NOVATEC

Secure Development On Kubernetes

Security Meetup by SBA Research
10.06.2020

Andreas Falk

Introduction

Andreas Falk
Novatec Consulting

andreas.falk@novatec-gmbh.de / @andifalk

https://www.novatec-gmbh.de/beratung/agile-security

Agenda

1. What Can Go Wrong?
2. Application Security
3. Container Security
4. Kubernetes Security
5. Kubernetes Secrets

Where are the Slides and the Code?

Look here:

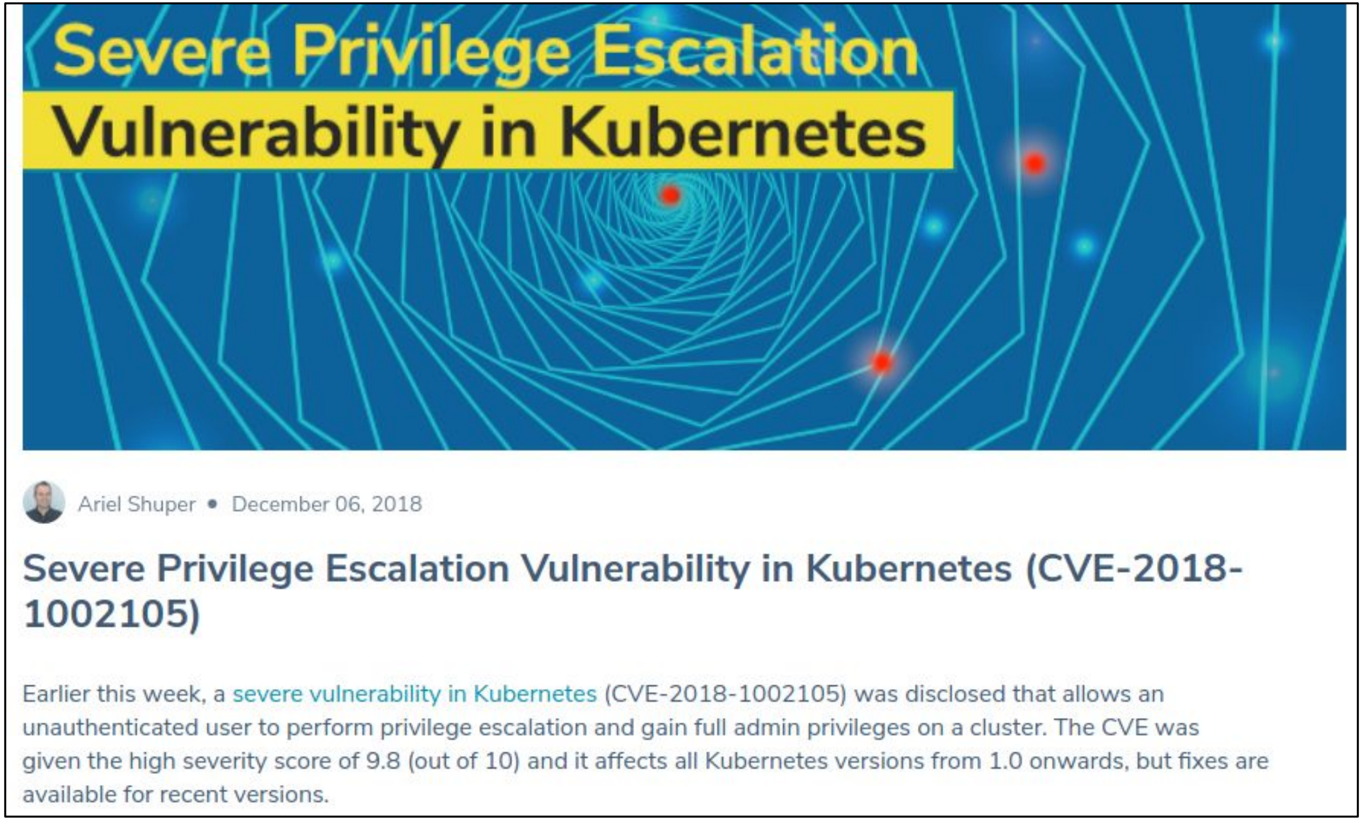
https://github.com/andifalk/secure-development-on-kubernetes

What can go wrong?

Introduction

Severe Vulnerability in Kubernetes

Source: https://blog.aquasec.com



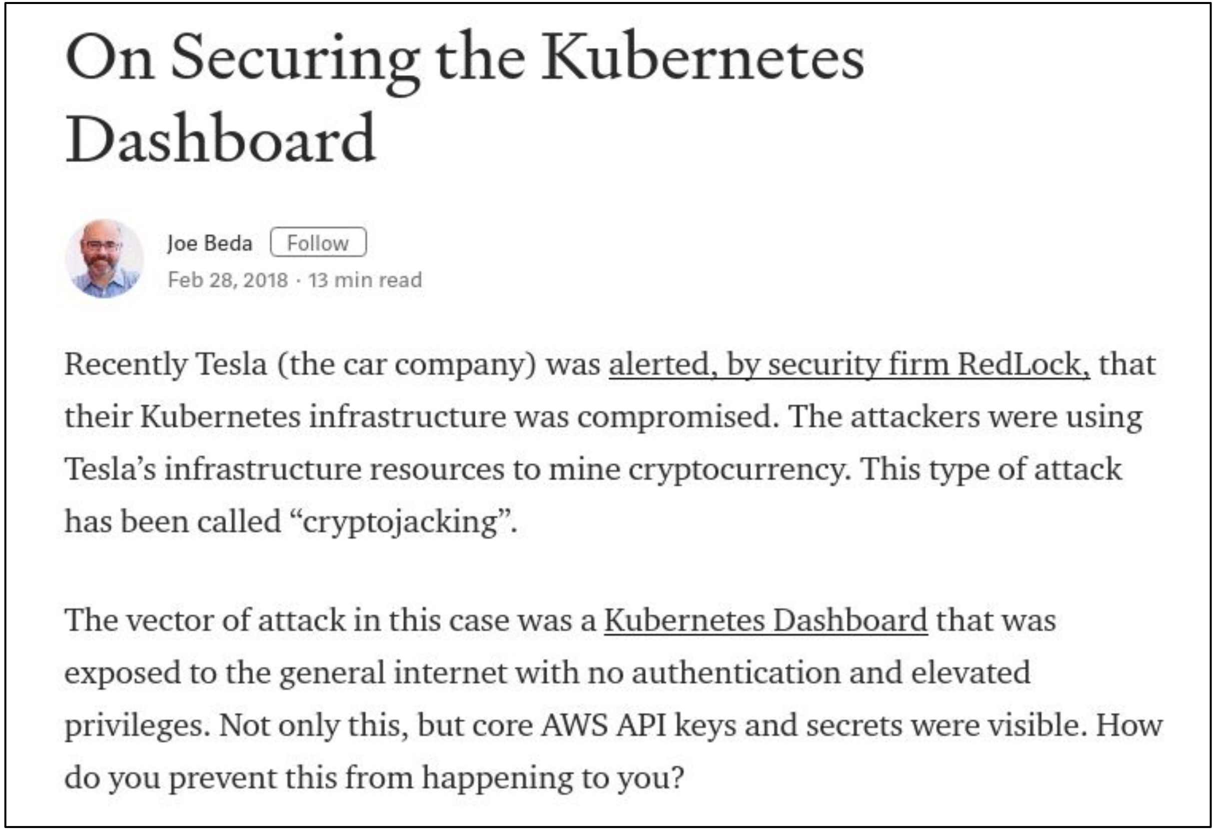
Ariel Shuper • December 06, 2018

Severe Privilege Escalation Vulnerability in Kubernetes (CVE-2018-1002105)

Earlier this week, a severe vulnerability in Kubernetes (CVE-2018-1002105) was disclosed that allows an unauthenticated user to perform privilege escalation and gain full admin privileges on a cluster. The CVE was given the high severity score of 9.8 (out of 10) and it affects all Kubernetes versions from 1.0 onwards, but fixes are available for recent versions.

Crypto Mining Via K8s Dashboard

Source: https://blog.heptio.com



On Securing the Kubernetes Dashboard

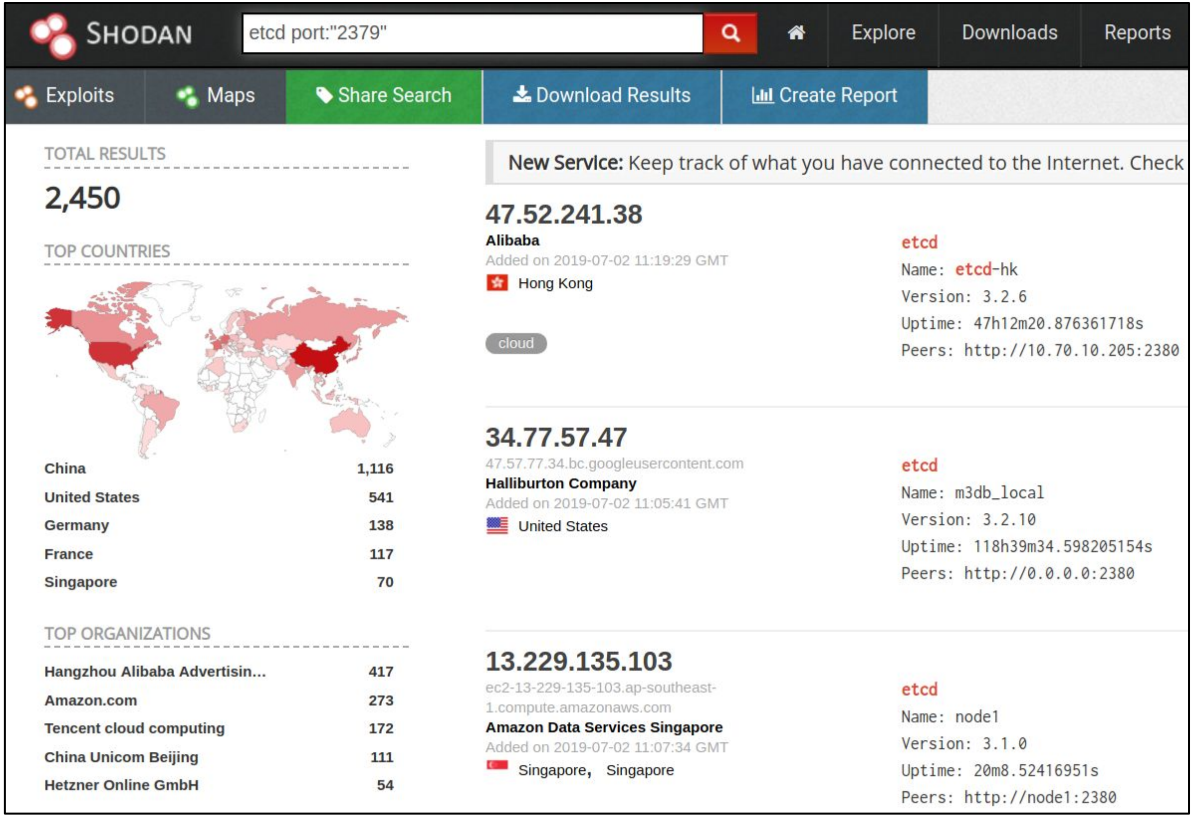
Joe Beda Follow

Feb 28, 2018 · 13 min read

Recently Tesla (the car company) was alerted, by security firm RedLock, that their Kubernetes infrastructure was compromised. The attackers were using Tesla's infrastructure resources to mine cryptocurrency. This type of attack has been called "cryptojacking".

The vector of attack in this case was a Kubernetes Dashboard that was exposed to the general internet with no authentication and elevated privileges. Not only this, but core AWS API keys and secrets were visible. How do you prevent this from happening to you?

