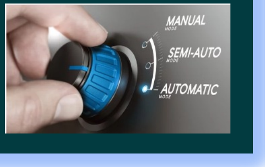
Kubernetes on, what’s next?

Experience out of the field

Speaker:
Dinant Paardenkooper – Innovator

Topics:
- Kubernetes
- Extra addon parts design decissions
- Usecase experience out of the field



Introduction

Dinant Paardenkooper

Rol: Handson Cloud Native Solution Architect (Azure, VMWare)
Cloud Native | Kubernetes | Automation | IaC | Spreker

Drive: Innovation, Business requirements transform to praktical technical solutions

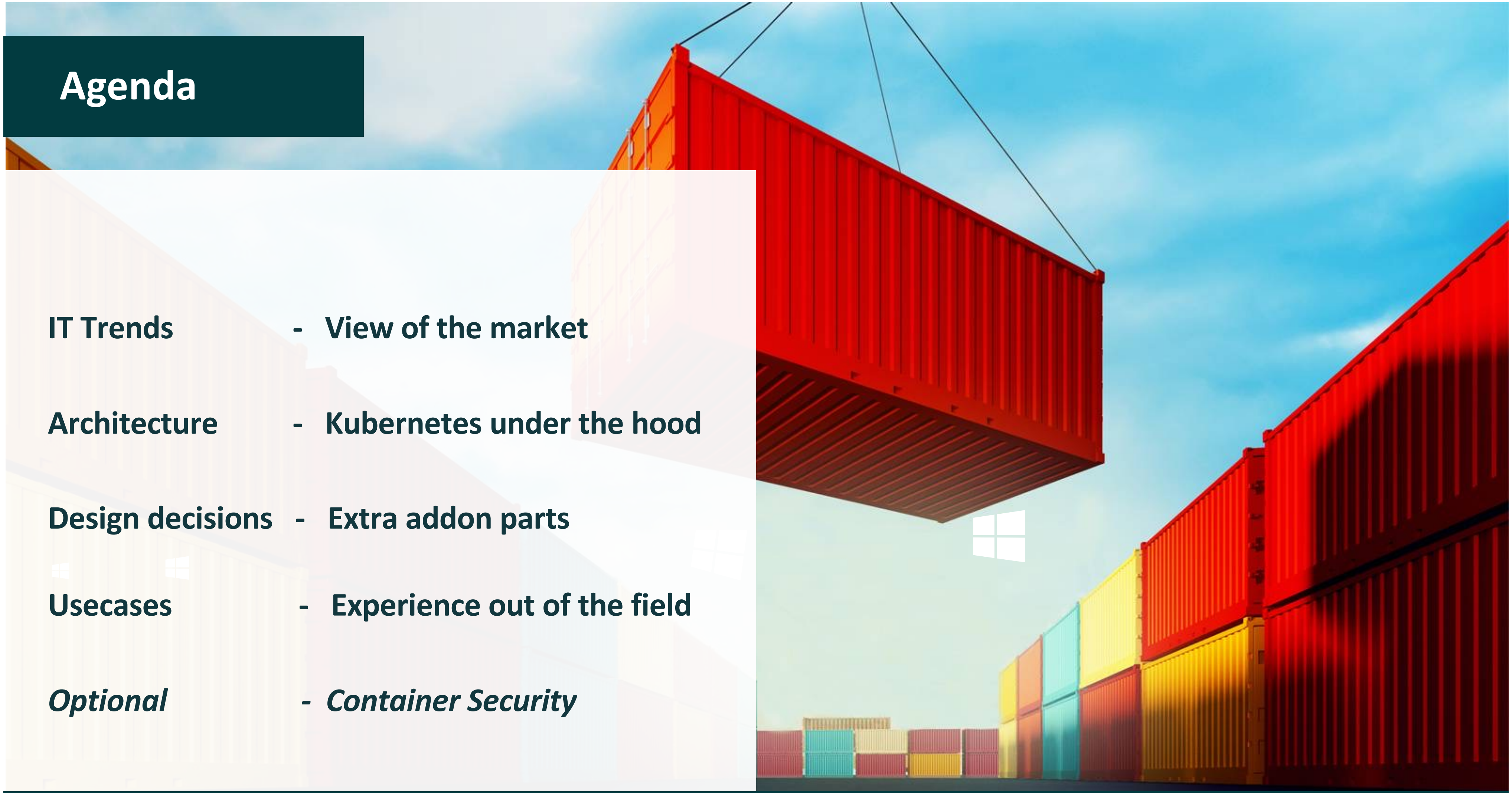
Hobby’s: Play Gitaar, innovating, running, squash

E-mail: d.paardenkooper@IT-Impressive.nl

LinkedIn: www.linkedin.com/in/dinantpaardenkooper

CERTIFIED kubernetes APPLICATION DEVELOPER
CERTIFIED KUBERNETES APPLICATION DEVELOPER
CERTIFIED kubernetes ADMINISTRATOR
CERTIFIED KUBERNETES ADMINISTRATOR
RANCHER ACADEMY CERTIFICATE OF COMPETENCY
RANCHER ACADEMY CERTIFIED RANCHER OPERATOR
Terraform ASSOCIATE HashiCorp CERTIFIED
TERRAFORM ASSOCIATE HASHICORP CERTIFIED
Microsoft CERTIFIED DevOps Engineer
MICROSOFT CERTIFIED AZURE DEVOPS
Microsoft CERTIFIED Azure Architect Expert
MICROSOFT CERTIFIED AZURE SOLUTION ARCHITECT

