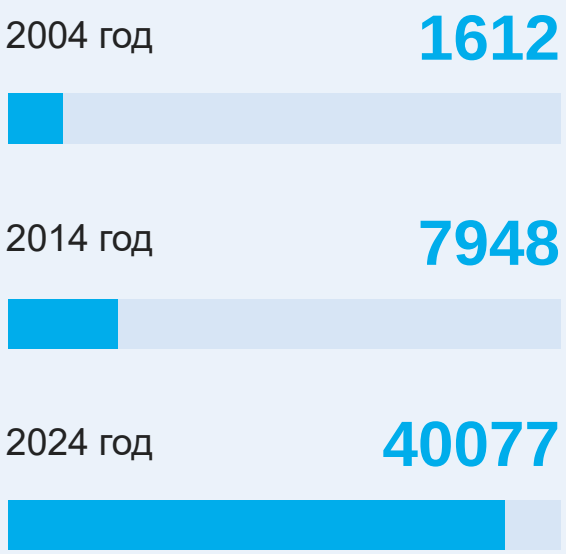
От образа до продакшна: как управлять рисками в контейнерной среде

TI

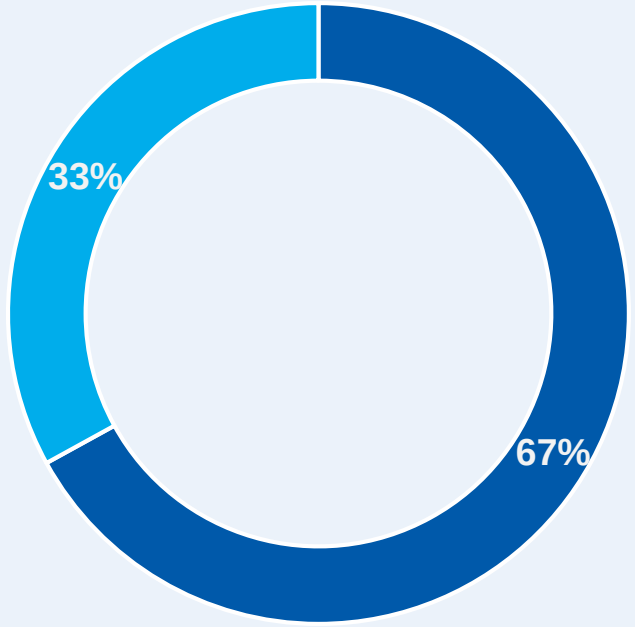
Тренды по безопасности контейнеризации

Купол

Рост количества угроз безопасности



Сталкивалась ли организация с замедлением разработки из-за проблемы уязвимости контейнерной среды?



Red Hat Report

30% сообщили, что их организация была оштрафована в результате инцидента

47% организаций потеряли прибыль или клиентов из-за инцидента с безопасностью контейнеров

33% организаций считают, что текущее решение безопасности контейнеров замедляет разработку

7 инцидентов, связанных с безопасностью, в среднем в год пережили организации

Риски контейнерных сред разработки

Купол

Риски образов

+ Уязвимости в образе
+ Дефекты конфигурации
+ Встроенное malware (вирусы, секреты и т. д.)
+ Недоверенные образы (другой registry, другой базовый образ)

Риски реестров

+ Старые образы (не поддерживаются вендором)
+ Контроль целостности образов

Риски оркестратора

+ Неограниченный административный доступ
+ Плохое разграничение связей между контейнерами
+ Некорректная конфигурация оркестратора

Риски compliance

+ Нарушения международных стандартов PCI DSS, NIST и других
+ Нарушения требований регуляторов (КИИ/ГИС)
+ Ошибки при конфигурации кластеров и контейнеров

