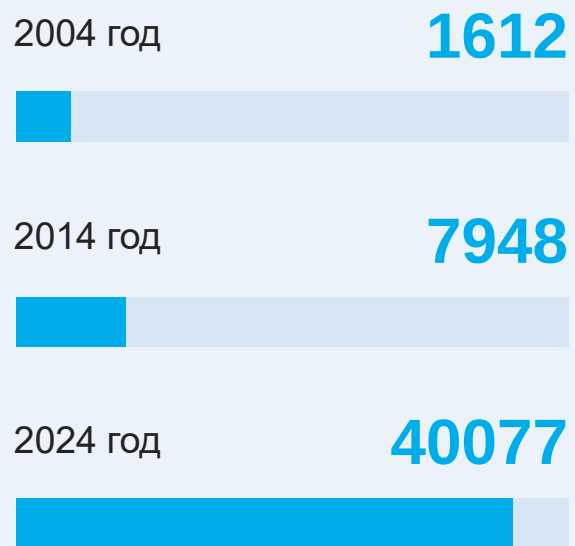


От образа до продакшна: как управлять рисками в контейнерной среде

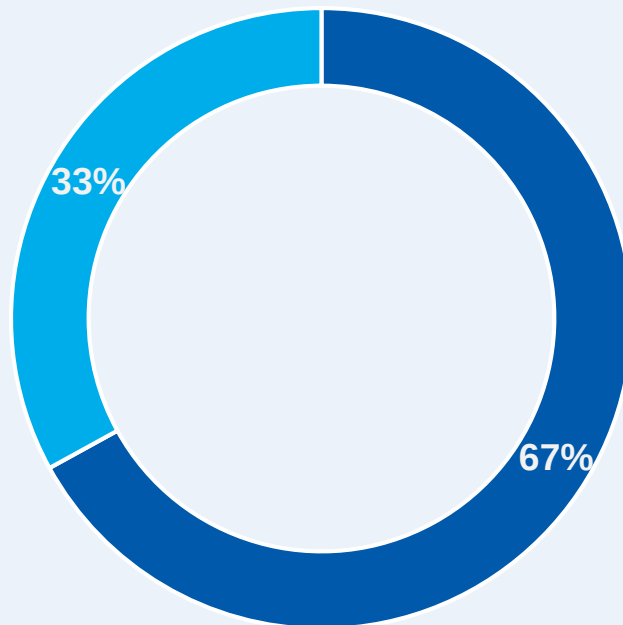


Тренды по безопасности контейнеризации

Рост количества угроз безопасности



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



■ Да ■ Нет

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

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

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

Главная > Уязвимости > Реестры образов

Иван Иванов

Уязвимости

Образы

Уязвимости | **Реестры образов** | Разовая проверка

Реестр:

Отчёты о сканировании уязвимостей для образов из реестров

Репозиторий	Тэг	Уровень риска	Уязвимости	Факторы риска	Статус сканирования	Размер образа	Архитектура	Последний скан
☒ ubi7/s2l-core	240325	8	4 14 18 2	<>	Сканирование уязвимостей	76.66 МБ	amd64	31.07.2024, 16:19:09
☐ ubi7/s2l-core	240422	7	3 10 12 2	<>		75.49 МБ	amd64	31.07.2024, 16:19:02
☐ ubi7/s2l-core	240715	3	2 2	<>		76.32 МБ	amd64	31.07.2024, 16:18:54
☐ ubi7/s2l-core	latest	2				79.87 МБ	amd64	31.07.2024, 16:18:46
☐ ubi7/s2l-core	240603	5	3 6 5 1	<>		76.11 МБ	amd64	31.07.2024, 12:57:50
☐ ubi7/s2l-core	240422		10 12 2	<>		75.49 МБ	amd64	31.07.2024, 12:57:49
☐ ubi7/s2l-core	240403		13 18 2	<>		76.71 МБ	amd64	31.07.2024, 12:57:48
☐ ubi7/s2l-core	240503		7 6 1	<>		76 МБ	amd64	31.07.2024, 12:57:45
☐ ubi7/s2l-core	240617	5	4 5 1	<>		76.3 МБ	amd64	31.07.2024, 12:57:06
☐ ubi7/s2l-core	240624	5	2 4 5 1	<>		76.3 МБ	amd64	31.07.2024, 12:56:36

