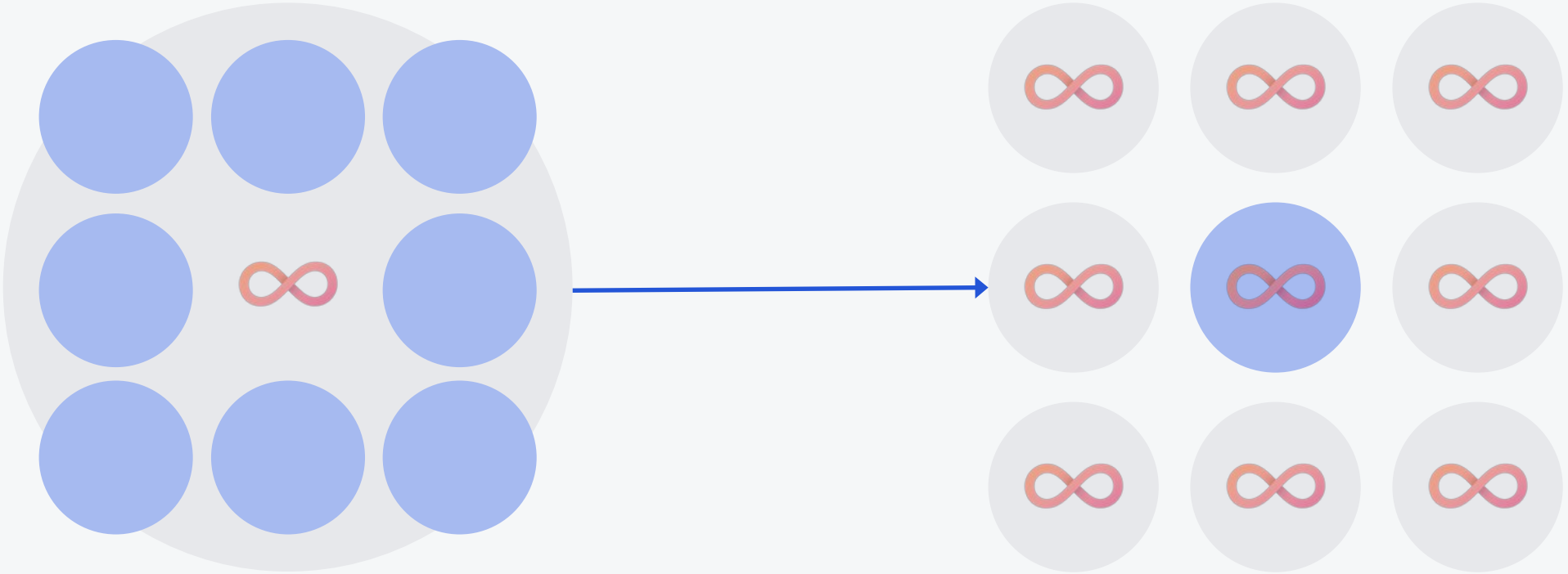
Как мы строили платформу на базе Kubernetes и старались не скатиться в «кубер с аутентификацией»

ГАЗПРОМБАНК

Трансформация и импортозамещение. Что происходит?



- Большая автоматизированная система
- Большая команда
- Много банковских продуктов

