит статус на "прочитано" и автоматически переместиться на соответствующую вкладку.

14.3 Ответ на сообщение

- 1. Откройте сообщение на просмотр (см. «Рис. 253») и нажмите кнопку **Ответить**. Откроется окно "Новое сообщение" (см. «Рис. 252»).
- 2. Укажите в окне необходимую информацию и нажмите кнопку Отправить.

14.4 Отметить сообщения прочитанными

Действие выполняется на вкладке Новые сообщения.

Чтобы отметить все новые сообщения прочитанными, нажмите кнопку Прочитать все.

Чтобы отметить конкретные сообщения прочитанными, установите нужные флаги и нажмите кнопку **Прочитать выбранные**.

14.5 Отметить прочитанные сообщения как непрочитанные

Действие выполняется на вкладке Прочитанные.

Чтобы отметить все прочитанные сообщения не прочитанными, нажмите кнопку Пометить все непрочитанным.

Чтобы отметить конкретные сообщения непрочитанными, установите нужные флаги и нажмите кнопку **Пометить выбранные как непрочитанные**.

14.6 Экспорт сообщений

- 1. Перейдите на нужную вкладку.
- 2. Нажмите на кнопку Экспортировать в сяу.
- 3. Будет сформирован документ в формате .csv.
- 4. Нажмите кнопку Скачать и укажите путь для сохранения файла.

14.7 Удаление сообщений

Для удаления сообщения нажмите кнопку 🔟 в соответствующей строке.

Для удаление всех сообщений с выбранной вкладки нажмите кнопку **Удалить все**.

Для удаления конкретных сообщений, установите нужные флаги и нажмите кнопку Удалить.

15. Профиль пользователя

В разделе пользователю доступны следующие действия:

- «Изменение информации о своей учетной записи»;
- «<u>Изменение пароля</u>»;
- «<u>Подключение аутентификатора</u>»;
- «<u>Выход из всех сессий</u>»;
- «Просмотр журнала изменений учетной записи»;
- «<u>Настройка оповещений</u>»;
- «Просмотр истории действий в платформе».

Для перехода в профиль пользователя нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Профиль**. Откроется страница "Профиль" (см. «Рис. 254»).

рофиль												
Информаци	ия о пользователе											
Имя пользоват	теля user											
Email	user@host.ru											
Имя	Василий											
Фамилия	Иванов											
Часовой пояс												
Роли	cluster_manager_access	correlator_R	reports_R	incident_R	offline_access	incident_type_R	scan_results_R	uma_authorization	apikeys_C	software_compliance_checks_R		
Группы	users											
Настройки Уведом Уведом	оповещений илять при изменениях инцидентов илять при изменениях активов	00000044										
Настройки Уведом Уведом Уведом Уведом Сохранить	оповещений млять при изменениях инцидентов млять при изменениях активов млять при срабатывании правил кор импять при автоматической остановки	реляции е правил корр	еляции									
Настройки Уведом Уведом Уведом Уведом Сохранить	оповещений млять при изменениях инцидентов млять при изменениях активов млять при срабатывании правил корј млять при автоматической остановки	реляции е правил корр	еляции									
Настройки Уведом Оведом Уведом Уведом Уведом Уведом Уведом Уведом Оведом Ува Оведом Ово Ово Ово Оведом Ово	оповещений млять при изменениях инцидентов млять при изменениях активов млять при срабатывании правил корј млять при автоматической остановка оррии действий Сущиость	реляции е правил корри	еляции Кем изменен		Дейстане	Сис	темное	Ю сущиюсти		ID связанной сущности	Детали	Дята созда
Настройки Уведоч Уведоч Уведоч Уведоч Сокранить Юиск по исто Серанис Эмц	оповещений млять при изменениях инцидентов млять при изменениях активов млять при срабатывании правил корд млять при автоматической остановки оррии действий Сущность records.rmc.entities. .rules	реляции корр	еляции Кем изменен		Действие Изменение	Сис	темное	ID сущности 9а2364c5-45a5-44	71-b9ba	ID связанной сущности	Детали Показать детали	Дата созда 14:23:25 12

Рис. 254 – Раздел "Профиль"

Информация в разделе отображается в следующих блоках:

- Информация о пользователе в блоке отображаются персональные данные пользователя:
 - логин для входа в платформу;
 - адрес электронной почты;
 - имя пользователя;
 - фамилия пользователя;
 - часовой пояс;
 - список ролей, которые назначены пользователю;

- список групп, в которые добавлен пользователь.
- Настройка оповещений в блоке выполняется настройка оповещений;
- Поиск по истории действий в блоке выполняется поиск и просмотр истории действий в платформе.

15.1 Изменение информации о своей учетной записи

- 1. Перейдите в профиль пользователя.
- 2. Нажмите кнопку **Настройки учетной записи**. Откроется форма "Изменение учетной записи" (см. «Рис. 255»).

Изменени	1e <u>-</u>	учетной записи	* Обязательные поля
Имя пользователя		user	
E-mail	*	user@host.ru	
Имя	*	Василий	
Фамилия	*	Иванов	
		Отмен	а Сохранить

Рис. 255 – Форма "Изменение учетной записи"

- 3. Укажите в окне следующую информацию:
 - в поле E-mail измените адрес электронной почты;
 - в полях Имя и Фамилия измените соответствующие данные пользователя.
- 4. Нажмите кнопку Сохранить.

15.2 Изменение пароля

- 1. Перейдите в профиль пользователя.
- 2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Пароль**. Откроется форма "Смена пароля" (см. «Рис. 256»).

Смена парс	ЯЛ	Все поля обязательны
Пароль		
Новый пароль		
Подтверждение пароля		
		Сохранить

Рис. 256 – Форма "Смена пароля"

3. Укажите в окне следующую информацию:

- в поле Пароль укажите текущий пароль;
- в полях Новый пароль и Подтверждение пароля укажите новый пароль.
- 4. Нажмите кнопку Сохранить.

15.3 Подключение аутентификатора

- 1. Перейдите в профиль пользователя.
- 2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Аутентификатор**. Откроется форма "Смена пароля" (см. «Рис. 257»).

утентификатор	* Обязательны по/
1. Установите <a href="https://freeotp.github.io/" https:="" play.google.com"="" target="_blank
доступны на Google Play<th>">FreeOTP</th> или Google Authenticator. Оба приложения a> и в Apple App Store.	">FreeOTP
• FreeOTP	
Google Authenticator	
2. Откройте приложение и просканируйте баркод, либо введи	те ключ.
Unable to scan?	
3. Введите одноразовый код, выданный приложением, и наж	иите сохранить для завершения установки.
Provide a Device Name to help you manage your OTP devices.	
Одноразовый * код	
Device Name	
	Отнона
	UIMEHA

Рис. 257 – Форма "Аутентификатор"

- 3. Выполните инструкцию, указанную на форме.
- 4. Нажмите кнопку Сохранить.

15.4 Выход из всех сессий

1. Перейдите в профиль пользователя.

2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Сессии**. Откроется страница "Сессии" (см. «Рис. 258»).

IP	Начата	Последний доступ	Истекает	Клиенты
172.30.253.1	Mar 18, 2025, 3:41:16 PM	Mar 18, 2025, 4:57:54 PM	Mar 19, 2025, 1:41:16 AM	radar-ui account
172.30.253.1	Mar 18, 2025, 4:20:45 PM	Mar 18, 2025, 4:55:46 PM	Mar 19, 2025, 2:20:45 AM	radar-ui

Рис. 258 – Страница "Сессии"

3. Нажмите кнопку Выйти из всех сессий.

15.5 Просмотр журнала изменений учетной записи

- 1. Перейдите в профиль пользователя.
- 2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Журна**л. Откроется страница "Лог учетной записи" (см. «Рис. 259»).

Лог учетной записи									
Дата	Событие	IP	Клиент	Детали					
Mar 18, 2025, 4:23:37 PM	logout	172.30.254.1							
Mar 18, 2025, 4:20:45 PM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin					
Mar 18, 2025, 4:05:46 PM	login	172.30.254.1	radar-ui	auth_method = openid-connect , username = admin					
Mar 18, 2025, 4:05:45 PM	login	172.30.254.1	radar-ui	auth_method = openid-connect , username = admin					
Mar 18, 2025, 4:05:36 PM	login	172.30.254.1	account	auth_method = openid-connect , username = admin					
Mar 18, 2025, 3:41:16 PM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin					
Mar 18, 2025, 10:42:03 AM	logout	172.30.253.1							
Mar 18, 2025, 10:41:29 AM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin					
Mar 18, 2025, 10:39:52 AM	logout	172.30.253.1							
Mar 18, 2025, 10:39:28 AM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin					

Рис. 259 – Страница "Лог учетной записи"

На странице отображается следующая информация:

- Дата дата и время события;
- Событие тип события;
- **IP** IP-адрес, с которого выполнено событие;
- Клиент наименование сервиса;
- Детали детали события.

