R-Vision

SOAR+TI как способ компенсировать

возможности ушедшего с российского рынка ПО

Иван Чувилин
Руководитель Presale
ichuvilin@rvision.ru

О чем будем говорить?

- Что сейчас происходит в ИБ
- Как действовать
- Реализованные кейсы на проектах:
  проблемы со сканерами уязвимостей, СЗИ и SIEM.

Что случилось

Ушли либо приостановили деятельность в РФ:

- ✓ **SIEM**
  MicroFocus (ArcSight SIEM), Fortinet (FortiSIEM), RSA NetWitness, IBM (Qradar SIEM), Rapid7 InsightIDR
- ✓ **Сканеры уязвимостей**
  Qualys, Tenable (Nessus) , IBM (Qradar VM), F-Secure, Rapid 7 (Nexpose Vulnerability Scanner)
- ✓ **UBA**
  Exabeam, модули в ArchSight, Qradar
- ✓ **Threat Deception**
  TrapX, Illusive
- ✓ **SOAR**
  Fortinet, PaloAlto, IBM, Micro Focus, Cisco NGFW, системы обнаружения вторжений, Anti-DDoS, антивирусы, песочницы и пр.
- ✓ **ITSM, CMDB**
  Micro Focus, Ivanti, Atlassian (Jira)

Ужесточение требований на законодательном уровне:

- ✓ Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (исполнение до 1 января 2025 г)
- ✓ Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
- ✓ ФЗ от 14.07.2022 №266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»
- ✓ № 187-ФЗ «О безопасности КИИ РФ»
- ✓ законопроект об оборотных штрафах за утечку личных данных

С чего начать?

- Какие бизнес процессы есть в организации
- Из чего они состоят
- Какие риски к ним относятся
- Какие меры защиты уже внедрены

