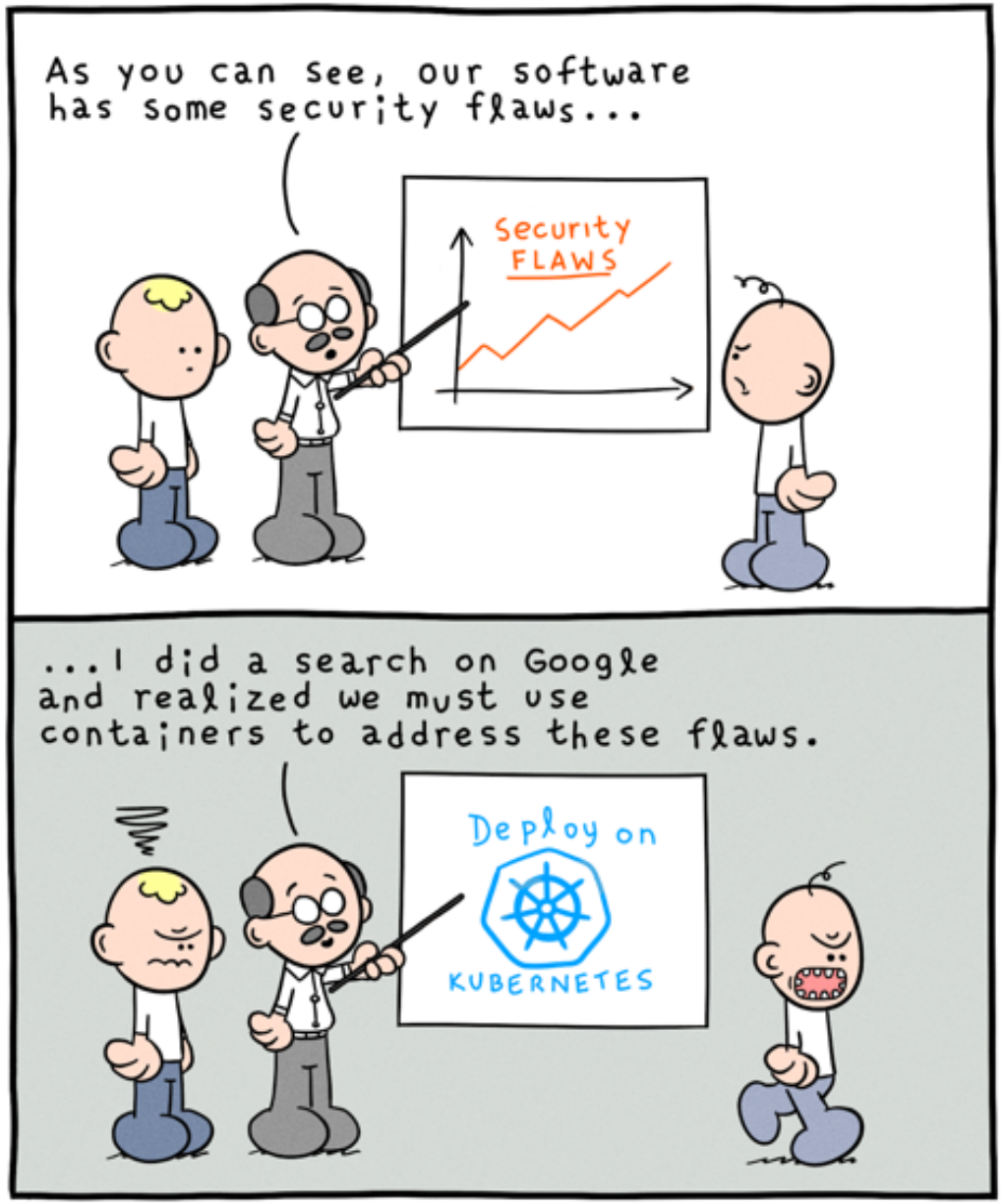
Secure your Kubernetes Containers

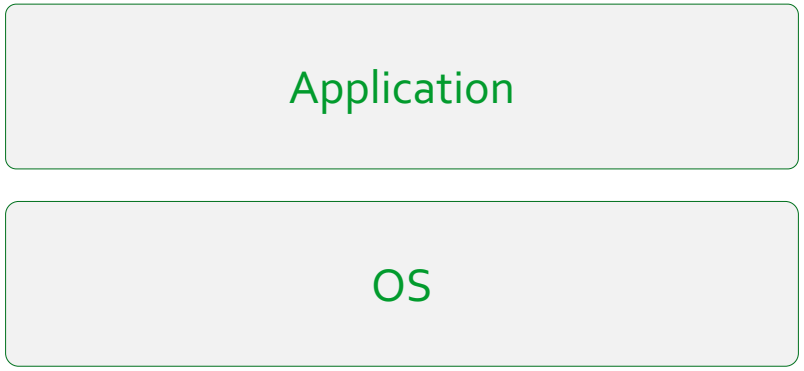
Hossam Barakat

Lead Consultant at Telstra Purple

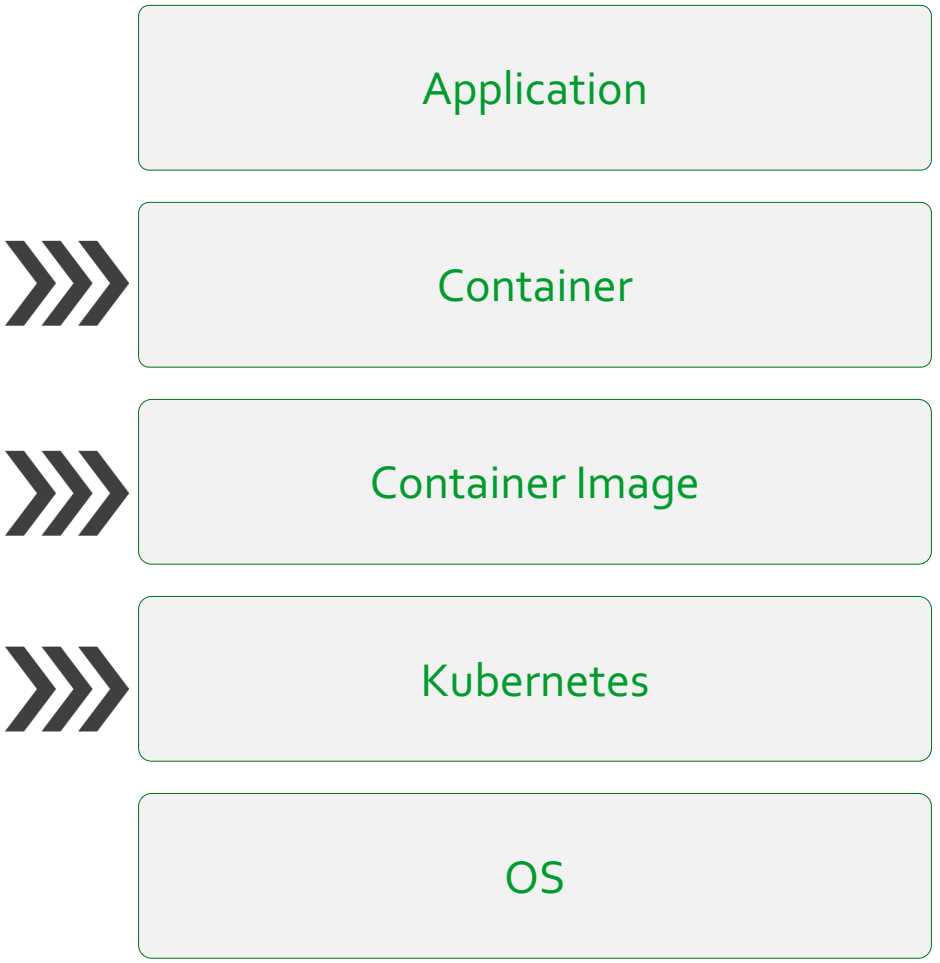
@hossambarakat_


As you can see, our software has some security flaws...
Security FLAWS
...I did a search on Google and realized we must use containers to address these flaws.
Deploy on
KUBERNETES
Daniel Stori {turnoff.us}

