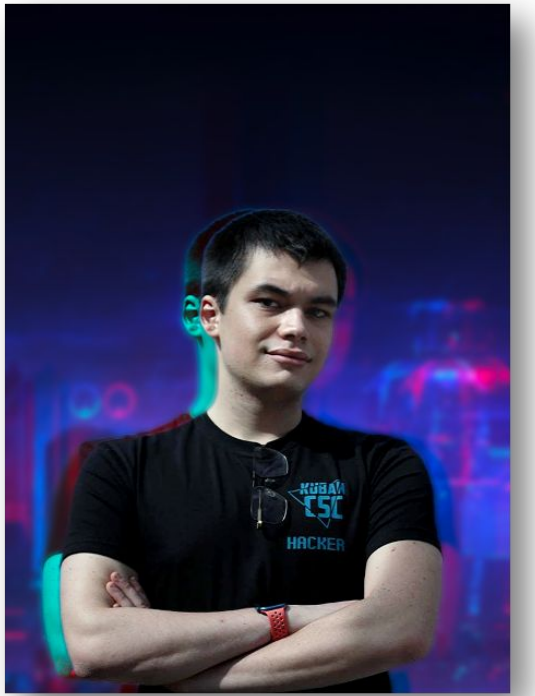
Сказ о рулевом и прорехах в пиджаке

Как защитить k8s

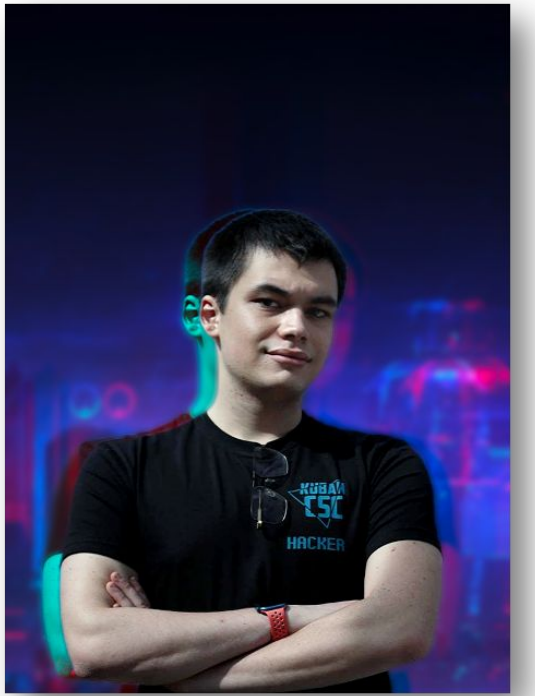
whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries



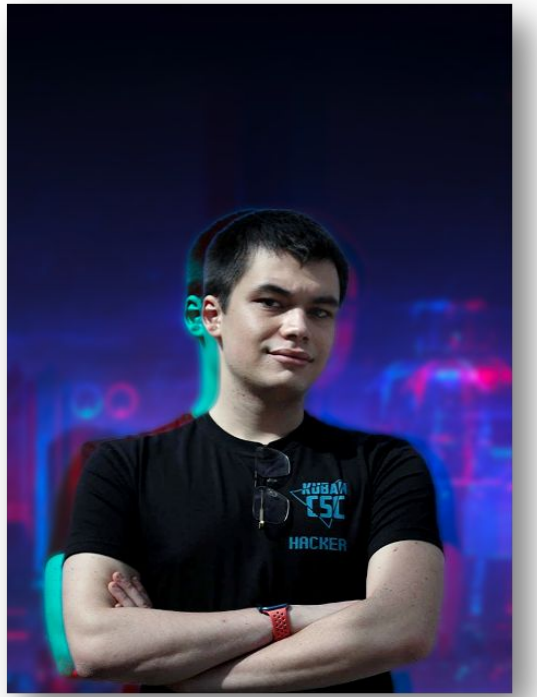
whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries
- DevOps - это не работа, а состояние души