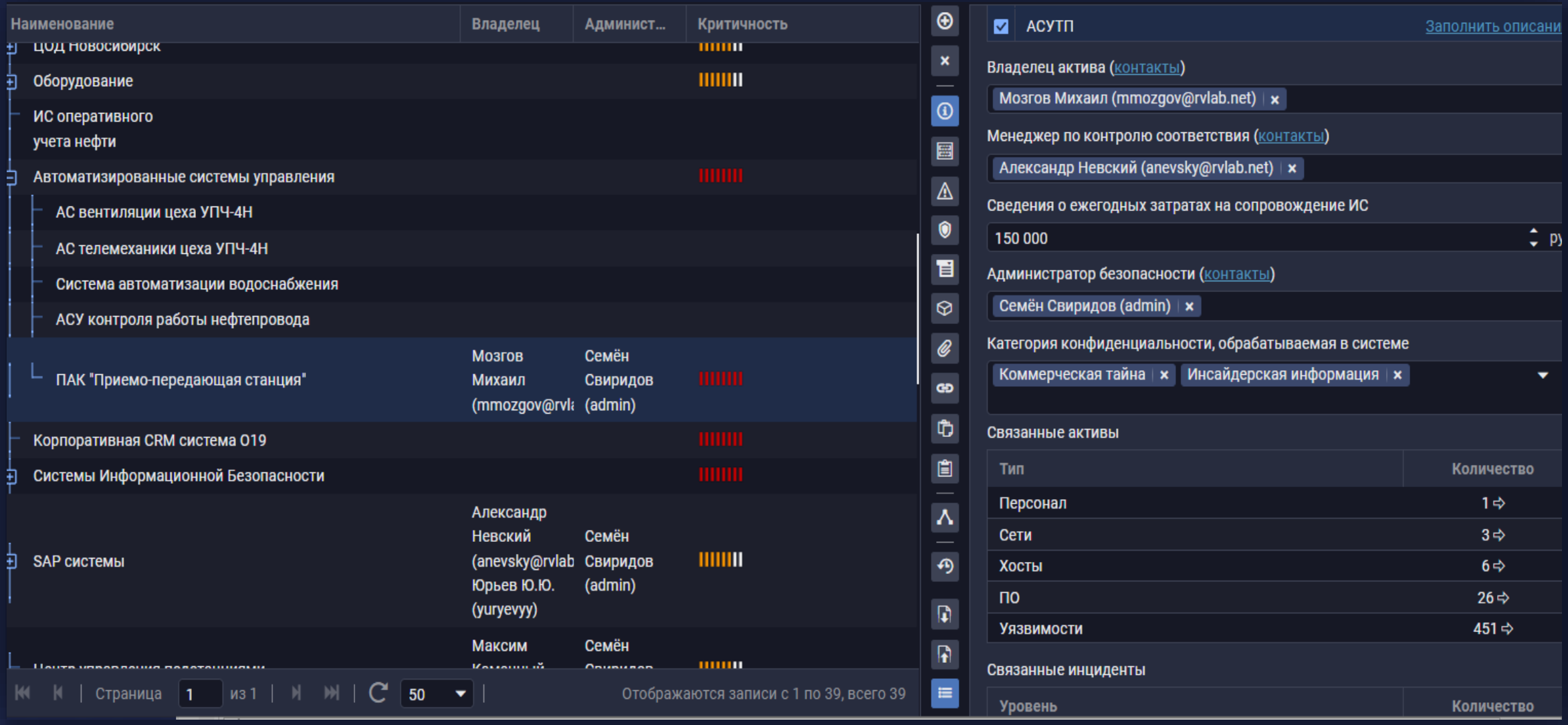
КЕЙС № 0
Управление активами

Кейс № 0 Проведите инвентаризацию активов

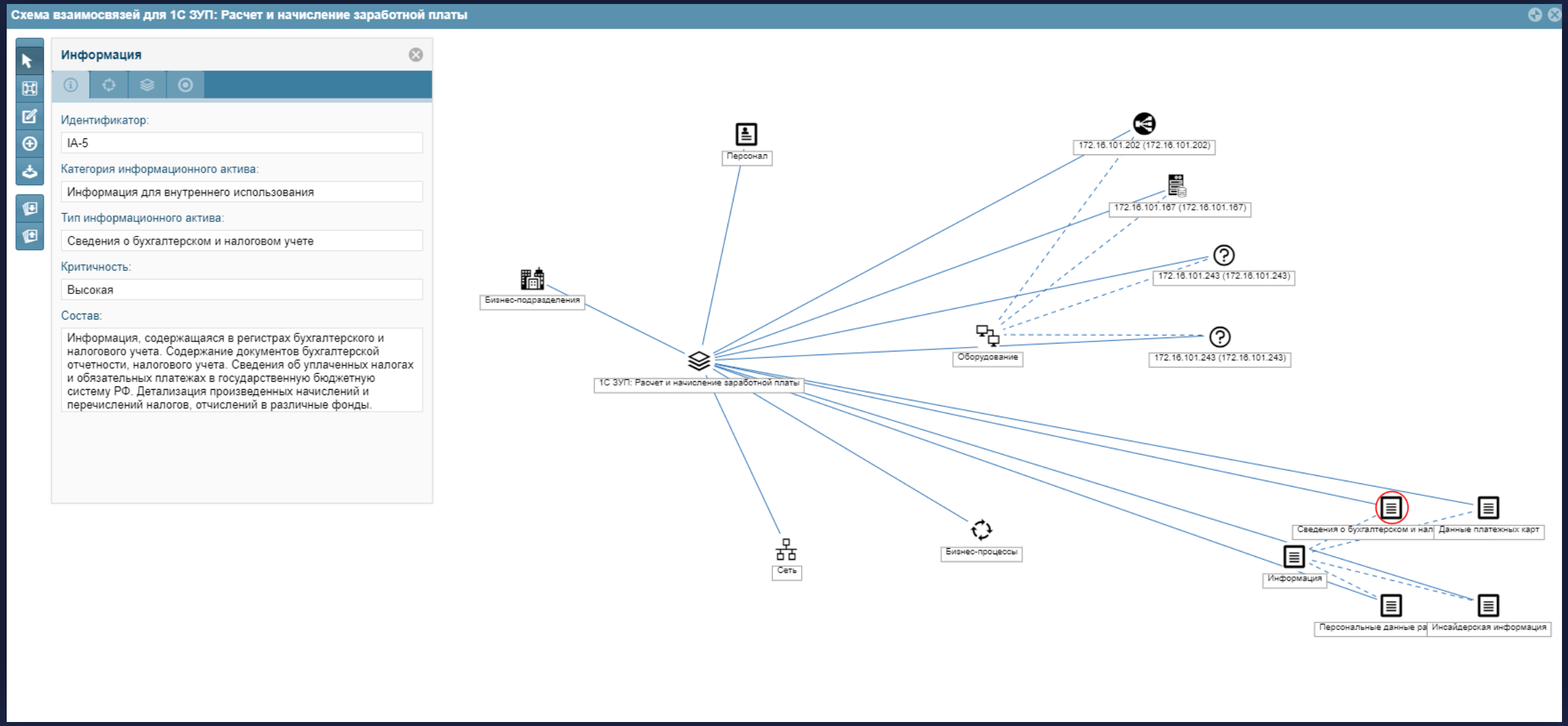
Внешние системы: AV, VM, SIEM, ITSM, CMDB

