goto;

GOTO
Copenhagen 2021

#GOTOcph

Securing Danish Healthcare using Cloud Native

Frederik Mogensen
Infrastructure Engineer

Cloud Native

*“Cloud native computing is an approach in software development that utilizes cloud computing to "**build and run scalable applications** in modern, **dynamic environments** such as **public, private, and hybrid clouds"**.*

*Technologies such as **containers, microservices, serverless functions and immutable infrastructure**, deployed via **declarative code** are common elements of this architectural style”*

https://en.wikipedia.org/wiki/Cloud_native_computing

Common Danish Telemedicine Platform

Telemedicine Platform

- Covering all of Denmark
  - 5 regions + 98 municipalities
- Helping chronically ill patients to live at home
- Defining different questionnaires for each illness
- Patients measuring and responding to questionnaires daily

Photo by Jair Lázaro on Unsplash

Photo by Philipp Katzenberger on Unsplash

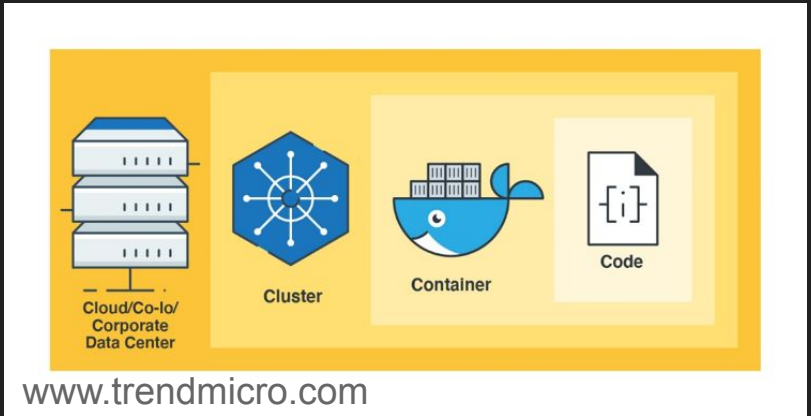
Platform Focus

Handling healthcare data demands a high focus on

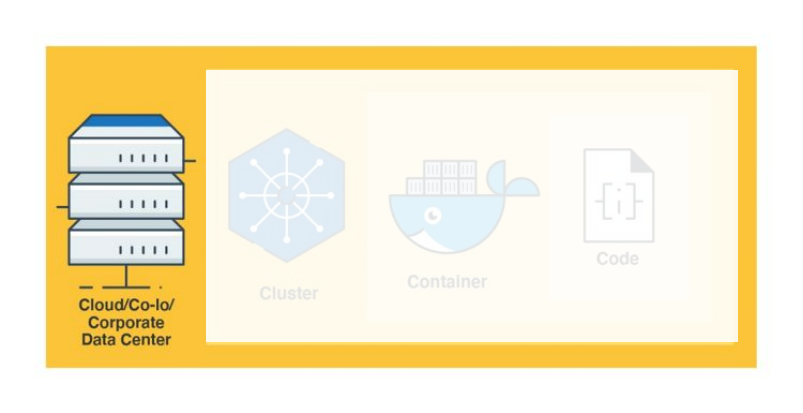
- Stability
- Observability
- Security

Defense-in-depth using

The 4C's of Cloud Native security



Cloud / Co-lo / Corporate Data Center



Cloud provider security

Area of Concern

- Network access
- Access to Cloud Provider API
- Disk Encryption
- Database access
- Internet access
- Misconfiguration / drifting configuration

Photo by Mauro Sbicego on Unsplash

Cloud provider security

- Infrastructure as code ensures systems consistent
- IaC allows for security scanning of code

Short demo

```
$ tfscan
```

Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Kubernetes Infrastructure

Area of Concern

- Network access to API Server
- Network access to Nodes
- Kubernetes access to Cloud Provider API
- Access to etcd
- etcd Encryption

Kubernetes Infrastructure

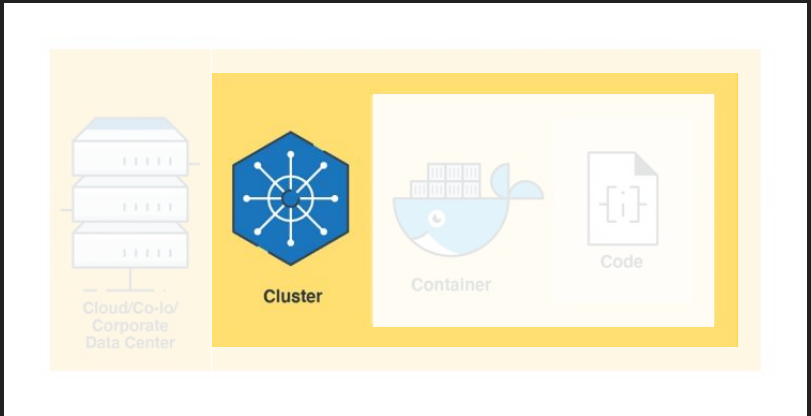
Short demo

```
$ docker run -it --rm --network host \
      aquasec/kube-hunter --interface

$ curl -k https://172.18.0.2:6443/version
```

Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Cluster



Static Cluster Security

Area of Concern

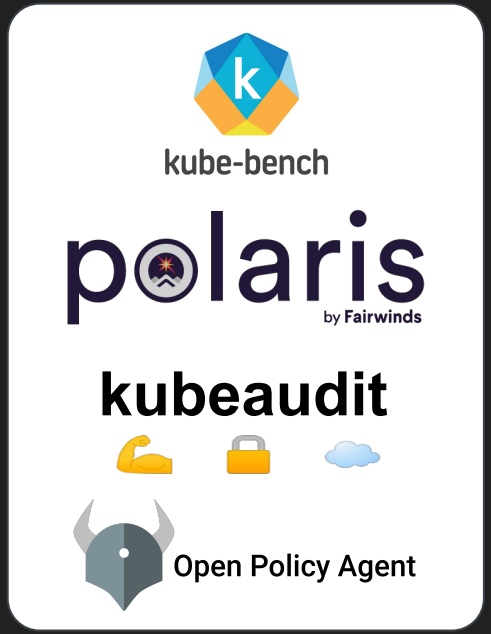
- RBAC Authorization (Access to the Kubernetes API)
- Pod Security Policies (Deprecated)
  - Run as Root?
  - Allow host paths?
  - Allow privileged?
- Quality of Service (and Cluster resource management)
- Network Policies
- TLS For Kubernetes Ingress

Static Cluster Security

Short demo

```
$ polaris dashboard
```

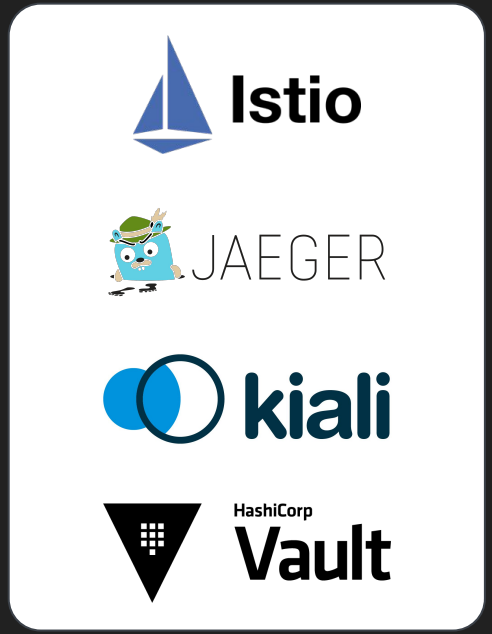
```
$ kubeaudit all -f demo.yaml
```



Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Runtime Cluster Security

- Pod Communication
  - JWT validation
  - mTLS Data Layer encryption
  - Network policies
- Monitoring Traffic
  - Tracing specific calls
  - Graphing all traffic between services
- Secrets & Certificates
  - Service Accounts



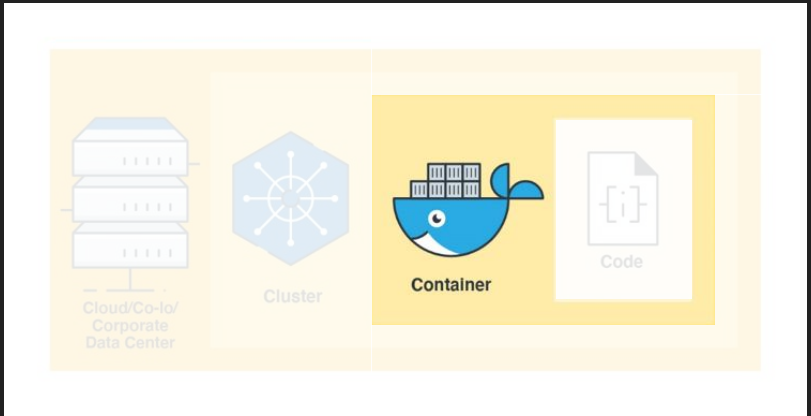
Intruder Detection / Intruder Prevention

Short demo

```
$ docker-compose up
```

Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Container



Container Security

Area of Concern

- Container Vulnerability Scanning
- OS Dependency Security
- Image Signing and Enforcement
- Disallow privileged users
- Use container runtime with stronger isolation

