DEVSECOPS

Строим безопасное современное приложение

Амир Алиев | Консультант по ИБ

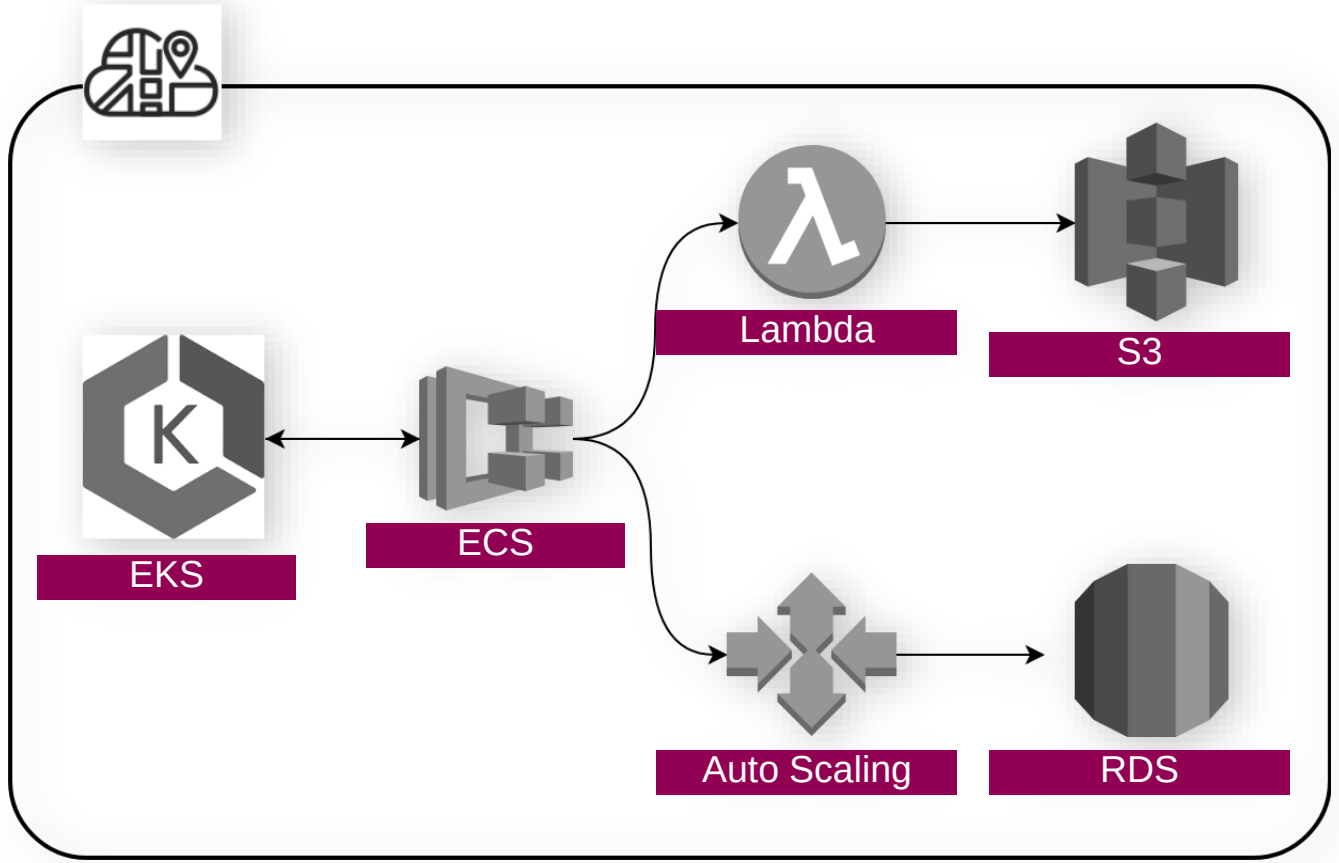
aaliev@checkpoint.com

YOU DESERVE THE BEST SECURITY

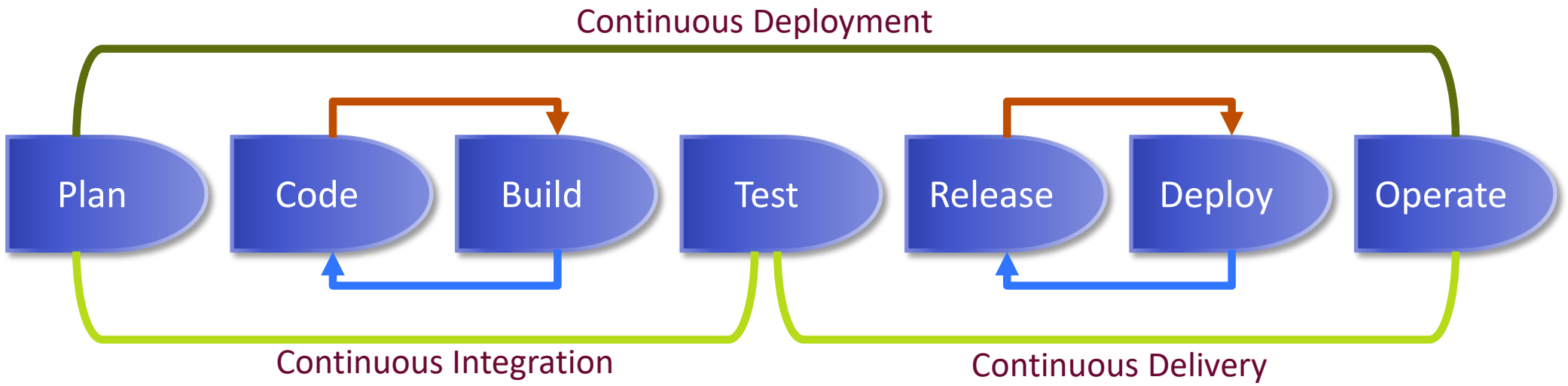
Современные приложения

Гибкость – в первую очередь

1. Небольшие фрагменты кода, которые создают приложение
2. Платите за то, что используете
3. Доставка за секунды
4. В одном клике от продуктива