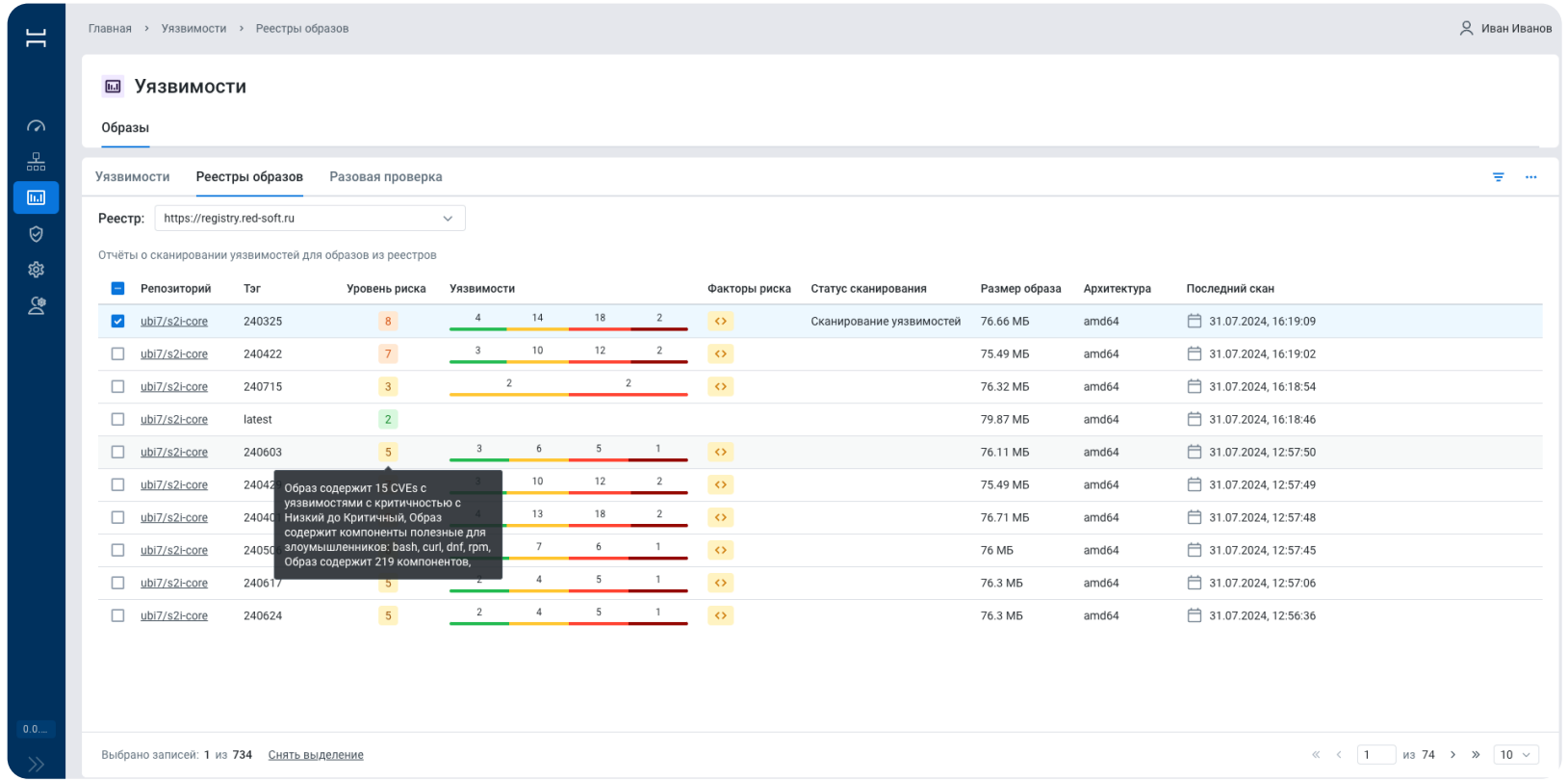
Риски ОС хоста

+ ОС избыточна для запуска контейнеров
+ Уязвимости в компонентах ОС, которые могут влиять на работу приложения
+ Некорректное использование пользовательских доступов
+ Изменения в файловой системе хоста

