

И С Т О | +IT

НОТА

20
25

ДЕНЬ

Синтез
ИННОВАЦИЙ

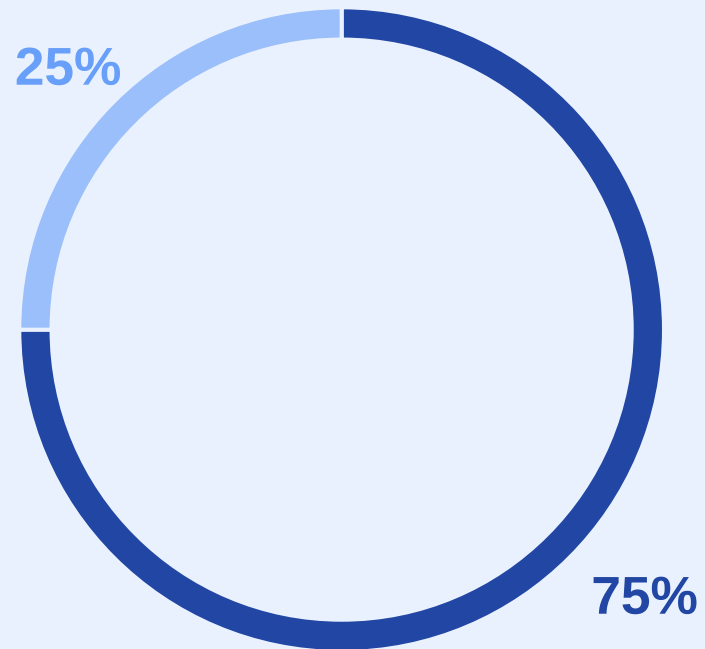


БЕЗОПАСНОСТЬ
КОНТЕЙНЕРНЫХ СРЕД:
ВЫЗОВЫ И РЕШЕНИЯ ДЛЯ ИТ



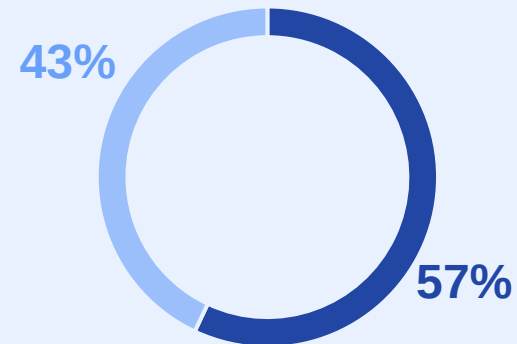
СТАТИСТИКА ИМПОРТОЗАМЕЩЕНИЯ

Общий уровень импортозамещения

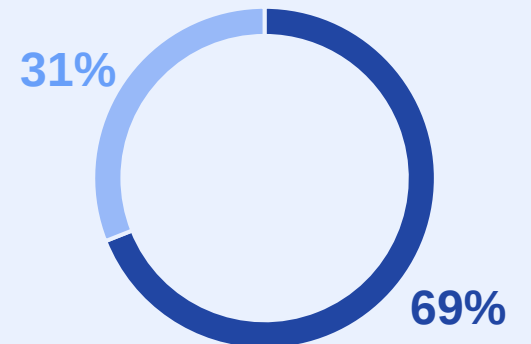


■ Зарубежные решения ■ Отечественные решения

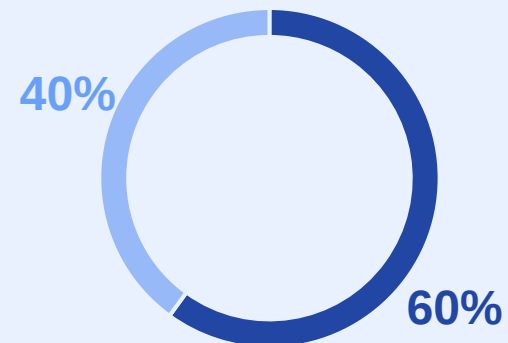
Госсектор



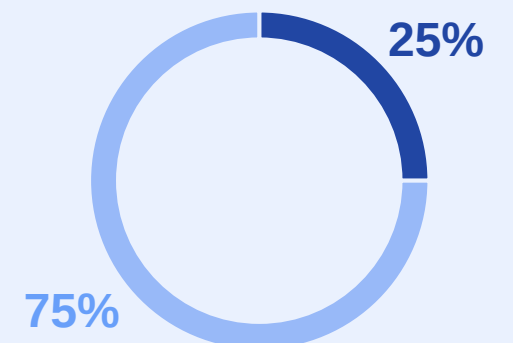
Промышленность



КИИ

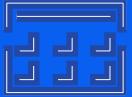


Банковский сектор



ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

≡ ☉ ☰ ☱ | +IT



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 приложении



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	24042	3	3 10 12 2	<>		75.49 МБ	amd64	31.07.2024, 12:57:49
☐ ubi7/s2l-core	24040	4	4 13 18 2	<>		76.71 МБ	amd64	31.07.2024, 12:57:48
☐ ubi7/s2l-core	24050	7	7 6 1	<>		76 МБ	amd64	31.07.2024, 12:57:45
☐ ubi7/s2l-core	240617	5	2 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

