БЕКОН'26

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Зачем бизнесу нужна отдельная команда защиты K8s?

Панченко Николай

Независимый эксперт K8s Security

О себе:

БЕКОН'26

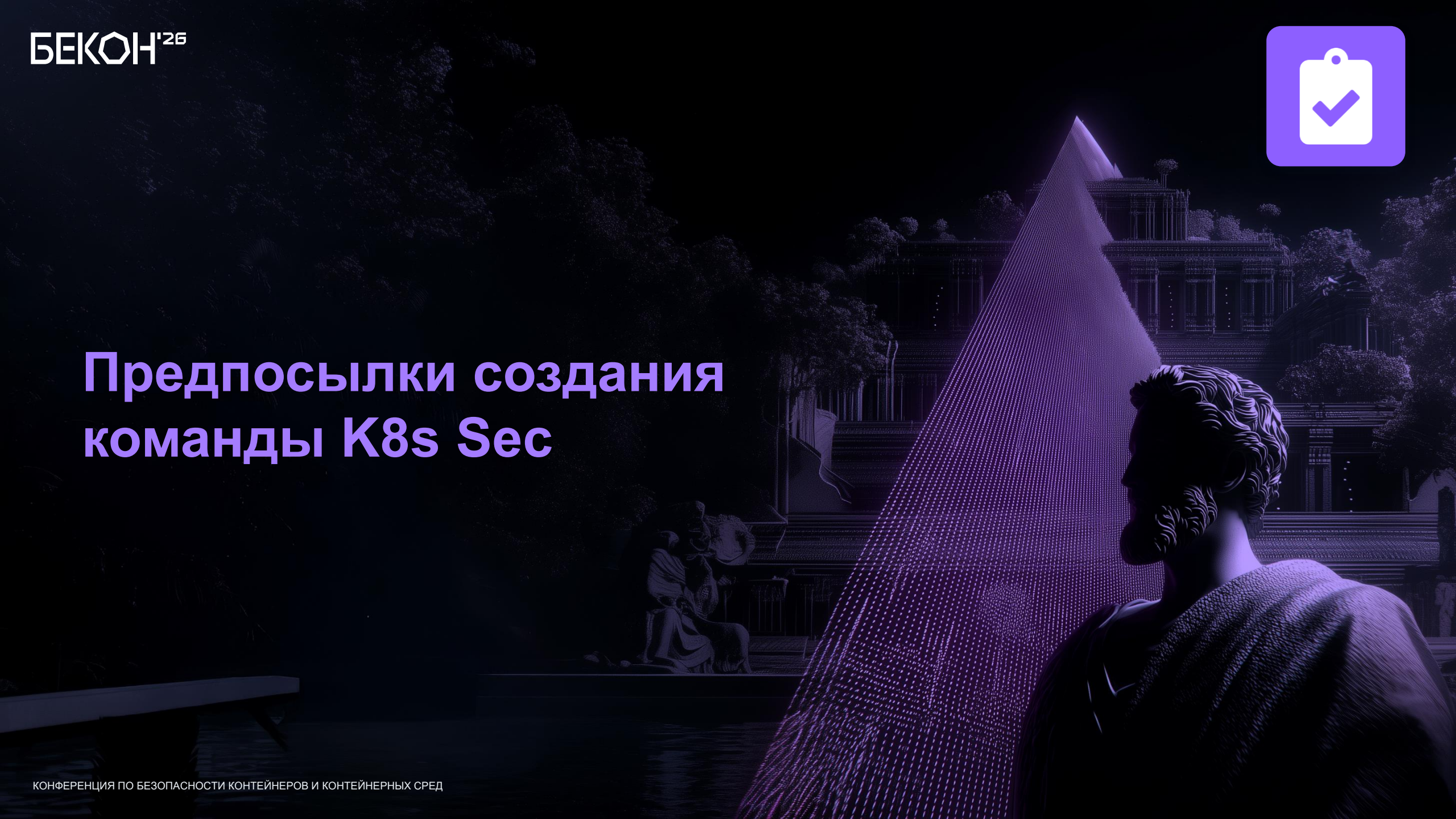
- Панченко Николай
- Более 10 лет в IT и ИБ
- Более 5 лет занимаюсь изучением K8s и устройством Cloud-окружений
- Поработал как в стартапах, так и в “кровавых энтерпрайзах”
- Выступал на OffZone, PHDays, Highload++, Бекон =)

План:

БЕКОН'26

1. Предпосылки создания команды K8s Sec
2. Экономическое обоснование
3. Техническое обоснование
4. Стратегическое обоснование
5. Задачи команды
6. Варианты размещения команды
7. Выводы

БЕКОН'26



Предпосылки создания команды K8s Sec

5 июня 2024 Москва, LOFT HALL#2

БЕКОН'24

Конференция по БЕзопасности КОНтейнеров и контейнерных сред

Подразделение для защиты k8s

Артем Мерец

Тинькофф

* Ссылка: https://old.luntry.ru/wp-content/uploads/2024/06/1_merecz-pochemu-zashhitoj-k8s-dolzhno-zanimatsya-czeloe-podrazdelenie.pdf

Дисклеймер!

