

И С Т С | +IT

НОТА

20
25

ДЕНЬ

Синтез
ИННОВАЦИЙ

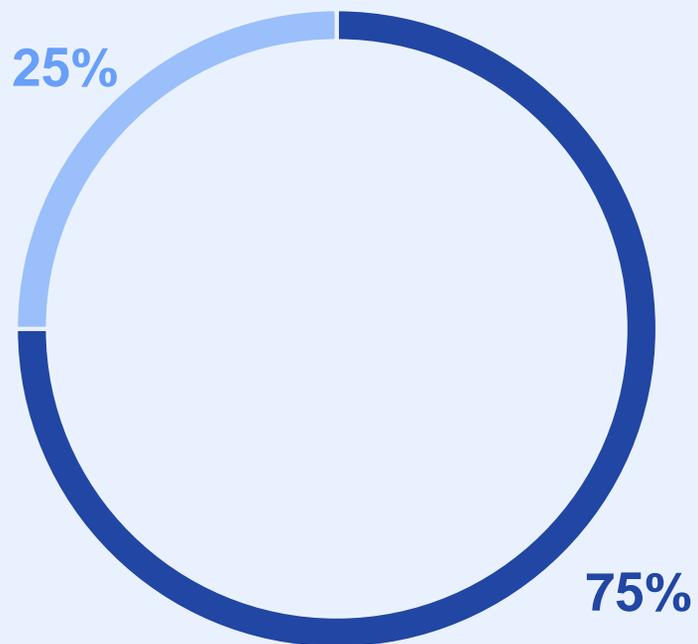
ITC

БЕЗОПАСНОСТЬ
КОНТЕЙНЕРНЫХ СРЕД:
ВЫЗОВЫ И РЕШЕНИЯ ДЛЯ ИТ

+ IT

СТАТИСТИКА ИМПОРТОЗАМЕЩЕНИЯ

Общий уровень импортозамещения

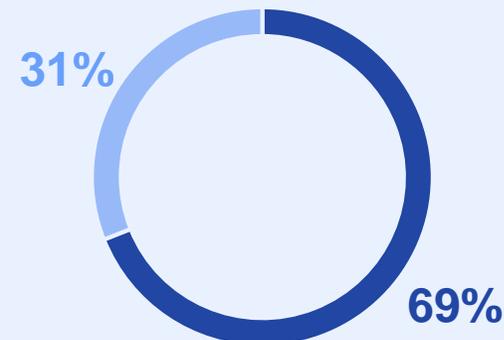


■ Зарубежные решения ■ Отечественные решения

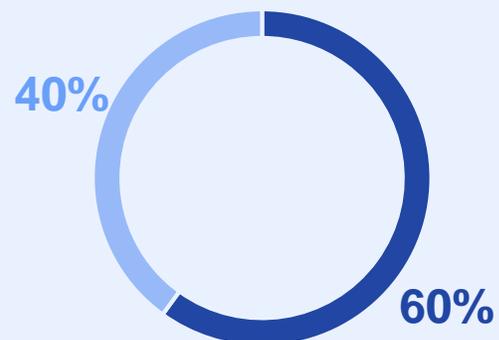
Госсектор



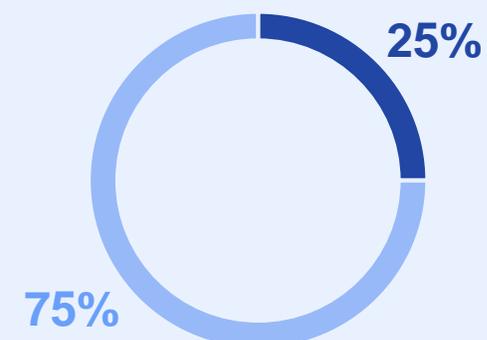
Промышленность



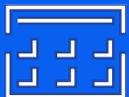
КИИ



Банковский сектор



ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ



Ограниченность ресурсов

- Высокая стоимость разработки
- Дороговизна сертификации
- Нехватка оборудования



Долгий цикл разработки

- Сложность создания новых продуктов
- Зависимость от внешних обновлений



Проблемы интеграции и совместимости

- Неполная замена зарубежных систем
- Привязанность к международным стандартам



Кадровый дефицит

- Нехватка специалистов
- Отток специалистов
- Недостаток образовательных программ