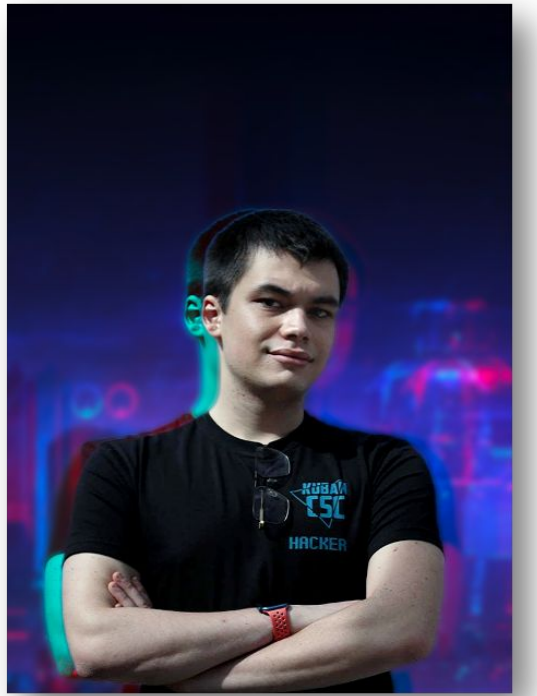
whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries
- DevOps - это не работа, а состояние души
- 3 года несу DevOps в массы в разных ВУЗах страны



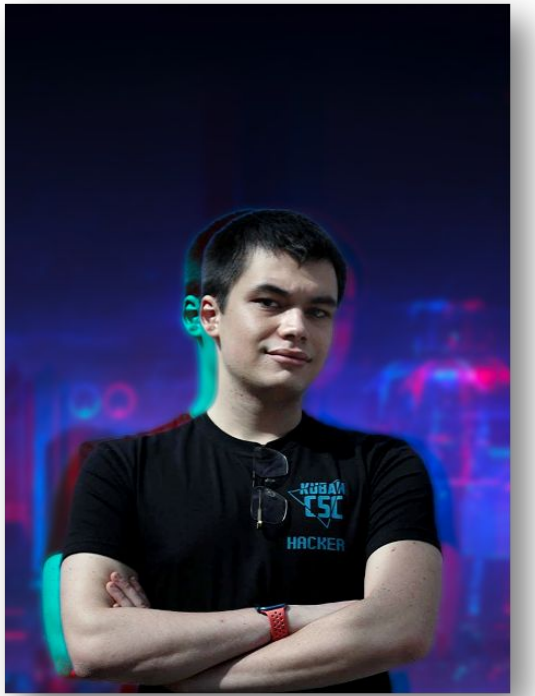
whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries
- DevOps - это не работа, а состояние души
- 3 года несу DevOps в массы в разных ВУЗах страны
- Руководитель команды разработки сервисов и DevOps на VrnCTF и CentralCTF, тех.специалист «Летней школы CTF 2023»



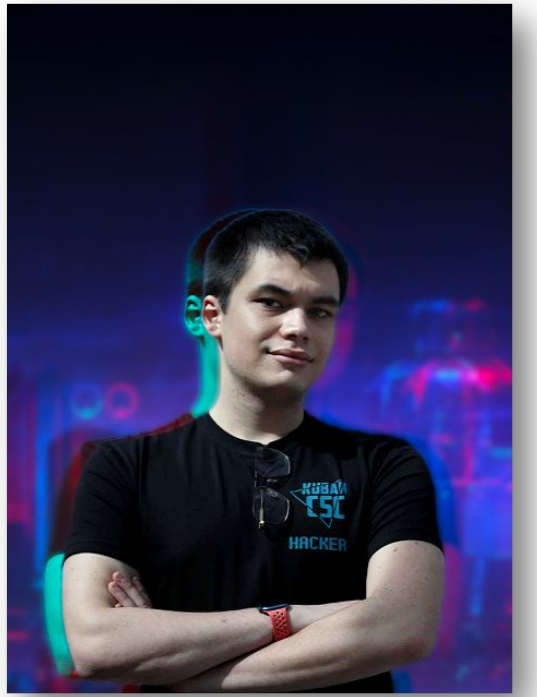
whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries
- DevOps - это не работа, а состояние души
- 3 года несу DevOps в массы в разных ВУЗах страны
- Руководитель команды разработки сервисов и DevOps на VrnCTF и CentralCTF, тех.специалист «Летней школы CTF 2023»
- Игрок CTF команды ONO



whoami

- TechLead команды разработки и поддержки сервисов ИБ в Wildberries
- DevOps - это не работа, а состояние души
- 3 года несу DevOps в массы в разных ВУЗах страны
- Руководитель команды разработки сервисов и DevOps на VrnCTF и CentralCTF, тех.специалист «Летней школы CTF 2023»
- Игрок CTF команды ONO
- Преподаю в DevOps магистратуре ИТМО



