

Основы анализа СЗИ в контейнерном исполнении с помощью Luntry

Анатолий Карпенко

Luntry

whoami

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



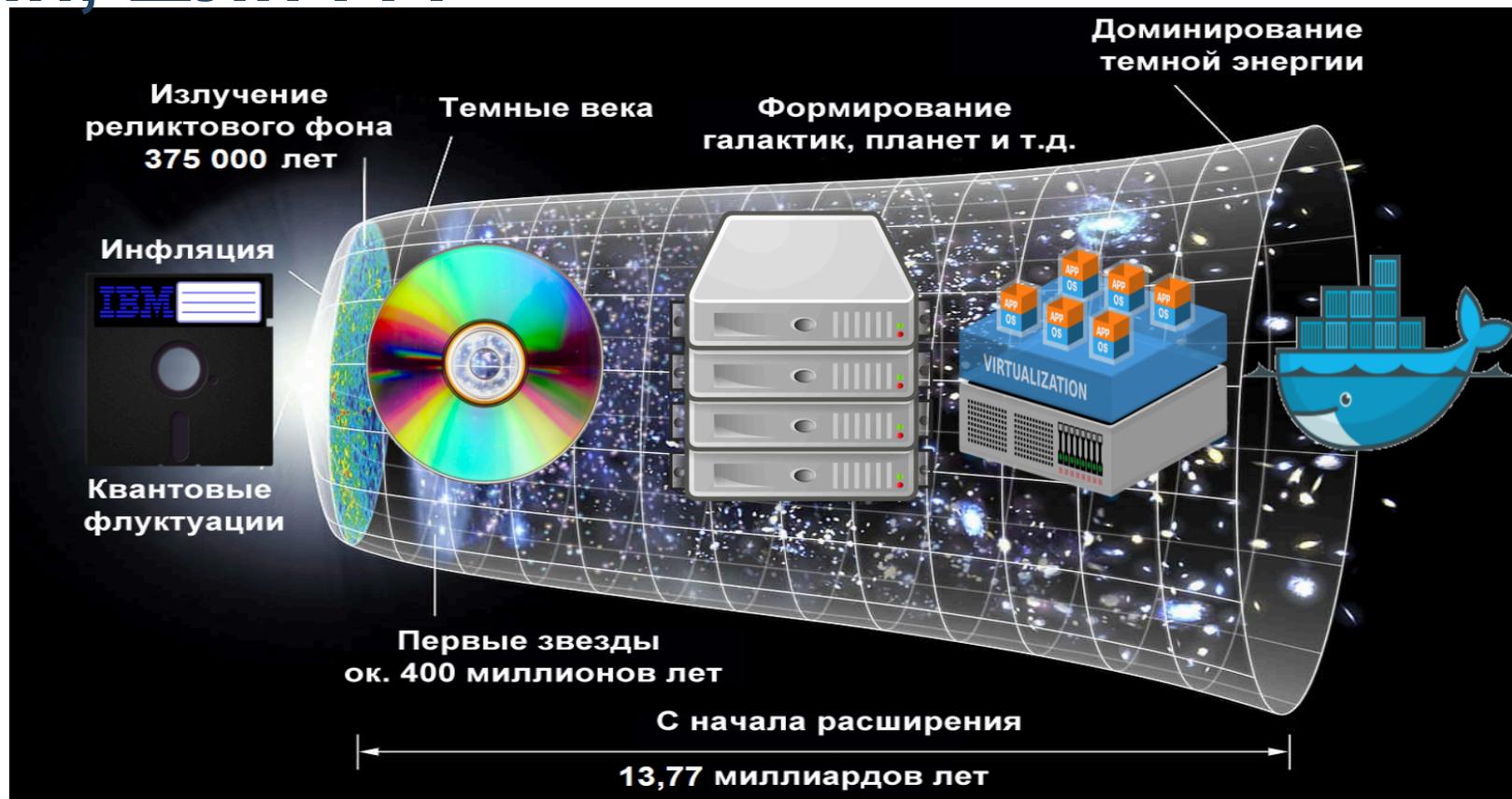
Спасибо

Андрей Слепых

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

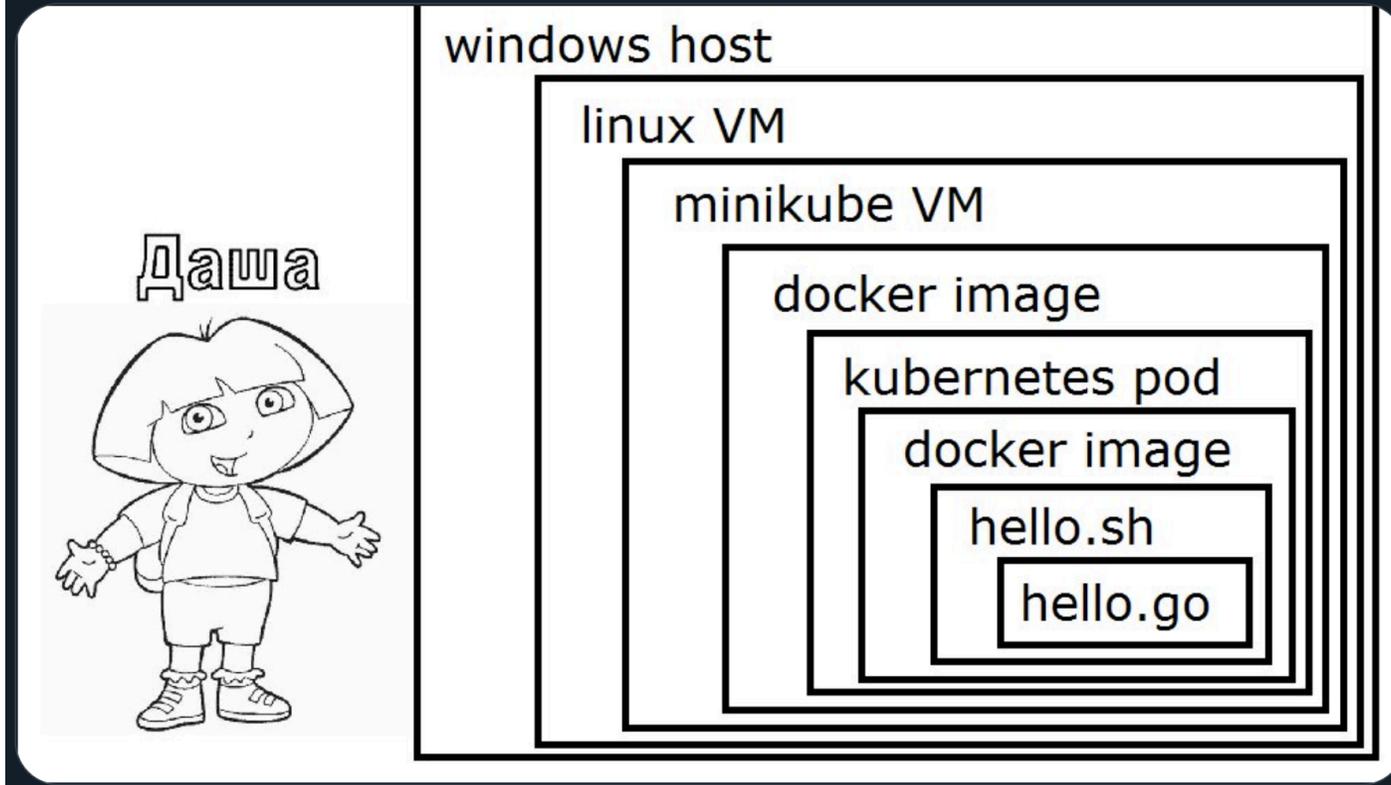


Мы шли, шли . . .