Attack Vectors

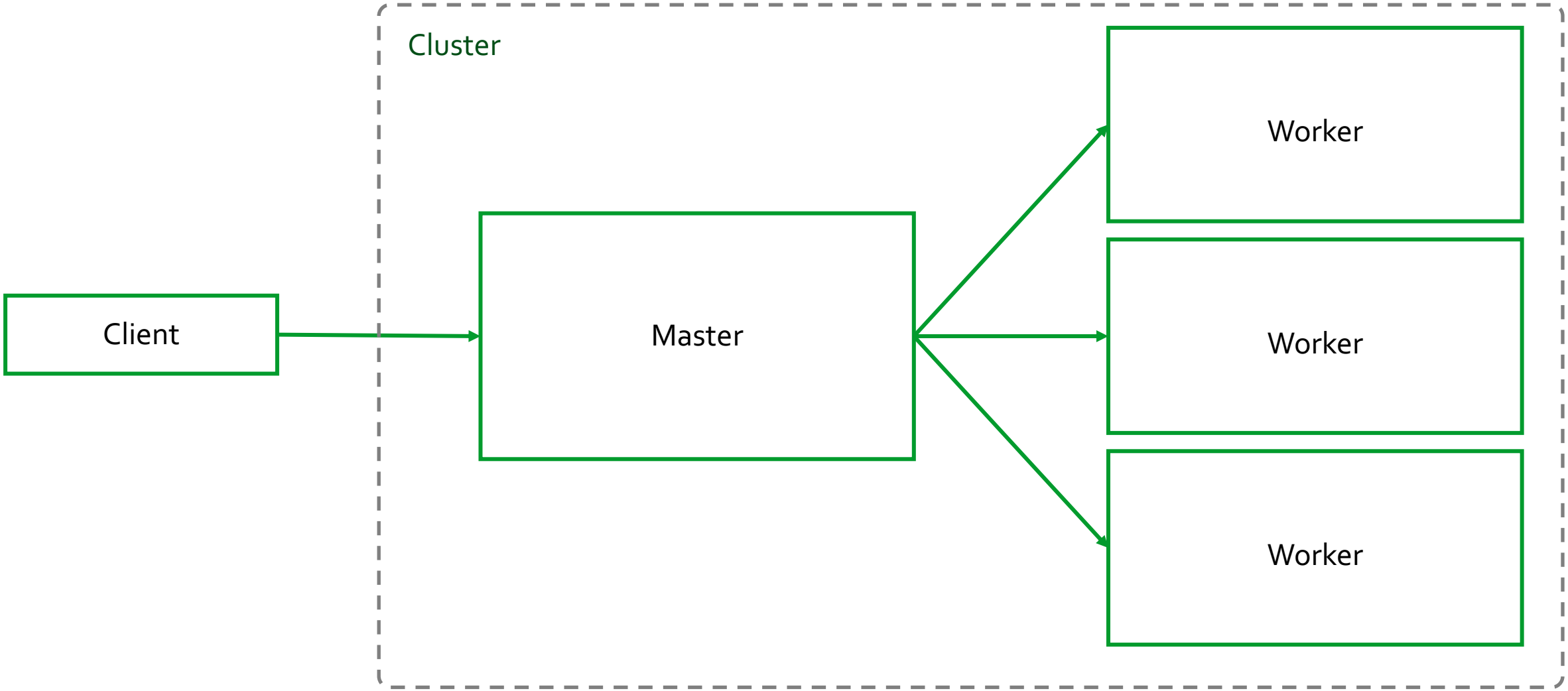


Attack Vectors

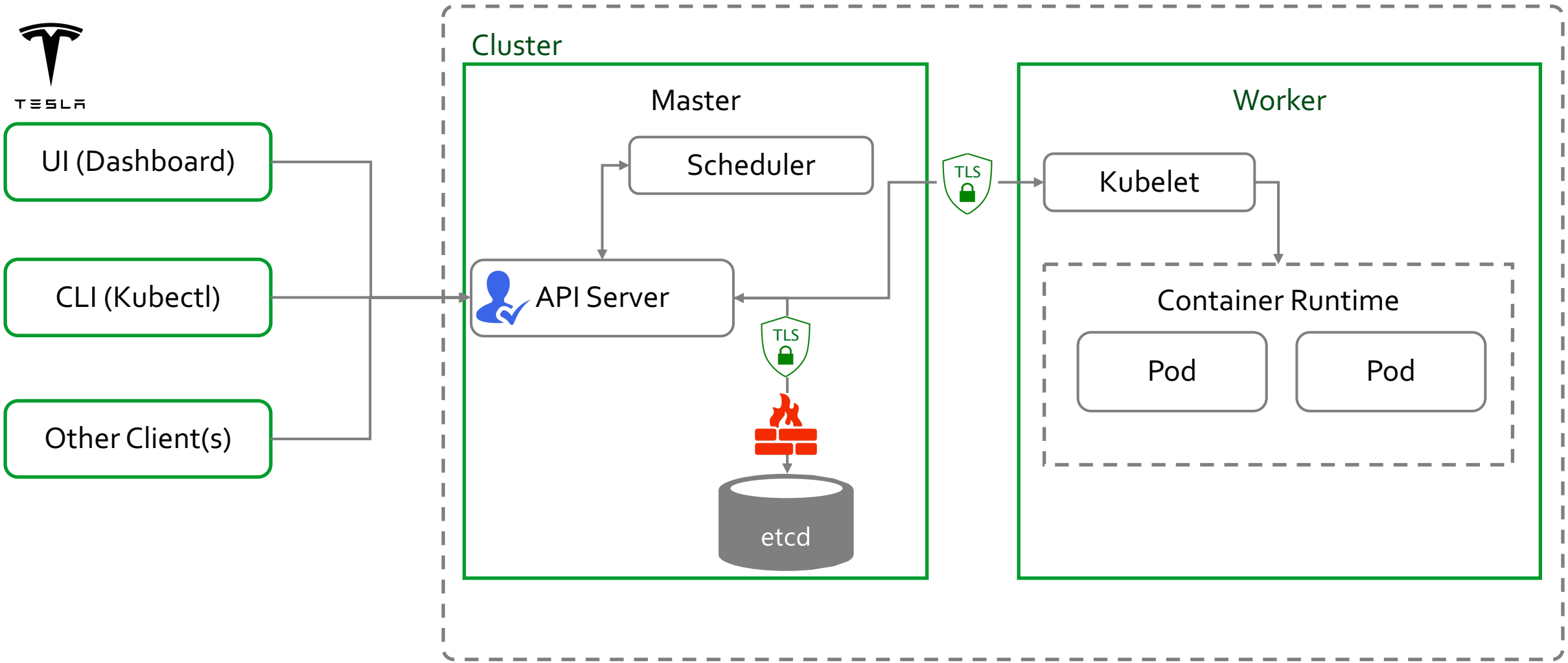


Kubernetes Cluster

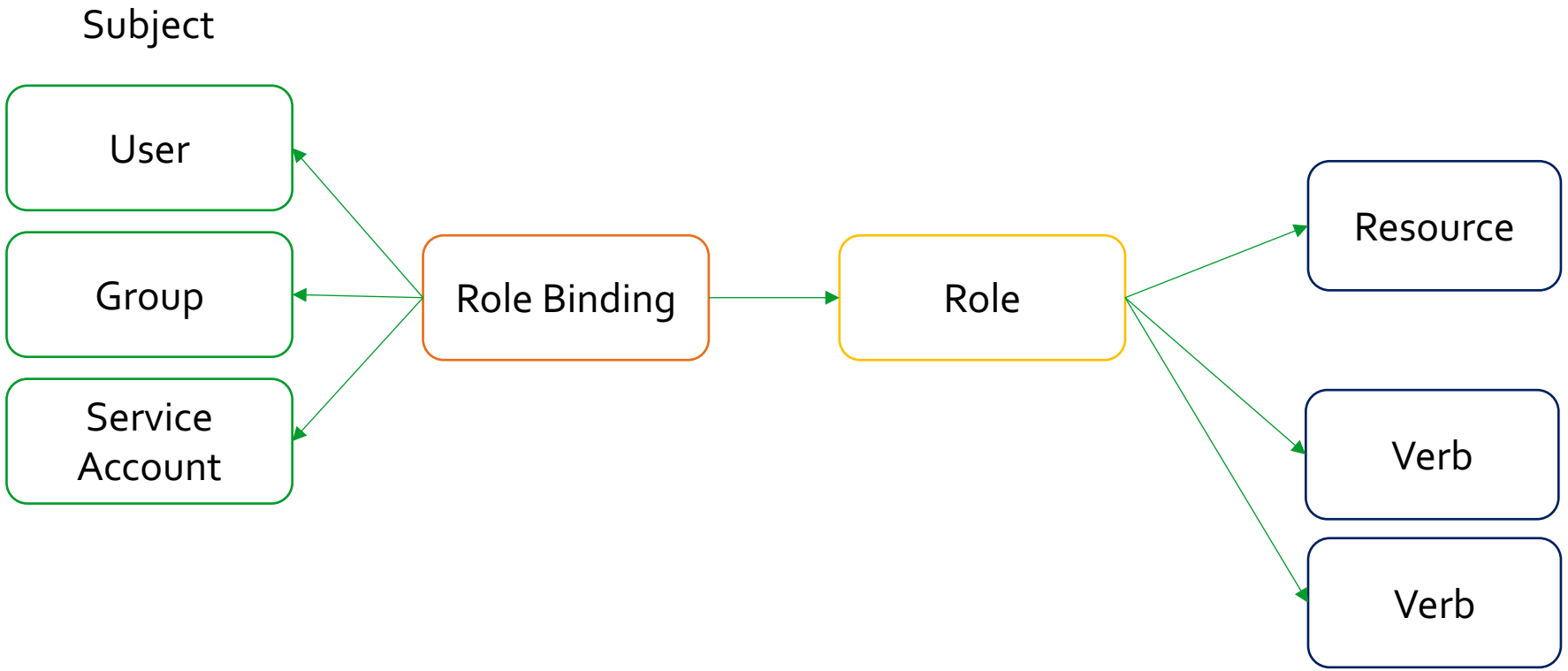
Kubernetes Architecture



Kubernetes Architecture



Role Based Access Control (RBAC)



Service Account

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: webapp-service-account
  namespace: default
```

Role Based Access Control (RBAC)

Role

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: my-role
  namespace: default
rules:
  - apiGroups: [""]
    resources: ["pods"]
    verbs: ["get", "list"]
```

Role Binding

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: my-role-binding
  namespace: default
subjects:
  - kind: ServiceAccount
    name: webapp-service-account
    namespace: default
roleRef:
  kind: Role
  name: my-role
  apiGroup: rbac.authorization.k8s.io
```

Role Based Access Control (RBAC)

Pod