Пролог


k8s, как он должен быть
DevOps, который старается догнать все тренды
k8s у себя


Приемка
релиза

#1 - Уязвимая конфигурация подов

Container != VM

Механизмы изоляции в контейнере

- Linux Namespaces
- Capabilities
- Cgroups
- Seccomp
- AppArmor

Linux Namespaces

- Cgroups
- PID
- UTS
- Mount
- IPC (InterProcessConnection)
- Network
- User

Capabilities

Разрешение процессов на исполнение системных вызовов. Их около 20, определены в capabilities.h

- CAP_SYS_ADMIN - монтирование и размонтирование файловых систем
- CAP_NET_RAW - разрешить использовать сокеты RAW и PACKET
- CAP_SYS_MODULE - установка модулей ядра

Для начала отключим изоляцию

```
spec:
    hostNetwork: true
    hostIPC: true
    hostPID: true
```

Мама всегда говорила, что я привилегированный!

```
securityContext:
    allowPrivilegeEscalation: true
    privileged: true
```

Заставим под уехать на мастер

```
nodeSelector:
        node-role.kubernetes.io/master: ""
```

А если?

Нам админ запретил шедулиться на мастер!

Нам можно!

```
tolerations:
        - effect: NoSchedule
          operator: Exists
```

И на сладкое

```
volumes:
        - name: hostvol
          hostPath:
                path: /
volumeMounts:
        - mountPath: /host
          name: hostvol
```

Выводы

- Не запускать privileged контейнеры безо всякой для этого причины

Выводы

- Не запускать privileged контейнеры безо всякой для этого причины
- root в контейнерах недопустим

Выводы

- Не запускать privileged контейнеры безо всякой для этого причины
- root в контейнерах недопустим
- AllowPrivilegeEscalation - запрет потомкам иметь больше полномочий, чем родитель

Как это ~~запретить~~ контролировать?

Как это ~~запретить~~ контролировать?

Контроллеры политик:

- OPA Gatekeeper
- Kyverno

Как это ~~запретить~~ контролировать?

Контроллеры политик:

- OPA Gatekeeper
- Kyverno

Стандарты:

- CIS Benchmark
- Pod Security Standarts

#2 - Supply Chain Attacks

За чем стоит следить?

- Целостность образов

За чем стоит следить?

- Целостность образов
- Уязвимости библиотек

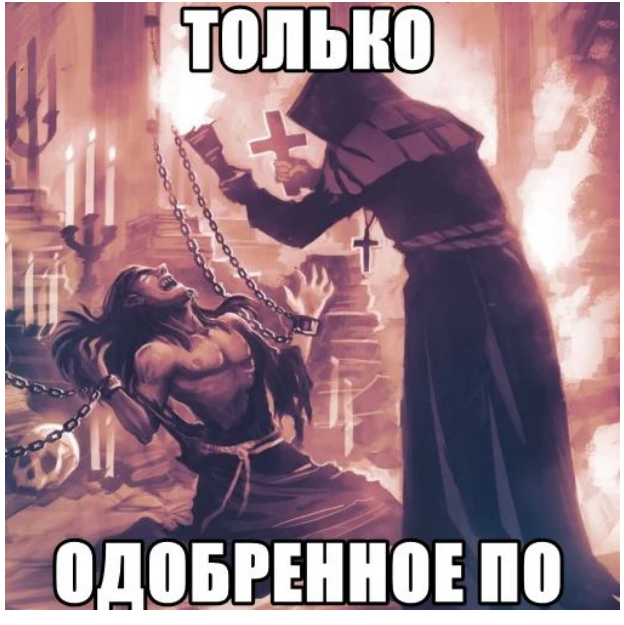
За чем стоит следить?

- Целостность образов
- Уязвимости библиотек
- Уязвимости open-source продуктов

Контроль целостности

- Механизм подписи образов как часть деплоя
  - Cosign
  - Notary

- Kyverno & Trivy уже умеют в проверку подписей!
- SLSA!