≡ ⊞ ⊞ ⊞ | +IT

- 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 the NexusWatchman application interface. The main window is titled 'Уязвимости' (Vulnerabilities) and shows a table of scan results. The table has columns for 'Репозиторий' (Repository), 'Тэг' (Tag), and 'Уровень риска' (Risk Level). The results are as follows:

Репозиторий	Тэг	Уровень риска
nexuswatchman.t1-consulting.ru:8123	vuln2	10
nexuswatchman.t1-consulting.ru:8123	vuln_astra_1	10
registry.red-soft.ru	ubi8/ubi-minimal	2

On the right side, the 'Детали образа' (Image Details) panel shows information about the scanned image: 'nexuswatchman.t1-consulting.ru:8123/vasylii/astra:vuln_astra_1'. Below this, the 'Уязвимости' (Vulnerabilities) section lists several CVEs with their severity levels and associated packages. The 'BDBU:2018-00463' vulnerability is highlighted, showing a 'Средний уровень' (Medium level) of risk. The description of this vulnerability mentions a NULL Pointer Dereference in the libjpeg-turbo library.

ПРОВЕРКА НА СООТВЕТСТВИЕ СТАНДАРТАМ

≡ ⊞ ⊞ ⊞ | +IT

- 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

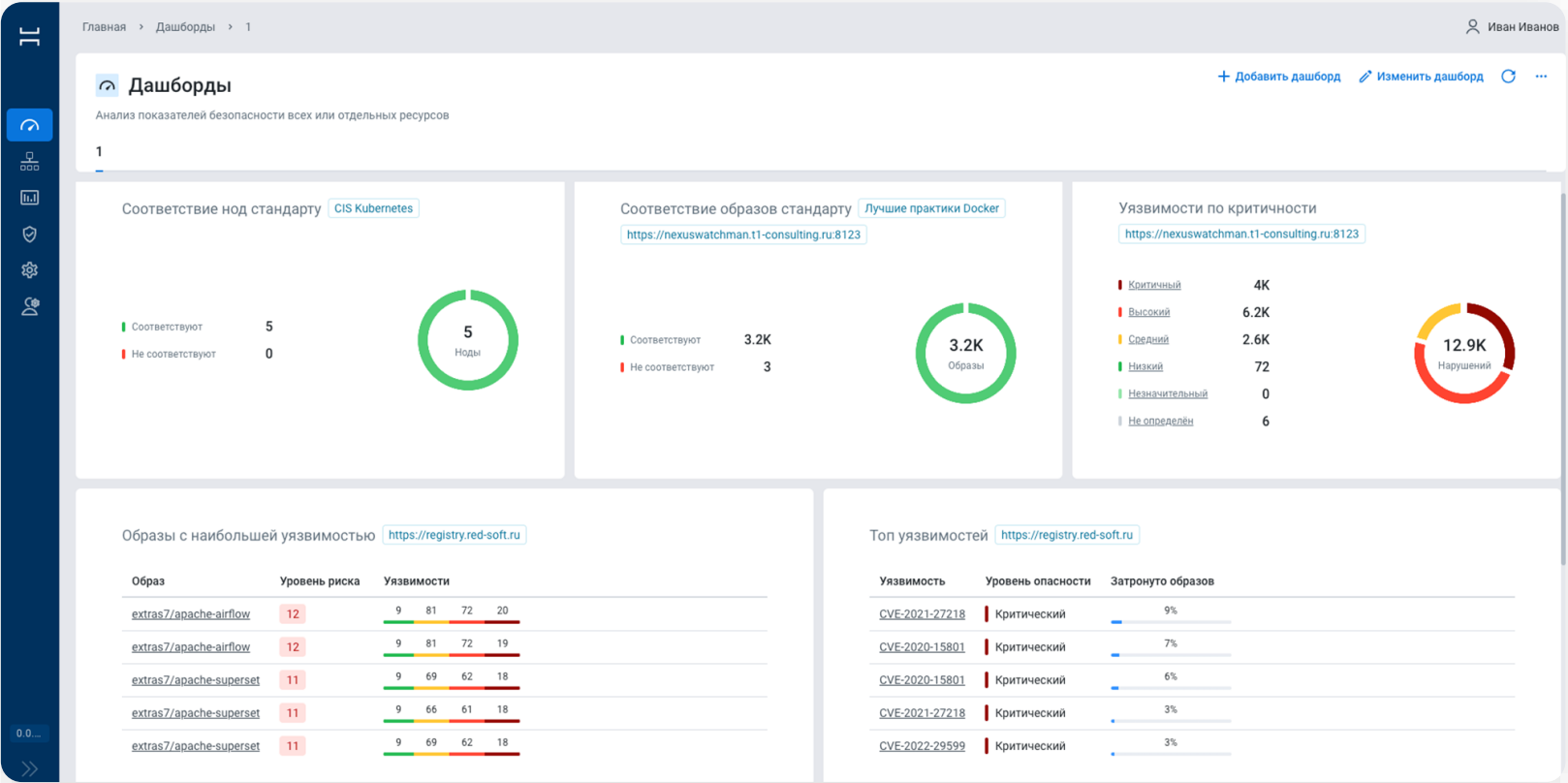
Название правила	Стандарт	Пункт правил	Тип	Уровень соответствия	Объекты с нарушениями	Всего объектов
Название правила	×	Пункт пра...	Тип			
Ensure that the kubel...	CIS Kubernetes		worker	0%	5	5
Ensure that the kubel...	CIS Docker		worker	0%	5	5
Ensure that the --kub...	CIS Kubernetes	4.1.5	worker	0%	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