Agenda



IT Trends - View of the market

Architecture - Kubernetes under the hood

Design decisions - Extra addon parts

Usecases - Experience out of the field

Optional - Container Security

IT Trends

IT Trends

According to Gartner

Composable Applications

Decision Intelligence

Hyperautomation

AI Engineering

Data Fabric

Cybersecurity Mesh

Privacy-Enhancing Computation

Cloud-Native Platforms

Distributed Enterprise

Total Experience

Autonomic Systems

Generative AI

IT Trends

Arccording to Gartner

Composable Applications

Decision Intelligence CI/CD

Hyperautomation

AI Engineering Infra As Code

Data Fabric

Cybersecurity Mesh

Privacy-Enhancing Computation

Cloud-Native Platforms

Kubernetes en security

Distributed Enterprise

Total Experience

Autonomic Systems

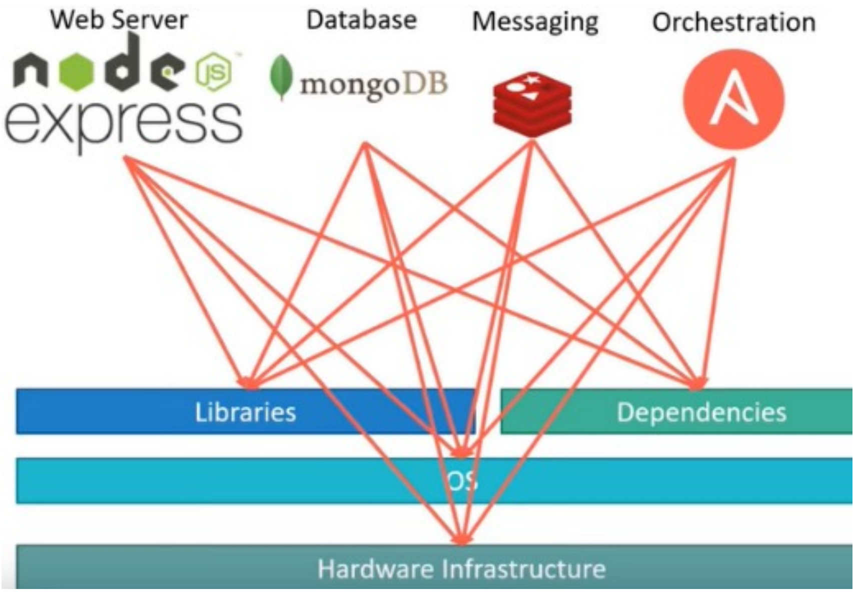
Generative AI

Products out of the Market

Kubernetes	RED HAT OPENSHIFT Container Platform		RANCHER	VMware Tanzu
Security	Twistlock	aqua	sysdig	RedLock
CI/CD	GitLab	Azure DevOps	GitHub Actions	vRealize Automation 8.0
Infrastructure as Code	Scripting	+	HashiCorp Terraform	PowerShell

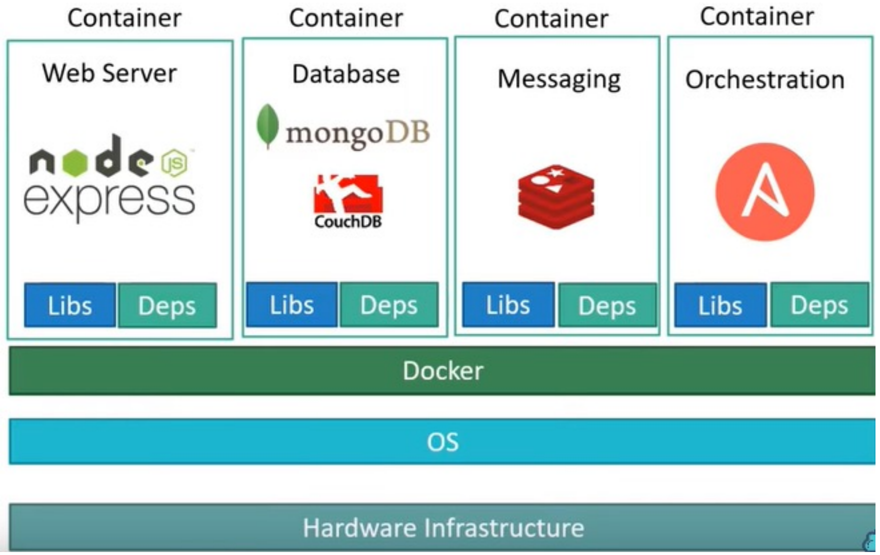
What is a container?