SLSA

- Гайдлайн по внедрению безопасных процессов соблюдения целостности сборочных артефактов и безопасности конвейеров
- Имеет 3 уровня сложности
- Стандартизация сопроводительной информации по сборке - provenance

SBOM

- Software Bill of Materials
- Стандарт документации об использованных зависимостях

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.5.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "library",
      "name": "acme-library",
      "version": "1.0.0"
    }
  ]
}
```

Профилактика от LotL атак & залатываем дырки

Профилактика от LotL атак & залатываем дырки

- Living of the Land - атака с использованием легитимного ПО, установленного в системе

Профилактика от LotL атак & залатываем дырки

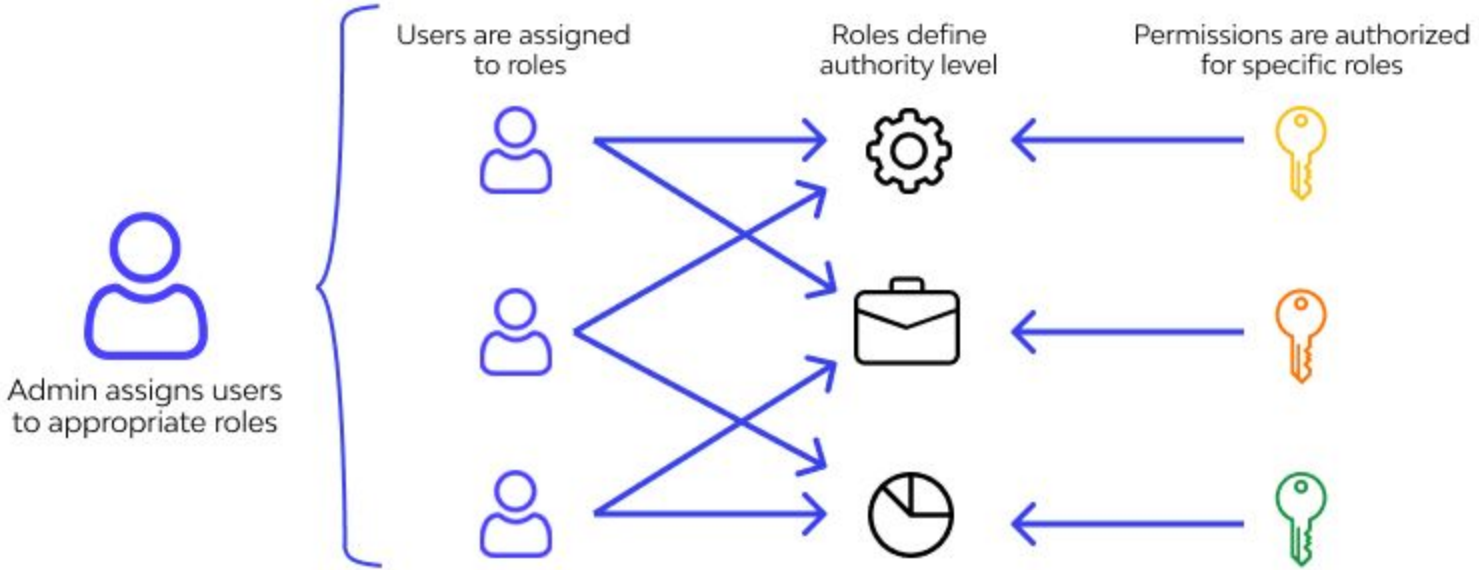
- Living of the Land - атака с использованием легитимного ПО, установленного в системе
- Использование расширенного образа на Dev-стендах, и Distroless/Scratch - на Pre-Prod & Prod

Профилактика от LotL атак & залатываем дырки

- Living of the Land - атака с использованием легитимного ПО, установленного в системе
- Использование расширенного образа на Dev-стендах, и Distroless/Scratch - на Pre-Prod & Prod
- Trivy-сканер - ваша правая рука

#3 - RBAC & Secrets

Role-Based Access Control



Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”
- Возможность делать RoleBindings должна быть у доверенных систем и людей

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”
- Возможность делать RoleBindings должна быть у доверенных систем и людей
- Избегать выдачи cluster-admin

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”