БЕКОН'26

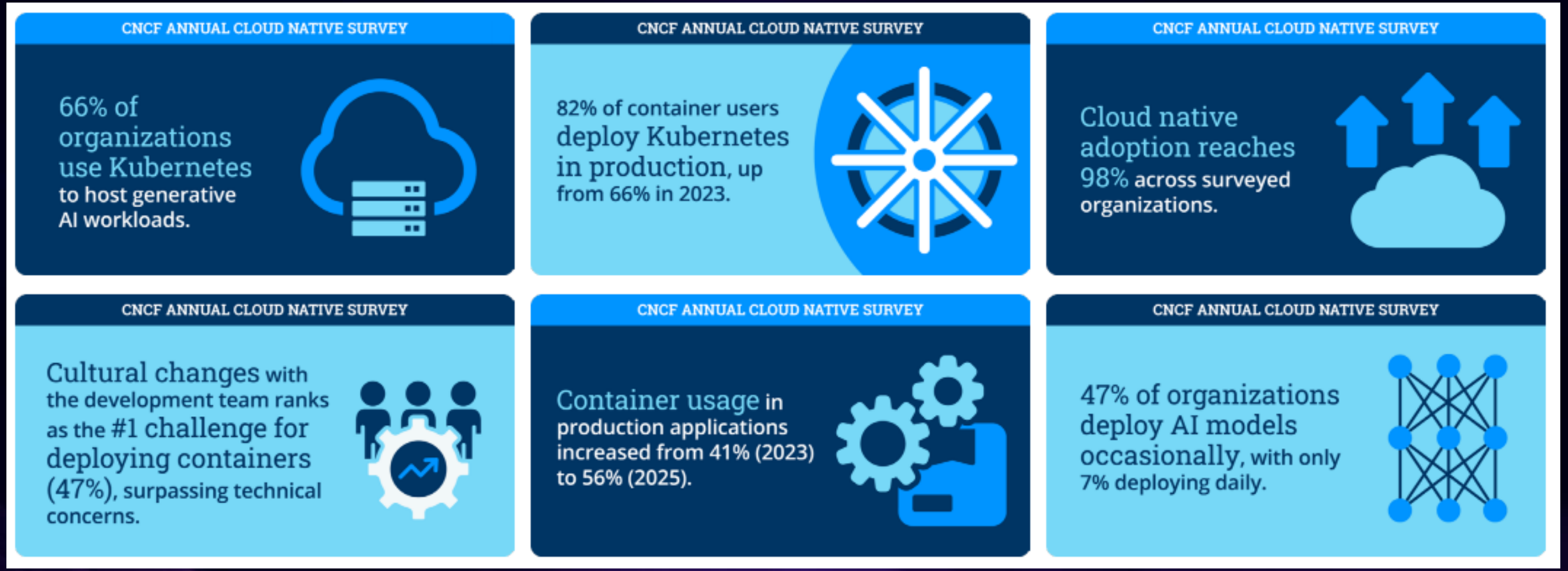
Говорим про отрасль в целом:
есть как более, так и менее зрелые компании

Релевантность относительно вашей компании предлагается определять самостоятельно!

Достигать цели и решать проблемы можно по-разному —
обсуждаем возможные схемы и варианты — часть даже работает =)

CNCF Annual Cloud Native Survey 2026

БЕКОН'26



* Ссылка: https://www.cncf.io/wp-content/uploads/2026/01/CNCF_Annual_Survey_Report_final.pdf

CNCF Annual Cloud Native Survey 2026

БЕКОН'26

98%

организаций используют облачный подход

82%

организаций используют K8s в prod-окружении

66%

организаций используют K8s для AI-нагрузок

K8s – мировой стандарт для размещения контейнерных нагрузок

* Ссылка: https://www.cncf.io/wp-content/uploads/2026/01/CNCF_Annual_Survey_Report_final.pdf

Есть ли отличия в защите IaaS от PaaS?

БЕКОН'26

K8s – мировой стандарт для размещения контейнерных нагрузок

Отличается ли инфраструктура K8s от классического облака IaaS?

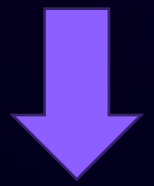
Да – K8s это PaaS

K8s расширяет поверхность атаки
и приносит новые пункты в модель угроз

Раз новая модель, то где брать экспертов?

БЕКОН'26

K8s расширяет поверхность атаки
и приносит новые пункты в модель угроз



Аутсорс –
Команда ИБ
“на стороне”

Выращивание
в уже имеющейся
команде ИБ

Подготовка
выделенной
команды ИБ

Эксперты нужны, а где брать ресурсы?

БЕКОН'26

Аутсорс –
Команда ИБ
“на стороне”

Выращивание
в уже имеющейся
команде ИБ

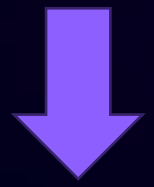
Подготовка
выделенной
команды ИБ

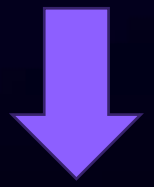
Нужны “ресурсы”, “люди”, “деньги”, “ФОТ”, “ставки” и т.д.

