Deckhouse
ФЛАНТ

Pod Security Standards — только начало

Как выстроить полноценную модель безопасности в Kubernetes

Deckhouse
ФЛАНТ

Игорь Бужин

Инженер Deckhouse Академии, «Флант»

Чем занимаюсь:

Разрабатываю и провожу курсы
по продуктам экосистемы Deckhouse

Опыт:

- 2016 — научный сотрудник в области информационной безопасности, преподаватель
- 2024 — автор курсов, в том числе «Инструменты безопасности в DKP» (Deckhouse Академия)

О чём поговорим

01 **Стандарты безопасности в Kubernetes:** стандартов много, единого инструмента нет

02 **Почему защита от побега из контейнера так важна:** примеры побега из контейнера

03 **Как ограничивать контейнер:** Security Context

04 **Pod Security Standards:** что это такое и почему их недостаточно

05 **Инструменты для безопасности подов в DKP:** OperationPolicy и SecurityPolicy

06 **Демо:** как применять политики безопасности подов на реальном кластере DKP

О компании «Флант»

Deckhouse
ФЛАНТ

17+
лет опыта
в Open Source

С 2017
года используем
Kubernetes в production

№1
контрибьютор в проекты
CNCF из России

500+
сотрудников

>260
компаний-пользователей

В топе
вендоров ИТ-решений для банков*
и промышленности**

Реестр
российского ПО

Лицензии и сертификат
ФСТЭК России

АРПП
«Отечественный софт»

* Рейтинг «Крупнейшие ИТ-вендоры в банках», TAdviser, 2024
** Рейтинг «Крупнейшие ИТ-вендоры в промышленности», TAdviser, 2024

ФЛАНТ

Синергия опыта вендора, интегратора, сервисной и консалтинговой компании

Deckhouse

Deckhouse — продуктовое подразделение, разработчик продуктов для построения надёжной enterprise-инфраструктуры

DaaS

DaaS — комплексное DevOps-сопровождение инфраструктуры в режиме 24/7 силами выделенной DevOps-команды

Express 42

«Экспресс 42» — DevOps-консалтинг. От анализа узких мест в ИТ-процессах до создания роадмапа изменения ИТ для реализации цифровой трансформации

Deckhouse Academy

Учим построению стабильной и надёжной ИТ-инфраструктуры на базе эффективного использования продуктов экосистемы Deckhouse

Deckhouse Академия

deckhouse.ru/academy

Обучение даёт необходимые знания и навыки для:

- построения надёжной и стабильной ИТ-инфраструктуры на основе Deckhouse Kubernetes Platform
- эффективной эксплуатации платформы и управления ею
- обеспечения безопасности
- разработки и построения процессов CI/CD

Программы обучения включают:

- онлайн-лекции, вебинары
- видеолекции
- демонстрацию работы
- Q&A-сессии
- лабораторные работы в персональном кластере в сопровождении инструктора
- разбор реальных кейсов участников

Deckhouse Академия

deckhouse.ru/academy

Практико-ориентированные курсы:

Администрирование Deckhouse Kubernetes Platform

Установка и обновление, встроенные модули, управление узлами, пользователями и доступами, control plane

40 академических часов

Использование Deckhouse Kubernetes Platform: запуск и администрирование приложений

Базовые сущности и механизмы Kubernetes, запуск, настройка и публикация приложений, организация доступа

47 академических часов

Инструменты безопасности в Deckhouse Kubernetes Platform

Механизация угроз, политика безопасности, механизмы распределения прав и управления секретами, аудит кластера

42 академических часа

Бесплатный курс для клиентов и партнёров:

Возможности и инструменты Deckhouse Kubernetes Platform

Доступ к курсу для всех клиентов DKP включён в гарантийную техническую поддержку без дополнительной оплаты в рамках действующей лицензии

Сертификация администратора DKP:

