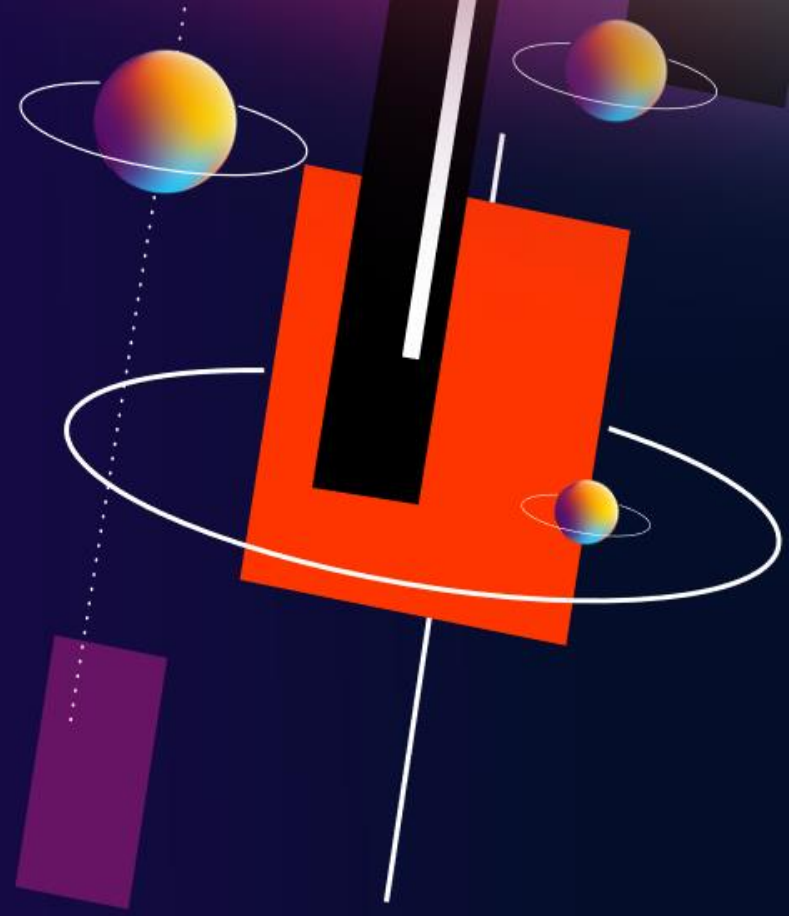
Безопасность Kubernetes-кластеров: вредные советы

Дмитрий Евдокимов

Founder & CTO Luntry



DevOps Conf 2024

Обо мне

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- Специализация – безопасность контейнеров и Kubernetes
- CFP DevOpsConf, HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор Telegram-канала “k8s (in)security”
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Организатор конференции по безопасности контейнеров - БеКон
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, DevOops, KuberConf, VK Kubernetes Conference, HighLoad++, БеКон и др.

План доклада

- Введение
- Вредные советы
  - Установка антивируса на Nodes кластера
  - Сканирование хостовой ОС на Nodes кластера на известные уязвимости в пакетах
  - Блокировка выкатки образов с чувствительной информацией
  - Блокировка выкатки образов на основании информации об уязвимостях
- Заключение

Disclaimer

Все пункты взяты с реальных корпоративных требований, технических заданий, внутренних документов, описывающий процессы и т.д.

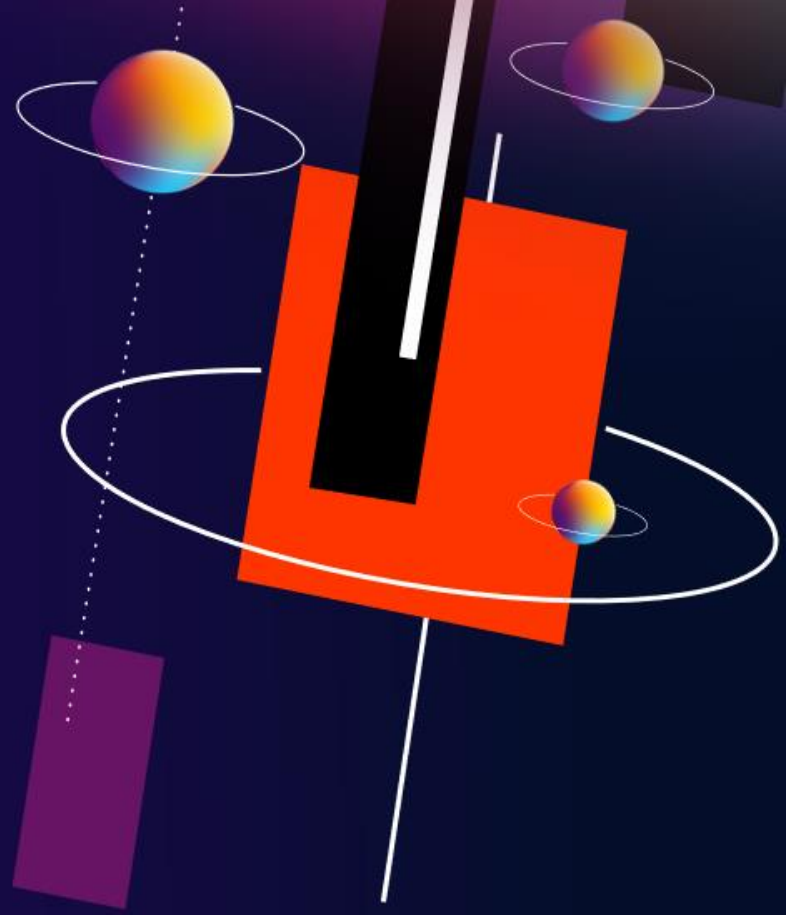
Компании из абсолютно разных секторов: от финансового и ретейл до нефтегазового и социальных сетей.

Наш опыт за последние 4 года.

Все это можно использовать, главное понимайте последствия!

Введение

Начнем с базовой теории



DevOps Conf 2024

Kubernetes

Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.

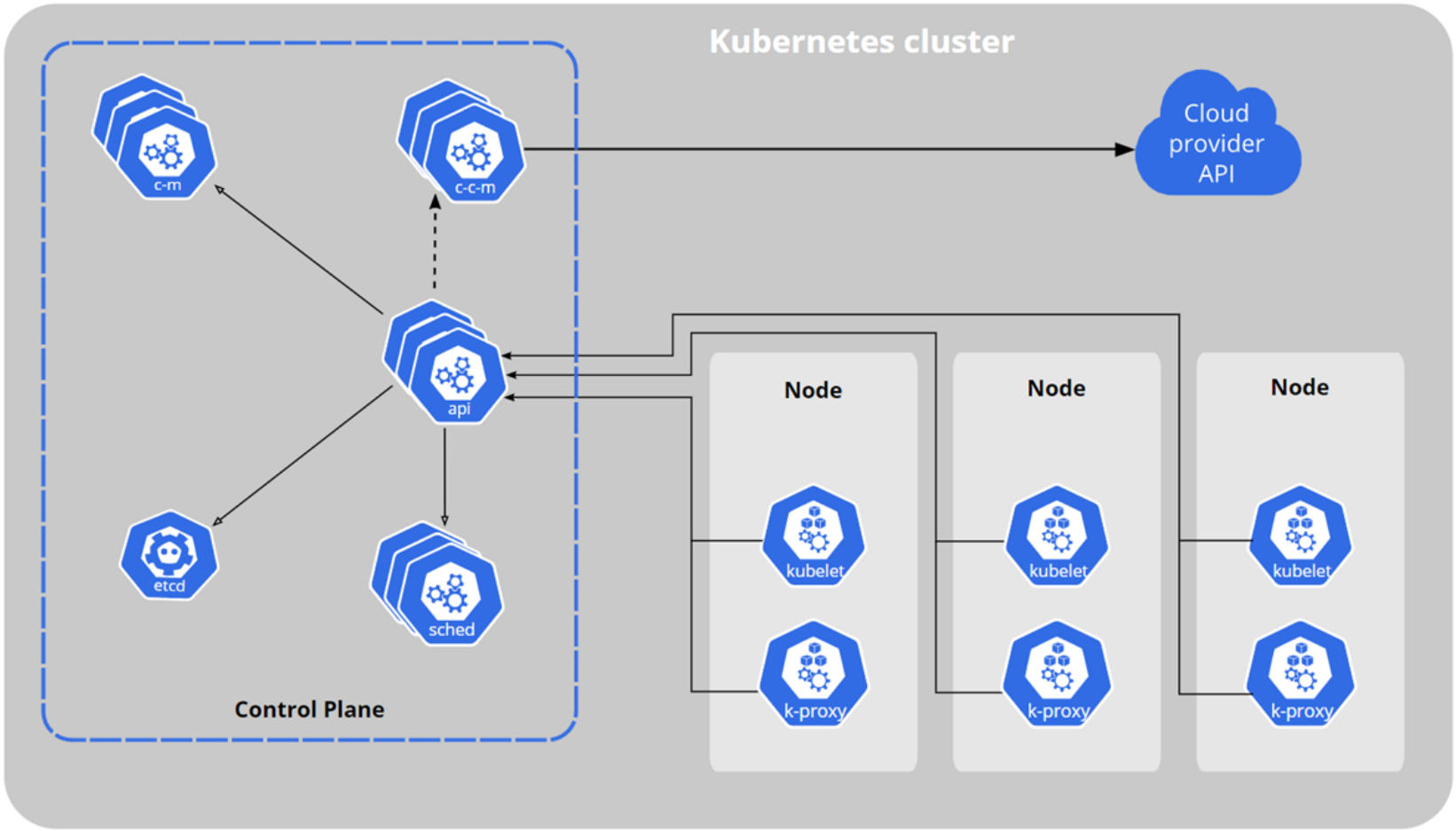
It groups containers that make up an application into logical units for easy management and discovery. Kubernetes builds upon 15 years of experience of running production workloads at Google, combined with best-of-breed ideas and practices from the community.

