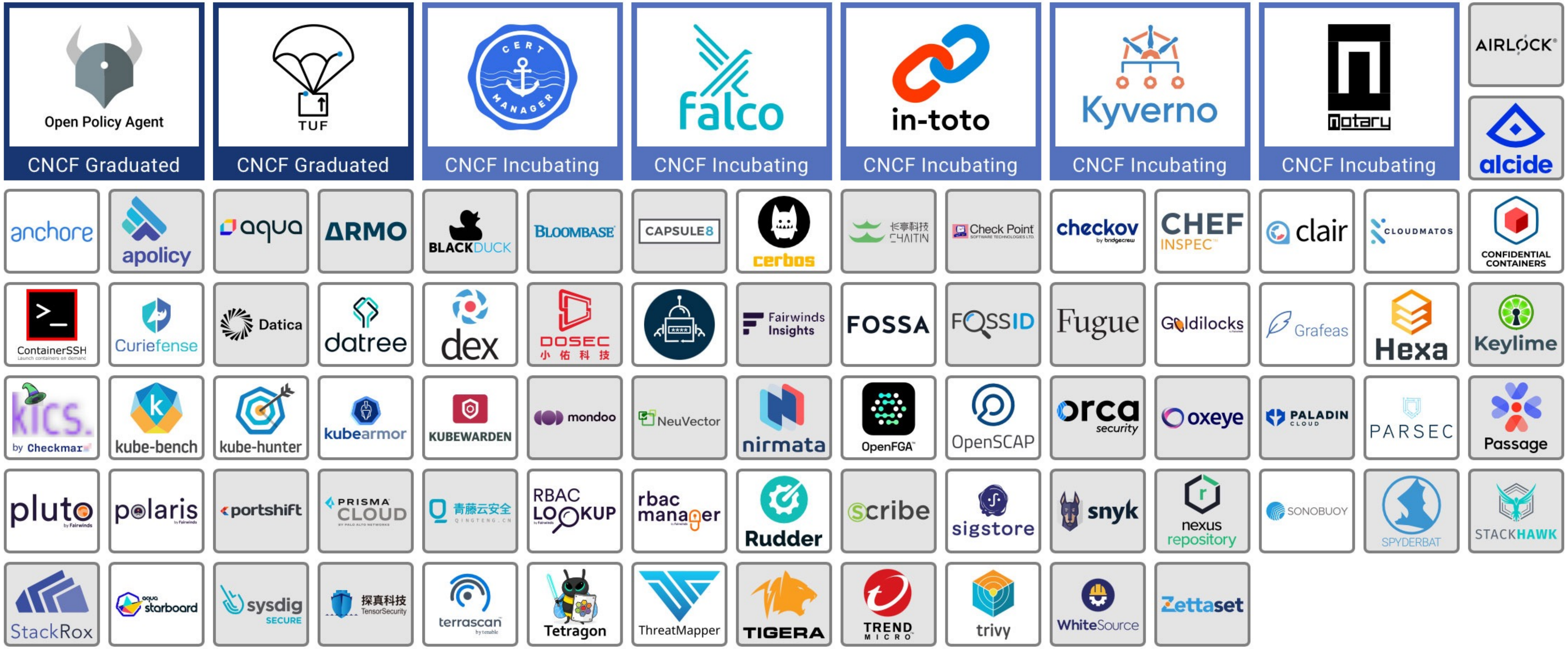
Cloud, Cluster, Container and Code
An introduction to Kubernetes Security

