2 ИЮНЯ 2026, МОСКВА, ЛОФТ ГОЭЛРО

БЕКОН LUNTRY '26

ЕДИНСТВЕННАЯ КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ
КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

«Оператор Всевластия» для разработки распределенных систем и управления сетевой безопасностью

Хренов Никита | Альфа-Банк

БЕКОН'26

Оператор Всевластия

для разработки распределённых систем и управления сетевой безопасностью





Никита Хренов

10 лет в ИТ

9 лет в Альфа-Банке,
от разработчика
до системного архитектора

Последние 2 года: технический лидер
дирекции развития и сопровождения
производственных платформ

Сегодня вы узнаете

Зачем эльфам, гномам и людям Platform Engineering

IDP не только Identity Provider

Можно ли просто так взять и создать создать NetworkPolicy

Где искать правду

Удалось ли достичь Всевластия в Альфа-Банке



Средиземье DevSecOps

Сетевая безопасность



Разработка

AaC – structurizr/likec4

Library/SDK/Framework

Угрозы

- Отсутствие единого источника правды
- Разрозненные абстракции
- Сложность инфраструктуры
- Ручные правки манифестов



Безопасность

Kyverno

Calico

Istio

Эксплуатация

Kubernetes

IaC – Terraform/Ansible

Observability – Jaeger/Grafana



Властелин Platform Engineering

« Platform Engineering — это не о замене DevOps. Это о масштабировании DevOps через продуктовый подход»

– Келси Хайтауэр, Google

Ключевые понятия:

- Internal Developer Platform (IDP)
- Self-Service
- Golden Paths
- Abstraction



Властелин Platform Engineering

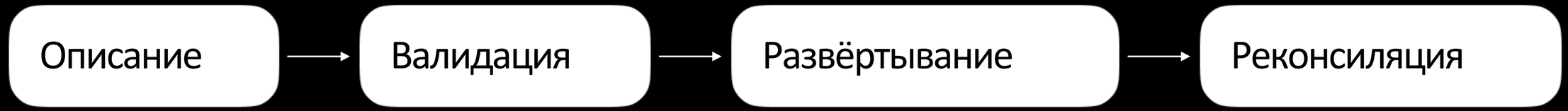
Платформенный инженер Саурон

Цели IDP:

- Ускорить вывод новых функций в продакшн
- Снизить операционный overhead
- Предоставить единый источник правды об устройстве устройстве системы (Everything-as-Code)
- Обеспечить согласованность архитектурных и безопасностных требований на этапе проектирования (Security-by-Design)