```
kind: Pod
apiVersion: v1
metadata:
  name: webapp
spec:
  serviceAccountName: webapp-service-account
  containers:
  - name: webapp
    image: hossambarakat/k8s-security-webapp
    ports:
        - containerPort: 3000
```

CIS Kubernetes Benchmark

- Document that provide guidance for establishing a secure configuration posture for Kubernetes
- Specific recommendations with a description, rationale, method of audit and remediation
- Can be automated with kube-bench

Container Images

Images Security

- Never run as root
  - Set USER in Dockerfile
- Minimal base image
  - Alpine 2 MB
  - Ubuntu 60 MB
- Trusted base image
- Private image registry
- Do **NOT** use latest tag
- Vulnerability scans

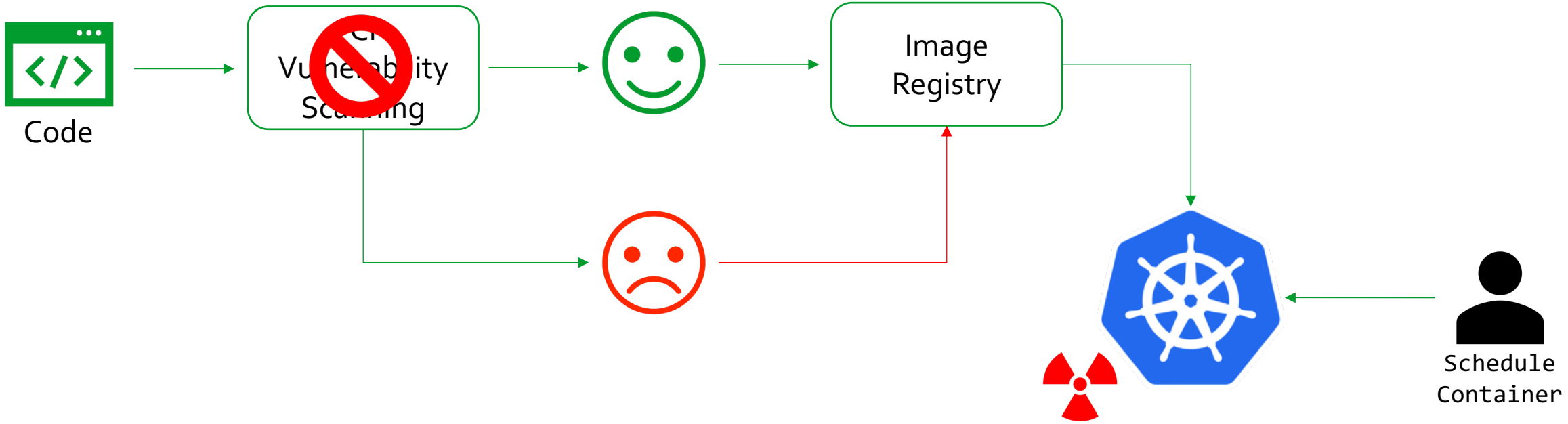
Image Scanning Tools

- aquasecurity/trivy
- coreos/clair
- optiopay/klar
- aquasecurity/microscanner
- Aqua Security
- Twistlock

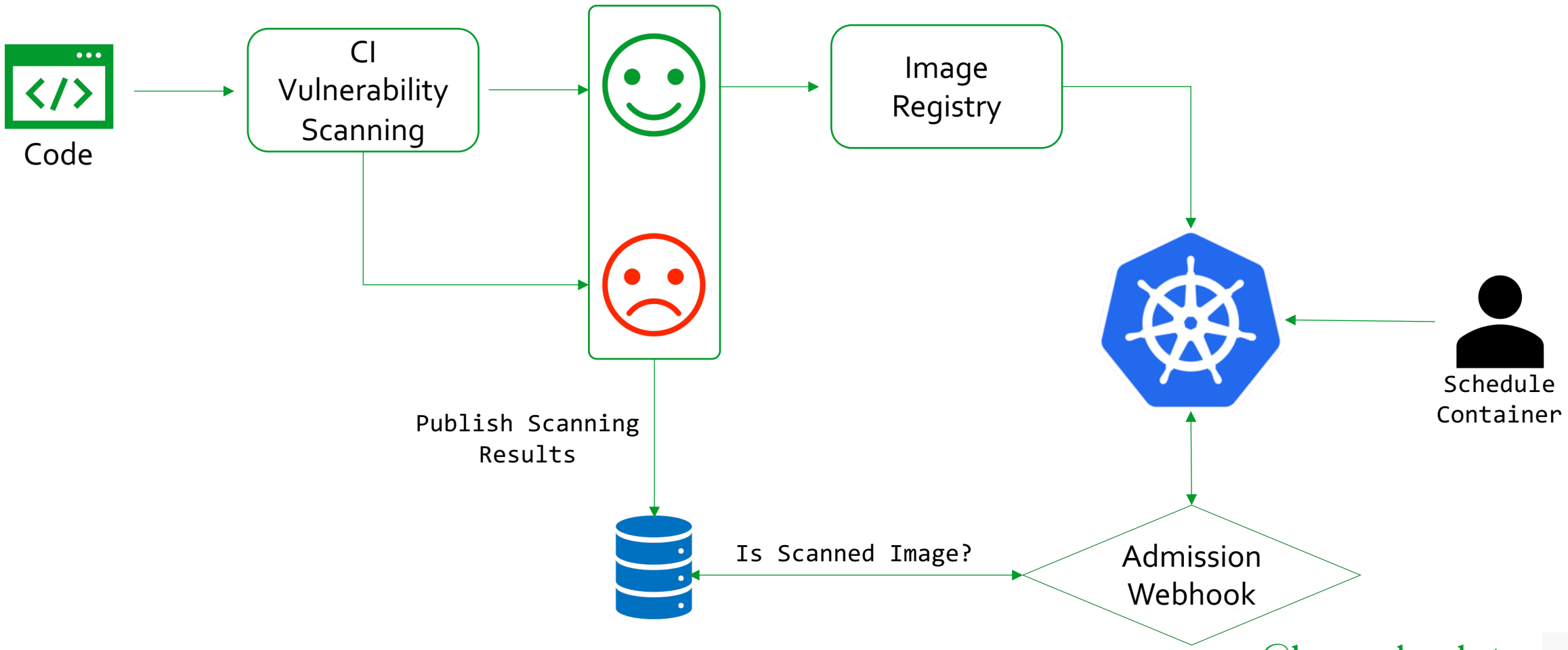
Trivy