Power of containers



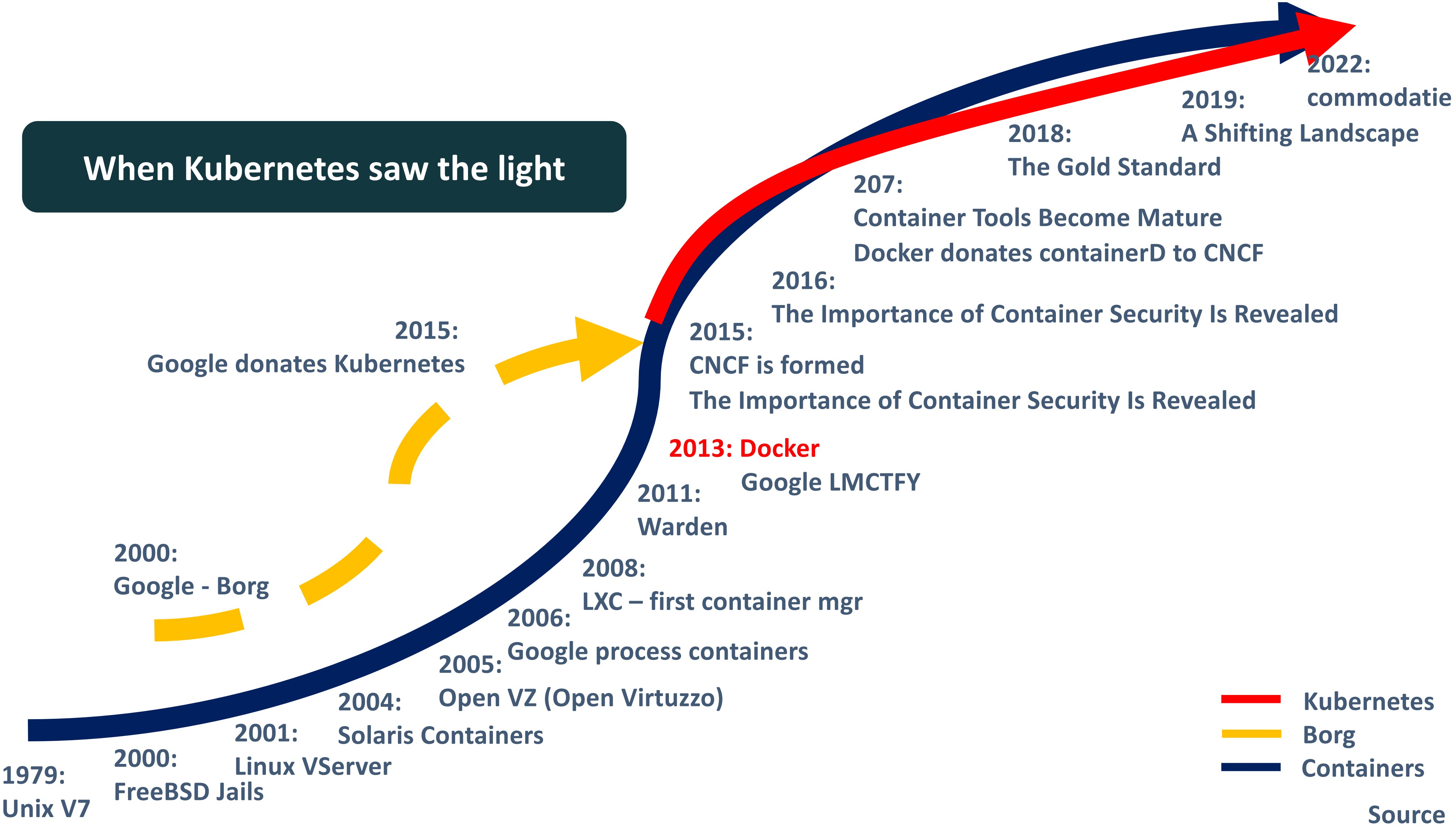
Traditioneel

VS



Containerized

When Kubernetes saw the light



1979:
Unix V7

2000:
FreeBSD Jails

2001:
Linux VServer

2004:
Solaris Containers

2005:
Open VZ (Open Virtuzzo)

2006:
Google process containers

2008:
LXC – first container mgr

2011:
Warden

Google LMCTFY

2013: Docker

2015:
CNCF is formed
The Importance of Container Security Is Revealed

2016:
The Importance of Container Security Is Revealed

207:
Container Tools Become Mature
Docker donates containerD to CNCF

2018:
The Gold Standard

2019:
A Shifting Landscape

2022:
commodatie

2000:
Google - Borg

2015:
Google donates Kubernetes

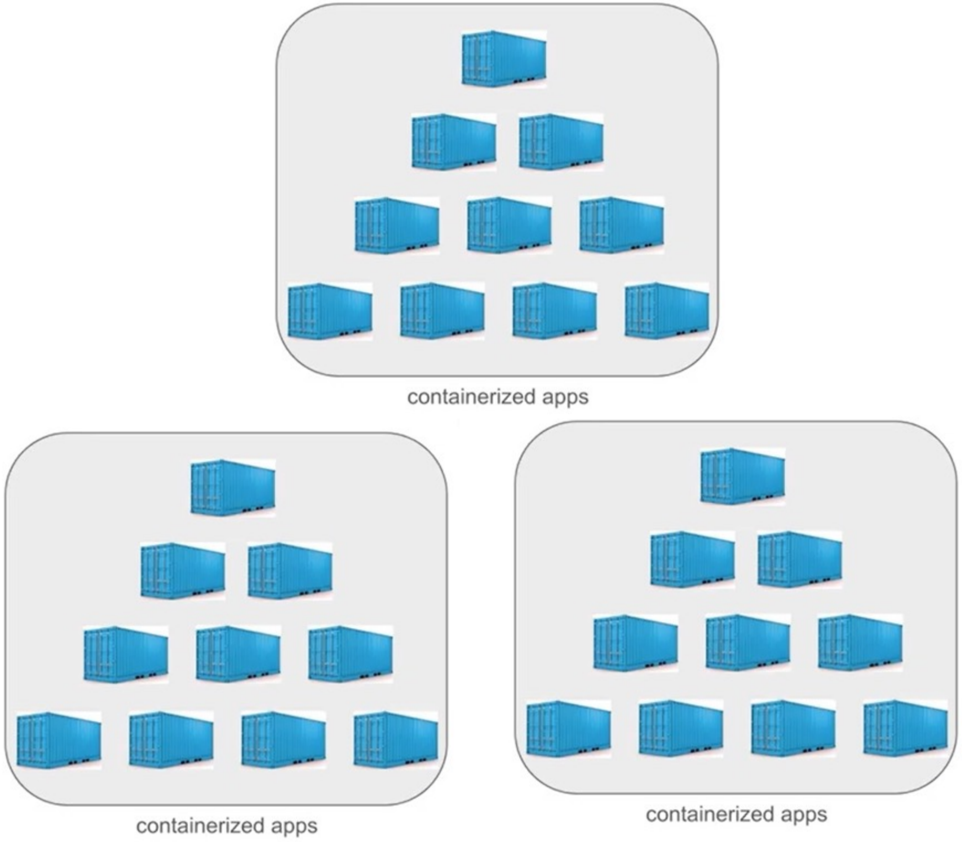
🟥 Kubernetes
🟨 Borg
🟦 Containers

Source

Container challenges

How to solve?

Schale
Support
Loadbalancing
Storage
Security
RBAC
And more …



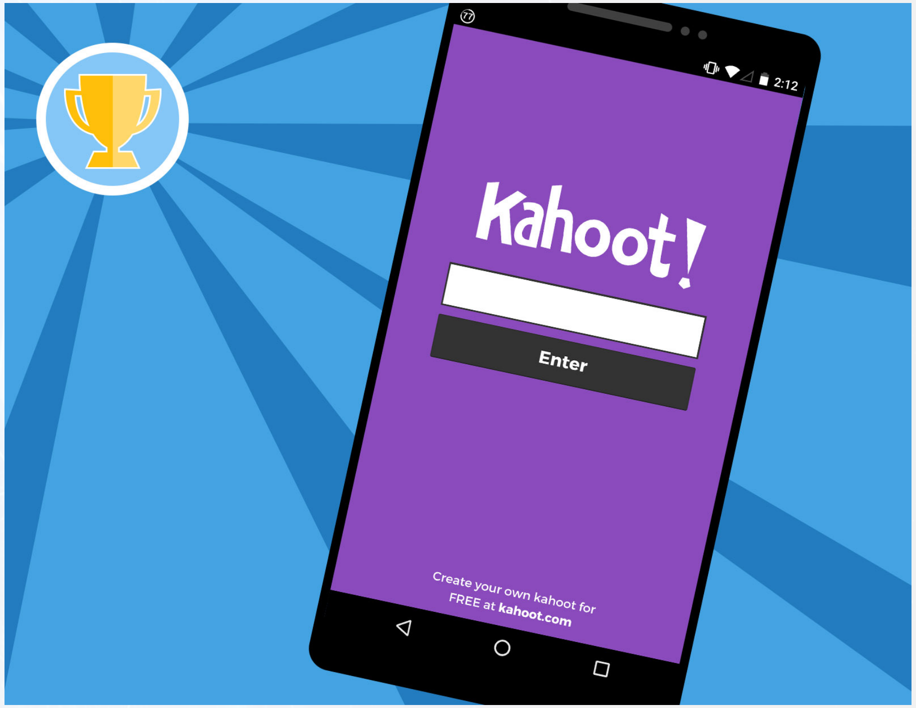
Kubernetes

Knowledge check

Kahoot!