15.6 Настройка оповещений

- 1. Перейдите в профиль пользователя.
- 2. В блоке **Настройка оповещений** включите/выключите уведомления о следующих событиях:

- изменение инцидентов;
- изменение активов;
- произошла "сработка" правила корреляции;
- произошла автоматическая остановка правила корреляции.
- 3. Нажмите кнопку Сохранить.

15.7 Просмотр истории действий в платформе

Пример блока Поиск по истории действий приведен на «Рис. 260».

Поиск по истории действий									
Фильтры + Сортировка 1 Дата создания × Сбросить Применить С © ©									
Сервис	Сущность	Кем изменен	Действие	Системное	ID сущности	ID связанной сущности	Детали	Дата создания	
Cruddy	records.cruddy.entities.user	user	records.cruddy.actions .edit	Нет	afef0a74-82ed-4e95-87cb	-	Показать детали	11:57:16 18.03.2025	
РМЦ	records.rmc.entities.logmule_go _rules	-	Изменение	Да	9a2364c5-45a5-4471-b9ba	-	Показать детали	14:23:25 17.03.2025	
РМЦ	records.rmc.entities.logmule_go _rules	-	Изменение	Да	01ad109a-87f9-4d58-8fe1	-	Показать детали	12:39:40 17.03.2025	
РМЦ	Фильтр потока	-	Изменение	Да	f97192dd-a270-41e1-90cb	-	Показать детали	12:39:40 17.03.2025	
РМЦ	Ключ табличного списка	-	Изменение	Да	229da3c0-2f9c-4fb6-b8b9		Показать детали	12:39:40 17.03.2025	
РМЦ	records.rmc.entities.logmule_go _rules	-	Создание	Да	01ad109a-87f9-4d58-8fe1	-	Показать детали	12:21:35 17.03.2025	
РМЦ	Фильтр потока	-	Изменение	Да	f97192dd-a270-41e1-90cb	-	Показать детали	12:21:35 17.03.2025	
РМЦ	Ключ табличного списка	-	Изменение	Да	229da3c0-2f9c-4fb6-b8b9	-	Показать детали	12:21:35 17.03.2025	
РМЦ	records.rmc.entities.logmule_go _rules	-	Изменение	Да	d873fe67-4d86-43db-86e2	-	Показать детали	12:16:16 17.03.2025	
РМЦ	records.rmc.entities.logmule_go _rules	-	Создание	Да	d873fe67-4d86-43db-86e2	-	Показать детали	12:16:01 17.03.2025	
< 1 2 3 4	5 6 7 162 >	10 / страница 🗸							

Рис. 260 – Блок "Поиск по истории действий"

В блоке отображается следующая информация:

- Сервис наименование сервиса, в котором было выполнено действие;
- Сущность наименование сущности, над которой было выполнено действие;
- **Кем изменен** логин пользователя, выполнившего действие. Если пользователь не указан, то действие было выполнено платформой;
- Действие описание выполненного действия;
- Системное признак, выполнено ли действие платформой: Да, Нет;
- ІD сущности идентификатор сущности, над которой было выполнено действие;
- ІD связанной сущности идентификатор связанной сущности;
- Дата создания дата и время создания записи о выполненном действии.

По кнопке Детали можно посмотреть подробную информацию о действии (см. «Рис. 261»).



Рис. 261 – Окно "Показать детали"

16. Интеграции

16.1 RT Protect EDR

16.1.1 Общие сведения

16.1.1.1 Характеристики системы

Наименование системы – RT Protect Endpoint Detection and Response (далее RT Protect EDR).

Назначение системы – обнаружение целенаправленных атак и сложных угроз.

Разработчик системы – АО «РТ-Информационная безопасность» — организация прямого управления Государственной корпорации «Ростех».

Сайт – <u>РТ-Информационная безопасность</u>.

Возможности, предоставляемые интеграцией:

- выполнение активных действий на активах;
- импорт активов из RT Protect EDR в Платформу Радар;
- синхронизация инцидентов.

Настройка интеграции с системой RT Protect EDR приведена в разделе «<u>Настройка интеграции RT</u> <u>Protect EDR</u>».

Приемы работы с интеграцией приведены в разделе «<u>Работа с интеграцией RT Protect EDR</u>».

16.1.1.2 Активные действия

Система **RT Protect EDR** позволяет выполнять удаленные действия на активе для предотвращения распространения потенциальных угроз.

В рамках интеграции активными действиями являются шаблоны команд для OC Windows и Linux.

Например, для завершения процесса по его идентификатору, будут использованы следующие команды:

• Linux:

```
# kill -9 {{ .pid }}
```

• Windows:

```
# taskkill /PID {{ .pid }} /T /F
```

Перечень действий доступных в интеграции по умолчанию:

- Завершить процесс по PID будет завершен процесс по идентификатору процесса на активе;
- Заблокировать порт соответствующий порт будет заблокирован на прием/отправку сообщений;
- Заблокировать входящий трафик с IP будет заблокирован трафик с соответствующего IP-адреса;

- **Включить изоляцию актива** соответствующий актив будет изолирован в локальной сети;
- Выключить изоляцию актива изоляция актива будет снята;
- **Включить защиту** включить встроенные в систему **RT Protect EDR** средства защиты на выбранном активе;
- **Выключить защиту** отключить встроенные в систему **RT Protect EDR** средства защиты на выбранном активе.

Действие над активом может быть выполнено следующими способами:

- автоматически, по результатам сработки правила корреляции;
- вручную, при анализе актива, на котором выявлены инциденты.

Управление активными действия выполняется в разделе «EDR действия».

16.1.1.3 Синхронизация инцидентов и активов

При синхронизации инцидентов выполняется обмен информацией об инцидентах на активах между системами со следующими особенностями:

- для назначения инцидентов в каждой системе должен быть пользователь, имеющий права на работу с инцидентами;
- при возникновении конфликтов при синхронизации приоритет отдается Платформе Радар;
- при удалении инцидентов из Платформы Радар есть два варианта выбора:
 - удалить также и в RT Protect EDR;
 - отключить синхронизацию инцидента и удалить только в платформе.
- при наличии верхнеуровневой системы, синхронизация будет выполняться по цепочке **Верхнеуровневая система** → **Платформа Радар** → **RT Protect EDR**;
- для выполнения синхронизации необходимо настроить периодическую задачу синхронизации (см. раздел «Шаг 2. Настройка задачи синхронизации активов»).

16.1.1.4 Параметры типа интеграции RT Protect EDR

Для просмотра параметров типа интеграции перейдите в раздел **Параметры** → **Типы интеграций** и нажмите кнопку ⁽²⁾ в строке с наименованием **RT Protect EDR**. Откроется форма просмотра параметров типа интеграции.

Информация на форме отображается на следующих вкладках:

• Интеграции. На вкладке отображается список связанных интеграций (см. «Рис. 262»);

≡	K	пангео 172.30.2 радар 172.30.2	252.105 ~ T i	ипы интеграций	Лицензия активна до:	2026-04-30	 Документация 	I (3 admin \checkmark
â		← Типин	нтеграции						
Q									
(i)		Интеграции	Задачи интегра	ции Команды интеграции	Логи выполенных действий				
⊊Ē									C
		Название инте	еграции			Статус			
ð		RT Protect EDR	а 172.30.250.1	50		Активно			
P.	>	< 1 >	20 / страница	a 🗸					
¥K									
449									
Ø									

Рис. 262 – Просмотр типа интеграции RT Protect EDR. Вкладка "Интеграции"

• Задачи интеграции. Пример вкладки приведен на «Рис. 263».

≡		нгео дар 172.30.252.105 ∨ Типы интег	раций Лицензия акт	ивна до: 2026-04-30 🕕 Докум	иентация 🔘 admin 🗸
â	÷	- Тип интеграции			
Q					
(i)	Ин	нтеграции Задачи интеграции Ком	анды интеграции Логи выполенных действий		
⊊.					С
-	3	Задача интеграции	Название	Cron	Состояние
ů	C	Синхронизация активов	Сихронизация актва	*/5 * * * *	Активно
* <i>P:</i> •		< 1 > 20 / страница ~			
Ж					
411					
Ø					

Рис. 263 – Просмотр типа интеграции RT Protect EDR. Вкладка "Задачи интеграции"

На вкладке отображается информация о периодических задачах, выполняемых в рамках всех связанных интеграций:

- Задача тип периодической задачи;
- Название наименование периодической задачи;
- Cron CRON-выражение, описывающее периодичность задачи;
- Состояние состояние задачи: Активно, Неактивно.
- Команды интеграции. Пример вкладки приведен на «Рис. 264».

≡	Ķ	^{лангео} 172.30.252.105 ∨ Типы интеграций	Лицензия активна до: 2026-04-30	$©$ Документация 🔘 admin \smallsetminus
â		← Тип интеграции		
Q				
(i)		Интеграции Задачи интеграции Команды интеграции	Логи выполенных действий	
Ç.				C
		Интеграция	Скрипт	Статус
ð		RT Protect EDR на 172.30.250.150	Включить изоляцию актива	Активно
<i>%</i> :	>	RT Protect EDR на 172.30.250.150	Заблокировать порт	Активно
¥		RT Protect EDR на 172.30.250.150	Выключить изоляцию актива	Активно
494		RT Protect EDR на 172.30.250.150	Включить защиту	Активно
Ø		RT Protect EDR на 172.30.250.150	Выключить защиту	Активно

Рис. 264 – Просмотр типа интеграции RT Protect EDR. Вкладка "Команды интеграции"

На вкладке отображается информация об активных действиях, созданных в рамках интеграций:

- Интеграция наименование интеграции, для которой исполняется команда;
- Скрипт наименование команды;
- Статус состояние команды: Активно, Неактивно.
- Логи выполненных действий. Пример вкладки приведен на «Рис. 265».