- Возможность делать RoleBindings должна быть у доверенных систем и людей
- Избегать выдачи cluster-admin
- Для RBAC следует использовать также системы аудита

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”
- Возможность делать RoleBindings должна быть у доверенных систем и людей
- Избегать выдачи cluster-admin
- Для RBAC следует использовать также системы аудита
- Вести контроль и за уже ненужными аккаунтами

Чем меньше знает под - тем крепче спит девопс

- Выключите автомаунт сервисных аккаунтов
- Исходите из принципа “наименьших полномочий”
- Возможность делать RoleBindings должна быть у доверенных систем и людей
- Избегать выдачи cluster-admin
- Для RBAC следует использовать также системы аудита
- Вести контроль и за уже ненужными аккаунтами
- Политики настраиваются на уровне Admission Controller

А что там с секретиками?)

- По умолчанию в etcd секреты не шифруются

А что там с секретиками?)

- По умолчанию в etcd секреты не шифруются
- Можно попробовать encryption in rest (но он все еще в бете)

А что там с секретиками?)

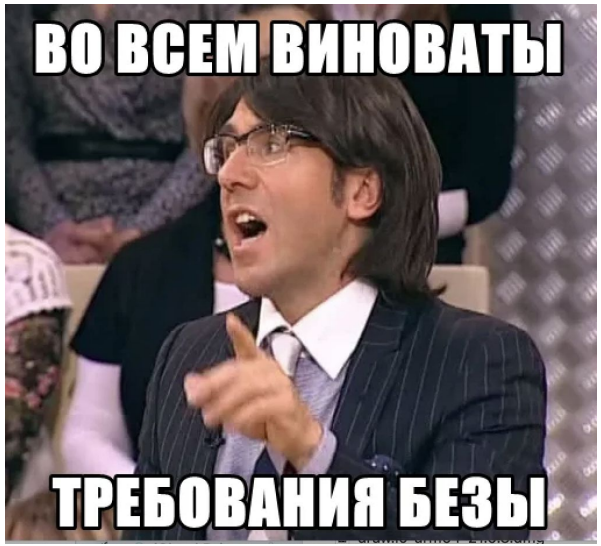
- По умолчанию в etcd секреты не шифруются
- Можно попробовать encryption in rest (но он все еще в бете)
- Vault никто не отменял, однако не надо переусердствовать :)

А что там с секретиками?)

- По умолчанию в etcd секреты не шифруются
- Можно попробовать encryption in rest (но он все еще в бете)
- Vault никто не отменял, однако не надо переусердствовать :)

А что там с секретиками?)

- По умолчанию в etcd секреты не шифруются
