Let’s build a platform!

In a Microsoft shop stuck in the 90s

Hi, I'm Carlos

SRE @ Payvision

tech problems don't exist.
people problems exist.

@gapingvoid

THE
NEVERENDING
STORY

Context

- May 2018 ~ Today!

- 1:1 App / VM Model (600+ VMs)
- Everything on-premise
- PCI DSS

More Context

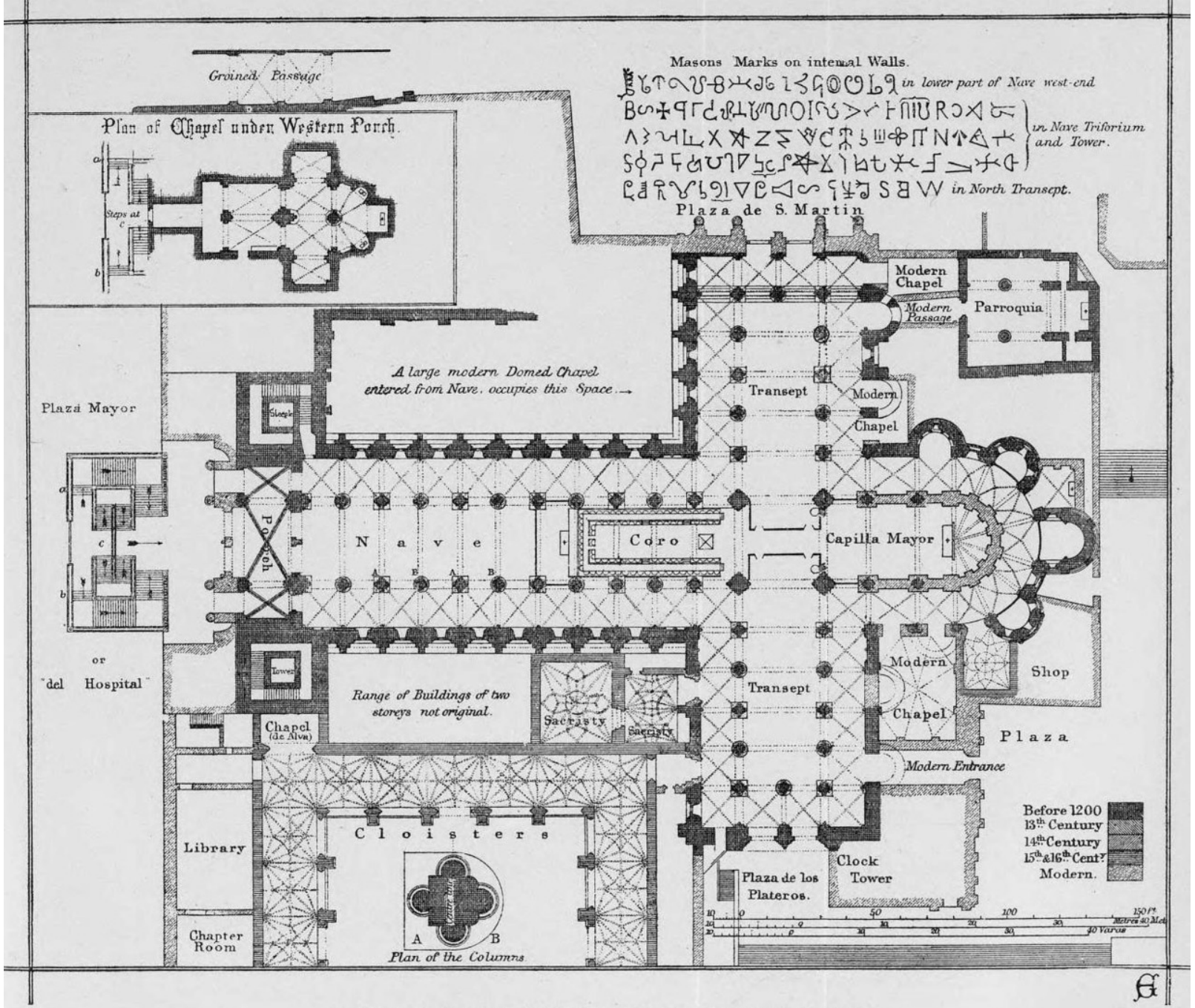
- Windows Server 2008
- Barely any Linux VM

- CV driven development

- Almost everything manual
- Almost no CI/CD

How to start?