Pods

Pods are the smallest deployable units of computing that you can create and manage in Kubernetes.

https://kubernetes.io/

Компоненты Kubernetes



API server

Cloud controller manager *(optional)*

Controller manager

etcd (persistence store)

kubelet

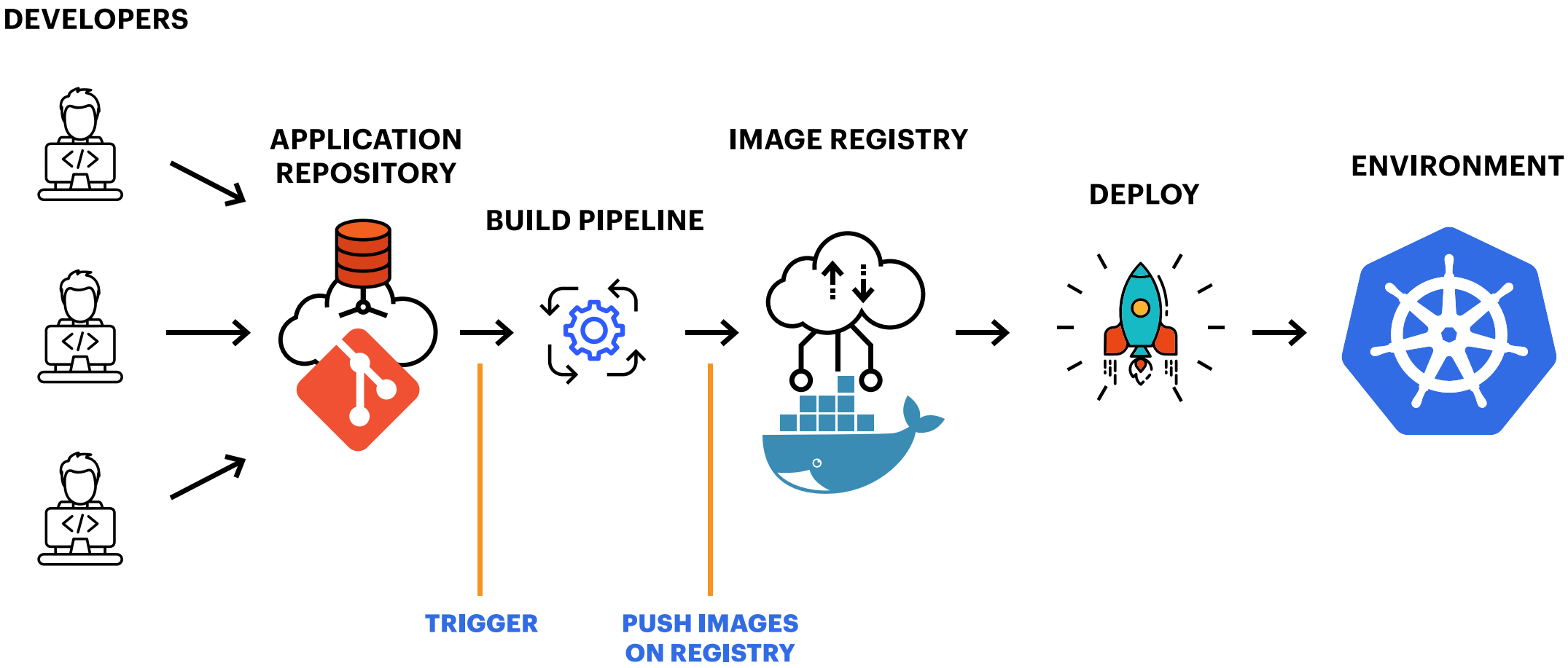
kube-proxy

Scheduler

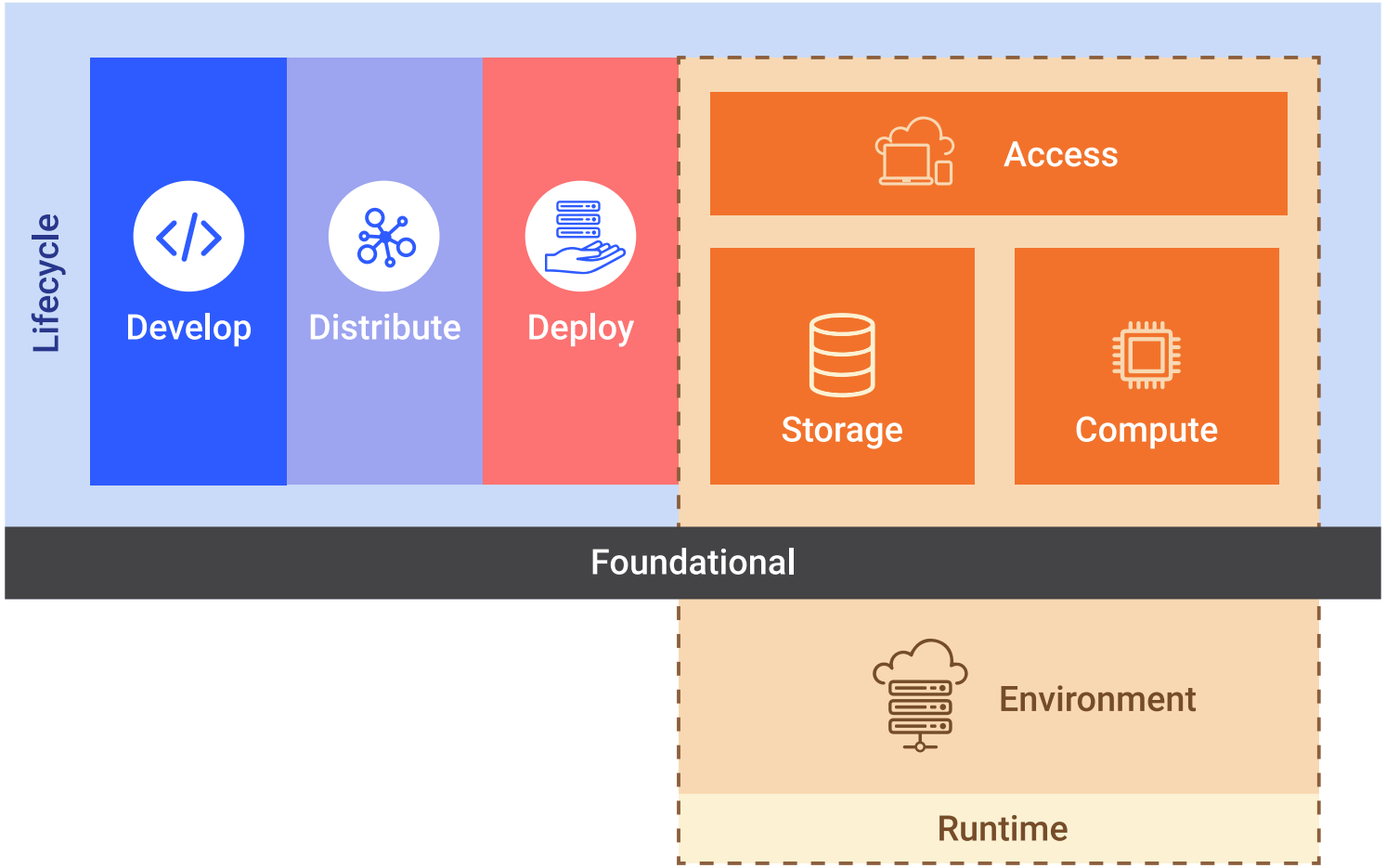
Control plane

Node

Не Kubernetes единым

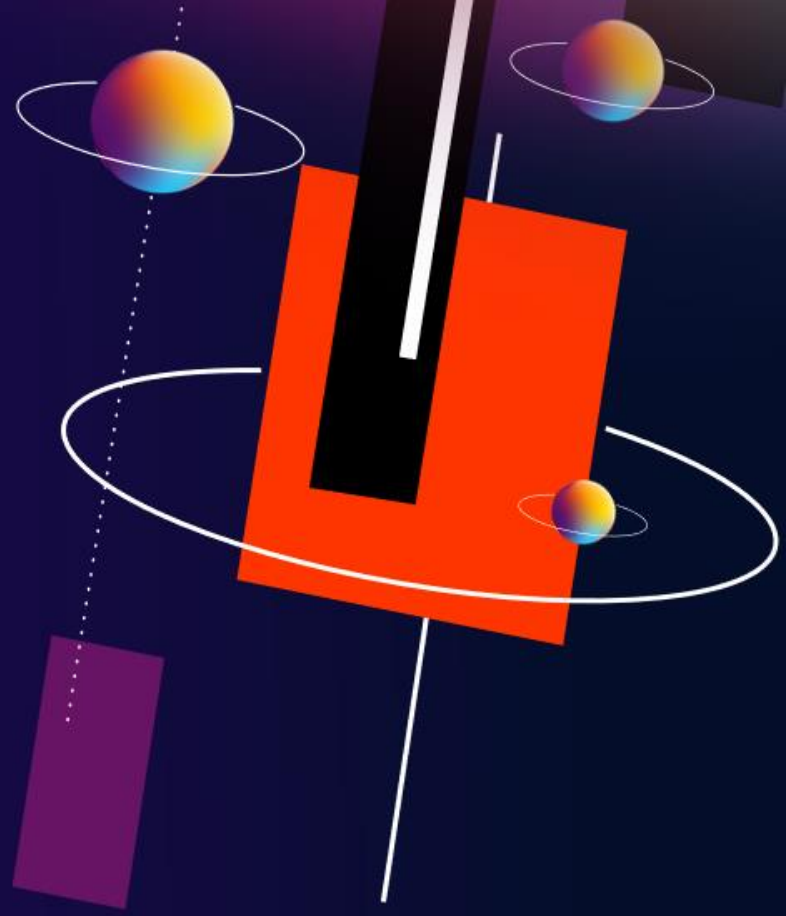


Shift Left/Everywhere Security



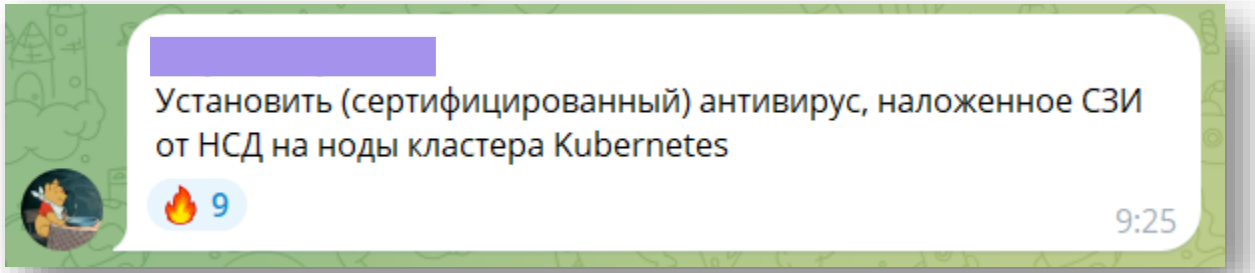
Вредные советы

Вроде классно, но нет



DevOps Conf 2024

#1 Установка антивируса на Nodes кластера



[Победитель конкурса “Вредные советы”]

Основания

- Прописано в общем корпоративном стандарте информационной безопасности

- Обнаружить вредоносную активность на хостовой ОС

Последствия

- Неэффективное использование вычислительных ресурсов Nodes

- Негативное влияние на микросервисы

Реальная жизнь

- Ставят агенты антивируса в отключенном виде

- Заносят почти все в список исключений для агента

Что говорят стандарты

Стандарты:

- CLOUD NATIVE SECURITY WHITEPAPER
- CIS Kubernetes Benchmark
- NSA/CISA Kubernetes Hardening Guide
- Kubernetes Security Technical Implementation Guide (STIG)
- PCI Security Standards Council: Guidance for Containers and Container Orchestration Tools
- NIST Special Publication 800-190 "Application Container Security Guide“
