



Купол

Купол.Контейнеры

Система защиты контейнерных сред разработки

И С Т С | +IT



Основные проблемы защиты системы контейнеризации

Мониторинг и контроль

Как обеспечить мониторинг и контроль контейнеров и системы оркестрации?



Безопасность

Как обеспечить безопасность системы и анализировать уязвимости?



Контроль целостности

Как обеспечить контроль целостности образов и данных?



Визуализация и отчёты

Как визуализировать использование ресурсов и реализовать составление отчётности?



Купол.Контейнеры

Программный продукт по обеспечению безопасности контейнерных сред разработки

Ценность для клиента

- + Безопасность инфраструктуры с использованием контейнерных платформ
- + Оценка рисков на всех этапах работы с контейнерами
- + Повышение отказоустойчивости разрабатываемых и используемых приложений
- + Оптимизация использования ресурсов и выявление аномалий

Функции

Мониторинг состояния кластеров

- + Непрерывное сканирование состояния образов и конфигурационных файлов
- + Мониторинг и контроль запуска контейнеров в runtime



Карта компонентов кластера и отчётность

- + Построение карты компонентов кластера на основе данных встроенного сканера
- + Визуализация ресурсов и трафика кластера



Контроль целостности образов

- + Отслеживание изменений конфигураций
- + Контроль запуска процессов внутри контейнера в соответствии с политиками безопасности



Управление политиками безопасности контейнеров

- + Централизованное управление политиками всех кластеров
- + Создание и изменение собственных политик и использование преднастроенных политик



Управление уязвимостями

- + Проверка образов на наличие уязвимостей по международной базе уязвимостей
- + Встроенный механизм согласования принятия решений по каждой уязвимости
- + Классификация уязвимостей по влиянию на образы



Сценарии использования



Защита контейнерных сред разработки и приложений

Защите процесса разработки CI/CD построенного на контейнерной архитектуре с использованием оркестратора



Проверка соответствия требованиям и стандартам

Проверка системы на предмет соответствия политикам безопасности. Единая точка управления политиками кластеров



Организация защищенной сервисной инфраструктуры

Анализ уязвимостей и проверка на соответствие стандартам безопасности приложений и сервисов на базе контейнерной архитектуры