MARIAE
NASCENTI



SANTIAGO DE CAMPOSTELA.—PLANTA DE LA CATEDRAL

landscape.cncf.io

CNCF Cloud Native Interactive Landscape

CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION

The Cloud Native Trail Map (png, pdf) is CNCF's recommended path through the cloud native landscape. The cloud native landscape (png, pdf), serverless landscape (png, pdf), and member landscape (png, pdf) are dynamically generated below. Please open a pull request to correct any issues. Greyed logos are not open source. Last Updated: 2020-03-04 08:22:52Z

You are viewing 1,339 cards with a total of 2,073,154 stars, market cap of $15.28T and funding of $68.74B.

Reset Filters

Grouping: N/A

Sort By: N/A

Category: N/A

CNCF Relation: Any

License: Any

Organization: Any

Headquarters Location: Any

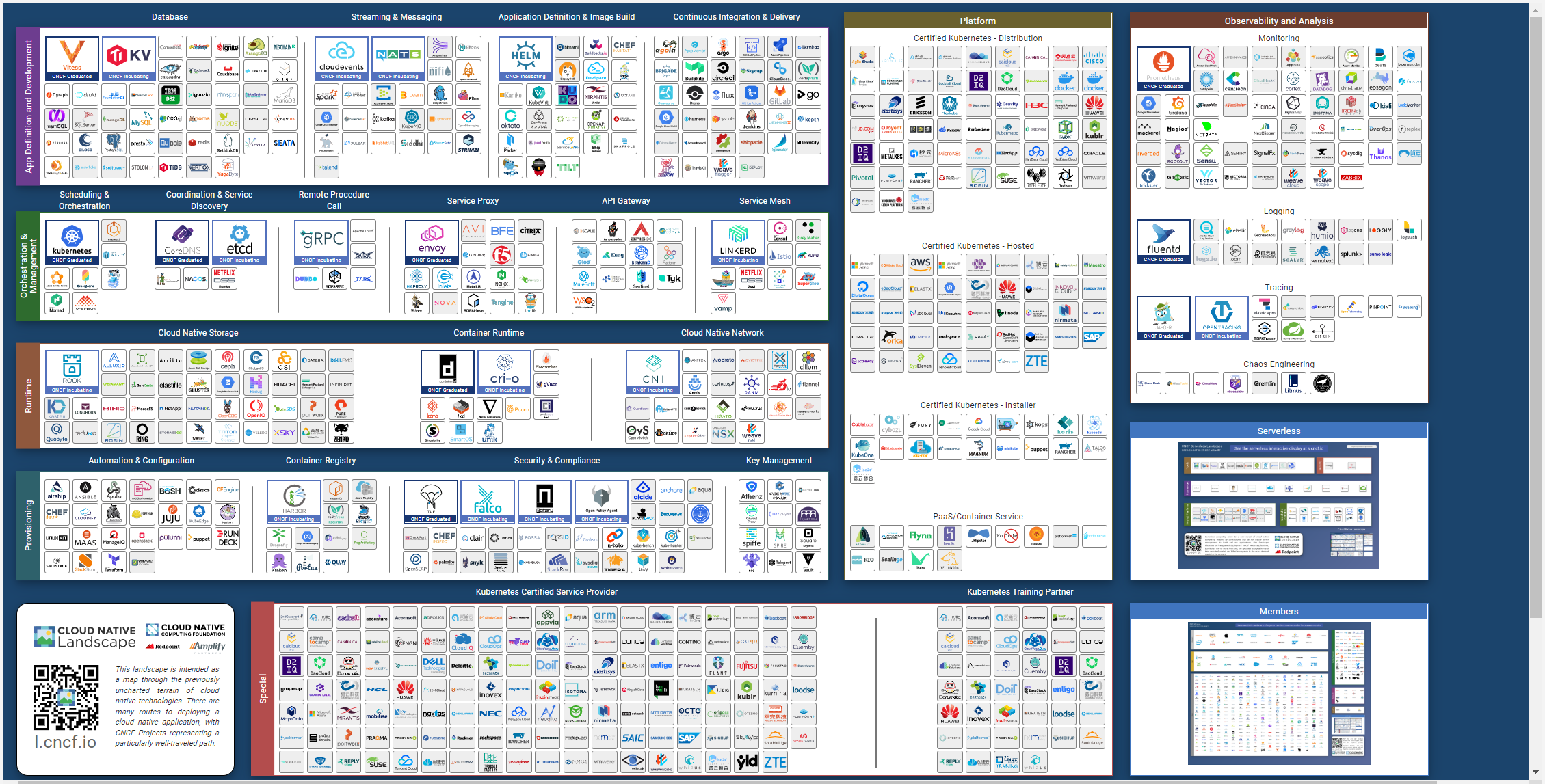
Example filters:

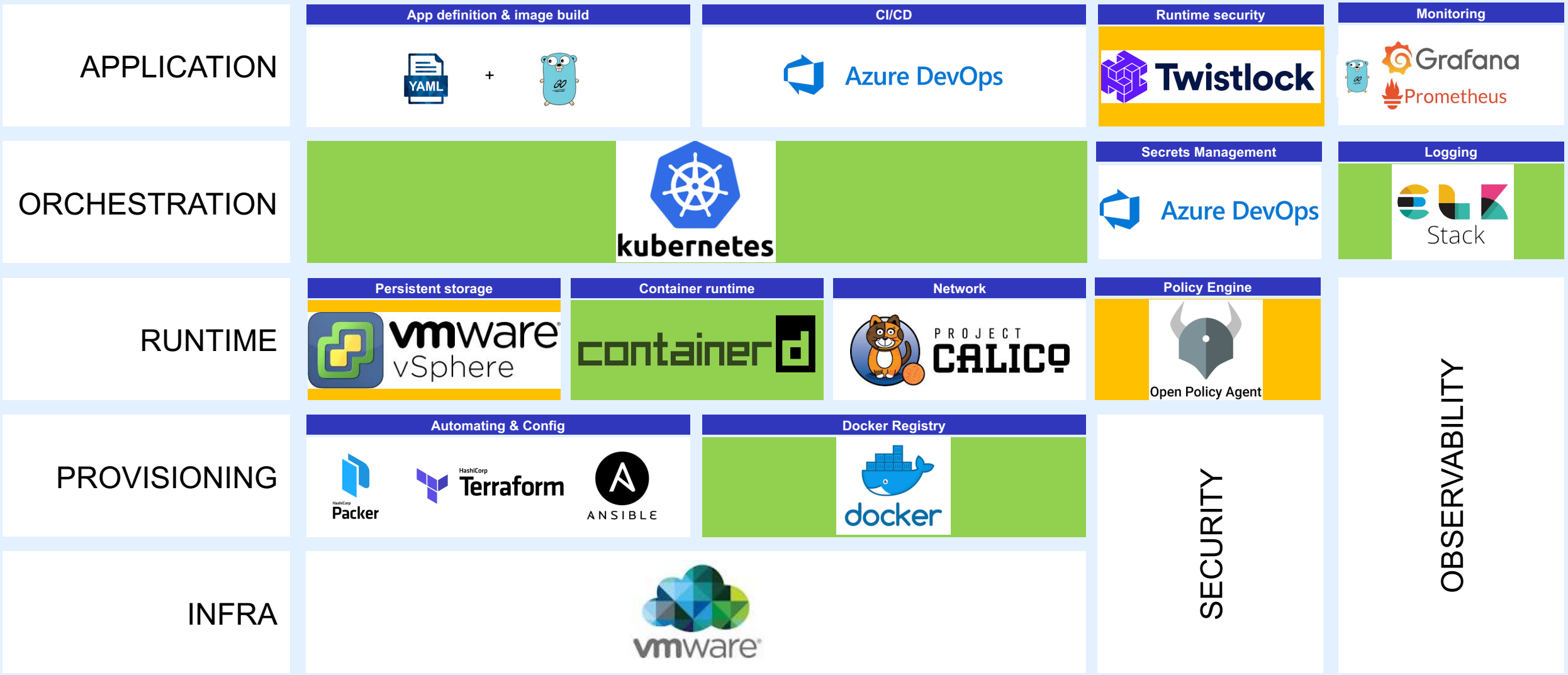
- Cards by age
- Open source landscape
- Member cards
- Cards by stars
- Cards from China
- Certified K8s/KCSP/KTP
- Cards by MCap/Funding