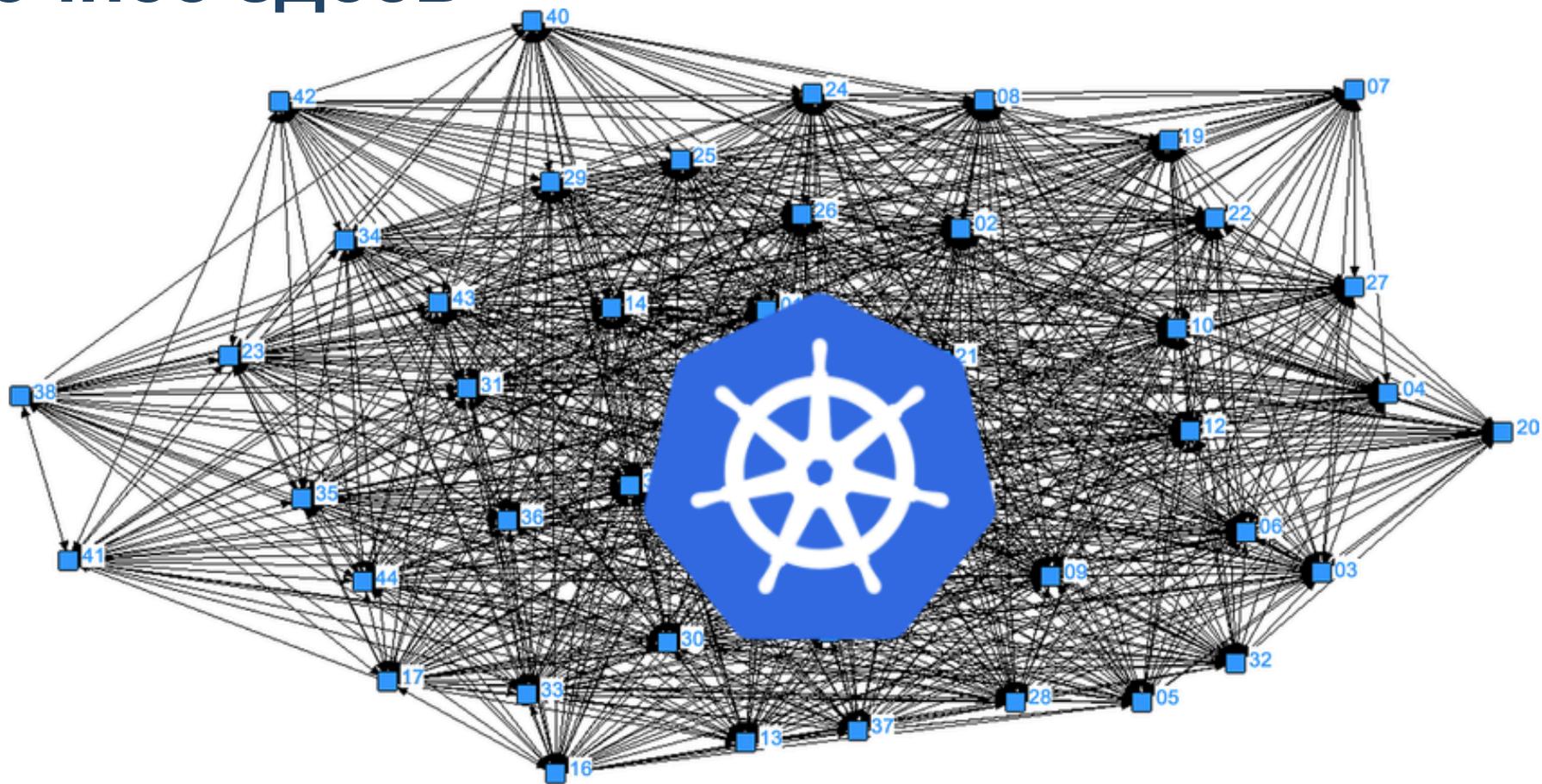


... и оказались здесь

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



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

Id: 391324a3-d08e-4a02-8d3f-d226ed984fdd Start Time: 29.01.2025 23:30:00 Compare: 