Образ содержит 15 CVEs с уязвимостями с критичностью с Низкий до Критичный, Образ содержит компоненты полезные для злоумышленников: bash, curl, dnf, rpm, Образ содержит 219 компонентов,

Выбрано записей: 1 из 734 [Снять выделение](#)

<< 1 из 74 >> 10

Детальная информация по сканированию образов

- + 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
- 

Главная > Уязвимости > Образы > Реестры образов

Уязвимости

Образы

Разовая пр

Реестр:

Отчёты о сканировании уязвимостей для образов из ре

☐ Репозиторий

☐ ubuntu

☐ ubuntu

☐ ubuntu

☐ sectestnj

☐ sectestmak

☐ registry.access.redhat.com/redhat-openjdk-18/openjdk18

☐ node

☐ debian

☐ debian

☐ composer

Найдено записей: 15

Детали образа

Образ: 172.31.142.57:8123/ubuntu:xenial-20170710

ИД: sha256:1eb35305b7a931dc1b9a8406fe020456c131b260060a4621d22e3f2f573b3db8

Размер образа: 44.96 МБ

ОС: Ubuntu 16.04

Версия: 16.04 (Xenial)

Архитектура: amd64

Последний скан: 6 июня 2025 г. в 14:02:56 [Сканировать](#)

Статус подписи: [Подписать](#)

Уязвимости

Пакеты

Секреты

Слои

Комплаенс

Подписи

Антивирус

[Экспорт](#)

Уязвимость	Уровень опасности ↓	Пакет	Факторы риска	База уязвимостей	Рейтинг EPSS
☒ CVE-2018-16865	Высокий уровень	systemd	<>		2%
☐ CVE-2018-16864	Высокий уровень	systemd	<>		0%
☐ CVE-2018-16864	Высокий уровень	libudev1	<>		0%
☐ CVE-2019-3462	Высокий уровень	libapt-pkg5.0	<>		10%
☐ CVE-2017-9445	Высокий уровень	systemd	<>		4%
☐ CVE-2021-33910	Высокий уровень	systemd	<>		0%
☐ CVE-2017-9445	Высокий уровень	libudev1	<>		4%
☐ CVE-2018-16865	Высокий уровень	libudev1	<>		2%
☐ CVE-2021-33910	Высокий уровень	libudev1	<>		0%
☐ CVE-2018-1000001	Высокий уровень	libc-bin	<>		20%

Найдено записей: 580

CVE-2018-16865

Высокий уровень

Идентификаторы других систем описаний уязвимостей

CVE-2018-16865

Package systemd

Название

Уязвимость в бинарной системе хранения служебной информации systemd-journald операционной системы Debian, позволяющая нарушителю вызвать отказ в обслуживании или повысить привилегии в системе

Описание

An allocation of memory without limits, that could result in the stackclashing with another memory region, was discovered in systemd-journaldwhen many entries are sent to the journal socket. A local attacker, or aremote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or