Download as CSV

Landscape | Card Mode | Serverless | Members

80%





To be determined or implemented

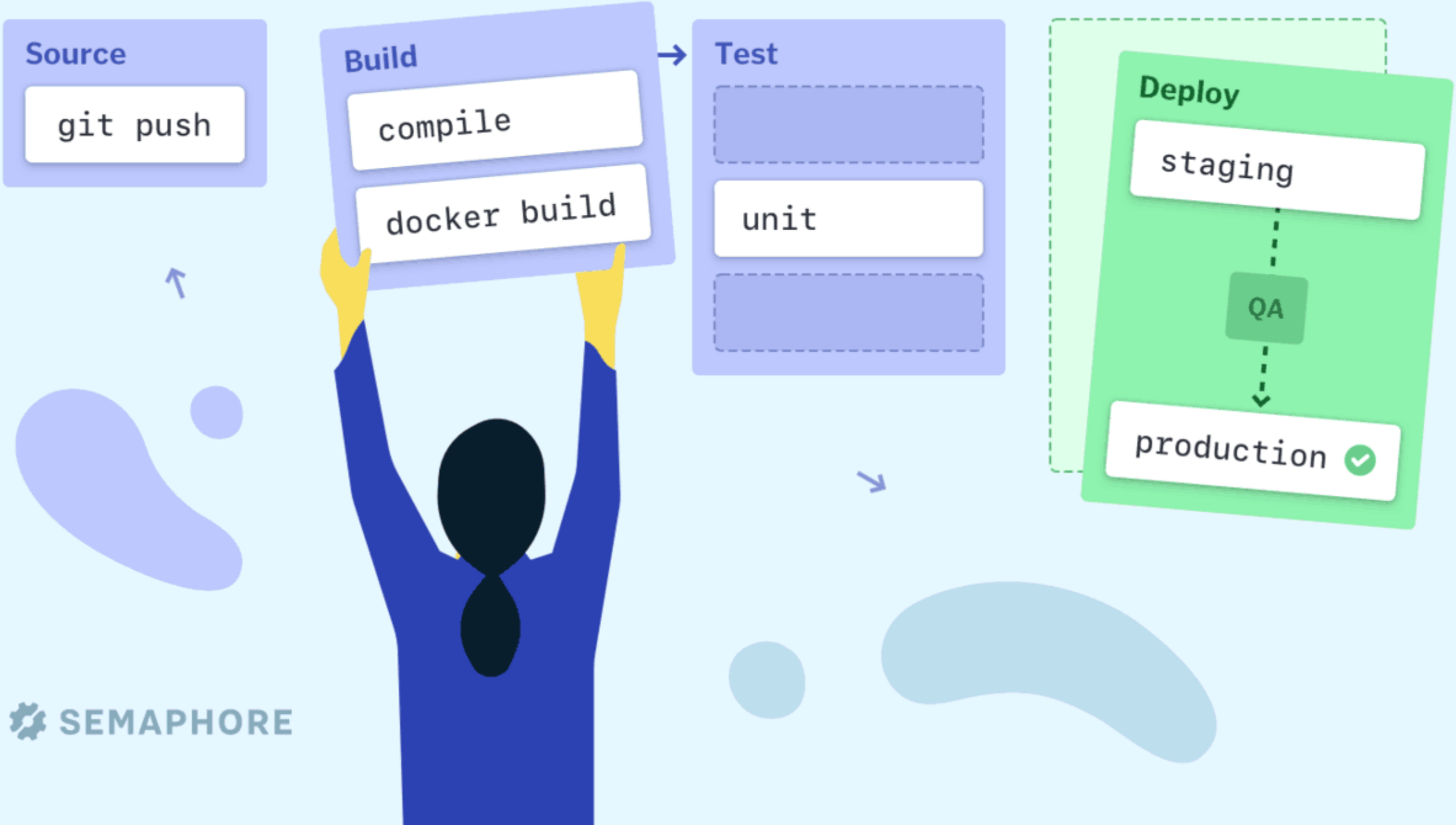
System

The Vision (Aug 2018)

- **The Platform (team?) will solve it all!**
  - Based on Kubernetes
  - Support for Devs & Ops
  - The money-making machine goes last

But… WHY?