```
➜  ~ trivy hossambarakat/k8s-security-webapp
2019-09-09T09:20:34.097+1000    INFO    Updating vulnerability database...
2019-09-09T09:20:35.024+1000    WARN    You should avoid using the :latest tag as it is cached. You need to specify '--clear-cache' option when :latest image is chan
2019-09-09T09:20:36.060+1000    INFO    Detecting Alpine vulnerabilities...

hossambarakat/k8s-security-webapp (alpine 3.9.4)
================================================
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

+---------+------------------+----------+-------------------+---------------+--------------------------------+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |             TITLE              |
+---------+------------------+----------+-------------------+---------------+--------------------------------+
| musl    | CVE-2019-14697   | HIGH     | 1.1.20-r4         | 1.1.20-r5     | musl libc through 1.1.23       |
|         |                  |          |                   |               | has an x87 floating-point      |
|         |                  |          |                   |               | stack adjustment imbalance,    |
|         |                  |          |                   |               | related...                     |
+---------+------------------+----------+-------------------+---------------+--------------------------------+
➜  ~
```

Vulnerability Scanning CI Pipeline Integration

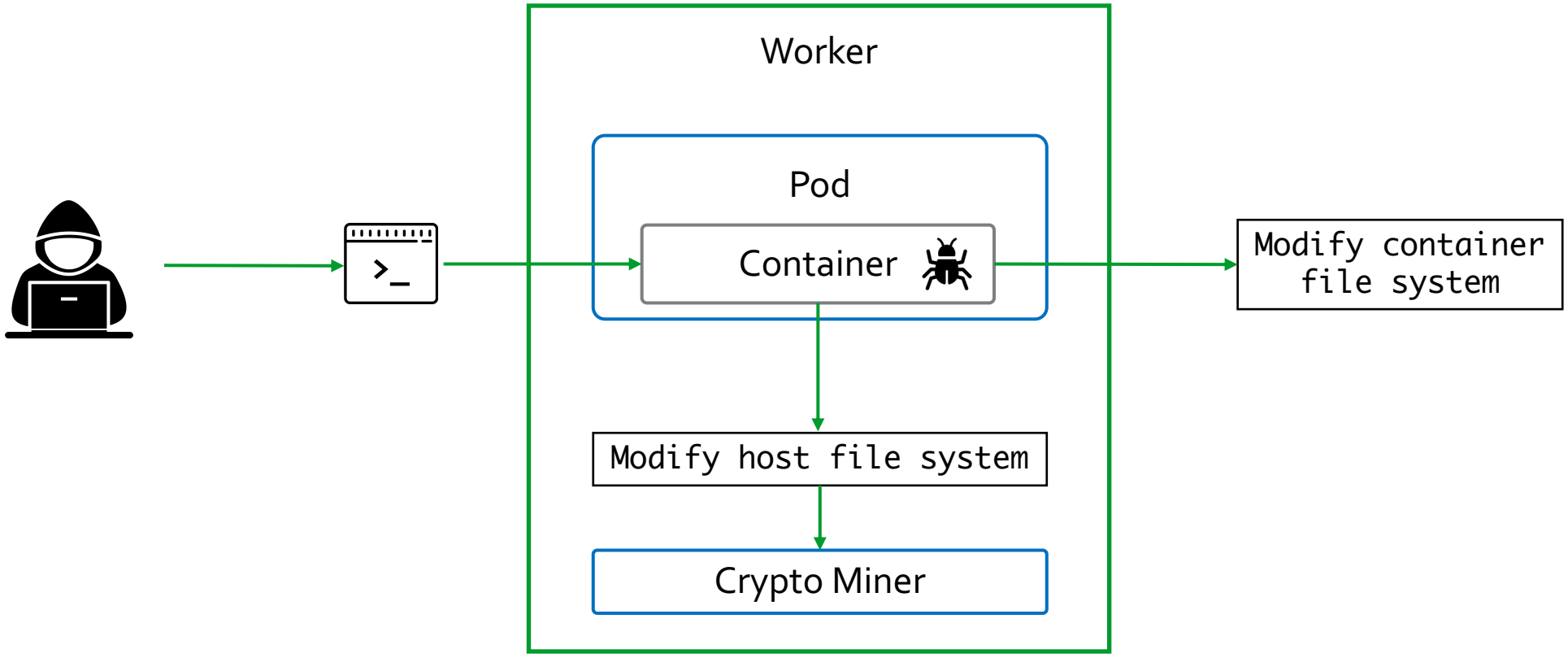


Vulnerability Scanning CI Pipeline Integration



Containers

Privilege Escalation



Hacker icon by karina from the Noun Project

Demo

Privilege Escalation

Security Context

- **RunAsUser**
- **RunAsGroup**

```
securityContext:
    runAsUser: 1000
    runAsGroup: 3000
```

Security Context

- **AllowPrivilegdeEscalation**

```
securityContext:
  allowPrivilegeEscalation: false
```

Security Context

- **ReadOnlyRootFilesystem**

```
securityContext:
  readOnlyRootFilesystem: true
```

Security Context

- RunAsUser
- RunAsGroup
- AllowPrivilegdeEscalation
- ReadOnlyRootFilesystem

