Disrupting Kubernetes security

and

Advanced Kubernetes concepts in practice

Agenda

Pirsos.io presentation and demo

Advanced Kubernetes concepts in practice

Q&A

Pirsos.io

Pirsos.io - problems we are solving

Certificate management is hard to automate

Certificate management is hard in dynamic environments

Certificate management is hard

It should be easier and consistent

47% of companies come across challenges with security

37% of companies have difficulty scaling

Pirsos.io - what is it exactly

Works both on Openshift and Kubernetes
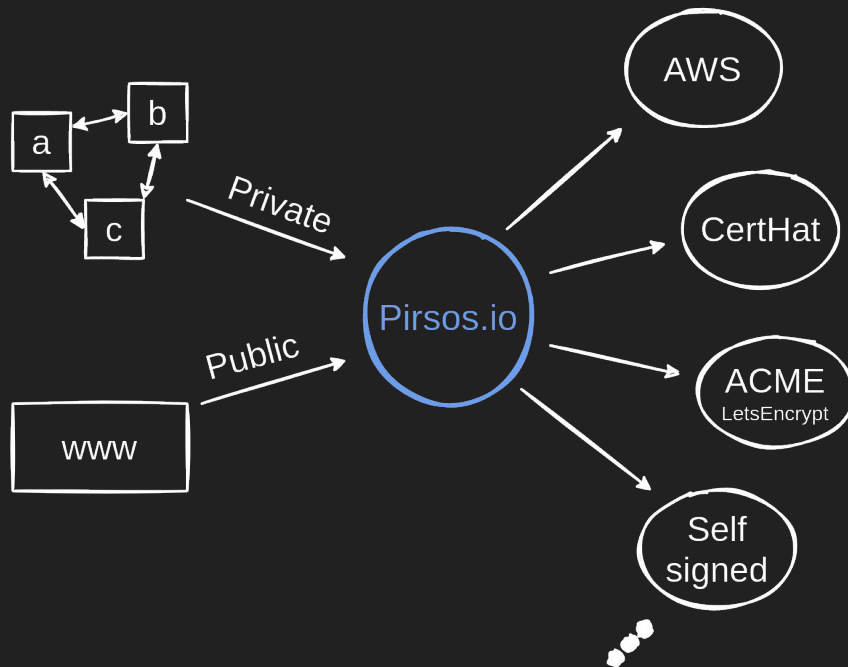
Automate your certificate management

Secure both public websites and microservices

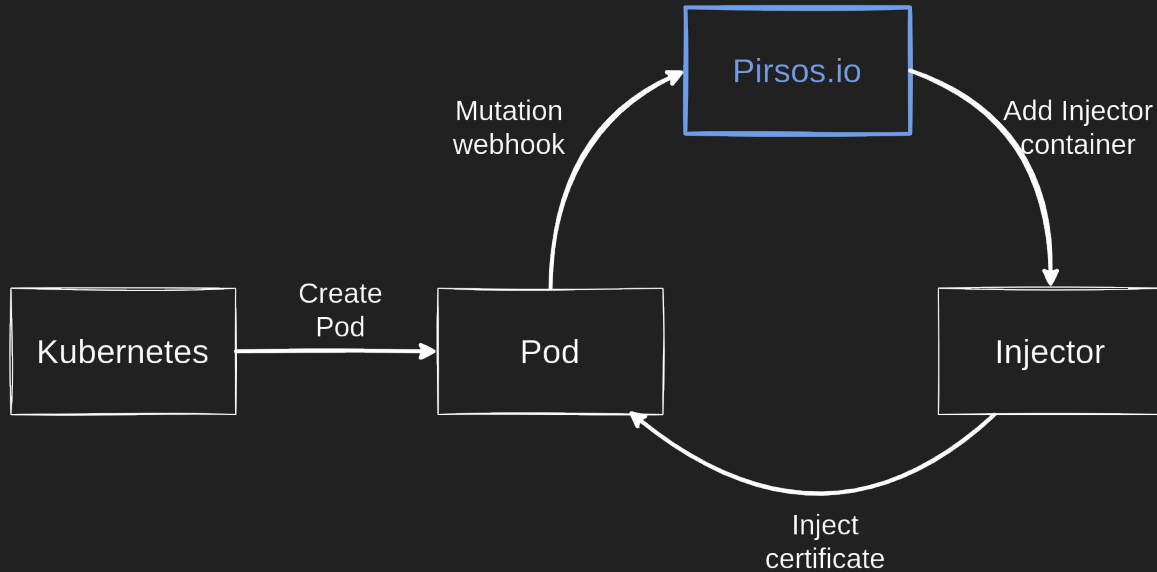Integrate with multiple certificate providers

Multiple certificate types

Manage it yourself, or… Don't!