Играем в игру “Как продать команду?” =)

БЕКОН'26

Нужны “ресурсы”, “люди”, “деньги”, “ФОТ”, “ставки” и т.д.



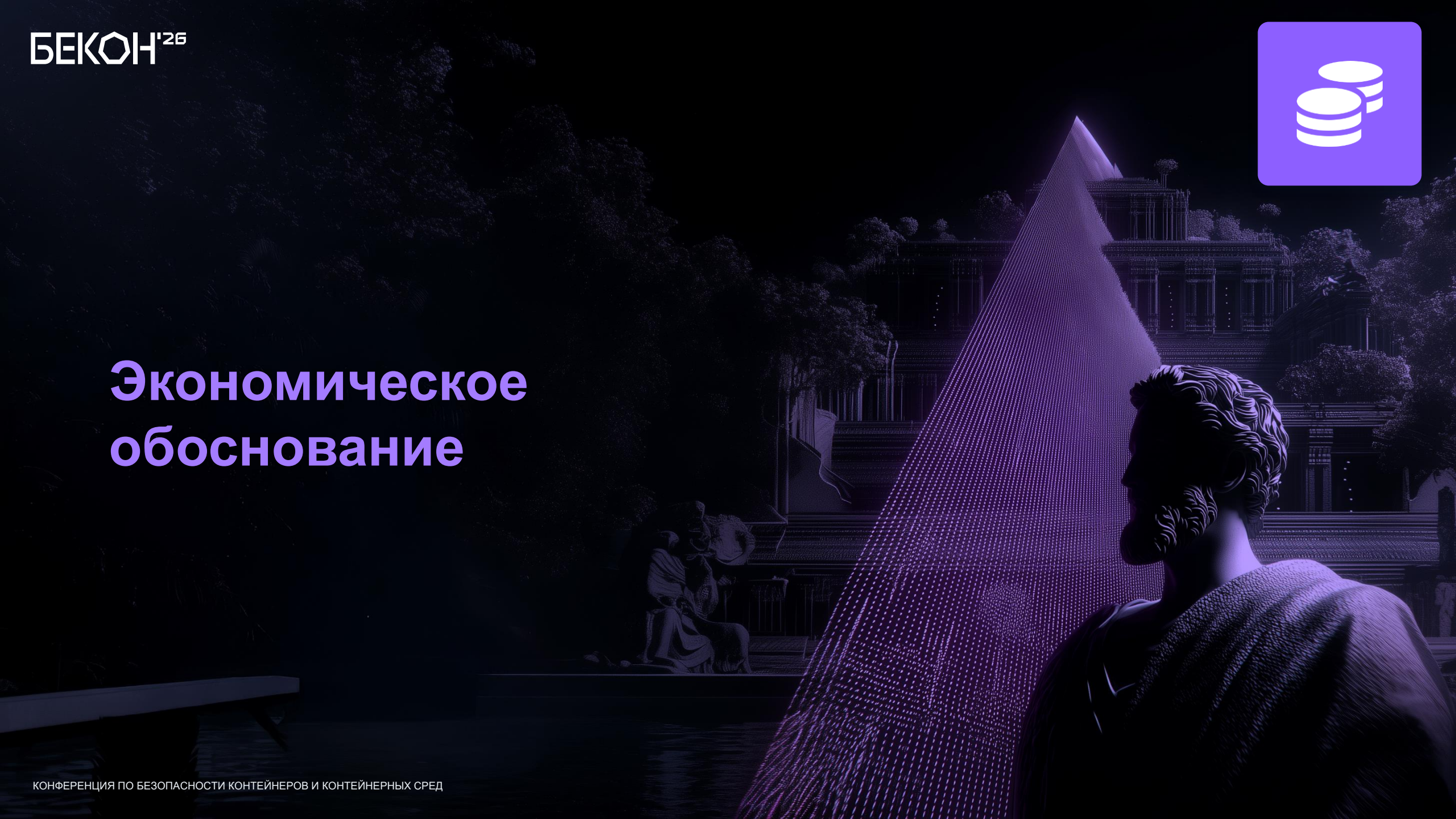


Экономическое обоснование

Техническое обоснование

Стратегическое обоснование

БЕКОН'26



Экономическое обоснование

Экономическое обоснование

БЕКОН'26

Отвечает на вопрос — сколько стоит ошибка в K8s?

Один кластер часто обслуживает десятки-сотни-тысячи сервисов сразу

Остановка бизнеса = прямые финансовые потери

- K8s кластер — целевой рантайм — там живет бизнес
- Один K8s кластер держит тысячи бизнес-приложений
- Прямые потери за каждый час недоступности
- Репутационный ущерб и отток клиентов

Высокая стоимость внесения правок “на горячую”

- Перекатка кластера “на горячую” — долго и дорого в Ч/Д **
- Чем позже прилетает архитектурное изменение ИБ, тем выше его стоимость
- Координация многих команд — затрагивает IT, ИБ и Бизнес
- Раздутие сроков VS вынужденные “опасные” согласования

Регуляторные риски: КИИ и оборотные штрафы

- ЗОКИИ
- 152-ФЗ – Закон о ПДн
- Оборотные штрафы за раскрытие ЧД*
- Нарушение требований ФСТЭК, ФСБ
- ГОСТ 57580 и др.