Инвентаризация R-Vision

Ручная настройка



Результат: CMBD для ИБ/ИТ, ресурсно-сервисная модель



Результат: CMBD для ИБ/ИТ, ресурсно-сервисная модель

КЕЙС № 1
Vulnerability Management

Сканер уязвимостей – альтернативы по качеству нет

- **Open Source**
  необходимо настраивать и поддерживать самостоятельно, не хватает контекста

- **Отечественный сканер**
  ложные срабатывания, слепые зоны, отсутствие приоритезации, качество продукта

- **Импортные решения из дружественных стран**
  нет сертификата ФСТЭК, нет проектов и опыта использования

Решение

Процесс работы с уязвимостями на базе **R-Vision SOAR + сканер**:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ Приоритезация
- ✓ Автоматизированное управление

Управление уязвимостями: инвентаризация

R-Vision SOAR:

- ✓ список всех активов и полная, подробная информация по ним
- ✓ ресурсно-сервисная модель
- ✓ нет слепых зон

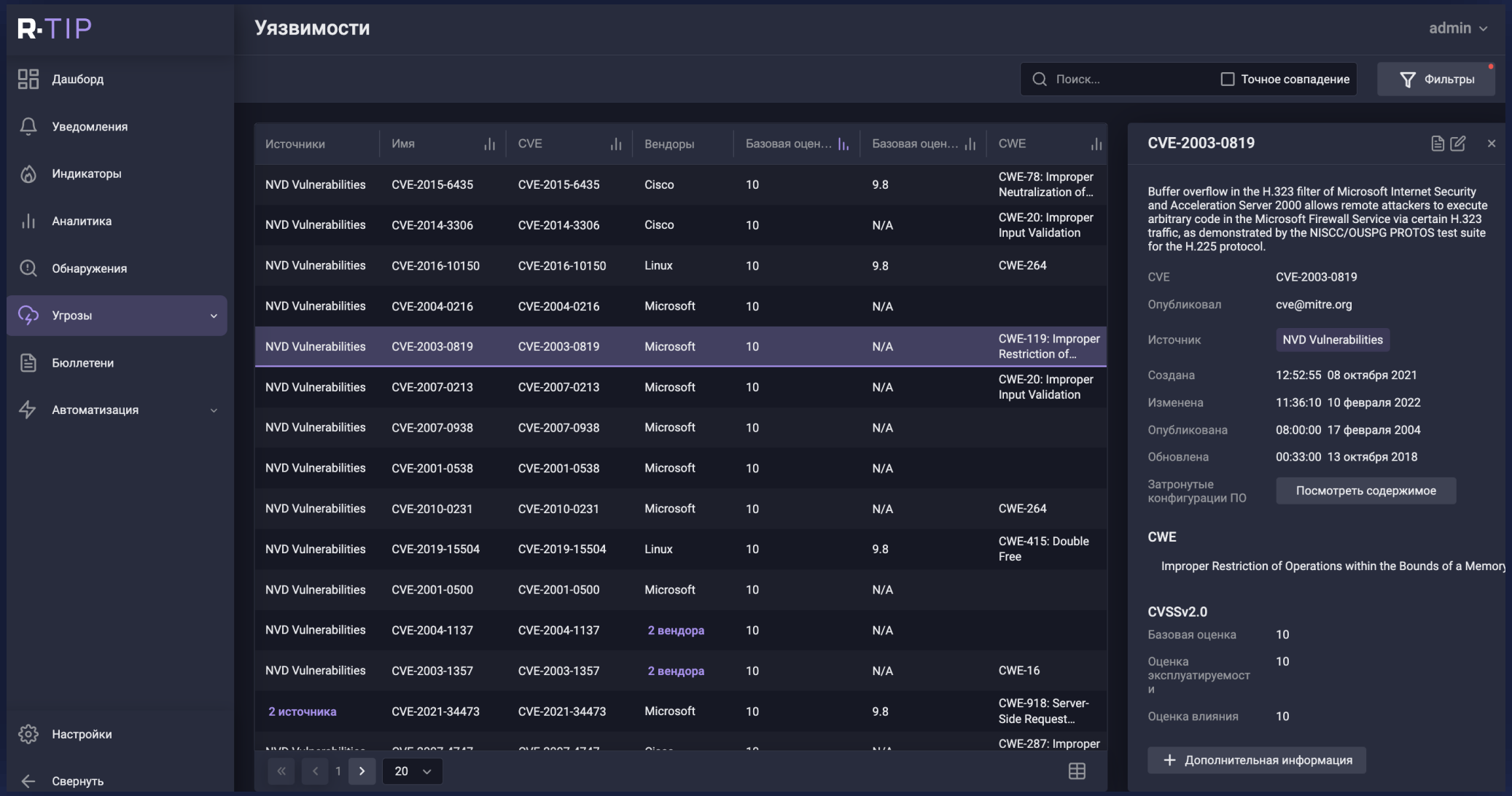
Управление уязвимостями: сканирование

Любой подходящий сканер:

- ✓ список уязвимостей
- ✓ оценка CVSS

Работа с уязвимостями на базе R-Vision SOAR + сканер:

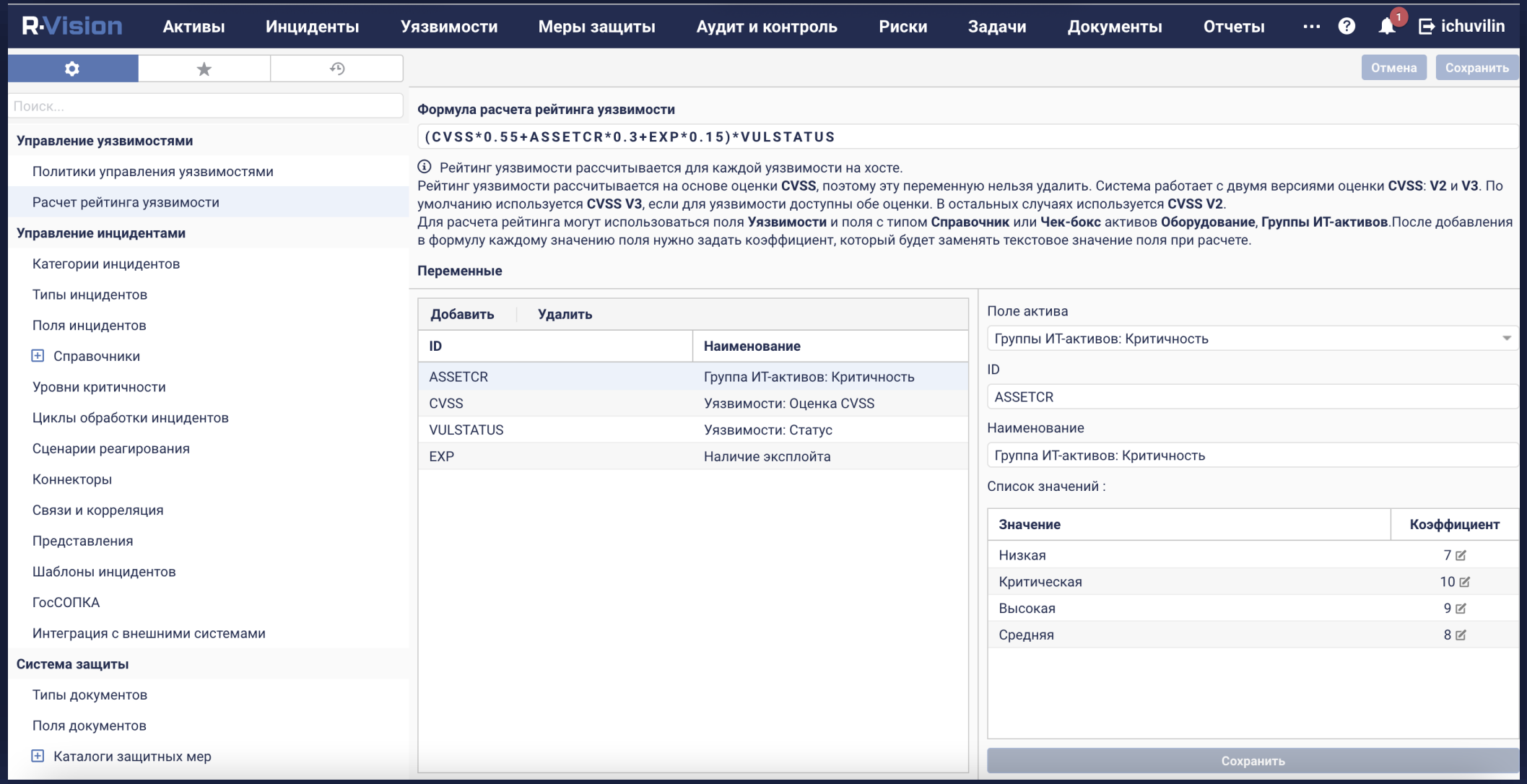
- ✓ Инвентаризация
- ✓ Сканирование
- ✓ **Обогащение**
- ✓ Приоритезация
- ✓ Автоматизированное управление



Управление уязвимостями: обогащение

Работа с уязвимостями на базе R-Vision SOAR + сканер:

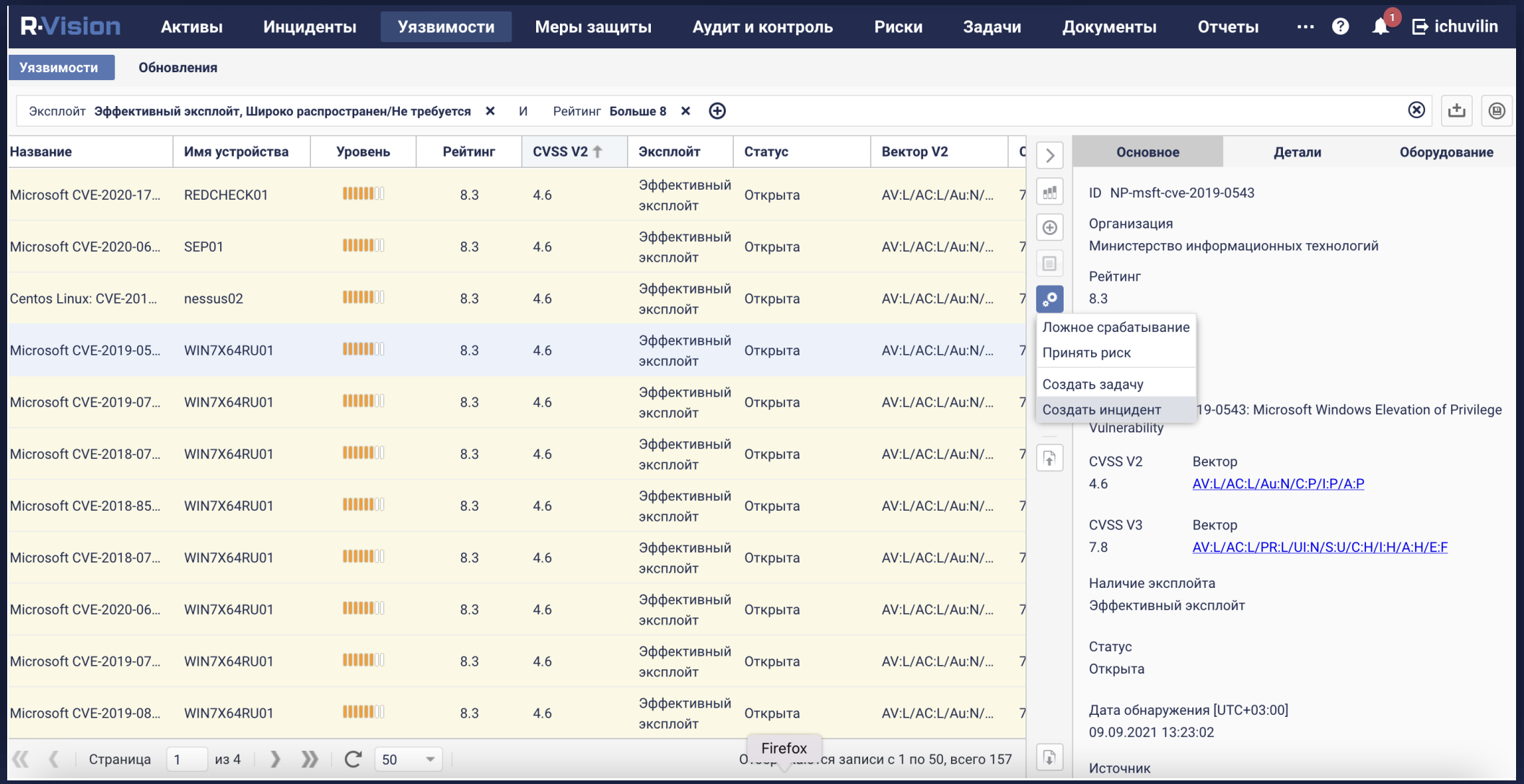
- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ **Приоритезация**
- ✓ Автоматизированное управление