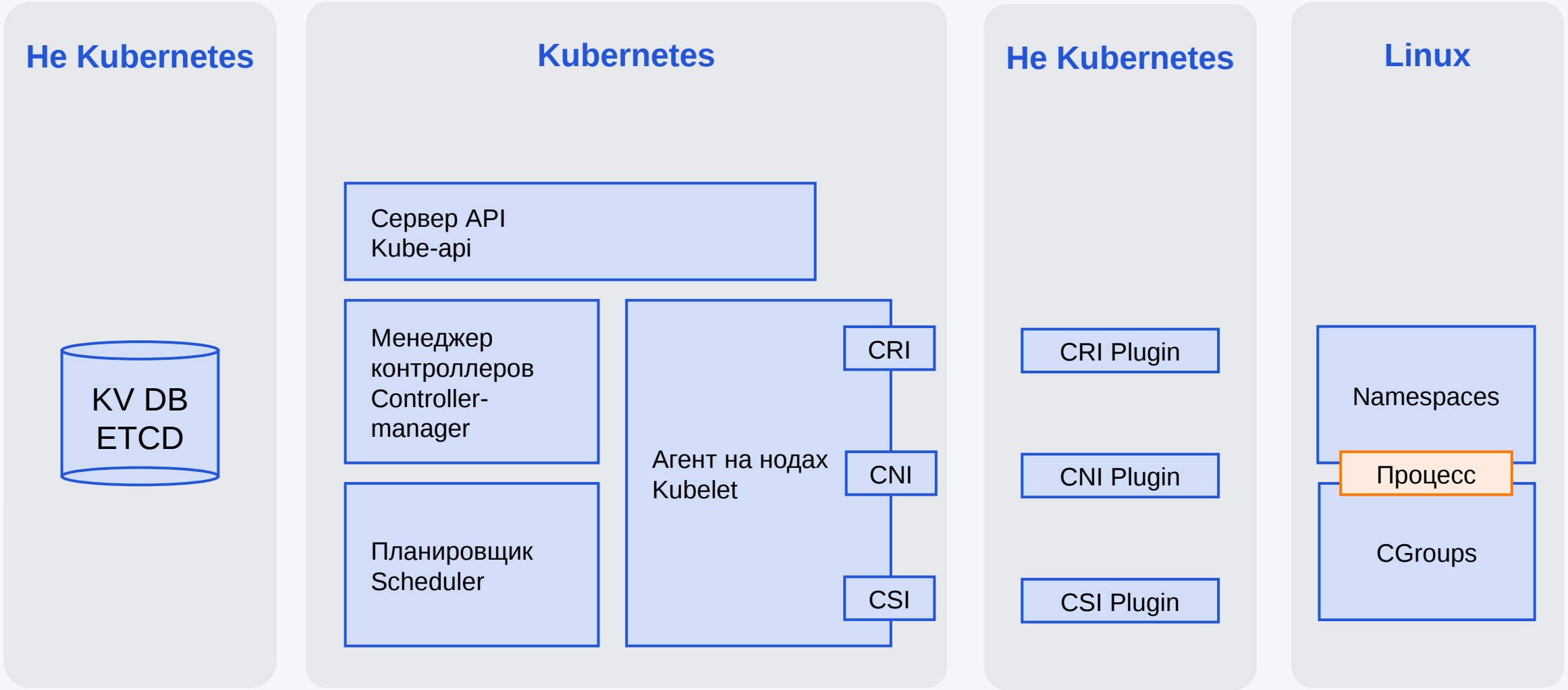
- Команды отвечают за свои банковские продукты
- Есть платформа, которая отвечает за глобальные сервисы

Как обеспечить техническую сторону трансформации?
CI / CD и Kubernetes

И что нужно понимать, когда собираешься внедрять Kubernetes:

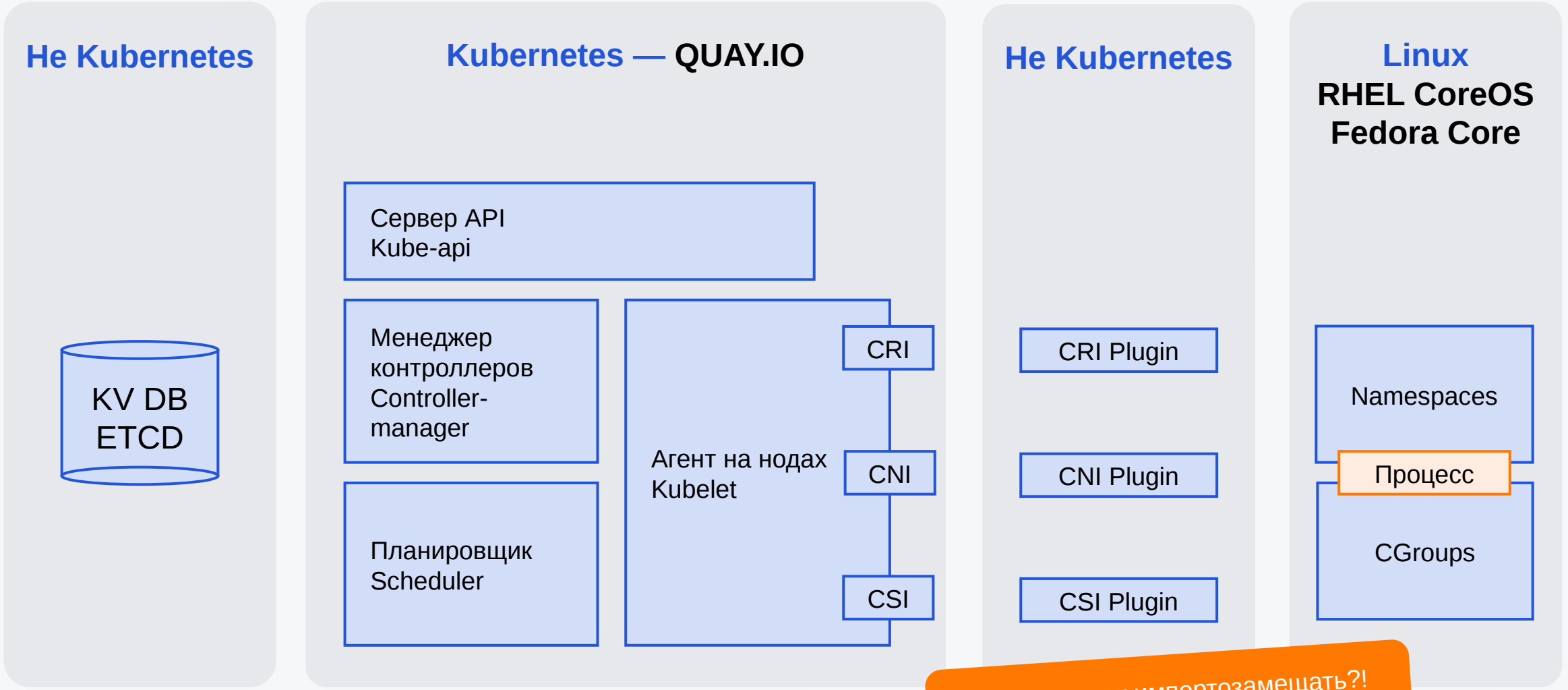
1. Kubernetes «из коробки» — не готовая платформа, скорее заготовка для создания платформ
2. Kubernetes, в первую очередь, дает набор задокументированных API
3. Еще Kubernetes «из коробки» дает ряд базовых сервисов, которые обеспечивают жизненный цикл сущностей внутри кластера
4. На самом деле Kubernetes не умеет даже запускать контейнеры

Kubernetes – заготовка



Openshift – платформа от Red Hat

Openshift и OKD



Строим свою платформу

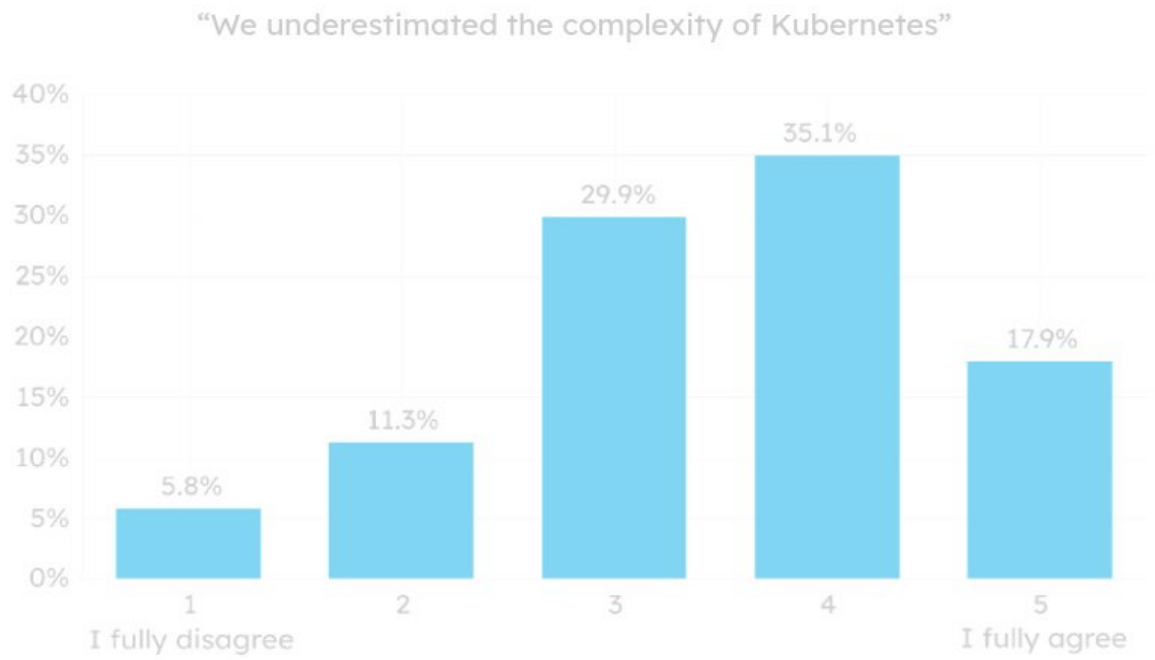
Какие вызовы задача кидает лиду команды внедрения Kubernetes