3. Control Plane Configuration

2 Controls (0 Pass) (1 Fail) (0 Error) (0 W)

4. Worker Nodes

9 Controls (0 Pass) (9 Fail) (0 Error) (0 W)

Контроль состояния Kubernetes-кластера

3 Controls (0 Pass) (3 Fail) (0 Error) (0 W)

6 Controls (0 Pass) (6 Fail) (0 Error) (0 W)

Демо

Id	Status	Severity	Name	Success rate	Resources
4.2.1	FAIL	HIGH	Ensure that the --anonymous-auth argument is set to false	0.00 %	
Profile applicability: Level 1 - Worker Node					
Description: Disable anonymous requests to the Kubelet server.					
Rationale: When enabled, requests that are not rejected by other configured authentication methods are treated as anonymous requests. These requests are then served by the Kubelet server. These requests should rely on authentication to authorize access and disallow anonymous requests.					

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.

SBOM Vulnerabilities Malware

Type: SBOM Report

Name: registry.luntry.com-tests-malware-cryptominer-container-613a60b1

Updated: 05.11.2024 10:45:01

Registry: registry.luntry.com

Repository: registry.luntry.com/tests/malware-cryptominer-container

Tag: 2.0.2

Scanner Name: Syft

Scanner Version: 0.99.0

Report Components(20)

Управление безопасностью образов

Демо

Package	Version
alpine-baselayout	3.4.0-r0
<pre>1 --- 2 name: "alpine-baselayout" 3 version: "3.4.0-r0" 4 licenses: 5 - "GPL-2.0-only" 6 type: "apk" 7 purl: "pkg:apk/alpine/alpine-baselayout@3.4.0-r0?arch=x86_64&distro=alpine-3.17.3" 8 foundBy: "apkgdb-cataloger" 9 metadataType: "ApkMetadata" 10 metadata:</pre>	

Безопасность Runtime

- **Неизвестные/непонятные/нежелательные процессы**
- **Взаимодействие с ФС**
- **Взаимодействие с сетью**

Сетевая безопасность

- Что доступно снаружи
- Что ходит наружу
- Использование NetworkPolicy
- Изоляция Namespaces



Сетевая безопасность (пример)

	Сервис 1	Сервис 2	Сервис 3	...
Сервис 1		ID_1	—	
Сервис 2	ID_1		ID_2	
Сервис 3	—	ID_2		
...				

Сетевая безопасность (пример)

