R-Vision

Новые подходы в банальных процессах (SIEM, VM)

Вячеслав Ковалев
Руководитель пресейл-группы

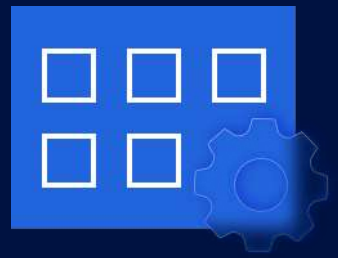
Процессы в LM/SIEM

1

Сбор и обработка событий ИБ

Используются продукты: LM и SIEM

Настройка модели данных

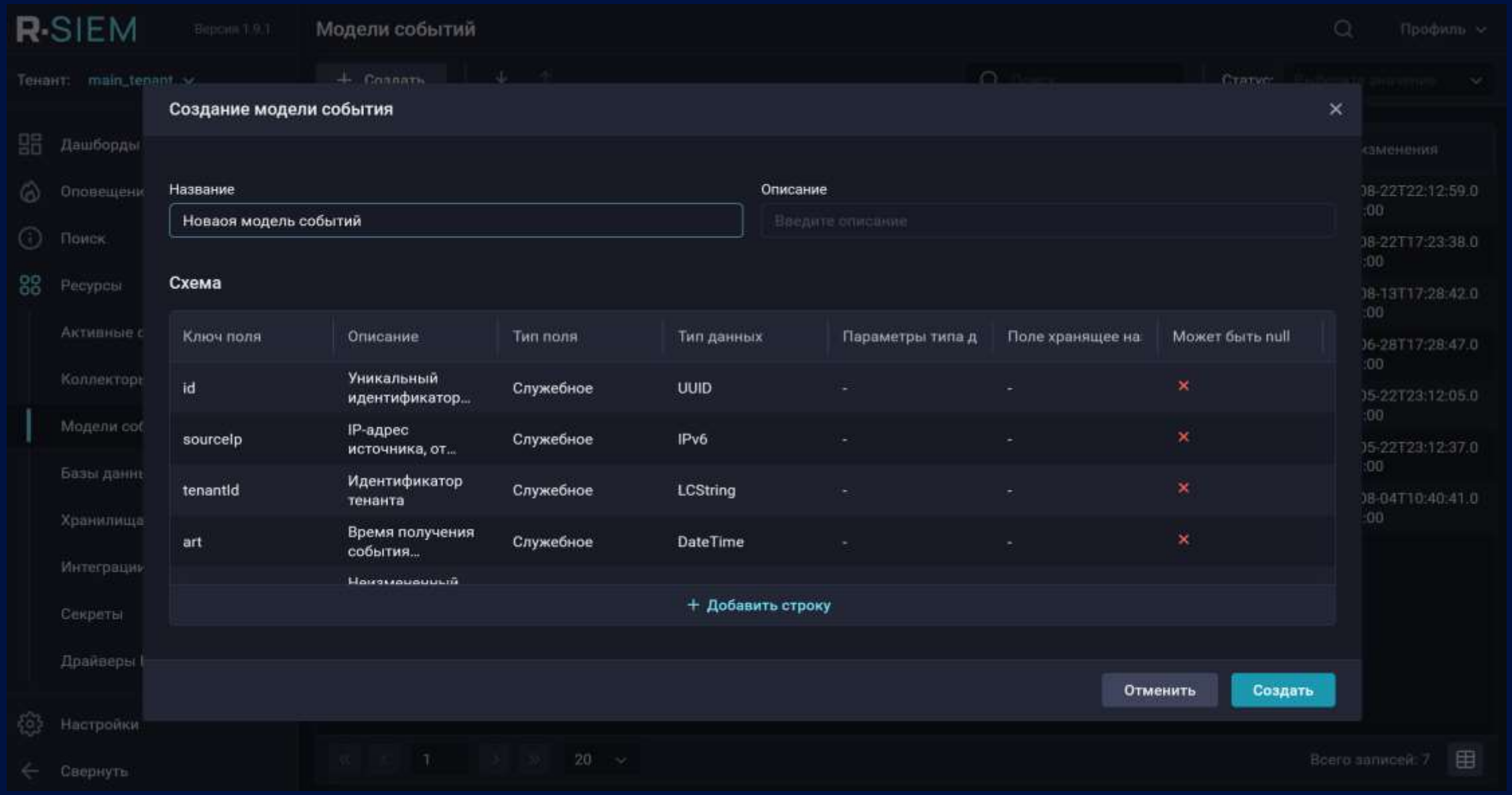


Модель событий

Позволяет собирать и хранить любую необходимую информацию

- Настроенная модель событий
- Универсальная модель данных с возможностью быстрого расширения
- Доступно создание пользовательской модели данных