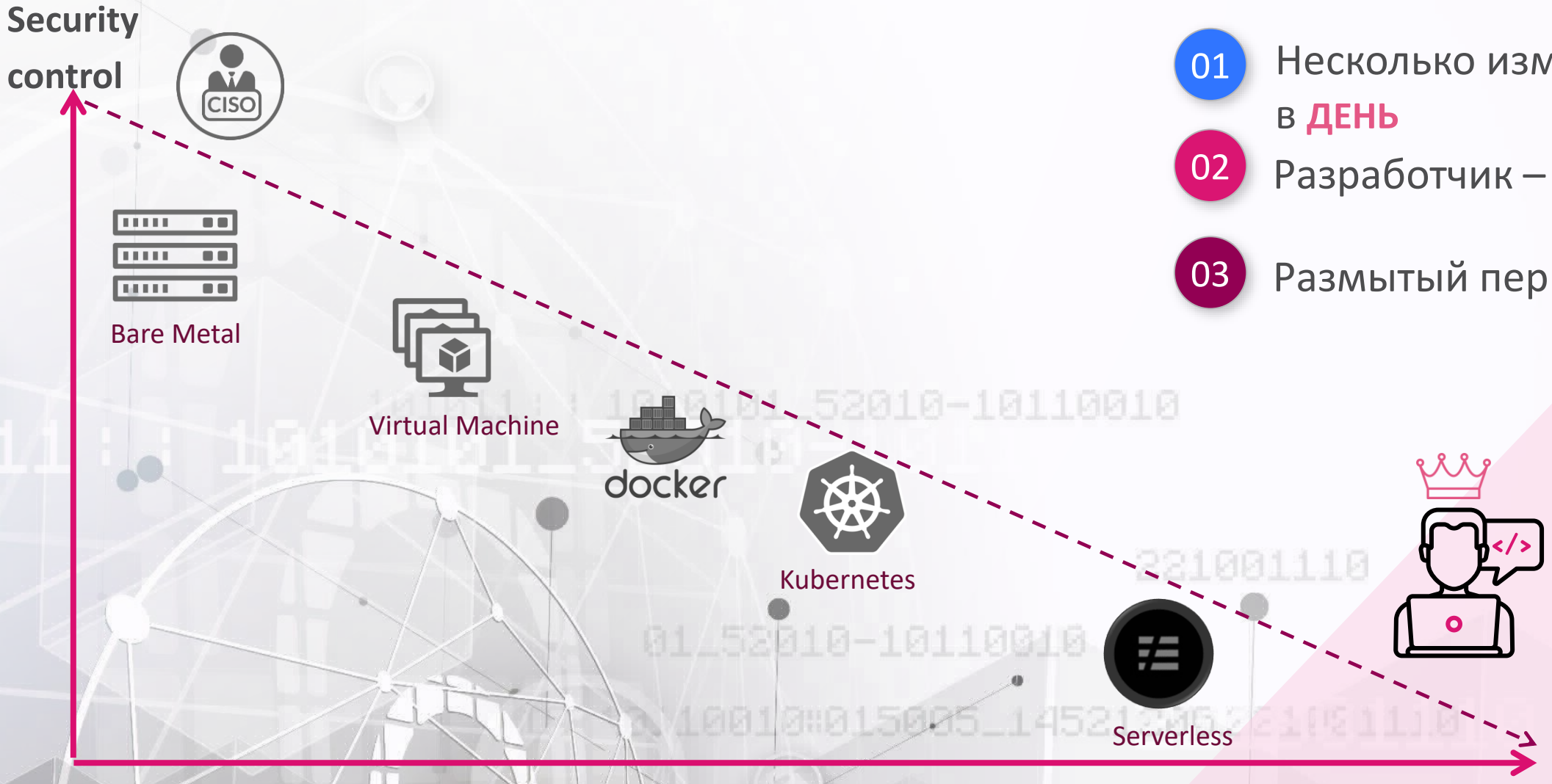
Continuous Integration / Continuous Deployment



AWS CodeCommit
AWS CodePipeline
Jenkins
git
Travis CI
CHEF
Terraform

AWS Elastic Beanstalk
AWS CodeDeploy
AWS Lambda
AWS X-Ray
AWS CloudTrail
AWS CloudFormation
AWS OpsWorks
AWS ECS
AWS Config
AWS CloudWatch

Технологии развиваются, а безопасность?

