DevSecOps в разрезе **Kubernetes**

Привет!

Меня зовут Илья

Более 10 лет в IT. Сейчас работаю ведущим инженером в Glovo, Барселона.

До этого был:

- Сисадмином
- DBA
- Бакенд разработчиком
- Тимлидом

План на сегодня:

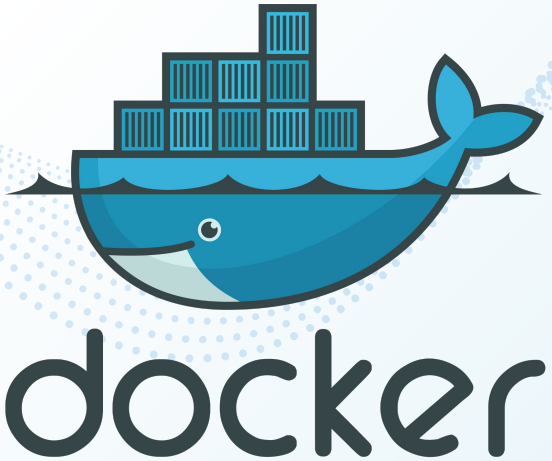
- Обзор Kubernetes
- Распространенные атаки и защита от них

Скорость доставки VS Безопасность

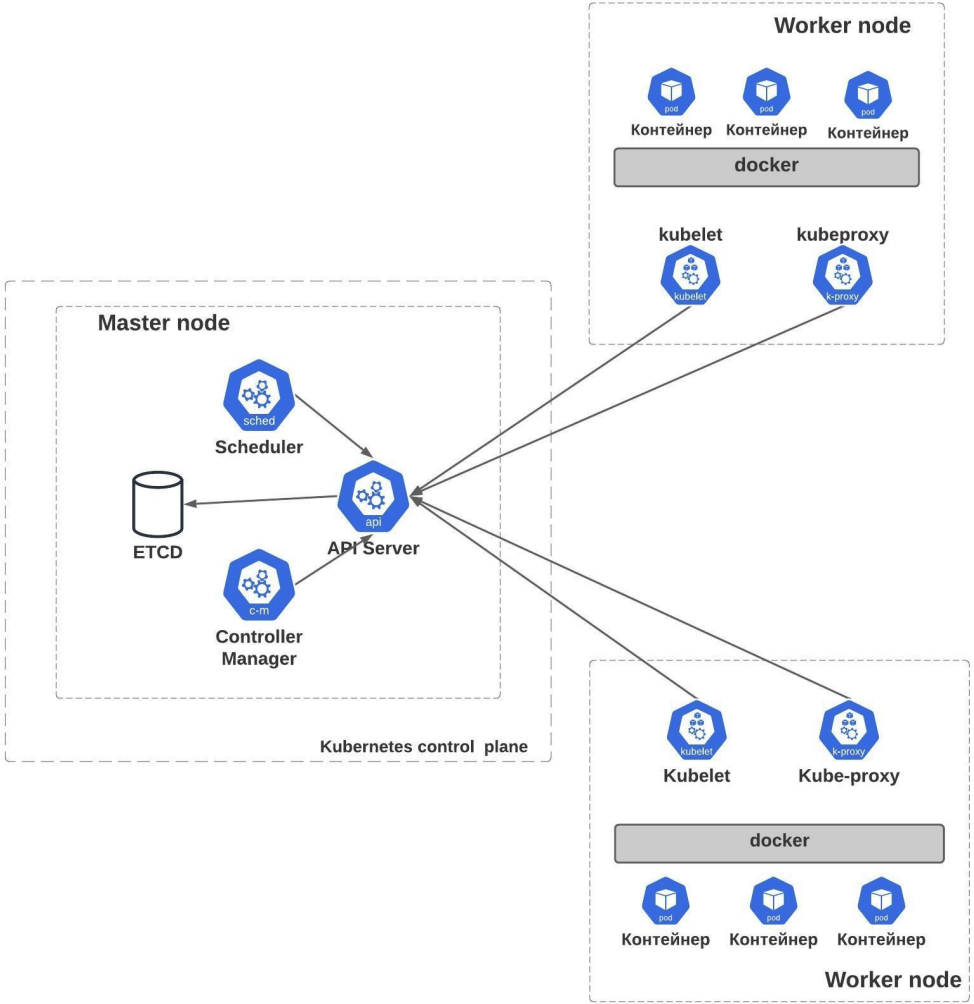
Контейнеры, Контейнеры, Контейнеры, Контейнеры...

Что такое Kubernetes?

Kubernetes — это платформа для оркестрации развёртывания и масштабирования контейнерных приложений и управления ими.