Open ETCD Ports in Kubernetes (1)



TOTAL RESULTS

2,450

TOP COUNTRIES

China	1,116
United States	541
Germany	138
France	117
Singapore	70

TOP ORGANIZATIONS

Hangzhou Alibaba Advertisin...	417
Amazon.com	273
Tencent cloud computing	172
China Unicom Beijing	111
Hetzner Online GmbH	54

New Service: Keep track of what you have connected to the Internet. Check

47.52.241.38
Alibaba
Added on 2019-07-02 11:19:29 GMT
Hong Kong
cloud

```
etcd
Name: etcd-hk
Version: 3.2.6
Uptime: 47h12m20.876361718s
Peers: http://10.70.10.205:2380
```

34.77.57.47
47.57.77.34.bc.googleusercontent.com
Halliburton Company
Added on 2019-07-02 11:05:41 GMT
United States

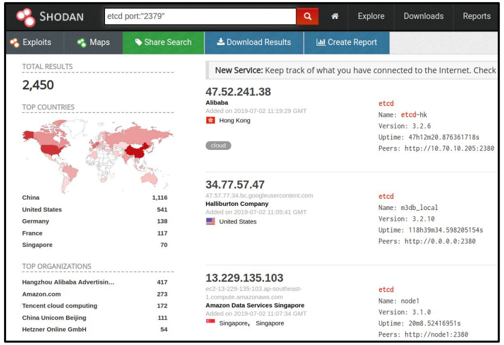
```
etcd
Name: m3db_local
Version: 3.2.10
Uptime: 118h39m34.598205154s
Peers: http://0.0.0.0:2380
```

13.229.135.103
ec2-13-229-135-103.ap-southeast-1.compute.amazonaws.com
Amazon Data Services Singapore
Added on 2019-07-02 11:07:34 GMT
Singapore, Singapore

```
etcd
Name: node1
Version: 3.1.0
Uptime: 20m8.52416951s
Peers: http://node1:2380
```

https://shodan.io

Open ETCD Ports in Kubernetes (2)



TOTAL RESULTS

2,450

TOP COUNTRIES

China	1,116
United States	541
Germany	138
France	117
Singapore	70

TOP ORGANIZATIONS

Hangzhou Alibaba Advertisin...	417
Amazon.com	273
Tencent cloud computing	172
China Unicom Beijing	111
Hetzner Online GmbH	54

New Service: Keep track of what you have connected to the Internet. Check

47.52.241.38
Alibaba
Added on 2019-07-02 11:19:29 GMT
Hong Kong
cloud

```
etcd
Name: etcd-hk
Version: 3.2.6
Uptime: 47h12m20.876361718s
Peers: http://10.70.10.205:2380
```

34.77.57.47
47.57.77.34.bc.googleusercontent.com
Halliburton Company
Added on 2019-07-02 11:05:41 GMT
United States

```
etcd
Name: m3db_local
Version: 3.2.10
Uptime: 118h39m34.598205154s
Peers: http://0.0.0.0:2380
```

13.229.135.103
ec2-13-229-135-103.ap-southeast-1.compute.amazonaws.com
Amazon Data Services Singapore
Added on 2019-07-02 11:07:34 GMT
Singapore, Singapore

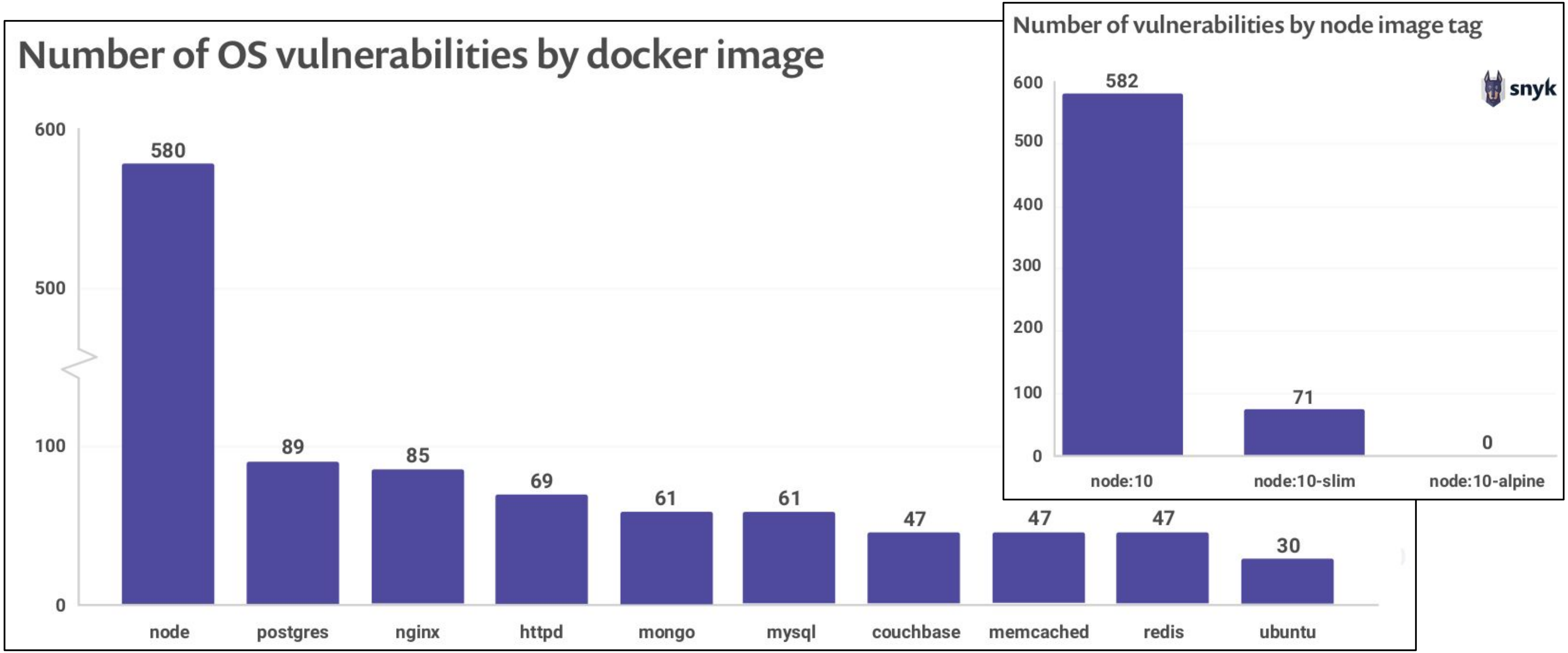
```
etcd
Name: node1
Version: 3.1.0
Uptime: 20m8.52416951s
Peers: http://node1:2380
```

```
$ etcdctl --endpoints=http://xx.xx.xx.xx:2379
cluster-health

member b97ee4034db41d17 is healthy: got healthy
result
from http://xx.xx.xx.xx:2379
cluster is healthy
```

https://github.com/etcd-io/etcd/releases

Vulnerable Docker Images

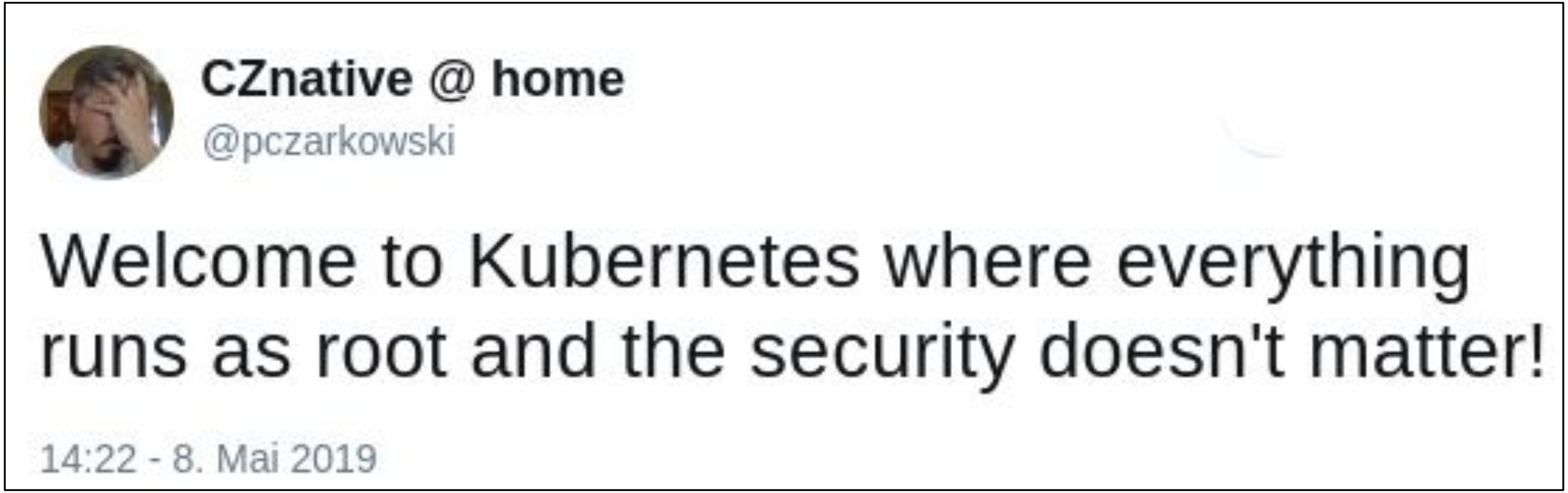
Source: The state of open source security report (snyk.io)



Number of OS vulnerabilities by docker image

Number of vulnerabilities by node image tag

All is Root 😱



CZnative @ home

@pczarkowski

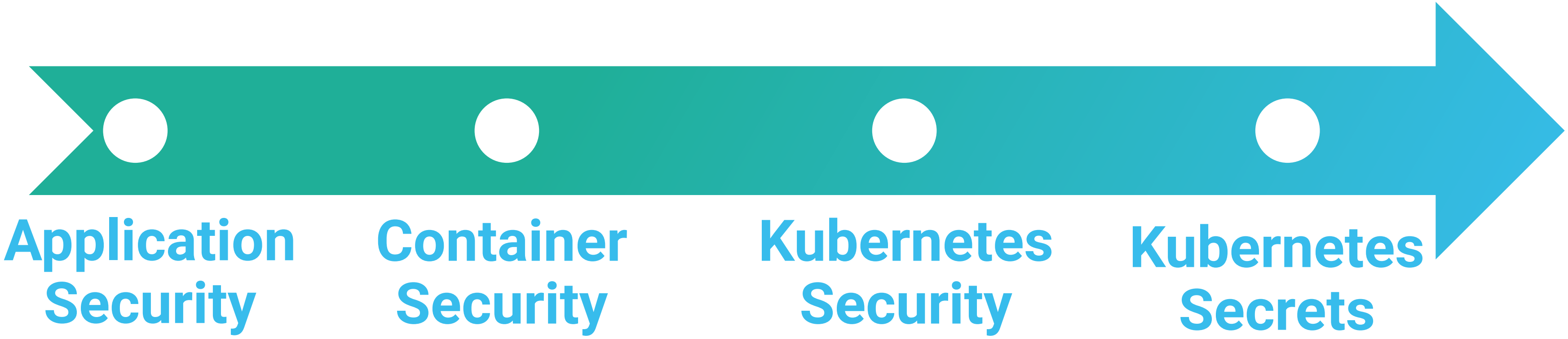
Welcome to Kubernetes where everything runs as root and the security doesn't matter!

14:22 - 8. Mai 2019

So what can WE do as Developers?

Application- / Docker- / K8s-Security

The Path for Secure Development on K8s



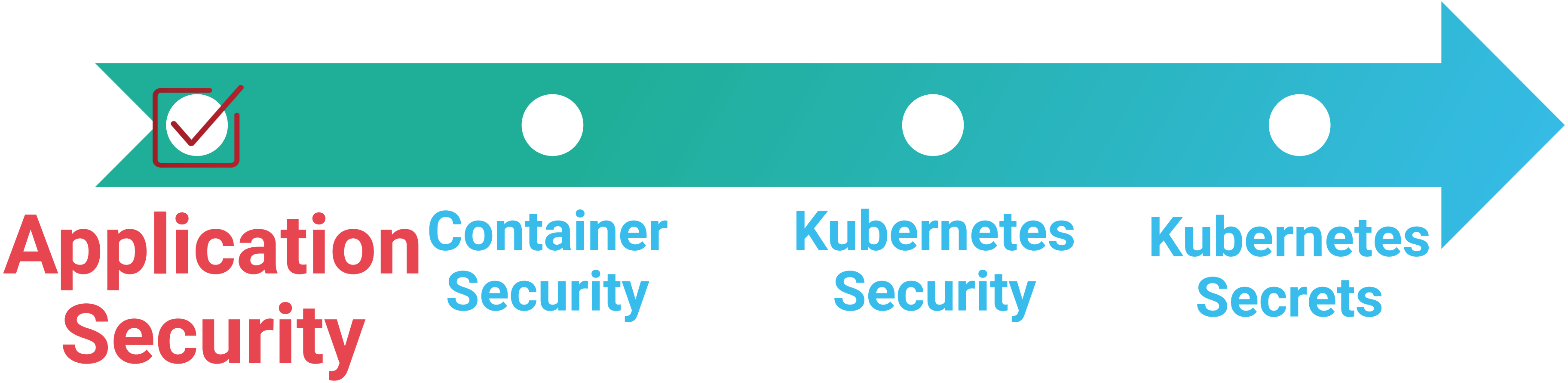
Application Security

Container Security

Kubernetes Security

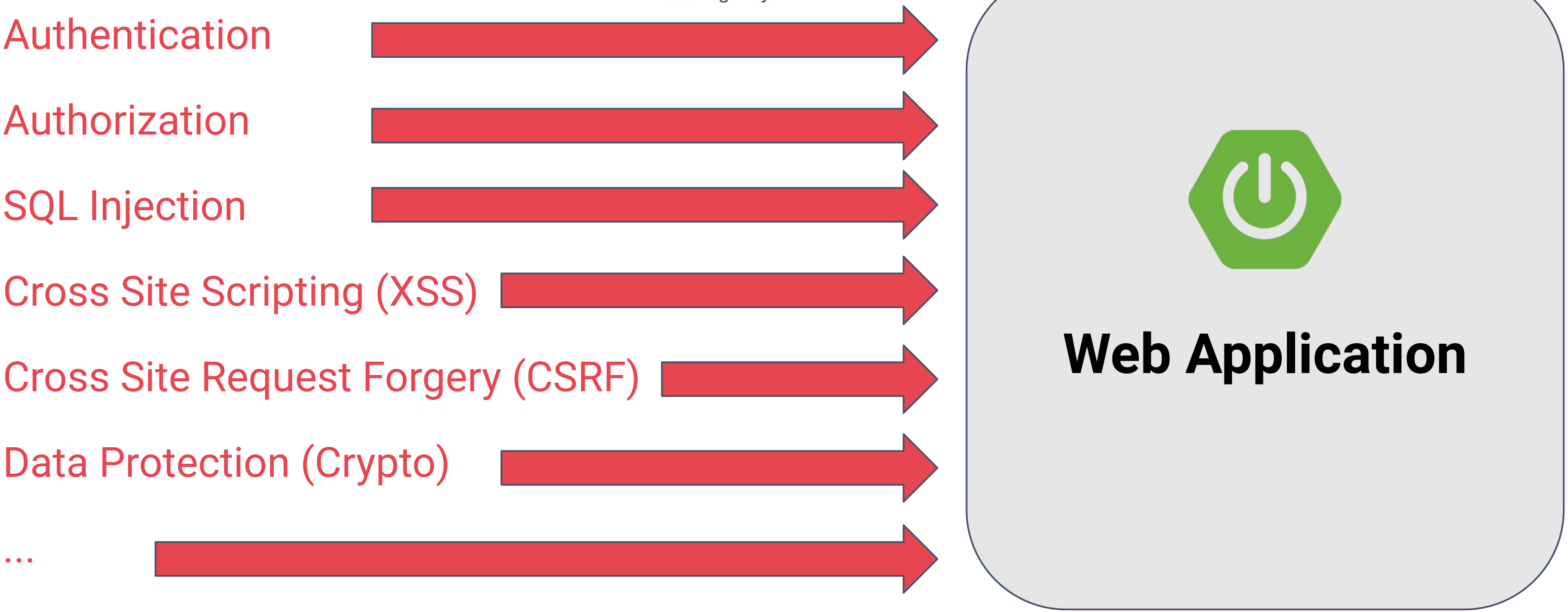
Kubernetes Secrets

The Path for Secure Development on K8s



Application Security

OWASP
Open Web Application
Security Project



Authentication

Authorization

SQL Injection

Cross Site Scripting (XSS)