- Приказ ФСТЭК России №118. Требования по безопасности информации к средствам контейнеризации

Рекомендации

- Получите письмо от руководства о разрешении не ставить антивирус на кластер Kubernetes
- Используйте специализированные контейнерные ОС для хоста
  - Talos, Flatcar Container Linux, Fedora CoreOS, openSUSE MicroOS, Bottlerocket, Container-Optimized OS

- Презентация "Сочетание несочетаемого в Kubernetes: удобство, производительность, безопасность", HighLoad++ 2022

#2 Сканирование хостовой ОС на Nodes кластера на известные уязвимости в пакетах

Основания

- Прописано в общем корпоративном стандарте информационной безопасности

- Предотвратить компрометацию Node через известные уязвимости

Последствия

- Огромные отчеты об уязвимостях с большим количеством false positive-результатов

- Огромное количество времени, потраченное дорогими инженерами на митинги и мало эффективную работу

Реальная жизнь

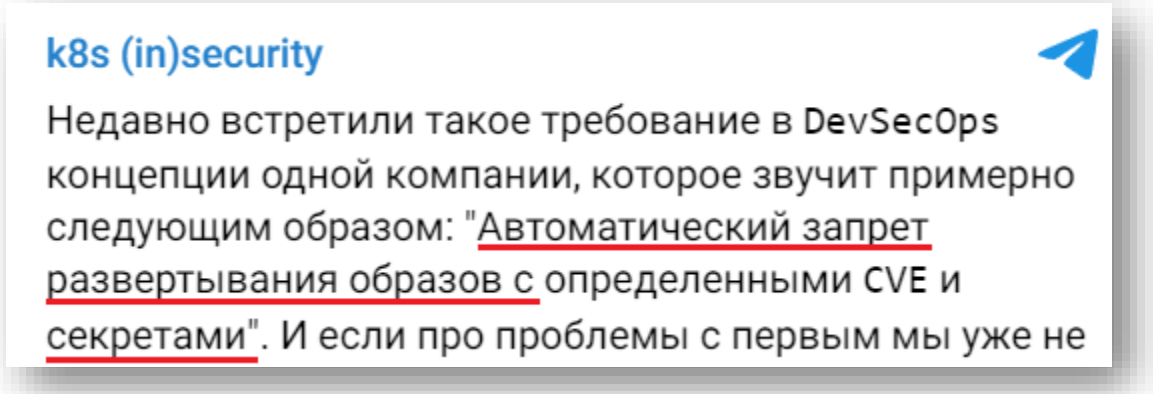
- Контейнеры используют пакеты из образа, а не с хоста
- Сценарии с запусков ПО вне контейнеров на Node – это другой класс проблем
  - Node Allocatable фича для kubelet
- На Node кластера и без уязвимостей хватает векторов
  - Container Runtime Socket
  - сертификаты, ServiceAccount Token, Envs и т.д.
- Разработчики платформы Kubernetes не рассматривают сценариев взаимодействия человека с Nodes
  - продакшн-окружение с чувствительной информацией
  - специальные операторы
  - kubectl debug