РИСКИ КОНТЕЙНЕРНЫХ СРЕД РАЗРАБОТКИ

Риски образов

- Уязвимости в образе
- Дефекты конфигурации
- Встроенное malware (вирусы, секреты и т. д.)
- Недоверенные образы



Риски реестров

- Небезопасные соединения
- Старые образы (не поддерживаются вендором)
- Контроль целостности образов



Риски оркестратора

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



Риски контейнеров

- Уязвимости в запущенном ПО
- Неограниченный сетевой доступ из контейнеров
- Небезопасная конфигурация контейнера
- Уязвимости в самом приложения



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	
<input checked="" type="checkbox"/>	ubi7/s2l-core	240325	8	4 14 18 2	<>	Сканирование уязвимостей	76.66 МБ	amd64	31.07.2024, 16:19:09
<input type="checkbox"/>	ubi7/s2l-core	240422	7	3 10 12 2	<>		75.49 МБ	amd64	31.07.2024, 16:19:02
<input type="checkbox"/>	ubi7/s2l-core	240715	3	2 2	<>		76.32 МБ	amd64	31.07.2024, 16:18:54
<input type="checkbox"/>	ubi7/s2l-core	latest	2		<>		79.87 МБ	amd64	31.07.2024, 16:18:46
<input type="checkbox"/>	ubi7/s2l-core	240603	5	3 6 5 1	<>		76.11 МБ	amd64	31.07.2024, 12:57:50
<input type="checkbox"/>	ubi7/s2l-core	24042	3	10 12 2	<>		75.49 МБ	amd64	31.07.2024, 12:57:49
<input type="checkbox"/>	ubi7/s2l-core	24040	3	13 18 2	<>		76.71 МБ	amd64	31.07.2024, 12:57:48
<input type="checkbox"/>	ubi7/s2l-core	24050	3	7 6 1	<>		76 МБ	amd64	31.07.2024, 12:57:45
<input type="checkbox"/>	ubi7/s2l-core	240617	5	2 4 5 1	<>		76.3 МБ	amd64	31.07.2024, 12:57:06
<input type="checkbox"/>	ubi7/s2l-core	240624	5	2 4 5 1	<>		76.3 МБ	amd64	31.07.2024, 12:56:36

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

« < 1 из 74 > » 10 ▾

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.

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 предустановленным и пользовательским правилам
- Проверка образа на соответствие стандартам CIS



The screenshot displays a web-based interface for vulnerability scanning. The main panel shows a table of vulnerabilities with columns for 'Уязвимость' (Vulnerability), 'Уровень опасности' (Risk Level), 'Пакет' (Package), and 'Факторы риска' (Risk Factors). The table lists several vulnerabilities, including BDU:2018-00463 (Medium risk) and several BDU:2019-00693 (Critical risk) and BDU:2020-01426 (High risk) entries.

The right-hand pane provides a detailed view of the selected vulnerability, BDU:2018-00463. It includes the following information:

- Образ (Image):** nexuswatchman.t1-consulting.ru:8123/vasylili/astra:vuln_astra_1
- ИД (ID):** sha256:ba9ff3eeac9a8e5ad745a2d34c500cdf137ae89164c3de7b4a75b4ee64fbcfaa
- Размер образа (Image Size):** 561.75 МБ
- ОС (OS):** Astra Linux
- Архитектура (Architecture):** amd64
- Последний скан (Last Scan):** 31 июля 2024 г. в 12:50:33

The detailed view also shows the package name 'libjpeg62-turbo' and a description of the vulnerability: 'Уязвимость компонентов jpostct и jquant1 библиотек для работы с изображениями libjpeg-turbo связана с ошибками разменовки указателей. Эксплуатация уязвимости может позволить нарушителю действующему удалённо, вызвать отказ в обслуживании при помощи специально сформированного JPEG-файла.'

ПРОВЕРКА НА СООТВЕТСТВИЕ СТАНДАРТАМ

- Проверка на соответствие стандартам CIS K8S
- Проверка на соответствие стандартам CIS Docker
- Возможность создавать 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 -autb...	CIS Kubernetes	4.2.2	worker	0%	5	5