Администратор Deckhouse Kubernetes Platform

Экзамен, проверяющий навыки установки и настройки Deckhouse Kubernetes Platform

Deckhouse
ФЛАНТ

Pod Security Standards — только начало

Как выстроить полноценную модель безопасности в Kubernetes

Стандарты безопасности и модель 4C

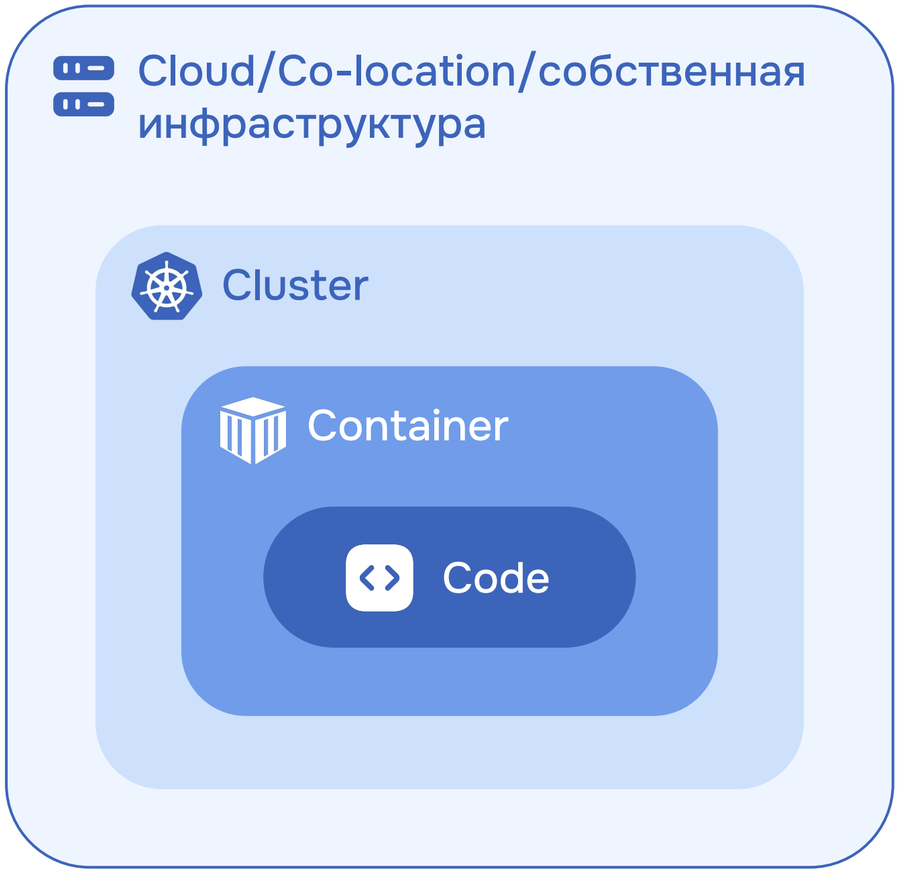
01 Принципы Zero Trust, **NIST SP 800-207**