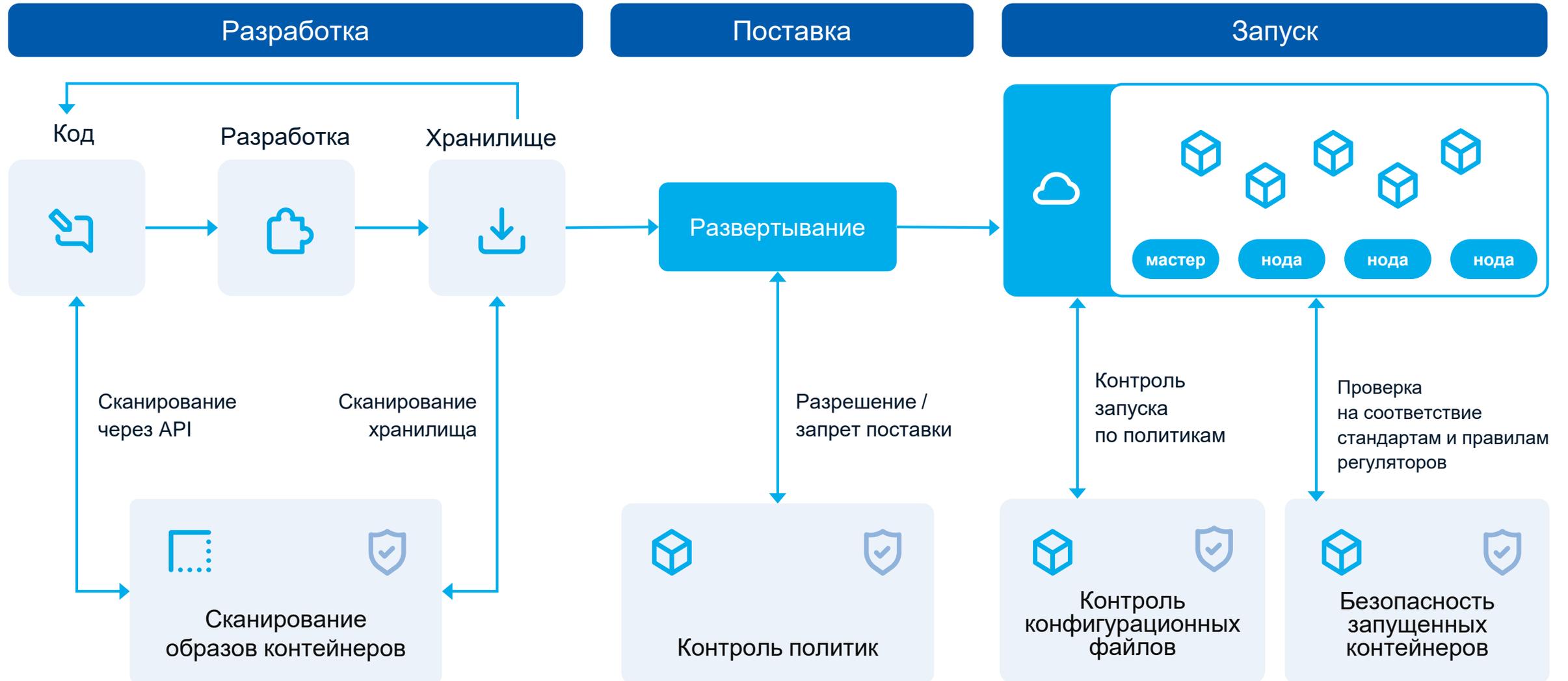
Оптимизация и визуализация работы контейнерной системы

Централизованный анализ работы системы, включая анализ использования ресурсов, наличия уязвимостей и создания отчетов

Защита системы контейнеризации



Схема внедрения



Сканирование образов контейнеров

Главная > Уязвимости > Образы > Реестры

Уязвимости

Образы

Реестры образов Разовая проверка

Реестр:

Отчёты о сканировании уязвимостей д

- Репозиторий
- k8s/nota.kupol/frontend
- k8s/nota.kupol/frontend
- k8s/nota.kupol/frontend
- ansible/ansible_rsync
- k8s/nota.kupol/frontend
- debian11_minimal/minimal_image_deb
- astra1.7/node_build_image_astra1.7_ar
- astra1.7/base_image_astra1.7_amd64
- k8s/nota.kupol/keycloak
- cicd/build_astra1.7_amd64

0.0...

Найдено записей: **1365**

Детали образа

Образ nexuswatchman.t1-consulting.ru:8123/astra1.7/base_image_astra1.7_amd64:0.0.0-240118141023.gd7381bb0-0

ИД [sha256:58ffe0be6923f1af8c9e148c6514f3338f6c0466318464ca8251aa54410c3902](#)