Рекомендации

- Создавайте и анализируйте для своего кластера:
  - модель угроз (threat modeling)
  - поверхность атаки (attack surface)
  - модели нарушителя (threat actors)
- Используйте специализированные контейнерные ОС для хоста
  - Talos, Flatcar Container Linux, Fedora CoreOS, openSUSE MicroOS, Bottlerocket, Container-Optimized OS
- Обновляйте ядро ОС

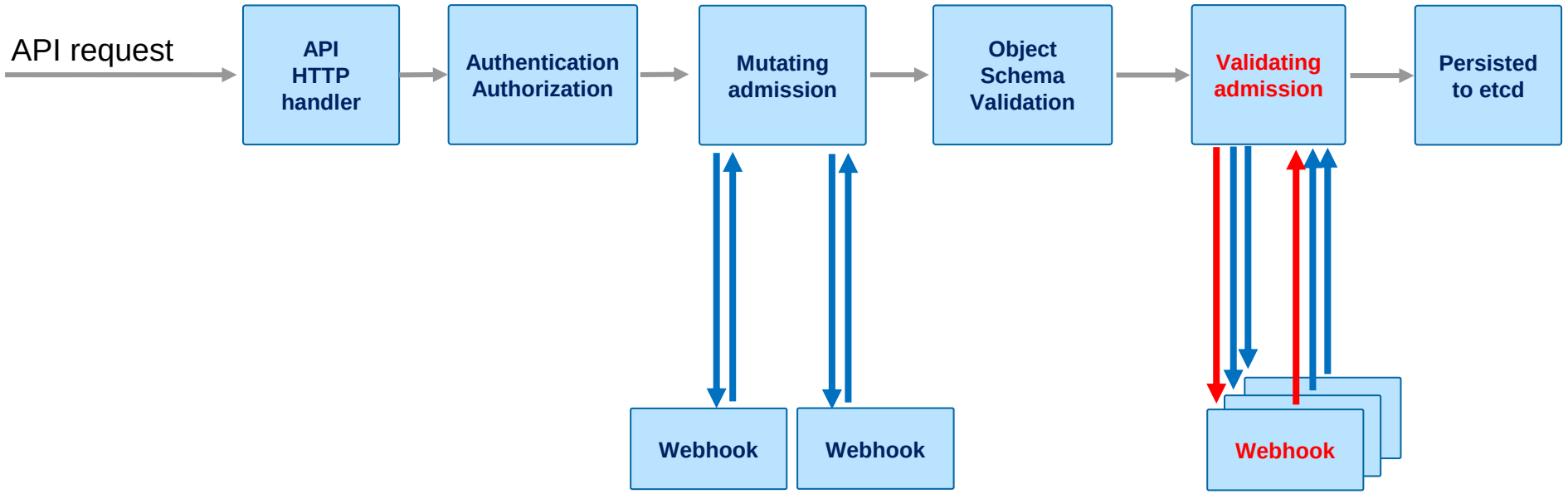
- Презентация "Сочетание несочетаемого в Kubernetes: удобство, производительность, безопасность", HighLoad++ 2022

#3 Блокировка выкатки образов с чувствительной информацией



Основания

- Не допустить утечки критичной информации
  - На validating admission webhook провести проверку и при необходимости заблокировать выкатку



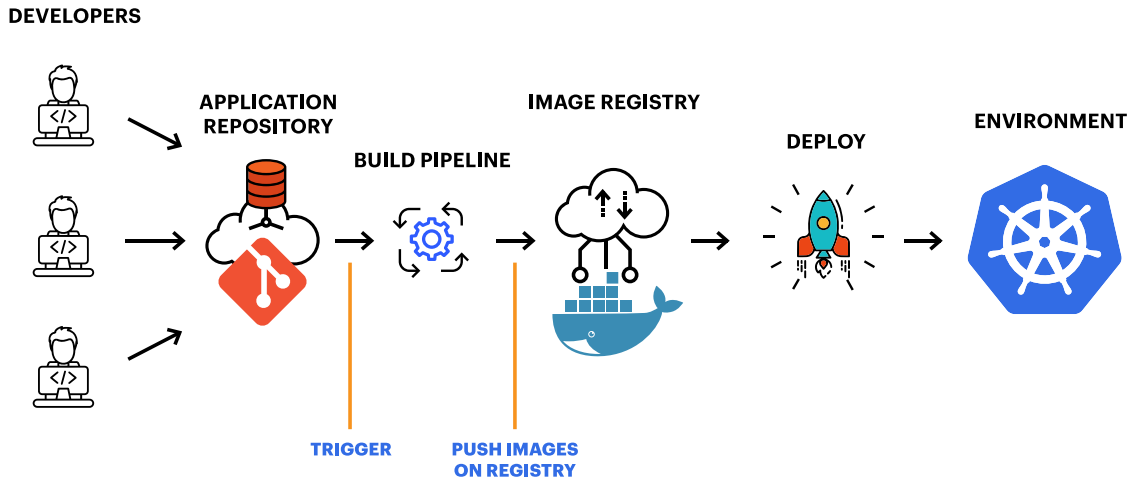
Последствия

- Срывы релизов

- Продолжение утечки критичной информации

Реальная жизнь

- Критичная информация может находиться только в промежуточном слое образа
  - В runtime для внешнего атакующего недоступна
- Критичная информация в образе уже лежит в Image registry
  - Любой сотрудник с pull может извлечь ее
  - Это уже инцидент, требующий отзыва и ротации данных

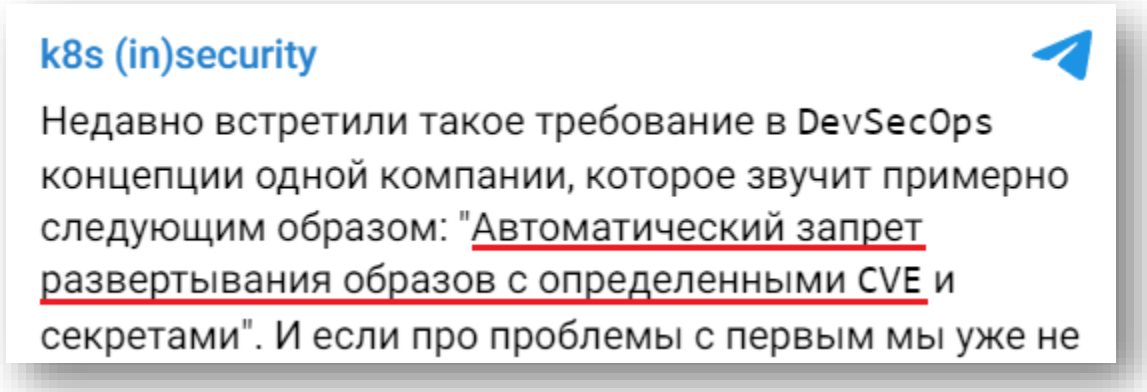


Рекомендации

- CI/CD pipeline должен падать при обнаружении чувствительной информации в слоях образа
- CI/CD pipeline должен завершаться шагом подписи образа
- На validating admission webhook (Policy Engine) должна быть проверка подписи образа
- Используйте registry staging