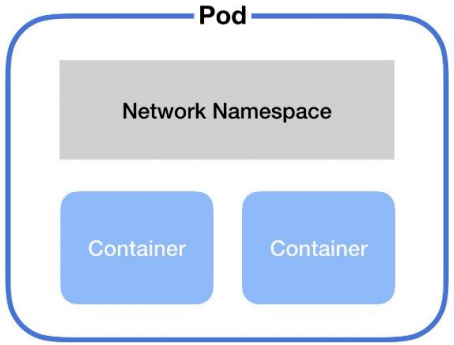


Kubernetes-кластер

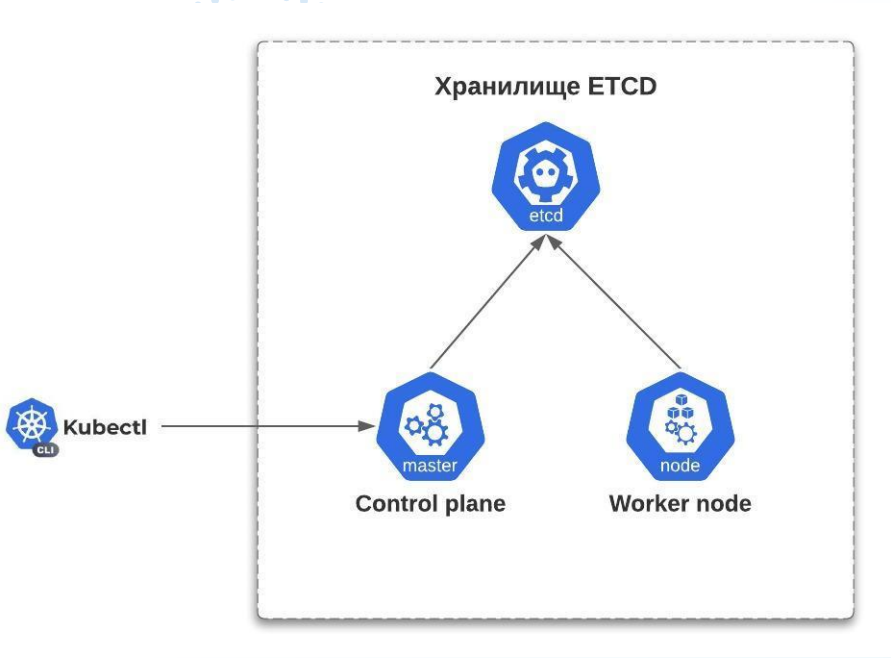


Pods

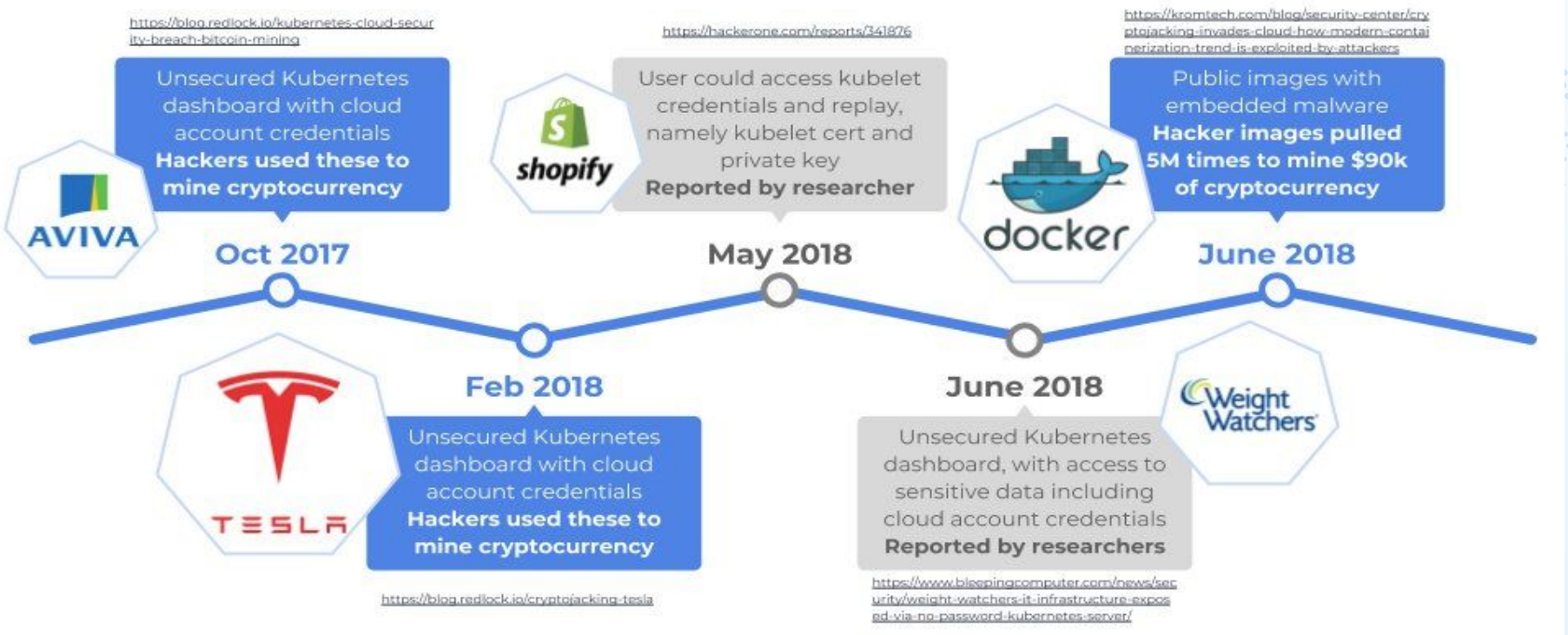
Pod — это один или группа контейнеров.
Pod — это единственный объект в Kubernetes, который приводит к запуску контейнеров.
Нет pod — нет контейнера!