ОС Astra Linux

Последний скан 28 февраля 2024 г. в 10:24:37 [Сканировать](#)

Уязвимости Пакеты Секреты Слои ↑ Экспорт

Уровень опасности	Пакет	Уязвимость
● Критический уровень	libtcl8.6	BDU:2022-01774
○ Средний уровень	libip4tc0	CVE-2019-11360
○ Высокий уровень	gnupg-utils	BDU:2023-03850
○ Высокий уровень	libkrb5support0	BDU:2022-06933
○ Средний уровень	libssl1.1	BDU:2022-04284
○ Средний уровень	libssl1.1	CVE-2022-4304
○ Высокий уровень	libssl1.1	CVE-2022-4450
○ Высокий уровень	libssl1.1	BDU:2023-00675
○ Высокий уровень	libssl1.1	BDU:2023-03652
○ Высокий уровень	libssl1.1	BDU:2023-00665

Package libtcl8.6

Идентификатор BDU:2022-01774

Fix status 0:8.6.9+dfsg-2+ci202302131725+astra1

Описание

Рекомендации по устранению:
 - <https://wiki.astralinux.ru/astra-linux-se17-bulletin-20>: CVE: CVE-2021-35331
 ** DISPUTED ** In Tcl 8.6.11, a format string vulnerability allows code execution via a crafted file. NOTE: multiple third parties are affected by this finding.