Настройка модели данных



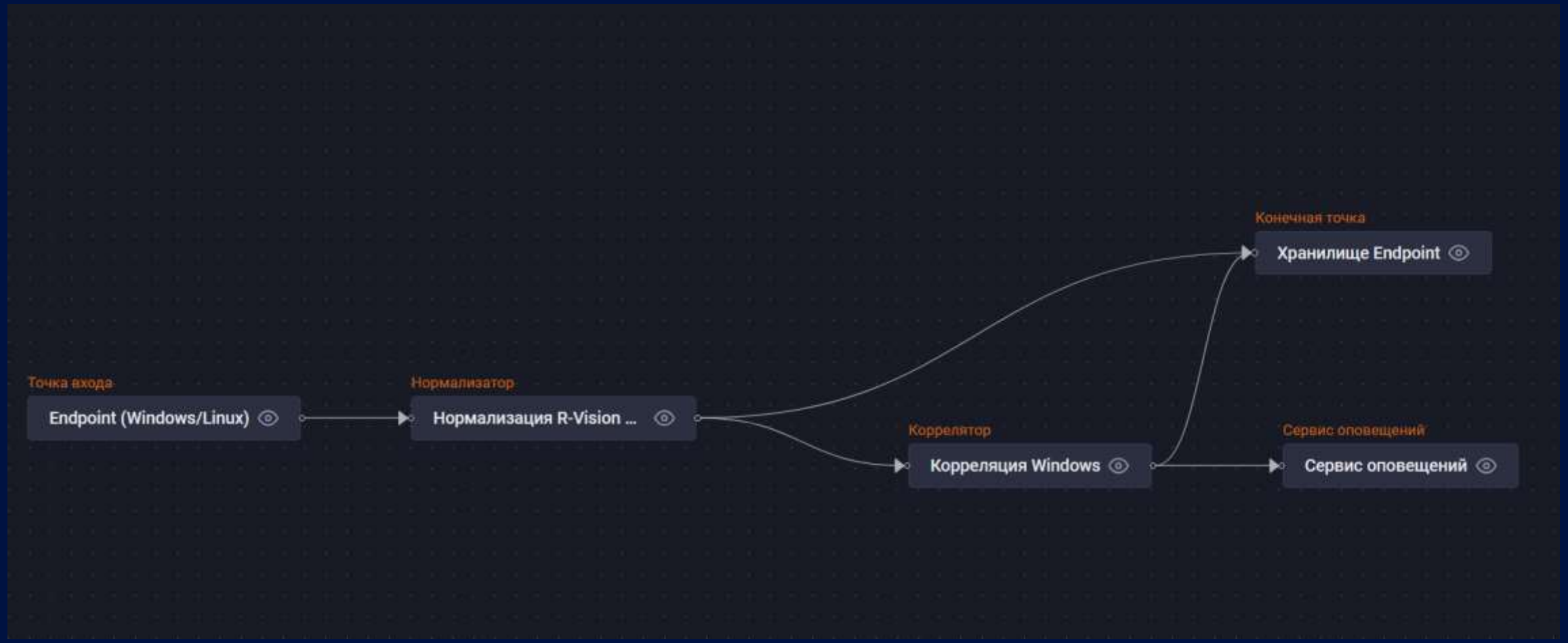
Подключение источников и распределение потоков данных

Конвейер обработки событий

Единое окно для работы со всеми элементами для сбора и обработки событий

- Визуальное управление потоком событий
- Быстрое подключение новых источников информации
- Гибкость при конфигурировании компонентов конвейера