≡	٢	пангео 172.30.252.105 ∨ Типі Радар	ы интеграций	Лицензия активна до	: 2026-04-30 🛈 Доку	ментация 🔘 ad	lmin 🗸
â		← Тип интеграции					
Q							
(1)		Интеграции Задачи интеграции	Команды интеграции	и выполенных действий			
⊊:							C
-		Актив	Интеграция	Команда	Параметры	Выполнено	
ō		WIN-EDR-AGENT	RT Protect EDR на	Заблокировать входящий	ip: 199.0.0.1	15:10:28 21.03.2025	٢
<i>%</i> .	>	WIN-EDR-AGENT	RT Protect EDR на	Заблокировать порт	port: 16000	15:10:18 21.03.2025	0
я		WIN-EDR-AGENT	RT Protect EDR на	Заблокировать входящий	ip: 123.123.123.123	15:08:03 21.03.2025	0
494		WIN-EDR-AGENT	RT Protect EDR на	Заблокировать входящий	ip: 199.0.0.1	13:56:55 21.03.2025	0
Ø		WIN-EDR-AGENT	RT Protect EDR на	Заблокировать порт	port: 16000	13:56:50 21.03.2025	0

Рис. 265 – Просмотр типа интеграции RT Protect EDR. Вкладка "Логи выполненных действий"

На вкладке отображается журнал выполненных действий:

- Актив наименование актива, на котором выполнено действие;
- **Интеграция** наименование интеграции, в рамках которой было выполнено действие;
- Команда наименование выполненного действия;
- Параметры информация о параметрах выполненного действия.

Для просмотра результата выполнения действия нажмите кнопку ^(O) в соответствующей строке. Откроется окно "Результат" (см. «Рис. 266»).



Рис. 266 – Окно "Результат"

16.1.2 EDR действия

О механизме активных действий, доступных в рамках интеграции **RT Protect EDR**, можно ознакомиться в разделе «».

EDR действия могут находиться в следующих состояниях:

- Активно действие становится доступным при настройке правил корреляции и при работе над активами;
- Неактивно действие добавлено в платформу, но не может быть использовано.

Работа с EDR действиями включает в себя следующие процессы:

- 1. «<u>Создание EDR действия</u>».
- 2. «<u>Просмотр EDR действия</u>».
- 3. «<u>Редактирование EDR действия</u>».
- 4. «Дублирование EDR действия».
- 5. «Изменение статуса EDR действия».
- 6. «<u>Экспорт EDR действий</u>».
- 7. «<u>Импорт EDR действий</u>».
- 8. «<u>Удаление EDR действий</u>».

Для работы с EDR действиями перейдите в раздел Параметры → EDR действия (см. «Рис. 267»).

E K PAHFE0 172.30.252.105	√ EDR pa	ействия		L	Пицензия активна до: 2026-04-30 🕕 🕚	Документация 🔘 admin 🗸
Рабочий стол	EDR д	ействия				
Q. События						
🕐 Инциденты 🗸 🗸	7 C	адать Удалить Удалить все Экспортировать Экспортировать все Экспорти	ировать выбранные в csv 3	Экспортировать в csv Импортировать		Выбрано: 0 С
		Наименование действия	Статус	Создано	Обновлено	
С Д АКТИВЫ У		Завершить процесс по PID	Активно	12:30:56 13.03.2025	13:35:29 18.03.2025	© / ii
Соответствие ПО ~		Заблокировать порт	Активно	12:30:57 13.03.2025	15:15:29 27.03.2025	@ Ø 🖻
🗴 Коррелятор 🗸 🗸		Заблокировать входящий траффик с IP	Активно	12:26:09 13.03.2025	10:56:22 31.03.2025	© ∥ <u>n</u>
ж Источники 🗸		Включить изоляцию актива	Активно	12:58:15 25.03.2025	12:58:15 25.03.2025	@ Ø fi
👫 Параметры 🔷		Выключить изоляцию актива	Активно	12:58:15 25.03.2025	12:58:15 25.03.2025	© / 🗇
Основные параметры		Включить защиту	Активно	12:58:15 25.03.2025	12:58:15 25.03.2025	@ Ø fi
Оповещения по задерж		Выключить защиту	Активно	12:58:15 25.03.2025	12:58:15 25.03.2025	© / 🗇
Черный список ID плаги		Завершить процесс по PID - Дубль	Неактивно	12:30:56 13.03.2025	13:56:33 31.03.2025	@ Ø fi
Фоновые задачи						
Интеграции		ioyonpormuo -				
EDR действия						
Типы интеграций						
🛞 Администрирование 🗸						

Рис. 267 – Раздел "EDR действия"

16.1.2.1 Создание EDR действия

1. Нажмите кнопку Создать. Откроется форма Создание действия EDR (см. «Рис. 268»).

← Создание действия EDR		Удалить	Дублировать	Сбросить	Сохра	анит	Ъ
Тип интеграции							
RT Protect EDR							\sim
Наименование действия *							
Завершить процесс по PID - Дубль							
Переменные *							
Число ~	PID процесса	pid			-		+
Команды Linux *							
kill -9 {{ .pid }}				_	+ /	► ·	\downarrow
Команды Windows *							
taskkill /PID {{ .pid }} /T /F				-	+ /	r -	\downarrow
Неактивно							

Рис. 268 – Форма "Создание действия EDR"

- 2. Укажите на форме следующую информацию:
 - в поле **Тип интеграции** из выпадающего списка выберите значение "*RT Protect EDR*";
 - в поле Наименование действия укажите наименование EDR действия;
 - в блоке полей **Переменные** добавьте необходимое количество параметров, по которым будет выполнено действие:
 - нажмите кнопку +;
 - в поле Переменная выберите тип параметра: строка, число, логический;
 - в поле **Название параметра** укажите название параметра для отображения в платформе;
 - в поле **Имя параметра** укажите наименование параметра. По указанному значению будут выполняться команды для OC Linux и Windows.
 - в блоке полей **Команды Linux** и **Команды Windows** добавьте необходимое количество команд для OC Linux и Windows. Команды будут исполняться в заданном порядке. Для изменения порядка исполнения команд используйте кнопки ↑, ↓;
 - для активации действия в поле **Статус** установите переключатель в положение "*Включен*".
- 3. Нажмите кнопку Сохранить.

16.1.2.2 Просмотр EDR действия

Для просмотра информации об EDR действии нажмите кнопку 💿 в строке нужного действия. Откроется форма "Просмотр действия EDR".

Информация на форме разделена по трем вкладкам:

- Основные настройки информация о параметрах EDR действия;
- Связанные интеграции информация об интеграциях, в которых задействовано действие;
- Логи выполненных действий журнал выполнения действия EDR.

Основные настройки

Пример вкладки "Основные настройки" приведен на «Рис. 269».

 Просмотр действия EDR 	Удалить	Дублировать	Редактировать						
Основные настройки Связанные интеграции Логи выполенных действий									
Тип интеграции									
RT Protect EDR									
Наименование действия *									
Заблокировать порт									
Переменные *									
Число 🗸	Πορτ	port							
Команды Linux *									
sudo iptables -A INPUT -p tcpdport {{ .port }} -j DROP									
sudo iptables -A INPUT -p udpdport {{ .port }} -j DROP									
sudo ufw deny {{ .port }}									
Команды Windows *									
netsh advfirewall firewall add rule name="Block Port {{ .port }}" dir=in action=block p	netsh advfirewall firewall add rule name="Block Port {{ .port }}" dir=in action=block protocol=TCP localport={{ .port }}								
netsh advfirewall firewall add rule name="Block Port {{ .port }}" dir=in action=block	etsh advfirewall firewall add rule name="Block Port {{port }}" dir=in action=block protocol=UDP localport={{port }}								
Активно									

Рис. 269 – Форма "Просмотр действия EDR". Вкладка "Основные настройки"

На вкладке отображается следующая информация:

- Тип интеграции наименование типа интеграции, к которой относится действие;
- Наименование действия название EDR действия в платформе;
- **Переменные** информация о параметрах EDR действия: Тип переменной, Название действия, Имя действия;
- Команды Linux список команд для OC Linux;
- Команды Windows список команд для OC Windows;
- Информация о состоянии EDR действия: Активно, Неактивно.

Связанные интеграции

Пример вкладки "Связанные интеграции" приведен на «Рис. 270».