Dennis Hemeier | CloudPirates GmbH & Co. KG

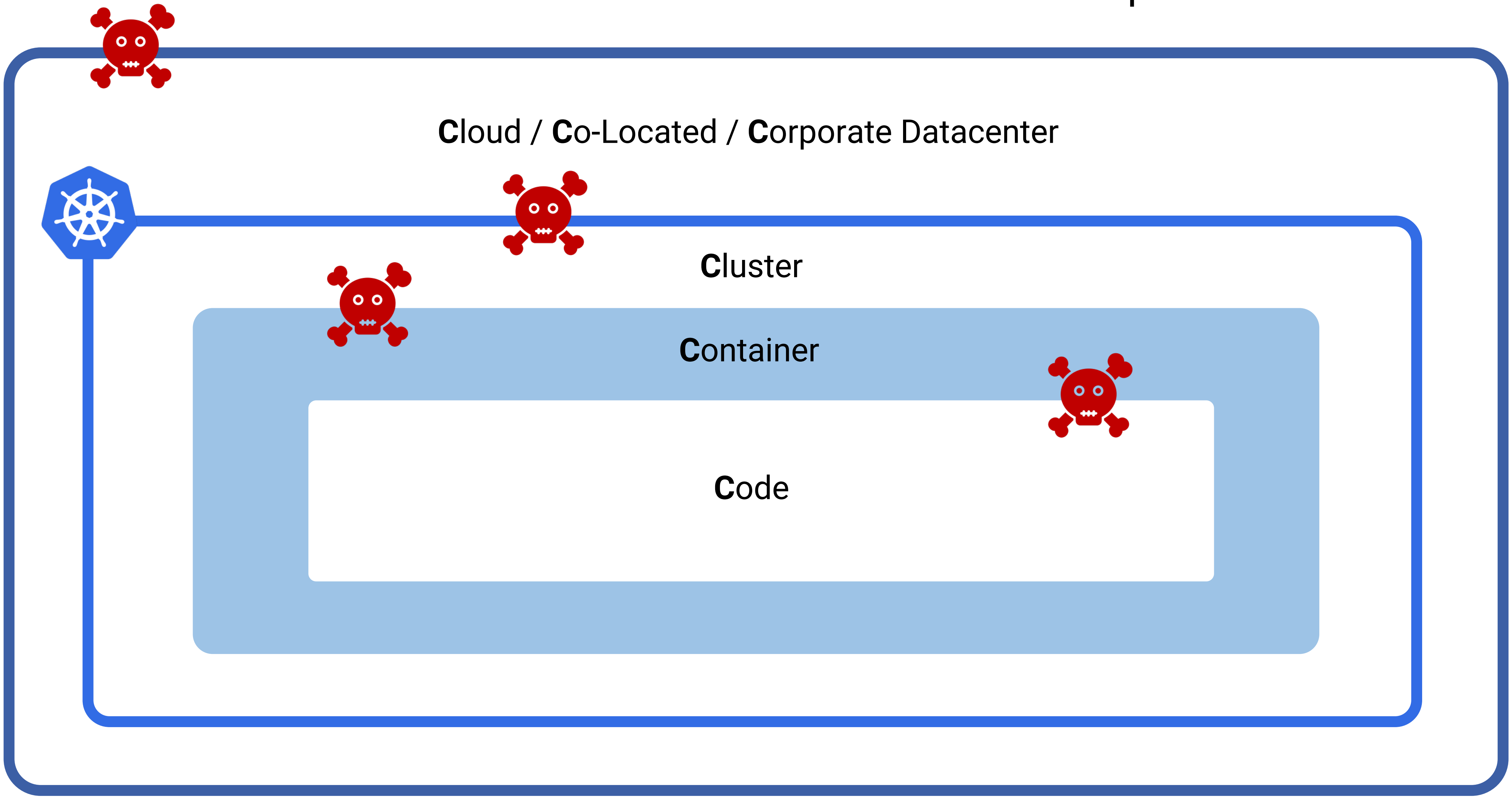
CloudPirates

Security in **Kubernetes** and **Cloud Native** can be **complex**...



81 Tools for Security & Compliance: landscape.cncf.io

Introduction to the **4C** Concept



Cloud / **C**o-Located / **C**orporate Datacenter

Cluster

Container

Code

Dennis Hemeier

Cloud Native Solutions Architect and
Co-Founder @ CloudPirates

Focus on **Kubernetes**
and **Cloud Native Technologies** since 2016

Consulting & Implementation in all steps of the Application Lifecycle on enterprise level

100+ Trainings and workshops held
(Mostly in German though)

Cloud

Networking and Firewalls, Access Restrictions

Node / Control Plane Networking

What

- Reduce attack surface over network

Why

- Block all external traffic to your cluster
- Prevent network attacks

How

- Use VPCs from your Cloud Provider
- Create isolated Cluster Subnets / VLANs in your own infrastructure
- If needed: Connect external services over Site-2-Site VPN connections