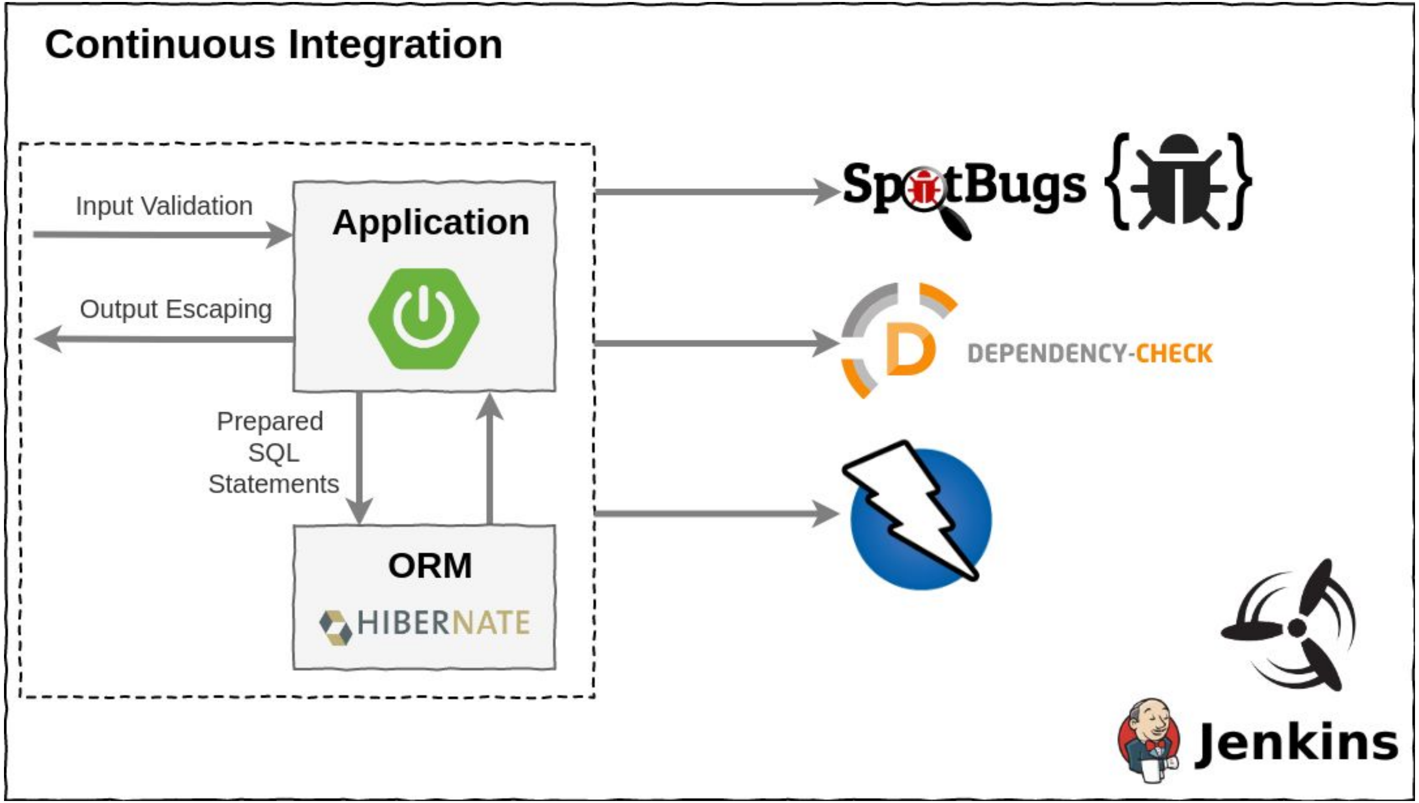
Cross Site Request Forgery (CSRF)

Data Protection (Crypto)

...

Web Application

Application Security

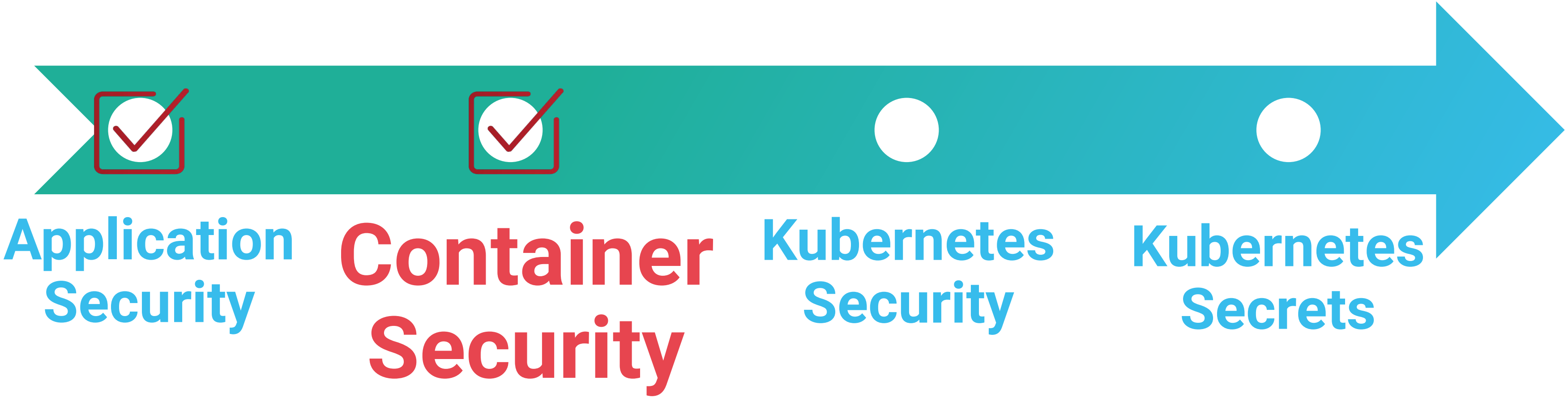


Live Demo: Show me the code

Iteration 1: Application Security

https://github.com/andifalk/secure-development-on-kubernetes

The Path for Secure Development on K8s



☑ Application Security

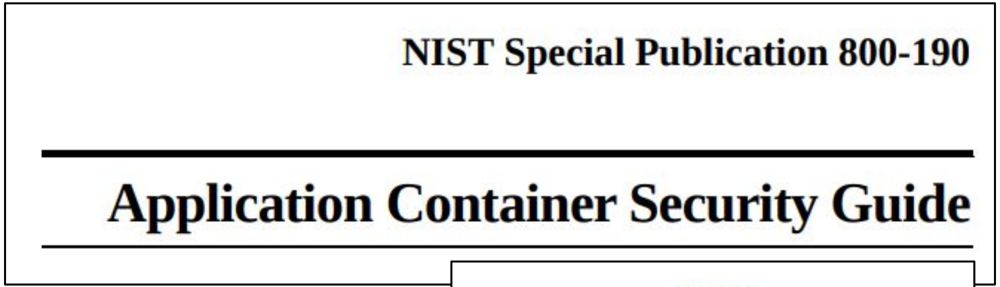
☑ **Container Security**

○ Kubernetes Security

○ Kubernetes Secrets

OWASP Docker Top 10

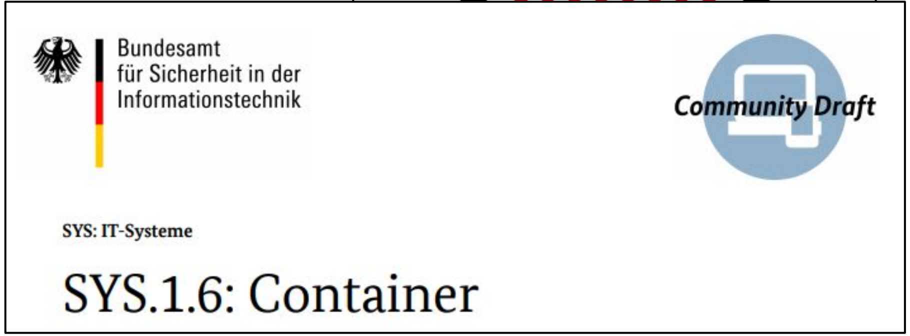
1. Secure User Mapping
2. Patch Management Strategy
3. Network Segmentation and Firewalling
4. Secure Defaults and Hardening
5. Maintain Security Contexts
6. Protect Secrets
7. Resource Protection
8. Container Image Integrity and Origin
9. Follow Immutable Paradigm
10. Logging



NIST Special Publication 800-190

Application Container Security Guide

OWASP
Container Security Verification Standard



Bundesamt
für Sicherheit in der
Informationstechnik

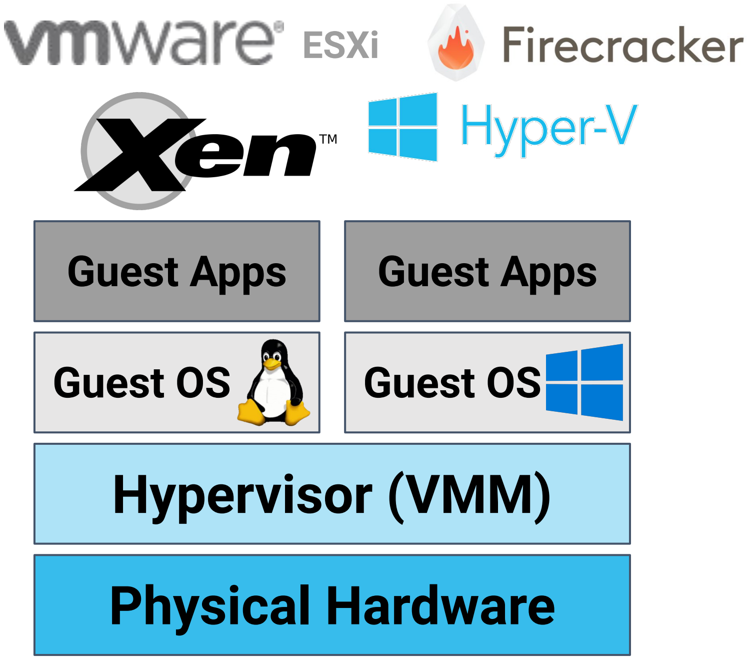
Community Draft

SYS: IT-Systeme

SYS.1.6: Container

https://github.com/OWASP/Docker-Security
https://doi.org/10.6028/NIST.SP.800-190
https://github.com/OWASP/Container-Security-Verification-Standard
https://www.bsi.bund.de

Virtual Machine (VM) Basics



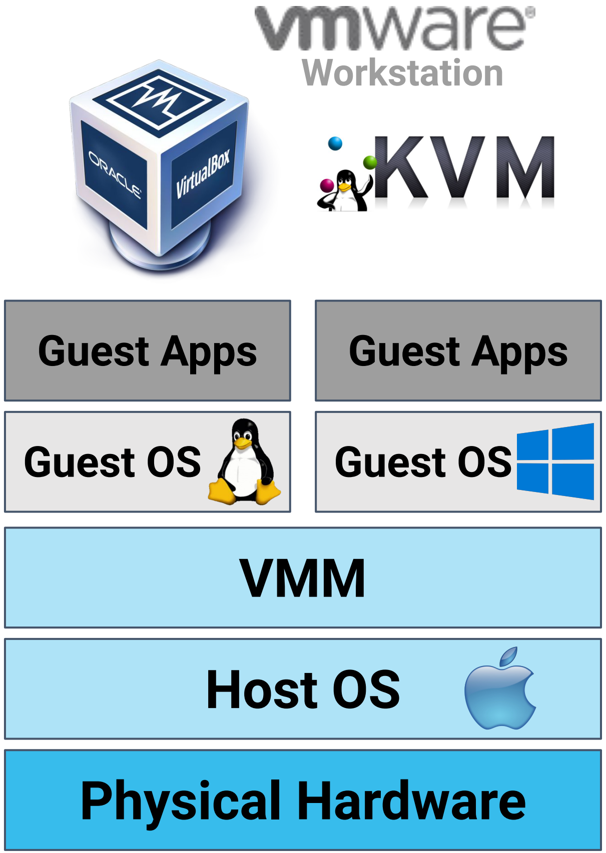
Guest Apps | Guest Apps

Guest OS | Guest OS

Hypervisor (VMM)