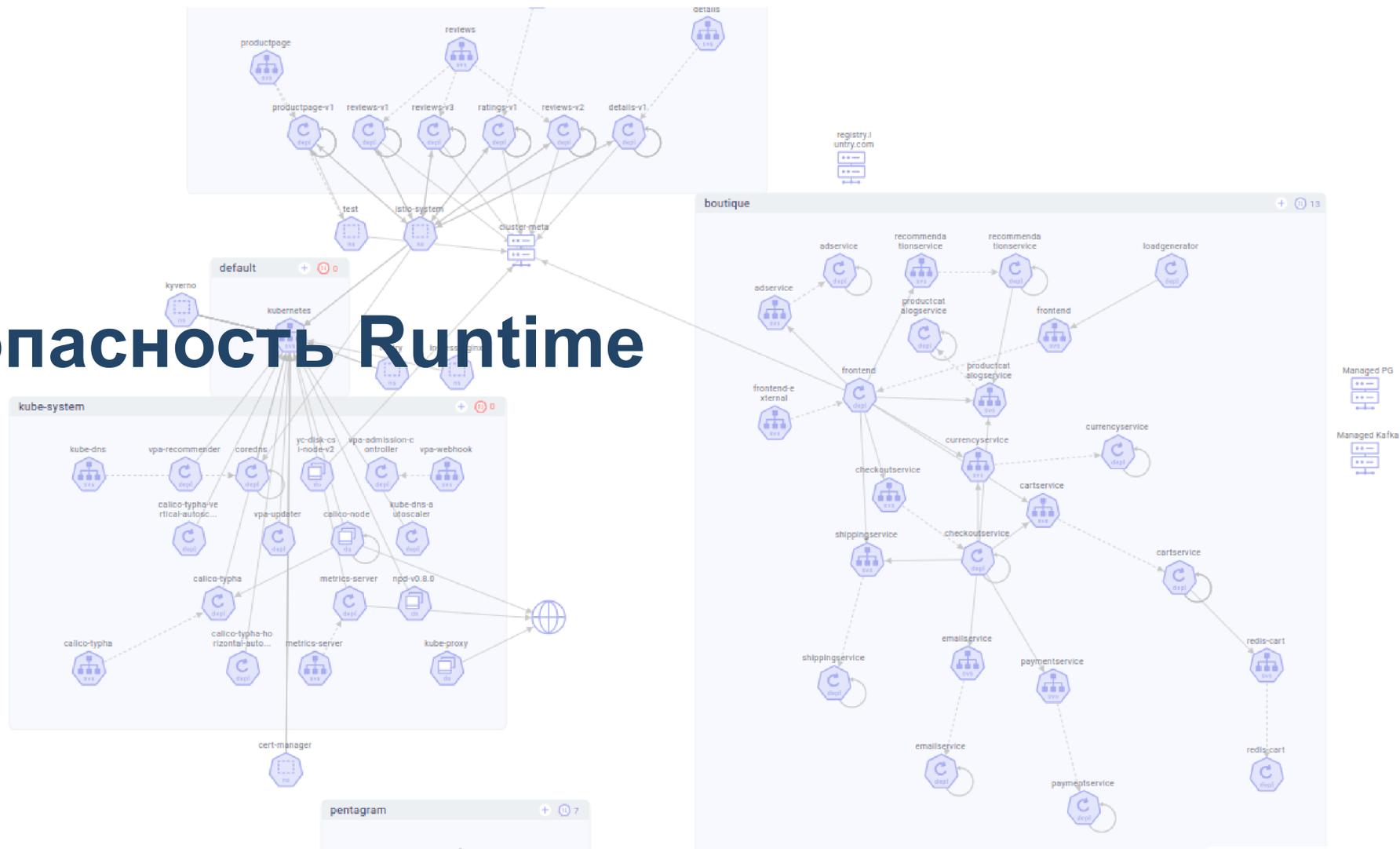
Модуль	VIZ	DP	CD	CA	CO	EXP	POL	CHA	GAT	RET	SEN	COL	SBO	SBS	VLN	WAT	NET	LNK
VIZ		ID1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
DP	ID1		—	—	ID2	—	ID3	—	—	—	—	—	—	ID4	—	—	—	ID5
CD	—	—		ID7	—	ID8	—	—	—	—	—	—	—	—	—	—	—	—
CA	—	—	ID7		—	—	—	—	—	—	—	—	—	—	—	—	—	—
CO	—	ID2	—	—		—	—	—	—	—	—	—	—	—	—	—	—	—
EXP	—	—	ID8	—	—		—	—	—	—	—	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