Проверка на соответствие стандартам

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



Главная > Комплаенс > Уровень соответствия > CIS Benchmarks

Иван Иванов

Комплаенс

Уровень соответствия Ноды

Уровень соответствия

CIS Benchmarks Лучшие практики Docker PCI DSS NIST Пользовательские

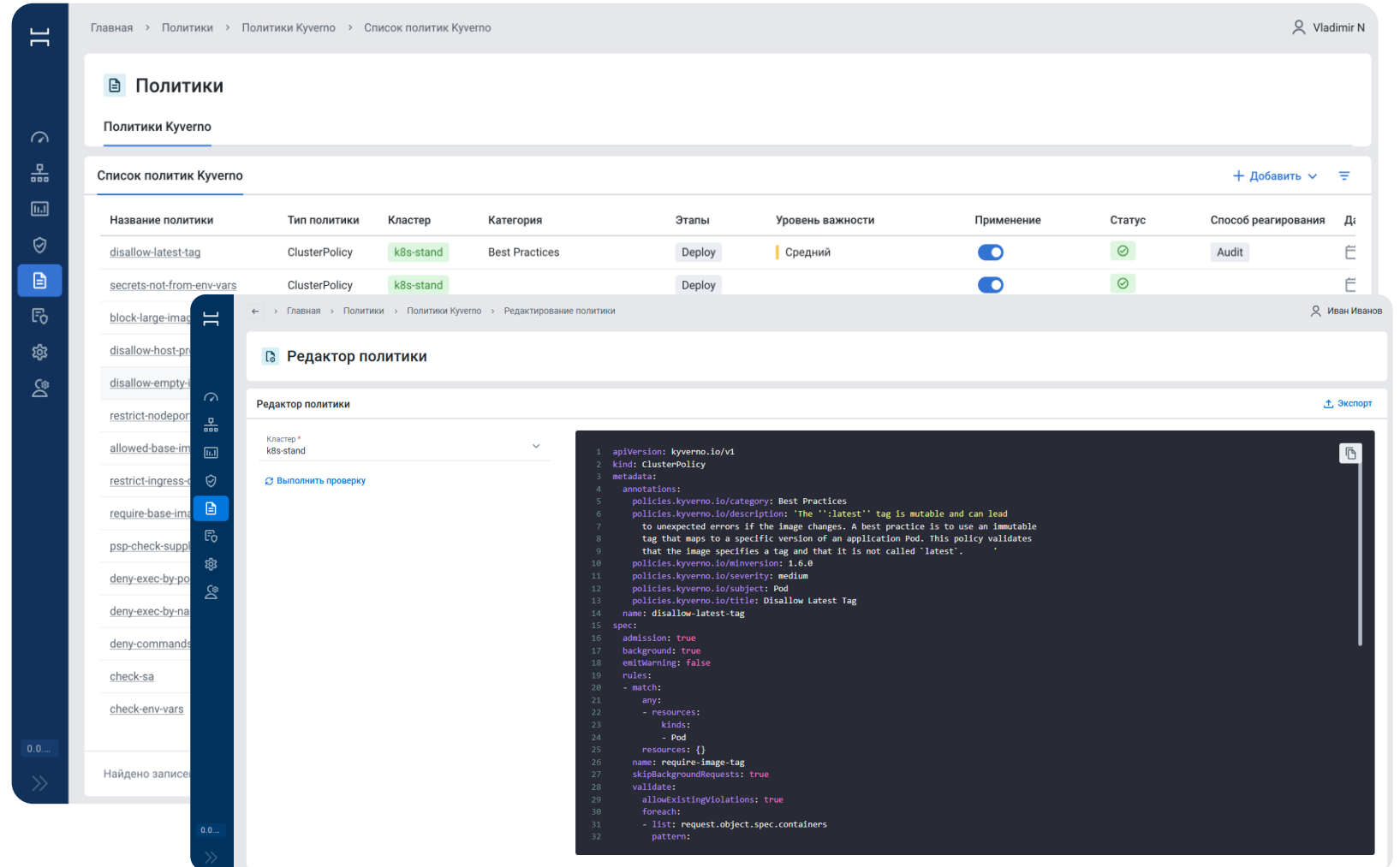
Название правила	Стандарт	Пункт правил	Тип	Уровень соответствия	Объекты с нарушениями	Всего объектов
Ensure that the kubelet service file permissions are set to 600 or more restrictive	CIS Kubernetes 1.8	4.1.1	worker	0%	5	5
Ensure that the kubelet service file ownership is set to root:root	CIS Kubernetes 1.8	4.1.2	worker	100%	0	5
Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive	CIS Kubernetes 1.8	4.1.5	worker	100%	0	5
Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root	CIS Kubernetes 1.8	4.1.6	worker	100%	0	5
If the kubelet config.yaml configuration file is being used validate permissions set to 600 or...	CIS Kubernetes 1.8	4.1.9	worker	0%	5	5
If the kubelet config.yaml configuration file is being used validate file ownership is set to ro...	CIS Kubernetes 1.8	4.1.10	worker	100%	0	5
Ensure that the --anonymous-auth argument is set to false	CIS Kubernetes 1.8	4.2.1	worker	0%	5	5
Ensure that the --authorization-mode argument is not set to AlwaysAllow	CIS Kubernetes 1.8	4.2.2	worker	0%	5	5
Ensure that the --client-ca-file argument is set as appropriate	CIS Kubernetes 1.8	4.2.3	worker	0%	5	5
Ensure that the --make-iptables-util-chains argument is set to true	CIS Kubernetes 1.8	4.2.6	worker	100%	0	5
Ensure that the --rotate-certificates argument is not set to false	CIS Kubernetes 1.8	4.2.10	worker	100%	0	5
Ensure auditing is configured for the docker daemon	CIS Docker 1.6	1.1.3	automated	0%	5	5
Ensure auditing is configured for Docker files and directories - /run/containers	CIS Docker 1.6	1.1.4	automated	0%	5	5