Physical Hardware

Type 1 Virtual Machine Monitor



Guest Apps | Guest Apps

Guest OS | Guest OS

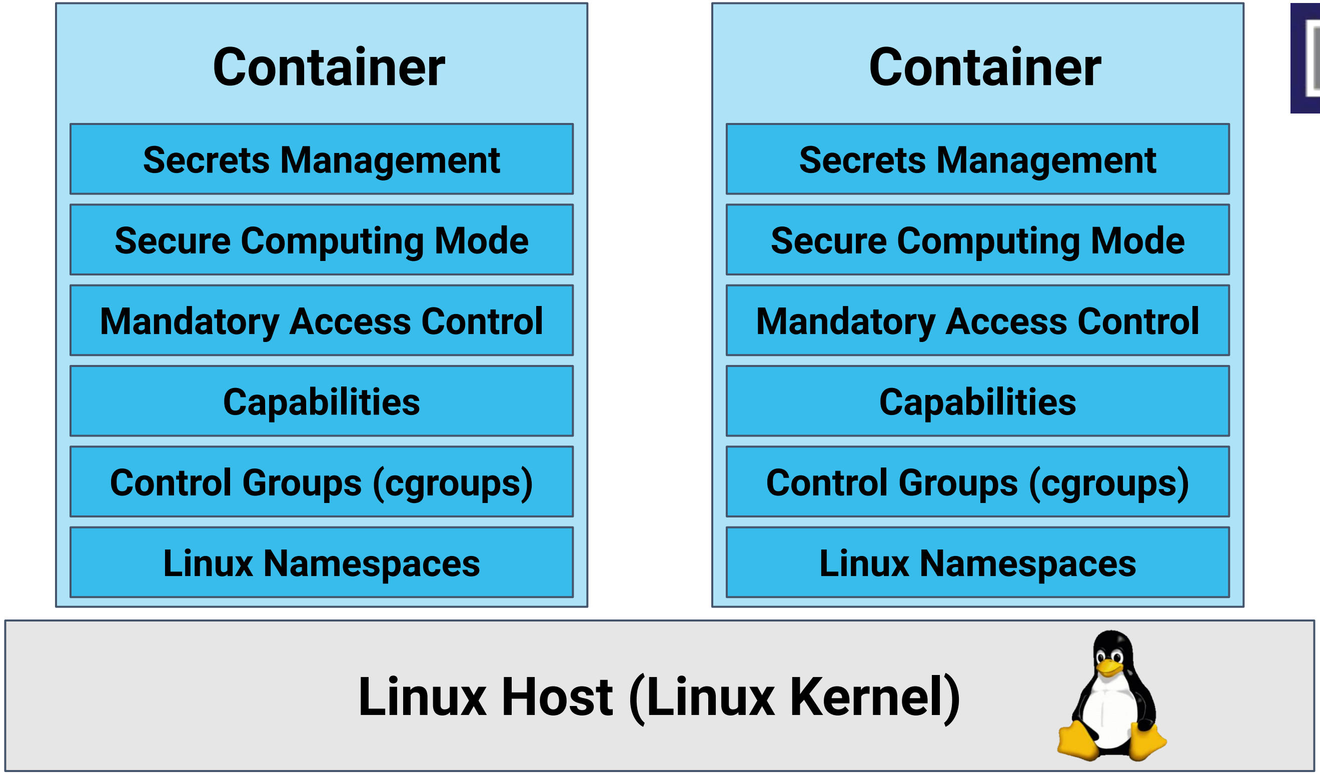
VMM

Host OS

Physical Hardware

Type 2 Virtual Machine Monitor

Container (Security) Basics



Container

- Secrets Management
- Secure Computing Mode
- Mandatory Access Control
- Capabilities
- Control Groups (cgroups)
- Linux Namespaces

Container

- Secrets Management
- Secure Computing Mode
- Mandatory Access Control
- Capabilities
- Control Groups (cgroups)
- Linux Namespaces

Linux Host (Linux Kernel)

OPEN CONTAINER INITIATIVE

docker

rkt

LXD

Linux Kernel Namespaces

- Process IDs
- Network
- Mount Points
- Inter-Process Communications (IPC)
- User & Group IDs
- Unix Timesharing System (UTS): hostname & domain names
- Control groups (cgroups)

```
$ man namespaces
$ sudo lsns
```

Linux Control Groups (cgroups)

- Resource Limits
  - CPU
  - Memory
  - Devices
  - Processes
  - Network

For Java this only works with container aware JDK versions as of **OpenJDK 8u192** or above
Recommendation: Use Java 11

Linux Capabilities

- Break up privileges into smaller units
  - CAP_SYS_ADMIN
  - CAP_NET_ADMIN
  - CAP_NET_BIND_SERVICE
  - CAP_CHOWN
  - …

```
$ man capabilities
$ docker run --cap-drop=ALL --cap-add=NET_BIND_SERVICE
```

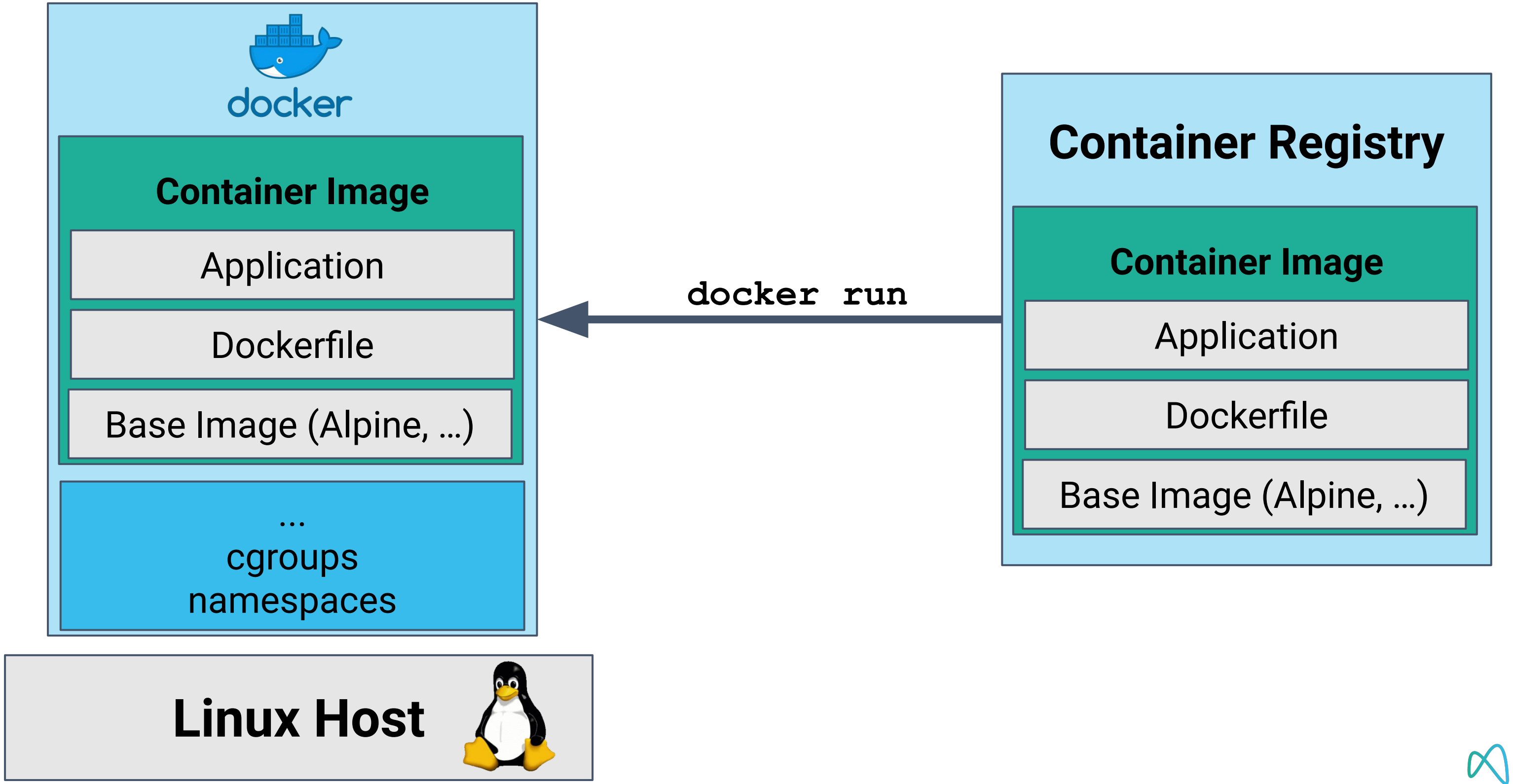
http://man7.org/linux/man-pages/man7/capabilities.7.html

Linux Mandatory Access Control & System Calls

- Restrict System Calls
  - Secure Computation Mode (seccomp)
  - Google gVisor
- Linux Kernel Security Modules (MAC)
  - AppArmor
  - Security-Enhanced Linux (SELinux)

https://docs.docker.com/engine/security/seccomp
https://apparmor.net
https://en.wikipedia.org/wiki/Security-Enhanced_Linux
https://gvisor.dev/docs

Docker Images



docker

Container Image

Application

Dockerfile

Base Image (Alpine, …)

…
cgroups
namespaces

Linux Host

```
docker run
```

Container Registry

Container Image

Application

Dockerfile

Base Image (Alpine, …)

Say No To Root!

USER directive in Dockerfile

```
FROM openjdk:11-jre-slim
COPY hello-spring-kubernetes-1.0.0-SNAPSHOT.jar app.jar
EXPOSE 8080
RUN addgroup --system --gid 1002 app && adduser
    --system --uid 1002 --gid 1002 appuser
USER 1002
ENTRYPOINT java -jar /app.jar
```

https://opensource.com/article/18/3/just-say-no-root-containers

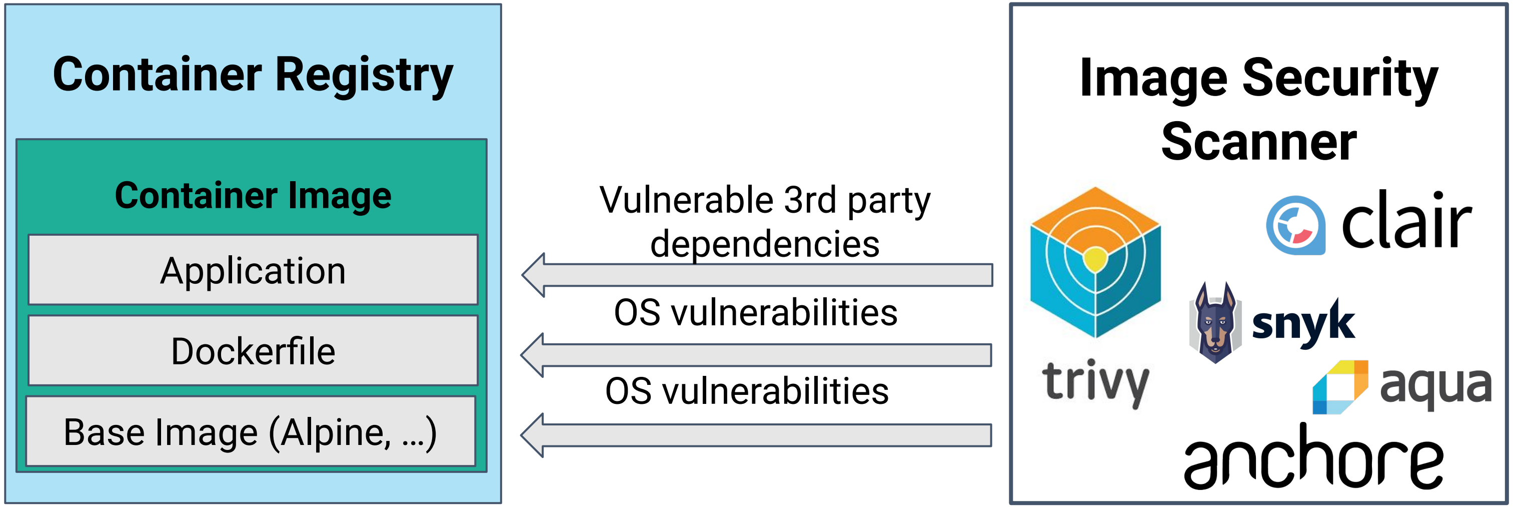
Say No To Root!

Use JIB and Distroless Images

```
plugins {
  id 'com.google.cloud.tools.jib' version '...'
}

jib {
 container {
   user = 1002
 }
}
```

https://github.com/GoogleContainerTools/jib

Docker Image Security



Container Registry

Container Image

Application

Dockerfile

Base Image (Alpine, ...)