← Просмотр действия EDR	Удалить Дублировать Редактировать				
Основные настройки Связанные интеграции Логи выполенных действий					
	C				
Интеграция	Статус				
RT Protect EDR	Активно				
< 1 > 10 / страница ~					

Рис. 270 – Форма "Просмотр действия EDR". Вкладка "Связанные интеграции"

На вкладке отображается список интеграций, в которых используется EDR действие, а также состояние интеграции.

Логи выполненных действий

Пример вкладки "Логи выполненных действий" приведен на «Рис. 271».

Просмотр действия	Удалить Дублир	овать Редактир	овать									
Основные настройки Связанные ин	Основные настройки Связанные интеграции Логи выполенных действий											
7							C	٢				
Актив	Параметры	Выполнено	Кем выполнен	Интеграция	Команда	Дата старта	Код возврата					
WIN-EDR-AGENT	port: 16000	15:10:18 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	15:10:00 21.03.2025	0	٢				
WIN-EDR-AGENT	port: 16000	13:56:50 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:56:39 21.03.2025	0	٢				
WIN-EDR-AGENT	port: 16000	12:30:31 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:30:18 21.03.2025	0	٢				
WIN-EDR-AGENT	port: 16000	12:17:49 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:17:38 21.03.2025	0	٢				
WIN-EDR-AGENT	port: 16000	10:35:54 20.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	10:35:36 20.03.2025	0	٢				
WIN-EDR-AGENT	port: 23123123	12:32:01 19.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:31:56 19.03.2025	1	٢				
WIN-EDR-AGENT	port: 23123123	12:29:57 19.03.2025		RT Protect EDR на 172.30.250.150	Заблокировать порт	12:29:52 19.03.2025	1	۲				
WIN-EDR-AGENT	port: 3212312312312	17:13:13 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	17:13:04 17.03.2025	1	٢				
WIN-EDR-AGENT	port: 3123123123	13:44:16 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:44:11 17.03.2025	1	۲				
WIN-EDR-AGENT	port: 13123123123213	13:32:59 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:32:56 17.03.2025	1	٢				
< 1 2 > 10 / страница												

Рис. 271 – Форма "Просмотр действия EDR". Вкладка "Логи выполненных действий"

На вкладке отображается следующая информация:

- Актив наименование актива, на котором выполнено EDR действие;
- Параметры информация о параметрах выполненного действия;
- Выполнено дата и время выполнения действия;
- Кем выполнено информация об инициаторе выполнения действия, например, правило корреляции или пользователь;
- Интеграция наименование интеграции, в рамках которой было выполнено действие;
- Команда наименование EDR действия;
- Дата старта дата и время запуска исполнения действия;
- Код возврата ответ, полученный при выполнении действия:
 - 0 успешный ответ;
 - 1 при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку 🔘 в соответствующей строке.

16.1.2.3 Редактирование EDR действия

Открыть EDR действие на редактирование можно двумя способами:

- На главной странице раздела нажмите кнопку 🖉 в строке нужного EDR действия.
- Перейдите на форму просмотра необходимого EDR действия и нажмите кнопку **Редактировать**.

Для редактирования EDR действия выполните следующие действия:

- 1. Откройте EDR действие на редактирование.
- 2. Внесите необходимые изменения.
- 3. Нажмите кнопку Сохранить.

16.1.2.4 Дублирование EDR действия

- 1. Откройте EDR действие на просмотр.
- 2. Нажмите кнопку **Дублировать**. Откроется окно "Дублировать действие EDR" (см. «Рис. 272»).

Дублировать действие EDR					
Наименование действия					
Завершить процесс по PID - Дубль					
Сбросить					
Дублировать					

Рис. 272 – Окно "Дублировать действие EDR"

- 3. При необходимости измените наименование действия и нажмите кнопку Дублировать.
- 4. Будет создано новое EDR действие на основе существующего.

16.1.2.5 Изменение статуса EDR действия

Для изменения статуса EDR действия в графе "Статус" установите переключатель в соответствующее положение.

Примечание: если у EDR действия есть связанные активные сущности, например правило корреляции или актив, то изменить статус действия будет нельзя.

16.1.2.6 Экспорт EDR действий

Для массового экспорта EDR действий установите нужные флаги и нажмите кнопку **Экспортировать**. Будет сформирован архив с EDR действиями в формате .zip.

Для экспорта всех EDR действий нажмите кнопку Экспортировать все.

Для массового экспорта EDR действий в формат CSV нажмите кнопку **Экспортировать** выбранные в csv.

Для экспорта всех EDR действий в формат CSV нажмите кнопку Экспортировать в csv.

16.1.2.7 Импорт EDR действий

- 1. Нажмите кнопку Импортировать.
- 2. В открывшемся окне укажите путь к архиву с EDR действиями.
- 3. Нажмите кнопку Открыть.

16.1.2.8 Удаление EDR действий

Примечание: для корректной работы интеграций не рекомендуется удалять EDR действия, установленные по умолчанию.

Для удаления EDR действия нажмите кнопку 🔟 в соответствующей строке.

Для массового удаления EDR действий установите нужные флаги и нажмите кнопку Удалить.

Для удаление всех EDR действий нажмите кнопку Удалить все.

16.1.3 Настройка интеграции RT Protect EDR

Платформа Радар позволяет настроить несколько независимых интеграций с системой RT Protect EDR. Например, если используется несколько управляющих серверов системы RT Protect EDR с разным списком подчиненных активов, то для каждого управляющего сервера нужно создать экземпляр интеграции с соответствующими настройками.

Все действия над интеграциями выполняются в разделе Параметры - Интеграции.

Перед выполнением настройки интеграции с **RT Protect EDR** выполните следующие действия:

- 1. Активируйте тип интеграции **RT Protect EDR**. Подробнее см. раздел «Типы интеграций».
- 2. Настройте EDR действия. Подробнее см. раздел «EDR действия».

Процесс настройки интеграции с **RT Protect EDR** включает в себя следующие шаги:

- «Шаг 1. Создание экземпляра интеграции с RT Protect EDR»;
- «Шаг 2. Настройка задачи синхронизации активов»;
- «Шаг 3. Настройка активных действий для интеграции»;
- «Шаг 4. Активация интеграции».

16.1.3.1 Шаг 1. Создание экземпляра интеграции с RT Protect EDR

- 1. Перейдите в раздел Параметры Интеграции.
- 2. Нажмите кнопку Создать. Откроется окно "Создание интеграции" (см. «Рис. 273»).

← Создание интеграции	Сбросить	Проверить	Сохранить
Название интеграции *			
RT Protect EDR с управляющим сервером на <ip-адрес сервера=""></ip-адрес>			
Статус			
Тип интеграции *			
RT Protect EDR			~
Адрес АРІ сервера *			
172.30.250.150			
Токен аутентификации			
Логин *			
admin			
Пароль *			
admin			
Порт *			
443			- +
Использовать задание синхронизации			
Использовать активные действия интеграции			
Сбросить Проверить Сохранить			

Рис. 273 – Создание интеграции с RT Protect EDR

- 3. Укажите в окне следующую информацию:
 - Название интеграции укажите наименование интеграции;
 - **Тип интеграции** из выпадающего списка выберите значение "*RT Protect EDR*". Поля формы автоматически изменятся для настройки выбранного типа интеграции;
 - Адрес АРІ сервера укажите IP-адрес, на котором располагается АРІ сервер RT Protect EDR;
 - Токен аутентификации укажите токен, полученный в системе RT Protect EDR;
 - Логин укажите логин для доступа к АРІ серверу;
 - Пароль укажите пароль для доступа к АРІ серверу;
 - Порт укажите порт, по которому выполняется подключение к АРІ серверу;
 - Использовать задание синхронизации установите переключатель в положения Включен для активации периодических задач синхронизации активов и инцидентов;
 - Использовать активные действия интеграции установите переключатель в положения Включен для активации возможности использования активных действий.
- 4. Нажмите кнопку Проверить. Будет выполнена проверка подключения к АРІ серверу.

5. Нажмите кнопку **Сохранить**. Сохранение интеграции будет доступно только после успешной проверки соединения с АРІ сервером.

16.1.3.2 Шаг 2. Настройка задачи синхронизации активов

- 1. Откройте интеграцию на редактирование (кнопка 🖉).
- 2. Перейдите на вкладку "Задачи интеграции" (см. «Рис. 274»).

Пангео 172.30.252		Интеграции		Лицензия активна до: 🗄	2026-04-30 ① Доку	ментация 🔘 admin 🗸				
Рабочий стол		 RT Protect EDR на 172.30.250.150 			Уд	алить Добавить задачу				
Q События										
④ Инциденты	D Инциденты Основные настройки <u>Задачи интеграции</u> Команды интеграции Логи выполенных действий									
с8 Активы	~	Добавить задачу Удалить Удалить все Переключить активности	b			Выбрано: 0 С				
		Задача интеграции	Название	Cron	Состояние					
Соответствие ПО	~	Синхронизация активов	Сихронизация актва	*/5 * * * *	Активно	Ø 🗊				
Ж Коррелятор	~	< 1 > 10 / страница ~								
ж Источники	~									
Нараметры	~									
Администрирование	~									

Рис. 274 – Настройка интеграции. Задачи интеграции

3. Нажмите кнопку Добавить задачу. Откроется окно "Добавить задачу" (см. «Рис. 275»).