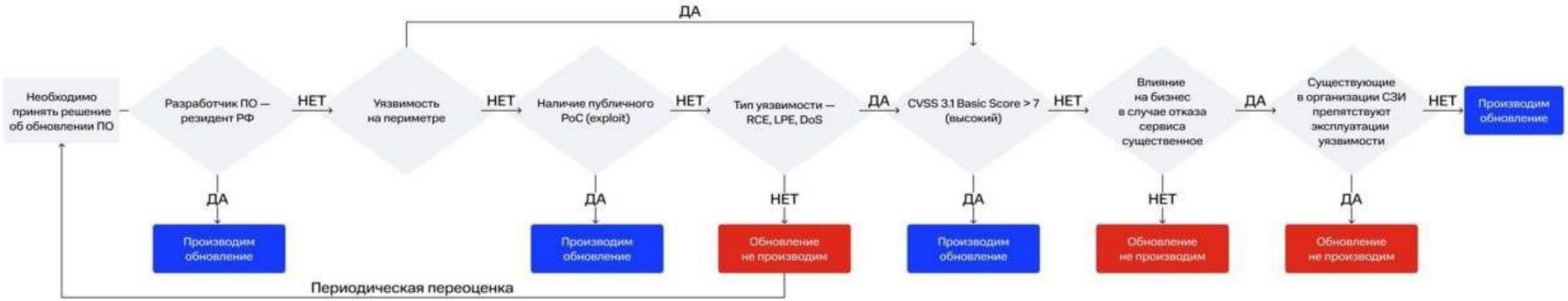
Рейтинг уязвимостей в R-Vision SOAR

Работа с уязвимостями на базе R-Vision SOAR + сканер:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ Приоритезация
- ✓ **Автоматизированное управление**



Автоматизация управления в R-Vision SOAR



Алгоритм принятия решения по обновлению критичного ПО от НКЦКИ

КЕЙС № 2
Blacklist на СЗИ

TIP как база для обогащения

Что произошло:

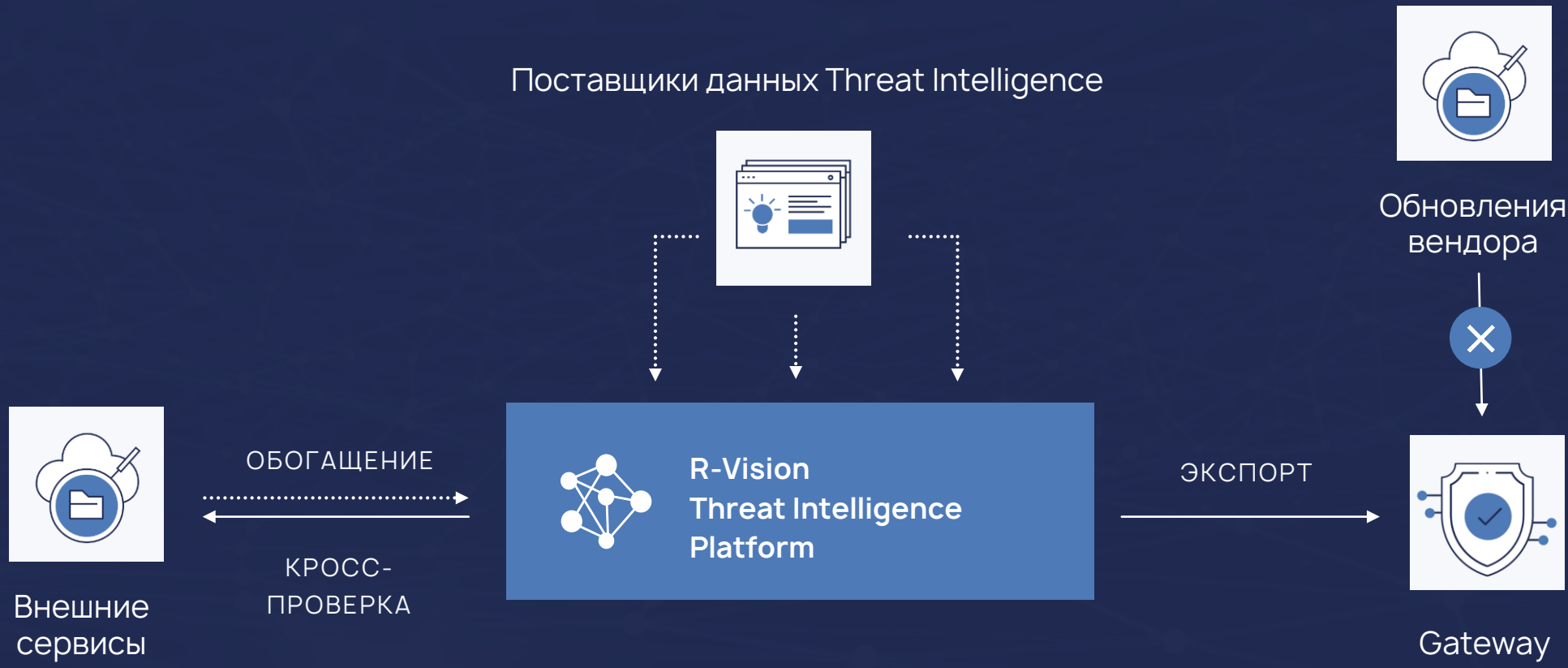
- Вендор отключил доступ к фидам и индикаторам в одностороннем порядке
- Gateway работает, но не защищает от новых угроз. Нет обновлений