Данные БДУ ФСТЭК
 Уязвимость компонента pmakehlr.c языка программирования C++ с недостаточной обработкой форматной строки. Эксплуататор может позволить нарушителю, действующему удаленно, конфиденциальным данным, нарушить их целостность при обслуживании с помощью специально созданных пакетов.

Вендор: Сообщество свободного программного обеспечения Open Source Software (OSS) "ИРБИТ"

Найдено записей: **749**

« < 1 из 75 > » 10 ▾

Детальная информация по сканированию образов

Главная > Уязвимости > Образы > Раз

Уязвимости

Образы

Реестры образов **Разовая проверка**

Отчёты о сканировании образов, добав

- Реестр
- nexuswatchman.t1-consulting.ru:8123
- 172.31.142.57:8123
- nexuswatchman.t1-consulting.ru:8123
- nexuswatchman.t1-consulting.ru:8123

0.0....

Найдено записей: 4

Детали образа

Образ nexuswatchman.t1-consulting.ru:8123/vasylii/astra:vuln3

ИД sha256:189c383f1a8dc26121c2e35edb5f574e7586379c664e868120552596db759c3c

ОС Astra Linux

Последний скан 28 февраля 2024 г. в 11:21:14 [Сканировать](#)

Уязвимости Пакеты **Секреты** Слои [Экспорт](#)

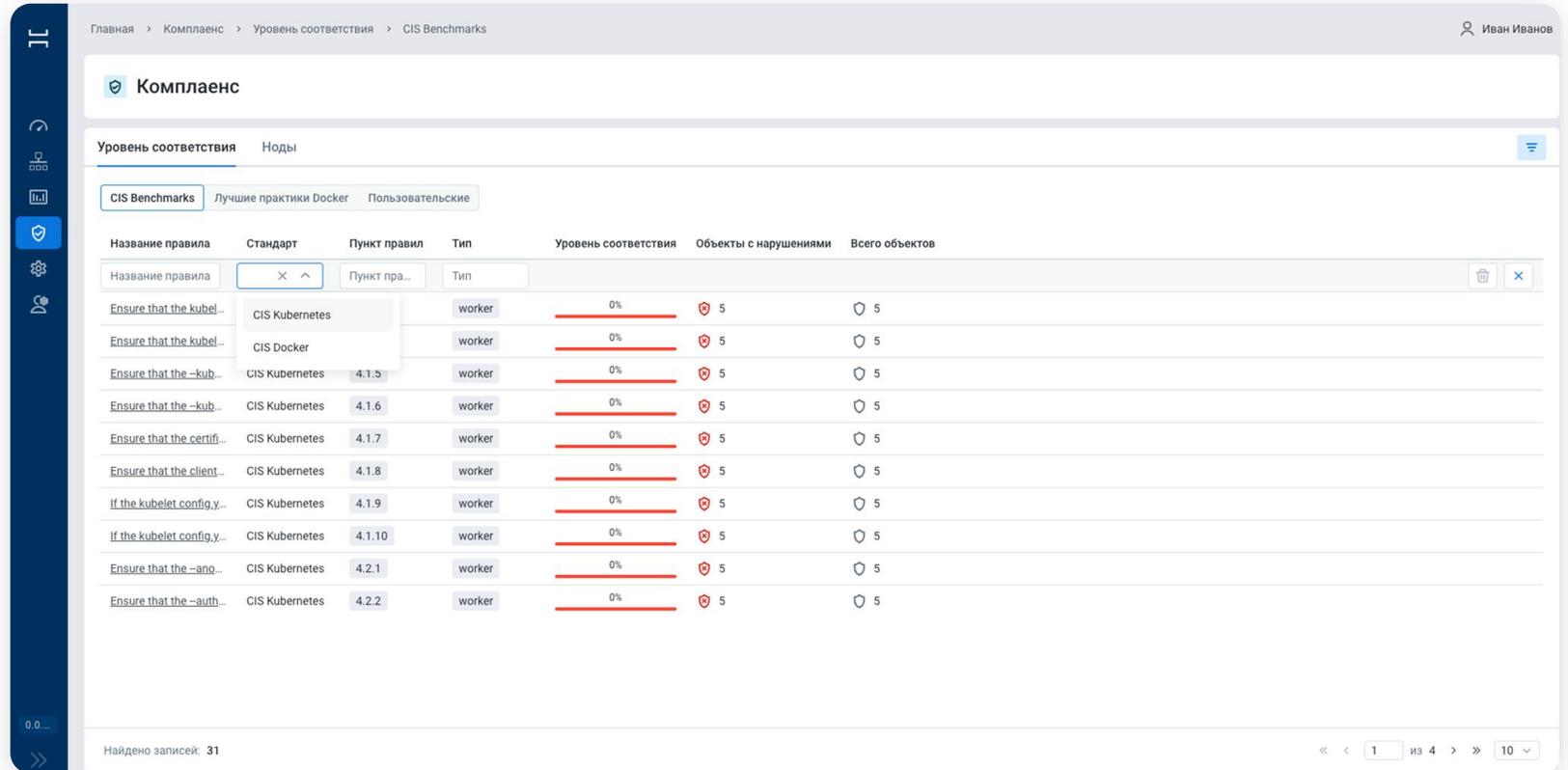
Тип	Правило	Уровень важности	Где нашли
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Cipher/_pycache_/test_pkcs1
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Cipher/test_pkcs1_15.py
Поиск по содержимому	AWS Session Token	Высокий	usr/lib/python3/dist-packages/Crypto/SelfTest/Hash/test_HMAC.py
Поиск по содержимому	Facebook Secret Key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Hash/test_MD4.py
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Signature/_pycache_/test_pkc
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Signature/test_pkcs1_15.py
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/_pycache_/ipa.cpython-3
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/ipa.py
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/network/a10/_pycache_
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/network/a10/a10.py

