Основы анализа СЗИ в контейнерном исполнении с помощью Luntry

Анатолий Карпенко

Luntry

whoami

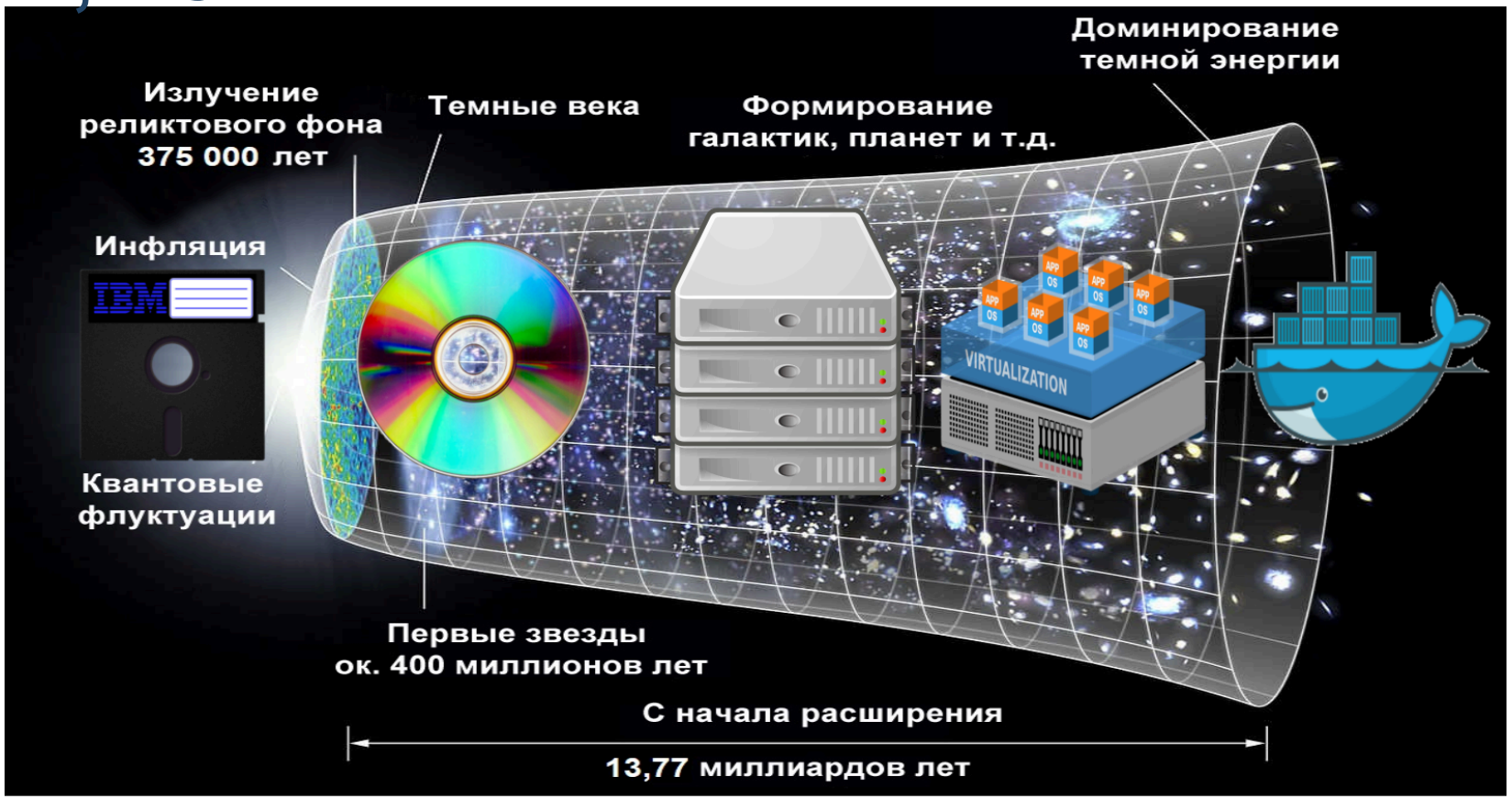
- Автоматизатор автоматизации в Luntry
- Любитель митапошных форматов: SPb Reliability Meetup, ITGM, TechTrain, DevOops, DEFCON'ы, B4CKSP4CE, DevOps40, SafeCode, БЕКОН
- Веду канал «Технологический Болт Генона»
- Рисую несмешные мемы