Найдено записей: 20

« < 1 из 1 > » 50

Политики Kyverno

- + 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

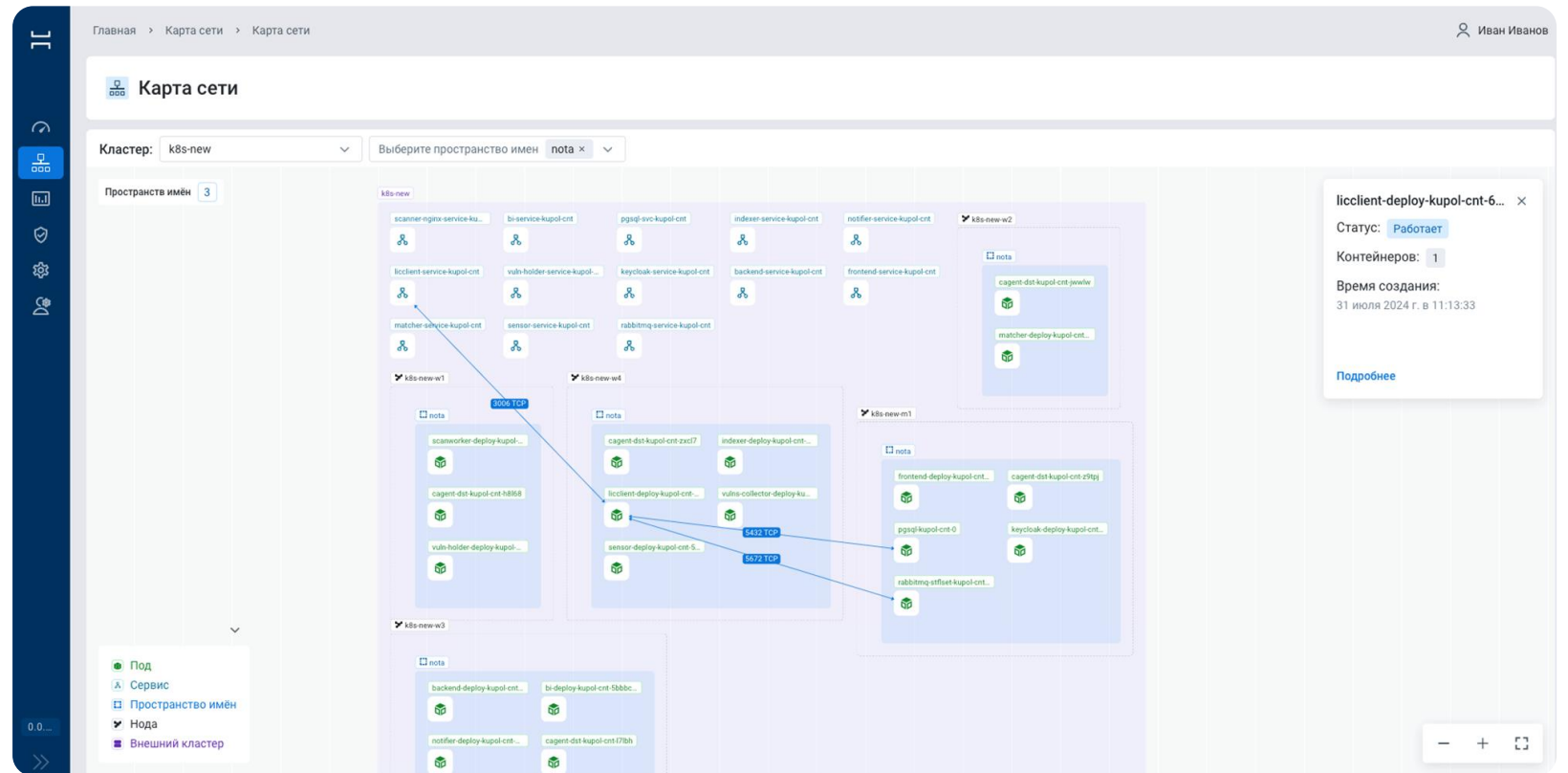


The screenshot displays the Kyverno web interface. The top navigation bar shows the user 'Vladimir N'. The main content area is titled 'Политики' (Policies) and shows a list of policies under the heading 'Список политик Kyverno'. The list includes columns for Name, Type, Cluster, Category, Stages, Importance Level, Application, Status, and Action. Two policies are visible: 'disallow-latest-tag' and 'secrets-not-from-env-vars', both of type 'ClusterPolicy' and associated with the 'k8s-stand' cluster. Below the list, the 'Редактор политики' (Policy Editor) is shown for the 'disallow-latest-tag' policy. It includes a dropdown for the cluster, a 'Выполнить проверку' (Run Check) button, and a code editor displaying the policy's YAML manifest.

```
1 apiVersion: kyverno.io/v1
2 kind: ClusterPolicy
3 metadata:
4   annotations:
5     policies.kyverno.io/category: Best Practices
6     policies.kyverno.io/description: 'The "latest" tag is mutable and can lead
7   to unexpected errors if the image changes. A best practice is to use an immutable
8   tag that maps to a specific version of an application pod. This policy validates
9   that the image specifies a tag and that it is not called "latest".'
10    policies.kyverno.io/minversion: 1.6.0
11    policies.kyverno.io/severity: medium
12    policies.kyverno.io/subject: Pod
13    policies.kyverno.io/title: Disallow Latest Tag
14  name: disallow-latest-tag
15  spec:
16    admission: true
17    background: true
18    emitWarning: false
19    rules:
20      - match:
21        any:
22          - resources:
23              kinds:
24                - Pod
25              resources: {}
26        name: require-image-tag
27        skipBackgroundRequests: true
28        validates:
29          allowExistingViolations: true
30          foreach:
31            - list: request.object.spec.containers
32              pattern:
```