Найдено записей: 26

« < 1 из 3 > » 10 ▾

Проверка на соответствие стандартам

- Проверка на соответствие стандартам CIS K8S
- Проверка на соответствие стандартам CIS Docker
- Возможность создать пользовательские правила



Главная > Комплаенс > Уровень соответствия > CIS Benchmarks

Иван Иванов

Комплаенс

Уровень соответствия: Ноды

CIS Benchmarks
Лучшие практики Docker
Пользовательские

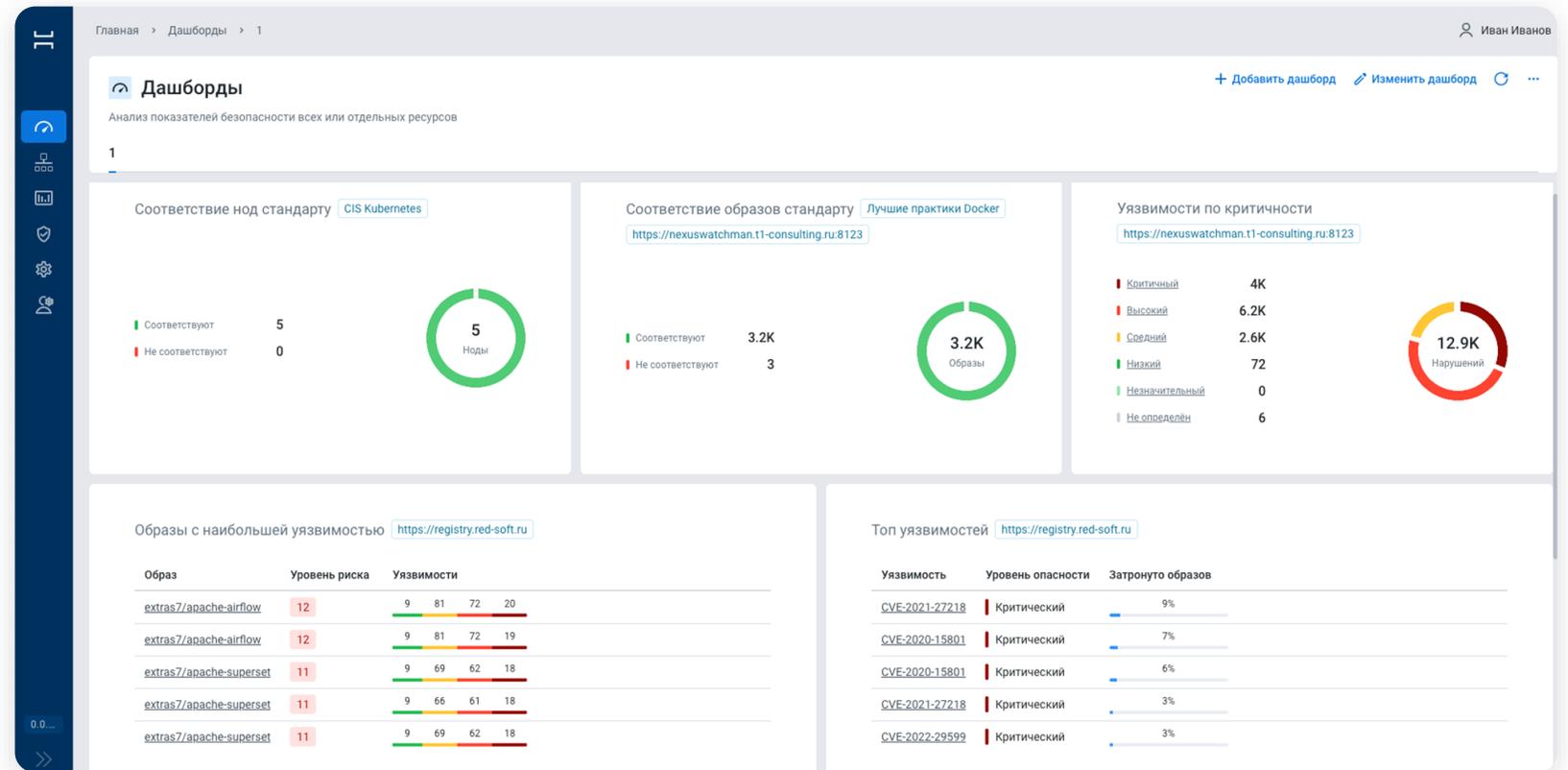
Название правила	Стандарт	Пункт правил	Тип	Уровень соответствия	Объекты с нарушениями	Всего объектов
Ensure that the kubel...	CIS Kubernetes		worker	0%	5	5
Ensure that the kubel...	CIS Docker		worker	0%	5	5
Ensure that the -kub...	CIS Kubernetes	4.1.5	worker	0%	5	5
Ensure that the -kub...	CIS Kubernetes	4.1.6	worker	0%	5	5
Ensure that the certifi...	CIS Kubernetes	4.1.7	worker	0%	5	5
Ensure that the client...	CIS Kubernetes	4.1.8	worker	0%	5	5
If the kubelet config.y...	CIS Kubernetes	4.1.9	worker	0%	5	5
If the kubelet config.y...	CIS Kubernetes	4.1.10	worker	0%	5	5
Ensure that the -ano...	CIS Kubernetes	4.2.1	worker	0%	5	5
Ensure that the -auth...	CIS Kubernetes	4.2.2	worker	0%	5	5