TIP как база для обогащения

Решение:

- Сделали экспорт в СЗИ в список правил запрета те индикаторы, которые имеют высокий рейтинг

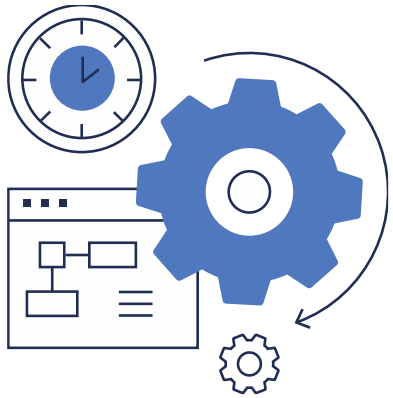
Решение


Поставщики данных Threat Intelligence
Обновления вендора
ОБОГАЩЕНИЕ
КРОСС-ПРОВЕРКА
R-Vision Threat Intelligence Platform
ЭКСПОРТ
Внешние сервисы
Gateway

КЕЙС № 3

SIEM: заменить нельзя оставить

Спешить с заменой SIEM не обязательно



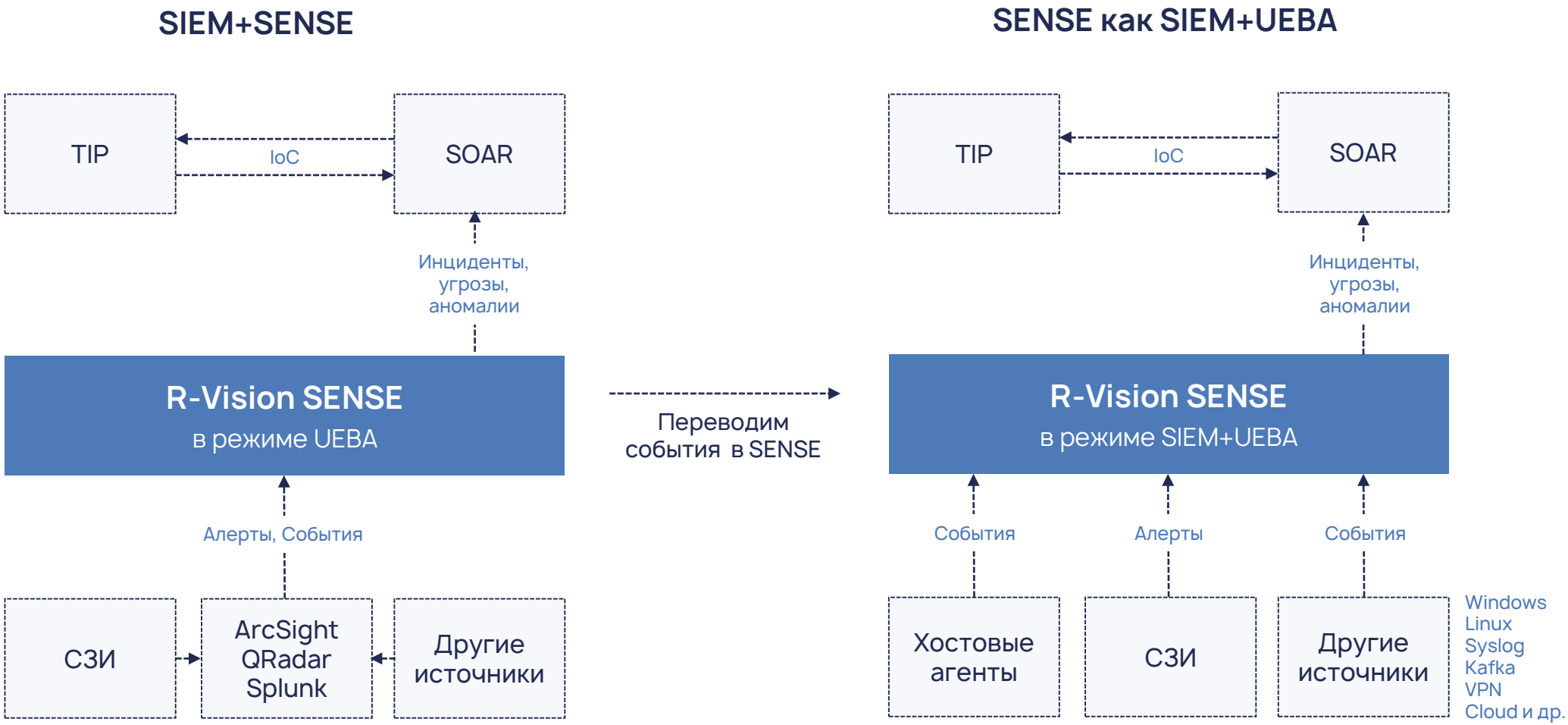
- ✓ Срочное обновление продукта не требуется, система работает – есть время все взвешенно обдумать
- ✓ Но хочется перестраховаться на случай, если с решением пойдет что-то не так