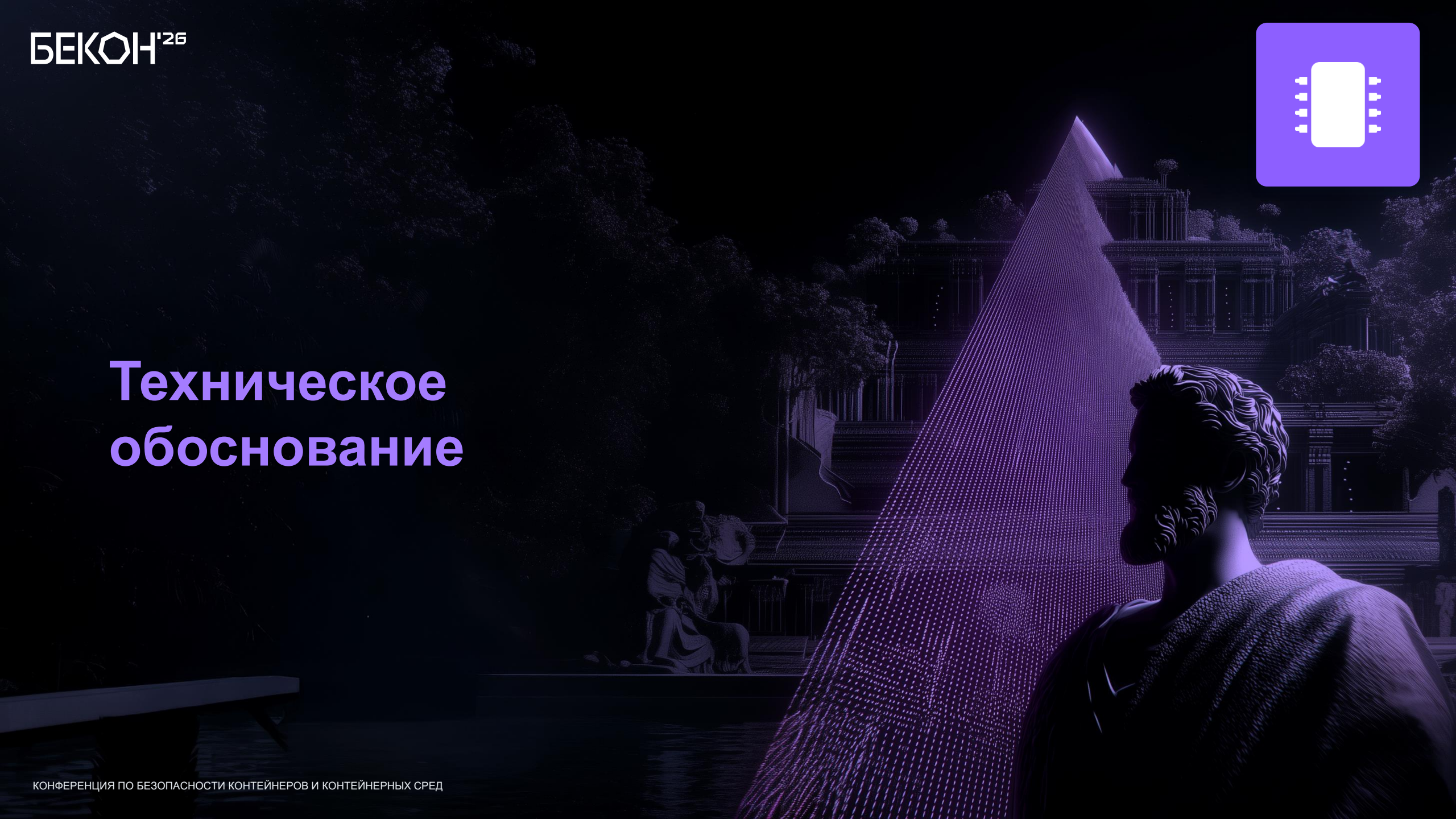
Цена восстановления кластера высока

- Дорогие инженеры заняты инцидентом, а не развитием кластера
- Стоимость простоя умножается на стоимость команды
- Выстраивание эффективного DRP — риск не восстановления кластера + ресурсозатратно в Ч/Д **

* ЧД – Чувствительные данные

** Ч/Д – ЧеловекоДни – людской ресурс =)

БЕКОН'26



Техническое обоснование

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Техническое обоснование

БЕКОН'26

Отвечает на вопрос — почему “обычная” ИБ-команда может не заметить ИБ рисков вокруг K8s?

