Kubernetes

Защита виртуальной инфраструктуры

Speaker

Илья Феоктистов

Более 10 лет в IT.

Сейчас работает Head of Devops в компании Bling, Барселона.

До этого работал: DBA, бэкенд-разработчик, тимлид.

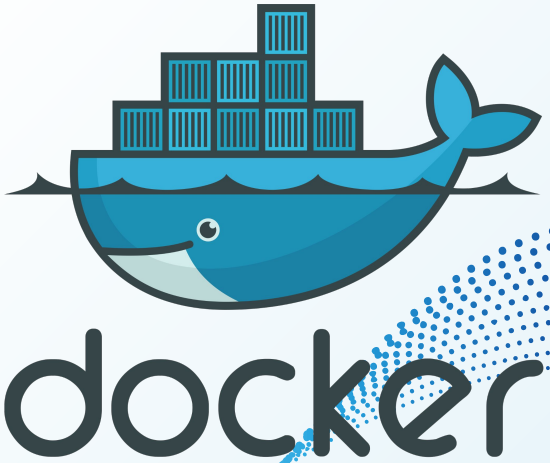
Certified Kubernetes Administrator, преподаватель в Skillbox и Otus.

План на сегодня:

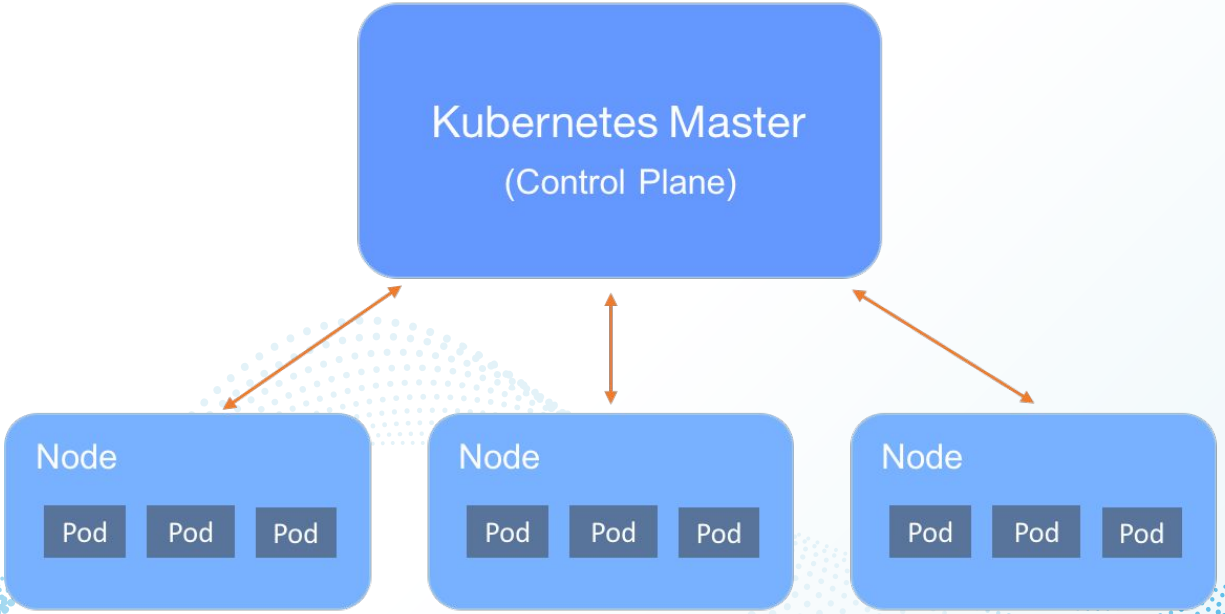
- Краткий обзор Kubernetes
- Распространенные атаки и защита от них

Что такое Kubernetes?