Сканирование образов контейнеров

Купол

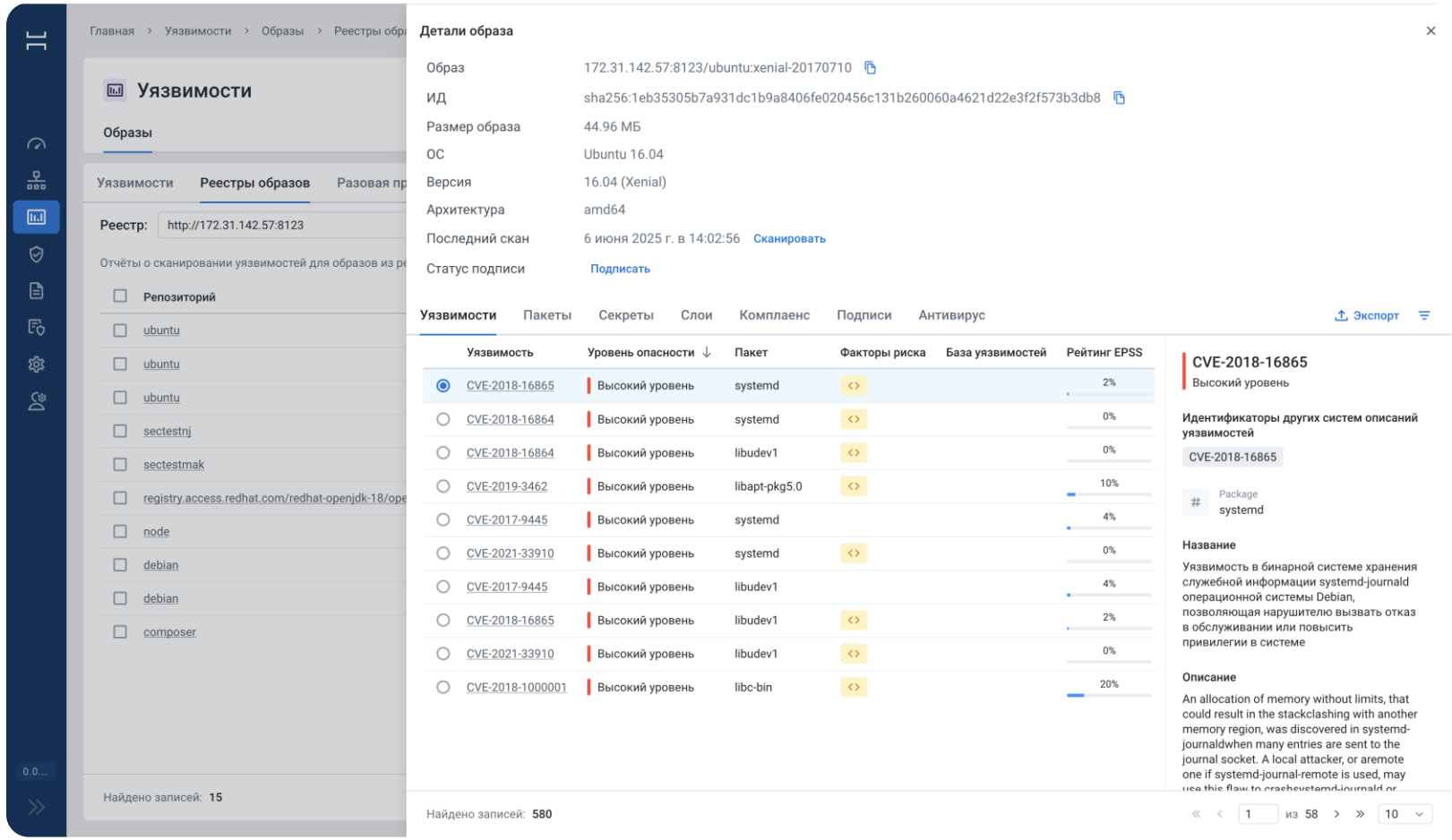
- \+ Сканирование реестров образов
- \+ Оценка риска работы с образом
- \+ Поиск на наличие эксплойтов, EOL и трендовых уязвимостей
- \+ Выгрузка отчётов CSV
- \+ Формирование SBOM (SPDX, CycloneDX)