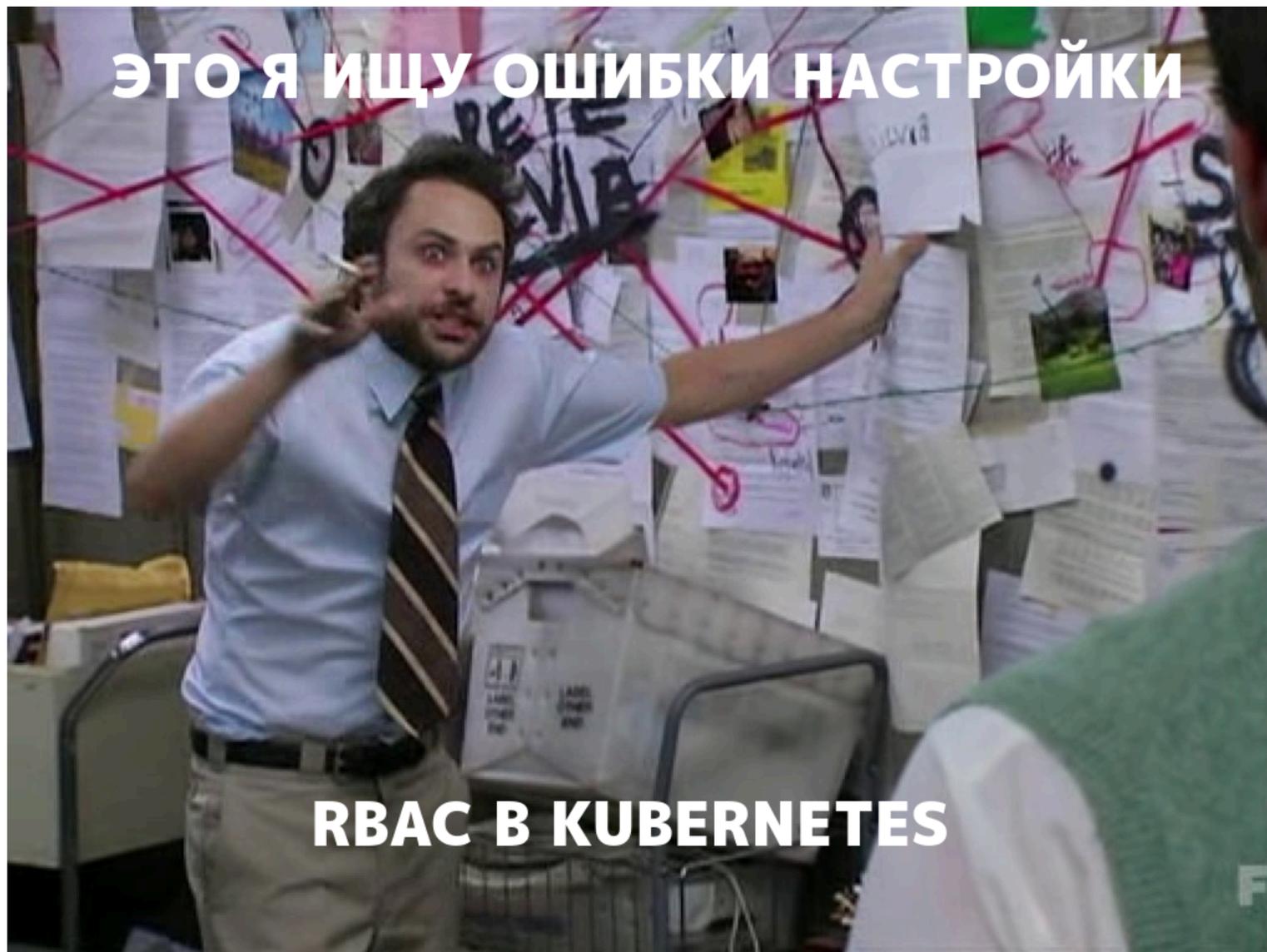
Demo



Анализ прав доступа

- Списки субъектов
- “*” в правах
- Доступ к критичным ресурсам
- Собственные правила