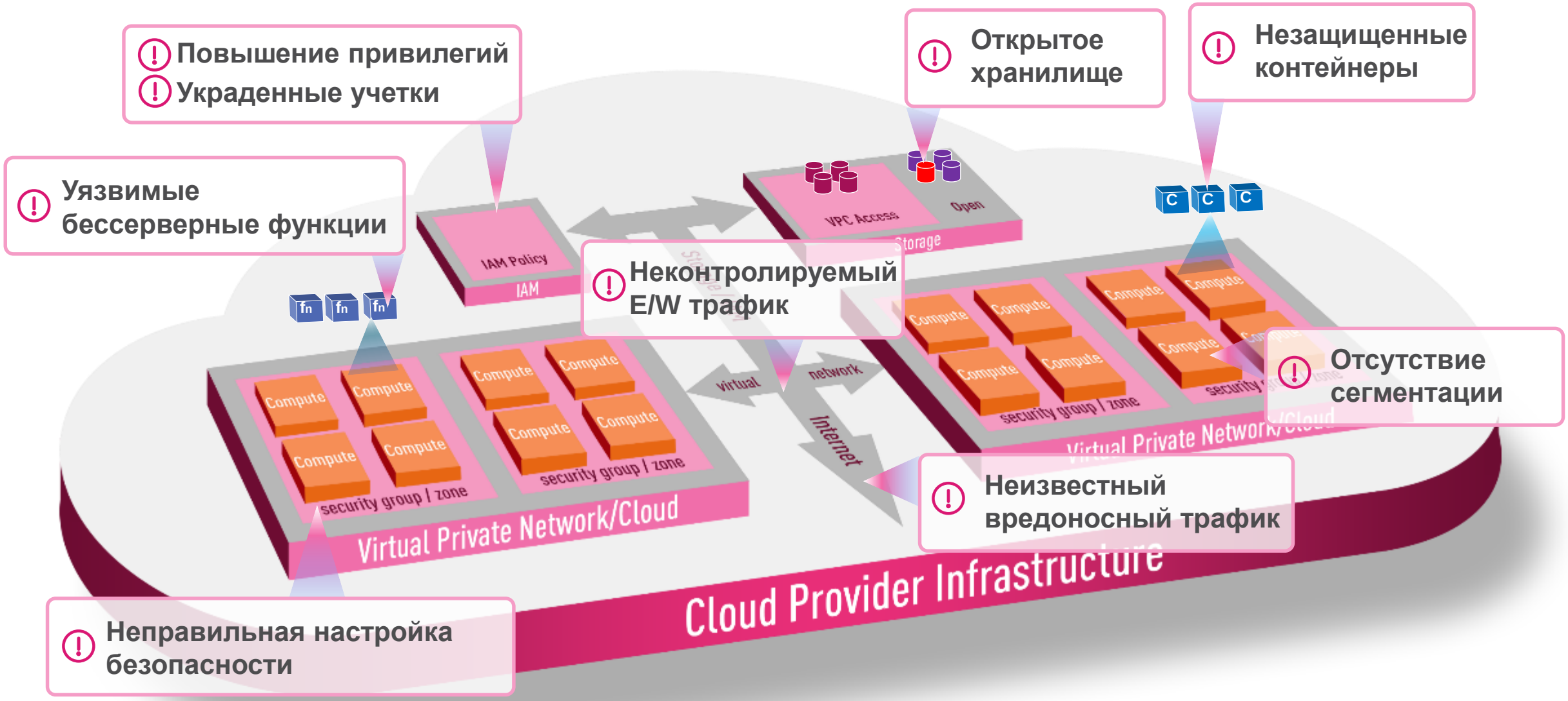


01 Несколько изменений в **ДЕНЬ**

02 Разработчик – царь горы

03 Размытый периметр

Ландшафт угроз облачной безопасности



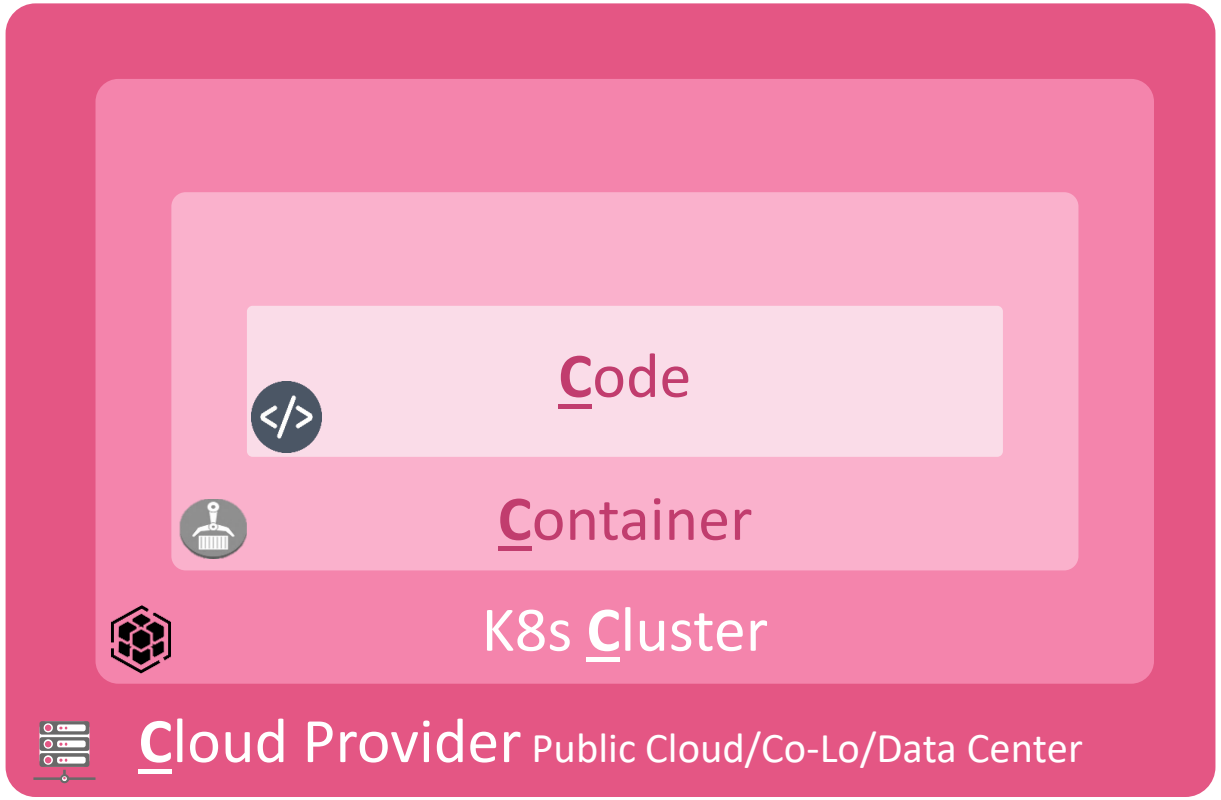