Оператор IDP



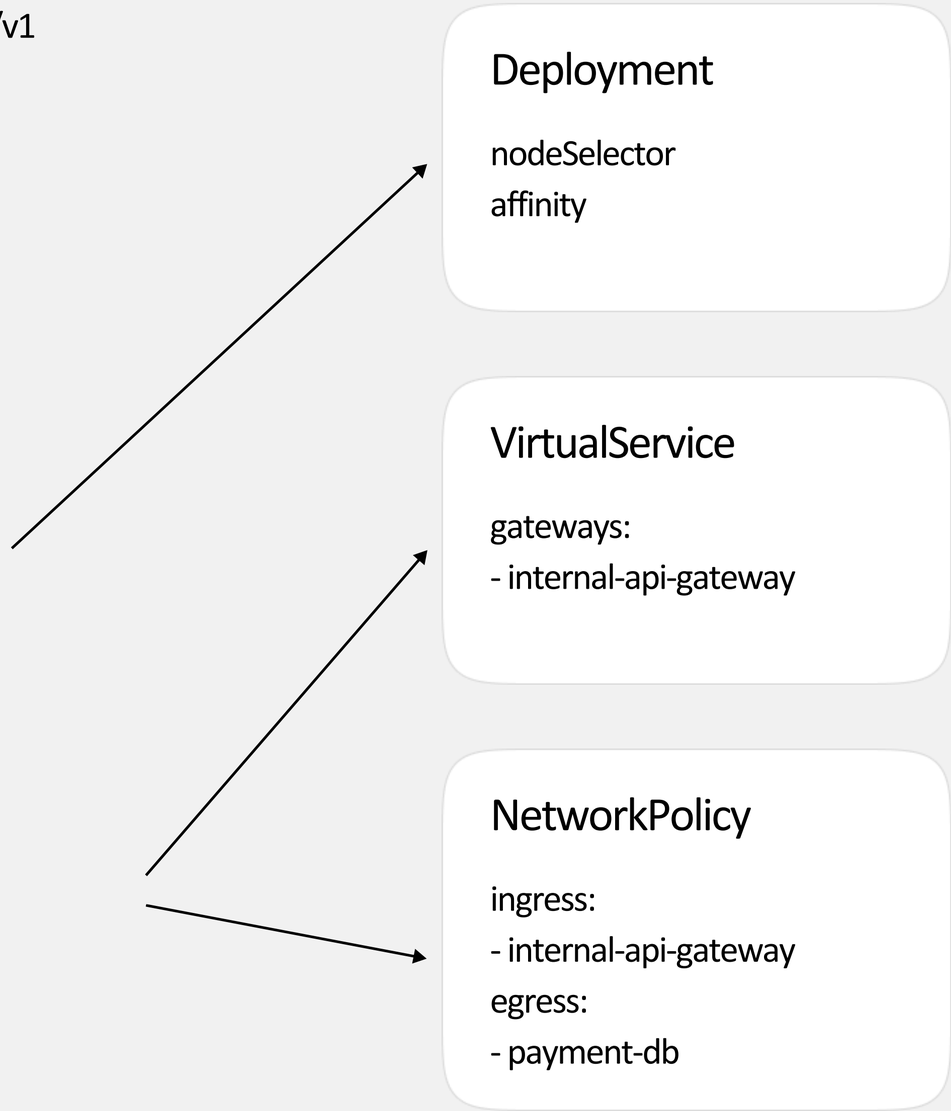
Декларативный подход

- Описание желаемого состояния приложения в виде DSL (YAML)
- Автоматическая реализация на инфраструктуре
- Отслеживание и устранение configuration drift

Custom Resource – «Одна абстракция, чтобы править всеми»

Оператор IDP

```
apiVersion: platform.alpha-bank/v1
kind: Application
metadata:
  name: payment-api
  namespace: payment
spec:
  type: JAVA_API
  image: payment-api:1.4.2
  replicas: 3
  network:
    tier: APP
    segment: PVLAN
  placement:
    isolationLevel: domain
    businessDomain: payment
  exposure:
    public: true
    gateway:
      type: INTERNAL_API_GW
  resources:
    - name: payment-db
      type: postgresql
      ref: prod-cluster
```