HTTPS Only Traffic

What

- Secure all external Ingress Resources with certificates

Why

- Block Man-in-the-Middle attacks
- Prevent traffic sniffing/spoofing

How

- Implement Cert-Manager for management of certificates
- Use HTTPS only access to your Ingress resources
- Easy integration with public (Let´s Encrypt) and private/custom CAs

Cluster

Authentication, RBAC, Audit Logs, Runtime Security

Authentication

What

- Use an external authentication provider

Azure Active Directory

AWS IAM

Identity and Access Management (IAM)

OpenID

KEYCLOAK

Why

- Get personalized cluster access
- Access logs

How

- Use tools like AzureAD, AWS IAM, Google Cloud IAM or OpenID connect
- Never share your default „admin“ kubeconfig

Access Control

What

- Limit access to your cluster

Why

- Block unwanted access to the Kubernetes API

How

- Use RBAC with least privileges applied
  i.e. grant only access for required namespaces and pods
- Block access to your production cluster

Audit Logs

What

- Get insights of security relevant, chronological set of records documenting the sequence of actions that happens in your cluster

Why

- Get details of what, when, who and where
- Detect unexpected activity

How

- Enable audit logs with external backend
- Configure alerts and visualization for important events

Runtime Security

What

- Observe the behaviour of your cluster

Why

- Detect threats at runtime
- Last line of protection

How

- Implement a runtime security tool
- Create security policies based on your needs

falco

kubearmor

Network Policies

What

- Control ingress and egress traffic

Why

- Prevent unwanted network access to applications
- Reduce attack surface

How

- Use a CNI with network policy support
- Create default rules to block all ingress and egress traffic
- Whitelist only traffic required by applications

PROJECT CALICO

ANTREA

cilium

weave net

Container

Image Signing & Scanning, Pod Security Standards

Image Scanning

What

- Regulary scan your container images

Why

- Detect and prevent running of applications with known CVEs

How

- Scan images at build time and on a regulary basis
- Block running of applications with critical CVEs

trivy

clair

HARBOR

Image Signing

What

- Sign your container images

Why

- Supply Chain Security
- Make sure your images are not modified between build and run

How

- Sign your container images in your CI/CD Pipelines
- Validate the signature inside your cluster

sigstore

notary

Pod Security Standards

What

- PSS defines three different policies from highly-permissive to highly-restrictive
- Privileged > Baseline > Restricted

Why

- Prevents known privilege escalations
- Enforce pod hardening best practices

How

- Use at minimum the Baseline Standards
- Enable the Pod Security Admission Controller

Kyverno

Open Policy Agent

KUBEWARDEN

Code

Code Analysis & Testing

Code Analysis

What

- Analyze your application with Static and Dynamic Application Security Testing (SAST, DAST)

Why

- Detect vulnerabilities and common errors

How

- Integrate SAST / DAST Analysis inside your CI/CD Pipelines
- Many tools covers automatic testing of different programming languages