Найдено записей: 31

« < 1 из 4 > » 10

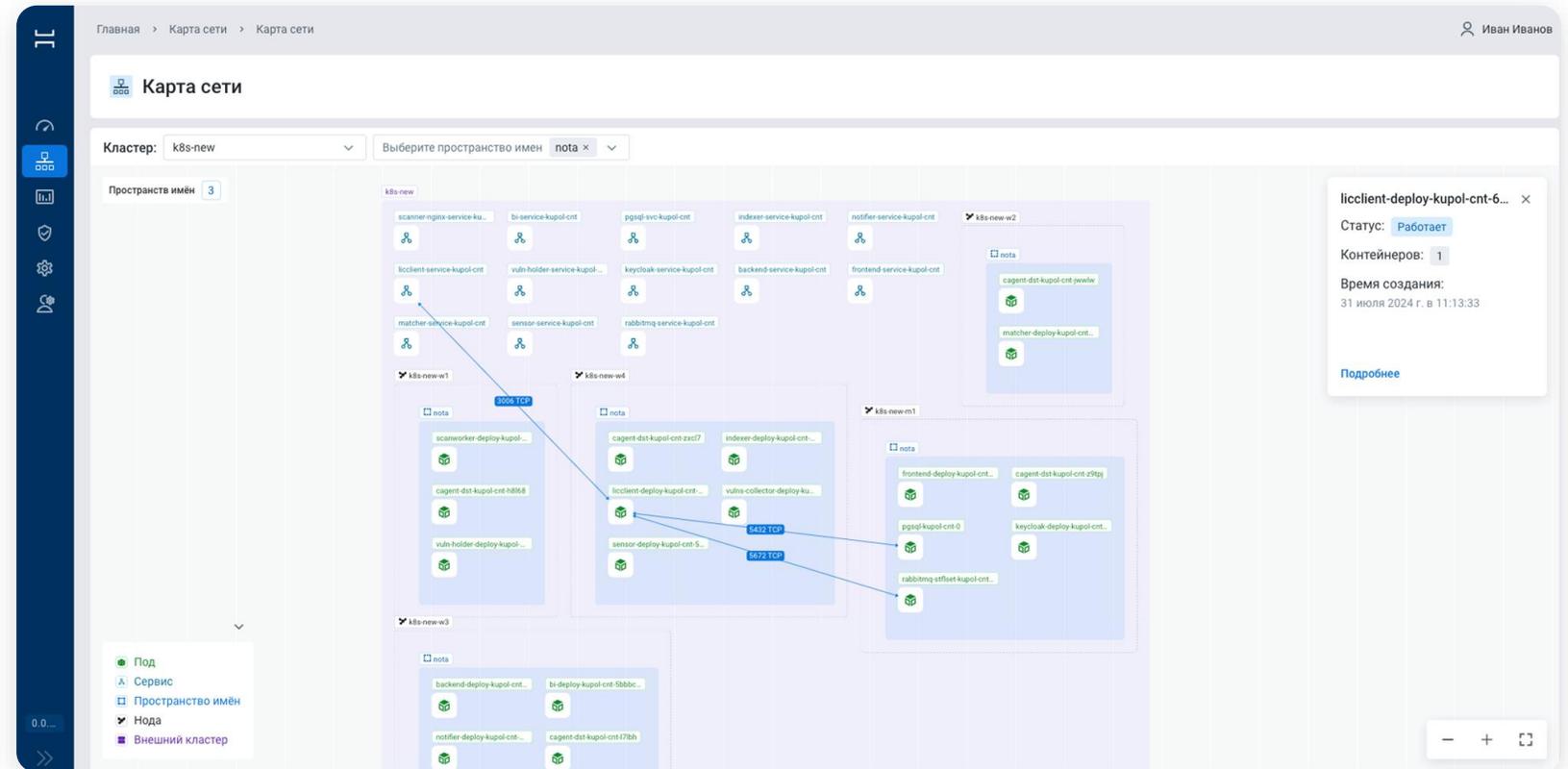
Дашборды

Гибкая настройка пользовательских дашбордов по результатам сканирования и выявленным несоответствиям стандартам



Карта сети

- Визуализация взаимодействия компонентов кластера
- Поддержка мультикластерности
- Визуализация трафика сетевых соединений





Купол

Спасибо за внимание

И С Т С | +IT