- Можно попробовать encryption in rest (но он все еще в бете)
- Vault никто не отменял, однако не надо переусердствовать :)



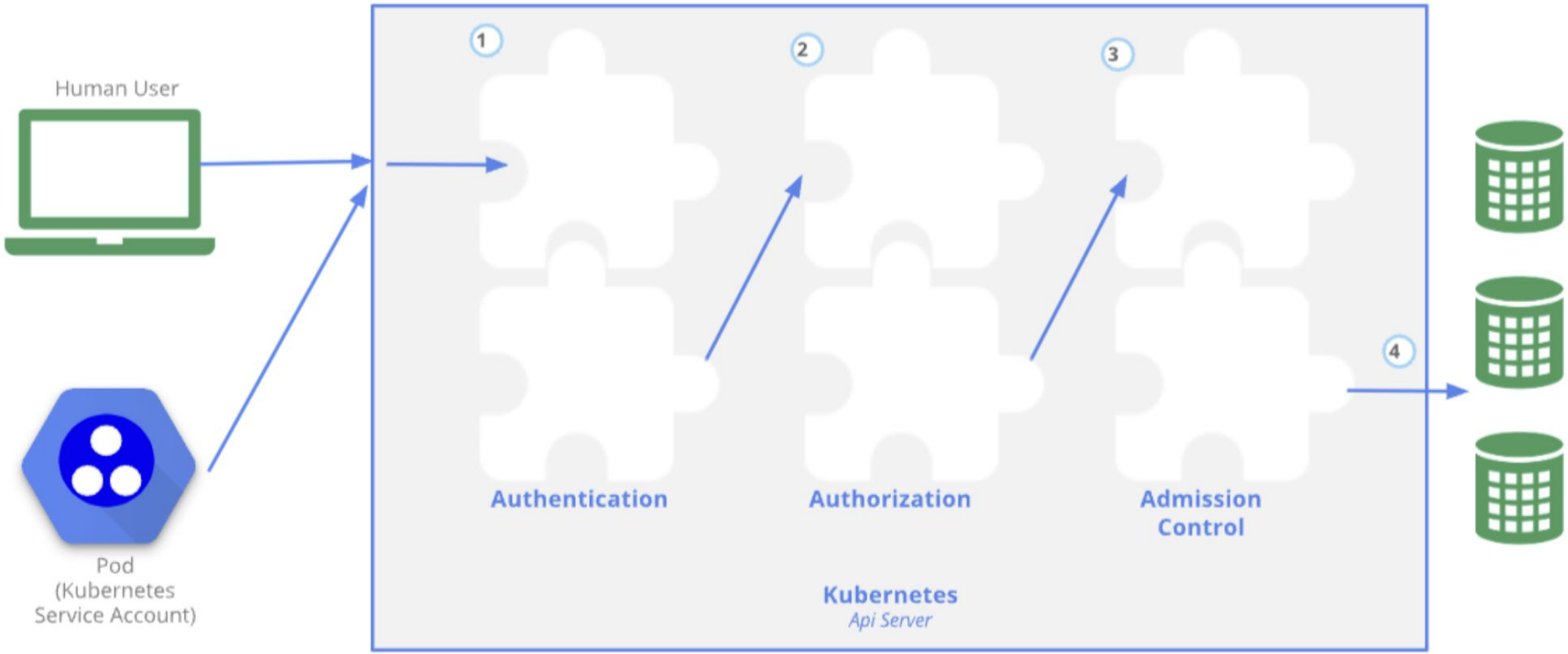
#4 - Централизованное соблюдение политик

У вас еще нет Admission Controller? Мы идем к вам!

Все используемые источники внешних ресурсов должны быть внесены в белый список:

- Менеджеры паролей
- Registry
- Хранилища файлов

#5 - Аутентификация


Human User
Pod
(Kubernetes
Service Account)
1
2
3
4
Authentication
Authorization
Admission
Control
Kubernetes
Api Server

Как защититься?

Как защититься?

- Не использовать аутентификацию по сертификатам

Как защититься?

- Не использовать аутентификацию по сертификатам
- Не изобретайте новых типов шифрования и аутентификации :)

Как защититься?

- Не использовать аутентификацию по сертификатам
- Не изобретайте новых типов шифрования и аутентификации :)
- 2FA по возможности

Как защититься?

- Не использовать аутентификацию по сертификатам
- Не изобретайте новых типов шифрования и аутентификации :)
- 2FA по возможности
- Не используйте ServiceAccounts для подключения извне

Как защититься?

- Не использовать аутентификацию по сертификатам
- Не изобретайте новых типов шифрования и аутентификации :)
- 2FA по возможности
- Не используйте ServiceAccounts для подключения извне
- Если надо - выпишите себе короткоживущий токен

Как защититься?

- Не использовать аутентификацию по сертификатам
- Не изобретайте новых типов шифрования и аутентификации :)
- 2FA по возможности
- Не используйте ServiceAccounts для подключения извне
- Если надо - выпишите себе короткоживущий токен