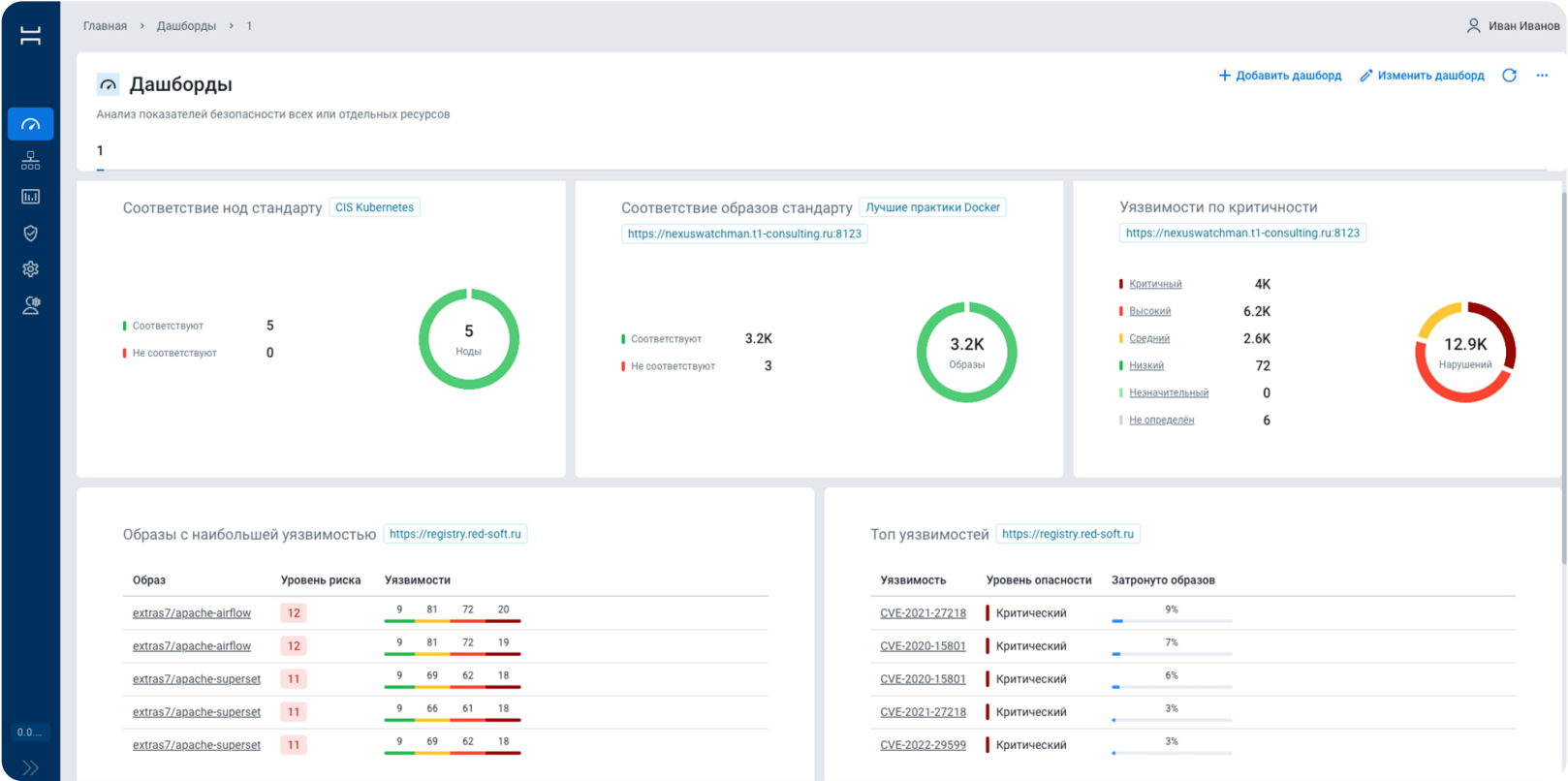
Карта сети

- + Визуализация взаимодействия компонентов кластера
- + Визуализация трафика сетевых соединений

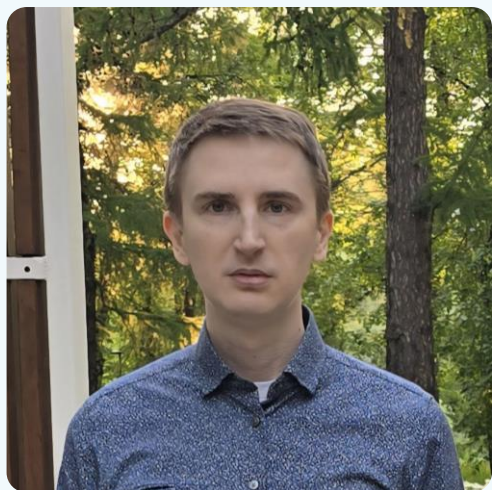


Дашборды

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



Спасибо за внимание



Андрей Конорев

Владелец продукта Купол.Контейнеры