Подключение источников и распределение потоков данных

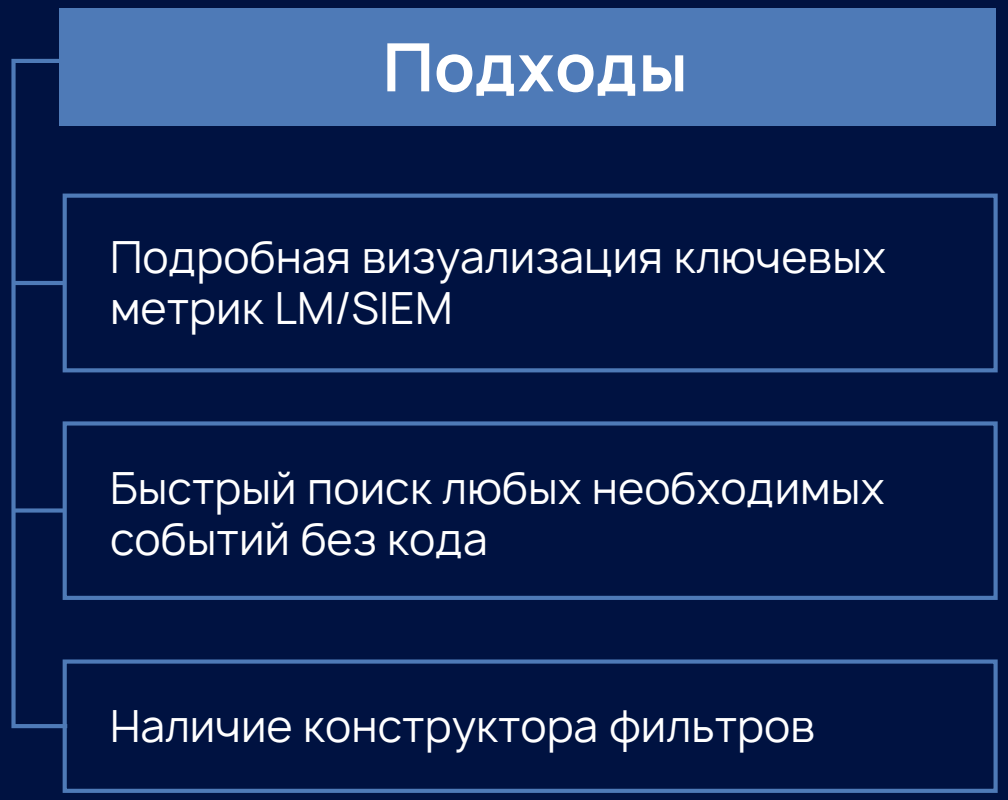


2

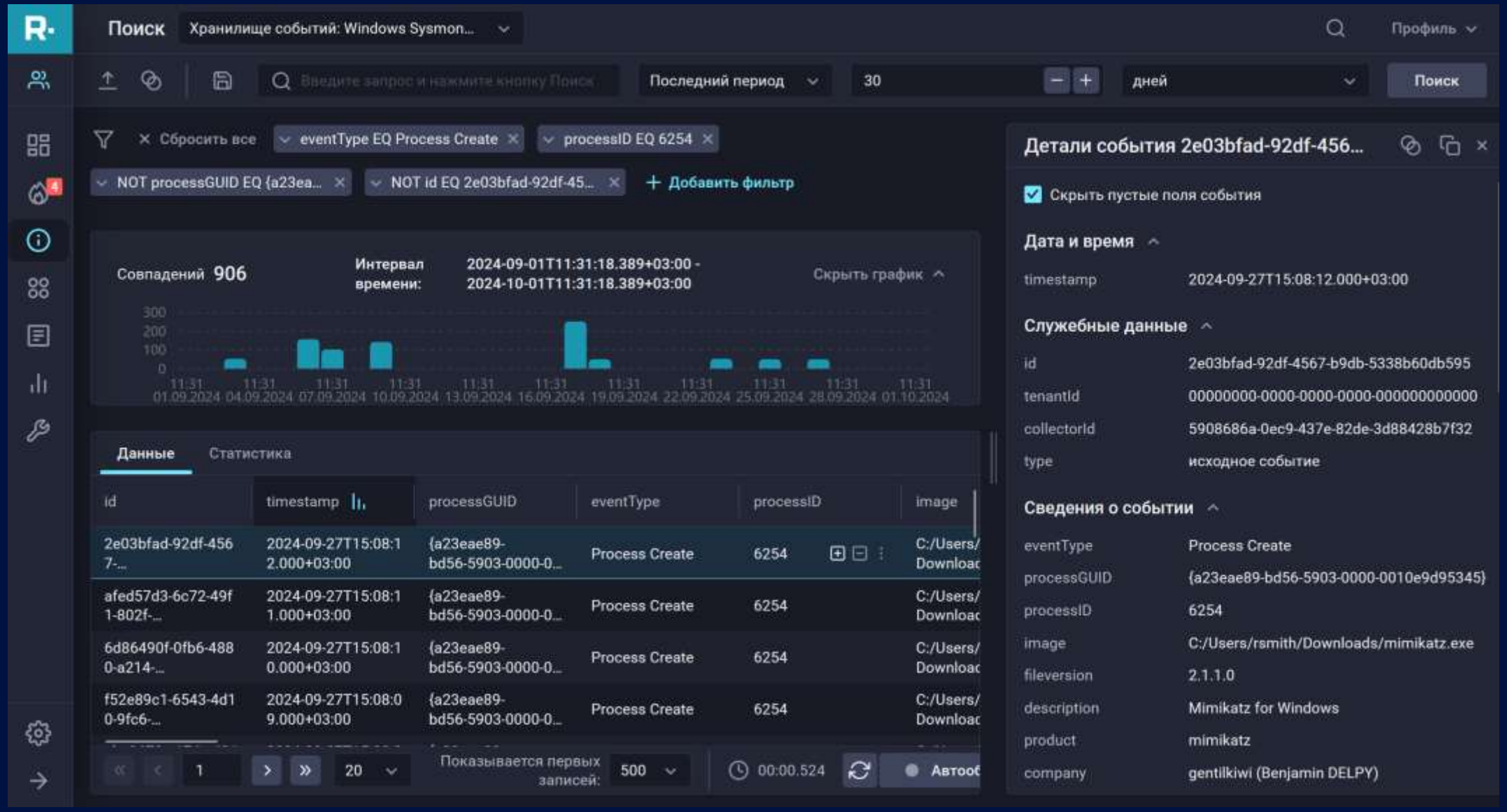
Работа с событиями ИБ

Используются продукты: LM и SIEM

Поиск и визуализация событий



Поиск и визуализация событий



3

Работа с контентом правил

Используются продукты: LM и SIEM

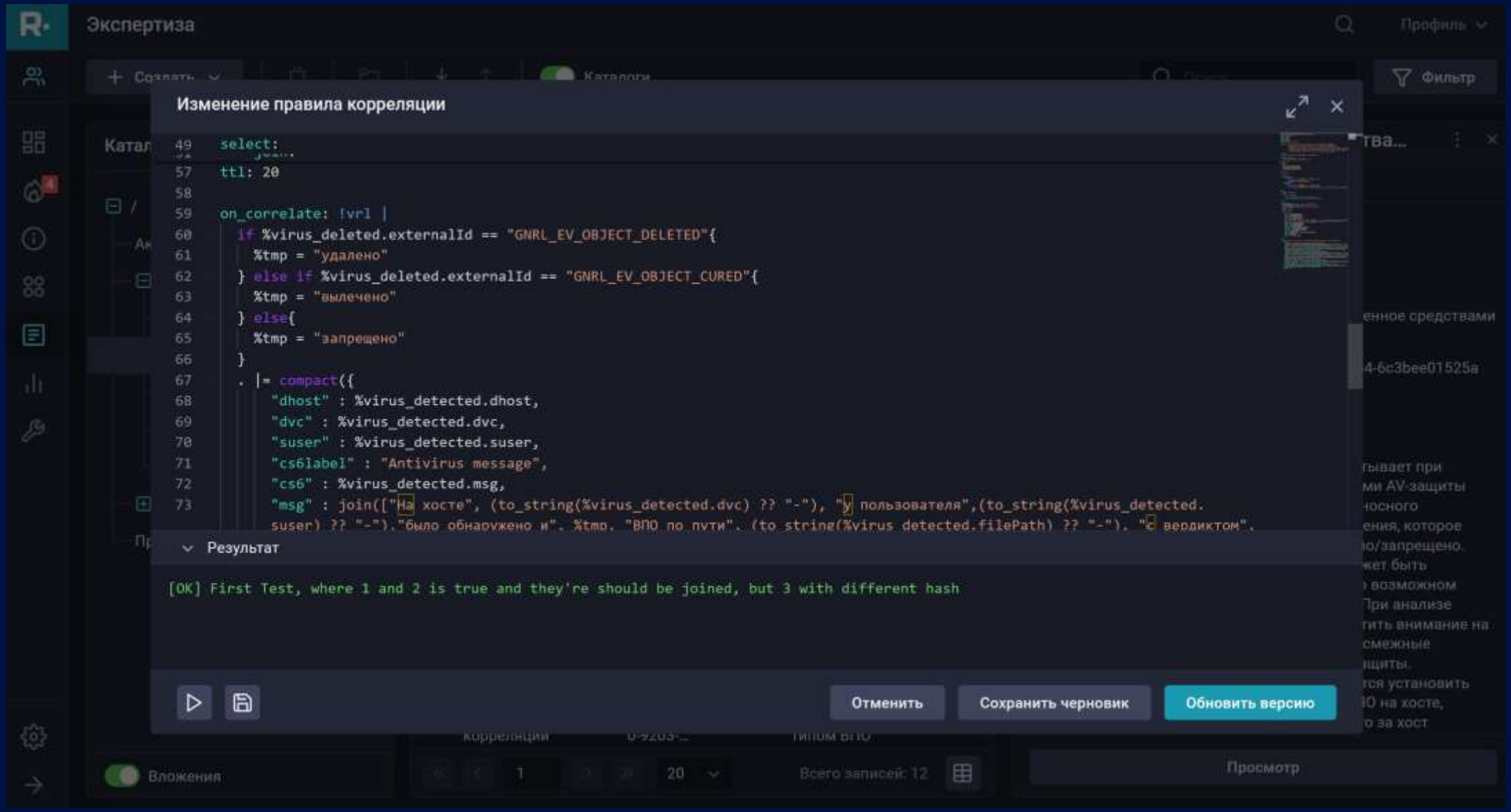
Разработка и модификация контента

As Code

Набор инструментов для профессионалов, позволяющий разрабатывать правила под любые требования организации