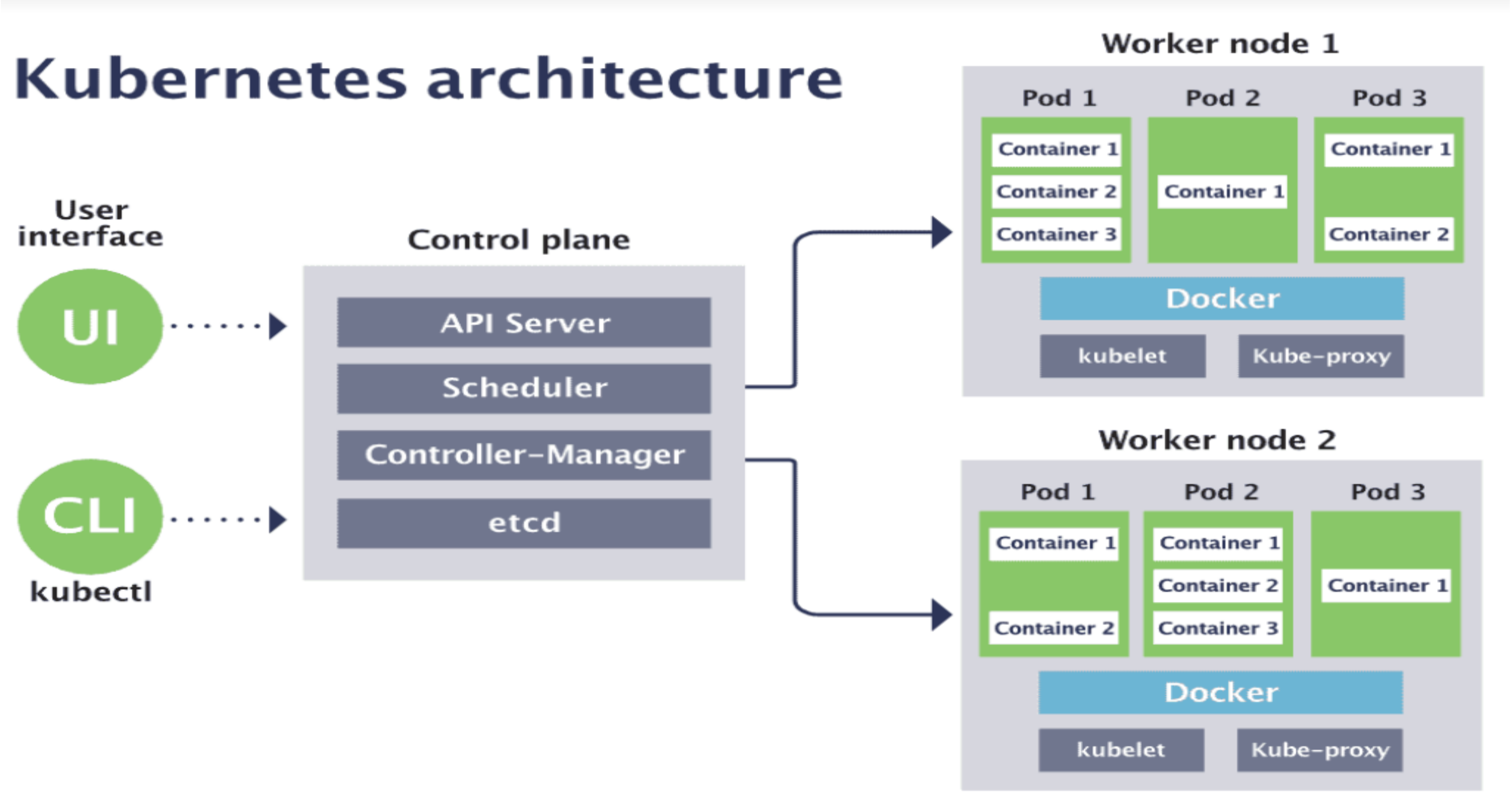
Download it on your smartphone!

- Fill in the code ….
- Press “Enter”



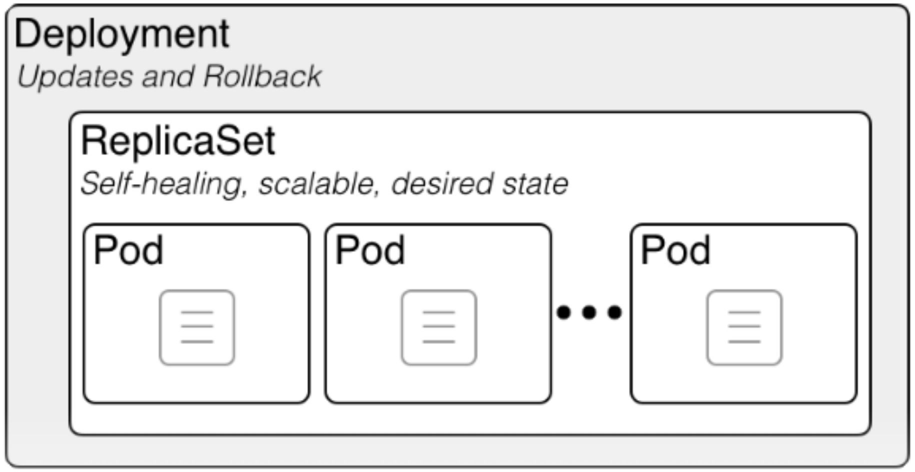
Architecture

Kubernetes architecture



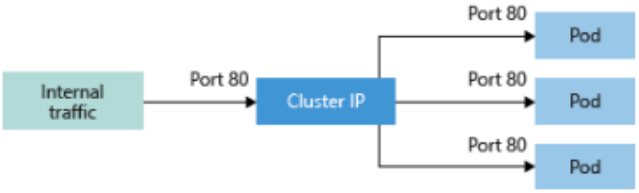
Terminology (1/2)

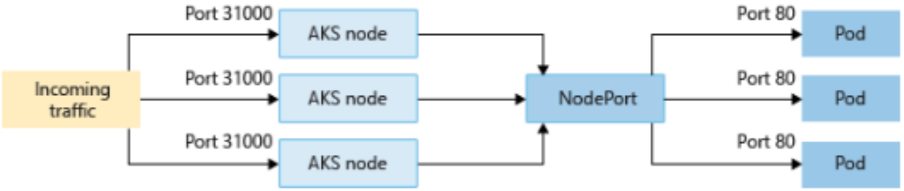
- Pod;
- Deployment;
- ReplicaSet;
- PersistentVolume en PersistenVolumeClaim;