Спасибо

Андрей Слепых

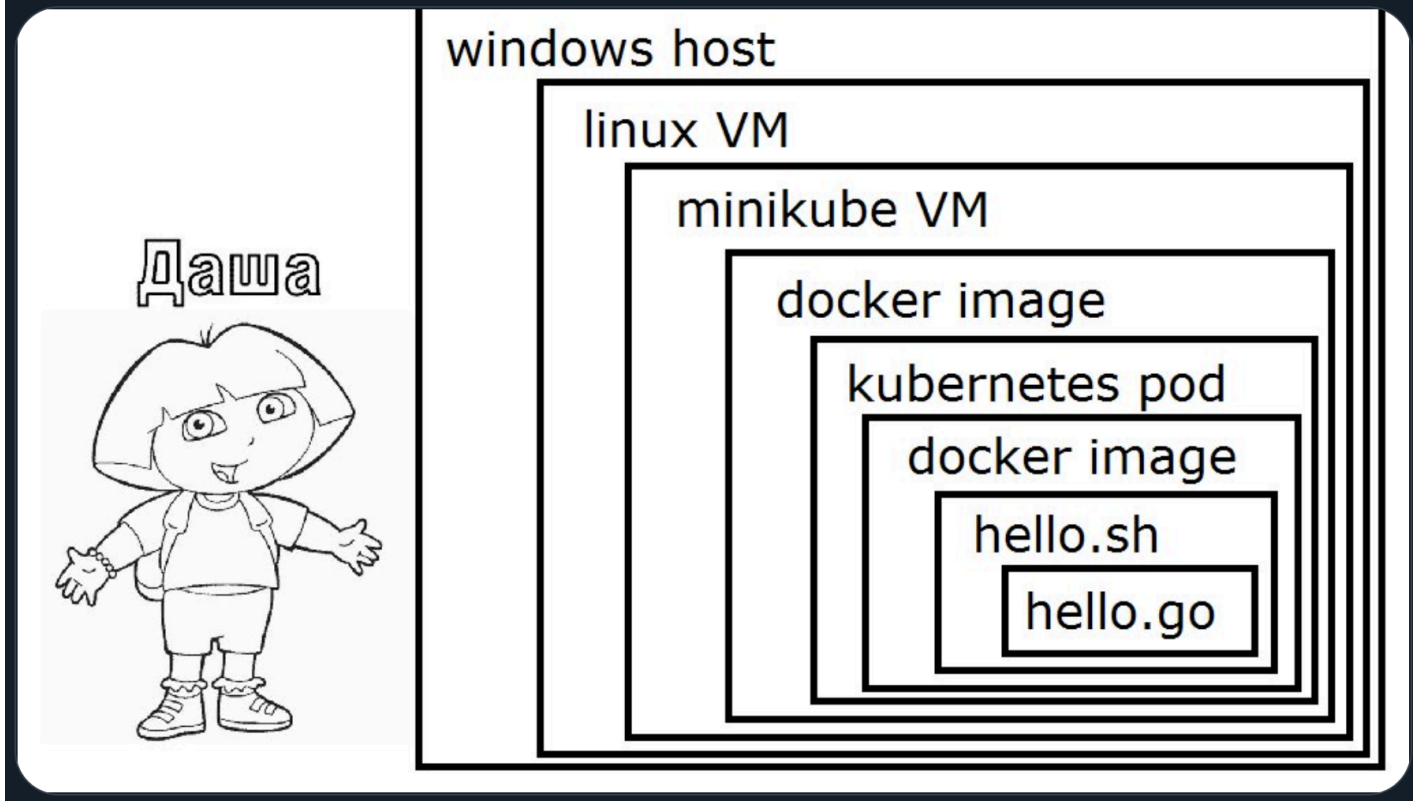
Эксперт центра внедрения и развития практик РБПО НТЦ "Фобос-НТ"

Мы шли, шли . . .