- Пользователям тоже выдавайте короткоживущие токены

#6 - Сетевая изоляция

Как готовить сети

- Иногда весьма полезно независимые блоки деплоить в разные кластеры (dev и prod)

Как готовить сети

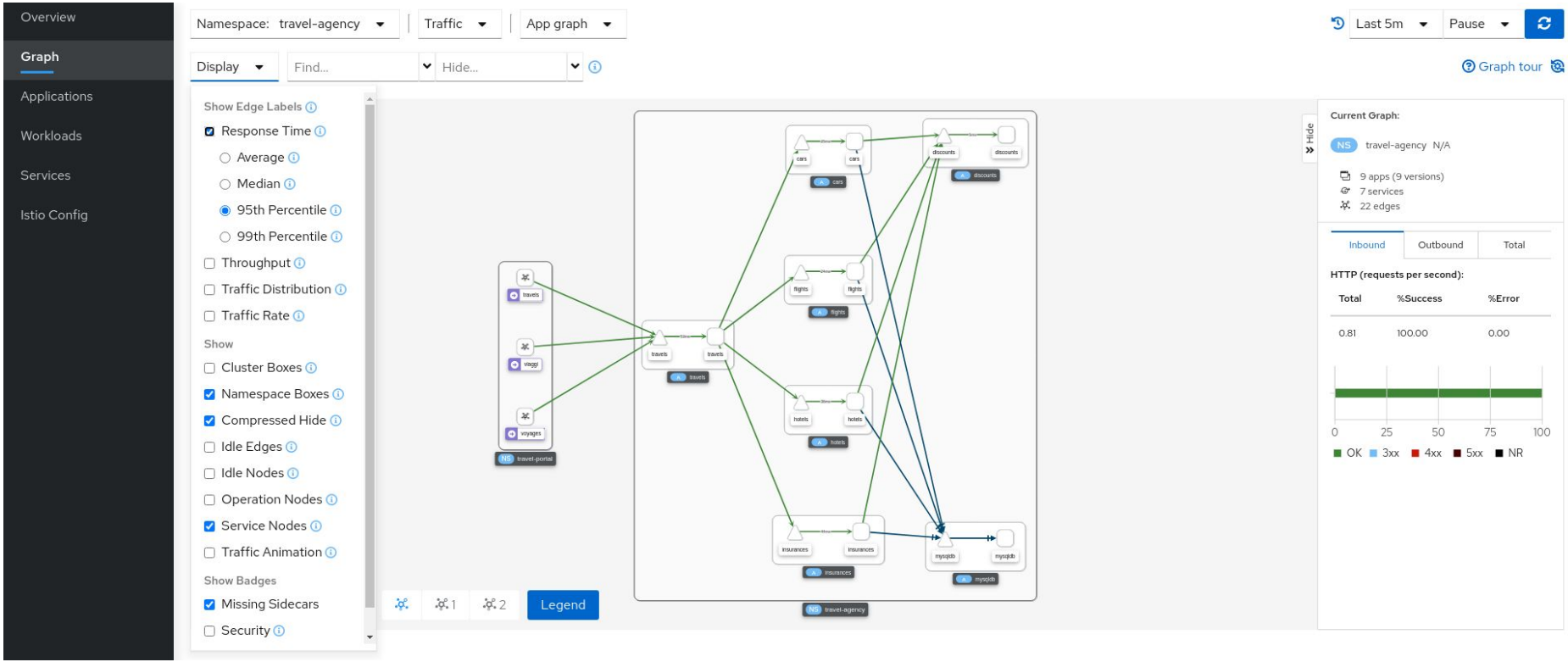
- Иногда весьма полезно независимые блоки деплоить в разные кластеры (dev и prod)
- Не пренебрегать встроенными NetworkPolicy

Как готовить сети

- Иногда весьма полезно независимые блоки деплоить в разные кластеры (dev и prod)
- Не пренебрегать встроенными NetworkPolicy
- Если стандартные кажутся сложными - попробуйте NetworkPolicy от вашего CNI Provider (Flannel, Calico)

Как готовить сети

- Иногда весьма полезно независимые блоки деплоить в разные кластеры (dev и prod)
- Не пренебрегать встроенными NetworkPolicy
- Если стандартные кажутся сложными - попробуйте NetworkPolicy от вашего CNI Provider (Flannel, Calico)
- Коль самурай истинно храбр - пусть пробует ServiceMesh


Overview
Graph
Applications
Workloads
Services
Istio Config
Namespace: travel-agency
Traffic
App graph
Last 5m
Pause
Display
Find...
Hide...
Graph tour
Show Edge Labels
Response Time
Average
Median
95th Percentile
99th Percentile
Throughput
Traffic Distribution
Traffic Rate
Show
Cluster Boxes
Namespace Boxes
Compressed Hide
Idle Edges
Idle Nodes
Operation Nodes
Service Nodes
Traffic Animation
Show Badges
Missing Sidecars
Security
Legend
Hide
Current Graph:
travel-agency N/A
9 apps (9 versions)
7 services
22 edges
Inbound
Outbound
Total
HTTP (requests per second):
Total
%Success
%Error
0.81
100.00
0.00
0
25
50
75
100
OK
3xx
4xx
5xx
NR

Поглядывайте за CVE!