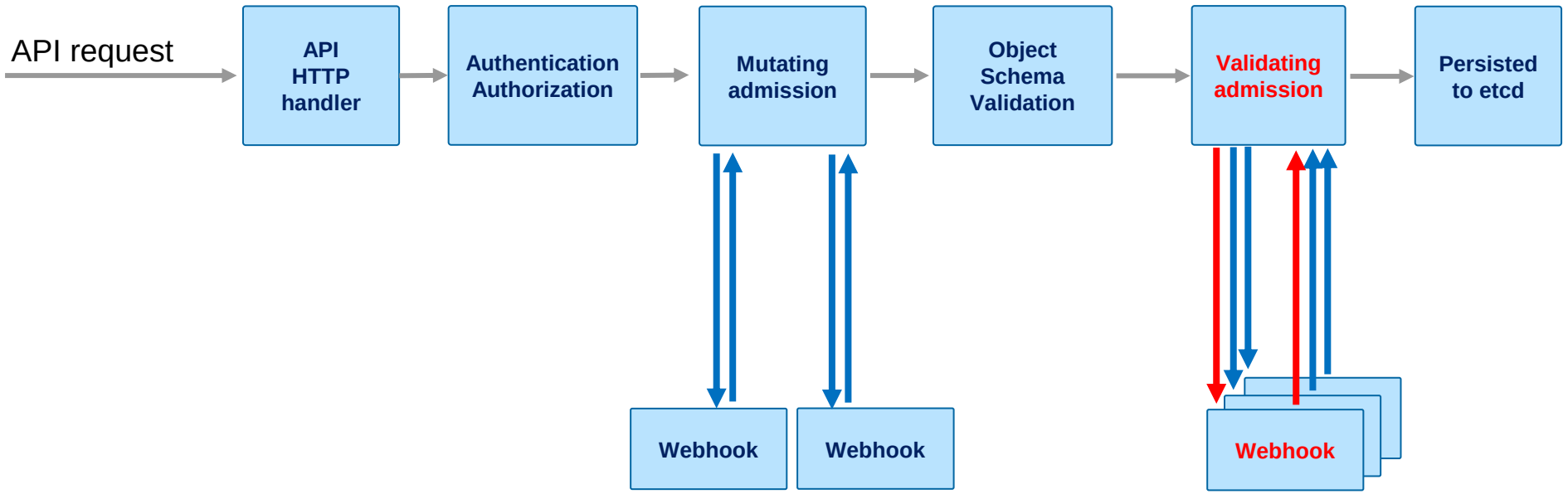
- Презентация "Классификация и систематизация средств безопасности для Kubernetes", CyberCamp MeetUp 2023

#4 Блокировка выкатки образов на основании информации об уязвимостях



Основания

- Не допустить появления в окружении определенных уязвимостей
  - На validating admission webhook провести проверку и при необходимости заблокировать выкатку