Kubernetes — это платформа для оркестрации контейнеров

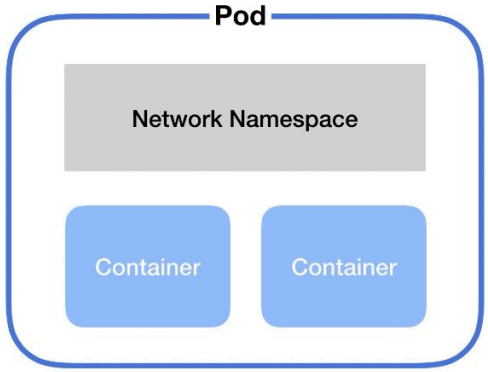


Kubernetes кластер



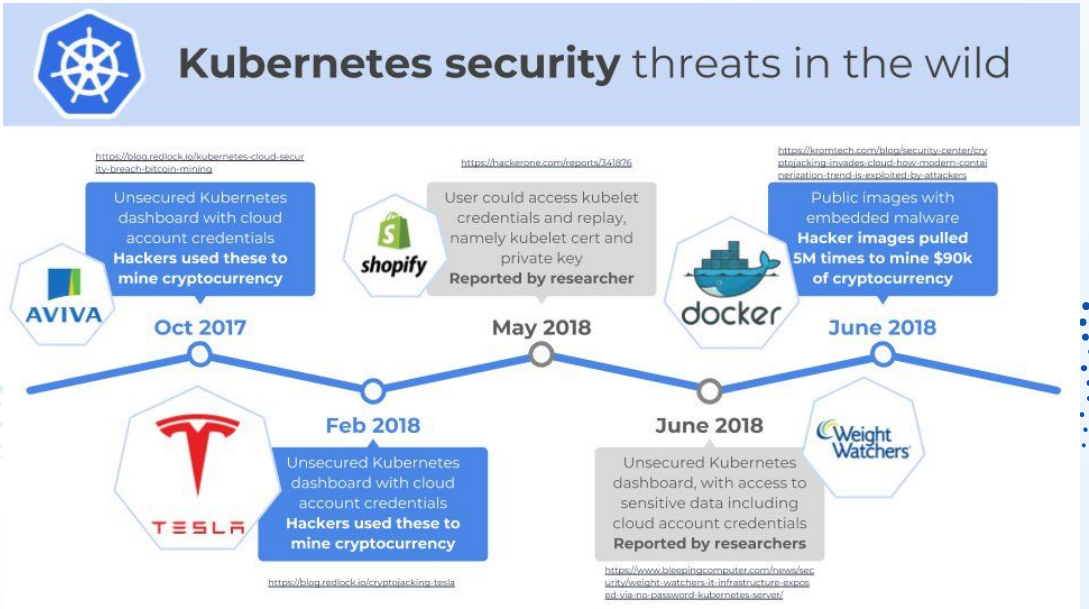
Pod

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



Масштабы бедствия

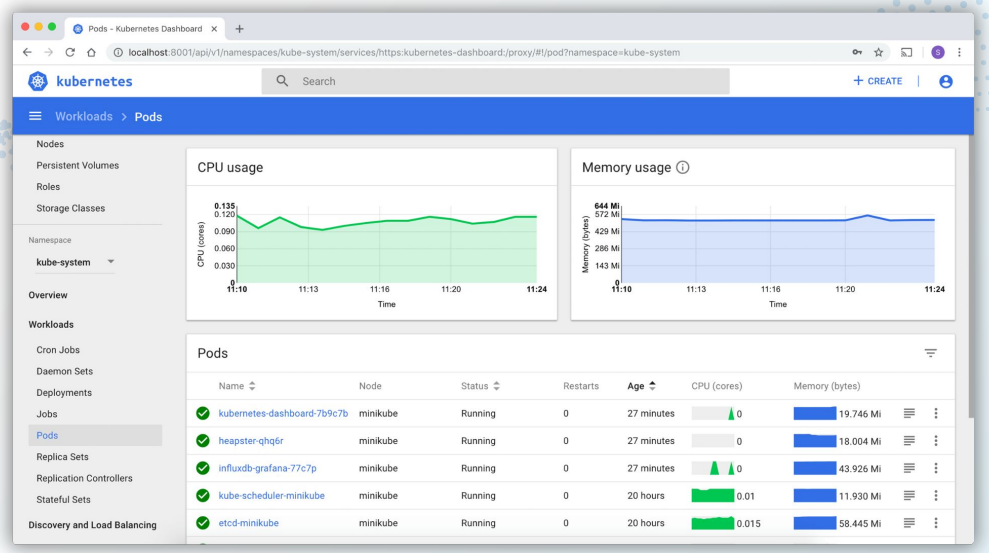
Год	Количество CVE
2015	3
2016	4
2017	4
2018	15
2019	37
2020	40
2021	43



Неавторизованный доступ к Kubernetes Dashboard

Как защититься:

- Не открывать в интернет
- Использовать с наименьшими правами, желательно read-only