Deployment

nodeSelector
affinity

VirtualService

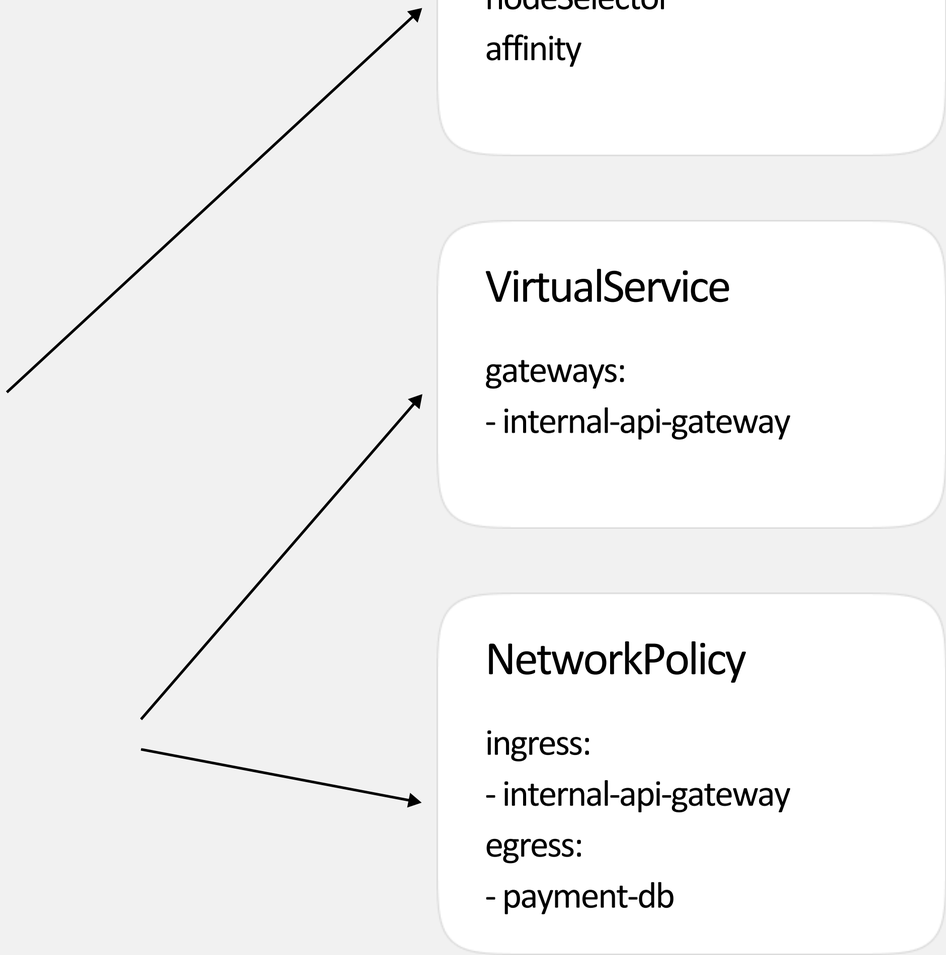
gateways:
- internal-api-gateway

NetworkPolicy

ingress:
- internal-api-gateway
egress:
- payment-db

Оператор IDP

```
apiVersion: platform.alpha-bank/v1
kind: Application
metadata:
  name: payment-api
  namespace: payment
spec:
  type: JAVA_API
  image: payment-api:1.4.2
  replicas: 3
  network:
    tier: APP
    segment: PVLAN
  placement:
    isolationLevel: domain
    businessDomain: payment
  exposure:
    public: true
    gateway:
      type: INTERNAL_API_GW
  resources:
    - name: payment-db
      type: postgresql
      ref: prod-cluster
```



Deployment

nodeSelector
affinity

VirtualService

gateways:
- internal-api-gateway

NetworkPolicy

ingress:
- internal-api-gateway
egress:
- payment-db

Валидация:

- CRD Validation Rules (CEL)
- Validating Admission Webhooks
- Custom Controller Validation

resources.contains(db)
  && network.segment != DMZ

exposure.public
  && gateway.type = INTERNAL_API_GW

  && network.segment = PVLAN

exposure.public ???