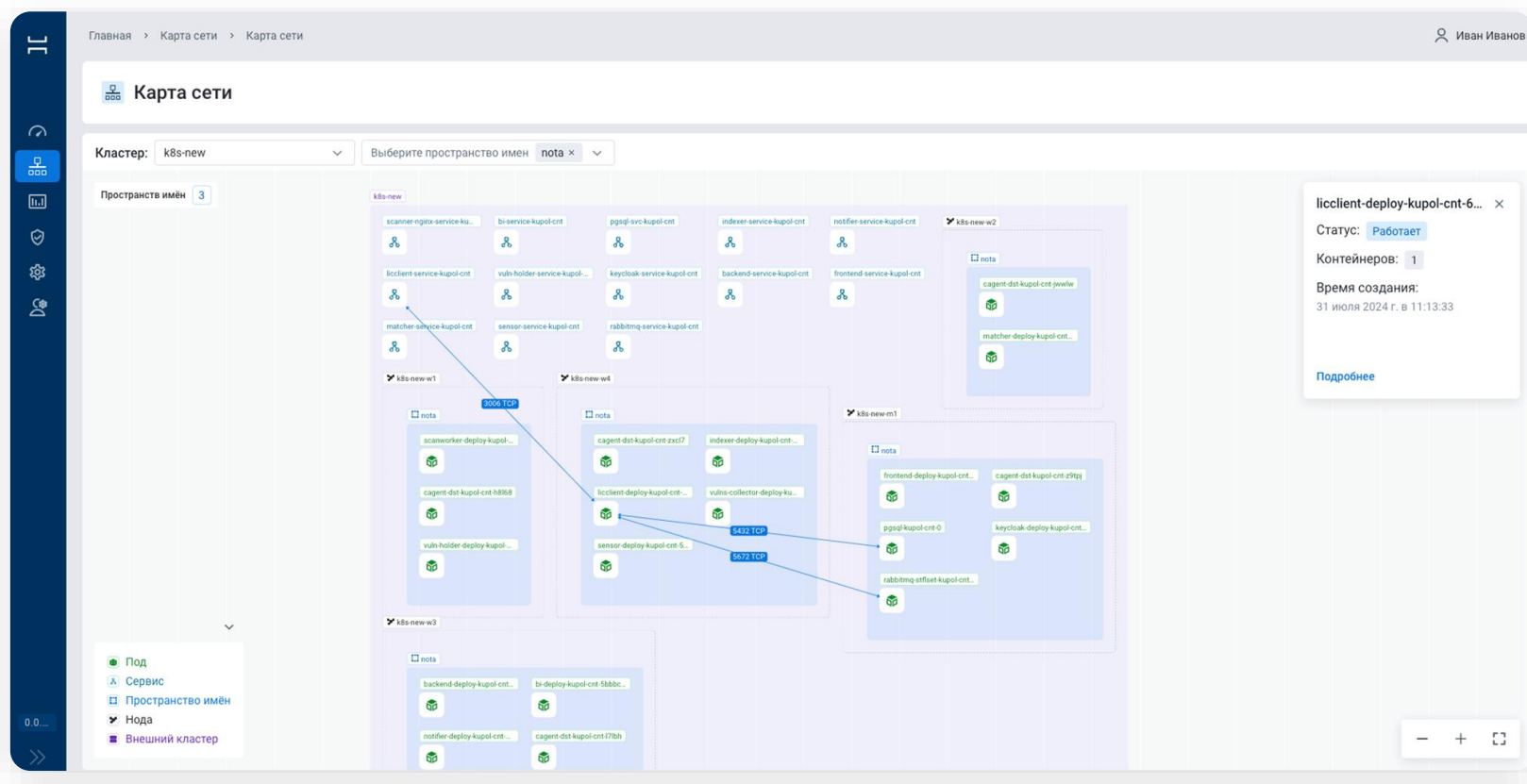
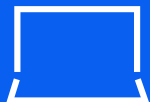
ДАШБОРДЫ

Гибкая настройка пользовательских дашбордов по результатам сканирования и выявленным несоответствиям стандартам



КАРТА СЕТИ

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



Н С Т С | + | Т І



Мария Зализняк

Руководитель направления развития продуктов
по информационной безопасности КУПОЛ

СПАСИБО ЗА ВНИМАНИЕ