Решение

- Мы поставили R-Vision SENSE как UEBA:
  снижаем false-positive, даем дополнительные
  инструменты анализа для более качественного детекта
  и выявления аномалий
- В нужный момент поток событий заворачивается
  напрямую в SENSE
- При этом правила переносятся, и система переходит
  в режим работы «SIEM + UEBA»

До 2025 года есть время на закупку расширенной лицензии и миграцию в R-Vision SENSE полностью

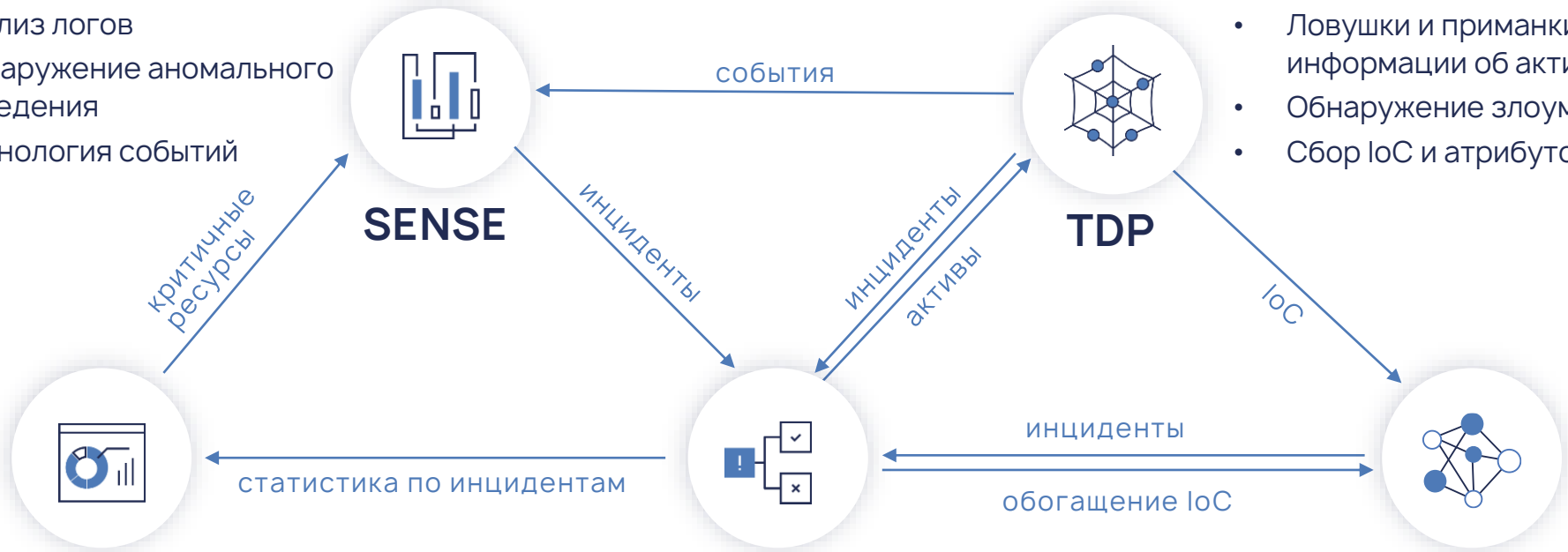
Схема работы SIEM+SENSE+SOAR



Экосистема R-Vision

- Анализ логов
- Обнаружение аномального поведения
- Хронология событий

- Ловушки и приманки на основе информации об активах
- Обнаружение злоумышленника
- Сбор IoC и атрибутов атакующего



- Полная картина ИБ
- Управление ИТ-активами
- Аудиты с ретроспективой
- Риски с учётом инцидентов

- Оркестрация, автоматизация ИБ
- Управление ИТ-активами
- Единое рабочее пространство для команды SOC
- Взаимодействие с регуляторами

- Агрегация всех данных TI
- Поиск IoC в инфраструктуре
- Экспорт IoC на СЗИ

R-Vision

+ 7 (499) 322 80 40

sales@rvision. ru

rvision.ru

Подписывайтесь на наш бесплатный дайджест ИБ: **rvision.ru/blog**