Добавить задачу		×
Название *		
Синхронизация активов каждые 5 ми	инут	
Cron *		
*/5 * * * *		
Состояние		
Задача интеграции *		
Синхронизация активов		~
	Сбросить	Сохранить

Рис. 275 – Окно "Добавить задачу"

- 4. Укажите в окне следующую информацию:
 - Название укажите название периодической задачи;
 - **Cron** укажите CRON-выражение, описывающее периодичность задачи. Подсказу по CRON-выражениям см. на <u>сайте</u>;
 - **Состояние** включите выполнение задачи синхронизации активов, установив переключатель в положение "Включен";

- Задача интеграции из выпадающего списка выберите задачу "Синхронизация активов".
- 5. Нажмите кнопку Сохранить.
- 6. Журнал выполнения задачи можно посмотреть в разделе **Администрирование** → **Кластер** → вкладка **Планировщик задач**.

16.1.3.3 Шаг 3. Настройка активных действий для интеграции

- 1. Откройте интеграцию на редактирование (кнопка 🖉).
- 2. Перейдите на вкладку "Команды интеграции" (см. «Рис. 276»).

ПАНГЕС 172.30.252.10	05 ~	Интеграции		Лицензия активна до: 2026-04-30	🛈 Документация 🔘 admin 🗸
Рабочий стол		← RT Protec	at EDR		Удалить
Q. События					
🛈 Инциденты 🗸		Основные настройки	Задачи интеграции Команды интеграции Логи выполенных действий		
с8 Активы 🗸		Переключить актив	ность		Выбрано: 0 С
			Скрипт	Статус	
Соответствие ПО			Включить изоляцию актива	Активно	
Ж Коррелятор ~			Заблокировать порт	О Активно	
ж Источники 🗸			Выключить изоляцию актива	Активно	
🙌 Параметры 🗸 🗸			Включить защиту	Активно	
🛞 Администрирование 🗸 🗸			Выключить защиту	Активно	
			Завершить процесс по PID	Активно	
	>)		Забложировать входящий траффик с IP	Активно	
		< 1 > 1	0 / страница \sim		

Рис. 276 – Настройка интеграции. Команды интеграции

3. В графе **Статус** включите необходимые действия, которые будут доступны при выявлении инцидентов на активах.

16.1.3.4 Шаг 4. Активация интеграции

Чтобы по интеграции выполнялось взаимодействие с системой **RT Protect EDR**, ее необходимо активировать.

Для активации интеграции перейдите в раздел **Параметры** → **Интеграции** и в колонке **Статус** установите переключатель в положение "Включен".

16.1.4 Работа с интеграцией RT Protect EDR

После настройки интеграции с **RT Protect EDR** в платформе станут доступны следующие возможности:

- «<u>Работа с правилами корреляции</u>»:
 - настройка активных действий, которые необходимо выполнить при "сработке" правила;
 - просмотр добавленных в правило корреляции активных действий.
 - «<u>Настройка правила корреляции</u>. Добавление активных действий
- 1. Начните процесс создания/редактирования правила корреляции.

Примечание: функции по настройке активных действий доступны, как и при создании с помощью визуального конструктора, так и без него.

2. Перейдите на вкладку Интеграции (см. «Рис. 277»).

≡	Кангео 172.	зо.252.105 ∨ Правила корреляции		Ли	цензия активна до: 2026-04-30 🔅	Э Документация	🔘 admin ~			
â	← Windows - Системные журналы были очищены									
0	2 D Основное Настройка фильтров потока Настройка алерта Настройка группера Конструктор условий Действия Интеграции ———————————————————————————————————									
٩ð	Создать	Создать Удалить соз Экспортировать Виспортировать все Экспортировать всях Импортировать в								
ß		Действие	Статус	Создано	Обновлено					
		Заблокировать порт	Активно	10:23:21 19.03.2025	10:23:48 19.03.2025		> □			
<i>7</i> +		Заблокировать входящий траффик с IP	🚺 Активно	12:01:02 19.03.2025	12:01:03 19.03.2025		⊘ ⊡			
ж	< 1	> 10 / страница ~								
+11										
0										

Рис. 277 – Конструктор правила корреляции. Вкладка "Интеграции"

3. Нажмите кнопку Создать. Откроется окно "Действия интеграции" (см. «Рис. 278» - «Рис. 279»).

деиствия интегр	ации					
Действие						
Заблокировать порт						\sim
Торт			Стратегия			
16000	- +	Из событий таксономии	Первый	\sim		
					Сбросить	Сохранить

Рис. 278 – Настройка действия интеграции с дополнительными параметрами

Действия интеграции		×
Действие		
Выключить изоляцию актива		~
	Сбросить	Сохранить

Рис. 279 – Настройка действия интеграции без дополнительных параметров

- 4. В открывшемся окне выберите действие.
- 5. В зависимости от выбранного действия поля формы будут автоматически изменены для настройки действия:
 - Для действий Завершить **процесс по PID**, Заблокировать **порт**, Заблокировать **входящий траффик с IP укажите** следующие сведения:
 - в поле Параметр укажите соответствующий параметр: идентификатор процесса, порт или IP-адрес. При необходимости можно выбрать параметр из полей таксономии. Для этого установите переключатель **Из полей**

таксономии в положение "Включен" и в поле Параметр из выпадающего списка выберите поле события;

- в поле **Стратегия** выберите стратегию передачи событий в правиле: передавать только первое событие в интеграцию или последнее;
- нажмите кнопку Сохранить.
- Для действий не требующих дополнительных настроек, нажмите кнопку Сохранить.
- 6. Активируйте добавленное действие. Для этого в графе Статус установите переключатель в положение "Включен".
- 7. Добавьте необходимое количество активных действий.
- 8. Завершите процесс создания/редактирования правила корреляции.

16.1.4.1.1 Просмотр действий интеграции

Для просмотра добавленных в правило действий интеграции откройте его на просмотр и перейдите на вкладку "Интеграции" (см. «Рис. 280»).

← Win	dows - Сист	емные журналы были очищены			Активное Перезапустить	🛙 Открыть редактор
Основн	ioe					
ID:		a3491b6f-46a1-43e4-ab22-9ec9c9a5530f				
Создано:		2025-03-18 14:15:00				
Изменен	D:	2025-03-19 12:02:08				
Тип прав	ила:	Визуальный конструктор				
Тип инци,	дента:	Windows - Системные журналы были очищены				
Описание	3:	Правило детектирует очистку журналов Windows.				
Ретроспе	ктивное:	Нет				
Сбор мет	рик:	Нет				
Максима. памяти (М	пьное значение Иб):	Нет				
Максима. сработок	пьное количество :	Нет				
За интеря	зал (секунд):	Нет				
Фильтры	потока событий:	Windows_event_logs_cleared				
Инциденты Создать	Результаты Удалить Удалить в	Интеграции Лог изменений Лог правила Метри се Экспортировать Экспортировать все Экспортирова	ки ать выбранные в сsv Экспортировать в сsv Ими	тортировать		Выбрано: 0 С
	Действие		Статус	Создано	Обновлено	
	Заблокировать пор	т	Активно	10:23:21 19.03.2025	10:23:48 19.03.2025	Ø 🗊
	Заблокировать вхо	дящий траффик с IP	С Активно	12:01:02 19.03.2025	12:01:03 19.03.2025	Ø 🗊
< 1	> 10 / страница					

Рис. 280 – Просмотр правила корреляции. Вкладка "Интеграции"

На вкладке отображается следующая информация:

- Действие наименование действия;
- Статус состояние действия: Активно, Неактивно;
- Создано дата и время добавления действия в правило корреляции;
- Обновлено дата и время изменения информации о действии в правиле корреляции.
- Работа с активами»:
 - выполнение активных действий по связанным интеграциям;
 - просмотр журнала выполненных действий на активе.
- «<u>Просмотр связей с</u> интеграциями и журнала выполненных действий

Откройте актив на просмотр (см. «Рис. 281»).