Vulnerable 3rd party dependencies

OS vulnerabilities

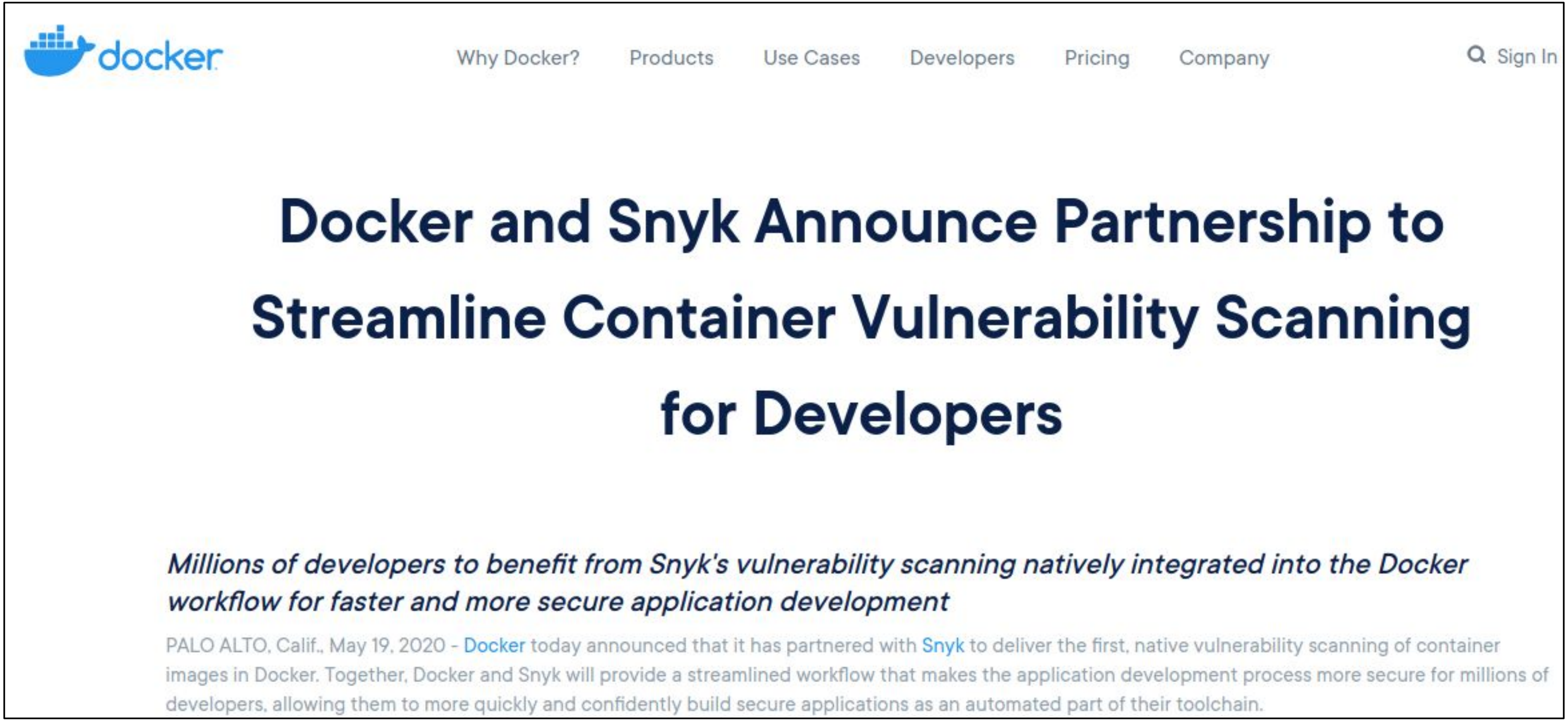
OS vulnerabilities

Image Security Scanner

Keep Being Secure

- Perform Image Scanning
  - Anchore
  - Clair
  - Trivy
- Use Up-To-Date Base Images

https://anchore.com/opensource/
https://github.com/coreos/clair
https://github.com/aquasecurity/trivy
https://www.docker.com/blog/announcing-scanning-from-snyk-for-docker



Docker and Snyk Announce Partnership to Streamline Container Vulnerability Scanning for Developers

Millions of developers to benefit from Snyk's vulnerability scanning natively integrated into the Docker workflow for faster and more secure application development

PALO ALTO, Calif., May 19, 2020 - Docker today announced that it has partnered with Snyk to deliver the first, native vulnerability scanning of container images in Docker. Together, Docker and Snyk will provide a streamlined workflow that makes the application development process more secure for millions of developers, allowing them to more quickly and confidently build secure applications as an automated part of their toolchain.

https://www.docker.com/press-release/Docker-Snyk-Announce-Partnership-Container-Vulnerability-Scanning

Live Demo: Show me the code

Iteration 2: Container Security

https://github.com/andifalk/secure-development-on-kubernetes

The Path for Secure Development on K8s

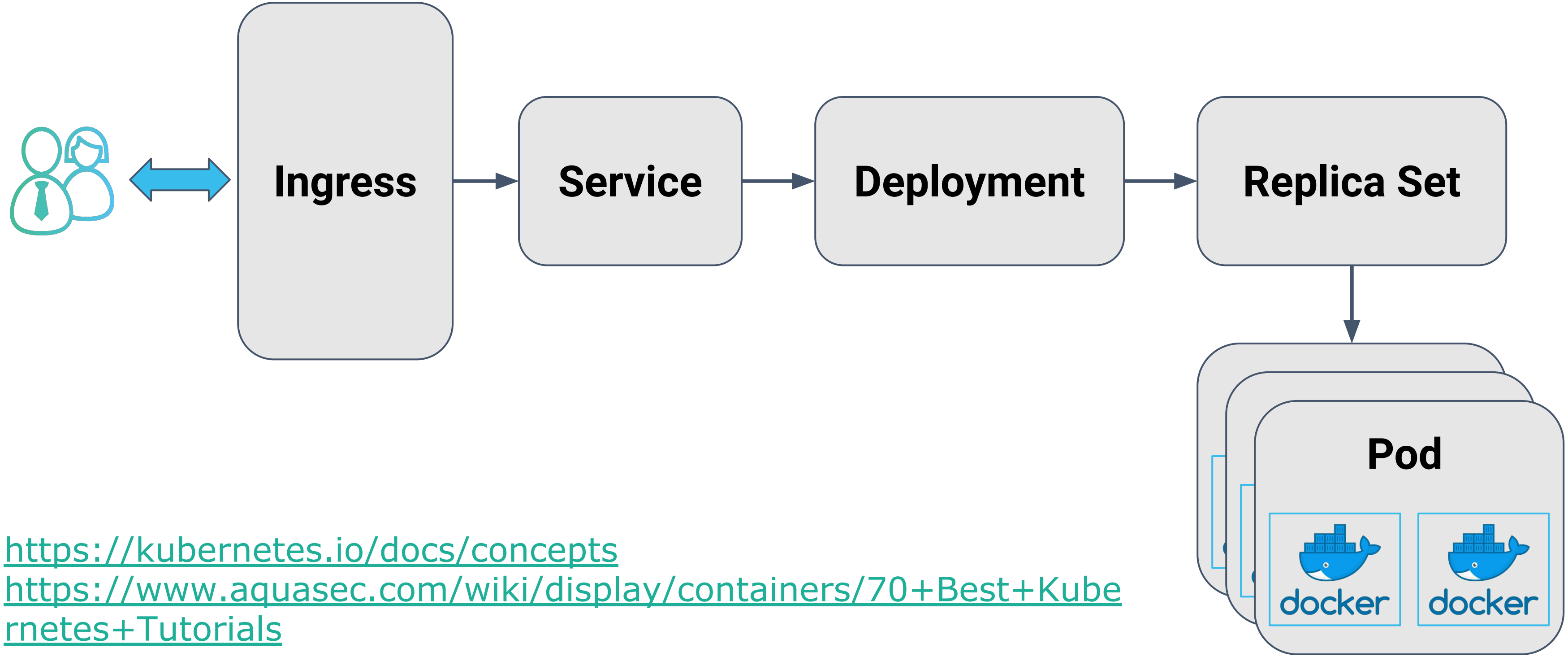
☑ Application Security

☑ Container Security

☑ Kubernetes Security

○ Kubernetes Secrets

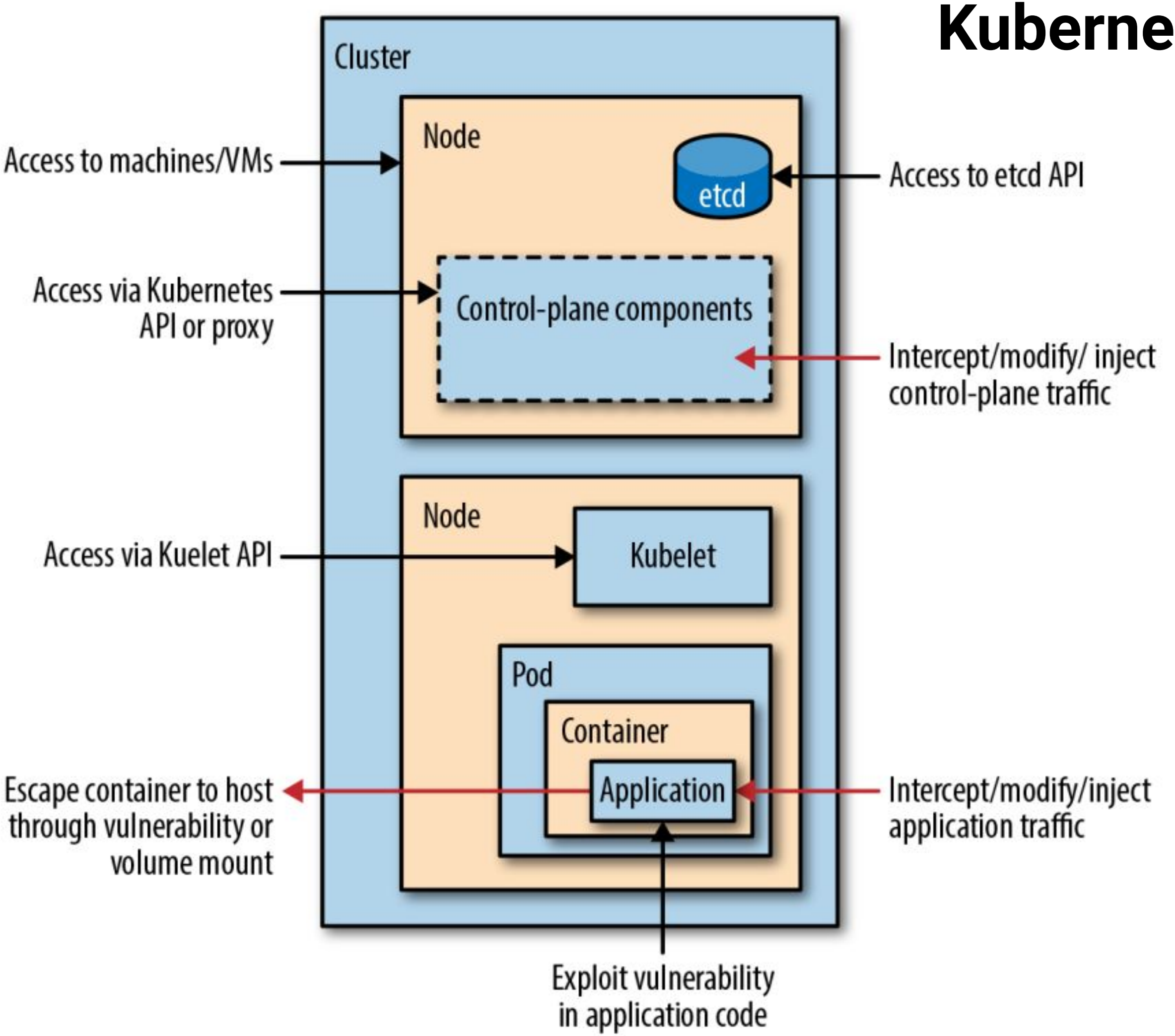
Kubernetes Basics



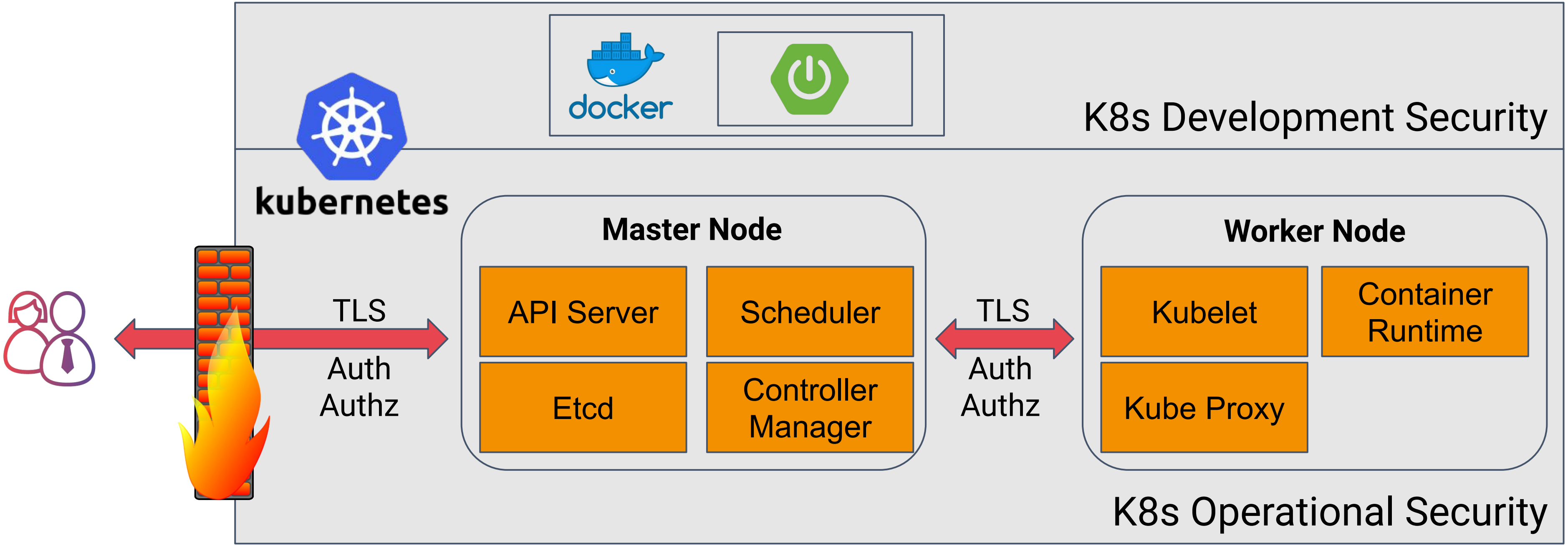
https://kubernetes.io/docs/concepts
https://www.aquasec.com/wiki/display/containers/70+Best+Kubernetes+Tutorials