Нельзя просто так взять и создать NetworkPolicy

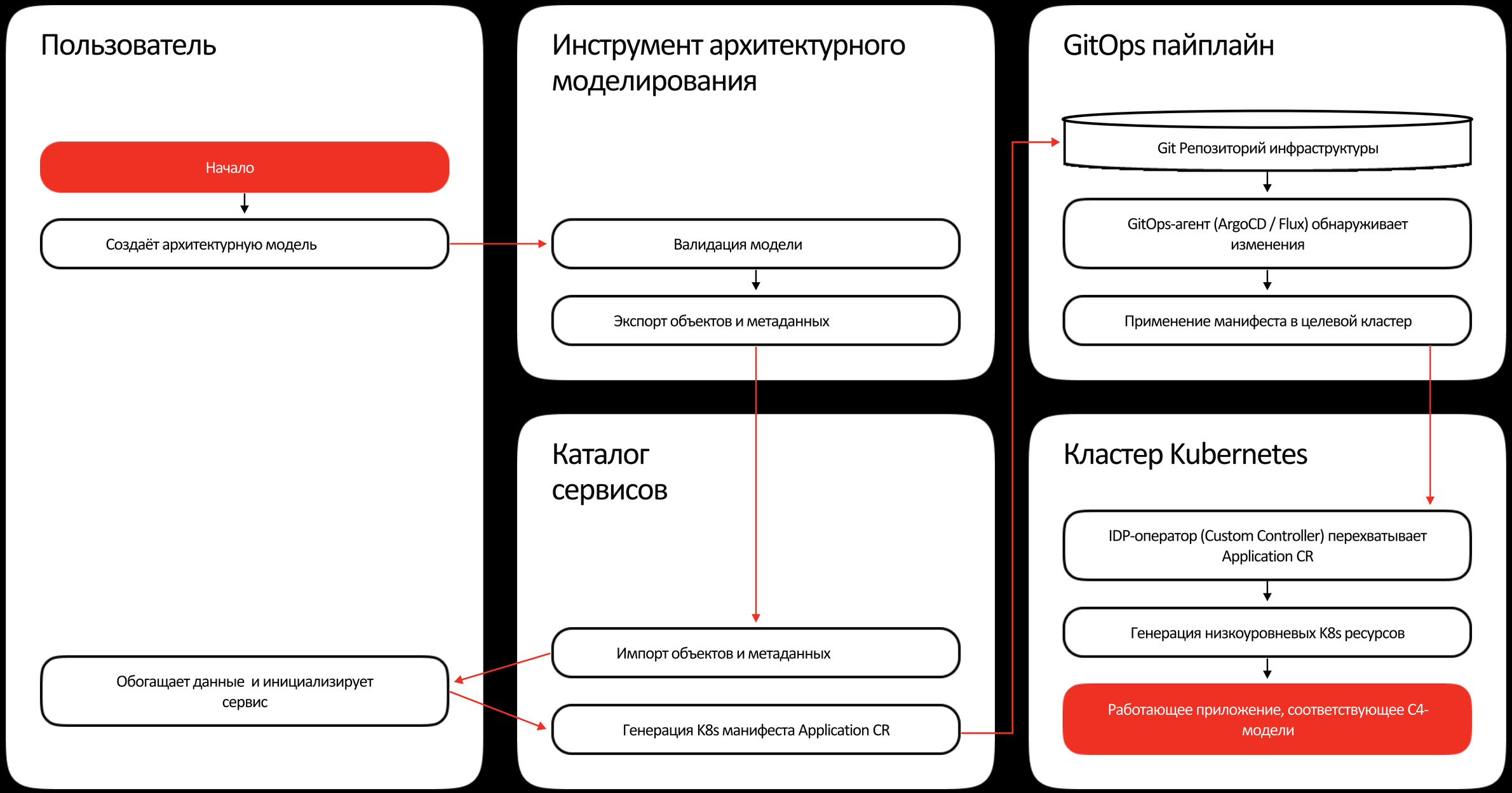
Архитектурная модель C4

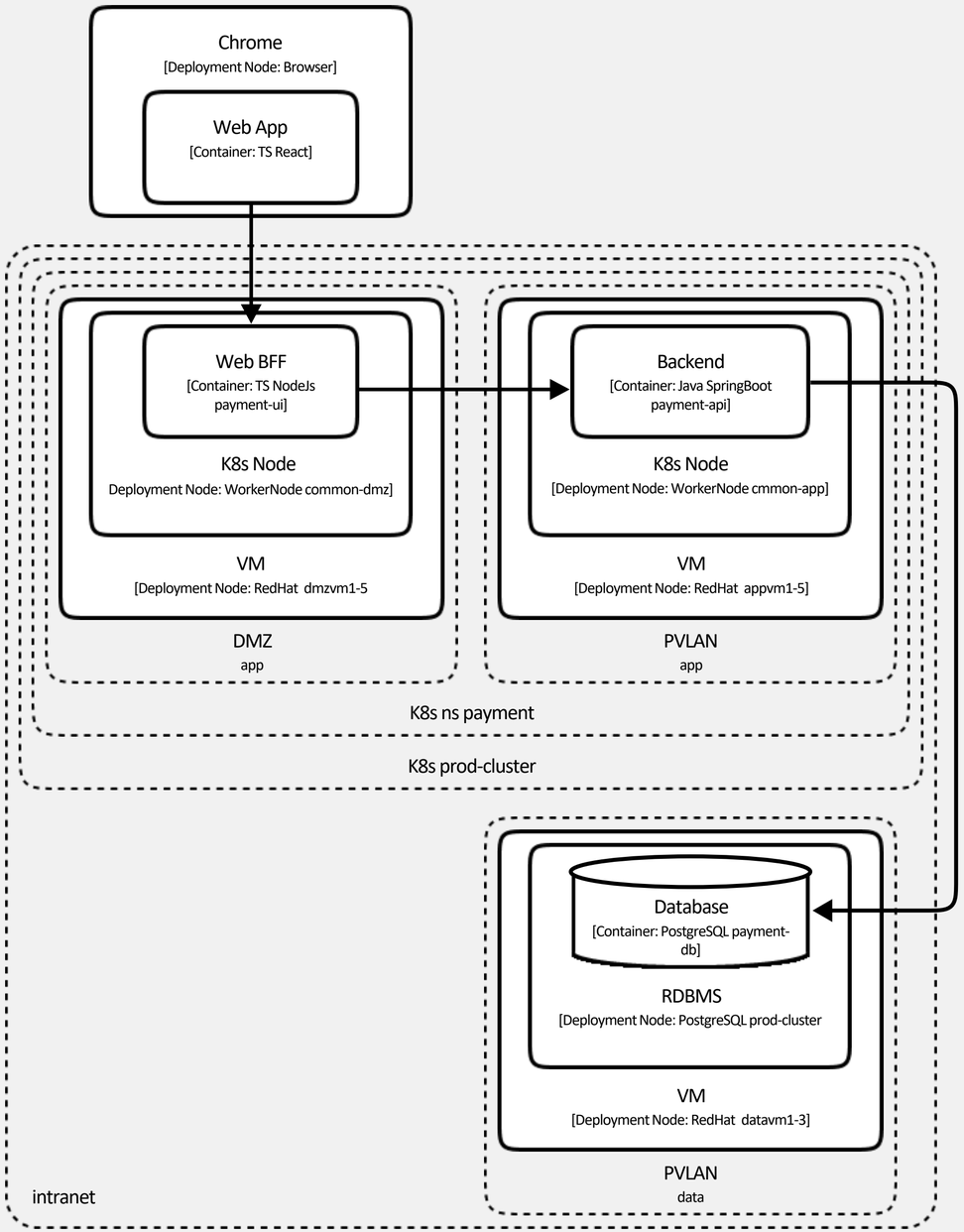
- Статические контекстные диаграммы (C1-2)
- Динамические диаграммы (потоки данных)
- Диаграммы развёртывания (размещение на инфраструктуре)