```
apiVersion: v1
kind: Pod
metadata:
  name: my-app
spec:
  securityContext:
    runAsUser: 1000
    RunAsGroup: 2000
  containers:
  - name: my-app
    image: my-app
    securityContext:
      allowPrivilegeEscalation: false
      readOnlyRootFilesystem: true
```

Enter *Pod Security Policy*

Pod Security Policy

- A Pod Security Policy is a cluster-level resource that controls the actions that a pod can perform and what it has the ability to access.
- The **PodSecurityPolicy** objects define a set of conditions that a pod must run with in order to be accepted into the system.

Pod Security Policy

- privileged
- volumes
- fsGroup
- runAsUser, runAsGroup
- readOnlyRootFilesystem
- allowedHostPaths
- hostNetwork
- Linux capabilities

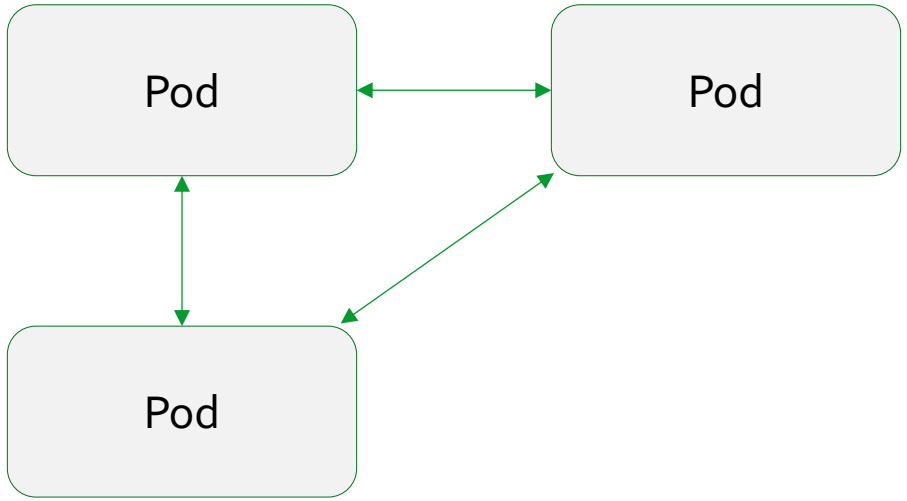
kube-psp-advisor

Command: `./kube-psp-advisor --namespace=psp-test`

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  creationTimestamp: null
  name: pod-security-policy-20181130114734
spec:
  allowedCapabilities:
  - SYS_ADMIN
  - NET_ADMIN
  allowedHostPaths:
  - pathPrefix: /bin
  - pathPrefix: /tmp
  - pathPrefix: /usr/sbin
  - pathPrefix: /usr/bin
  fsGroup:
    rule: RunAsAny
  hostIPC: false
  hostNetwork: false
  hostPID: false
  privileged: true
  runAsUser:
    rule: RunAsAny
  seLinux:
    rule: RunAsAny
  supplementalGroups:
    rule: RunAsAny
  volumes:
  - hostPath
  - configMap
  - secret
```