- Как обеспечить потребности бизнеса в обеспечении платформой новой организационной структуры
- Как обеспечить безопасность на платформе
- Как взаимодействовать с инфраструктурой
- Декомпозиция задач и проработка архитектуры

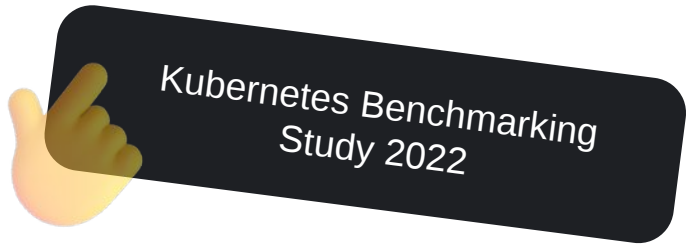
Тезисы после пройденного пути

- Создание платформы, ДАЛЕКО, не тоже самое, что Kubernetes с аутентификацией на 1-2 команды
- Если инфраструктура заточена под другое, придется в платформе оказывать очень много услуг. Будь готов к бесконечным интеграциям

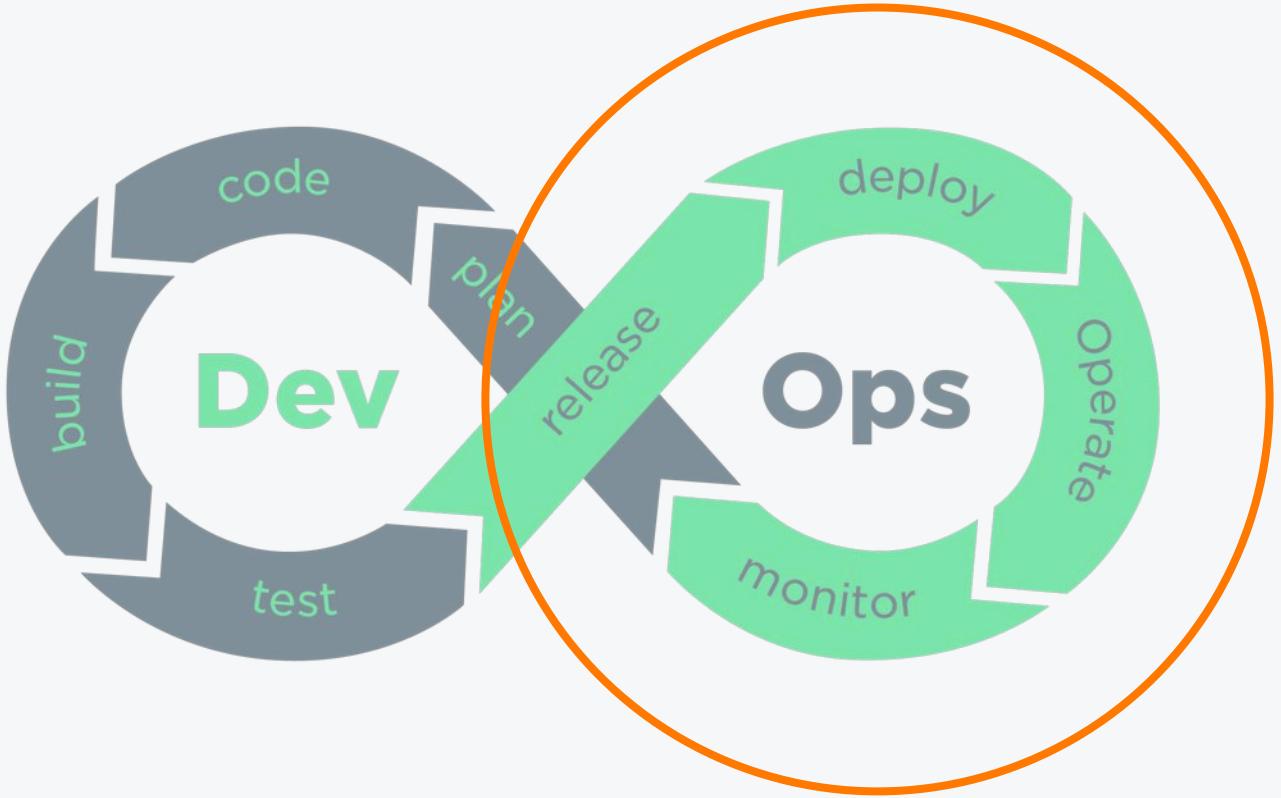
Строим свою платформу на базе Kubernetes. Не стоит недооценивать сложность