sonarqube

Semgrep

ZAP
Zed Attack Proxy

(Penetration) Testing

What

- Test your applications

Why

- Detect application errors and security risks

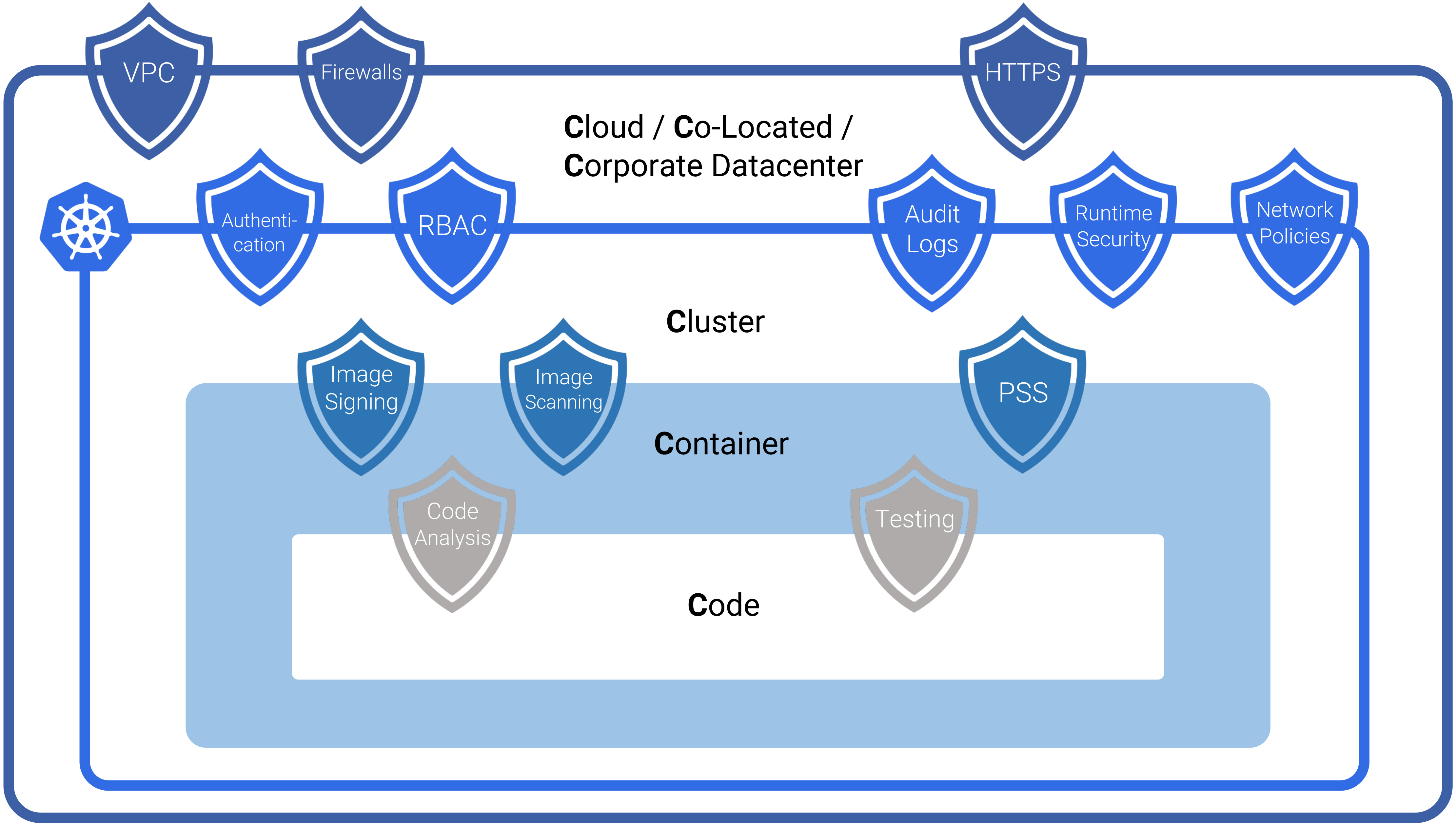
How

- Unit testing
- E2E testing – especially penetration tests

Demo Time

Demo Time – Summary

- Demo Cluster on Azure (AKS)
  - Private Networking
  - AzureAD Authentication + RBAC
- Cert-Manager + Let´s Encrypt
- Kyverno with the following policies applied
  - Pod Security Baseline + Restricted
  - Image Signing Checks
  - Some Best Practices (Pod Probes, Default Network Policies, …)
- Falco
- PolicyReports CRDs + Policy Reporter UI
  - kubernetes-sigs/wg-policy-prototypes
  - Proposal -> Work in Progress -> Not recommended for production


VPC
Firewalls
HTTPS
Cloud / Co-Located /
Corporate Datacenter
Authenti-
cation
RBAC
Audit
Logs
Runtime
Security
Network
Policies
Cluster
Image
Signing
Image
Scanning
PSS
Container
Code
Analysis
Testing
Code

Key Takeaways

- Start with a stable foundation
  - Private Cluster & HTTPS-Only
  - External Authentication & RBAC
  - Image Scanning & Signing
  - Pod Security Standards -> Baseline
- Extend if needed
- Use the official documentations:

  https://kubernetes.io/docs/concepts/security

  https://github.com/kubernetes/sig-security

Thank You 👏

Questions?

Explore the Policy Reporter by yourself

policy-reporter.kcd-munich.cloudpirates.io