Детальная информация по сканированию образов

Купол

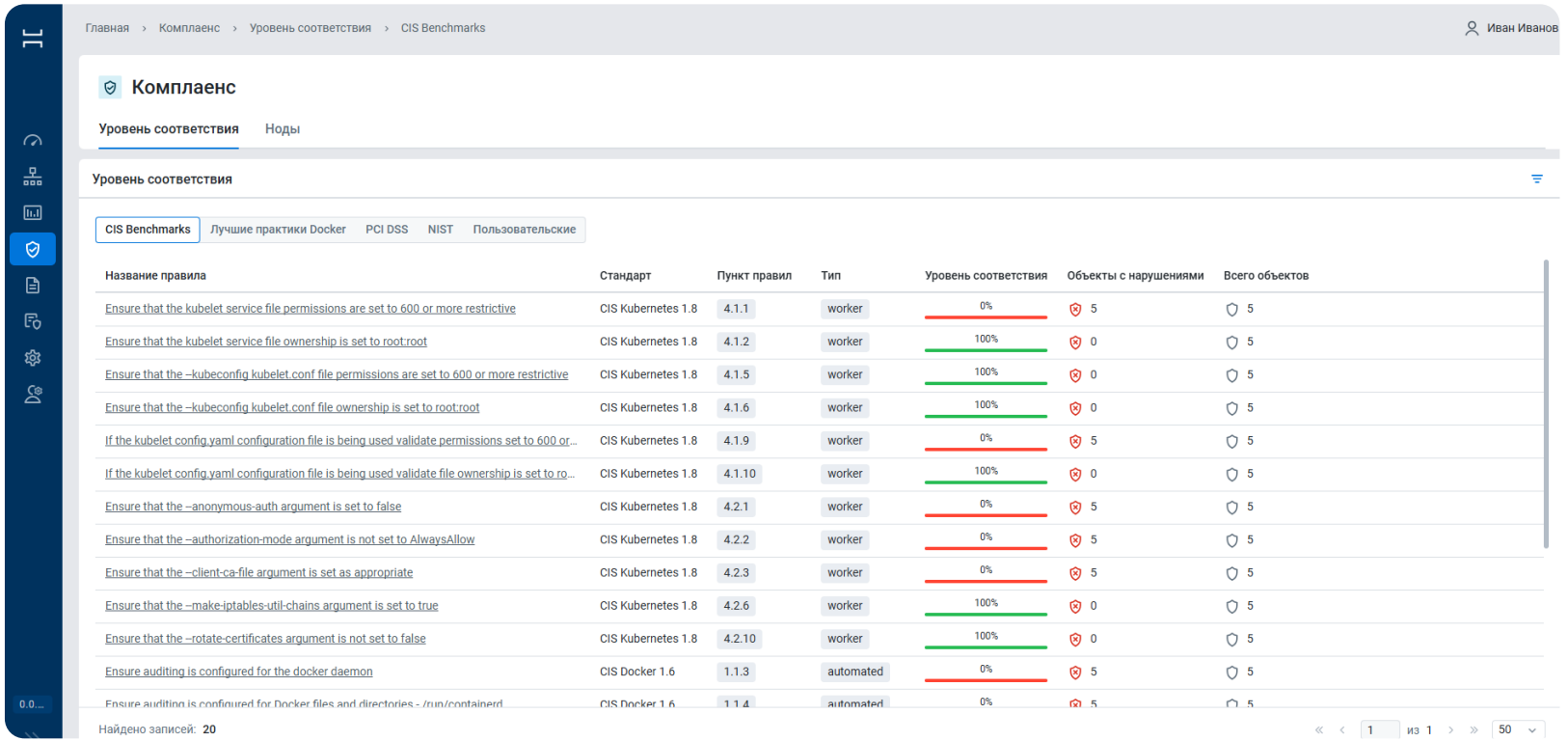
- + Сканирование образов по 17 базам данных уязвимостей (международные, отечественные, базы вендоров)
- + Поддержка образов на основе отечественных ОС
- + Поиск на наличие секретов по преднастроенным и пользовательским правилам
- + Проверка подписи образов
- + Механизмы принятия рисков
- + Проверка образов на вирусы