Over 53% of respondents (>3 on a scale from "fully disagree" = 1 to "fully agree" = 5) state they underestimated the complexity of Kubernetes. What's even more interesting, there's only a small difference between low and top performers (~± 3%). The majority of high performers actually agree they too have underestimated the difficulty of rolling out K8s.



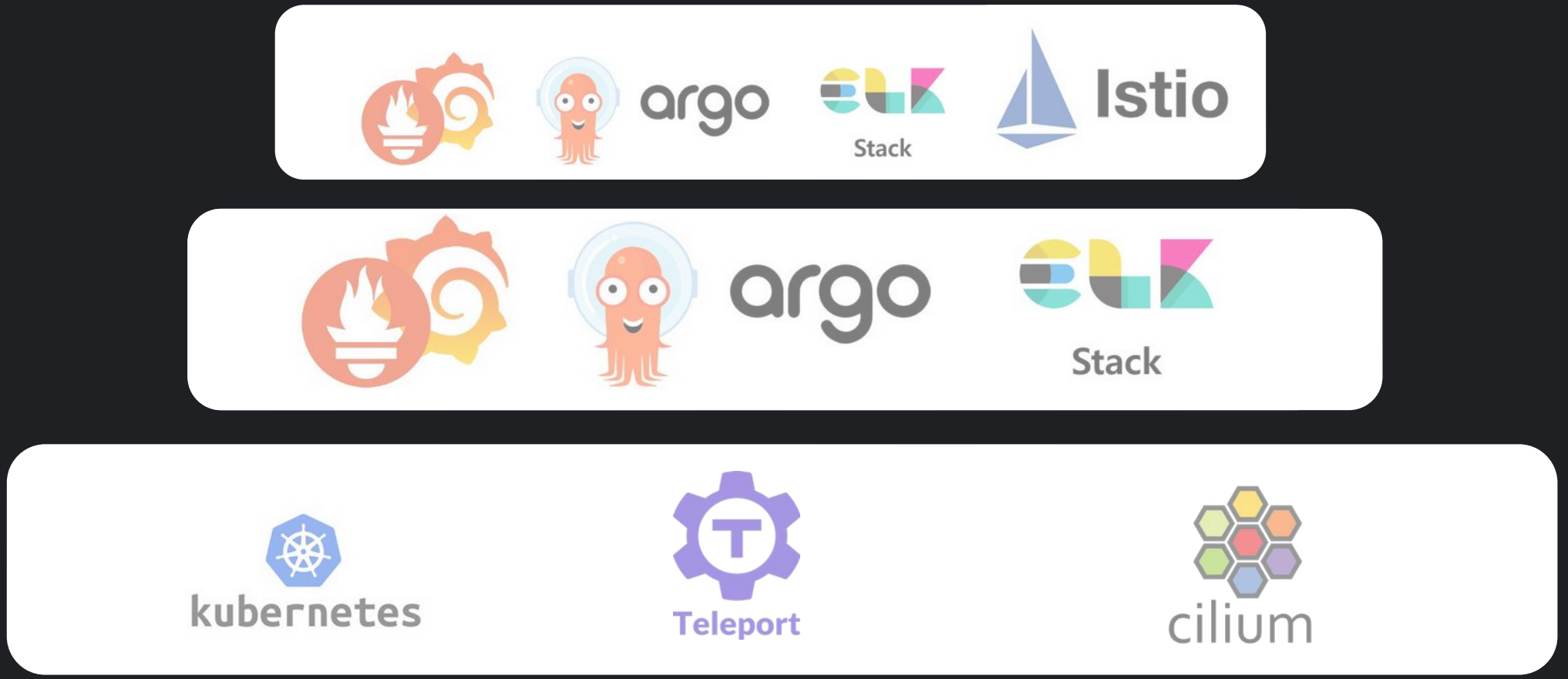
Наш кусок DevOps «Уробороса»