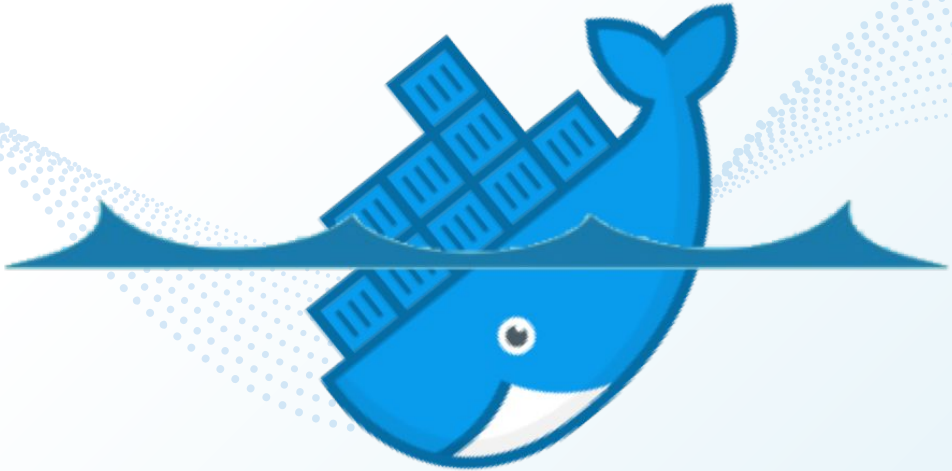


Манипуляции с docker образом

Подмена образа в репозитарии

Как защититься:

- Права на загрузку образов в репозитарий есть только у CI/CD системы
- Периодическое сканирование образов на уязвимости



Повышенные привилегии пода

- 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

Повышенные привилегии пода

Как защититься:

- Использовать **Pod Security Policies**:
  - Запретить запуск Pod'ов под root’ом
  - Ограничивать привилегии

Неавторизованный сетевой доступ

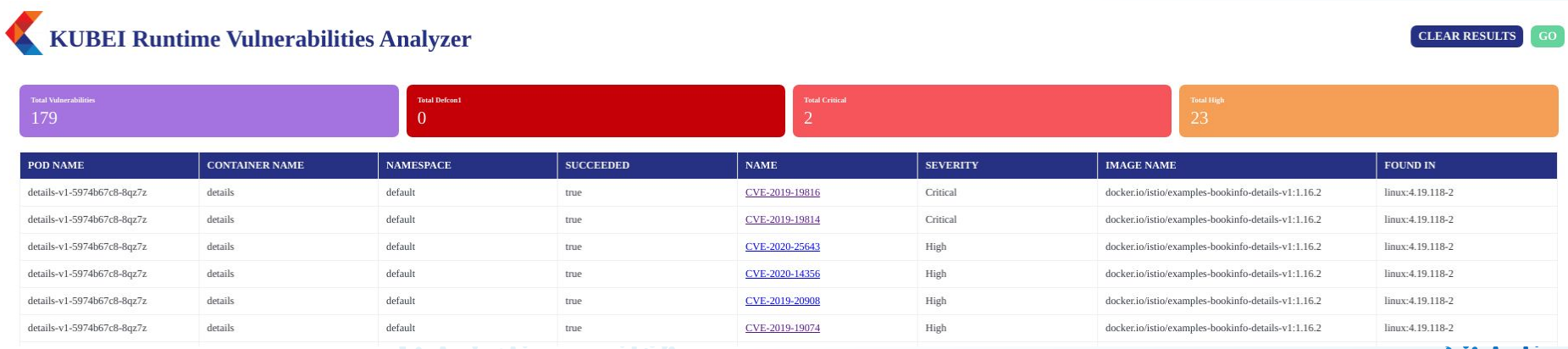
- По умолчанию любому pod’у доступен любой другой pod
- Скомпрометированный pod сможет прочитать, изменить или удалить данные из другого pod’а
- Поэтому нужно специально изолировать чувствительные к взлому поды

Неавторизованный сетевой доступ

Как защититься:

- **Network Policies:**
  - Позволяет блокировать трафик pod’ов
  - Иногда лучшая практика - политика “deny all” по умолчанию
  - Использовать white list
- Внедрить **Service Mesh:**
  - mTLS: каждому сервису по сертификату
  - Контроль Аутентификации и Авторизации
  - Контроль Egress трафика

Как протестировать свой кластер?



Как протестировать свой кластер?

```
$ ./kube-bench master
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[WARN] 1.1.1 Ensure that the --anonymous-auth argument is set to false (Not Scored)
[PASS] 1.1.2 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.3 Ensure that the --insecure-allow-any-token argument is not set (Not Scored)
[PASS] 1.1.4 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.5 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.6 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.7 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.8 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.9 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.10 Ensure that the admission control plugin AlwaysAdmit is not set (Scored)
[FAIL] 1.1.11 Ensure that the admission control plugin AlwaysPullImages is set (Scored)
[FAIL] 1.1.12 Ensure that the admission control plugin DenyEscalatingExec is set (Scored)
[WARN] 1.1.13 Ensure that the admission control plugin SecurityContextDeny is set (Scored)
[FAIL] 1.1.14 Ensure that the admission control plugin NamespaceLifecycle is set (Scored)
[FAIL] 1.1.15 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.19 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.20 Ensure that the --token-auth-file parameter is not set (Scored)
```

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