Последствия

- Деградация приложений

- Аварийное завершение приложений

- Отказ в обслуживании

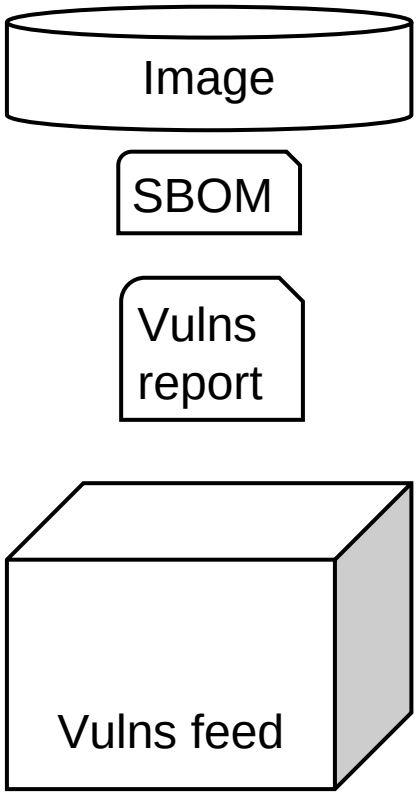
Реальная жизнь

Шаг 1

Infra

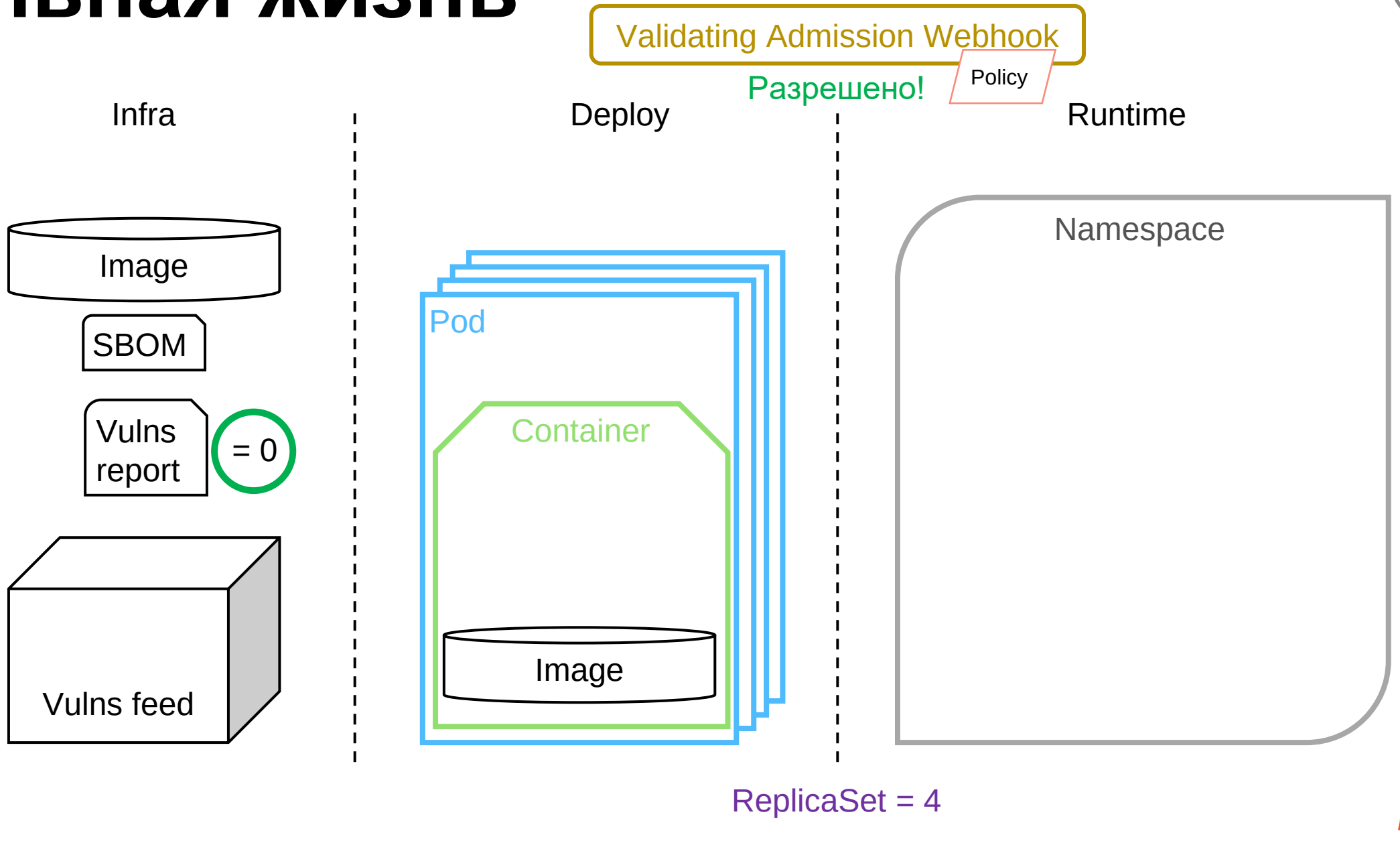
Deploy

Runtime



Реальная жизнь

Шаг 1



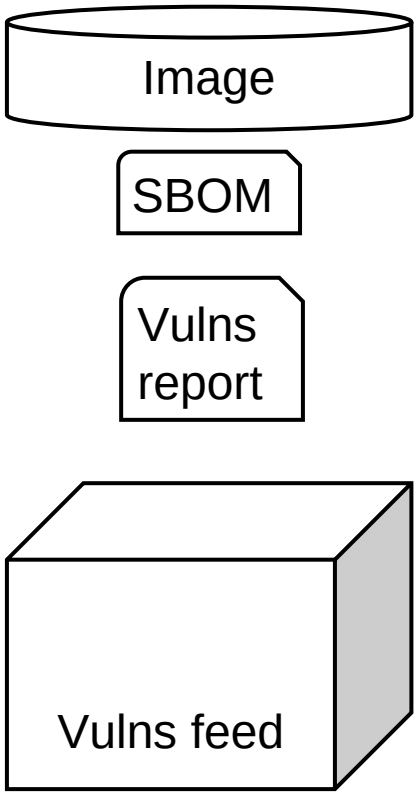
Реальная жизнь

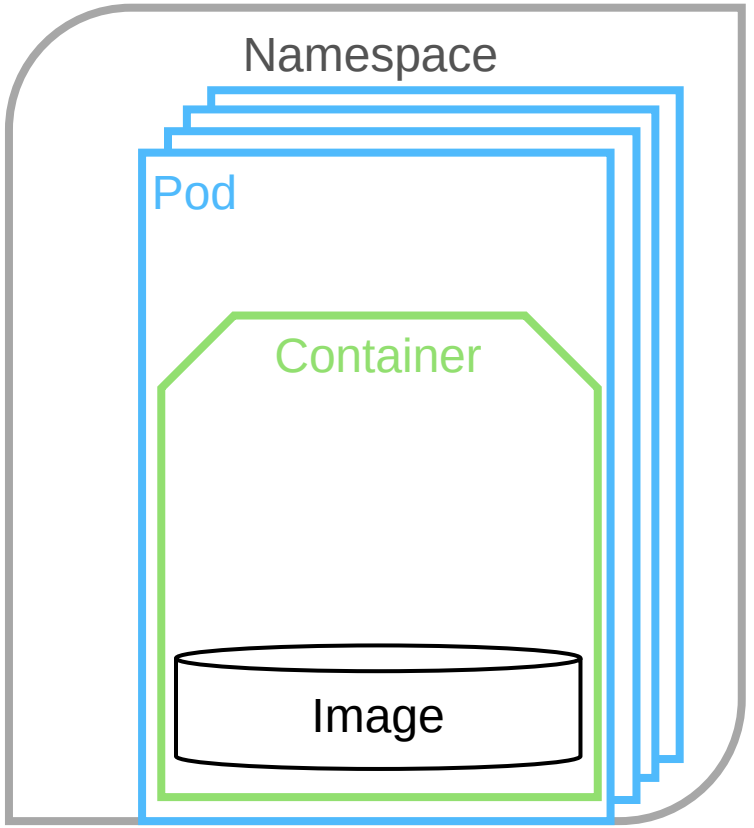
Шаг 2

Infra

Deploy

Runtime





ReplicaSet = 4

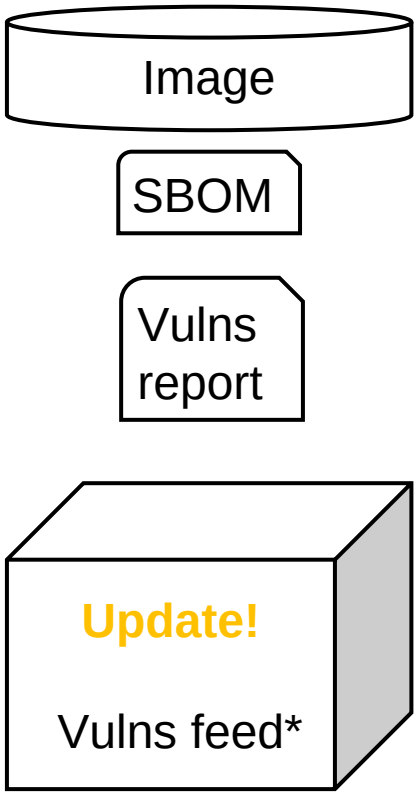
Реальная жизнь

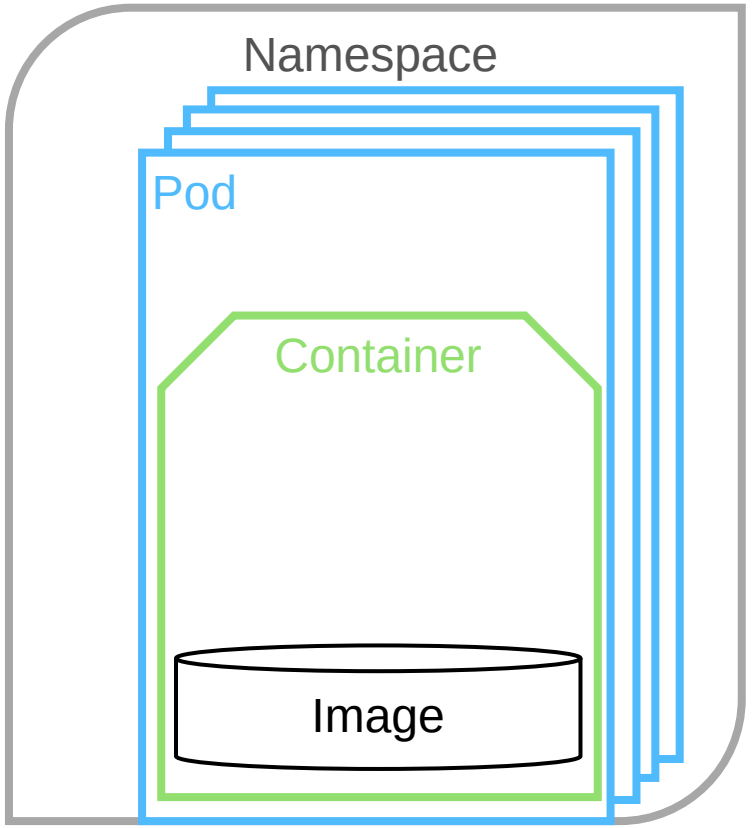
Шаг 3

Infra

Deploy

Runtime





ReplicaSet = 4