02 Application Container Security Guide,
NIST SP 800-190

03 OWASP Top 10 Kubernetes Risks

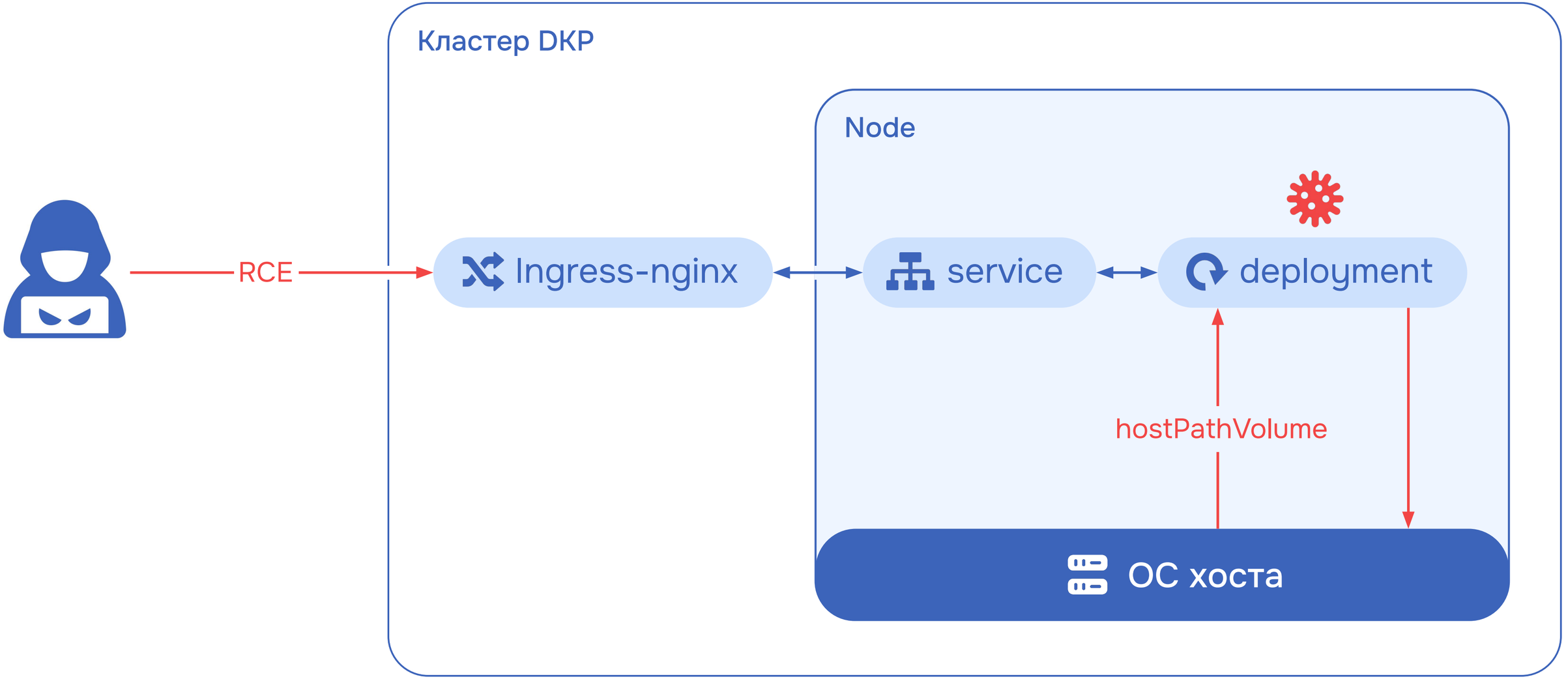
04 MITRE, Containers Matrix

05 Требования по безопасности информации
к средствам контейнеризации
(приказ ФСТЭК России от 4 июля 2022 г. № 118)