Проверка на соответствие стандартам

Купол

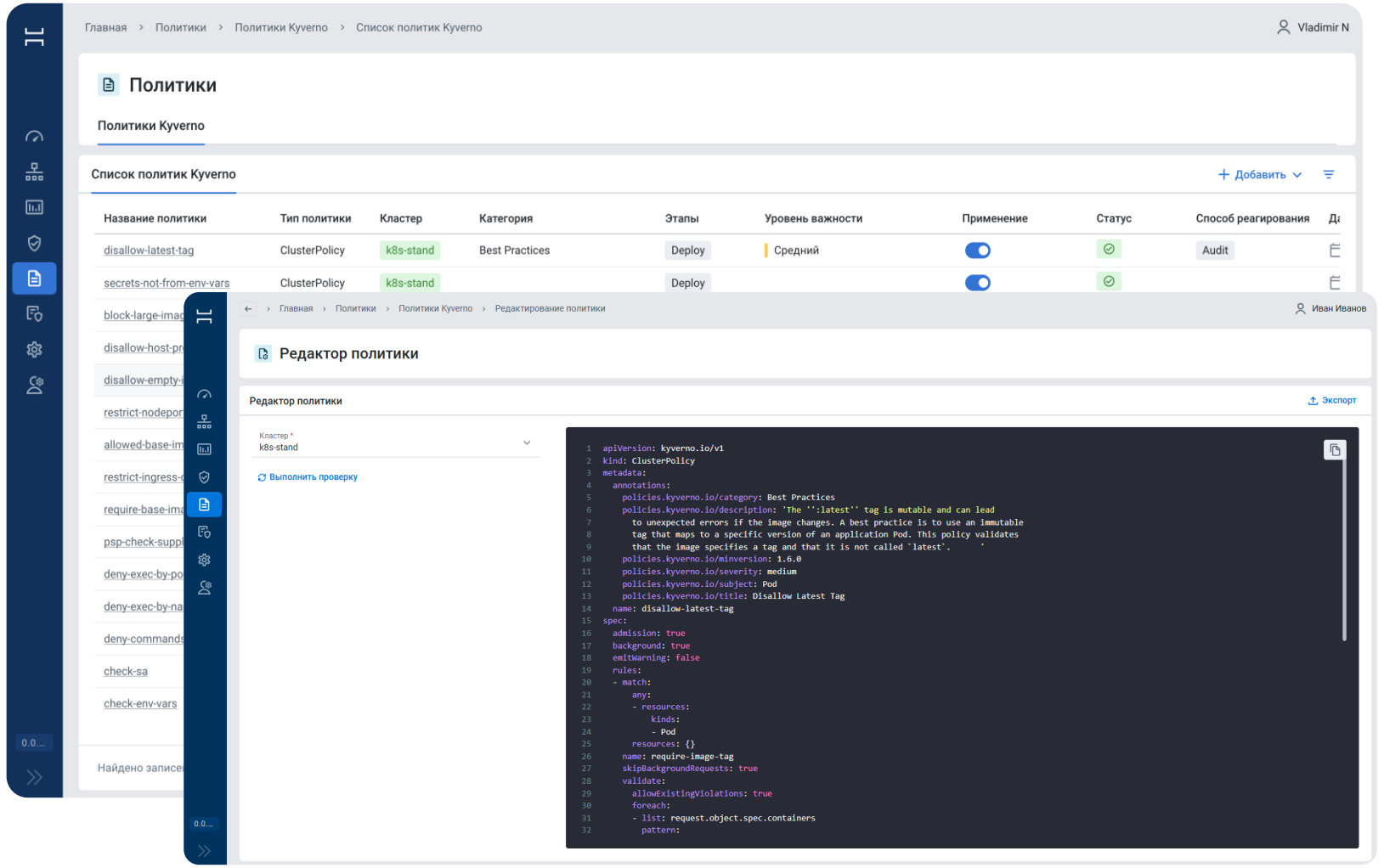
- \+ Проверка на соответствие стандартам CIS K8S
- \+ Проверка на соответствие стандартам CIS Docker, CIS Kubernetes, PCI DSS, NIST
- \+ Возможность создавать пользовательские правила