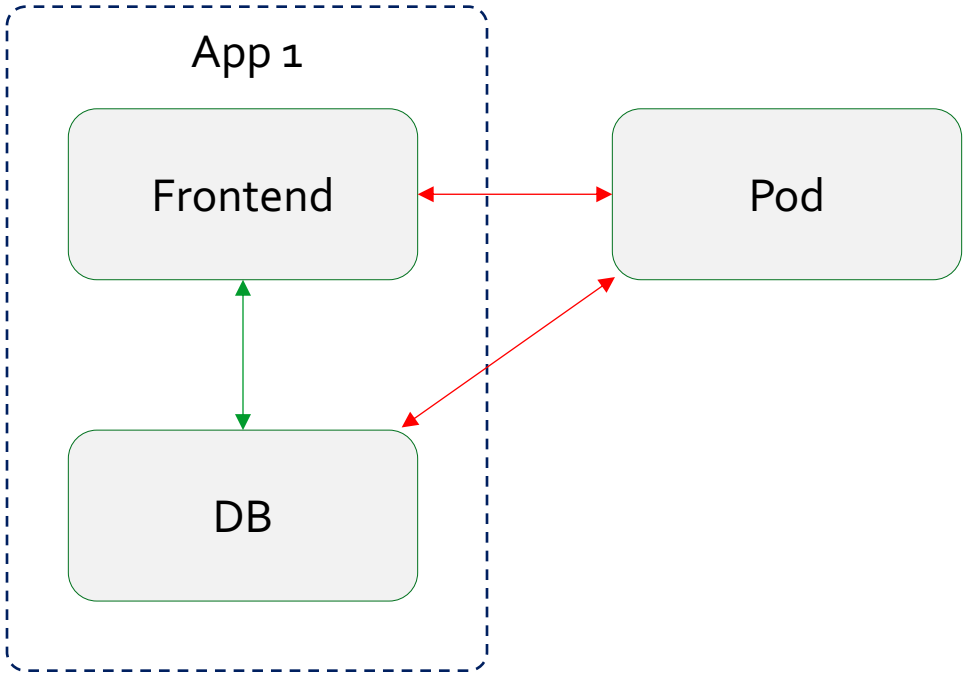
Network Communication

» All pods can communicate with each other



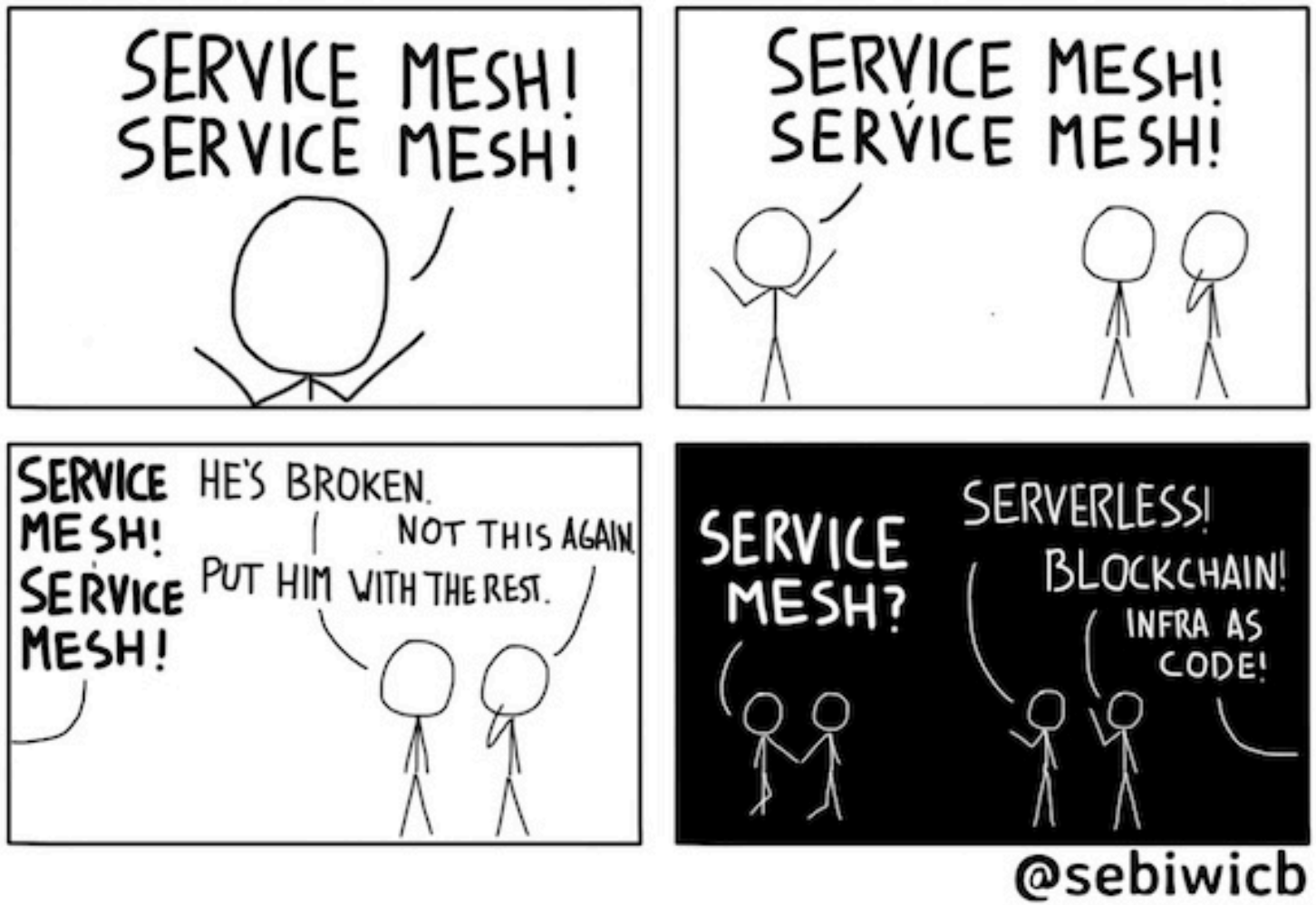
Network Communication

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: my-frontend-policy
spec:
  podSelector:
    matchLabels:
      app: db
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: frontend
```



Network Plugin

- Calico
- Cilium
- Kube-Router
- Weave Net
- ...


SERVICE MESH!
SERVICE MESH!
SERVICE MESH!
SERVICE MESH!
SERVICE MESH!
SERVICE MESH!
HE'S BROKEN.
NOT THIS AGAIN.
PUT HIM WITH THE REST.
SERVICE MESH?
SERVERLESS!
BLOCKCHAIN!
INFRA AS CODE!
@sebiwicb

Service Mesh

- Security specific policy enforcement
- End-to-end encryption
- Rolling certificates

Summary

Kubernetes Cluster

- Bootstrap TLS
- Authentication
- Enable RBAC
- CIS Benchmark

Container Images

- No root user
- Small images
- Do NOT use latest
- Private Image Registry
- Vulnerability Scans

Containers

- Pod Security Context
- Pod Security Policy
- Network Policy
- Service Mesh

Resources

- https://kubernetes-security.info
- Demos: http://github.com/hossambarakat/secure-k8s-containers

Questions?

#2019addo-devsecops

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire

Thank You

Hossam Barakat

@hossambarakat_