← WIN-EDR-A	GENT					Редактировать	🗅 Добавить в группу	Написать ответственном	y E
Основное				Сетевые	интерфейсы				
IP	172.30.250.161			Название	IP			MAC	
FQDN	-			Ethernet0	1	72 30 250 161			
MAC	-					2.00.200.101			
oc	Microsoft Windows	Server 2022 Standard Evaluation - 64 bit							
Группа актива	group			Програм	мное обеспечение				
Тип актива	Host			Arent RT Pr	otect EDR, версия - 2.0.178.2678				
Расположение	https://172.30.250.1	50/api/agent/1/		Microsoft Ec	dge, версия - 134.0.3124.51				
Ответственный	-			Microsoft Ec	dge, версия - 134.0.3124.66				
Группа ответственных				Показать бо	ольше 🗸				
Дата последнего сканирования	Не произведено			Аппарати	ное обеспечение				
Активен	Да								
В локальной сети Сетевая видимость	нет Штатный доступ в	Интернет через Ргоху		processor , i	apacity: 16 GB, PartNumber: , Seriall name: Intel(R) Xeon(R) Gold 5120 CI	Number: , Manufactur PU @ 2.20GHz, manuf	er: , ConfiguredClockSpeed: acturer: , caption: , numberOf	Cores: 8, addressWidth:	
Инциденты	api agent 1								C ©
Срочность	Назва	ние			Статус		Создано		
0.94	Windo	ws - Системные журналы были очищены			Новый		15:09:59 21.03.2025		
< 1 > 10/c	траница \vee								
Связи с интеграция	ями								
Интеграция			Тип интеграции	URI				Действие	
RT Protect EDR на 172.3	30.250.150		RT Protect EDR	https:	//172.30.250.150/api/agent/1/			Выполнить де	йствие
Логи выполенных и	действий								C ©
Команда		Параметры	Выполнено		Кем выполнен	И	теграция		
Заблокировать входящ	ий траффик с IP	ip: 199.0.0.1	15:10:28 21.03.2025		Windows - Системные журналы	были очищены R	Protect EDR на 172.30.250.	.150	٢
Заблокировать порт		port: 16000	15:10:18 21.03.2025		Windows - Системные журналы	были очищены R	Protect EDR на 172.30.250.	150	٢
Заблокировать входящ	ий траффик с IP	ip: 123.123.123.123	15:08:03 21.03.2025		admin	R	Protect EDR на 172.30.250.	150	۲
< 1 2 3	4 > 10 / cm	аница ~							

Рис. 281 – Просмотр актива

При интеграции с системой RT **Protect EDR при** анализе актива доступен просмотр следующей дополнительной информации:

- Блок Связи с интеграциями просмотр информации о связанных интеграциях:
 - Интеграция наименование интеграции;
 - Тип интеграции наименование типа интеграции;
 - URL URL адрес API сервера.
- Блок Логи выполненных действий просмотр журнала выполненных действий на активе:
 - Команда наименование выполненного действия;
 - Параметры информация о параметрах выполненного действия;
 - Выполнено дата и время выполнения действия;
 - Кем выполнено информация об инициаторе выполнения действия, например правило корреляции или пользователь;
 - Интеграция наименование интеграции, в рамках которой было выполнено действие;
 - Актив наименование актива, на котором выполнено действие;
 - Дата старта дата и время запуска исполнения действия;

- Код возврата ответ, полученный при выполнении действия:
 - 0 успешный ответ;
 - 1 при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку 🔘 в соответствующей строке.

16.1.4.1.2 Выполнение активных действий на активе

- 1. Откройте актив на просмотр (см. «Рис. 281»).
- 2. В блоке Связи **с интеграциями нажмите** кнопку Выполнить **действие**. Откроется окно "Выполнить действие" (см. «Рис. 282»).

RT Protect EDR Ha 1/2.30.250.150	~
Активные действия	
Заблокировать порт	\sim
Порт *	
Порт	-+

Рис. 282 – Окно "Выполнить действие"

- 3. Выполните в окне следующие действия:
 - в поле Интеграция выберите необходимую интеграцию с RT **Protect EDR**;
 - в поле Активные **действия из** выпадающего списка выберите действие, которое необходимо выполнить. Поля формы будут автоматически изменены для настройки выбранного действия;
 - при необходимости укажите дополнительные параметры, например идентификатор процесса, IP-адрес или порт;
 - нажмите кнопку Выполнить.
- Работа с инцидентами» просмотр журнала выполненных действий по инциденту;
- «Просмотр журнала выполнения действий по интеграции».

16.1.4.2 Работа с правилами корреляции

16.1.4.2.1 Настройка правила корреляции. Добавление активных действий

9. Начните процесс создания/редактирования правила корреляции.

Примечание: функции по настройке активных действий доступны, как и при создании с помощью визуального конструктора, так и без него.

10. Перейдите на вкладку Интеграции (см. «Рис. 277»).

≡∣		30.252.105 🗸 Правила корреляции		Ли	цензия активна до: 2026-04-30 ①Да	окументация 🤅	g) admin v
Â	← Wine	dows - Системные журналы были очищены				🗇 Удалить 🗸 🗸	Сохранить
Q							
0	Основное	Настройка фильтров потока Настройка алерта Настройка группера	Конструктор условий Действия Интегр	ации Тестирование			
сB	Создать	Удалить Удалить все Экспортировать Экспортировать все Экспортиров	вать выбранные в csv Экспортировать в csv Имп	ортировать		Выбра	ано: 0 С
ß		Действие	Статус	Создано	Обновлено		
		Заблокировать порт	Активно	10:23:21 19.03.2025	10:23:48 19.03.2025	Ø 🗇	
07		Заблокировать входящий траффик с IP	Активно	12:01:02 19.03.2025	12:01:03 19.03.2025	1	
ж	< 1	> 10 / страница ~					
+11							
0							

Рис. 277 – Конструктор правила корреляции. Вкладка "Интеграции"

11. Нажмите кнопку **Создать**. Откроется окно "Действия интеграции" (см. «Рис. 278» - «Рис. 279»).

Действия интег	рации				×
Действие					
Заблокировать пор	т				~
Порт			Стратегия		
16000	- +	Из событий таксономии	Первый 🗸		
				Сбросить	Сохранить

Рис. 278 – Настройка действия интеграции с дополнительными параметрами

Действия интеграции		×
Действие		
Выключить изоляцию актива		\sim
	Сбросить	Сохранить

Рис. 279 – Настройка действия интеграции без дополнительных параметров

- 12. В открывшемся окне выберите действие.
- 13. В зависимости от выбранного действия поля формы будут автоматически изменены для настройки действия:
 - Для действий Завершить процесс по PID, Заблокировать порт, Заблокировать входящий траффик с IP укажите следующие сведения:

- в поле Параметр укажите соответствующий параметр: идентификатор процесса, порт или IP-адрес. При необходимости можно выбрать параметр из полей таксономии. Для этого установите переключатель Из полей таксономии в положение "Включен" и в поле Параметр из выпадающего списка выберите поле события;
- в поле **Стратегия** выберите стратегию передачи событий в правиле: передавать только первое событие в интеграцию или последнее;
- нажмите кнопку Сохранить.
- Для действий не требующих дополнительных настроек, нажмите кнопку Сохранить.
- 14. Активируйте добавленное действие. Для этого в графе **Статус** установите переключатель в положение "Включен".
- 15. Добавьте необходимое количество активных действий.
- 16. Завершите процесс создания/редактирования правила корреляции.

16.1.4.2.2 Просмотр действий интеграции

Для просмотра добавленных в правило действий интеграции откройте его на просмотр и перейдите на вкладку "Интеграции" (см. «Рис. 280»).

← Window	rs - Системные журналы были очищены			Активное Перезапустить	🗷 Открыть редактор
Основное					
ID:	a3491b6f-46a1-43e4-ab22-9ec9c9a5530f				
Создано:	2025-03-18 14:15:00				
Изменено:	2025-03-19 12:02:08				
Тип правила:	Визуальный конструктор				
Тип инцидента:	Windows - Системные журналы были очищены				
Описание:	Правило детектирует очистку журналов Windows.				
Ретроспективно	ое: Нет				
Сбор метрик:	Нет				
Максимальное : памяти (Мб):	значение Нет				
Максимальное сработок:	количество Нет				
За интервал (се	акунд): Нет				
Фильтры потока	а событий: Windows_event_logs_cleared				
Инциденты Рез Создать Удалит	азультаты Интеграции Лог изменений Лог правила Метр ть <mark>Идалить все</mark> Экспортировать Экспортировать все Экспортиро	ики зать выбранные в сsv Экспортировать в сsv Ими	тортировать		Выбрано: 0 С
Дейс	ствие	Статус	Создано	Обновлено	
Забл	юкировать порт	🚺 Активно	10:23:21 19.03.2025	10:23:48 19.03.2025	Ø 🗊
Забл	юкировать входящий траффик с IP	О Активно	12:01:02 19.03.2025	12:01:03 19.03.2025	Ø 🗊
< 1 >	10 / страница \sim				

Рис. 280 – Просмотр правила корреляции. Вкладка "Интеграции"

На вкладке отображается следующая информация:

- Действие наименование действия;
- Статус состояние действия: Активно, Неактивно;
- Создано дата и время добавления действия в правило корреляции;
- Обновлено дата и время изменения информации о действии в правиле корреляции.