K8s кластер в компаниях часто реализован как PaaS*

Специфика построения PaaS для K8s

- Доп. расходы на контроль платформы: control plane, woker и др.
- Мультитенантность
- Контейнерная и сетевая изоляция нагрузок
- Эфимерность и динамичность нагрузок
- Размытый периметр (история про “веселые” Ingress, NodePort)

Декларативный подход описания нагрузки в K8s

- Есть ожидаемое и реальное состояние нагрузки
- Все манифесты хранятся в “нежном” ETCD
- Помимо самой нагрузки есть куча вспомогательных объектов
- Хитрый момент с квотами/лимитами для защиты от DDoS
- По умолчанию “секретница” в открытом виде

Глобальные особенности K8s

- “Швейцарский нож” с уклоном в контейнерный рантайм
- Не защищен из коробки + отвратительный D-in-D**
- Физические ограничения K8s по количеству объектов
- Специфичный комплаенс для нескольких уровней – 4c***

Специфичный CI/CD (supply chain)

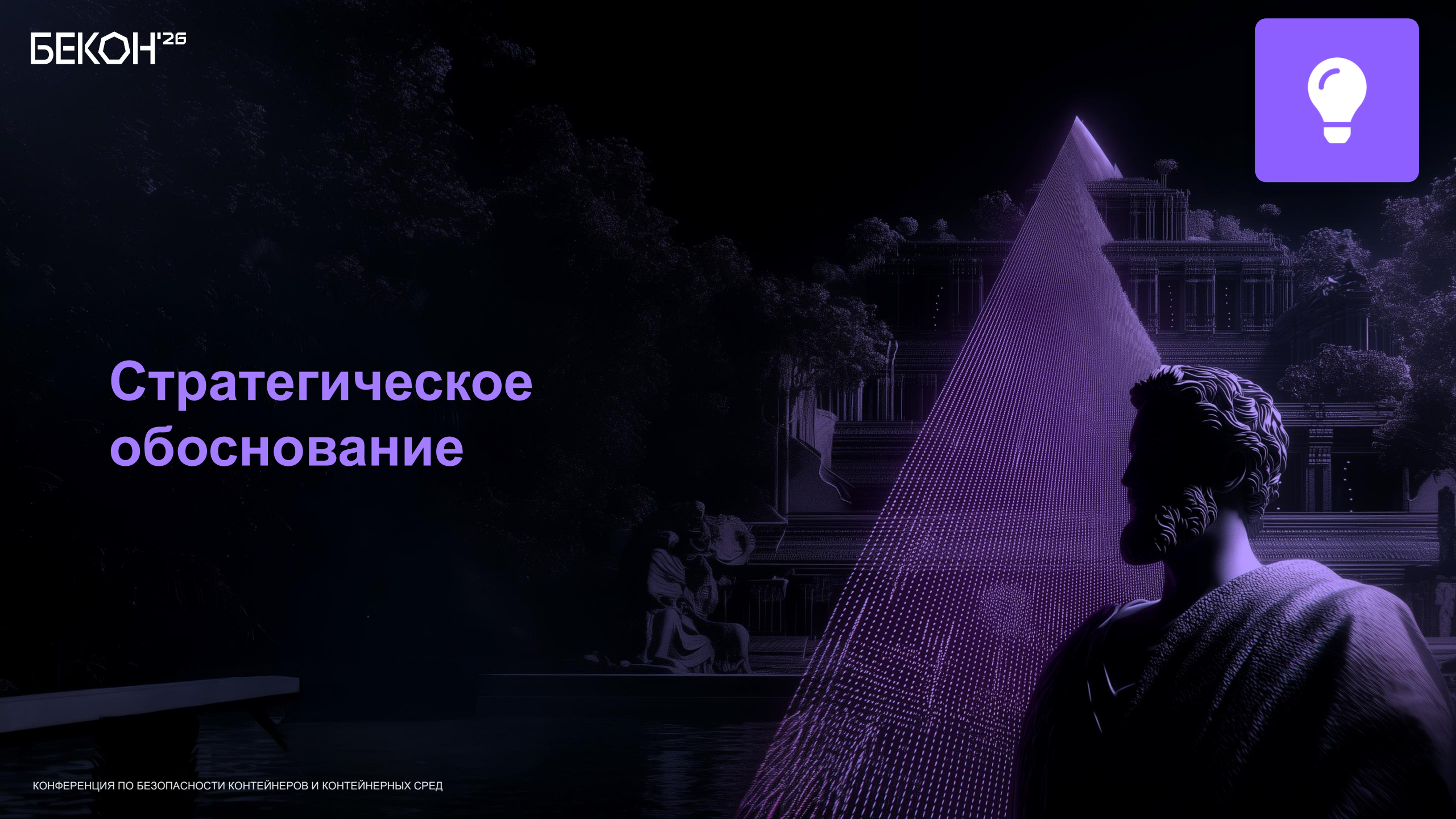
- Нагрузка зашита в Docker-образ, нужен контроль реестров
- Нагрузка заранее описывается через создание манифеста
- Нагрузка поставляется в кластер преимущественно через API
- Для API нужен специальный конфиг с нужным RBAC
- Размещение нагрузок происходит автоматически

* PaaS – platform as a service

** D-in-D – Defence-in-depth – защита в глубину

*** 4c – Code, Container, Cluster, Cloud

БЕКОН'26



Стратегическое обоснование

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Стратегическое обоснование

БЕКОН'26

Отвечает на вопрос — какие плюсы дает команда K8s Sec в стратегическом плане?

Стратегические планы обычно обсуждаются на уровне руководителей высокого уровня!