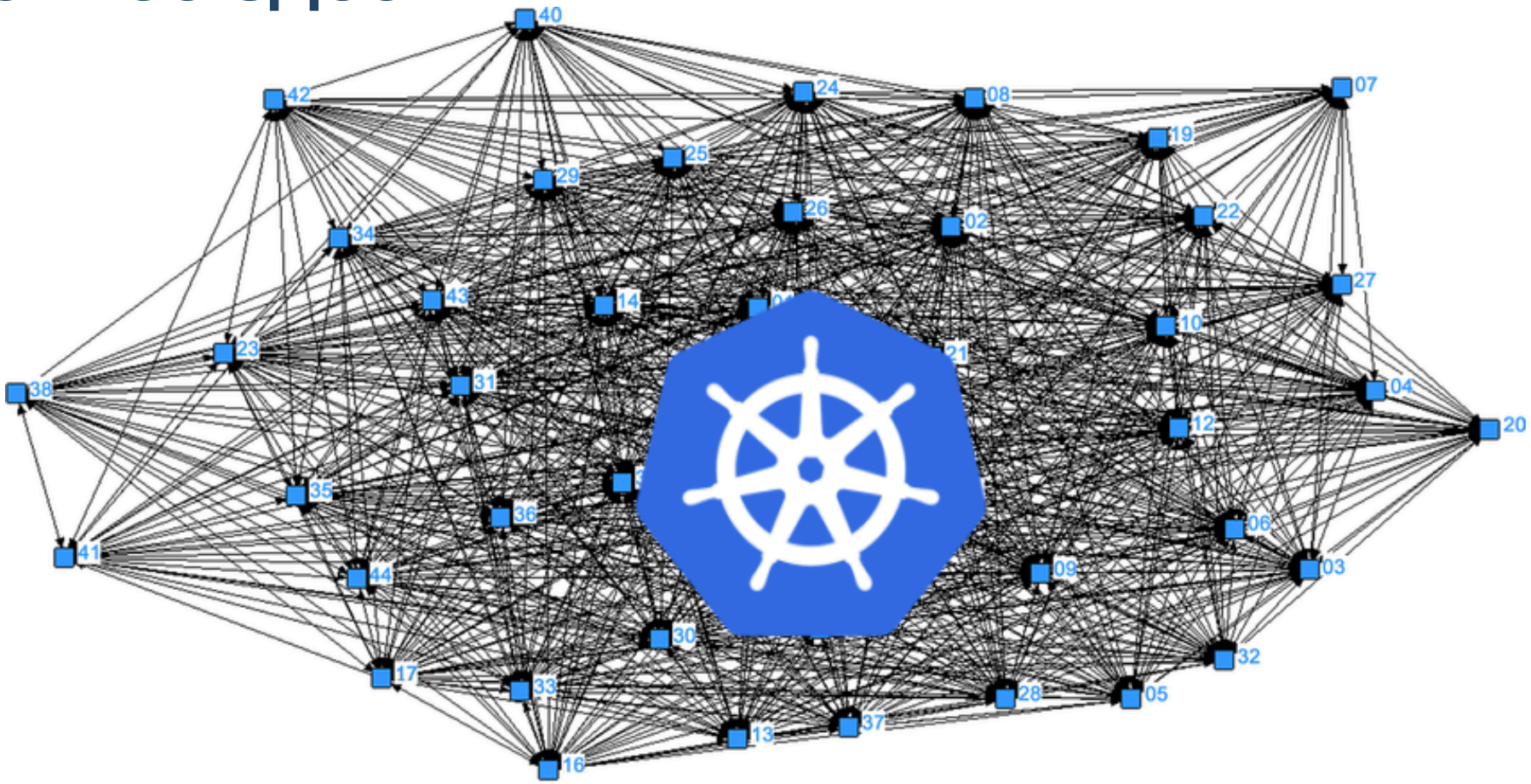

Доминирование
темной энергии
Излучение
реликтового фона
375 000 лет
Темные века
Формирование
галактик, планет и т.д.
Инфляция
IBM
VIRTUALIZATION
APP
OS
Квантовые
флуктуации
Первые звезды
ок. 400 миллионов лет
С начала расширения
13,77 миллиардов лет

. . . и оказались здесь

Помоги Даше-разработчице понять, на каком уровне протекает абстракция



. . . точнее здесь



Эксперт органа по сертификации (испытательной лаборатории)

Давайте разбираться!

Письмо ФСТЭК № 240/24/38 от 13 января 2025 г

- Инвентаризация образов контейнеров
- Список действий, разрешенных при взаимодействии компонентов средства между собой и внешними компонентами
- Не должно быть избыточных разрешающих правил доступа
- Правила доступа должны быть описаны в документации средства

https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-13-yanvarya-2025-g-n-240-24-38

Виды поставок приложений в контейнерном исполнении

ПРИЛОЖЕНИЯ
+
- оркестратор
- runtime
- . . .

- образы
- YAML-описания
- Helm
- . . .

КОМПЛЕКС ПРИЛОЖЕНИЯ

Контроль состояния Kubernetes-кластера

— Актуальные версии (актуальные версии 1.32, 1.31, 1.30)

- получают обновления только 3 последних релиза
- 14 месяцев (6+6+2)