Модель «The 4C's of Cloud Native security»: Концепция защиты облаков

Модель защиты «4C»

Эшелонированный подход:

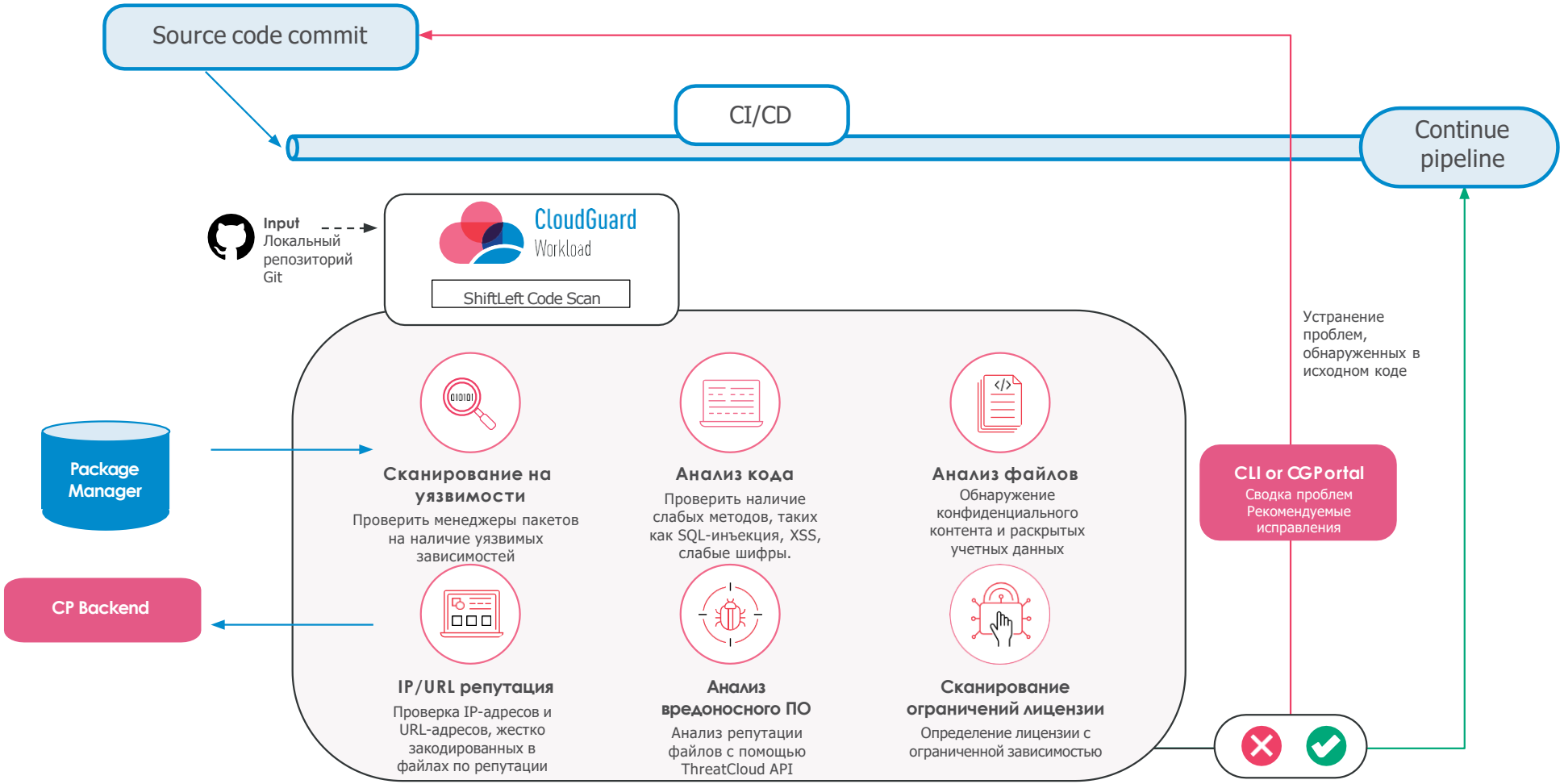
- Защищаем облачный периметр
- Сами ресурсы внутри облака
- Контейнеры/приложения
- Сам код этих приложений