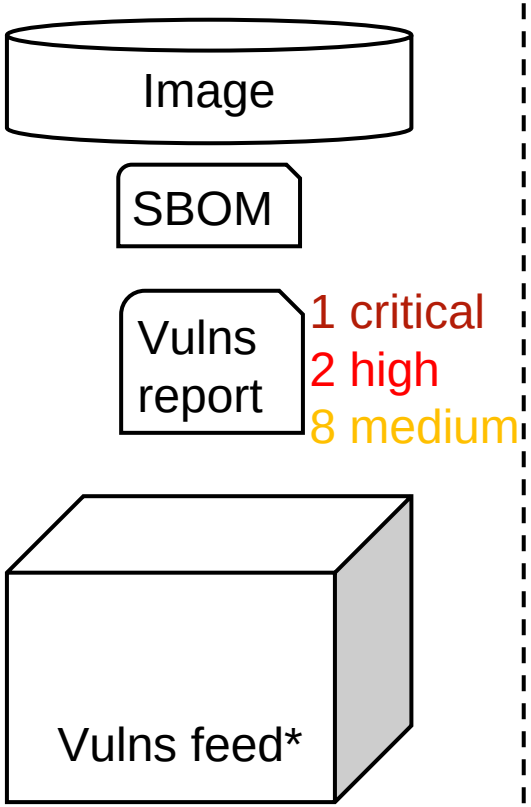
Реальная жизнь

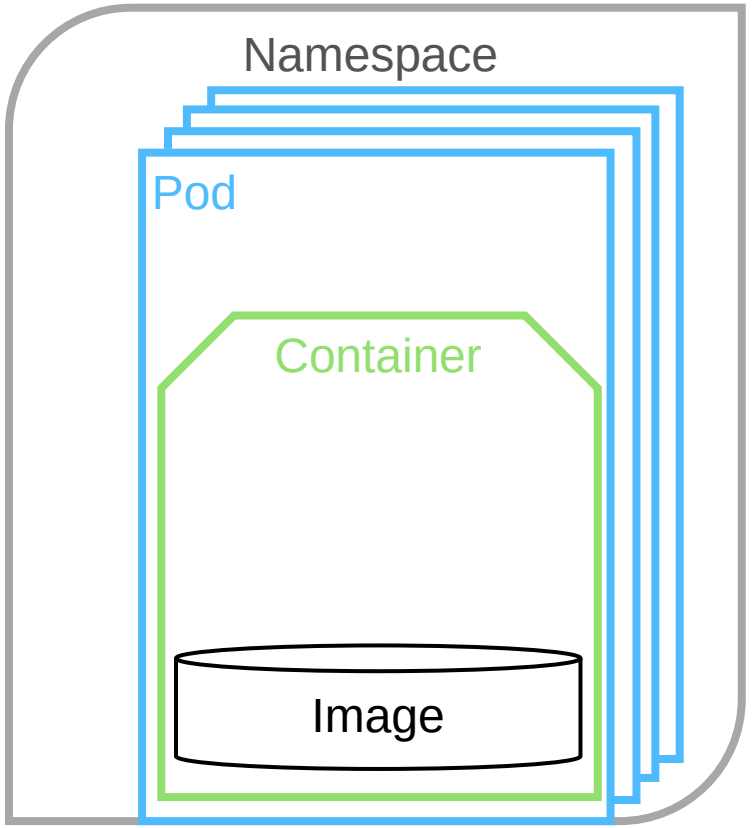
Шаг 4

Infra

Deploy

Runtime

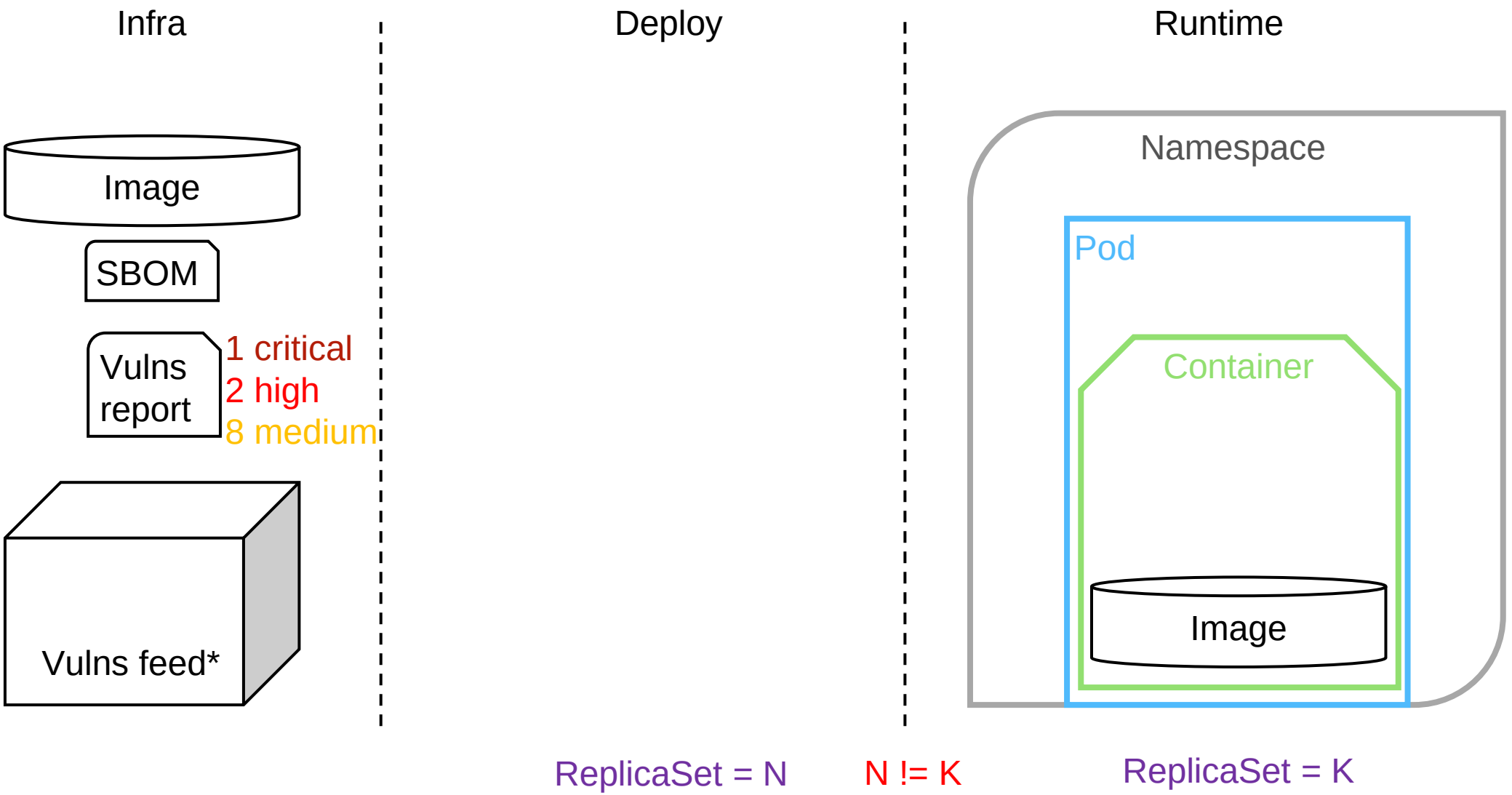




ReplicaSet = 4

Реальная жизнь

Шаг 5



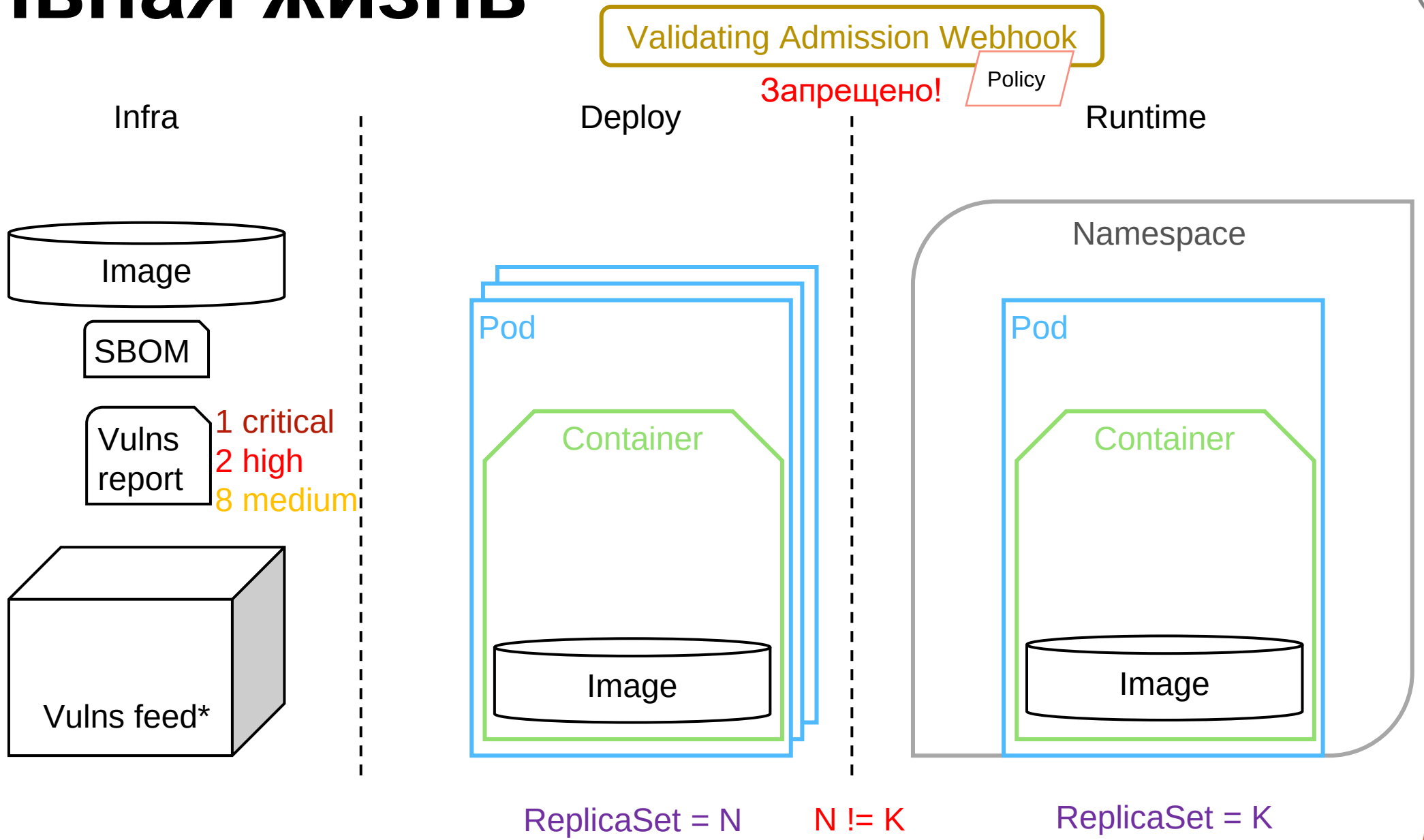
Реальная жизнь

Шаг 5

- Изменение количества Pods в Runtime:
  - Аварийное завершение по OOM
  - Упала Node и переезд Pods
  - Обновление Node и переезд Pods
  - Были вытеснены с одной Node на другую
  - Обновление Secret в переменных окружения
  - Обновили описания Deployment
  - Сработал autoscaler
  - …

