KUB201 - DEFENDING KUBERNETES

Course Learning Objectives

Defending Kubernetes builds on the foundations of Defending Containers. In five modules, this course covers best practices for securing systems that use Kubernetes. You'll look at security considerations that range over every stage of Kubernetes development, including the build phase, deployment, and runtime.

Module 1 covers the process of preparing an application for a Kubernetes deployment.
Module 2 covers how to lock down the API server.
Module 3 covers best practices for ensuring a secure cluster setup.
Module 4 covers securing the pods where your application runs.
And module 5 covers network policy and the rules that govern how pods communicate in a Kubernetes cluster.

Description

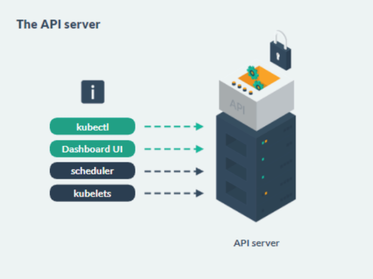
This course has been developed for DevOps and Systems Engineers who have some experience with Kubernetes and have completed Defending Containers as a prerequisite.

Audience

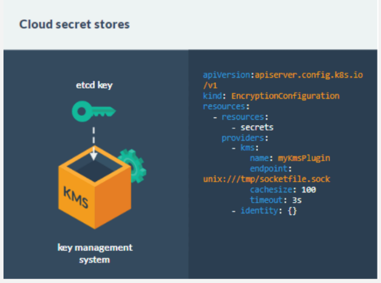
DevOps
Ops Engineers

Time Required

Tailored learning - 80 minutes total (approx.)



The API server



Cloud secret stores

```
apiVersion:apiserver.config.k8s.io
/v1
kind: EncryptionConfiguration
resources:
  - resources:
      - secrets
    providers:
      - kms:
          name: myKmsPlugin
          endpoint:
unix:///tmp/socketfile.sock
          cachesize: 100
          timeout: 3s
      - identity: {}
```

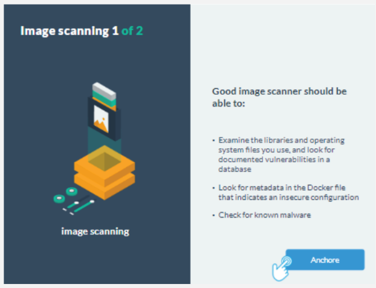


Image scanning 1 of 2

Good image scanner should be able to:

- Examine the libraries and operating system files you use, and look for documented vulnerabilities in a database
- Look for metadata in the Docker file that indicates an insecure configuration
- Check for known malware

Security Compass

KUB201 - DEFENDING KUBERNETES

Course Outline

1. Securing Images and the CI Pipeline

- In the past
- Shift security left
- Choosing base images
- Use minimal images
- Using images without vetting them
- Image scanning
- Best practice: Automate image scanning
- Scan images with an admission controller
- Code: Scan images with an admission controller
- Best practices for images

2. Protecting the API Server

- The API server
- API server attacks
- Newsflash: Cryptojacking attack at Tesla
- Review the kube-apiserver flags
- Close the insecure port
- Do not enable insecure ports
- Dashboard UI
- Use the Dashboard securely
- Dashboard proxy authentication
- Use RBAC to protect the API server
- Limiting RBAC privileges
- Managing RBAC complexity
- API server events
- Collect audit logs
- Setting an audit log policy
- Audit policy example
- Retrieving logs

3. Hardening Cluster Infrastructure

- Security in the trusted network
- Protect the configuration files
- Sensitive files
- Use TLS for every component
- Flags for TLS
- Encrypt the secrets in etcd
- Cloud secret stores
- Review configuration with kube-bench

4. Restricting Pods at Runtime

- Defense in depth with Kubernetes
- Limit the security context of your pods
- Choose a limited OS account
- Reject misconfigured pods
- Restrict your pods with seccomp
- Other tools
- Limit access to cluster resources
- RBAC guidelines

5. Hardening the Virtual Network

- The Kubernetes networking abstraction
- Understanding network traffic
- Kubernetes network policy
- Choosing a network policy implementation
- Define a minimal network policy
- Allow access to specific pods
- Fine-grained network policy
- Encrypt application traffic
- Using a service mesh

SecurityCompass