Дизайн защиты: Данный подход позволяет обеспечить безопасность на всех этапах жизни современных сервисов

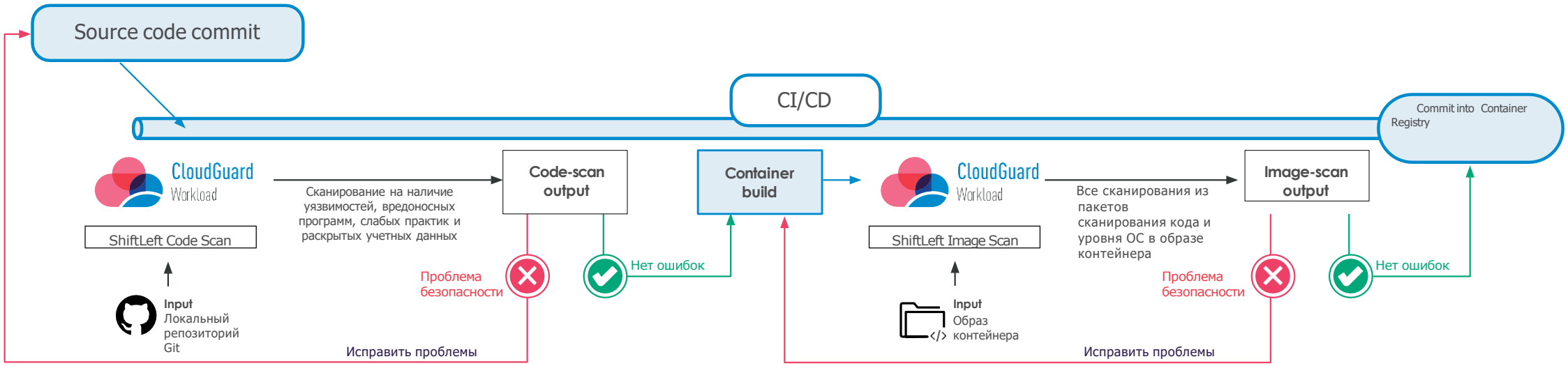


https://kubernetes.io/docs/concepts/security/overview/

Контролируем программный код

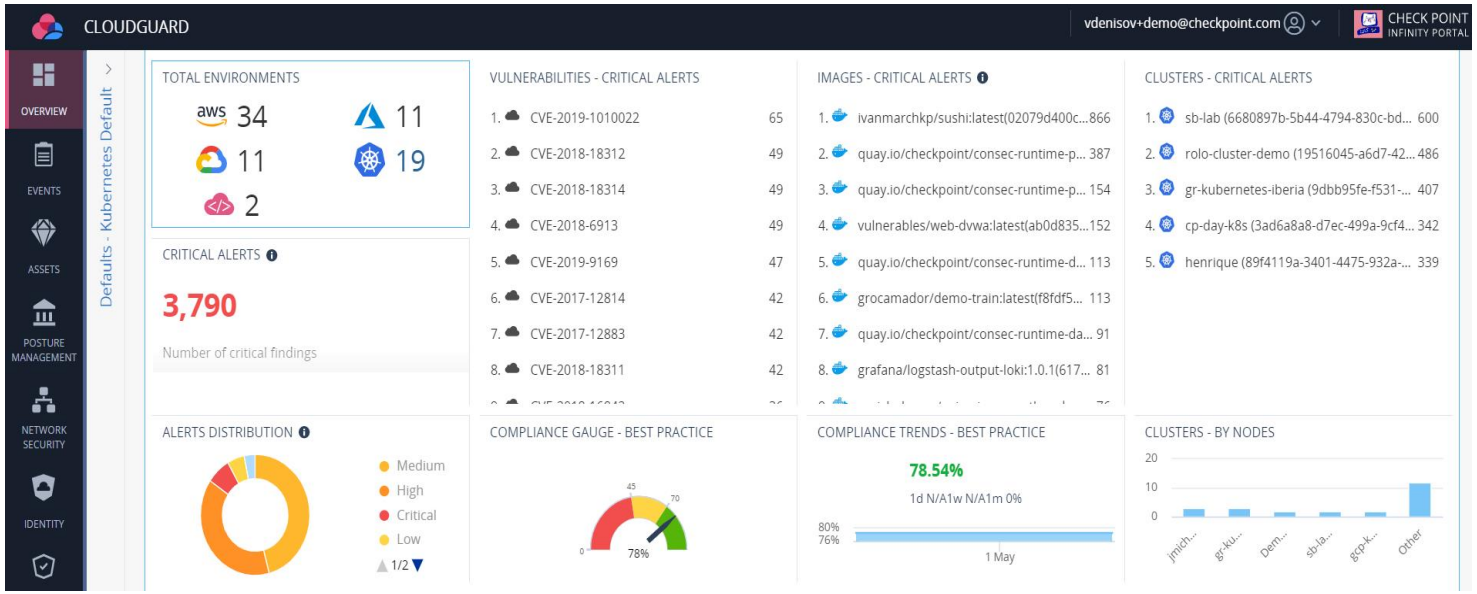


Пример встраивания в CI/CD для контейнеров



Контролируем безопасность контейнеров

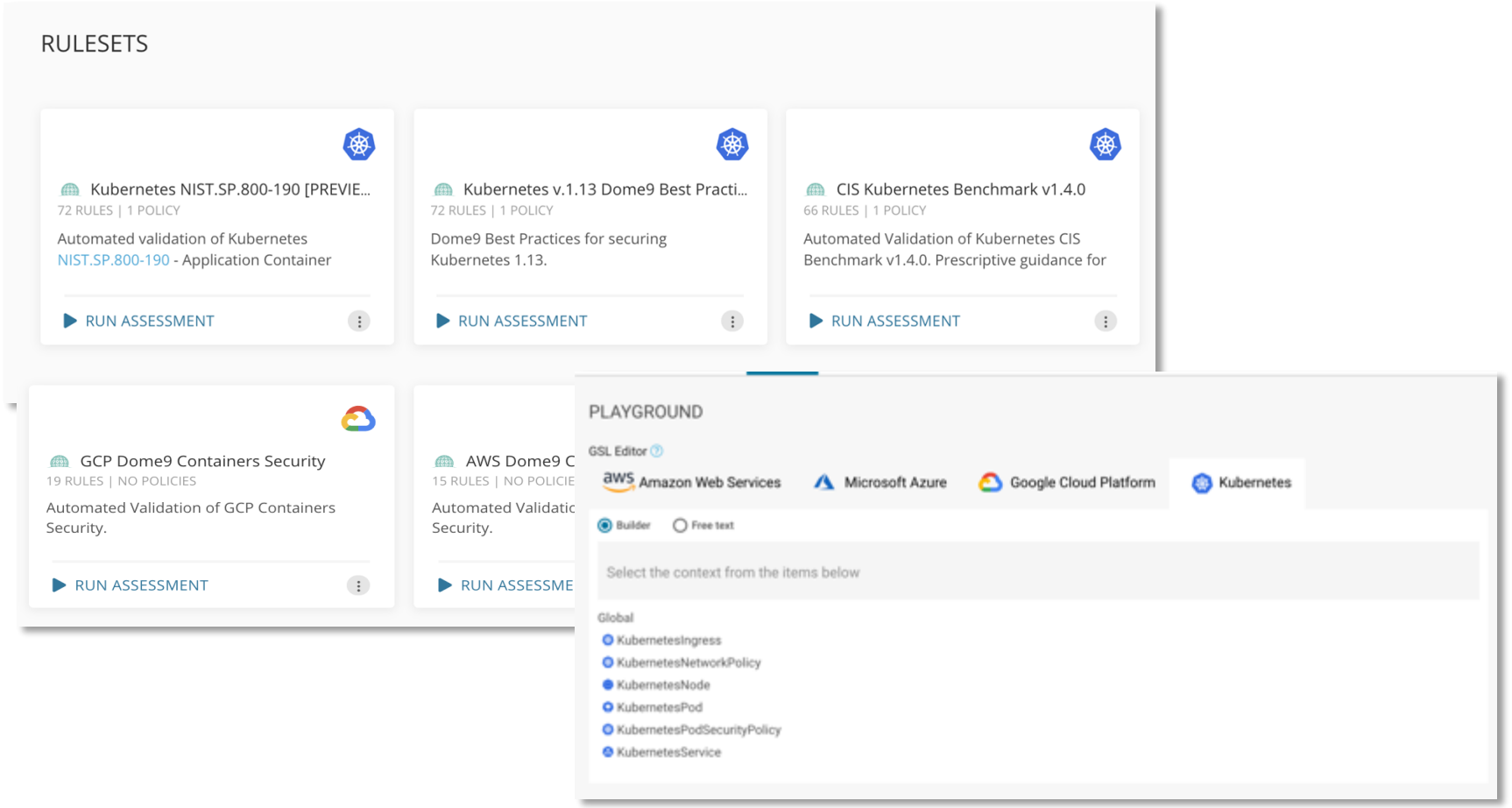
- Анализ уязвимостей и исходного кода внутри контейнеров
- Поиск аномалий в поведении запущенных контейнеров
- Защита API Kubernetes от неавторизованных изменений (Admission controller)