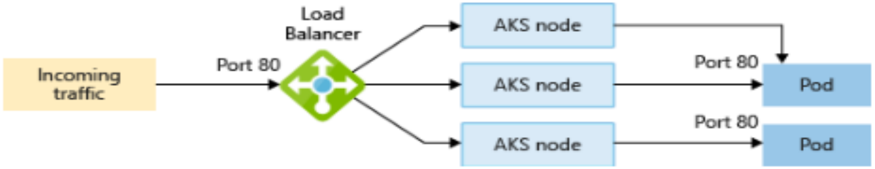


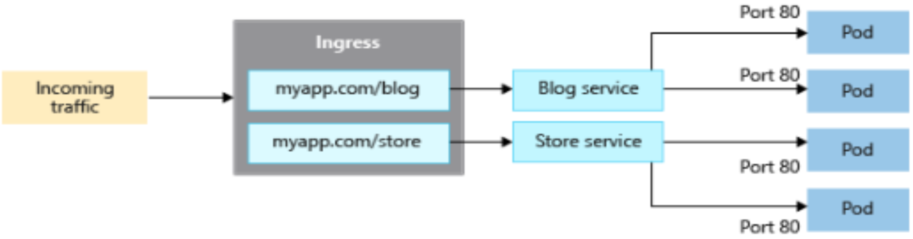
Terminology (2/2)