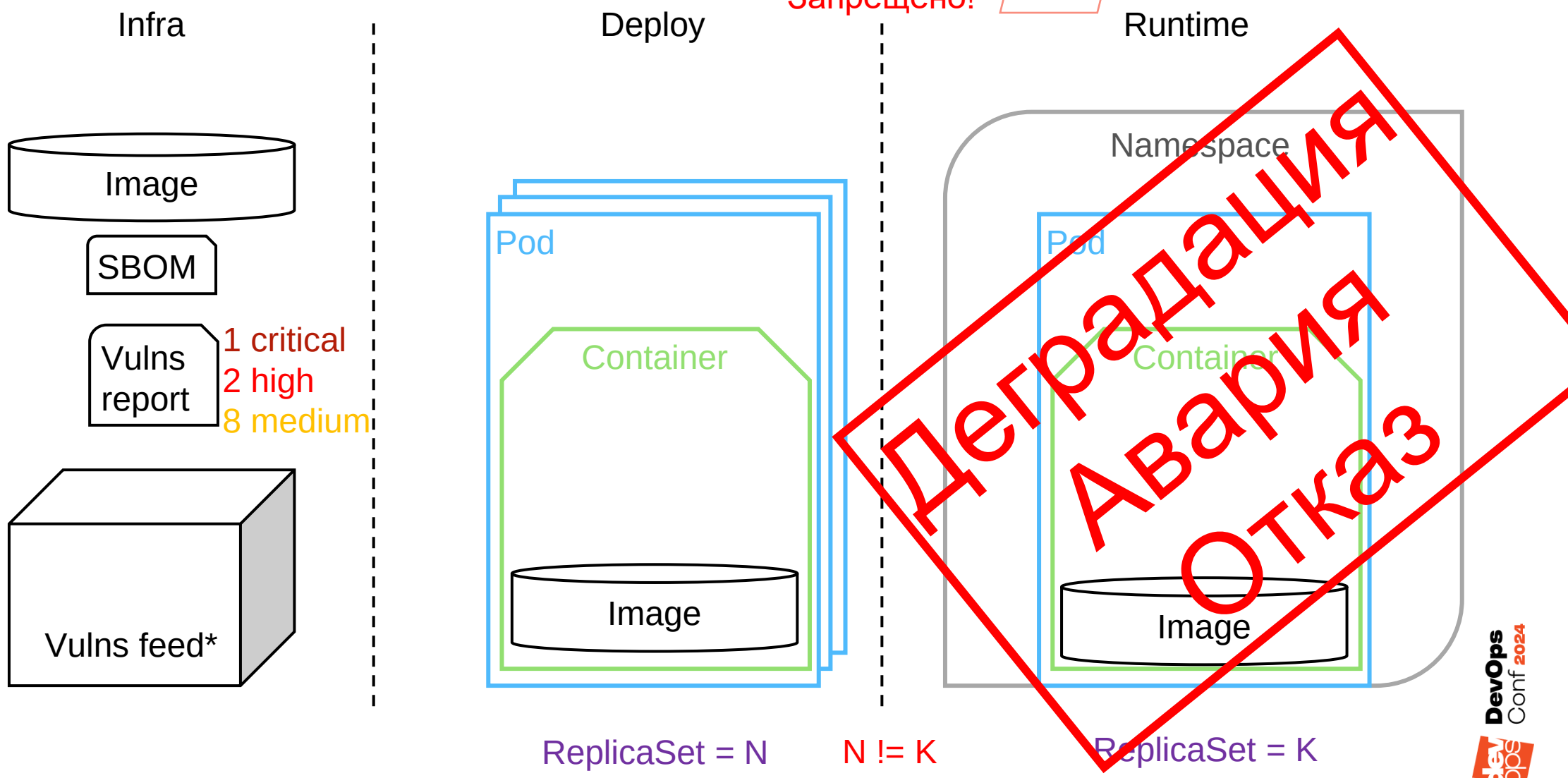
Реальная жизнь

Шаг 6



Реальная жизнь

Шаг 7



Рекомендации

- Нужно знать обо всех уязвимостях не на выкатке, а в любой момент времени
- Уменьшайте поверхность атаки
  - Distroless-образы, минималистичные образы и т.д.
- Стройте ZeroTrust
  - NetworkPolicy, AppArmor и т.д.

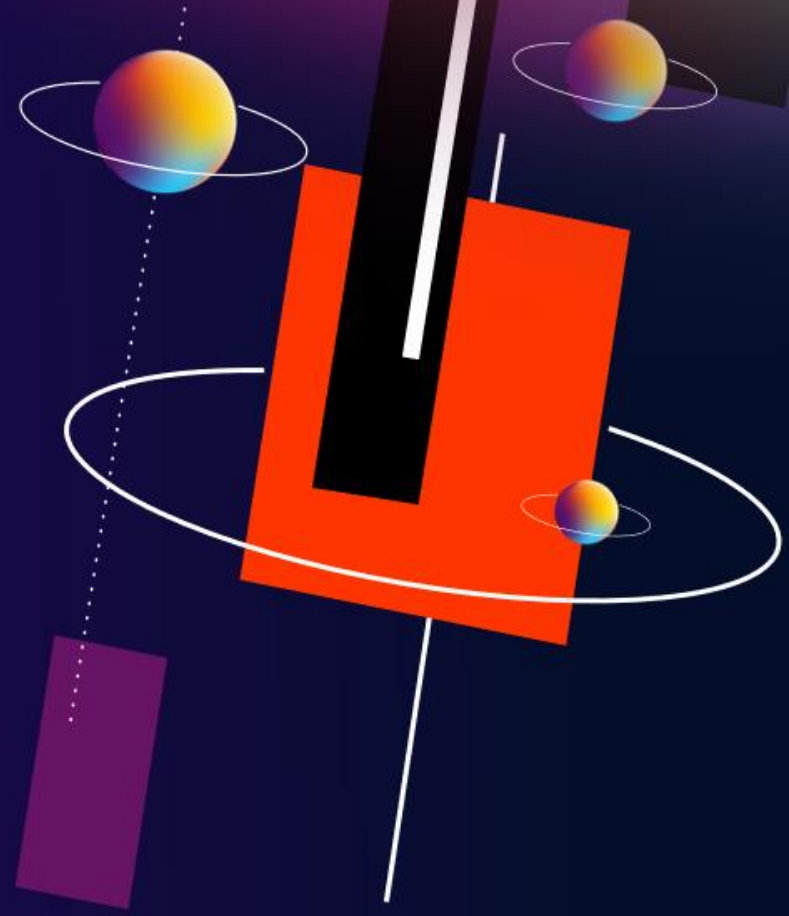
- Презентация "SCAзка о SCAнерах", Positive Hack Days 12
- Презентация "Patch management не поможет, фиксики не спасут"

#N и много других

- Установка N штук агентских средств ИБ на Node
- Множество блокирующих admission controllers
- Повсеместная блокировка на PolicyEngines
- Написание NetworkPolicy вручную или на текущих данных network flow
- Использование black-list-правил для Runtime Security с автоматической реакцией
- …

Заключение

Краткие итоги



DevOps Conf 2024

Выводы

- Учитывайте специфику оркестратора Kubernetes
- Безопасность не должна вредить эксплуатации
- Учитывайте модели нарушителя и поверхность атаки
- Правильная архитектура и подходы решают 90% проблем

Спасибо за внимание!

Дмитрий Евдокимов

Founder & CTO Luntry

Email: de@luntry.ru

Twitter: @evdokimovds

Personal: @Qu3b3c

Channel: @k8security

Site: www.luntry.ru

DevOps Conf 2024