Контролируем кластер Kubernetes

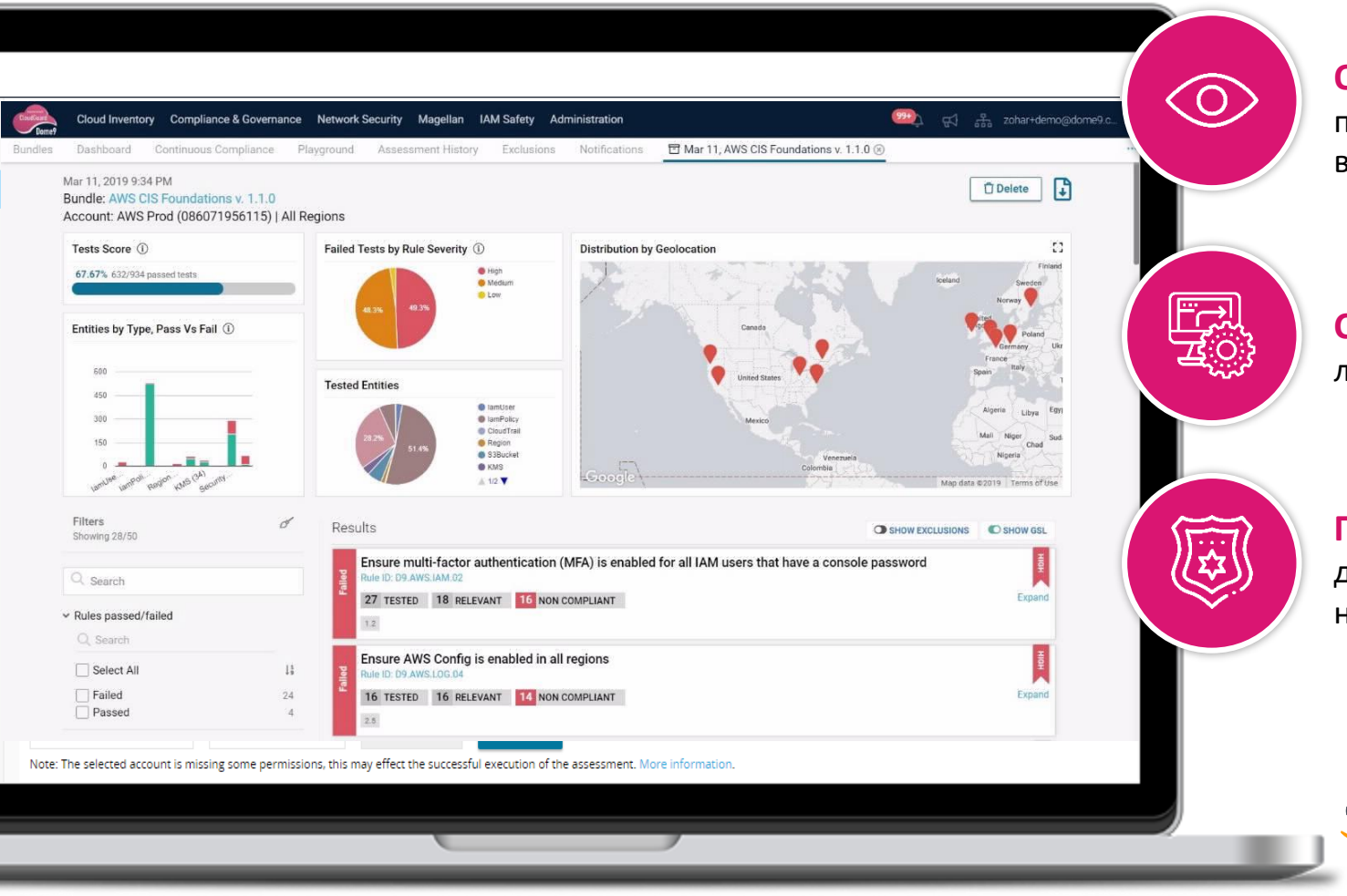
Анализ соответствия контейнеров

- ✓ Сотни готовых правил для оценки соответствия промышленным стандартам, например, **NIST 800-190** и **CIS Benchmarks для K8S**
- ✓ Постоянный анализ кластеров kubernetes и образов контейнеров на наличие уязвимостей и их конфигураций



Контролируем облако

Задачи



Обеспечить обзор всех серверов, функций, хранилищ, политик безопасности, IAM, виртуальных сетей и аккаунтов в публичных облаках и K8S

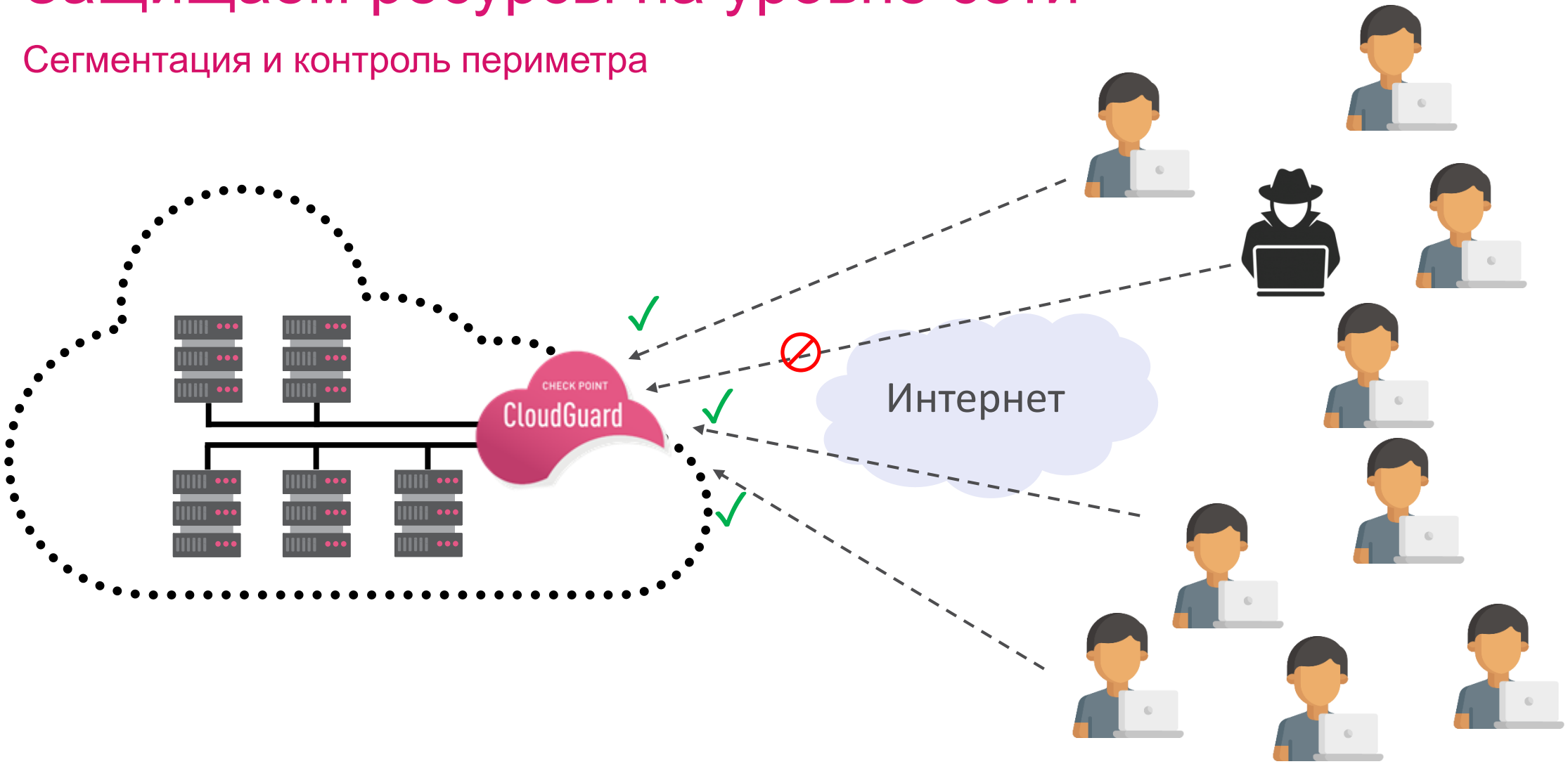
Соответствовать отраслевым стандартам защиты и лучшим практикам ИБ

Предотвратить кражу учетных записей, неавторизованный доступ к облакам, некорректные или злонамеренные изменения настроек безопасности

aws Google Cloud Azure

Защищаем ресурсы на уровне сети

Сегментация и контроль периметра



Какой должна быть защита современных публичных приложений и API?