Kubernetes attack vectors

Source:
Kubernetes Security, O'Reilly, 2018

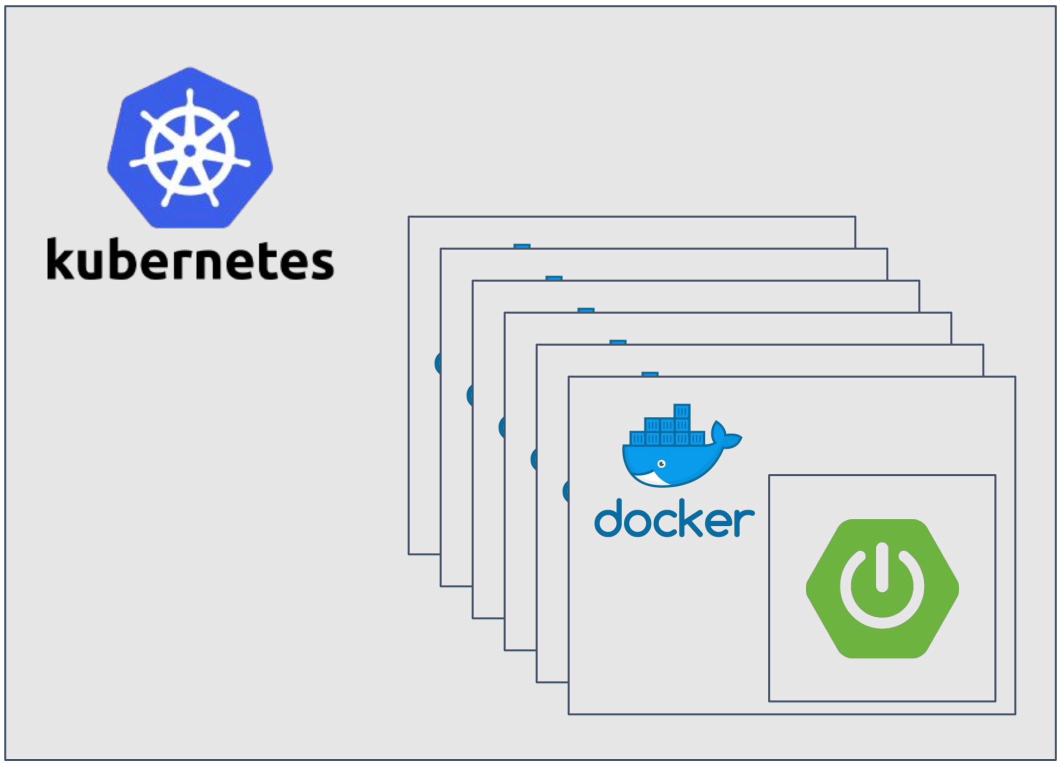

Cluster
Node
etcd
Access to machines/VMs
Access to etcd API
Access via Kubernetes API or proxy
Control-plane components
Intercept/modify/ inject control-plane traffic
Node
Kubelet
Access via Kuelet API
Pod
Container
Application
Escape container to host through vulnerability or volume mount
Intercept/modify/inject application traffic
Exploit vulnerability in application code

Operational / Development Kubernetes Security



https://kubernetes.io/docs/concepts/security/overview/#the-4c-s-of-cloud-native-security
https://learnk8s.io/production-best-practices/

Kubernetes Security



- Kubernetes Auditing
- Network Policies
- Role Based Access Control (RBAC)
- Resource Limits
- Pod Security Context
- Pod Security Policy
- Open Policy Agent

Resource Limits

```
spec:
  ...
  containers:
    resources:
      limits:
        cpu: "1"
        memory: "512Mi"
      requests:
        cpu: 500m
        memory: "256Mi"
  ...
```

https://kubernetes.io/docs/tasks/configure-pod-container/assign-cpu-resource
https://kubernetes.io/docs/tasks/configure-pod-container/assign-memory-resource

Pod/Container Security Context

```
spec:
  securityContext:
    runAsNonRoot: true
  containers:
    securityContext:
      allowPrivilegeEscalation: false
      privileged: false
      runAsNonRoot: true
      readOnlyRootFilesystem: true
      capabilities:
        drop:
          - ALL
```

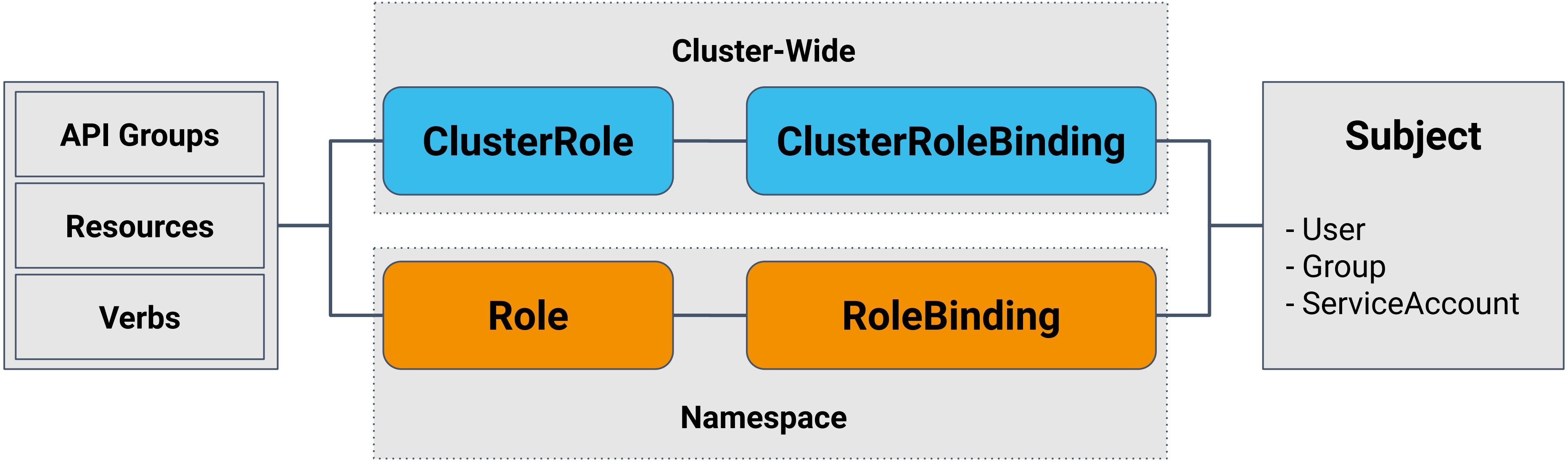
https://kubernetes.io/docs/tasks/configure-pod-container/security-context

Pod Security Policy (Still In Beta!)

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: no-root-policy
spec:
  privileged: false
  allowPrivilegeEscalation: false
  requiredDropCapabilities:
    - ALL
  runAsUser:
    rule: 'MustRunAsNonRoot'
  ...
```

https://kubernetes.io/docs/concepts/policy/pod-security-policy

Kubernetes Role Based Access Control (RBAC)



https://kubernetes.io/docs/reference/access-authn-authz/rbac/

Kubernetes Role Based Access Control (RBAC)

apiGroups	extensions, apps, policy, ...
resources	pods, deployments, configmaps, secrets, nodes, services, endpoints, podsecuritypolicies, ...
verbs	get, list, watch, create, update, patch, delete, use, ...

https://kubernetes.io/docs/reference/access-authn-authz/rbac/

Service Account

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: deploy-pod-security-policy
  namespace: default
```

https://kubernetes.io/docs/concepts/policy/pod-security-policy/#authorizing-policies

Pod Security Policy Role

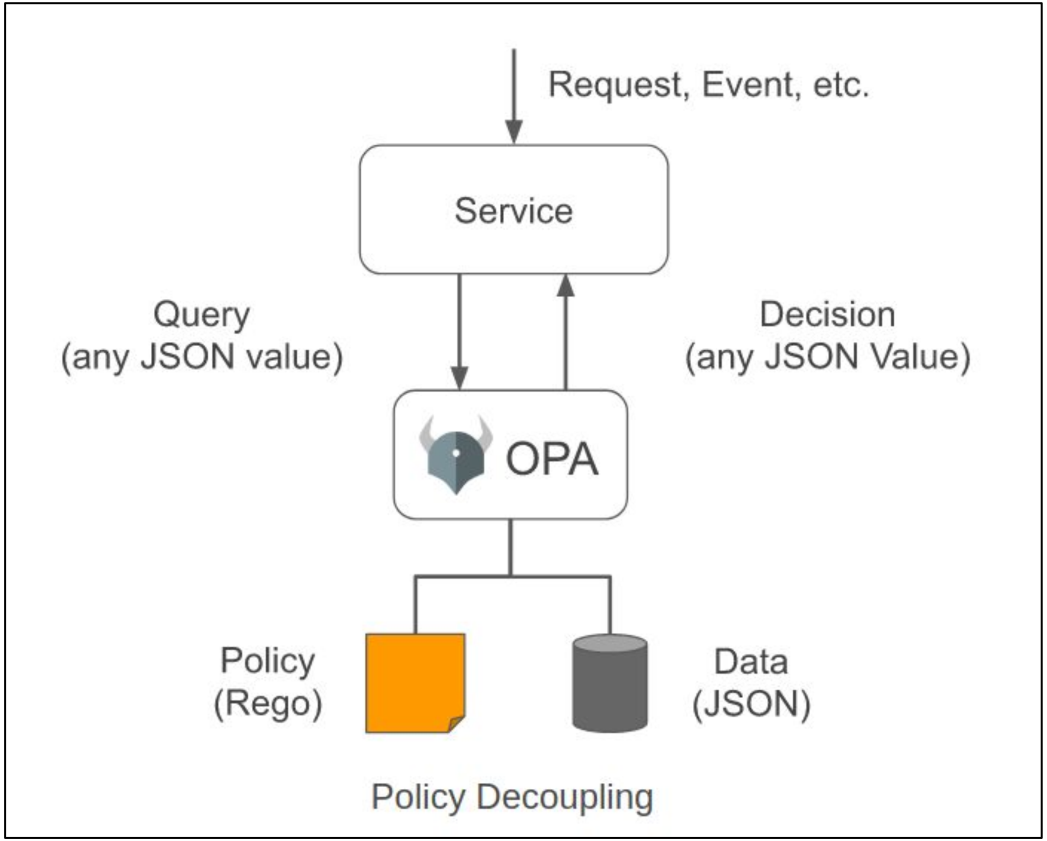
```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: no-root-policy-role
  namespace: default
rules:
  - apiGroups: ['policy']
    resources: ['podsecuritypolicies']
    verbs:     ['use']
    resourceNames:
      - no-root-policy
```

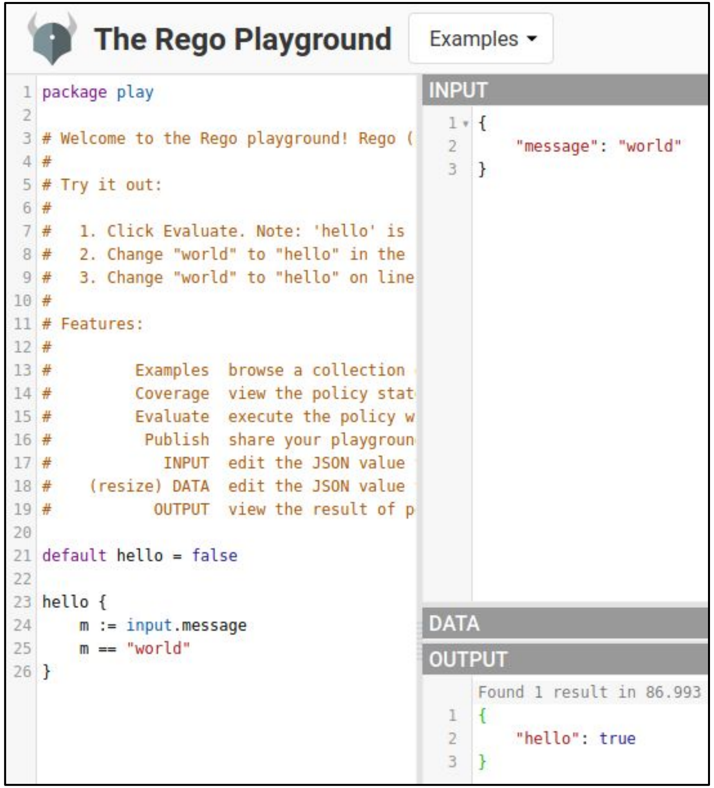
https://kubernetes.io/docs/concepts/policy/pod-security-policy/#authorizing-policies