Уникальная экспертиза

1. Более детальная модель угроз
2. Качественная установка приоритетов безопасности
3. Выставление более точных контролей SOC
4. Возможность закрывать задачи ИБ E2E*

Масштабируемость ИБ

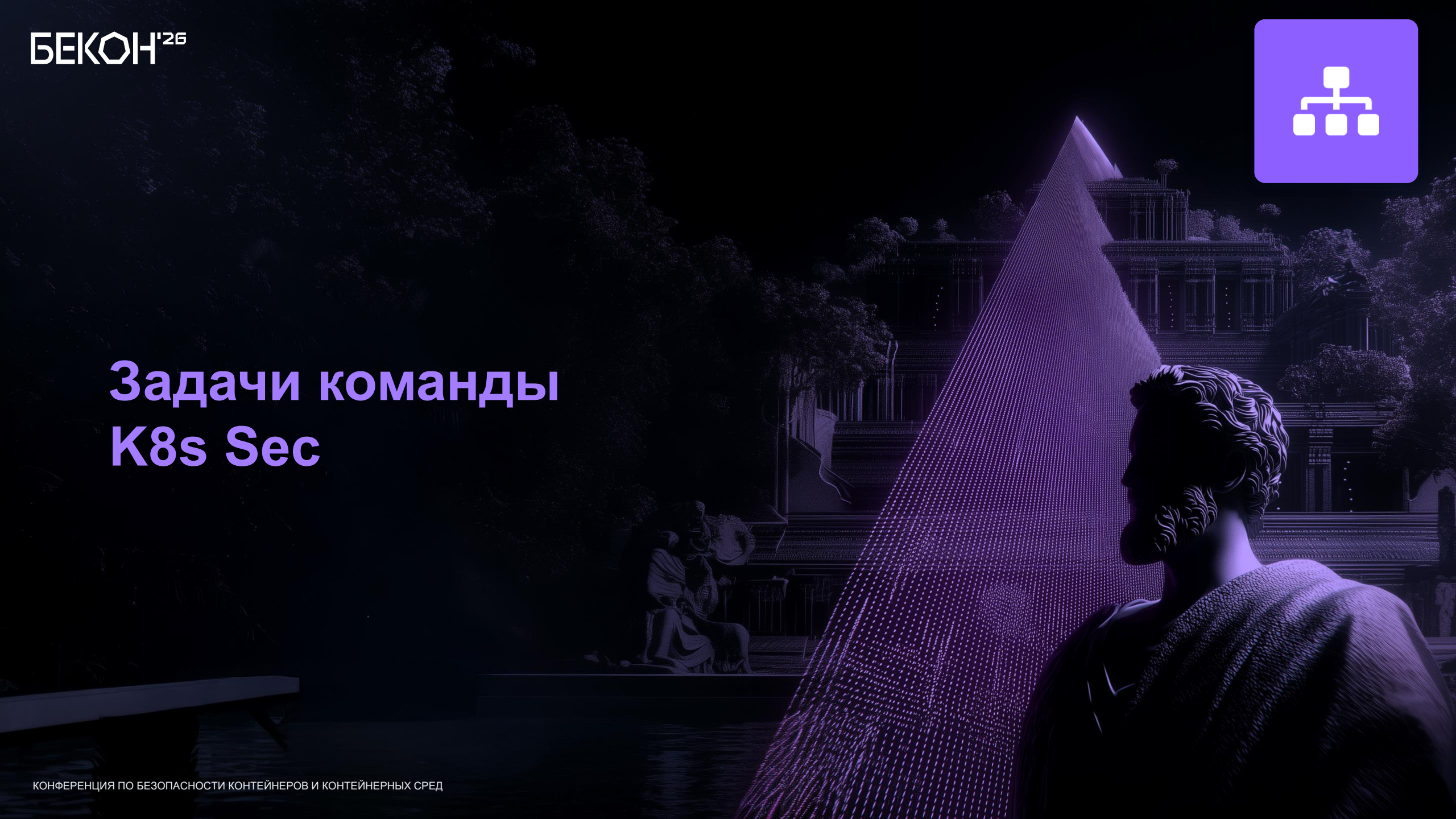
1. Построение защиты K8s по принципу Security by design
2. Горизонтальное скалирование кластеров автоматом транслирует решение безопасности
3. Нагрузки запускаются с учетом требований регулятора
4. Масштабируемые контроли

Ускоренная реакция ИБ

1. Ускоренная адаптация к новым угрозам ИБ относительно K8s
2. Отработанные схемы реагирования на атаки злоумышленника
3. Улучшенная митигация уязвимостей
4. Возможность писать собственный софт для защиты K8s

* E2E – End-to-end – самостоятельно, от начала до конца

БЕКОН'26



Задачи команды K8s Sec

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

За что отвечает команда защиты K8s?