Web Server

Kubernetes Ingress

Reverse Proxy

POD

API Gateway

Service Mesh

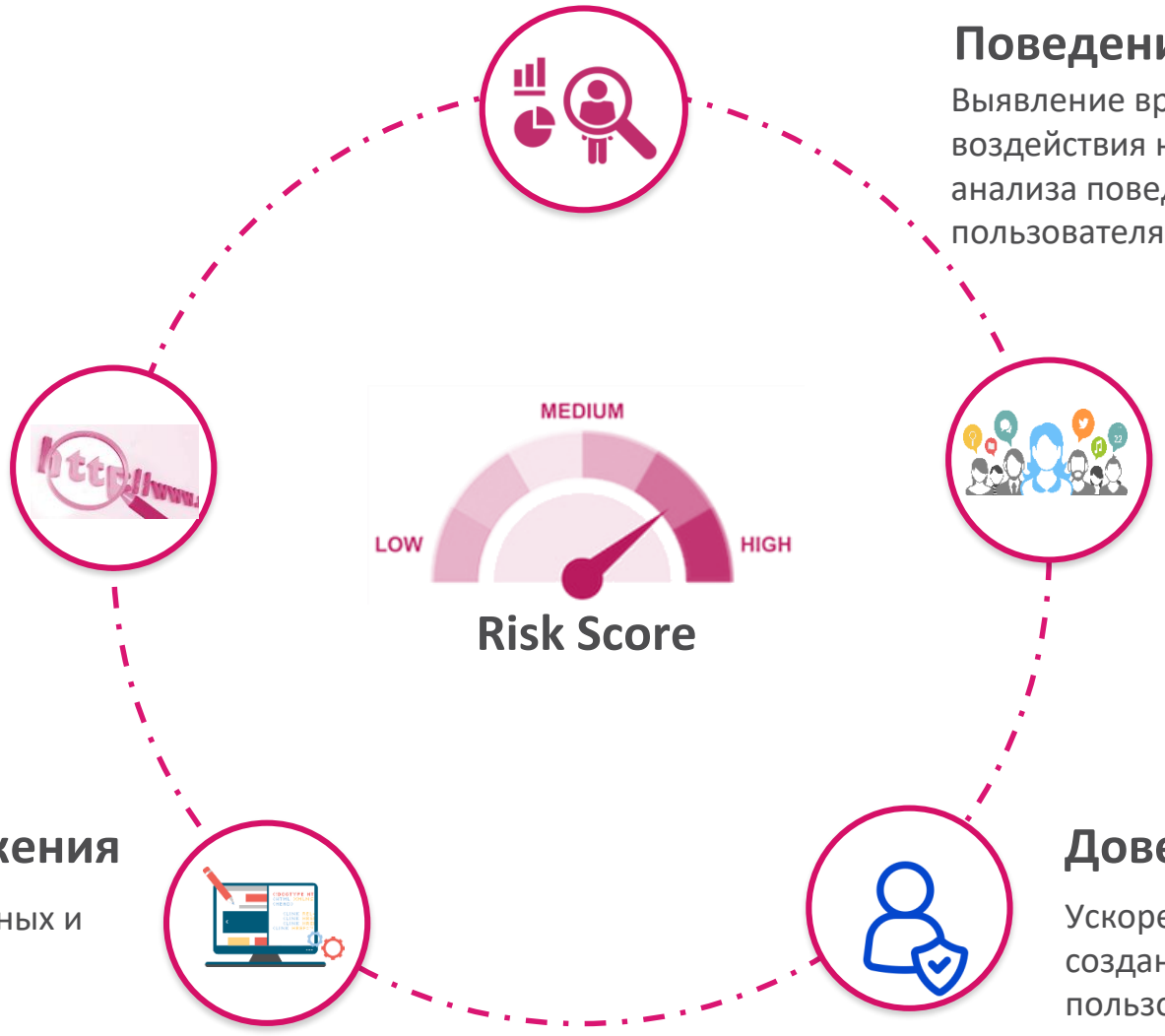
Linux VM

Serverless

Масштабируемость для любой рабочей нагрузки

Cloud Native CI/CD pipeline deployment

WAF: Важен контекст, а не только сигнатуры



Поведение пользователя

Выявление вредоносного воздействия на основе анализа поведения пользователя в прошлом

Поведение толпы

Непрерывное изучение активности пользователей с хорошей репутацией для адаптации защиты к приложению