16.1.4.3 Работа с активами

16.1.4.3.1 Просмотр связей с интеграциями и журнала выполненных действий

WIN-EDR-A	GENT					Редактировать	🗅 Добавить в группу	Написать ответственн	юму
Основное				Сетевь	е интерфейсы				
IP	172.30.250.161			Назван	le	IP		MAC	
FQDN	-			Etherne	0	172.30.250.161			
MAC	-								
oc	Microsoft Window	s Server 2022 Standard Evaluation - 64 bit							
Группа актива	group			Програ	ммное обеспечение				
Тип актива	Host			Arent RT	Protect EDR, версия - 2.0.178.267	8			
Расположение	https://172.30.250	.150/api/agent/1/		Microsoft	Edge, версия - 134.0.3124.51				
Ответственный	-			Microsoft	Edge, версия - 134.0.3124.66				
Группа ответственных	-			Показать	больше 🗸				
Дата последнего сканирования	Не произведено			Аппара	тное обеспечение				
Активен	Да			-					
Сетевая видимость	пет Штатный доступ в	з Интернет через Ргоху		processor	Capacity: 16 GB, PartNumber: , Se , name: Intel(R) Xeon(R) Gold 512	rialNumber: , Manufactu 0 CPU @ 2.20GHz, man	urer: , ConfiguredClockSpeed: ufacturer: , caption: , numberC	ofCores: 8, addressWidth:	
нциденты									C
Срочность	Наза	ание			Статус		Создано		
0.94	Wind	lows - Системные журналы были очищены			Новый		15:09:59 21.03.2025		
(1) 10/с вязи с интеграция	траница ~								
Интеграция			Тип интеграции	URI				Действие	
RT Protect EDR на 172.3	30.250.150		RT Protect EDR	http	s://172.30.250.150/api/agent/1/			Выполнить	 действие
оги выполенных д Г	цействий								C
оманда		Параметры	Выполнено		Кем выполнен	1	Интеграция		
аблокировать входящи	ий траффик с IP	ip: 199.0.0.1	15:10:28 21.03.	2025	Windows - Системные журн	алы были очищены	RT Protect EDR на 172.30.25(0.150	0
аблокировать порт		port: 16000	15:10:18 21.03.3	2025	Windows - Системные журн	алы были очищены	RT Protect EDR на 172.30.250	0.150	4
аблокировать входящ/	ий траффик с IP	ip: 123.123.123.123	15:08:03 21.03.3	2025	admin		RT Protect EDR на 172.30.250	0.150	0
Заблокировать порт Заблокировать входящи	ий траффик с IP	port: 16000 ip: 123.123.123.123	15:10:18 21.03. 15:08:03 21.03.	2025	Windows - Системные журн admin	алы были очищены	RT Protect EDR на 172.30.25(RT Protect EDR на 172.30.25(0.150	

Откройте актив на просмотр (см. «Рис. 281»).

Рис. 281 – Просмотр актива

При интеграции с системой **RT Protect EDR** при анализе актива доступен просмотр следующей дополнительной информации:

- Блок Связи с интеграциями просмотр информации о связанных интеграциях:
 - Интеграция наименование интеграции;
 - Тип интеграции наименование типа интеграции;
 - URL URL адрес API сервера.
- Блок Логи выполненных действий просмотр журнала выполненных действий на активе:
 - Команда наименование выполненного действия;
 - Параметры информация о параметрах выполненного действия;
 - Выполнено дата и время выполнения действия;
 - Кем выполнено информация об инициаторе выполнения действия, например правило корреляции или пользователь;

- **Интеграция** наименование интеграции, в рамках которой было выполнено действие;
- Актив наименование актива, на котором выполнено действие;
- Дата старта дата и время запуска исполнения действия;
- Код возврата ответ, полученный при выполнении действия:
 - 0 успешный ответ;
 - 1 при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку 🔘 в соответствующей строке.

16.1.4.3.2 Выполнение активных действий на активе

- 4. Откройте актив на просмотр (см. «Рис. 281»).
- 5. В блоке **Связи с интеграциями** нажмите кнопку **Выполнить действие**. Откроется окно "Выполнить действие" (см. «Рис. 282»).

Mutorpound	
интеграция	
RT Protect EDR на 172.30.250.150	~
Активные лействия	
Заолокировать порт	~
Порт *	
Порт	-+
	Выполнить

Рис. 282 – Окно "Выполнить действие"

- 6. Выполните в окне следующие действия:
 - в поле Интеграция выберите необходимую интеграцию с RT Protect EDR;
 - в поле **Активные действия** из выпадающего списка выберите действие, которое необходимо выполнить. Поля формы будут автоматически изменены для настройки выбранного действия;
 - при необходимости укажите дополнительные параметры, например идентификатор процесса, IP-адрес или порт;
 - нажмите кнопку Выполнить.

16.1.4.4 Работа с инцидентами

Откройте инцидент на просмотр (см. «Рис. 283»).

ID: 16 /indows - Системные журналь						CTO	Terrer Menu 2	Benavruponart		OMV
findows - Системные журналь						Cla	переназначить	Редактировать	написать ответственн	
	ы были очищены			Акт	ив					
Содержимое журнала событии Wi злоумышленника скрыть следы не можно ограничить выполнение от	ndows было удалено вручную. Эт законной деятельности путем уд	о событие может указыват аления журналов. С помоц и поступа путем назначени	ть на попытку цью групповой политик из прав и разрешений. Г	и 3	Название:	WIN-EDR-AG	GENT			
этом право/разрешение позволяет такие как резервное копирование представляет высокий риск, поэтс	учетной записи пользователя вы файлов и папок или выключение ми такие события сполиет тиате	полнять определенные де компьютера. Удаление фай	айствия на компьютере, йлов журнала	Тип		Host				
Источник: Коррелятор	ny raise coostini orogyor rajare			Инци	на денты актива 🗸	group				
Кол-во повторных открытий: 0 Кол-во происшествий: 1 Правило корреляции: Windows	- Системные журналы были очиц	цены		Инци	денты группы ак	тива 🗸				
та создания 21.03.2025 15:09:5	9									
инцидента Windows - Систем	ные журналы были очищены									
Показать описан	ие									
леднее 21.03.2025 15:09:5 исшествие	8									
азать больше 🗸										
зультат анализа										
хосте 172.30.250.161 были очищены e journal "security" was cleared комендации по устранению инцидента	журналы security, пользовател :	ем Administrator,								
хосте 172.30.250.161 были очищены e journal "security" was cleared комендации по устранению инцидента сшествия	журналы security, пользовател :	ем Administrator,								
хосте 172.30.250.161 были очищены journal "security" наs cleared омендации по устранению инцидента сцествия ать в событиях	журналы security, пользовател :	ем Administrator,							Выбрано: С	
хосте 172.30.250.151 были очицены journal "security" каз cleared окнецации по устранению инцидента сшествия ать в событиях FQDN	журналы security, пользовател :	ем Administrator,	IP			Отправлен	но в НКЦКИ	Начало активности	Выбрано: 0 Конец активности	
xorre 172.30.250.151 Guine ownerses 6 journal "security" was cleared werequizer no ycrparesso инцидента cuecrosus arts & coSurres FODN win-edr-agent.edr-agent.local 1 0 / crparessa ac	журналы security, пользовател	ен Administrator,	IP 172.30.250.161			отправлен Нет	но в НКЦКИ	Начало активности 15:09:58 21.03.2025	Выбрано: 0 Конец активности 15:09:58 21.03.2025	
хость 172.30.250.161 были очивных § Journal "security" каз cleared иницијента сицествия ать 8 событиях FODN win-edr-agent.edr-agent.local 1 > 10 / страникца ~	журналы security, пользовател :	ем Administrator,	IP 172.30.250.161			отправлен Нет	но в НКЦКИ	Начало активности 15:09:58 21.03.2025	Выбрано: 0 Конец активности 15:09:58 21.03.2025	
хосте 172.30.250.151 были очинени јошта] "зесцетку" наз сlеатеd сменидации по устранению инцидента ать в событник FGDN win-edr-agent.edr-agent.local 1) 10 / страница ~ выполенных действий	журналы security, пользовател :	ew Administrator,	IP 172.30.250.161			Отправлен Нет	но в НКЦКИ	Начало активности 15:09:58 21.03.2025	Выбрано: 0 Конец активности 15:09:58 21.03.2025	
хо(те 172.30.250.161 били очищени ј оџита) "зесистКу" наз с.Санте симендацик по устранению инцидента ать в событник FODN win-edr-agent.edr-agent.local 1) 10 / страница ~ выполенных действий ида	журналы security, пользовател : Параметры	ен Administrator,	IP 172.30.250.161 Да	ra crapta	Выполнено	Отправлен Нет	но в НКЦКИ	Начало активности 15:09:58 21.03.2025 Код возврата	Выбрано: 0 Конец активности 15:09:58 21.03.2025	
хо(те 172.30.250.161 бын очиврены 6 јовита) "scurity" каз сleared иницијента атъ в событиях FODN whr-edr-agent.edr-agent.local 1 >> 10 / страница ~ выполенных действий кировать входящий траффик с IP	журналы security, пользовател : Параметры ip: 199.0.0.1	AKTHB WIN-EDR-AGENT	IР 172.30.250.161 Дат 15:	ra crapra 10:18 21.03.2025	Выполнено 15:10:28 21.0.	Стправлен Нет 33.2025	но в НКЦКИ Интеграция RT Protect EDR на 172.30.250.15	Начало активности 15:09:58 21.03.2025 Код возврата 0 0	Выбрано: 0 Конец активности 15:09:58 21.03.2025 Кем выполнен Windows - Системвые журнала были санцен	

Рис. 283 – Просмотр инцидента

При интеграции с системой **RT Protect EDR** при анализе инцидента в блоке **Логи выполненных действий** доступен просмотр следующей дополнительной информации:

- Команда наименование выполненного действия;
- Параметры информация о параметрах выполненного действия;
- Актив наименование актива, на котором выполнено действие;
- Дата старта дата и время запуска исполнения действия;
- Выполнено дата и время выполнения действия;
- Кем выполнено информация об инициаторе выполнения действия, например правило корреляции или пользователь;
- Интеграция наименование интеграции, в рамках которой было выполнено действие;
- Код возврата ответ, полученный при выполнении действия:
 - 0 успешный ответ;
 - 1 при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку 🔘 в соответствующей строке.