РВАС



ЭТО Я ИЩУ ОШИБКИ НАСТРОЙКИ

РВАС В KUBERNETES

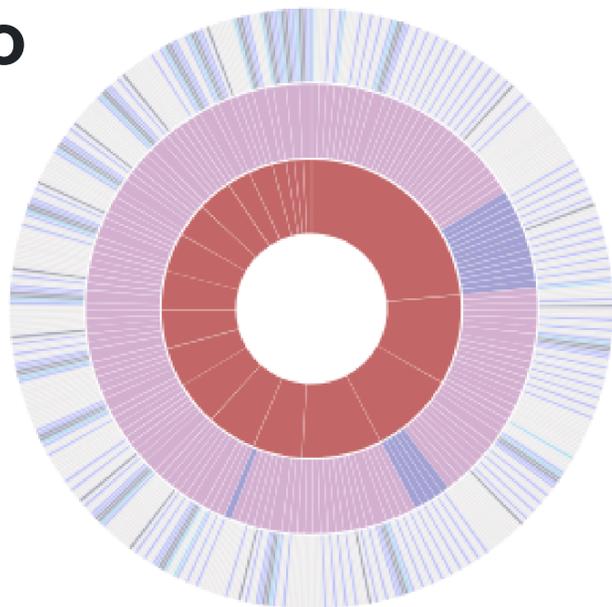
RBAC Смотрим RBAC



Group by Rule



Демо



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

Policy Engines

Runtime Policies

Policy Engines

Reaction Policies

Dashboard

Policies

Violations

Library

Total

4280

Violations

Pass

2813

Fail

1467

Policy Engine

Demo

Total

15

Audit

15

Policies

Enforce

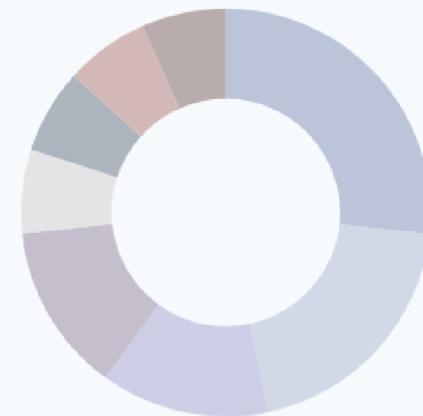
0

Warn

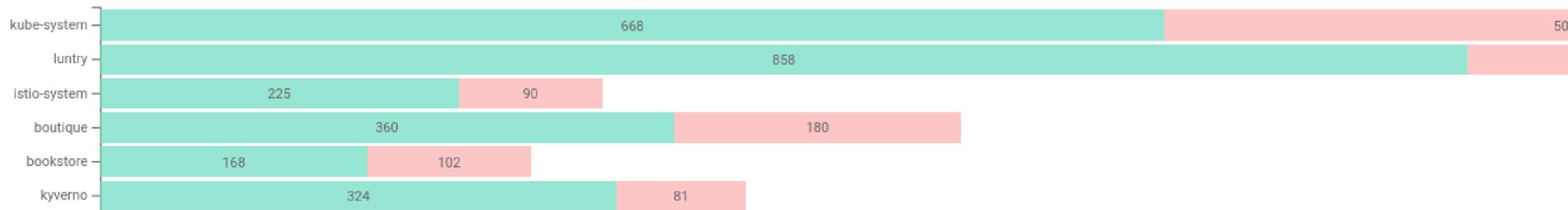
0

Dryrun

0



Policy Results per Namespace



Микросервисы и приложения

Microservices

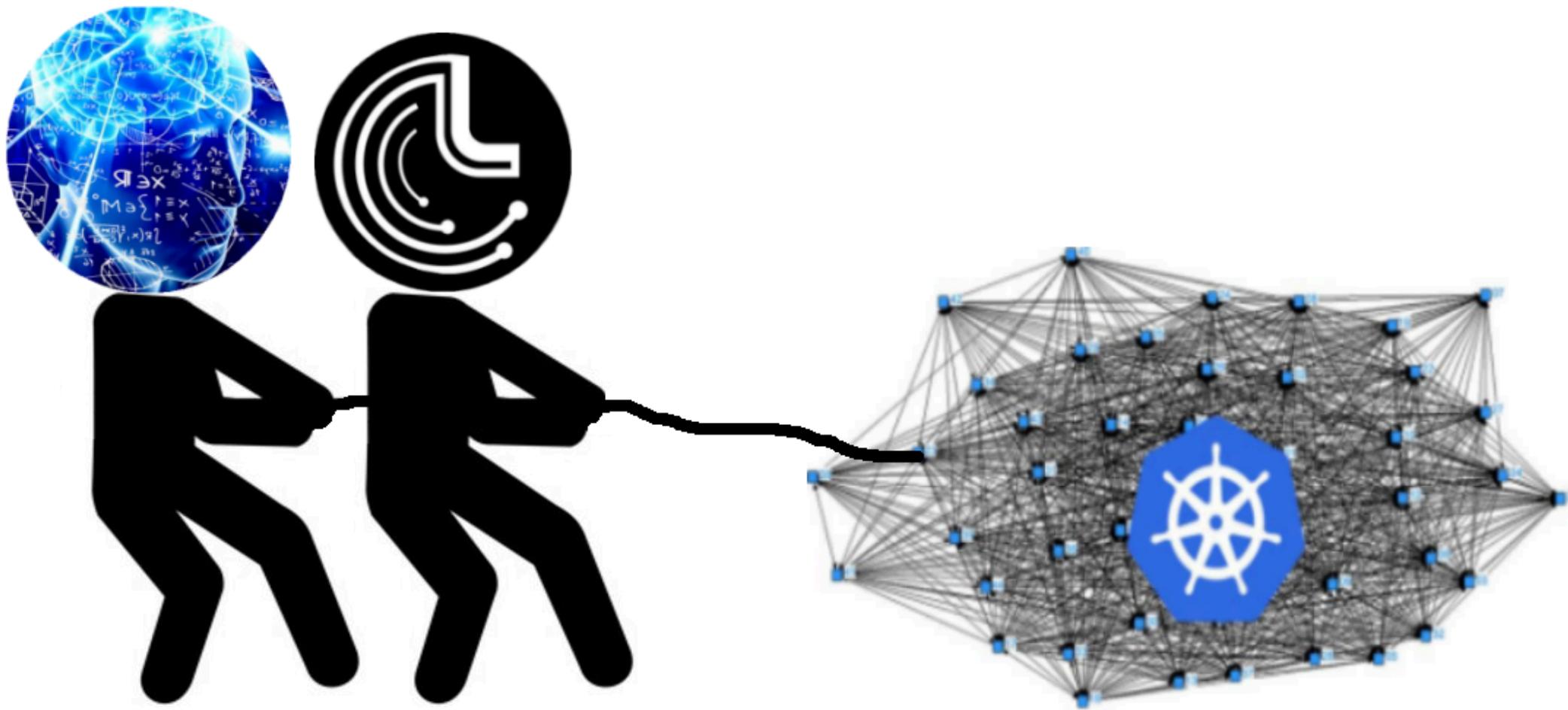
Search... Namespaces 2 0

<p>Deployment/bookstore:reviews-v3</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: bookstore</p>	<p>Deployment/bookstore:details-v1</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: bookstore</p>	<p>Deployment/bookstore:ratings-v1</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: bookstore</p>	<p>Deployment/bookstore:reviews-v1</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: bookstore</p>	<p>Deployment/bookstore:productpage-v1</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: bookstore</p>
<p>Deployment/luntry:luntry-sbom-scanner</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-charon</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-checker</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-watcher</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-networker</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>
<p>Deployment/luntry:luntry-sbom-operator</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-cmd-dispatcher</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-gateway</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-exporter</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>	<p>Deployment/luntry:luntry-retention</p> <p>Pods 0 Resources 0</p> <p>Cluster: main Namespace: luntry</p>

Смотрим приложения

Демо

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](https://t.me/@rusdacent)

channel: [@tech_b0lt_Genona](https://t.me/@tech_b0lt_Genona)

Вопросы?