Pirsos.io - integrations

- a
- b
- c

Private

Public

www

Pirsos.io

AWS

CertHat

ACME
LetsEncrypt

Self signed

Pirsos.io - how it works

Pirsos.io - Demo

Let's get to coding

Advanced Kubernetes concepts in practice

Admission controllers

Control Kubernetes objects using webhooks

Validate or mutate objects on the fly

Start it as a server and connect from any cluster

Admission controllers - validation

```
apiVersion: v1
kind: Pod
metadata:
  name: pod
  namespace: default
spec:
  containers:
    - name: hello-world
      image: hello-world
```

→

allowed: true

_____

allowed: false
reason: namespace 'default' not
             allowed

Admission controllers - mutation

```
apiVersion: v1
kind: Pod
metadata:
  name: pod
  namespace: default
spec:
  containers:
    - name: hello-world
      image: hello-world
```

→

```
apiVersion: v1
kind: Pod
metadata:
  name: pod
  namespace: default
  labels:
    mutated: true
spec:
  containers:
    - name: hello-world
      image: hello-world
```

Admission controllers - how we use them

Pirsos.io mutates new or updated Pod objects

Adds 1 init container and 1 sidecar container

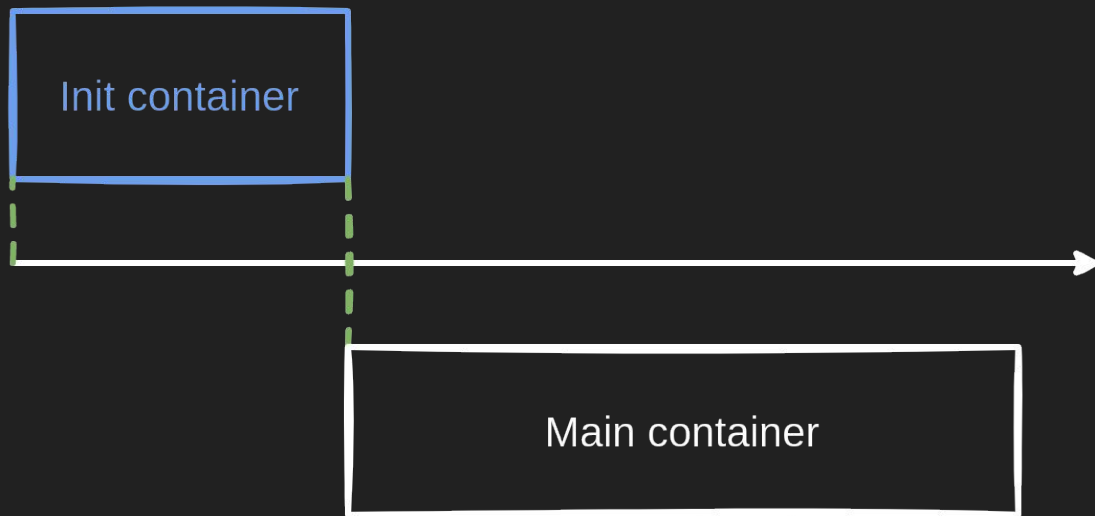Configuration for containers

Mounts volume

Admission controllers - how others use them

Kubernetes default admission controllers

Service mesh - inject proxy

LicenseSpring - application license management on Kubernetes/Openshift

Init containers - how it works

Init containers - how we use them

Certificate injector runs before the pod

Initializes certificates

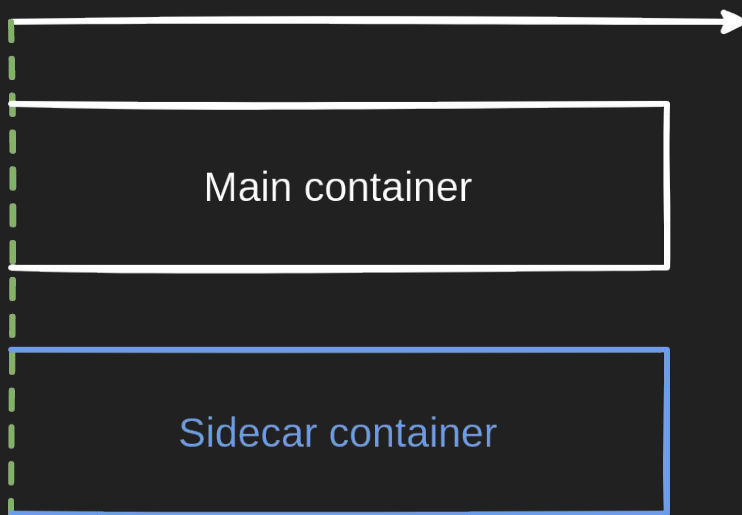Stores certificates in a volume or a Secret

Can disallow insecure Pods

Init containers - how others use them

Elasticsearch - install plugins

Service mesh - configure routing

Sidecar containers - how it works

Main container

Sidecar container

Sidecar containers - how we use them

Renewer container runs next to the main container

Restarts the pod after some time

New certificate issued

Sidecar containers - how others use them

Service mesh - proxy

Logging agents

slido

Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

Want to try out Pirsos?

Get in touch with:

leon@pirsos.io

edmon@pirsos.io

or

Visit Pirsos.io