Pod Security Policy Role Binding

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: deploy-pod-security-policy
  namespace: default
roleRef:
  kind: Role
  name: no-root-policy-role
  apiGroup: rbac.authorization.k8s.io
subjects:
  - kind: ServiceAccount
    name: deploy-pod-security-policy
    namespace: default
```

Open Policy Agent





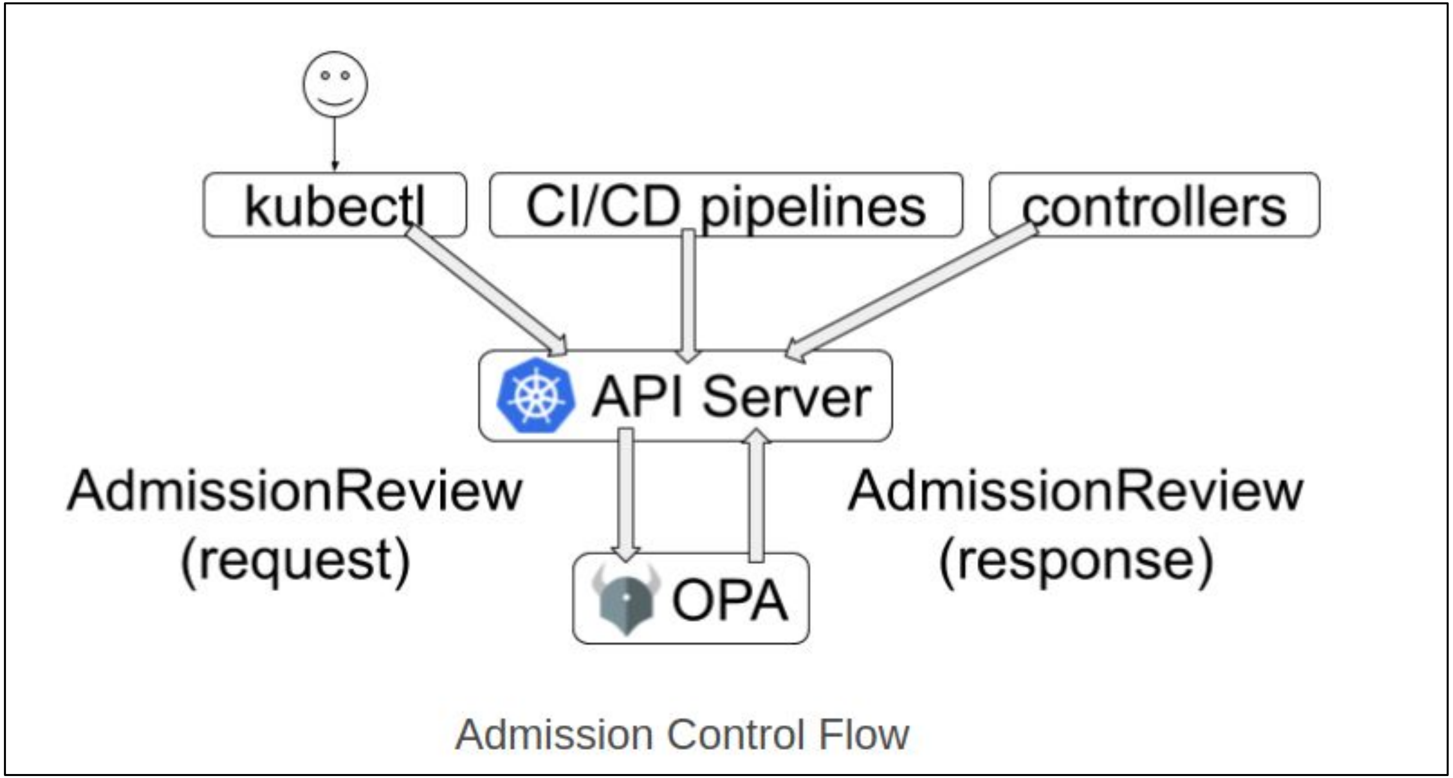
```
package play

# Welcome to the Rego playground! Rego (
#
# Try it out:
#
#   1. Click Evaluate. Note: 'hello' is
#   2. Change "world" to "hello" in the
#   3. Change "world" to "hello" on line
#
# Features:
#
#          Examples  browse a collection
#          Coverage  view the policy stat
#          Evaluate  execute the policy w
#           Publish  share your playgroun
#             INPUT  edit the JSON value
#      (resize) DATA  edit the JSON value
#            OUTPUT  view the result of p

default hello = false

hello {
    m := input.message
    m == "world"
}
```

```
{
    "message": "world"
}
```

```
Found 1 result in 86.993
{
    "hello": true
}
```

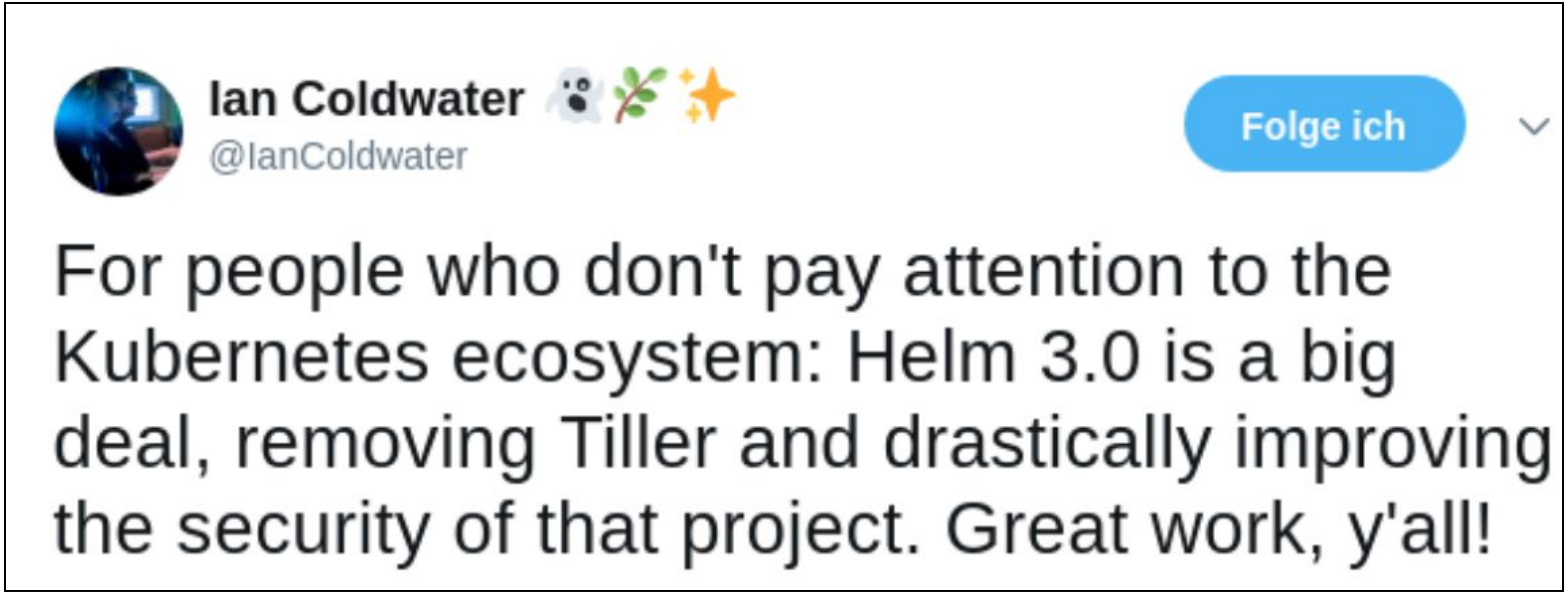
https://www.openpolicyagent.org
https://play.openpolicyagent.org

Open Policy Agent - Kubernetes Gatekeeper



https://github.com/open-policy-agent/gatekeeper

Helm 3 Is Here! 😀



Ian Coldwater 👻🌿✨
@IanColdwater

For people who don't pay attention to the Kubernetes ecosystem: Helm 3.0 is a big deal, removing Tiller and drastically improving the security of that project. Great work, y'all!

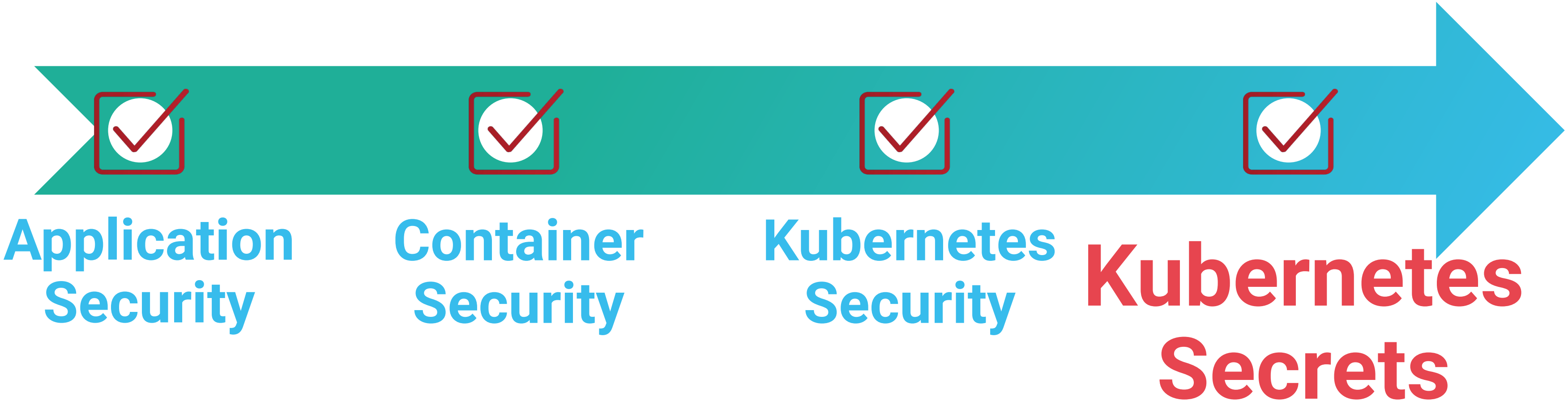
https://v3.helm.sh
https://helm.sh/docs/faq/#removal-of-tiller

Live Demo: Show me the code

Iteration 3: Kubernetes Security

https://github.com/andifalk/secure-development-on-kubernetes

The Path for Secure Development on K8s



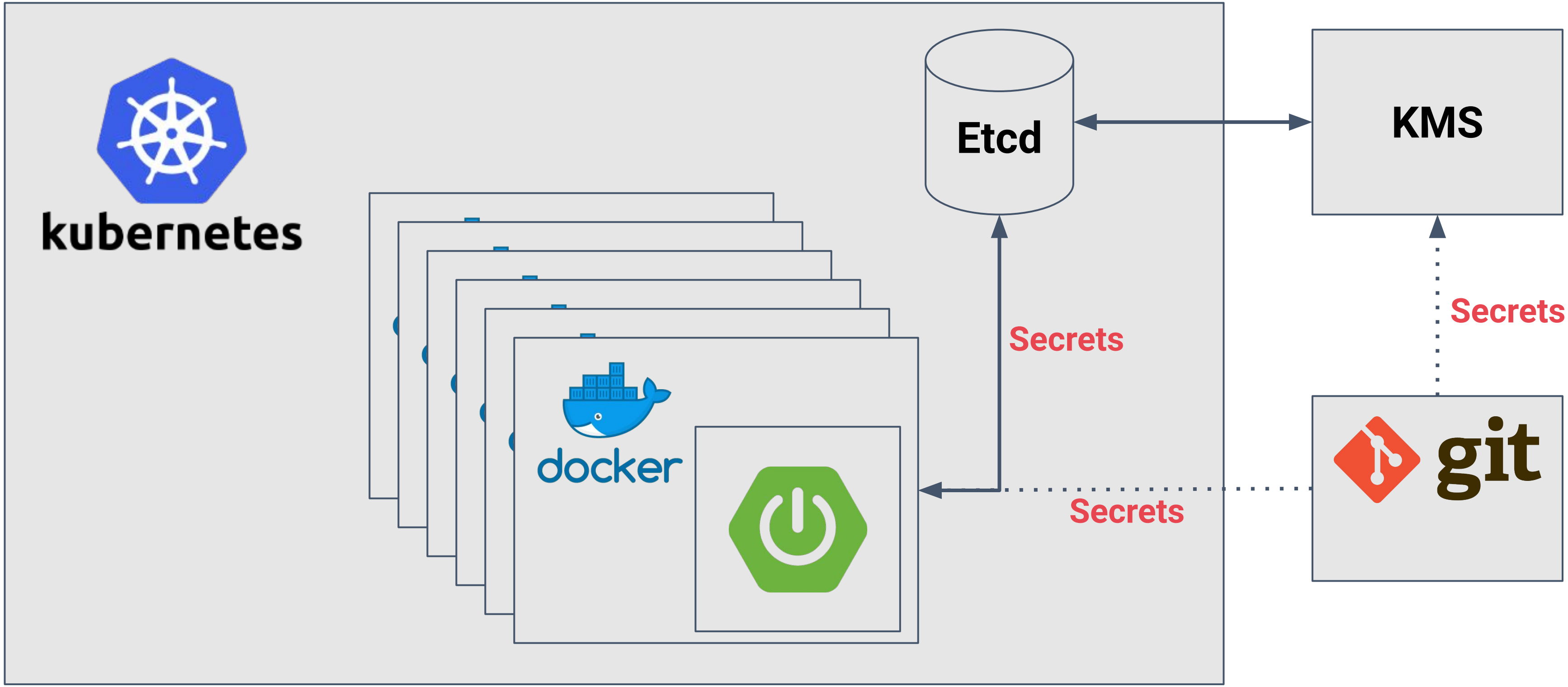
Application Security

Container Security

Kubernetes Security

Kubernetes Secrets

Kubernetes Secrets



Kubernetes Secrets

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: hello-spring-cloud-kubernetes
  namespace: default
type: Opaque
data:
  user.username: dXNlcg==
  user.password: azhzX3VzZXI=
  admin.username: YWRtaW4=
  admin.password: azhzX2FkbWlu
```