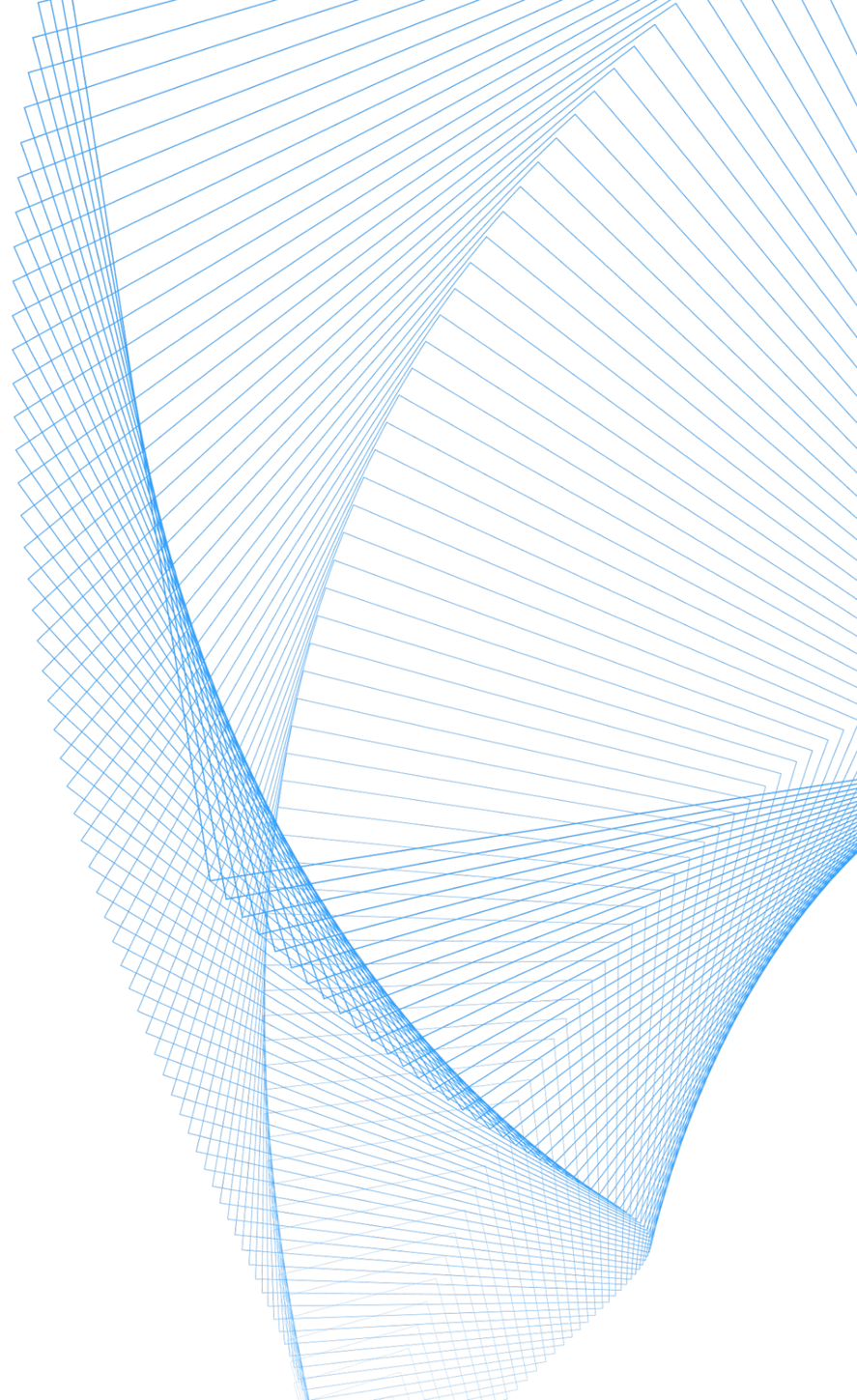
Побег из контейнера

Если реализовать Remote Code Execution, далее можно эксплуатировать уязвимости в приложении



Как митигировать такие атаки?

- Ограничивать привилегии
  и контролировать доступы контейнера
- Валидировать запускаемые поды
  на соблюдение правил безопасности