Политики Kyverno

Купол

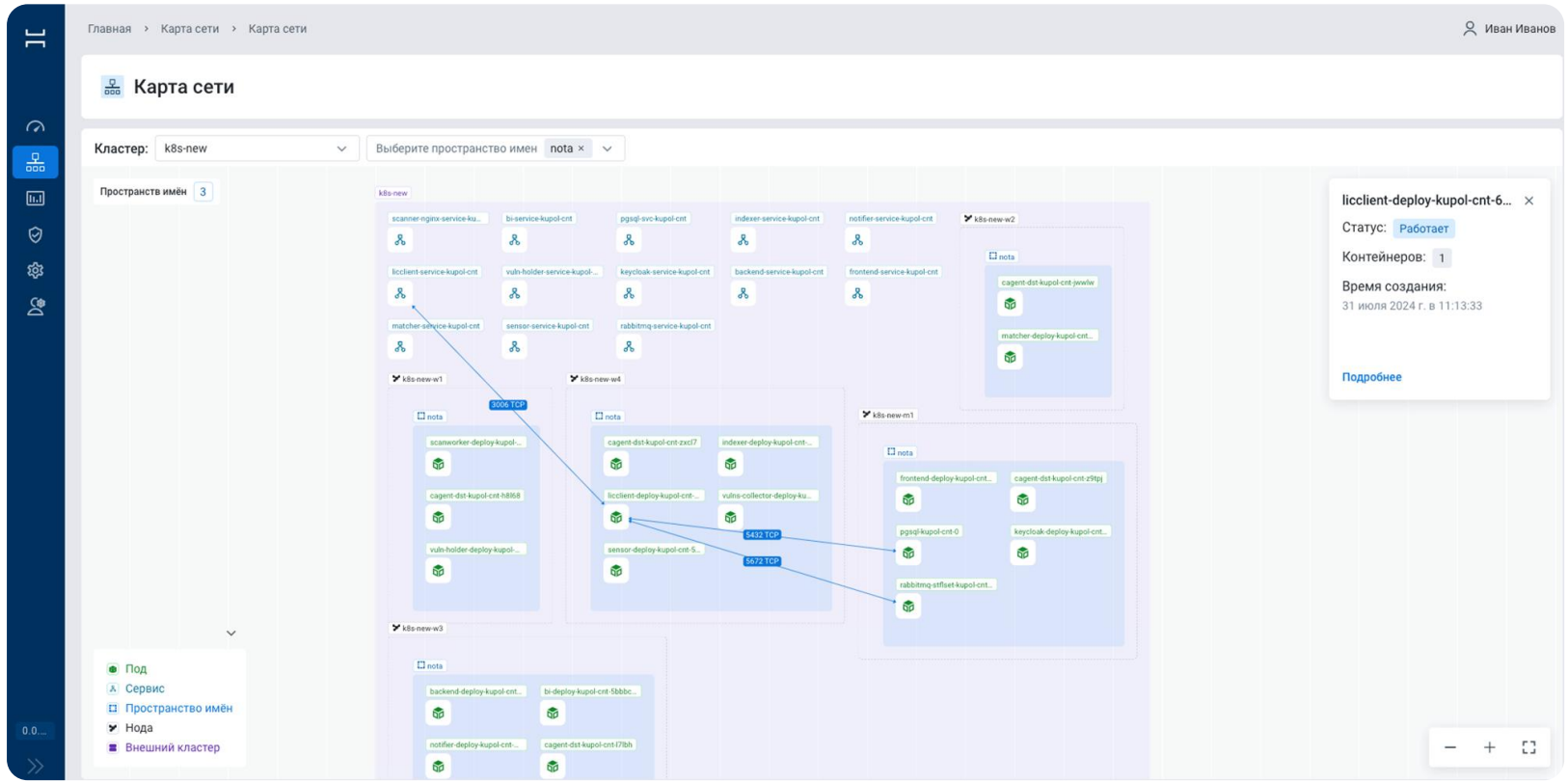
- Пользовательский интерфейс (UI) для просмотра, редактирования, применения и удаления политик Kyverno из кластера
- Валидация политики Kyverno перед применением в кластер
- Пакетная загрузка yaml-манифестов политик
- Отображение статуса актуального применения политики в кластере
- Экспорт политик в виде yaml-манифестов