- Services
- Ingress









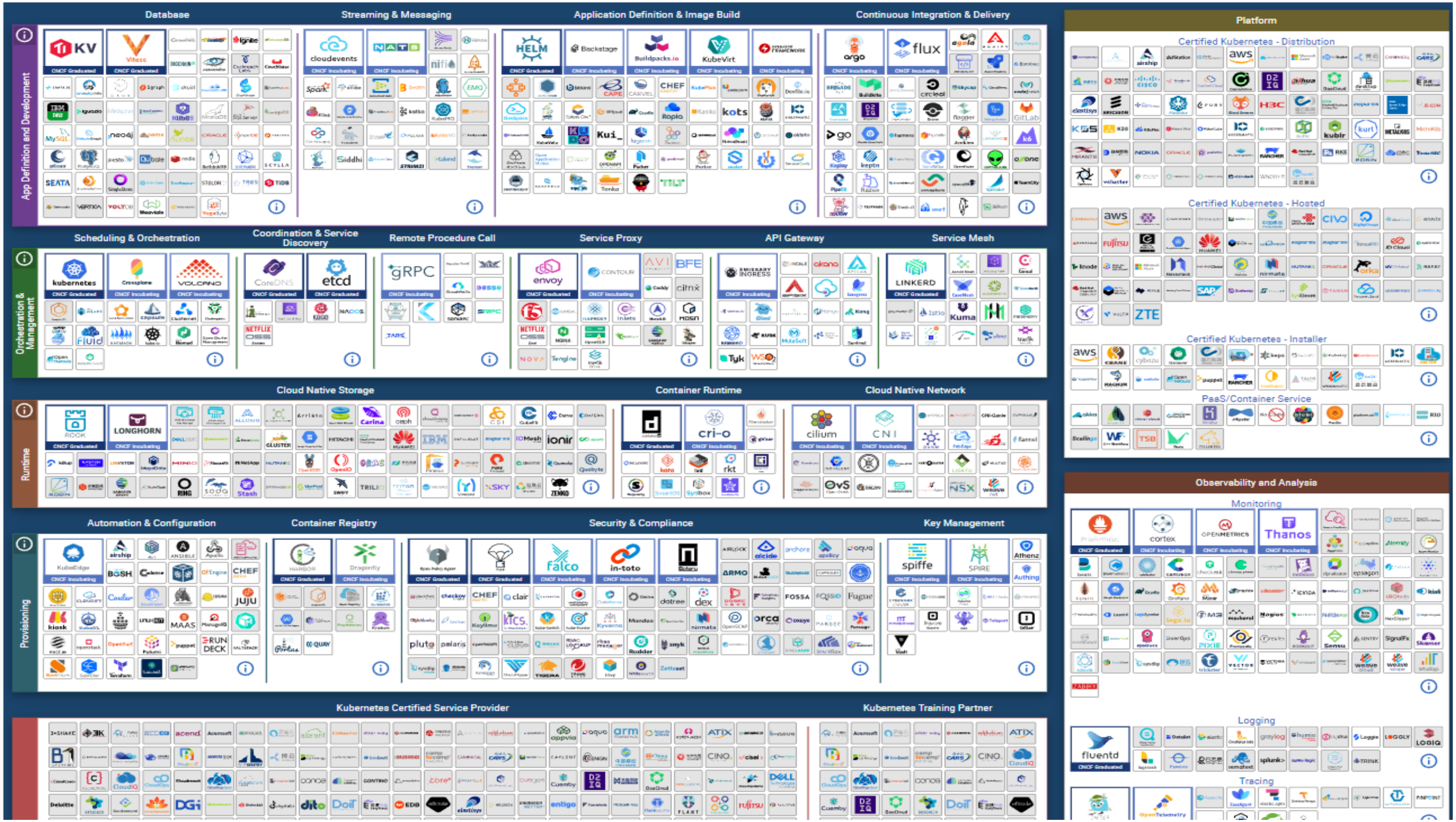
Addons

Platform

Automation

Application

Security



App Definition and Development

Database

Streaming & Messaging

Application Definition & Image Build

Continuous Integration & Delivery

Orchestration & Management

Scheduling & Orchestration

Coordination & Service Discovery

Remote Procedure Call

Service Proxy

API Gateway

Service Mesh

Runtime

Cloud Native Storage

Container Runtime

Cloud Native Network

Provisioning

Automation & Configuration

Container Registry

Security & Compliance

Key Management

Kubernetes Certified Service Provider

Kubernetes Training Partner

Platform

Certified Kubernetes - Distribution

Certified Kubernetes - Hosted

Certified Kubernetes - Installer

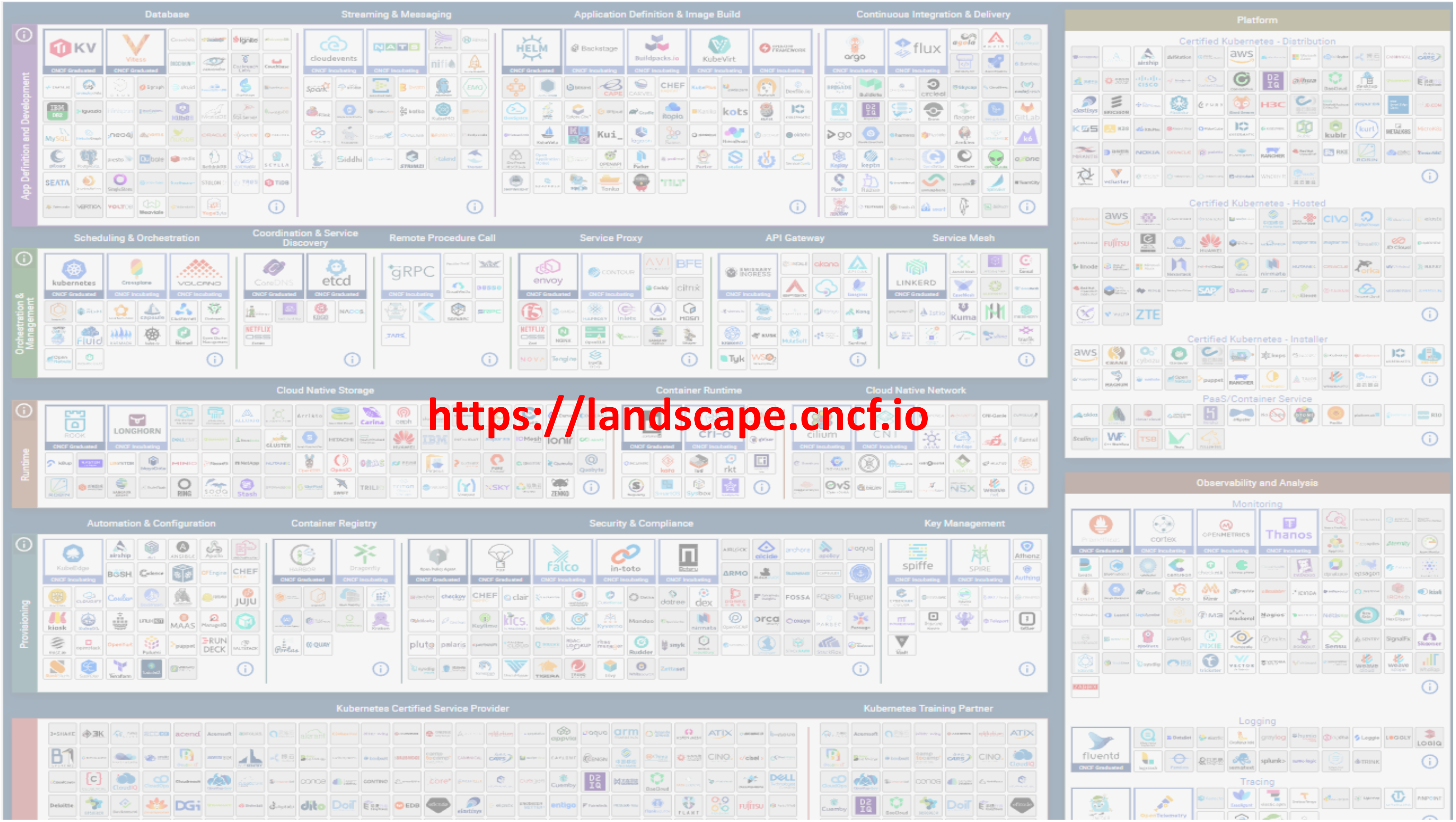
PaaS/Container Service

Observability and Analysis

Monitoring

Logging

Tracing


Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Platform
App Definition and Development
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Orchestration & Management
Cloud Native Storage
Container Runtime
Cloud Native Network
Runtime
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Provisioning
Observability and Analysis
Monitoring
Logging
Tracing
Kubernetes Certified Service Provider
Kubernetes Training Partner

https://landscape.cncf.io

Platform

Design decisions after understanding your environment

On-Prem

- Choose + Harden OS with CIS benchmark
- Choose Ingress controller;
- Custom Container Registry;
- Custom Network and LB;
- Setup Monitoring, storage, DR and IAM;
- Implement Persistent Storage;
- Patching and Lifecyclemgmt;
- Cost mgmt

RANCHER

RED HAT OPENSHIFT Container Platform

VMware Tanzu

Cloud

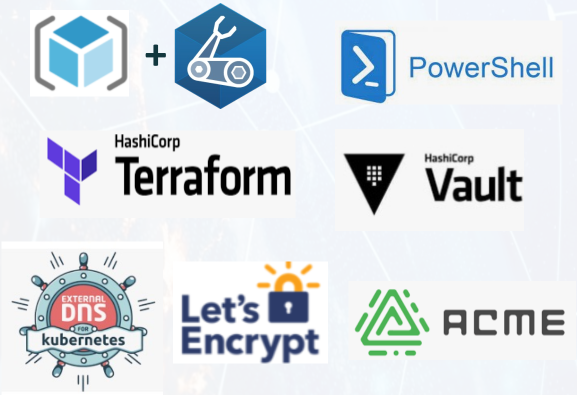
- Harden OS with CIS benchmark
- Choose Ingress controller;
- Integrated Container Registry;
- Integrated Network and LB;
- Integrated Monitoring, DR and IAM;
- Integrated Persistent Storage;
- Patching and Lifecyclemgmt;
- Cost mgmt

Automation

Design decisions after understanding organisation needs, skills and expertise in automating.

On-Prem

- Deploy infra via Infra as Code;
- Automate DNS and Certificate mgmt;
- Application Deployment.



Cloud

- Deploy infra via Infra as Code;
- Automate DNS and Certificate mgmt;
- Application Deployment.

Application

Design decisions after discovering Developers needs, skills and expertise

On-Prem

- Prometheus or Custom APM;
- Select CI/CD tooling auto deployment;
- Select Secret mgmt tooling;
- Code Repository;
- Choose application backup tooling;
- Custom image build process;
- Observability and incidentmgmt;

Azure DevOps

GitHub Actions

GitLab

HashiCorp Vault

kasten by Veeam

MetalLB

elastic

+

Cloud

- Integrated APM;
- Select CI/CD tooling auto deployment;
- Integraded Secret mgmt tooling;
- Code Repository;
- Choose application backup tooling;
- Custom image build process;
- Observability and incidentmgmt;

Security

Design decisions inform, demonstrate and discover the journey where the customers is.

On-Prem

- Decide setup connection to DB's;
- Select container security tooling;
- CD/CD pipeline and Registry scanning;
- Encrypt secrets and rotate;
- Secure namespaces, kubelet, KubeAPI;
- Use OPA policies and Network policies;
- Kubernetes Security Best Practices;
- Select Service Mesh if needed.