Тезисы после пройденного пути

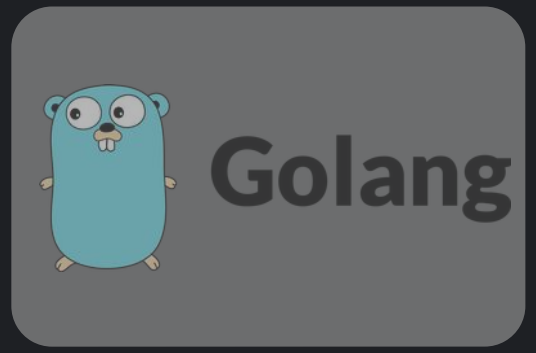
- Кластеры имеют предназначение
- Состав сервисов в тенанте зависит назначения кластера
- Важно понимать предназначение кластера, чтобы строить приоритеты по сервисам

Наша итоговая «пирамида Маслоу»



Четко разделяем платформу на слои. Разбираемся какие компетенции нужны

Какой уровень команды нужен



Тезисы после пройденного пути:

- Нужна команда «единорогов»
- В команду нужны люди с высоким уровнем soft-skills
- Лид должен подогревать интерес, всех членов команды

Безопасность. Наше все

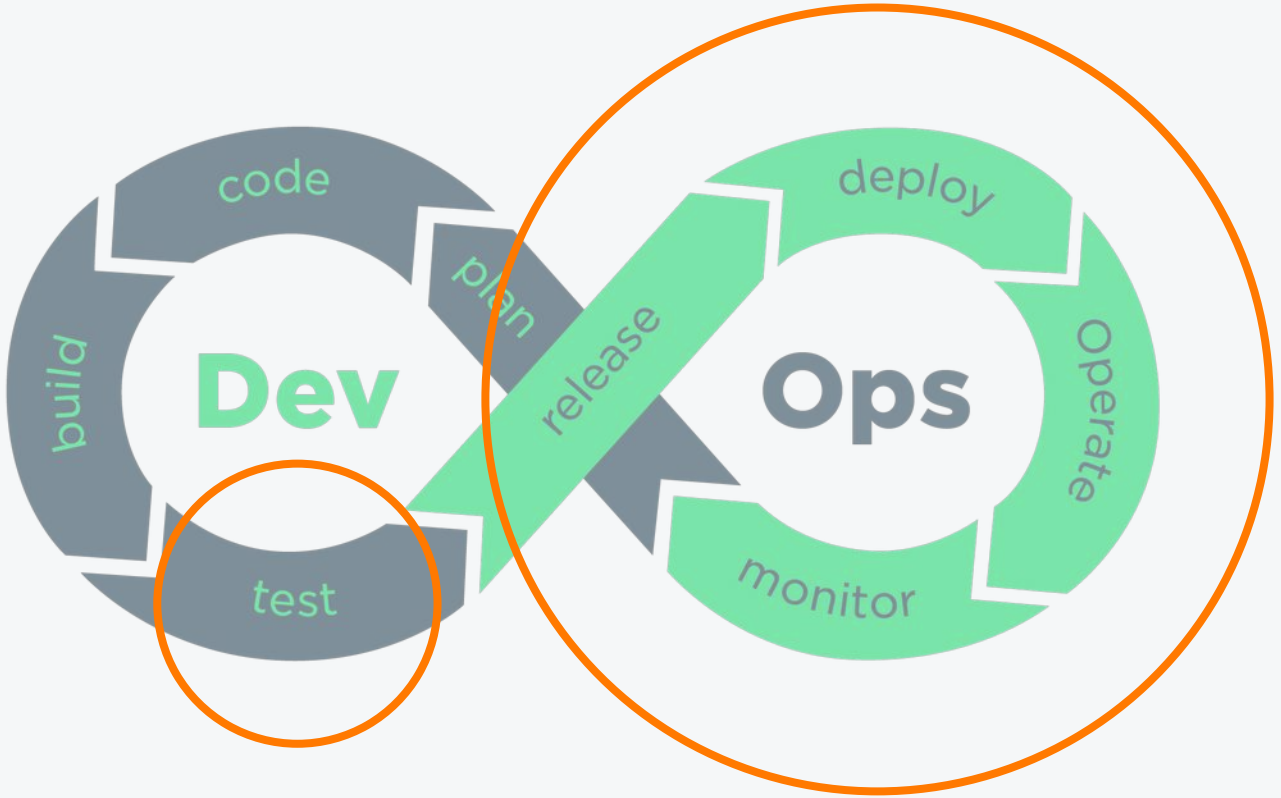
Тезисы после пройденного пути:

- Нужна команда «единорогов»
- В команду нужны люди с высоким уровнем soft-skills
- Лид должен подогревать интерес, всех членов команды

Средствами Teleport мы строили изоляцию теннантов
и ролевую модель команд

Средствами Cilium мы решали вопросы сетевой безопасности.
Самое важное — Egress IP

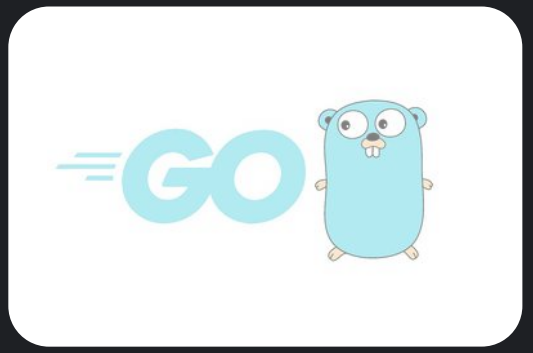
Когда становятся нужны операторы



Тезисы после пройденного пути

- Операторы жизненно необходимы, когда команды дорастают до высокой степени автоматизации тестирования

Какой уровень команды нужен



Тезисы после пройденного пути:

- Нужна команда «единорогов»
- В команду нужны люди с высоким уровнем soft-skills
- Лид должен подогревать интерес, всех членов команды

Тезисы после пройденного пути

- Создание платформы, ДАЛЕКО, не тоже самое, что Kubernetes с аутентификацией на 1-2 команды
- Инструменты все есть, а вот собрать из них платформу сложно.
- Нужна команда «крутых» специалистов.

Теперь немного про импортозамещение. Сборка Opensource в банковской среде.

Тезисы после пройденного пути

- Очень многие OSS проекты используют git submodule и тянут с github всякое
- Сборка компонентов идет в контейнерах

Импортозамещение

Тезисы

- Для нас лучшим выбором оказалась RedOS
- Часть компонентов мы взяли из пакетов RedOS, например, HAProxy
- При проектировании рекомендуется почитать внимательно *https://reestr.digital.gov.ru/news/315949/*
- Там есть список причин отказа внесения в реестр Минцифры