Доверенные пользователи

Ускорение обучения за счет создания списка доверенных пользователей

Содержимое приложения

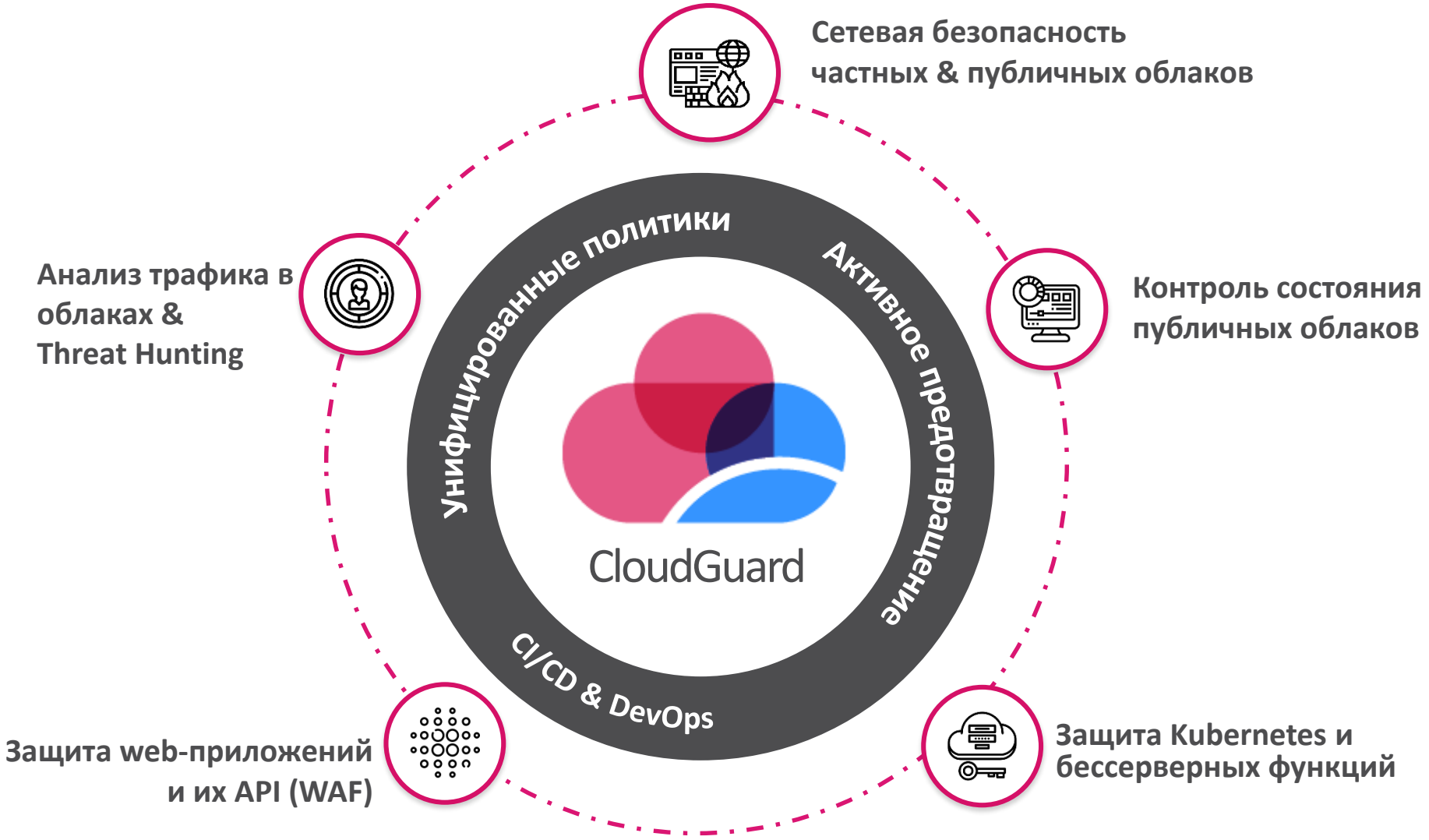
Изучение полей данных и значений

Транзакция

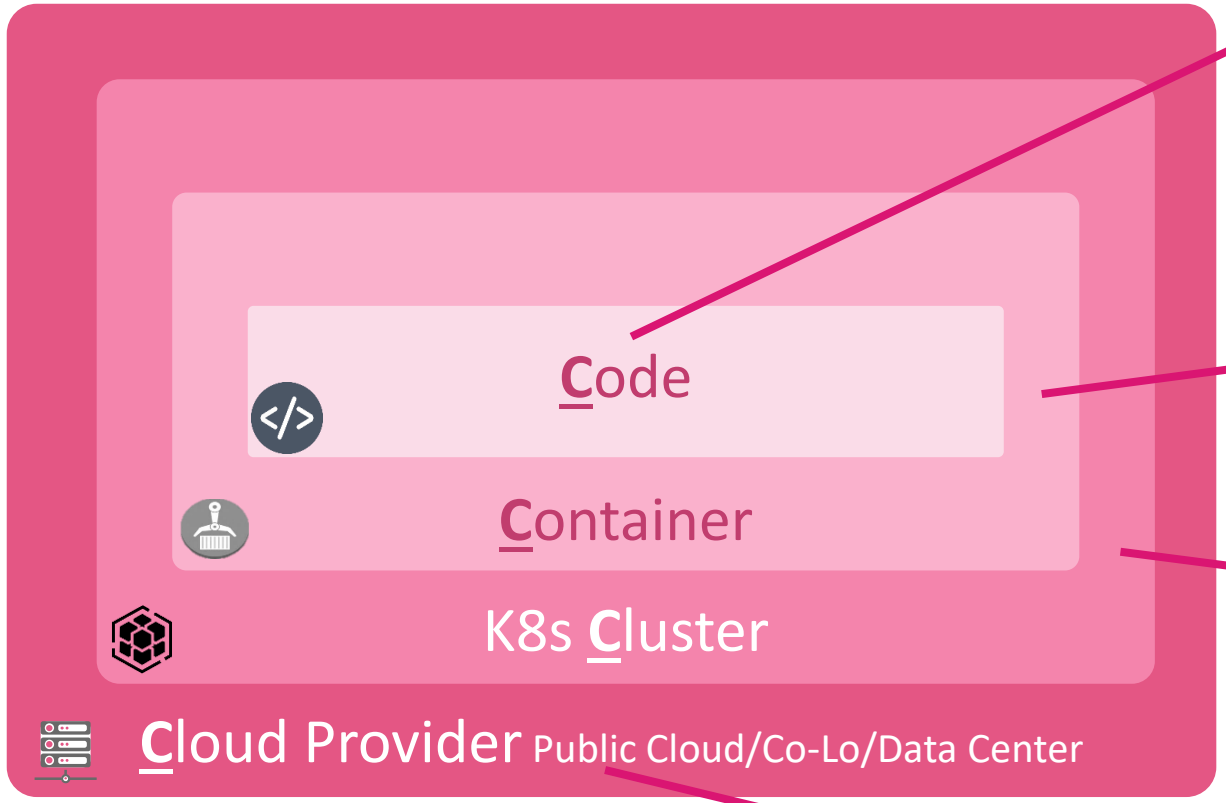
Извлечение индикаторов атаки из транзакции.

Оценка точности выявления на основе управляемого обученного алгоритма машинного обучения.

Единое решение защиты любых облаков



Модель 4C – Реализация



- Статический анализ кода
- Безопасность сторонних зависимостей

CloudGuard ShiftLeft

- Сканирование контейнеров на уязвимости и защита зависимостей ОС
- Подписывание образов
- Ограничение привилегированных пользователей
- Изоляция среды выполнения контейнеров

CloudGuard Workload

CloudGuard Workload

- Защита настраиваемых компонентов кластера
- Защита приложений, работающих в кластере

CloudGuard AppSec

CloudGuard AppSec

- Доступ к системе управления
- Сетевой доступ к узлам
- Доступ к API облачного провайдера

CloudGuard Network Security

CloudGuard Posture Management

CHECK POINT™

СПАСИБО

Амир Алиев | Консультант по ИБ

aaliev@checkpoint.com

YOU DESERVE THE BEST SECURITY