Twistlock aqua

sysdig RedLock

Falco Open Policy Agent

cilium Open Service Mesh

Istio LINKERD

Cloud

- Creating DB integration;
- Select container security tooling;
- CD/CD pipeline and Registry scanning;
- Encrypt and rotate secrets;
- Secure namespaces, kubelet, KubeAPI;
- Use OPA policies and Network policies;
- Kubernetes Security Best Practices;
- Select Service Mesh if needed.

Two usecases

Airgapped

Public Cloud

IT-IMPRESSIVE

YER

Usecase - Airgapped

Usecase - Airgapped

Platform Decisions

Topics	Decisions
- Choose+Harden OS with CIS benchmark	- Hardened CIS Ubuntu/Win OS
- Choose Ingress controller;	- Nginx Ingress controller;
- Custom Container Registry;	- Harbor Registry;
- Custom Network and LB;	- VMWare, F5 and later MetalLB;
- Setup Monitoring, storage, DR and IAM;	- Prometheus, VMWare and AD;
- Implement Persistent Storage;	- Netapp Trident and vSphere CSI;
- Patching and Lifecyclemgmt;	- Montly patching, Kubernetes N-1;
- Cost mgmt.	- Difficult to display.

Usecase - Airgapped

Automation Decisions

Topics

- Deploy infra via Infra as Code;
- Automate DNS and Certificate mgmt;
- App Deployment.

Decisions

- Terraform and Powershell;
- External DNS with Acme protocol;
- GitLab pipelines, Loadbalancer changed from F5 to MetalLB.

Usecase - Airgapped

Application Decisions

Topics	Decisions
- Prometheus or Custom APM;	- Prometheus and Graylog;
- Select CI/CD tooling auto deployment;	- GitLab pipelines;
- Code Repository;	- GitLab;
- Select Secret mgmt tooling;	- HashiCorp Vault;
- Choose application backup tooling;	- Kasten IO (Veeam);
- Custom image build process;	- GitLab pipelines;
- Observability and incidentmgmt;	- ElasticSearch;

Usecase - Airgapped

Some security decisions

Topics	Decisions
- Decide setup connection to DB’s;	- External DB outside Kubernetes;
- Select container security tooling;	- Aqua Enterprise;
- CD/CD pipeline and Registry scanning;	- Integration GitLab + Aqua Enterprise;
- Encrypt secrets and rotate;	- HashiCorp Vault;
- Secure namespaces, kubelet, KubeAPI;	- Kubernetes Security Best Practices;
- Use OPA policies and Network policies;	- OPA Policies and Falco;
- Kubernetes Security Best Practices;	- Kubernetes Security Best Practices;
- Select Service Mesh if needed.	- Not filled in yet.

Usecase – Public Cloud (Azure)

Usecase – Public cloud (Azure)

Platform Decisions

Topics	Decisions
- Choose+Harden OS with CIS benchmark	- Hardened CIS Ubuntu/Win OS
- Choose Ingress controller;	- Nginx Ingress controller;
- Custom Container Registry;	- Azure Container Registry;
- Custom Network and LB;	- Azure, Azure LoadBalancer;
- Setup Monitoring, storage, DR and IAM;	- AAD, Avail. Zones, ContainerInsights;
- Implement Persistent Storage;	- Azure Disk integrated;
- Patching and Lifecyclemgmt;	- Montly patching, Kubernetes N-1;
- Cost mgmt	- Pay as you go – Azure reservations.

Usecase – Public cloud (Azure)

Automation Decisions

Topics

- Deploy infra via Infra as Code;
- Automate DNS and Certificate mgmt;
- App Deployment.

Decisions

- Terraform, ARM and Biceps;
- External DNS, Azure DNS Zones and, Infoblox, Certs still manual;
- AzureDevops pipelines and Github Actions.

Usecase – Public cloud (Azure)

Application Decisions

Topics

- Prometheus or Custom APM;
- Select CI/CD tooling auto deployment;
- Code Repository;
- Select Secret mgmt tooling;
- Choose application backup tooling;
- Custom image build process;
- Observability and incidentmgmt.

Decisions

- Prometheus and Container Insights;
- GitHub Actions / AzureDevOps;
- Git;
- Azure KeyVault;
- Velero;
- GitLab pipelines;
- ElasticSearch and ServiceNow.

Usecase – Public cloud (Azure)

Some security decisions

Topics

- Decide setup connection to DB's;
- Select container security tooling;
- CD/CD pipeline and Registry scanning;
- Encrypt secrets and rotate;
- Secure namespaces, kubelet, KubeAPI;
- Use OPA policies and Network policies;
- Kubernetes Security Best Practices;
- Select Service Mesh if needed.

Decisions

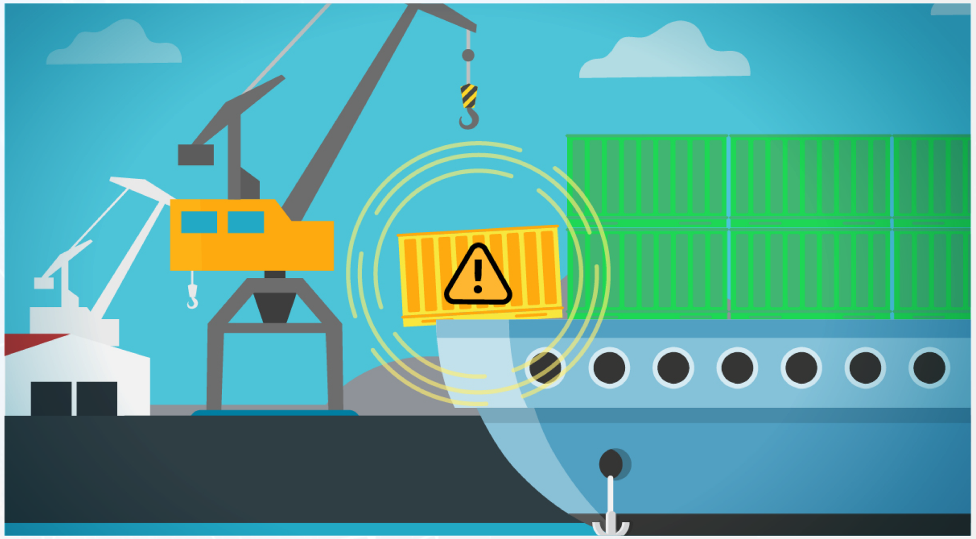
- External PAAS DB outside Kubernetes;
- Aqua Enterprise or Sysdig;
- Integration Aqua Enterprise or Sysdig;
- Azure KeyVault;
- Kubernetes Security Best Practices;
- OPA Policies and Falco;
- Kubernetes Security Best Practices;
- Not filled in yet.