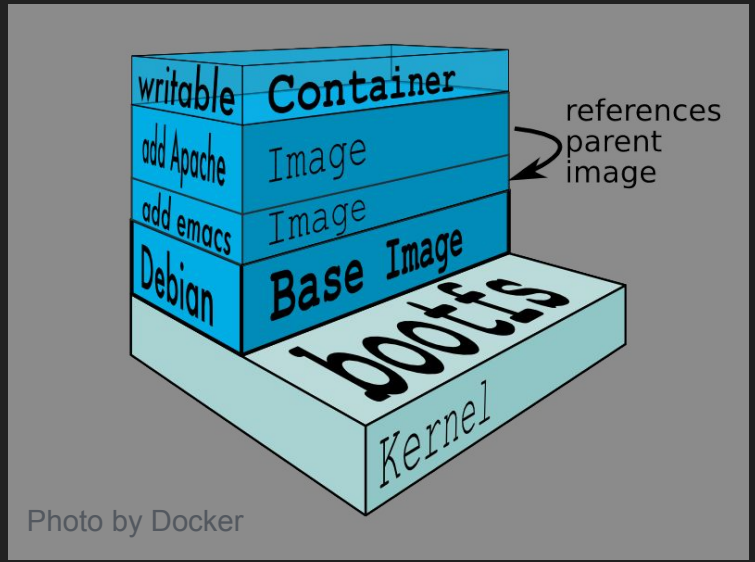


Image Scanning and Security

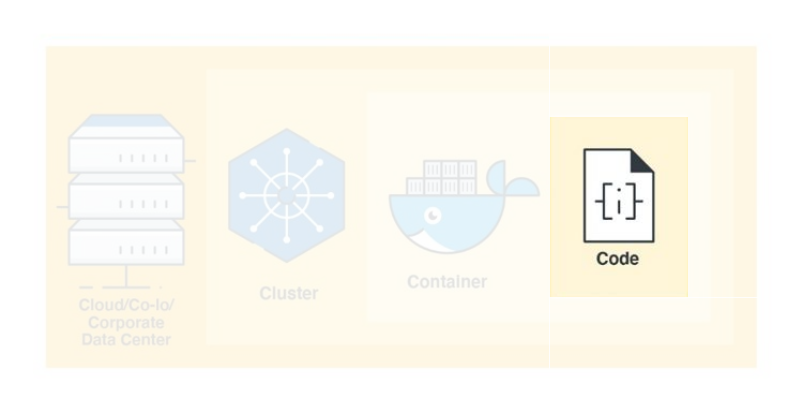
Short demo

```
$ trivy nginx:latest
$ trivy nginx:alpine
```


```
$ docker run -it --rm nginx:latest whoami
$ docker run -it --rm \
    nginxinc/nginx-unprivileged:stable-alpine whoami
```

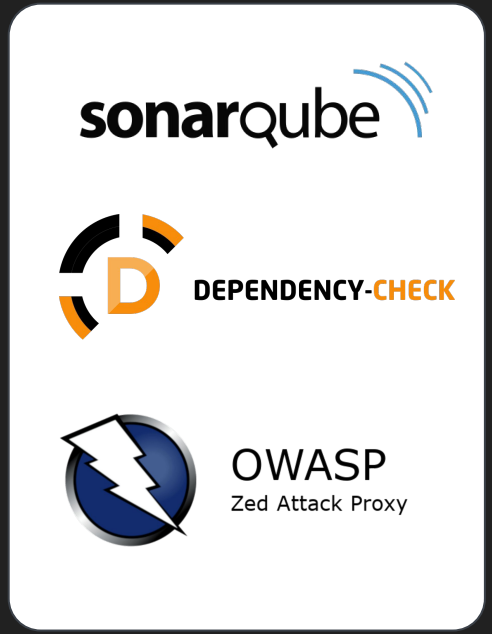
Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Code



Code Scanning

- Access over TLS only
- Limiting port ranges of communication
- 3rd Party Dependency Security
- Static Code Analysis
- Dynamic probing attacks



Examples are available at: https://github.com/mogensen/cloud-security-presentation/

Summary or Attack demo?

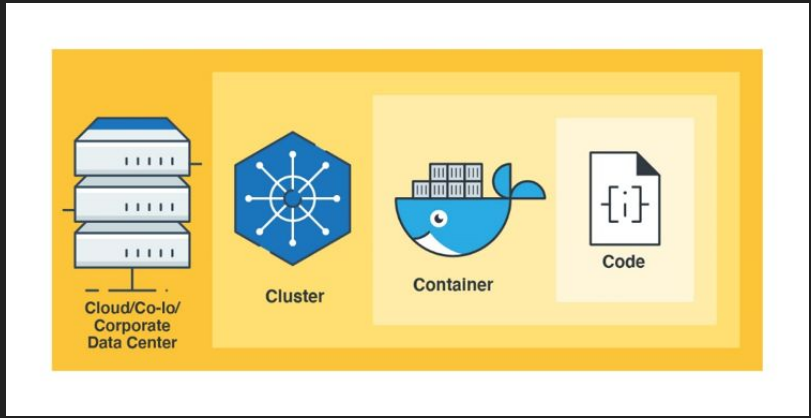
Summary or Attack demo?

Summary or Attack demo?

Cloud	Cluster	Container	Code
 TFSEC	polaris by Fairwinds Falco  Open Policy Agent  OWASP ModSecurity Core Rule Set THE 1ST LINE OF DEFENSE	 trivy	sonarqube

Summary and buzzwords

- Shift left on security, early focus
- Consider your vulnerabilities for all layers
  - Cloud
  - Cluster
  - Container
  - Code
- Automated scanning and analysis
- Remember that a creative mind finds stuff a machine can’t.



Thank you

Frederik Mogensen
@fmogensen

Examples are available at: https://github.com/mogensen/cloud-security-presentation/

goto;

Don’t forget to
vote for this session
in the **GOTO Guide app**