- Собственный плагин R-Object
- Гибкость при создании правил
- Детектирование инцидентов любой сложности
- Валидация и подсветка синтаксиса

Разработка и модификация контента



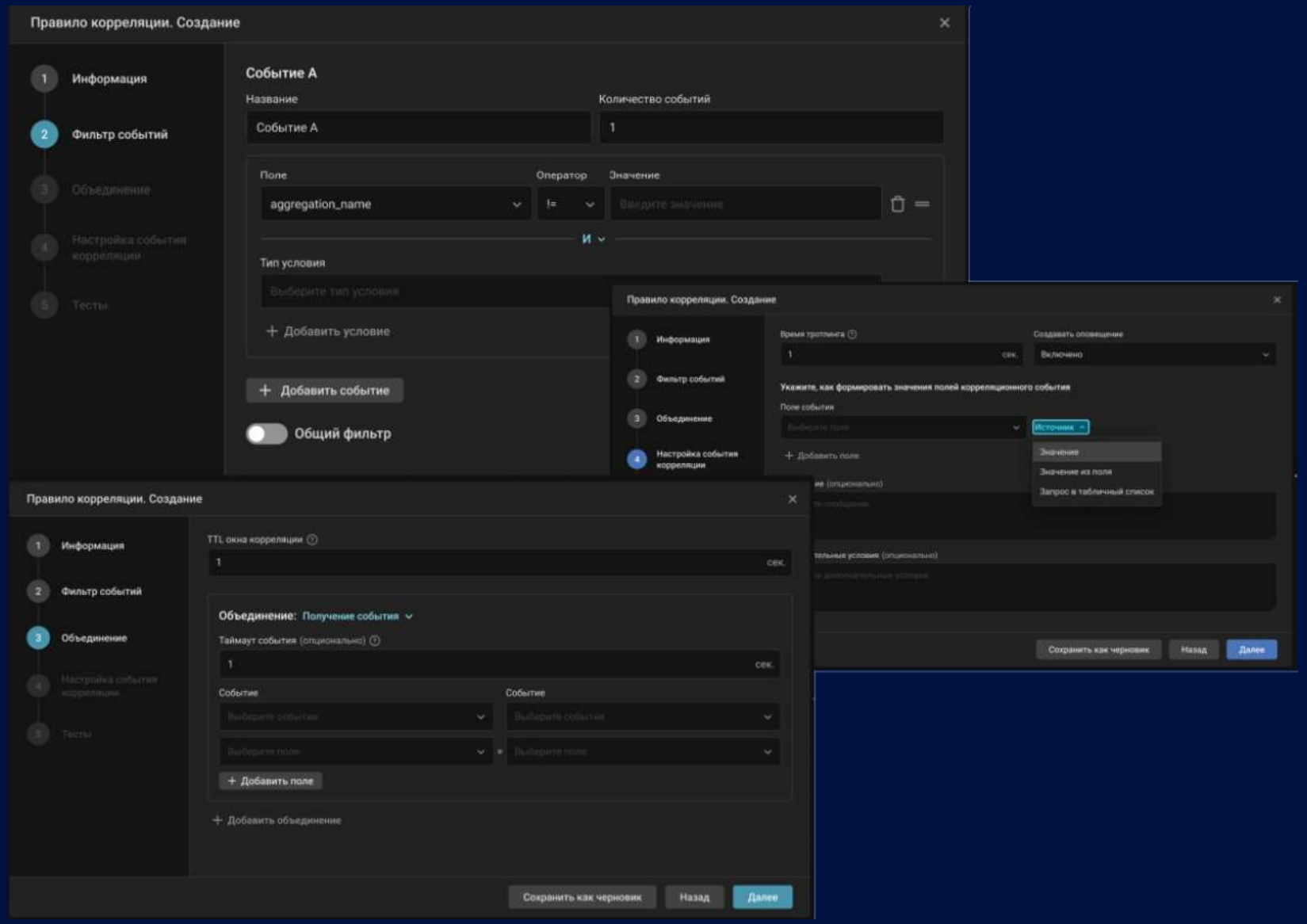
Разработка и модификация контента

Конструктор

Помогает оперативно составить
не сложные запросы для закрытия
потребностей детектирования

- Низкий порог входа
- Визуализация логики правила
- Интуитивный и понятный интерфейс

Разработка и модификация контента



Процессы в VM

Процесс управления уязвимостями

1

Проведение инвентаризации

Используются продукты: сканер уязвимостей

Инвентаризация

Даст полную информацию о защищаемых активах

Возможности:

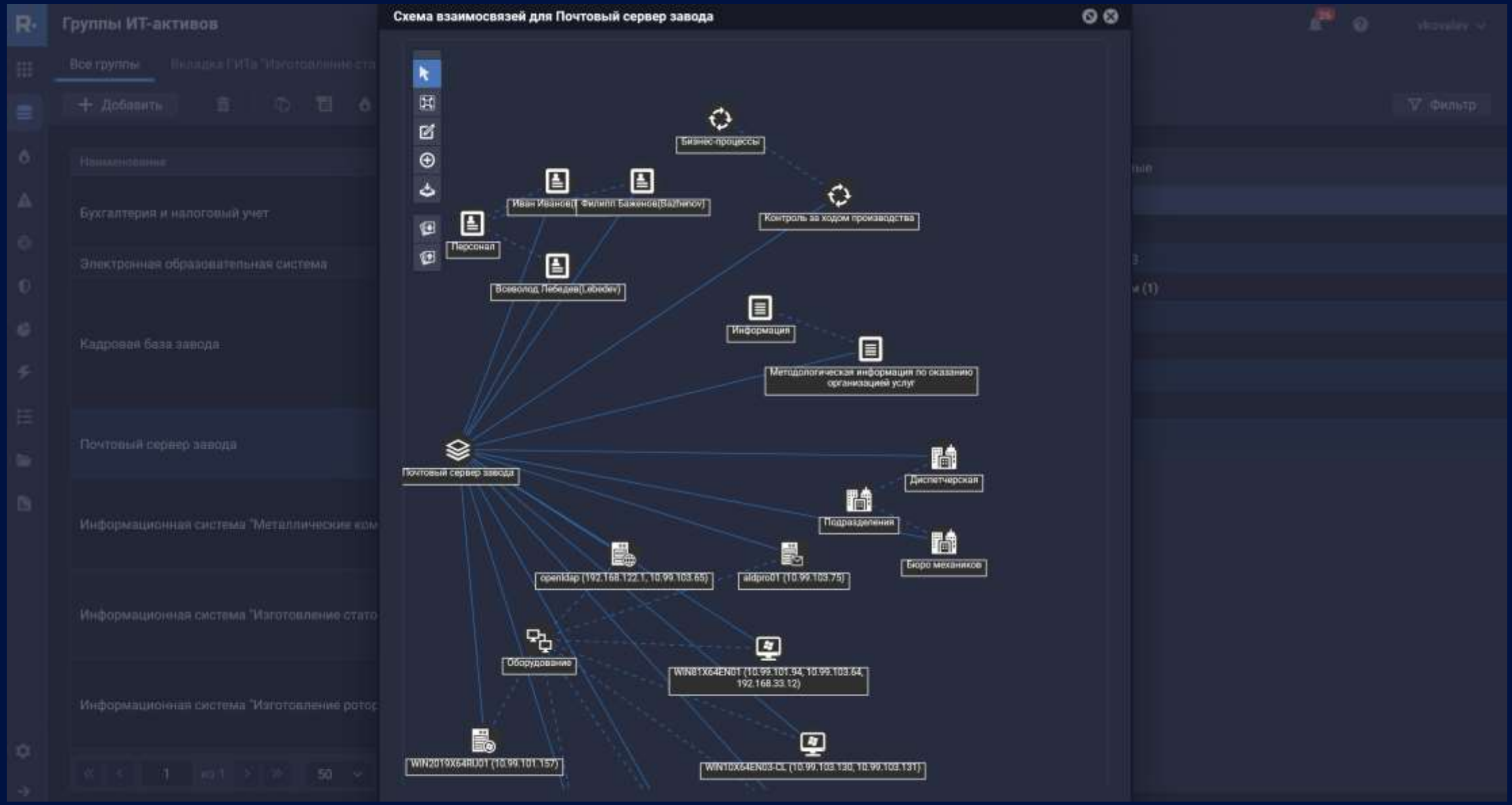
- **Быстрое** сканирование всей ИТ-инфраструктуры в режимах discovery и inventory
- Импорт информации из любых источников (сканеры, СЗИ, ИТ-системы)
- Автоматическая корреляция и дедупликация данных

От 3-х секунд

скорость сканирования одного устройства

Применение ресурсно-сервисной модели позволит сфокусировать внимание на защите **наиболее критичных хостов**

Инвентаризация



2

Выявление уязвимостей

Используются продукты: сканер уязвимостей

Выполнение задач на сканирование

Один коллектор сканера

- Определение уязвимостей на сервере
- Управление интервальным сканированием
- Одна задача на все виды ОС
- Автоподбор учетных записей
- Расписание сканирования с техническими паузами

3

Приоритетазия уязвимостей

Используются продукты: VM

Определение уровня критичности уязвимостей

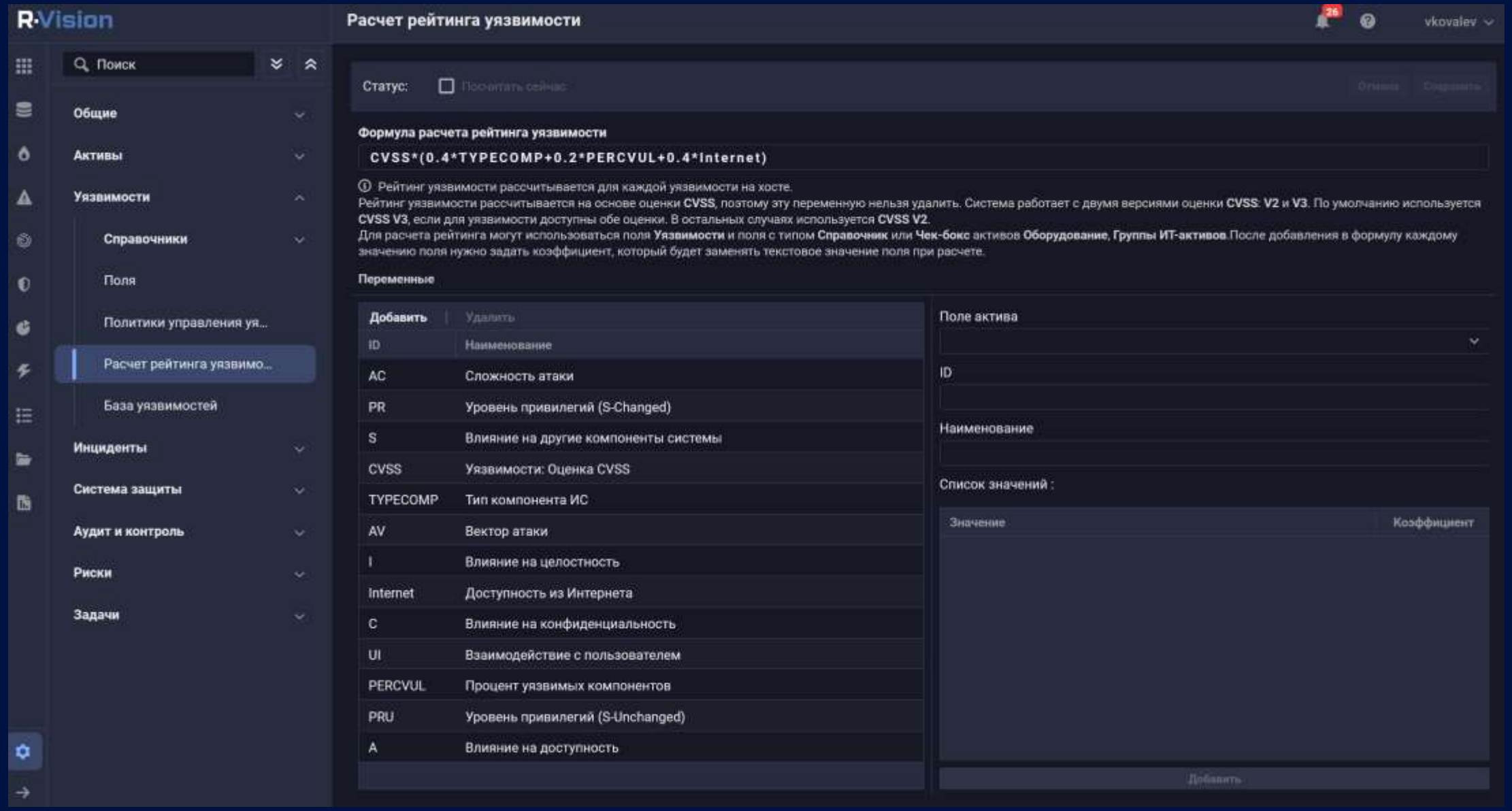
Расчет рейтинга на основе любых атрибутов:

- Уязвимости
- Оборудования
- Группы ИТ-активов

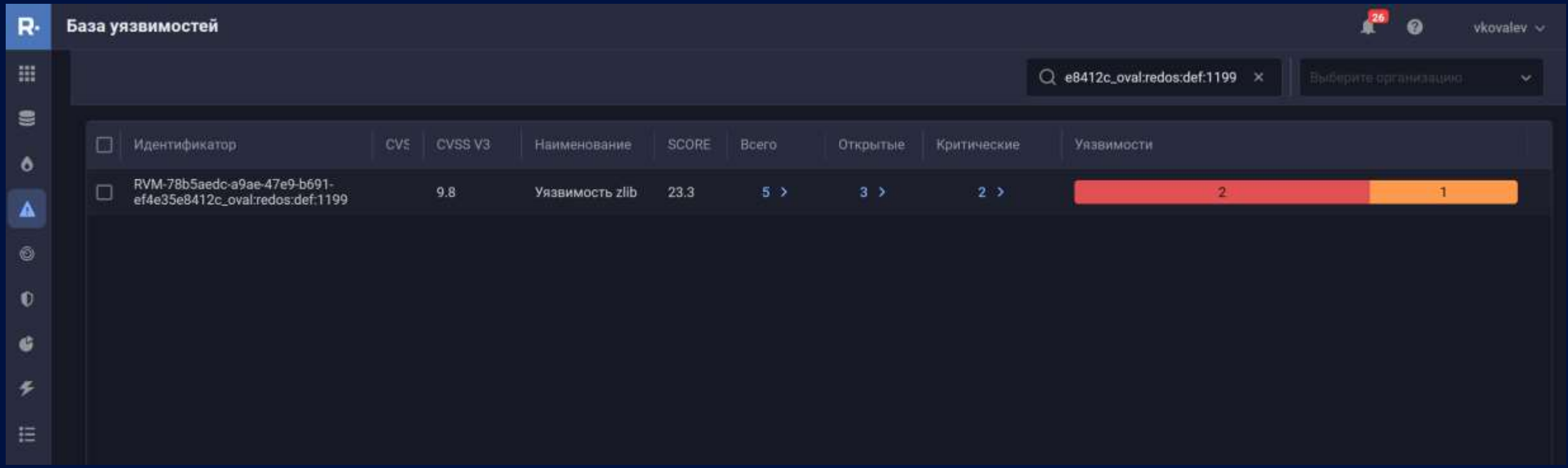
Приоритизация уязвимостей:

- По рекомендациям ФСТЭК
- На основании международных практик
- С учетом внутренних регламентов организации