— Исправленные компоненты

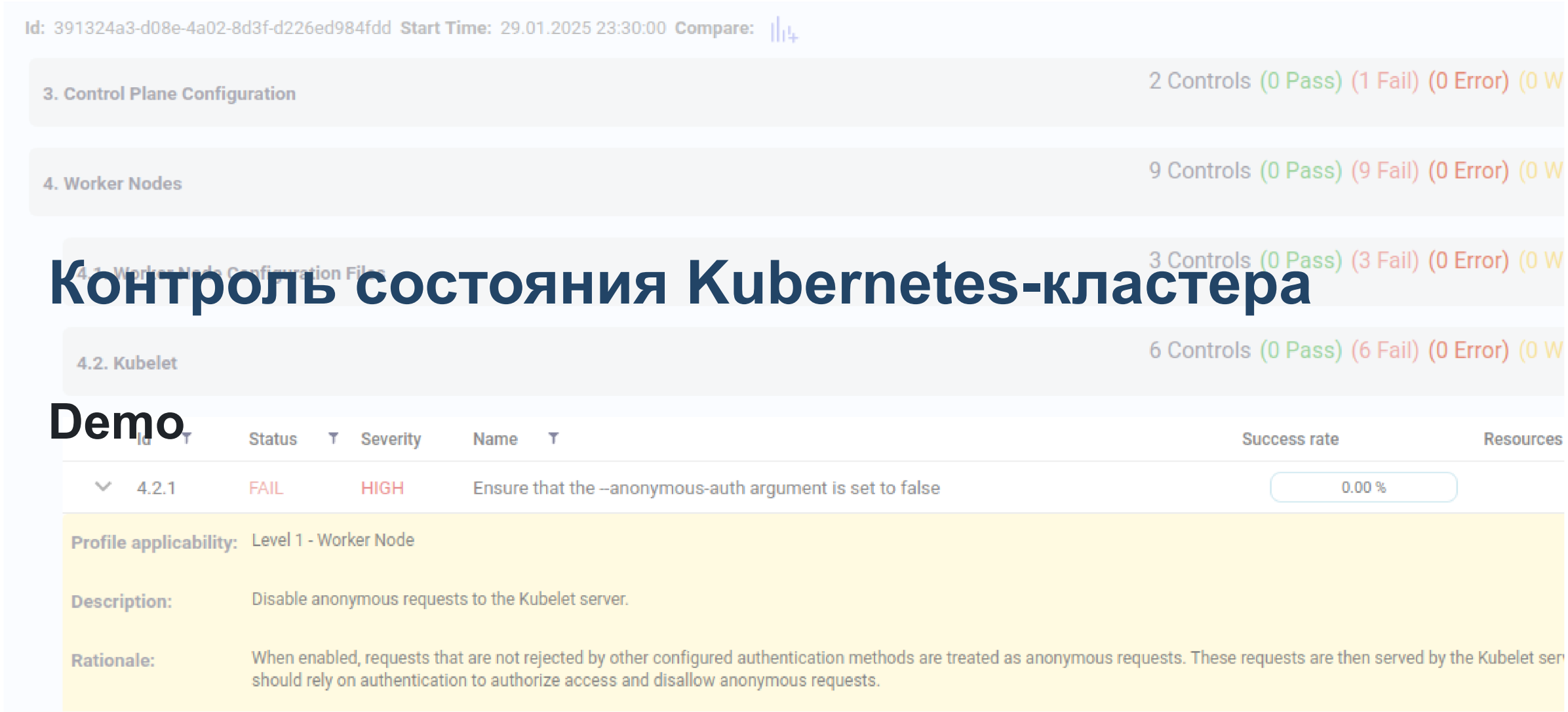
— Некорректные настройки кластера

Контроль состояния кластера (пример)

- CIS Kubernetes Benchmark
- Стендирование - это модель реального мира. Есть ограничения, но стремимся к реальному миру, а "харденинг" может подсветить проблемы.
- Рекомендации правок для документацию

Контроль состояния Kubernetes-кластера

Demo



Управление безопасностью образов

— ППК (перечень программных компонент) aka SBOM

— Уязвимости

— Недостатки Dockerfile

— Чувствительная информация