Карта сети

Купол

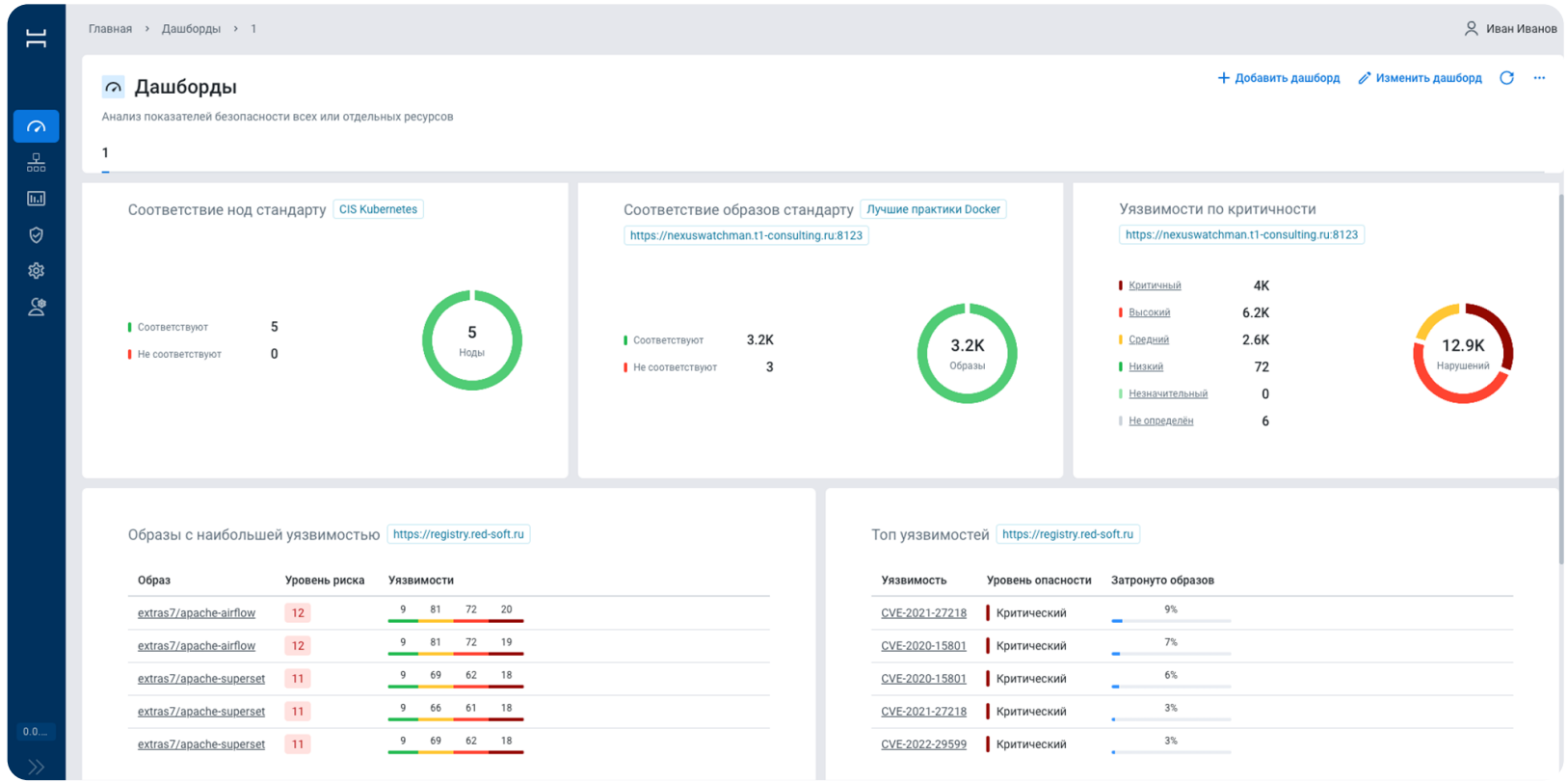
+ Визуализация взаимодействия компонентов кластера
+ Визуализация трафика сетевых соединений



Дашборды

Купол

Гибкая настройка пользовательских дашбордов по результатам сканирования на наличие уязвимостей и выявленным несоответствиям стандартам



Спасибо за внимание

Андрей Конорев
Владелец продукта Купол.Контейнеры