Определение уровня критичности уязвимостей



Определение уровня критичности уязвимостей



4

Устранение уязвимостей

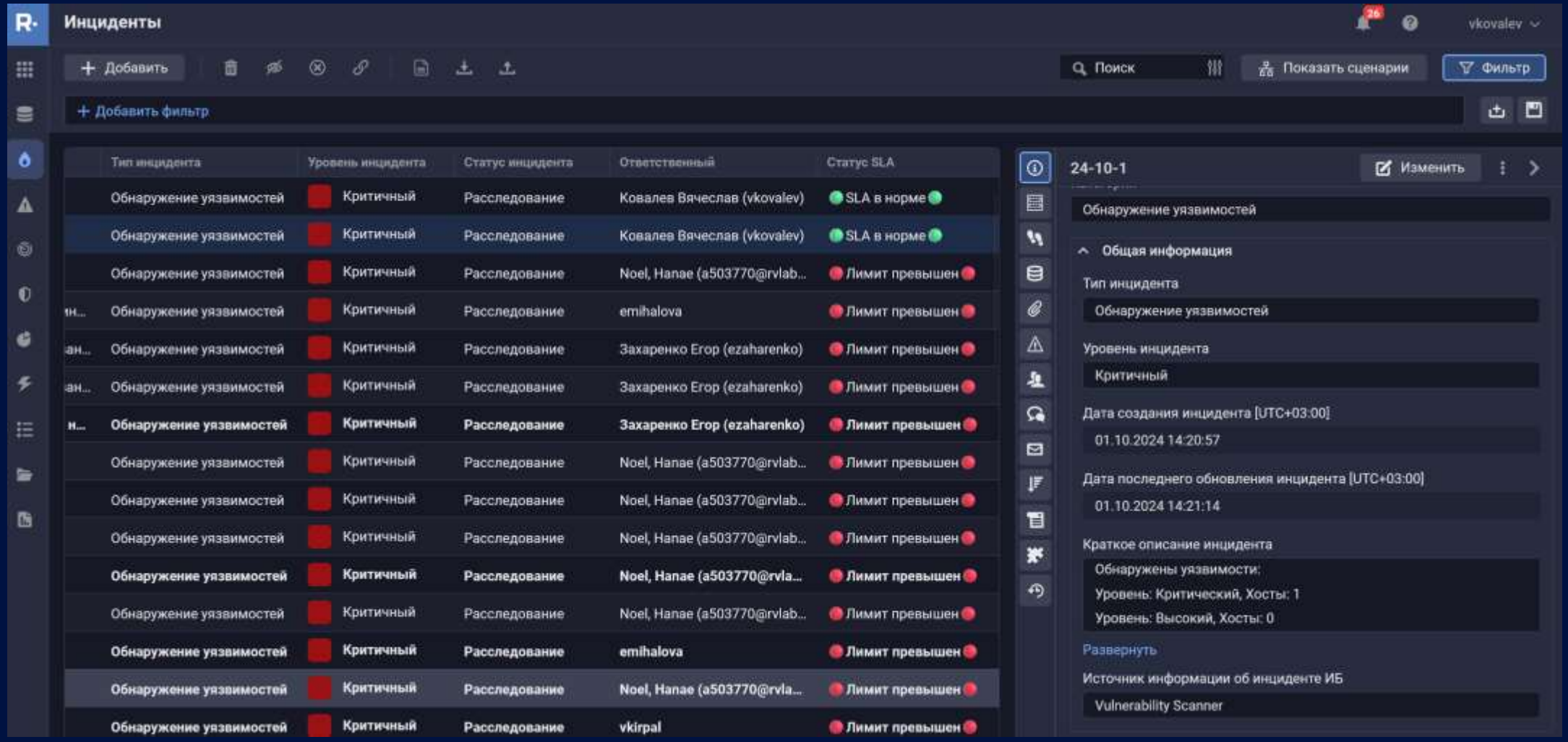
Используются продукты: VM

Обработка критичных уязвимостей

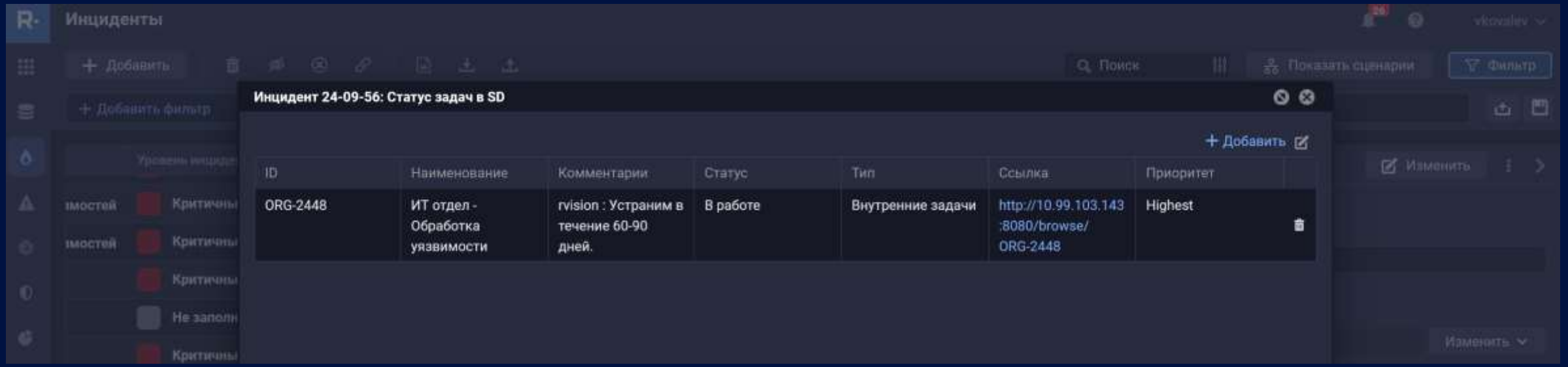
Выстроить процесс с помощью:

- Учета компенсирующих мер
- Построение статусной модели
- Политик управления уязвимостям
- Автоматизированная постановка задач и инцидентов
- Интеграции с внешними Service Desk решениями