16.1.4.5 Просмотр журнала выполнения действий по интеграции

Для просмотра журнала выполнения действий по экземпляру интеграции перейдите в раздел **Параметры** → **Интеграции**, откройте интеграцию на просмотр и перейдите на вкладку "Логи выполненных действий" (см. «Рис. 284»).

≡	Кангес 172.30.252.105 ∨ Интегра	оции				Лицензия активна до: 20	026-04-30 ① Документа	щия Q а	dmin ~
â	← RT Protect EDR на 17	2.30.250.150					Удали	Редактиро	вать
Q O	Основные настройки Задачи интегр	ации Команды интеграции Логи вы	поленных действий						
ςð	Логи выполенных действий							C	0
ø	Актив	Команда	Параметры	Выполнено	Кем выполнен	Интеграция	Дата старта	Код возврата	
18	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 199.0.0.1	15:10:28 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	15:10:18 21.03.2025	0	۵
ж	WIN-EDR-AGENT	Заблокировать порт	port: 16000	15:10:18 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	15:10:00 21.03.2025	0	۵
411	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 123.123.123.123	15:08:03 21.03.2025	admin	RT Protect EDR на 172.30.250.150	15:07:58 21.03.2025	0	٢
0	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 199.0.0.1	13:56:55 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	13:56:50 21.03.2025	0	۲
	WIN-EDR-AGENT	Заблокировать порт	port: 16000	13:56:50 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	13:56:39 21.03.2025	0	۵
	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 199.0.0.1	12:30:36 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:30:31 21.03.2025	0	۵
	WIN-EDR-AGENT	Заблокировать порт	port: 16000	12:30:31 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:30:18 21.03.2025	0	٢
	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 127.127.127.127	12:28:26 21.03.2025	admin	RT Protect EDR на 172.30.250.150	12:28:20 21.03.2025	0	۲
	WIN-EDR-AGENT	Заблокировать входящий траффик с IP	ip: 199.0.0.1	12:17:54 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:17:49 21.03.2025	0	۲
	WIN-EDR-AGENT	Заблокировать порт	port: 16000	12:17:49 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:17:38 21.03.2025	0	٢
	< 1 2 3 4 5 >	10 / страница <							

Рис. 284 – Просмотр интеграции. Вкладка "Логи выполненных действий"

На вкладке отображается следующая информация:

- Актив наименование актива, на котором выполнено действие;
- Команда наименование выполненного действия;
- Параметры информация о параметрах выполненного действия;
- Выполнено дата и время выполнения действия;
- Кем выполнено информация об инициаторе выполнения действия, например правило корреляции или пользователь;
- Интеграция наименование интеграции, в рамках которой было выполнено действие;
- Дата старта дата и время запуска исполнения действия;
- Код возврата ответ, полученный при выполнении действия:
 - 0 успешный ответ;
 - 1 при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку 🔘 в соответствующей строке.

16.2 Kaspersky Security Center

16.2.1 Характеристики системы

Наименование системы – Kaspersky Security Center (далее KSC).

Назначение системы – универсальная консоль централизованного управления различными решениями, продуктами и сервисами, которые обеспечивают информационную безопасность корпоративной ИТ-инфраструктуры.

Разработчик системы – АО «Лаборатория Касперского».

Сайт – Security Center | Лаборатория Касперского.

Возможности, предоставляемые интеграцией:

- синхронизация активов;
- использование сервиса **Sonar** для сканирования активов. Использование сервиса выполняется в соответствии с параметрами, указанными для экземпляра интеграции.

16.2.2 Настройка интеграции

Перед выполнением настройки интеграции активируйте тип интеграции **KSC**. Подробнее см. раздел «<u>Типы интеграций</u>».

Процесс настройки интеграции с КSC включает в себя следующие шаги:

- «Шаг 1. Создание экземпляра интеграции с KSC»;
- «Шаг 2. Создание задачи по синхронизации активов»;
- «Шаг 3. Активация экземпляра интеграции с KSC».

16.2.2.1 Шаг 1. Создание экземпляра интеграции с KSC

- 1. Перейдите в раздел Параметры Интеграции.
- 2. Нажмите кнопку Создать. Откроется окно "Создание интеграции" (см. «Рис. 285»).

← Создание интеграции	Сбросить	Проверить	Сохранить
Название интеграции *			
Интеграция с KSC			
Статус			
Тип интеграции *			
Kaspersky Security Center			~
Адрес сервера *			
172.30.254.101			
Имя пользователя *			
ksc_admin			
Пароль *			

Домен			
Сбросить Проверить Сохранить			

Рис. 285 – Создание интеграции с KSC

- 3. Укажите в окне следующую информацию:
 - Название интеграции укажите наименование интеграции;

- **Тип интеграции** из выпадающего списка выберите значение "*Kaspersky Security Center*". Поля формы автоматически изменятся для настройки выбранного типа интеграции;
- Адрес сервера укажите IP-адрес, на котором развернут API сервер KSC;
- **Имя пользователя** укажите имя пользователя для доступа к API серверу KSC. Убедитесь, что пользователь обладает необходимым набором прав для выполнения запросов к API серверу KSC;
- Пароль укажите пароль пользователя;
- Домен при необходимости укажите домен, в котором располагается API сервер KSC.
- 4. Нажмите кнопку **Проверить**. Будет выполнена проверка подключения к API серверу. После успешной проверки соединения с API сервером станет доступно сохранение экземпляра интеграции.
- 5. Нажмите кнопку Сохранить.

16.2.2.2 Шаг 2. Создание задачи по синхронизации активов

- 1. Откройте экземпляр интеграции на редактирование (кнопка 🖉).
- 2. Перейдите на вкладку "Задачи интеграции" (см. «Рис. 286»).

≡	K	ПАНГЕО РАДАР	172.30.254.60 ∨ Интеграции		Лицензия	активна до: 2026-	02-07 🤅	ЭДокументация	1 (2)) admin 🗸
â		←	Интеграция с KSC					Удалить	Добавити	ь задачу
Q										
()		Основ	ные настройки Задачи интеграции	Команды интеграции	Логи выполенных де	ействий				
⊒ ∃		Доба	вить задачу Удалить Удалить все	Переключить активность					Выбранс): 0 C
G			Задача интеграции 🕼	Название		Cron		Состояние		
Ø			Синхронизация активов	Синхронизация активов		01***		🚺 Активно		Ø 🗓
₩.	>	<	1 > 50 / страница ~							
Ж										
498										
Ø										

Рис. 286 – Настройка интеграции. Вкладка "Задачи интеграции"

3. Нажмите кнопку Добавить задачу. Откроется окно "Добавить задачу" (см. «Рис. 287»).

	X
Название *	
Синхронизация активов	
Cron *	
01***	
Состояние	
Задача интеграции *	
Синхронизация активов	\sim

Рис. 287 – Окно "Добавить задачу"

- 4. Укажите в окне следующую информацию:
 - Название укажите название периодической задачи;
 - **Cron** укажите CRON-выражение, описывающее периодичность задачи. Подсказу по CRON-выражениям см. на <u>сайте</u>;
 - **Состояние** включите выполнение задачи синхронизации активов, установив переключатель в положение "Включен";
 - Задача интеграции из выпадающего списка выберите задачу "Синхронизация активов".
- 5. Нажмите кнопку Сохранить.
- 6. Журнал выполнения задачи можно посмотреть в разделе **Администрирование** → **Кластер** → вкладка **Планировщик задач**.

16.2.2.3 Шаг 3. Активация экземпляра интеграции с KSC

Чтобы по экземпляру интеграции выполнялось взаимодействие с системой **KSC**, ее необходимо активировать.

Для активации интеграции перейдите в раздел **Параметры** → **Интеграции** и в колонке **Статус** установите переключатель в положение "Включен".

16.2.3 Работа с интеграцией

В ходе работы интеграции будет выполняться сканирование активов в соответствии с параметрами периодической задачи:

1. Запускается периодическая задача.

- 2. Платформа Радар запрашивает у КSC информацию об агентах (активах).
- 3. Информация об активах добавляется в платформу.
- 4. На форме просмотра актива появляется дополнительная информация:
 - наименование экземпляра интеграции, в рамках которой получены сведение об активе;
 - наименование агента в системе KSC, на основании которого создан актив;
 - ссылка для просмотра агента непосредственно в системе KSC.

Для просмотра журнала выполнения действий по конкретной интеграции перейдите в раздел **Параметры** → **Интеграции**, откройте интеграцию на просмотр (кнопка ^(O)) и перейдите на вкладку "Логи выполненных действий".