— Вредоносное ПО и ПО двойного назначения

ППК (пример)

5.16.2.3 Контролировать и актуализировать перечень зависимостей ПО в соответствии с регламентом композиционного анализа на предмет наличия известных уязвимостей.

5.16.2.4 Осуществлять анализ заимствованных компонентов, составляющих поверхность атаки, на предмет наличия известных уязвимостей при сборке (непосредственно перед сборкой) ПО (модулей ПО, компонентов ПО).

Уязвимости (пример)

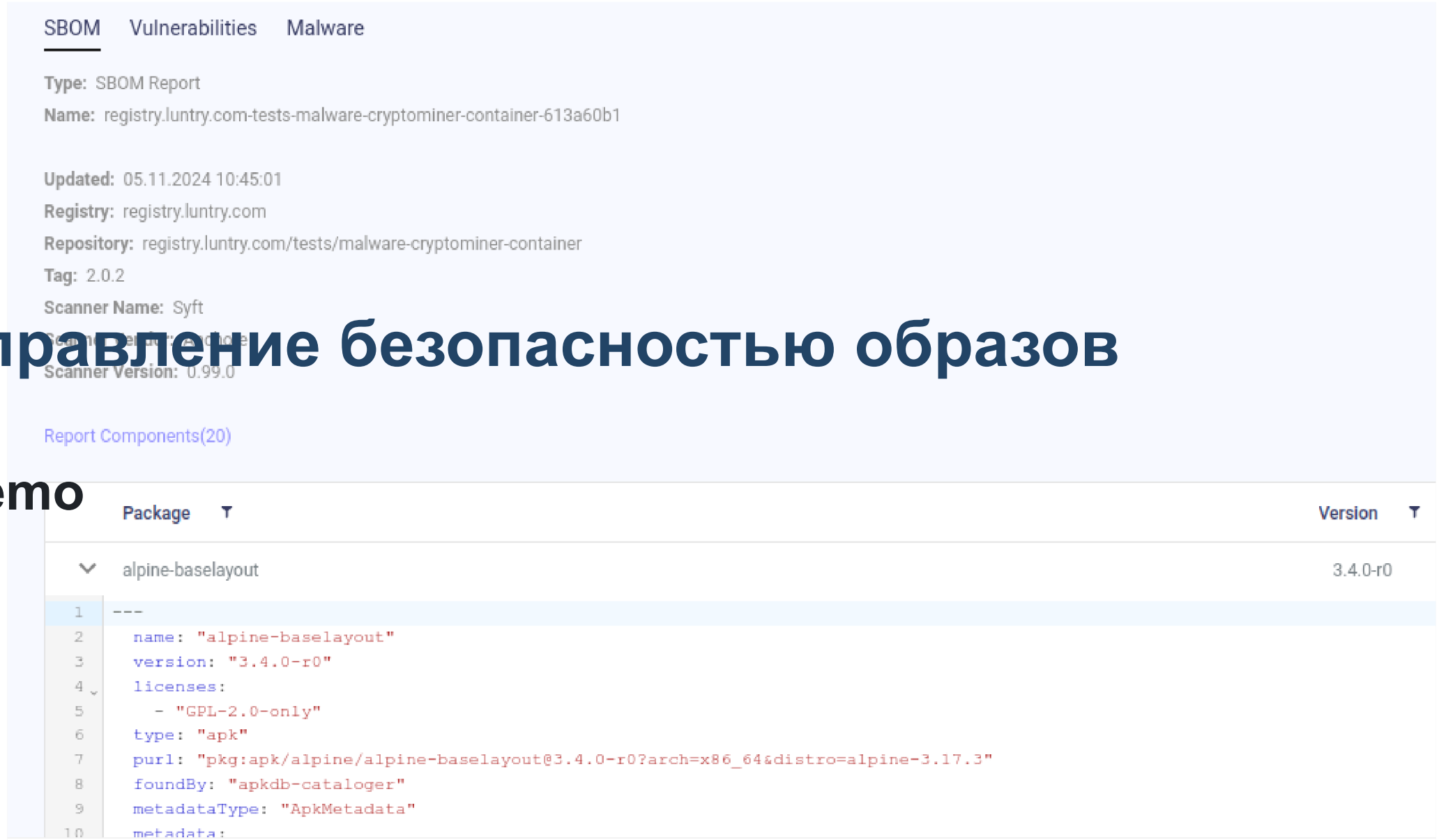
5.16.3.4 Результаты анализа заимствованных компонентов должны содержать следующие сведения:

- сведения о наличии/отсутствии известных уязвимостей в заимствованных компонентах;

- сведения о критичности выявленных уязвимостей в заимствованных компонентах.

Управление безопасностью образов

Demo



Безопасность Runtime

— Неизвестные/непонятные/нежелательные процессы

— Взаимодействие с ФС

— Взаимодействие с сетью

Сетевая безопасность

— Что доступно снаружи

— Что ходит наружу

— Использование NetworkPolicy

— Изоляция Namespaces

письмо ФСТЭК № 240/24/38 — список действий, при взаимодействии компонентов средства между собой и компонентами среды

Сетевая безопасность (пример)

Сетевая безопасность (пример)

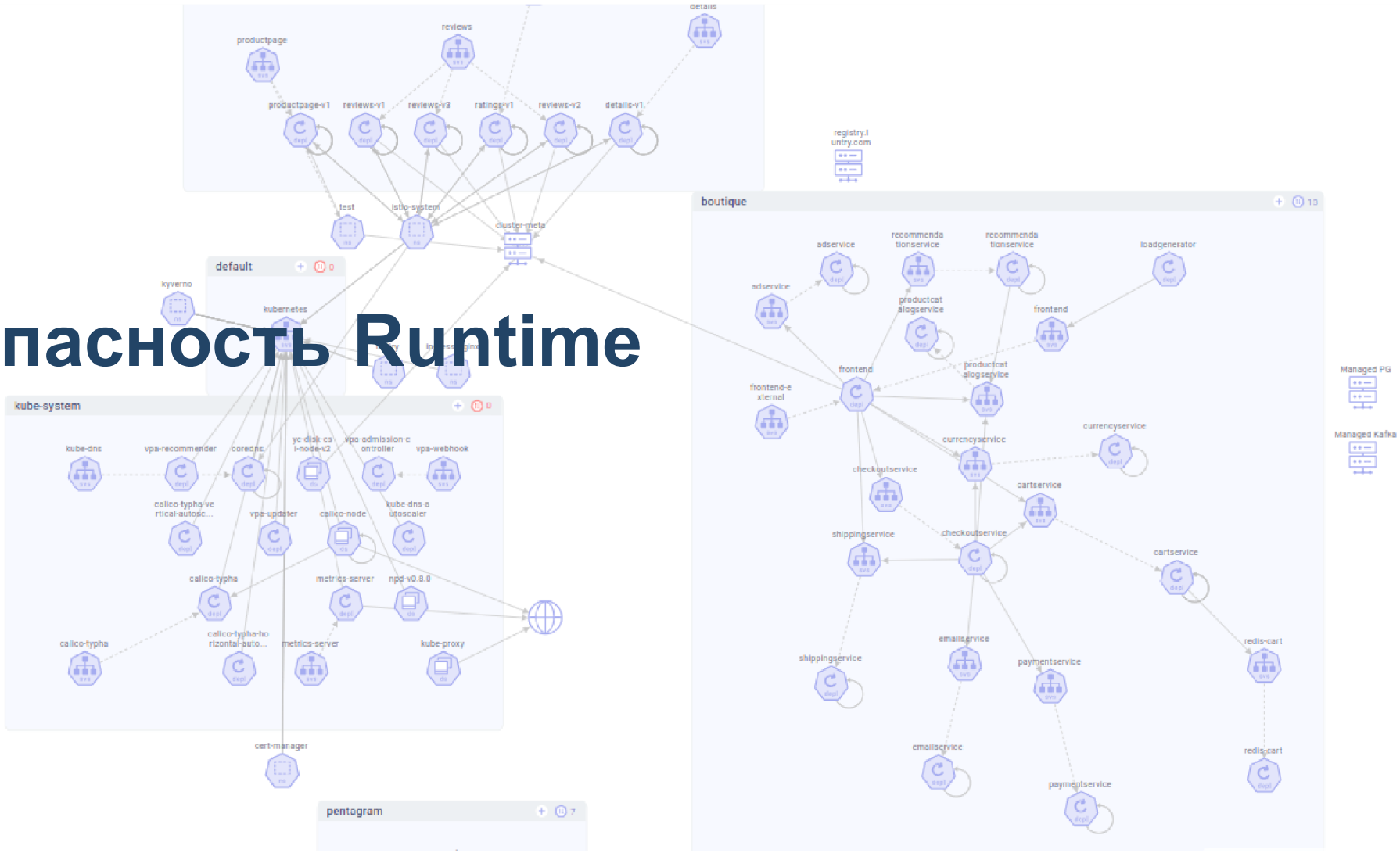
Модуль	VIZ	DP	CD	CA	CO	EXP	POL	CHA	GAT	RET	SEN	COL	SBO	SBS	VLN	WAT	NET	LNK
VIZ		ID1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
DP	ID1		—	—	ID2	—	ID3	—	—	—	—	—	—	ID4	—	—	—	ID5
CD	—	—		ID7	—	ID8	—	—	—	—	—	—	—	—	—	—	—	—
CA	—	—	ID7		—	—	—	—	—	—	—	—	—	—	—	—	—	—
CO	—	ID2	—	—		—	—	—	—	—	—	—	—	—	—	—	—	—
EXP	—	—	ID8	—	—		—	—	—	—	—	ID9	—	—	—	—	—	—
POL	—	ID3	—	—	—	—		—	—	—	—	—	—	—	—	—	—	—
CHA	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—	—	—
GAT	—	—	—	—	—	—	—	—		—	—	ID13	ID15	—	—	ID10	ID14	—
RET	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—
SEN	—	—	—	—	—	—	—	—	—	—		ID11	—	—	—	—	—	—
COL	—	—	—	—	—	ID9	—	—	ID13	—	ID11		—	—	—	—	ID12	—
SBO	—	—	—	—	—	—	—	—	ID15	—	—	—		—	—	—	—	—
SBS	—	ID4	—	—	—	—	—	—	—	—	—	—	—		—	—	—	—
VLN	—	—	—	—	—	—	—	—	—	—	—	—	—	—		—	—	—
WAT	—	—	—	—	—	—	—	—	ID10	—	—	—	—	—	—		—	—
NET	—	—	—	—	—	—	—	—	ID14	—	—	ID12	—	—	—	—		—
LNK	—	ID5	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	