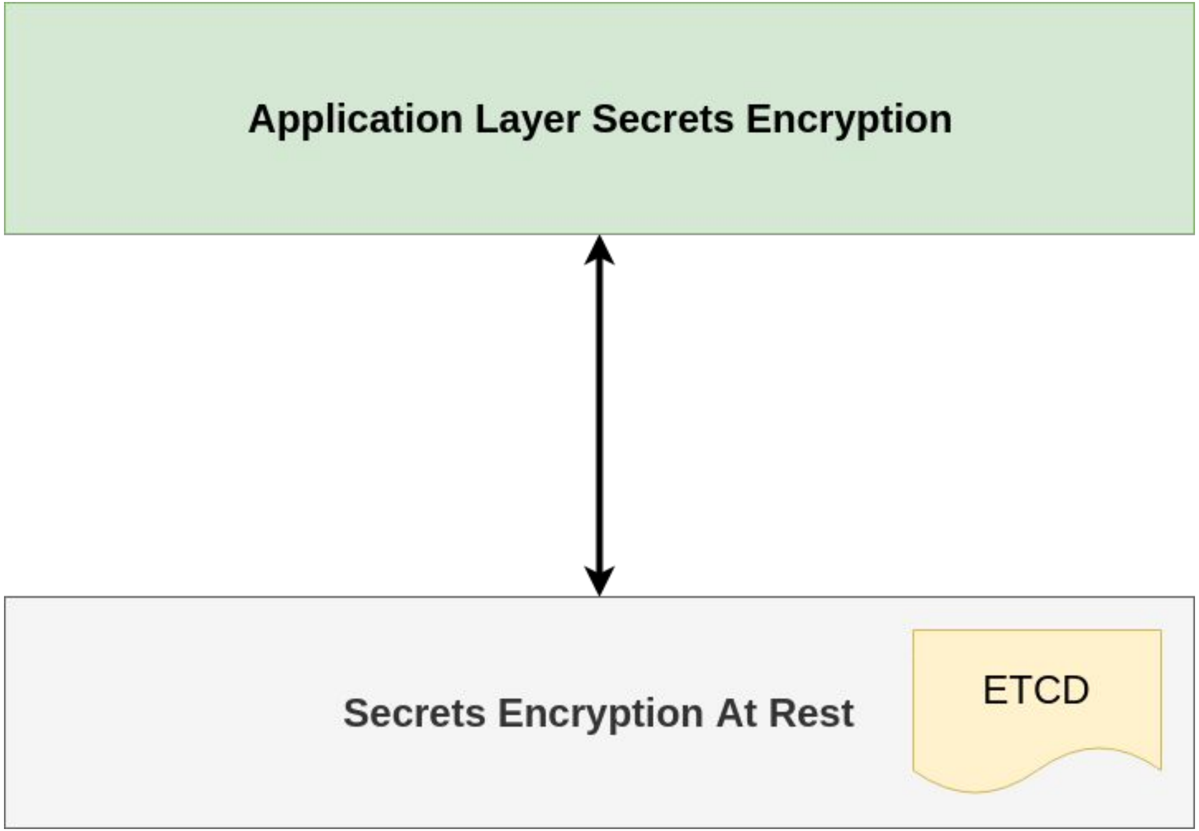
https://kubernetes.io/docs/concepts/configuration/secret

Kubernetes Secrets - Best Practices

- Encrypt Secret Data at Rest
  Only Base64 Encoded by Default!
- Applications interacting with secrets API should be limited using RBAC
- Mount secrets instead of ENV Mapping

https://kubernetes.io/docs/concepts/configuration/secret/#best-practices
https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data

Encryption Layers

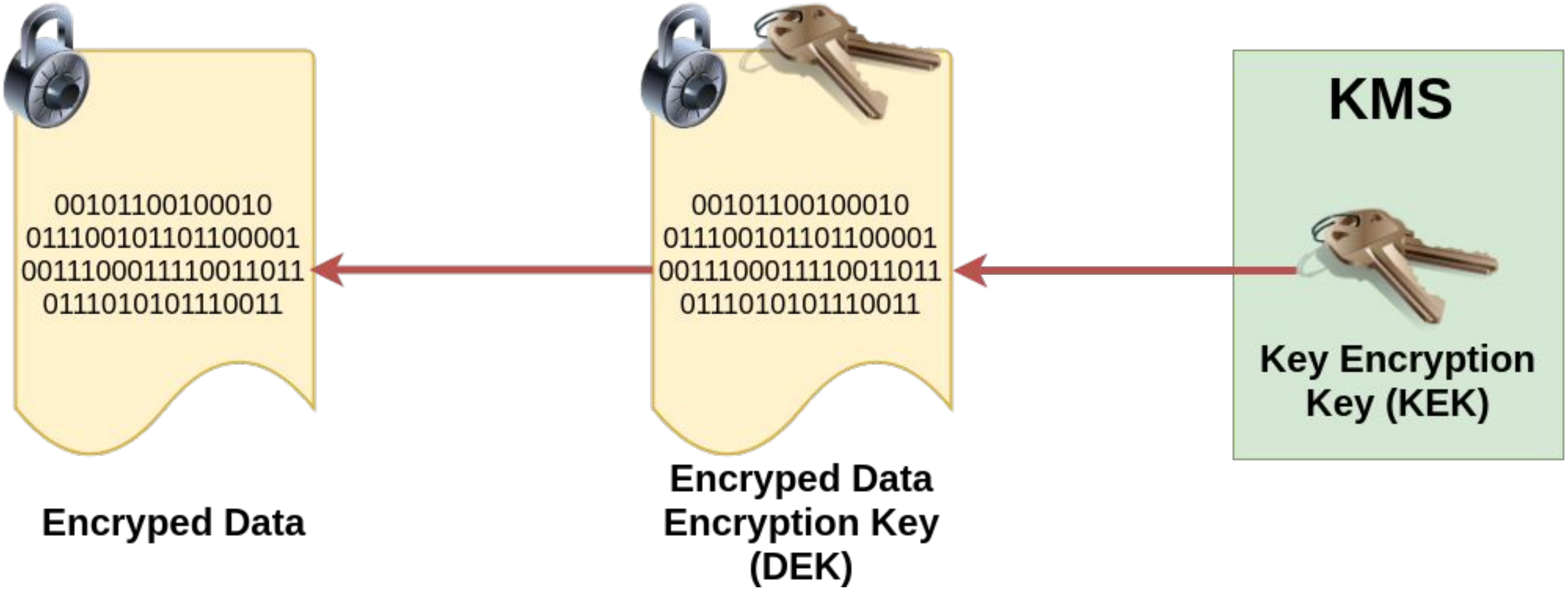


Application Layer Secrets Encryption

Secrets Encryption At Rest

ETCD

Envelope Encryption On Kubernetes



https://cloud.google.com/kms/docs/envelope-encryption
https://kubernetes.io/docs/tasks/administer-cluster/kms-provider

Key Management System (KMS) Providers

- Azure Key Vault
- Google Cloud KMS
- AWS KMS
- Hashicorp Vault
- …

https://github.com/Azure/kubernetes-kms
https://github.com/Azure/kubernetes-keyvault-flexvol
https://cloud.google.com/kms
https://aws.amazon.com/de/kms
https://learn.hashicorp.com/vault/kubernetes/external-vault

What about Secrets in git

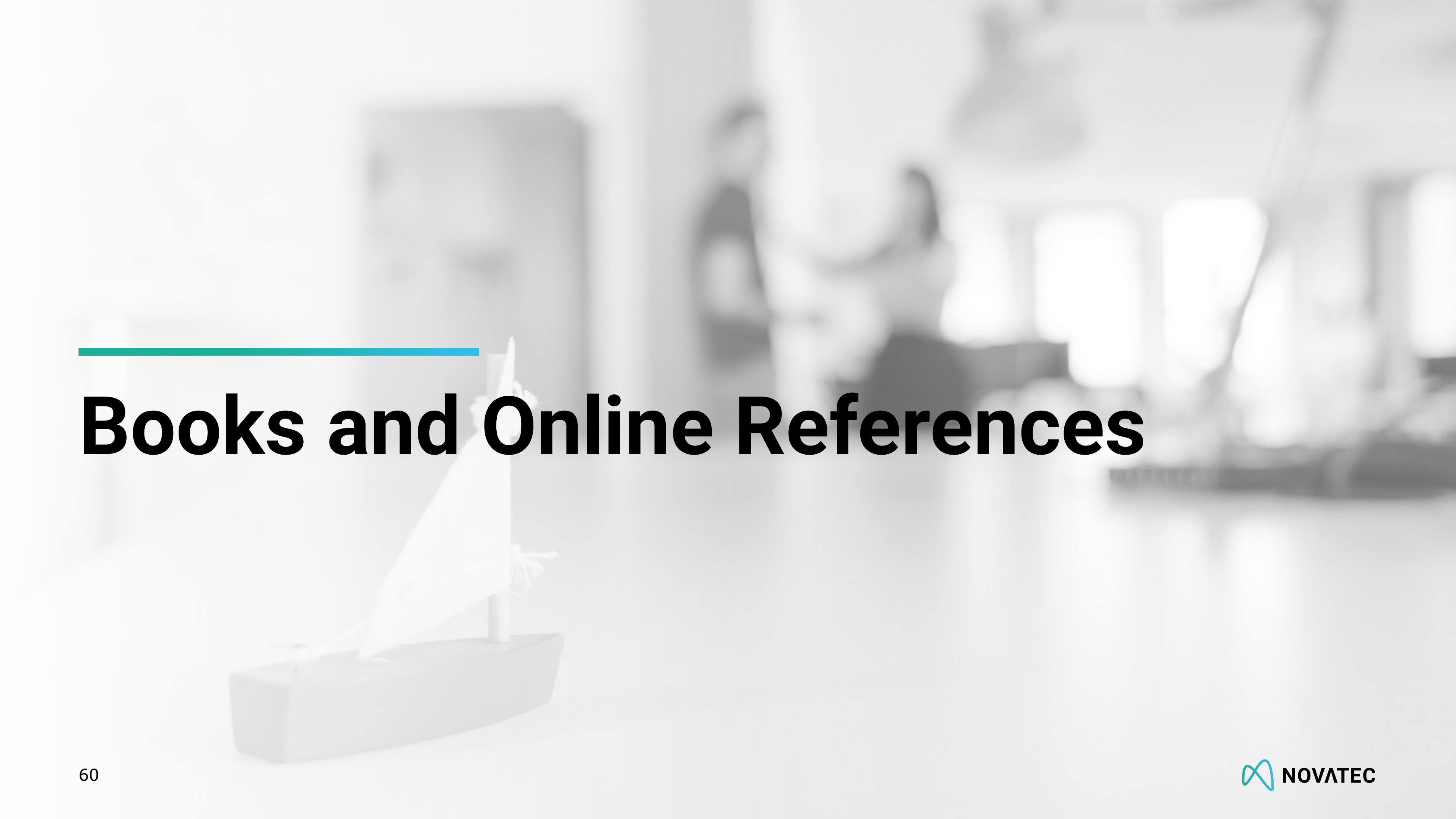
- Sealed Secrets
- Helm Secrets
- Kamus
- Sops
- Hashicorp Vault

https://learnk8s.io/kubernetes-secrets-in-git
https://github.com/bitnami-labs/sealed-secrets
https://github.com/futuresimple/helm-secrets
https://github.com/Soluto/kamus
https://github.com/mozilla/sops
https://www.vaultproject.io

Summary

Summary / Key Insights

- Containers use Linux Namespaces+Caps
- Say **NO** to root on K8s
- "**Least privilege**" for service accounts
- Keep K8s up-to-date and scan for security
- Ensure your secrets are **encrypted** in K8s
- **Scan** and keep container images **up-to-date**



Books and Online References

Books and Online References (1)

- Kubernetes Security, O'Reilly, 2018, ISBN: 978-1-492-04600-4
- Container Security, O'Reilly, 2020, ISBN: 978-1492056706
- https://github.com/andifalk/secure-development-on-kubernetes
- Crafty Requests: Deep Dive Into Kubernetes CVE-2018-1002105 - Ian Coldwater (Video)
- Ship of Fools: Shoring Up Kubernetes Security - Ian Coldwater (Video)
- https://kubernetes.io/docs/concepts/security/overview/#the-4c-s-of-cloud-native-security
- https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster
- https://opensource.com/article/18/3/just-say-no-root-containers
- https://github.com/GoogleContainerTools/jib
- https://anchore.com/opensource/
- https://github.com/coreos/clair
- https://github.com/aquasecurity/trivy
- https://www.owasp.org/index.php/OWASP_Docker_Top_10

Books and Online References (2)

- https://kubernetes.io/docs/tasks/configure-pod-container/assign-cpu-resource
- https://kubernetes.io/docs/tasks/configure-pod-container/assign-memory-resource
- https://kubernetes.io/docs/tasks/configure-pod-container/security-context
- https://kubernetes.io/docs/concepts/policy/pod-security-policy
- https://kubernetes.io/docs/reference/access-authn-authz/rbac/
- https://kubernetes.io/docs/concepts/configuration/secret
- https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data
- https://cloud.google.com/kms/docs/envelope-encryption
- https://kubernetes.io/docs/tasks/administer-cluster/kms-provider
- https://github.com/Azure/kubernetes-kms
- https://cloud.google.com/kms
- https://aws.amazon.com/de/kms

NOVATEC

Andreas Falk
Managing Consultant

Mobil: +49 151 46146778
E-Mail: andreas.falk@novatec-gmbh.de

Novatec Consulting GmbH

Dieselstraße 18/1
D-70771 Leinfelden-Echterdingen

T. +49 711 22040-700
info@novatec-gmbh.de
www.novatec-gmbh.de