БЕКОН'26

ИБ процессы

Контролируемое внесение изменений в систему с точки зрения процессов ИБ
Security by design
threat modeling

Сеть

NetworkPolicy и CNI
Сегментация pod→node
Zero trust для нагрузок

Архитектура и платформа

Построение систем с точки зрения PaaS
Разработка архитектурных решений ИБ
Харденинг control plane и worker нод

Контроль запуска и работы нагрузок

Харденинг нагрузок
Policy-as-code и admission control
Контроль AI-нагрузок и загружаемых моделей

IAM и доступы

RBAC и identity providers
Сервис-аккаунты и привилегии
Доступ к нодам и Control Plane

Контроль хранилищ

Контроль поставки секретов в runtime
Защита etcd
Контроль подключаемых хранилищ
Защита CSI

Vuln Management

Уязвимости компонентов K8s
Уязвимости аддонов куба
Уязвимости образов и нагрузок

Комплаенс

ГОСТ, CIS Benchmarks
Собственные стандарты
Требования фстэк, фсб

Контроль поставок (CI/CD)

сборка образов
SBOM,Подписи
Security gate
Supply chain атаки

Софт

Поддержка утилит комплексной защиты K8s
Разработка собственных инструментов ИБ
Автоматизация ИБ процессов

Контроль секретов

Контроль поставки секретов в runtime
Защита etcd и vault
Шифрование S2S и ротация секретов

Мониторинг и RedTeam

Помощь в написании контролей SOC
Помощь в расследовании инцидентов
Проведение пентестов

Команду «пилим» по возможностям и зонам ответственности

БЕКОН'26

Ни один человек не закроет все 12 доменов. Команда строится исходя из реальных компетенций, желания людей развиваться и приоритетов бизнеса — роли распределяются равномерно по необходимым доменам.