Упрощённая схема работы кластера

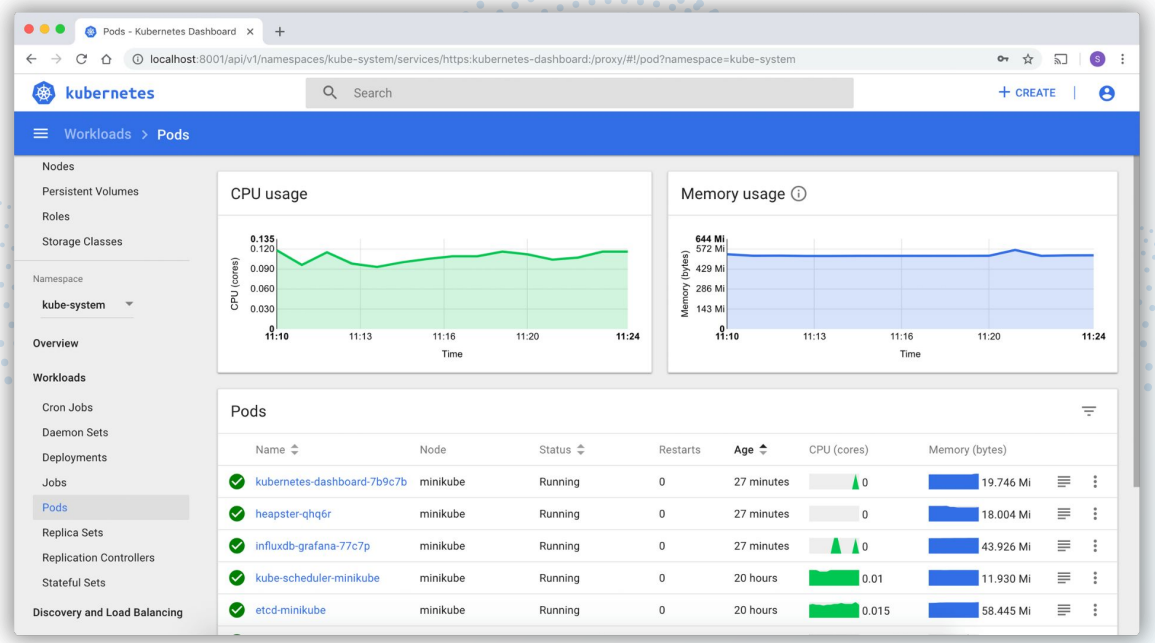


Kubernetes security threats in the wild



https://twitter.com/mayakaczorowski/status/1009111190998519815

Атака: неавторизованный доступ к Kubernetes Dashboard



Защита: неавторизованный доступ к Kubernetes Dashboard

- Не открывать в интернет
- Используйте RBAC
- Не давать повышенные привилегии Dashboard ServiceAccount

Атака: используя права pod’а

- Контейнеры в pod’е могут:
  - Быть запущены под root
  - Монтировать директории с хоста
  - Использовать порты хоста напрямую
  - Требовать повышения привилегий

- Скомпрометированные контейнеры могут воспользоваться всеми этими возможностями

Защита: Pod Security Policies

- Примеры использования:
  - Запретить запуск под root'ом
  - Ограничить привилегии

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: restricted
spec:
  privileged: false
  allowPrivilegeEscalation: false
  requiredDropCapabilities:
  hostNetwork: false
  runAsUser:
      rule: 'MustRunAsNonRoot'
```

Атака: неавторизованный сетевой доступ

- По умолчанию любому pod’у доступен любой другой pod
- Скомпрометированный pod сможет прочитать, изменить или удалить данные из другого pod’а
- Поэтому нужно специально изолировать чувствительные к взлому поды

Защита 1: Network Policies

- Позволяет заблокировать трафик pod’ов
- В особо чувствительных для безопасности местах лучшая практика - политика “deny all” по умолчанию
- Использовать white list

Защита 2: Istio

- mTLS: каждому сервису по сертификату
- Контроль Аутентификации и Авторизации
- Контроль Egress трафика
- OSI уровень 7

Спасибо за внимание!

Источники

- Повышаем безопасность микросервисов с Istio
  https://habr.com/ru/company/exness/blog/509110/
- 33+ инструмента для безопасности Kubernetes
  https://habr.com/ru/company/flant/blog/465141/
- Threat matrix for Kubernetes
  https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes
- CVE kubernetes database
  https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=kubernetes
- Kubei - a vulnerabilities scanning tool
  https://github.com/Portshift/kubei