AppArmor (пример)

На основе аналитики можем сгенерировать профиль, что позволяет формализовать и зафиксировать описание, что бы следовать минимальным привилегиям и ограничениям

Безопасность Runtime

Demo



Анализ прав доступа

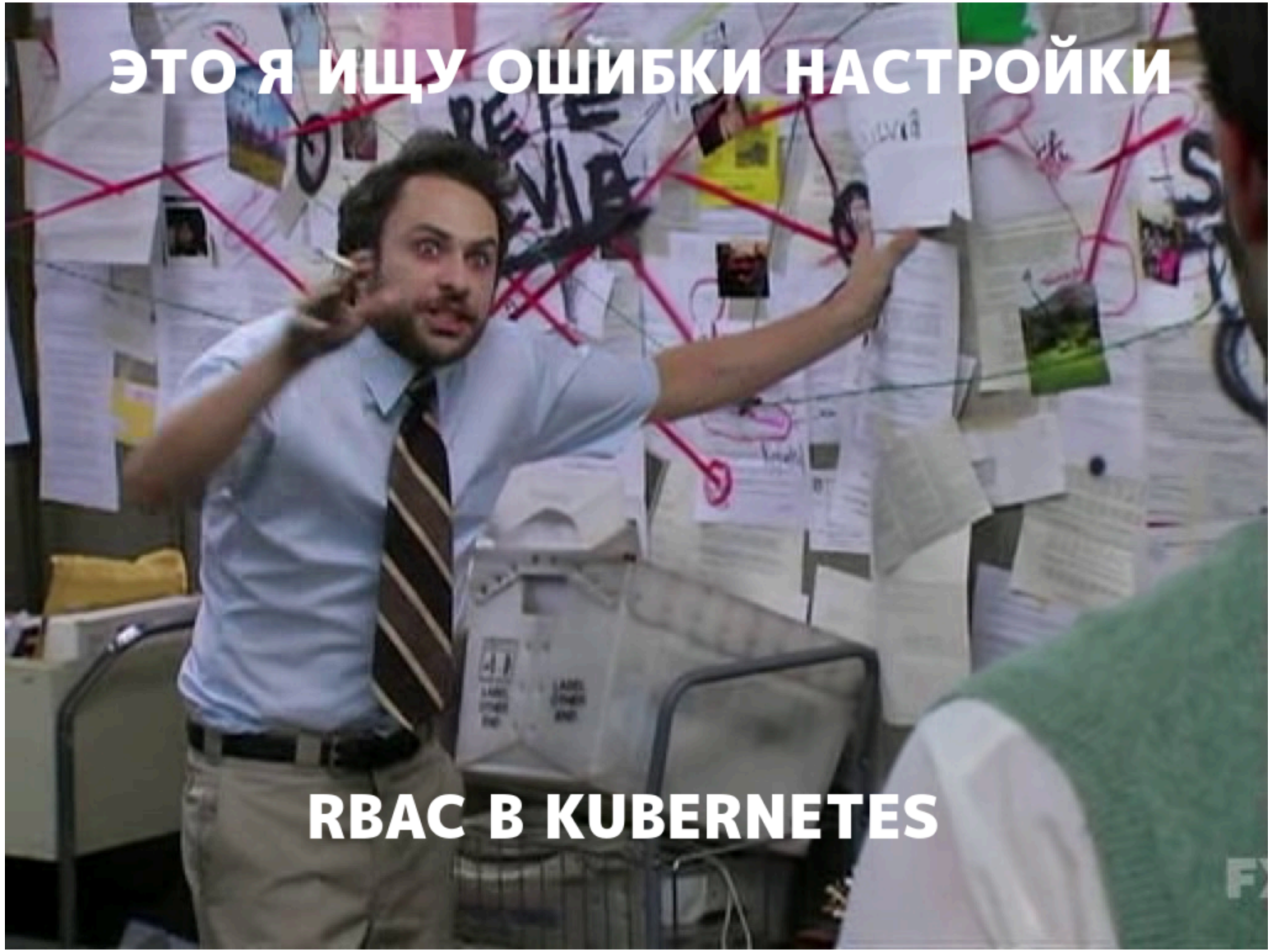
— Списки субъектов

— “*” в правах

— Доступ к критичным ресурсам

— Собственные правила

RBAC

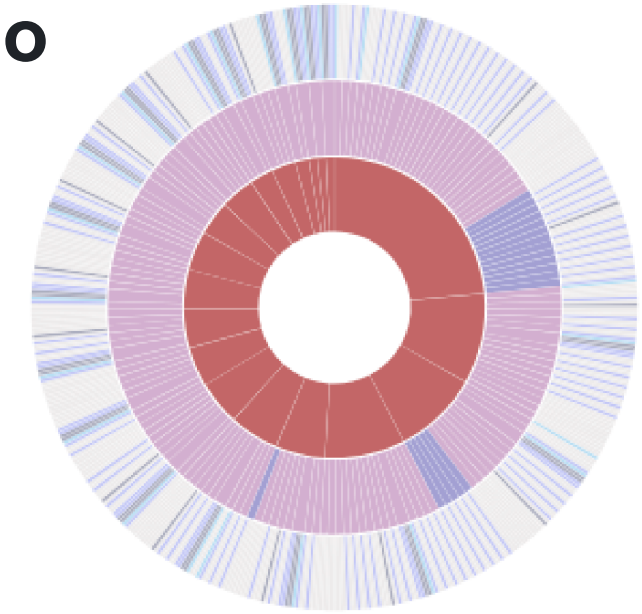


Смотрим RBAC

Demo

RBAC

Group by Rule



Roles
- Cluster role
- Role

Subjects
- Service Account
- User
- Group
- None

Rules
- critical
- high
- medium
- low
- info
- negligible

Exceptions

Allow read Secrets	
critical **Roles:** 42 **Subjects:** 40	This Role/ClusterRole contains permissions that allow to retrieve Secrets with sensitive data.

Проверка Kubernetes-ресурсов

— Pod Security Standard

— Контроль источника/подписи образов

— Использование библиотеки правил

Pod Security Standard

Определяет политику для пространств имен:

- Privileged — политика без ограничений, которая допускает эскалацию привилегий
- Baseline — политика с минимальными ограничениями, ограничивающая использование эскалаций привилегий
- Restricted — политика с максимальными ограничениями, соответствующая актуальным рекомендациям по безопасному запуску приложений в кластере