1

Оцениваем риски

Какие домены критичнее для вашей специфики и нагрузок

2

Смотрим на людей

Кто что умеет и чем хочет заниматься

3

Распределяем роли

Закрепляем домены за людьми, остальное — точки роста

Навыки: hard и soft одинаково важны

БЕКОН'26

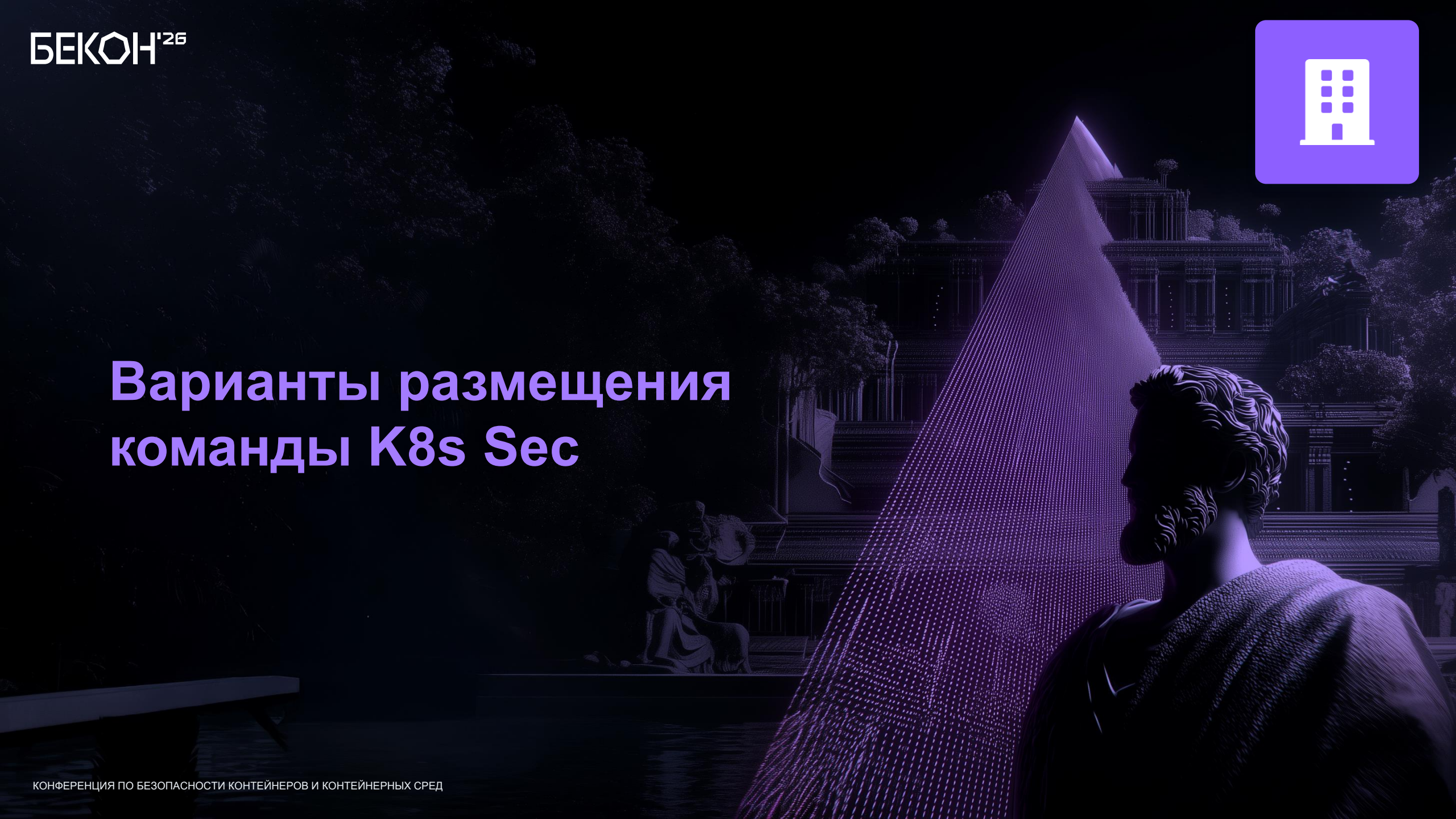
Hard skills

- Знание ОС Linux
- Глубокое понимание работы рантайма: контейнеры, образы, среды исполнения (containerd, CRI-O и т.д.)
- Знание внутреннего устройства Kubernetes: API, RBAC, network policies, admission controls etc.
- Clouds, IaC, policy-as-code, SRE, CI/CD
- Сети, криптография, управление секретами
- Комплаенс: CIS Benchmark, ГОСТы, требования регуляторов
- Программирование (Go, Rust, Python, Bash, Yaml)

Soft skills

- Коммуникабельность – общение с разработкой и бизнесом
- Умение понятно объяснять риски на языке бизнеса и денег
- Исполнительность – умение завершать дело до логического конца
- Партнёрство, а не «полиция»: важно помогать бизнесу, а не все запрещать
- Системное и архитектурное мышление
- Умение работать в команде и распределять/разделять зоны ответственности
- Терпение =)

БЕКОН'26

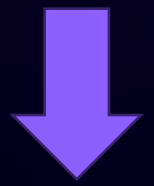


Варианты размещения команды K8s Sec

Раз новая модель, то где брать экспертов?

БЕКОН'26

K8s расширяет поверхность атаки
и приносит новые пункты в модель угроз



Аутсорс –
Команда ИБ
“на стороне”

Выращивание
в уже имеющейся
команде ИБ

Подготовка
выделенной
команды ИБ

Схема1: Размещение относительно ДИБ*

БЕКОН'26

Размещение с точки зрения имеющихся команд информационной безопасности напрямую

Внутри Infrasec

\+ Близость к инфраструктуре, безопасность с уклоном в харденинг ОС, Сеть и Управление доступом

– Теряем особенности размещения приложений, контроль манифестов и CI/CD

Внутри Appsec

\+ безопасность с уклоном в цепочку поставок и харденинг вокруг приложений

– Теряем в комплаенсе вокруг инфраструктуры, недостаточный контроль сети со стороны нод, минимальные ограничения ОС

МОЯ РЕКОМЕНДАЦИЯ

Архитектура / PaaS Sec

\+ Безопасность сконцентрирована у ИБ-архитекторов организации

– Требует зрелой культуры и чётких границ ответственности, есть прямая зависимость от команд-исполнителей

* ДИБ – департамент информационной безопасности

Схема2: Размещение относительно ДИБ*

БЕКОН'26

Размещение с точки зрения имеющихся команд ИБ в режиме “рабочей группы”

Архитектура / PaaS Sec

Проектирование кластера и платформенных сервисов с безопасностью бай дизайн

Infrasec: IAM и доступ

RBAC, ServiceAccounts, токены, разграничение прав, принцип наименьших привилегий

Appsec: Нагрузки

Контекст безопасности подов, ограничения, runtime-защита приложений

Appsec: CI/CD Sec

Доверенные образы, сканирование, подпись артефактов, защита CI/CD

Infrasec: Сеть

Network policies, сегментация сети, контроль трафика, сервис-меш

Infrasec: Диски/Секреты

Шифрование PV, управление секретами, защита etcd

PaperSec: Комплаенс

ГОСТ, CIS Benchmark, требования регуляторов, собственные стандарты безопасности

DevSec: Софт

Поддержка, написание и автоматизация инструментов безопасности платформы

* ДИБ – департамент информационной безопасности

Схема3: Платформенный подход

БЕКОН'26

Размещение с точки зрения платформенного подхода и выделенной команды ИБ

Внутри ИБ

\+ Глубокая экспертиза по ИБ

– Может отставать от скорости платформы и восприниматься как «тормоз»

Внутри IT-платформы

\+ Близость к IT-инфраструктуре, сотрудники – полноценные SRE, безопасность встроена в продукт

– Риск «замыливания» — ИБ как вторичный приоритет

МОЯ РЕКОМЕНДАЦИЯ

Гибрид / Platform Security

\+ Безопасность как часть платформы + функциональная связь с ИБ. Лучший горизонтальный скейлинг, ПРЯМАЯ ОТВЕТСТВЕННОСТЬ за фичи безопасности

– Требует зрелой культуры и чётких границ ответственности

БЕКОН'26

Выводы!

Выводы:

БЕКОН'26

1. Потеря кластера K8s имеет тяжелые экономические последствия
2. Защита K8s – полномасштабное стратегическое решение
3. Рекомендуемый вариант работы команды – предоставление безопасной платформы K8s
4. Не важно, где структурно размещена команда. Важно учитывать специфику работы K8s!

PS:

* Картинка взята из фильма “Человек-паук” 2002г.

БЕКОН'26

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Спасибо за внимание!

Вопросы?

Панченко Николай

Независимый эксперт K8s Security

@your_thoughts_are_mine

nickrzaion@gmail.com