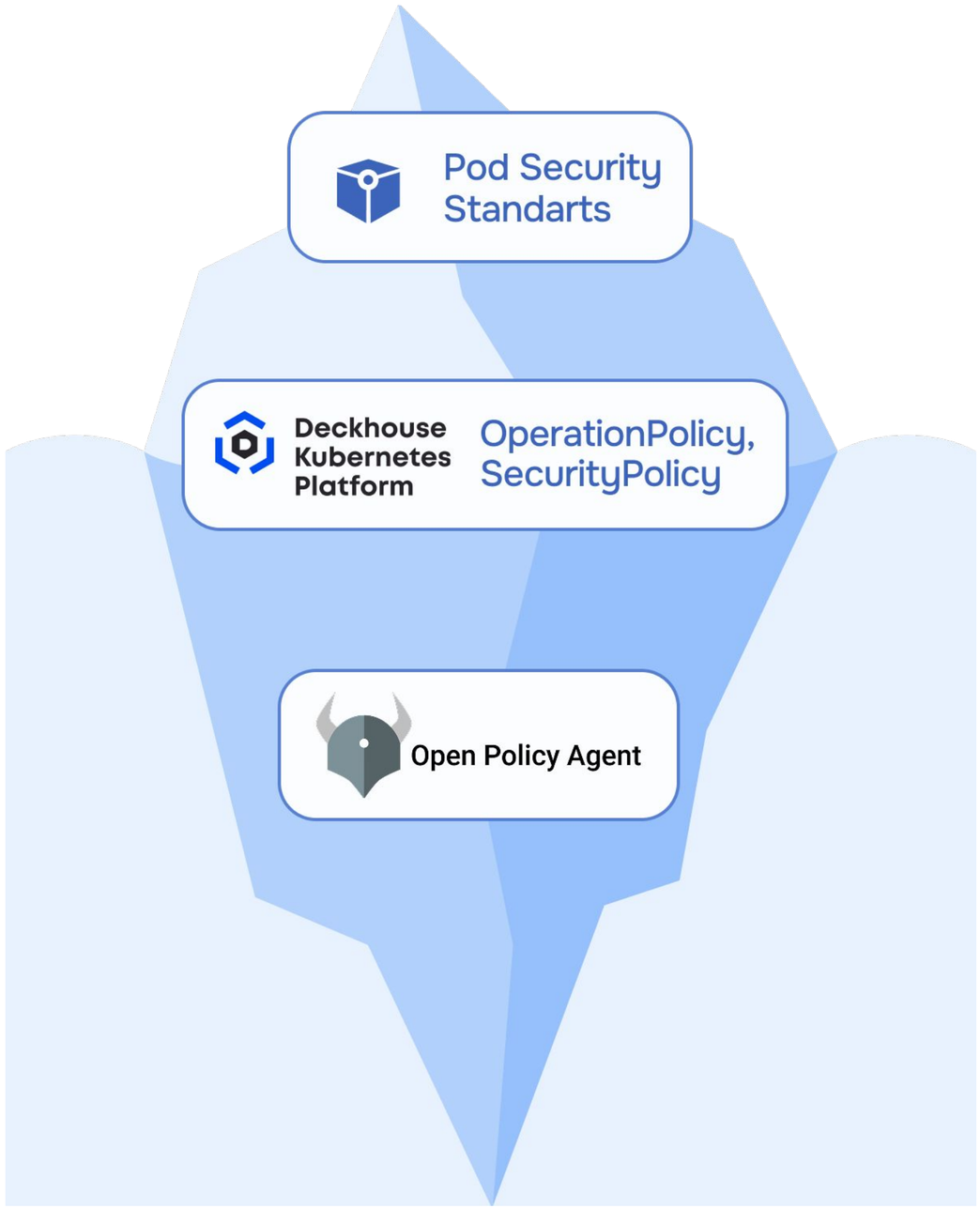


Security Context

На уровне пода и на уровне контейнера	Только на уровне пода	Только на уровне контейнера
appArmorProfile	fsGroup	allowPrivilegeEscalation
runAsGroup	fsGroupChangePolicy	capabilities
runAsNonRoot	supplementalGroups	privileged
runAsUser	supplementalGroupsPolicy	procMount
seLinuxOptions	sysctls	readOnlyRootFilesystem
seccompProfile		
windowsOptions		

Политики безопасности подов в DKP

- Использование готовых Pod Security Standards
- Настройка CRD (OperationPolicy, SecurityPolicy)
- Создание собственных политик — OPA Gatekeeper



Pod Security Standards

Privileged

Нет ограничений
(все поды в пространствах имён привилегированные)

Baseline

Политика по умолчанию в DKP

Запрет на:

- hostProcess=true
- Host Namespaces
- privileged=true

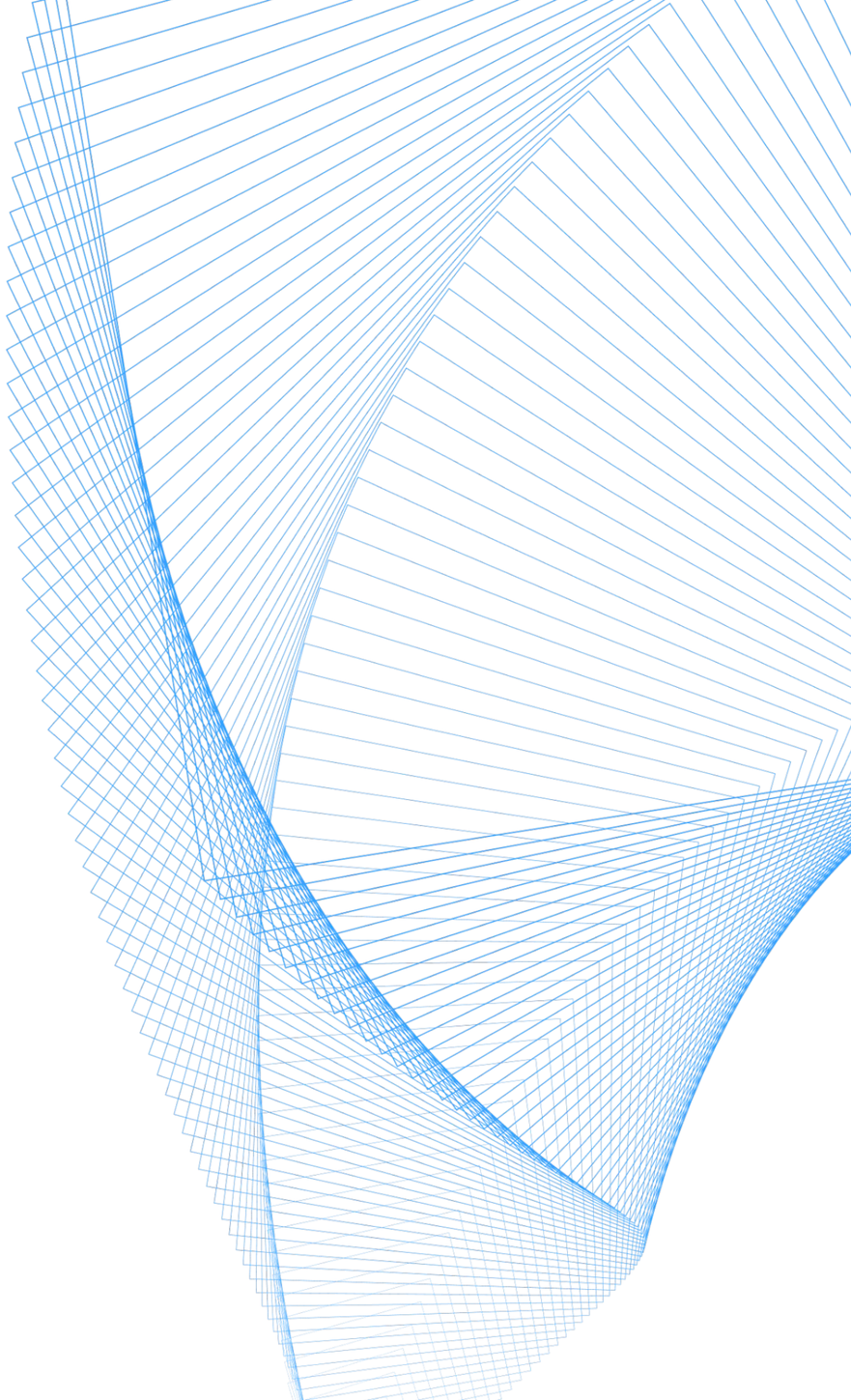
Если нет SecurityContext, то ок

Restricted

Обязательное наличие:

- SecurityContext
- Privilege Escalation=false
- runAsNonRoot=true

А если нужны дополнительные ограничения?



Сложный вариант: Gatekeeper

Шаблон проверки

```
kind: ConstraintTemplate
spec:
  crd:
    spec:
      names:
        kind: K8sAllowedRepos
<Правила создания расширения (кастомного ресурса)>
  targets:
    <Правила создаваемого ресурса>
```

Ресурс Constraints

```
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sAllowedRepos
spec:
  match:
    kinds:
 <Для каких API группы и kind применять>
    namespaceSelector:
<Лейбл для активации политики>
  parameters:
<Параметры проверки>
```

security.deckhouse.io/pod-policy=restricted

Пример targets на языке Rego в ConstraintTemplate

```
targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package d8.pod_security_standards.extended
violation[{"msg": msg}] {
      container := input.review.object.spec.containers[_]
      satisfied := [good | repo = input.parameters.repos[_] ; good = startswith(container.image, repo)]
      not any(satisfied)
      msg := sprintf("container <%v> has an invalid image repo <%v>, allowed repos are %v",
[container.name, container.image, input.parameters.repos])
    }

    violation[{"msg": msg}] {
      container := input.review.object.spec.initContainers[_]
      satisfied := [good | repo = input.parameters.repos[_] ; good = startswith(container.image, repo)]
      not any(satisfied)
      msg := sprintf("container <%v> has an invalid image repo <%v>, allowed repos are %v",
[container.name, container.image, input.parameters.repos])
    }
```

Простой вариант дополнительных требований

- **OperationPolicy** — позволяет задать типовые эксплуатационные требования без Rego
- **SecurityPolicy** — задаёт кастомные требования к безопасности

Модуль admission-policy-engine

Deckhouse
ФЛАНТ

Live demo

Курс «Инструменты безопасности в Deckhouse Kubernetes Platform»

Что изучите:

- Основы информационной безопасности в Kubernetes и Deckhouse Kubernetes Platform
- Безопасность пода
- Сетевые политики безопасности. Mutual TLS
- Управление доступом
- Управление сертификатами. Хранение и доставка секретов из Stronghold
- Выявление уязвимостей и аудит безопасности в кластере

Курс состоит из:

- Вводной видеолекции
- Онлайн-вебинаров с демонстрацией работы в кластере
- Практической части с выполнением лабораторных работ в реальном кластере DKP

Подробнее о курсе

О преподавателе

Игорь Бужин

Инженер Deckhouse Академии,
«Флант»

- В информационной безопасности — с 2016 года:
  от фундаментальных исследований до живых инфраструктур
- Разработал и запустил магистерскую программу по ИБ,
  вёл программы ДПО, преподаю в магистратуре
- С 2024 года — автор курсов по экосистеме Deckhouse,
  включая «Инструменты безопасности в DKP»

Почему на моих курсах интересно?

- Объясняю сложное просто
- Это практика, которую можно унести с собой
- Строю обучение слоями: от минимальной защиты до полного enforcement.
  Каждый шаг понятен и обоснован

Хотите закрывать уязвимости в Kubernetes, а не искать их?

Освойте все инструменты безопасности в DKP
на реальном кластере со скидкой **25 %**

Напишите промокод **SEC25**
на почту contact@deckhouse.ru **до 28 мая** включительно

Стать экспертом
по безопасности
Kubernetes

+7 (495) 721-10-27

deckhouse.ru