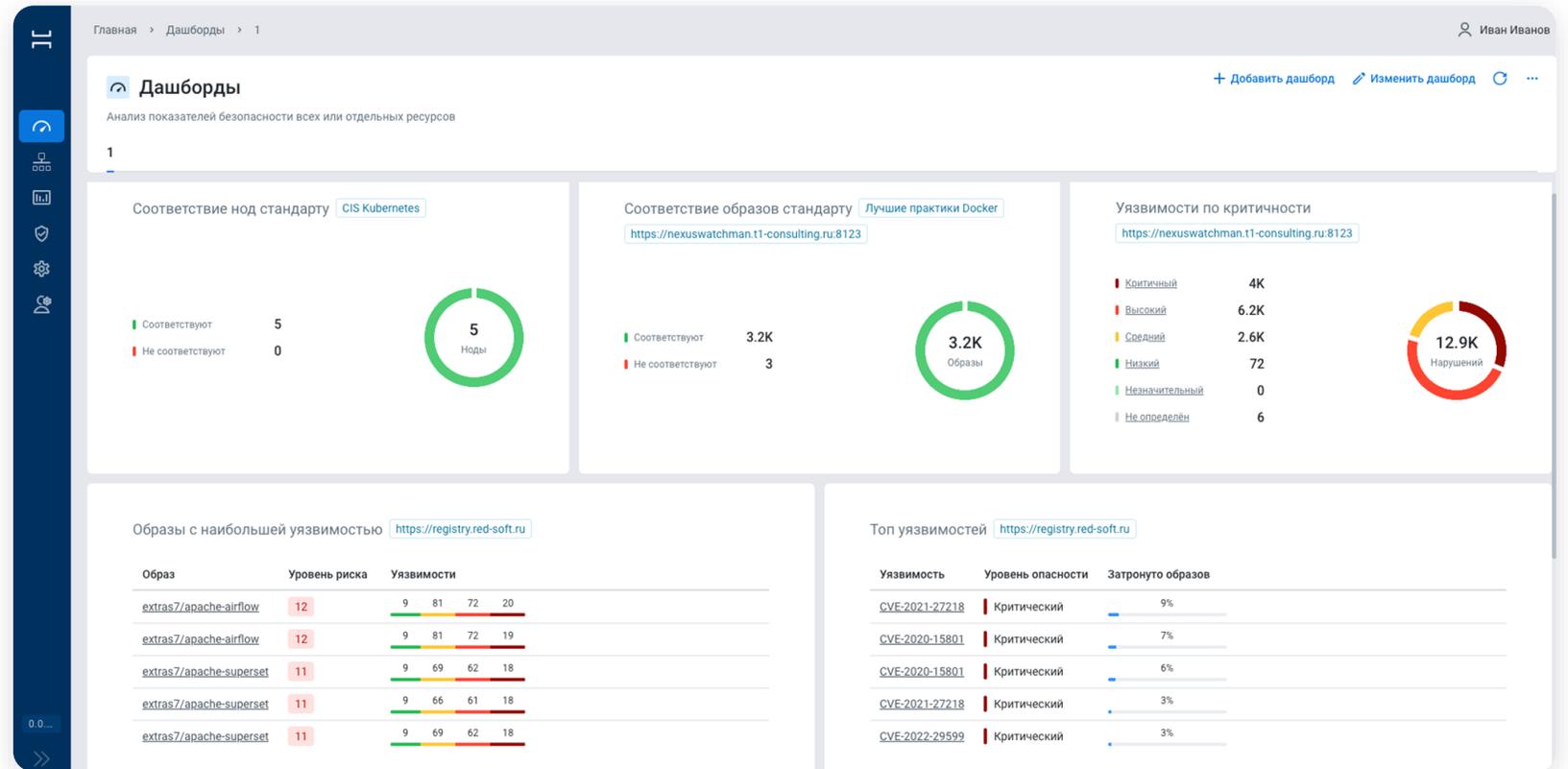
Найдено записей: 31

« < 1 из 4 > » 10 ▾

ДАШБОРДЫ



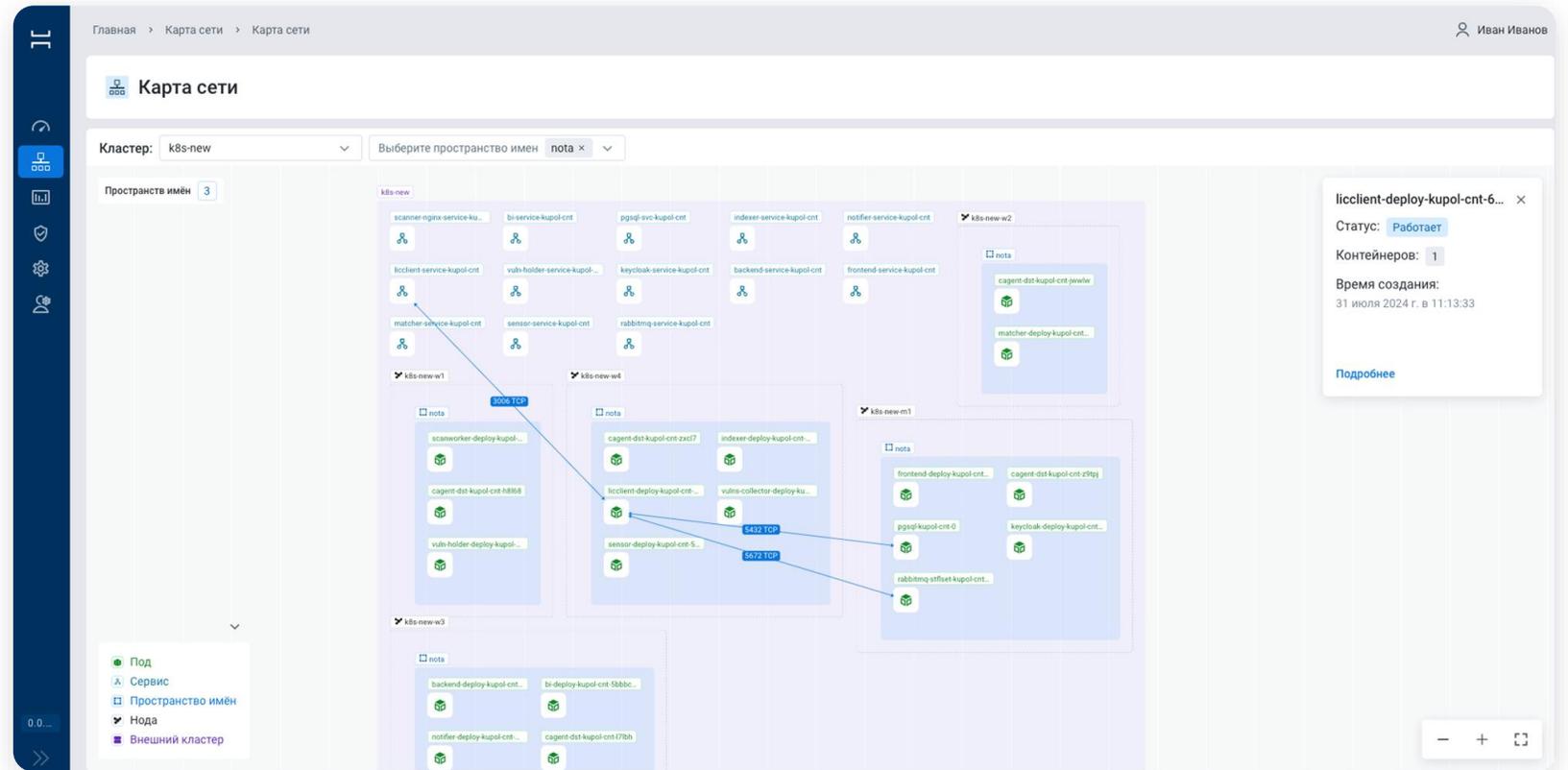
Гибкая настройка пользовательских дашбордов по результатам сканирования и выявленным несоответствиям стандартам



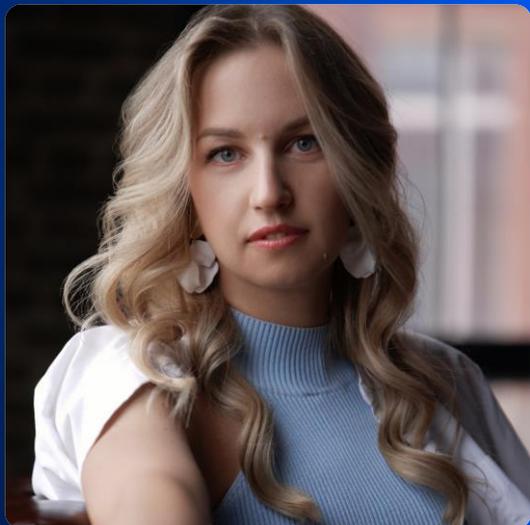
КАРТА СЕТИ



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



И С Т С | + | Т І



Мария Зализняк

Руководитель направления развития продуктов
по информационной безопасности КУПОЛ

СПАСИБО ЗА ВНИМАНИЕ