https://kubernetes.io/docs/concepts/security/pod-security-standards/

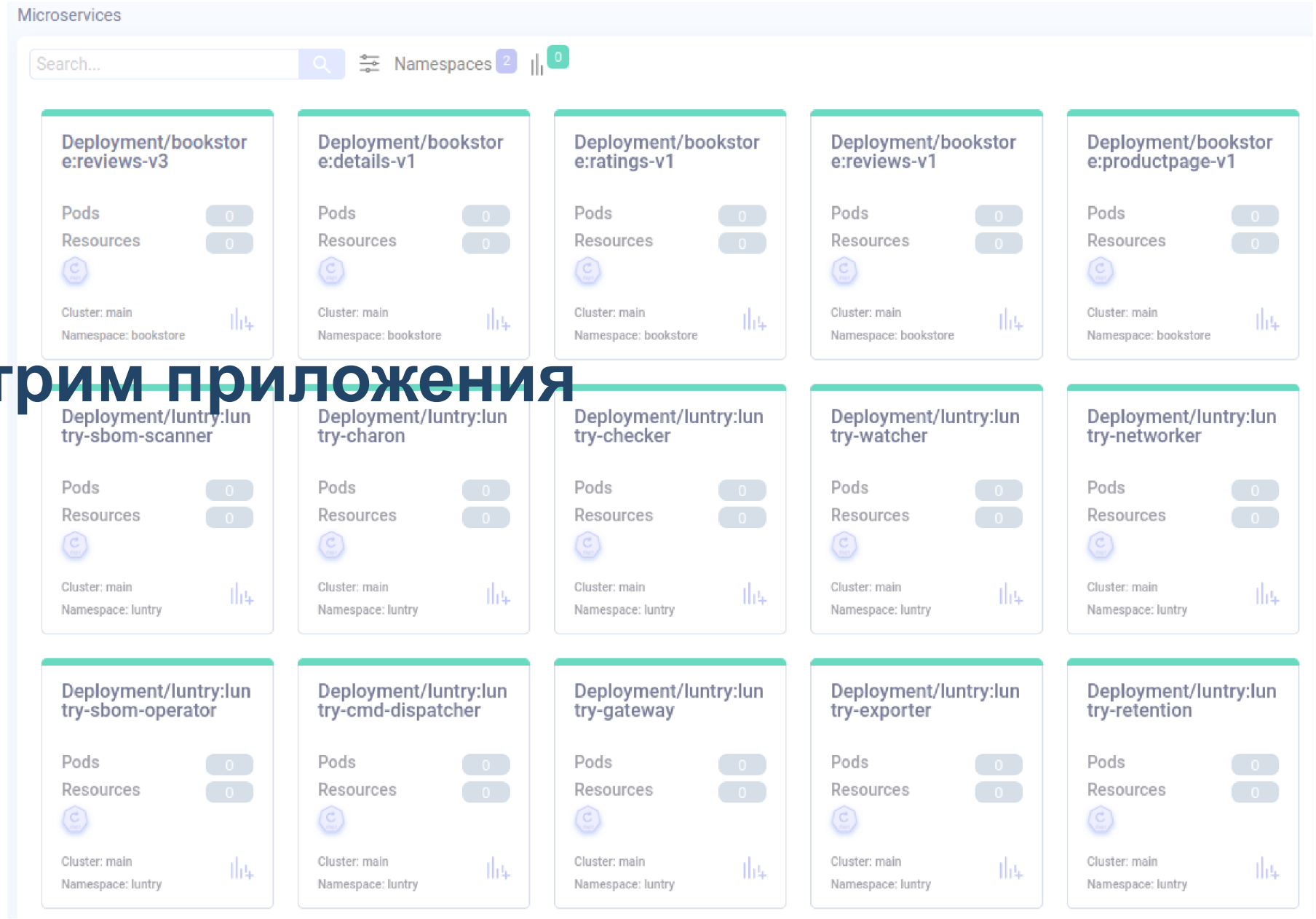
Policy Engine

Demo

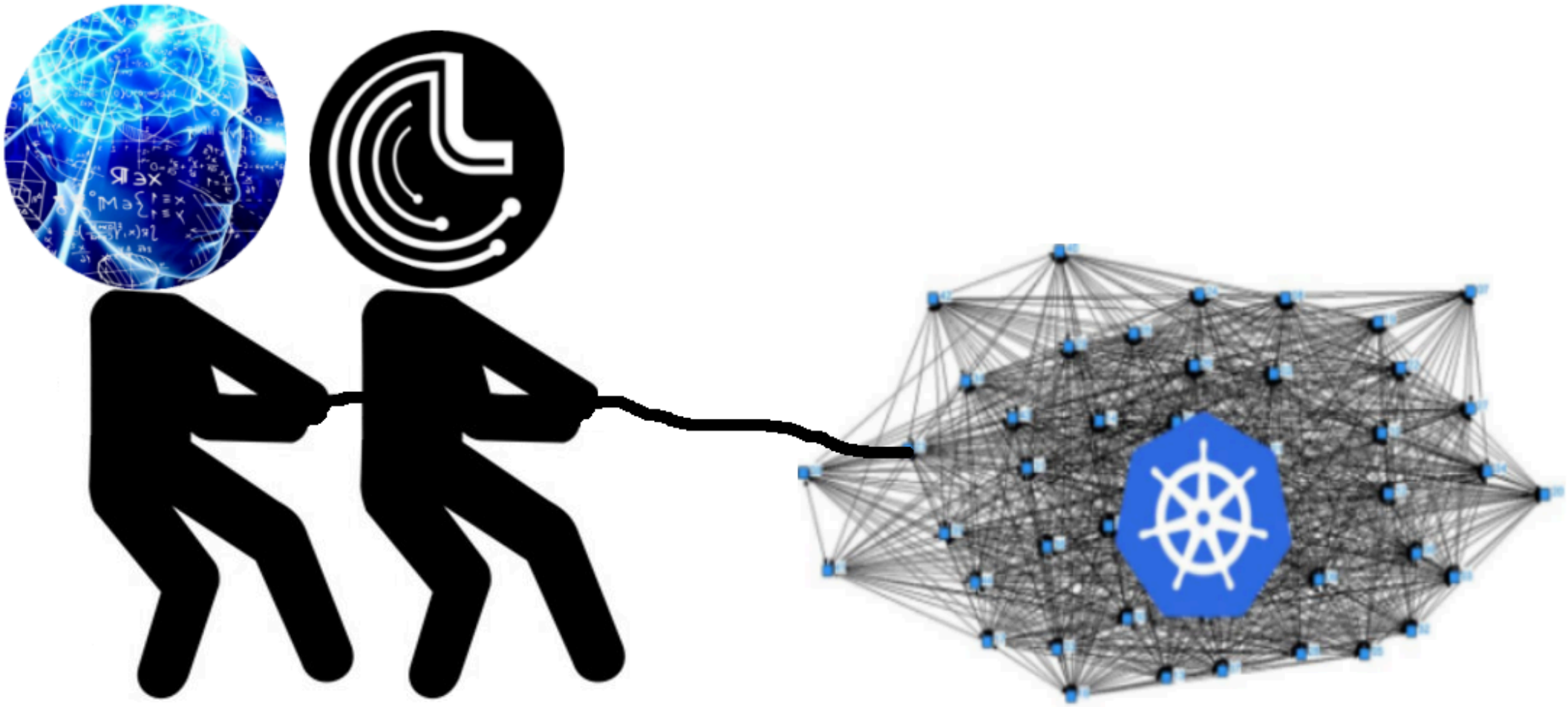
Микросервисы и приложения

Смотрим приложения

Demo



Вместо заключения



Полезные ссылки

- Приказ №118. Требования по безопасности информации к средствам контейнеризации (выписка)
- Национальный стандарт РФ ГОСТ Р 56939-2024 "Защита информации. Разработка безопасного программного обеспечения. Общие требования"
- О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

Спасибо за внимание!

site: luntry.ru

tg: @rusdacent

channel: @tech_b0lt_Genona

Вопросы?