Инструменты моделирования:

- likeC4
- structurizr
- IcePanel




Пользователь
Начало
Создаёт архитектурную модель
Обогащает данные и инициализирует сервис
Инструмент архитектурного моделирования
Валидация модели
Экспорт объектов и метаданных
Каталог сервисов
Импорт объектов и метаданных
Генерация K8s манифеста Application CR
GitOps пайплайн
Git Репозиторий инфраструктуры
GitOps-агент (ArgoCD / Flux) обнаруживает изменения
Применение манифеста в целевой кластер
Кластер Kubernetes
IDP-оператор (Custom Controller) перехватывает Application CR
Генерация низкоуровневых K8s ресурсов
Работающее приложение, соответствующее C4-модели




```yaml
apiVersion: platform.alpha-bank/v1
kind: Application
metadata:
  name: payment-ui
  namespace: payment
spec:
  type: NODEJS_BFF
  image: payment-ui:1.4.2
  replicas: 3
  network:
    tier: APP
    segment: DMZ
  dependencies:
    - name: payment-api
      type: INTERNAL
```

```yaml
NetworkPolicy

podSelector: payment-ui

ingress:
- ingress-dmz

egress:
- payment-api
```

```yaml
apiVersion: platform.alpha-bank/v1
kind: Application
metadata:
  name: payment-api
  namespace: payment
spec:
  type: JAVA_API
  image: payment-api:1.4.2
  replicas: 3
  network:
    tier: APP
    segment: PVLAN
  exposure:
    public: false
  resources:
    - name: payment-db
      type: postgresq
      ref: prod-cluster
```

```yaml
NetworkPolicy

podSelector: payment-api

ingress:
- payment-ui

egress:
- payment-db
```

Уровни Всевластия

Архитектурная модель + IDP Оператор = Сетевая Безопасность



Оператор + валидации

- Централизованное управление сетевыми политиками
- Источник правды – CR в Git
- Валидация схемы + простейшие бизнес валидации



Инструмент моделирования AaC + + валидация модели + генерация CR

- Источник правды – AaC в Git
- Объекты модели создаются руками
- Валидация моделей - Security-by-Design
- Консистентность модели и ландшафта в рамках happy path



Инструмент моделирования со слоем бизнес логики + PaaS + Discovery

- Источник правды – архитектурная модель
- Объекты модели создаются автоматически из PaaS и Discovery
- Инструмент моделирования реализует golden golden paths - Security-by-Design
- Консистентность модели и ландшафта обеспечивается PaaS и Discovery

Опыт Альфа-Банка

Оператор

- Самописный
  java operator sdk + Spring Boot
- Crossplane
  provider-sql

ArgoCD (GitOps)

Инструмент моделирования

- Самописный на базе модели C4
  Ручные согласования + OPA (GaC)
- uCMDB + самописные агенты (Discovery)

Сложности

Миграция существующих сервисов

Абстракция – компромисс между сложностью
и гибкостью

Версионирование CRD

UI/UX инструмента моделирования



Сегодня мы узнали

Зачем эльфам, гномам и людям Platform Engineering

Platform Engineering реализует
и масштабирует практики DevSecOps

IDP не только Identity Provider

IDP является центральным элементом Platform Engineering

Можно ли просто так взять и создать NetworkPolicy

Нельзя

Где искать правду

Архитектурная модель является единым источником правды для IDP

Удалось ли достичь Всевластия в Альфа-Банке

Ещё нет, но мы стараемся




БЕКОН'26
КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД
@NIKITAKHRENOV