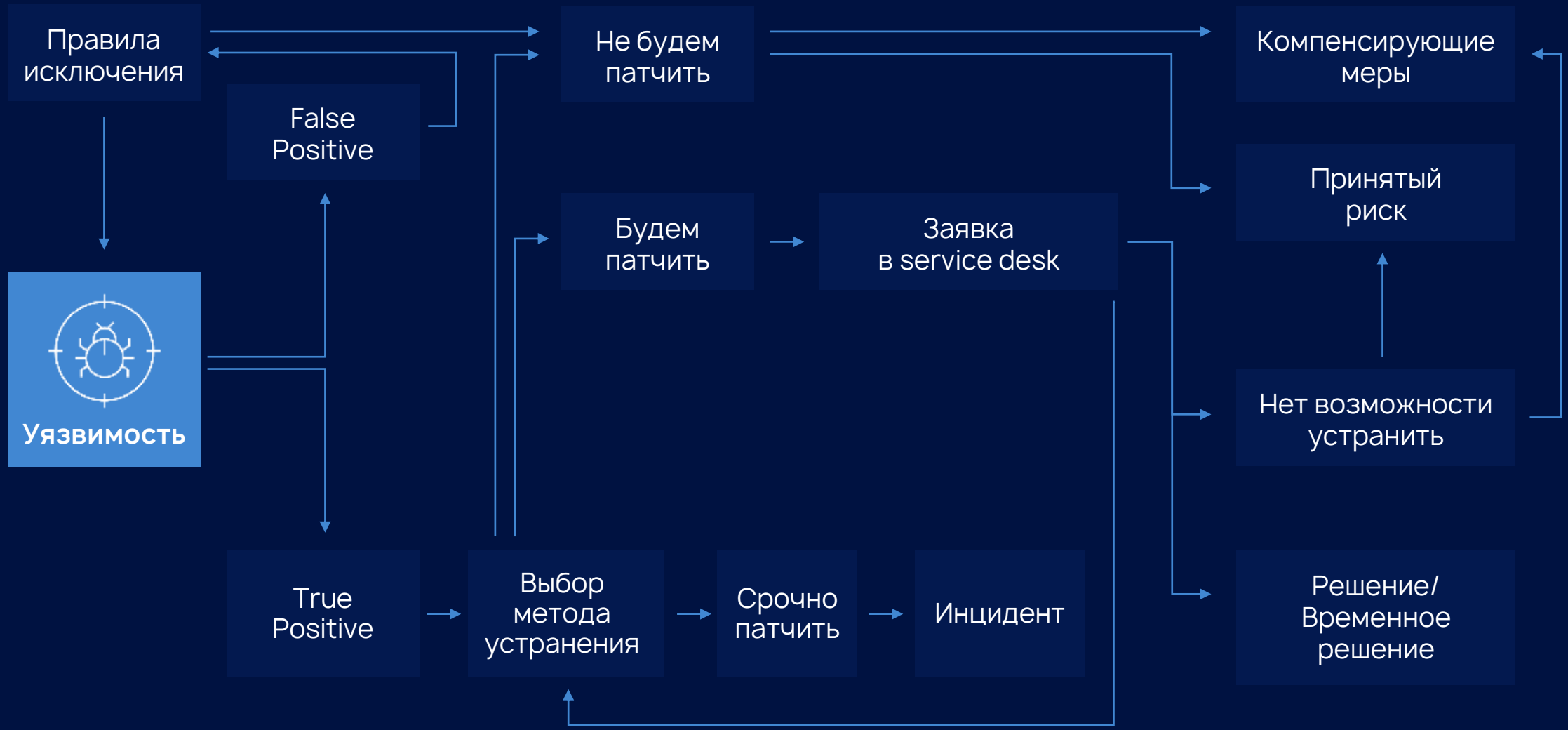
Обработка критичных уязвимостей



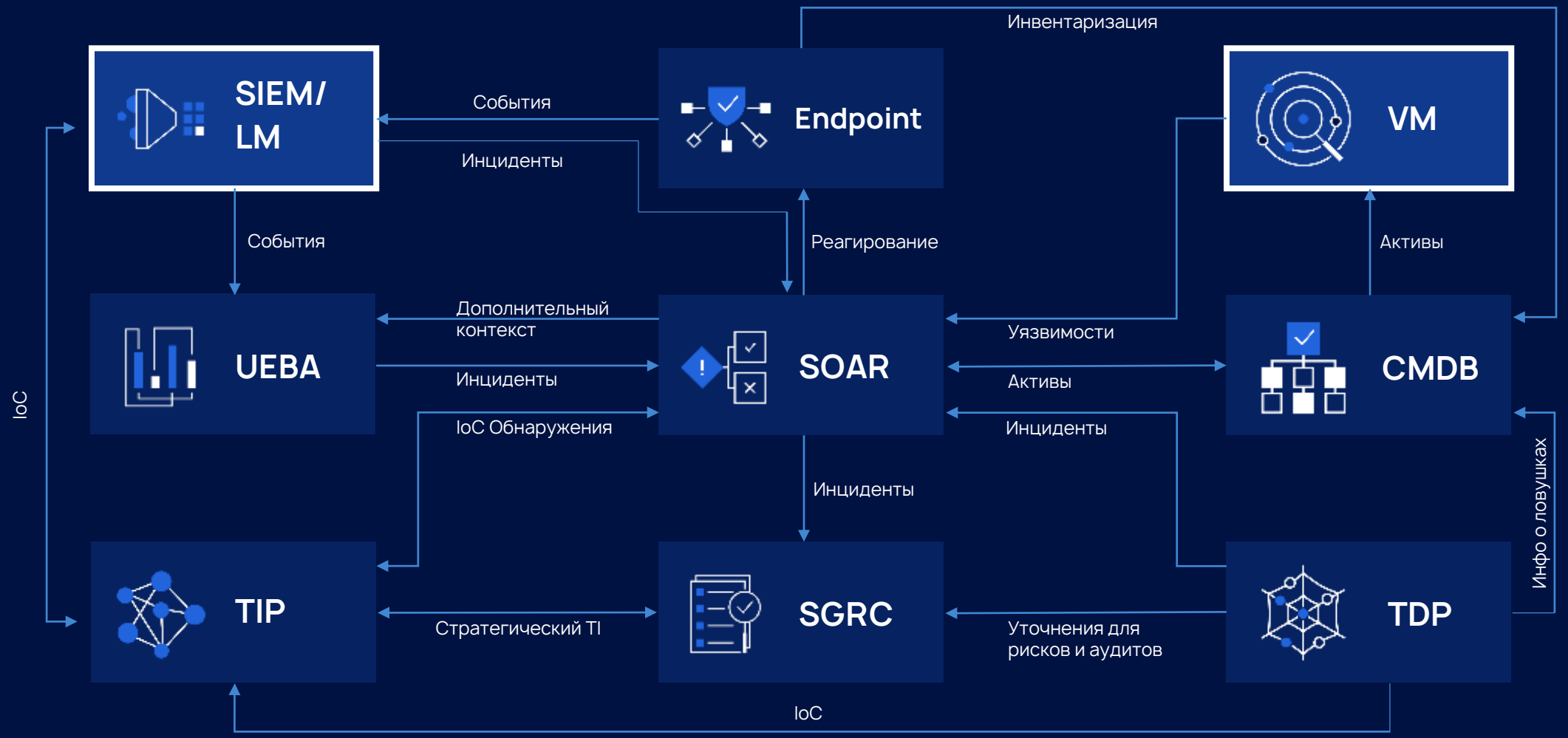
Обработка критичных уязвимостей



Как будем устранять уязвимость



Экосистема R-Vision Evo



R-Vision

Свяжитесь с нами удобным способом:

+7 (499) 322 80 40

sales@rvision.ru

Читайте наш Дайджест ИБ:

rvision.ru/blog

t.me/rvision_pro

vk.com/rvision_ru

rvision.ru