Kubernetes Security

Types of Riscs

Type Risico's

- Container image;
- Container Registry;
- Kubernetes orchestration;
- Container (runtime);
- Operating System Kubernetes Nodes;



Container image riscs

Defined riscs

- Vulnerabilities (CVE’s);
- Configuration defects;
- Embedded malware;
- Embedded clear text secrets;
- Untrusted images.

Mitigation measures

- Aqua can scan during build time (integration with Azure DevOps);
- Aqua can scan your Azure Container Registry;
- Aqua scans images on AKS hosts;
- Each image is scanned for vulnerabilities both in its OS packages and development language files.

Container Registry riscs

Defined riscs

- Insecure connections;
- Stale images;
- Insufficient authentication and authorization restrictions.

Mitigation measures

- Only allow images from specific (trusted) container registries;
- Allows daily scans of images to alert on out-of-date vulnerable packages, base-images and versions;
- Allows the admin to define stale images via custom checks and block them from running;
- Can integrate automated scans into your CI processes to ensure only authorized images can be used.

Kubernetes orchestrator riscs

Defined riscs

- Unbounded administrative access;
- Unauthorized access;
- Poorly inter-container connectivity;
- Mixing of workload sensitivity levels;
- Node trust.

Mitigation measures

- Audit logging;
- Set and enforce user access policies to container resources;
- Monitor user access, blocks, alerts unauthorized access attempts;
- Container Firewall limits network connectivity between workloads;
- Host integrity checks, including vulnerability scan, malware and CIS test to ensure nodes are secured.

Container riscs

Defined riscs

- Vulnerabilities within runtime software;
- Unbounded network access from containers;
- Insecure container runtime configuration;
- Application vulnerabilities.

Mitigation measures

- Threat mitigation defenses detect and prevent port scanning;
- Threat mitigation defenses to detect and prevent connections to IP addresses with poor reputation;
- Real-time audit events on policy violations, report to SIEM tooling;
- Check for configuration drift;
- Block non-compliant images
- Block/allow certain executables;
- Prevent certain volumes to be mounted in a container;
- Manage and enforce seccomp profiles to unwanted syscalls;
- Log all container events.

Operating system

Defined riscs

- Attack surface;
- Shared kernel;
- Host OS component vulnerabilities;
- Improper user access rights;
- Host file system tampering.

Mitigation measures

- Scans host for vulnerabilities and malware against the Center for Internet Security (CIS) benchmarks (Docker, K8s);
- Logs user login and logout events on the host, including invocation of sudo programs;
- Scans hosts for configuration issues per the CIS Docker Benchmark;
- Restrict containers from specific mounting volumes or from writing into specific volumes or directories.

Container Security

sysdig

aqua

Take aways

Understand environment

Choose an usecase

Start Small

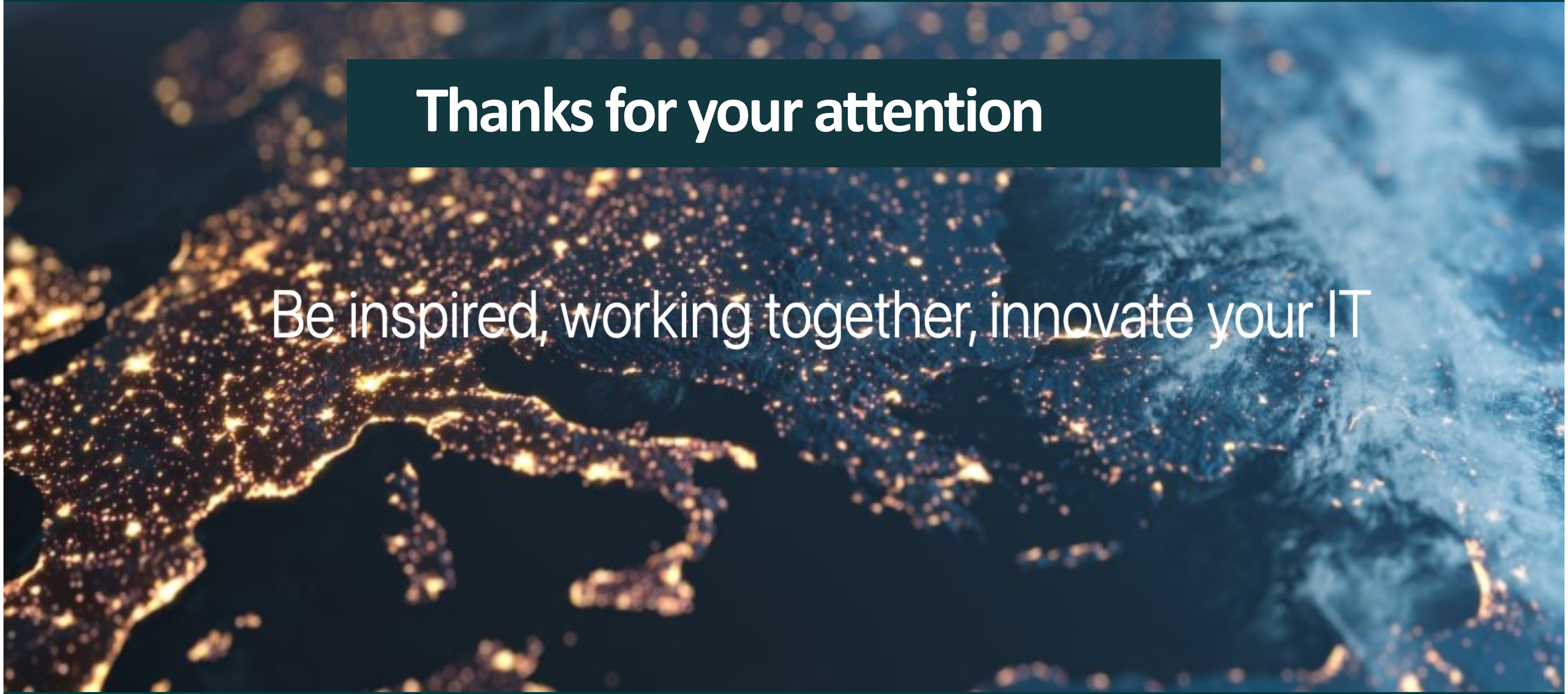
DRY-Principe

Repeat? Automate

Build & Test

Just do it!

Always Innovate



Thanks for your attention

Be inspired, working together, innovate your IT