A trip to PRODUCTION


Source
git push
Build
compile
docker build
Test
unit
Deploy
staging
QA
production
SEMAPHORE

1) Developer merges PR to repo (git)
2) CI triggers
   I. docker build –t …
   II. docker push …
3) Approvals?
4) CD triggers → 🚀 Production

REAL
COMMERCIAL

A. Developer updates branch (TFVC)
   1) No review
   2) No CI
B. A package is prepared (3+ days)
   1) Write deployment instructions (Excel)
   2) Tune Deploy.ps1 to needs
C. Developer creates CR#1
   1) 1+ weeks later, CR#1 is denied
   2) That's not the procedure!
   3) You are asking for a new machine.
D. CR#2 asks for new machine M#1 (3+ weeks)
   1) Change Request CR#2 goes to CAB
   2) CAB ignores change for too long
   3) CR#2 is applied!
E. M#1 is provisioned in wrong VLAN
F. Wait until next deployment window
G. CR#3 is applied in M#1
   1) Nothing works
   2) No one knows why
   3) Oh wait, it's in the wrong VLAN!
   4) Ask for another machine in proper VLAN!
H. CR#4 asks for M#2 (in another VLAN)
   1) Devs don't know which is proper VLAN
   2) Escalation
I. M#1 is granted a waiver
J. It works!
   1) This time **it only took 3 months**!

tech problems don't exist.
people problems exist.

@gapingvoid

Lessons Learnt & Mistakes

Auditors & Kubernetes

kube-bench

CIS benchmark v1.5.0 report for Kubernetes v1.17 PCI

Last 6 hours | 1m

Section 1.1: master node configuration files

CIS 1.1.1	CIS 1.1.2	CIS 1.1.3	CIS 1.1.4	CIS 1.1.5	CIS 1.1.6	CIS 1.1.7	CIS 1.1.8	CIS 1.1.9	CIS 1.1.10	CIS 1.1.10	CIS 1.1.12
FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL

CIS 1.1.13	CIS 1.1.14	CIS 1.1.15	CIS 1.1.16	CIS 1.1.17	CIS 1.1.18	CIS 1.1.19	CIS 1.1.20	CIS 1.1.21
FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS	PASS	PASS

Section 1.2: API server

CIS 1.2.1	CIS 1.2.2	CIS 1.2.3	CIS 1.2.4	CIS 1.2.5	CIS 1.2.6	CIS 1.2.7	CIS 1.2.8	CIS 1.2.9	CIS 1.2.10	CIS 1.2.11	CIS 1.2.12
FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	PASS	FAIL	PASS	PASS

CIS 1.2.13	CIS 1.2.14	CIS 1.2.15	CIS 1.2.16	CIS 1.2.17	CIS 1.2.18	CIS 1.2.19	CIS 1.2.20	CIS 1.2.21	CIS 1.2.22	CIS 1.2.23	CIS 1.2.24
FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS

CIS 1.2.25	CIS 1.2.26	CIS 1.2.27	CIS 1.2.28	CIS 1.2.29	CIS 1.2.30	CIS 1.2.31	CIS 1.2.32	CIS 1.2.33	CIS 1.2.34	CIS 1.2.35
PASS	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL

Section 1.3: controller manager

CIS 1.3.1	CIS 1.3.2	CIS 1.3.3	CIS 1.3.4	CIS 1.3.5	CIS 1.3.6	CIS 1.3.7
PASS	PASS	PASS	PASS	PASS	FAIL	PASS

CIS benchmark v1.5.0 report for Kubernetes v1.17 PCI (II)

Last 6 hours | 1m

Section 1.4: scheduler

CIS 1.4.1	CIS 1.4.2
PASS	FAIL

Section 2.1: etcd

CIS 2.1	CIS 2.2	CIS 2.3	CIS 2.4	CIS 2.5	CIS 2.6	CIS 2.7
FAIL	FAIL	PASS	FAIL	FAIL	PASS	FAIL

Section 3: control plane configuration

CIS 3.1	CIS 3.2.1	CIS 3.2.2
PASS	PASS	PASS

Section 4.1: worker node configuration files

CIS 4.1.1	CIS 4.1.2	CIS 4.1.3	CIS 4.1.4	CIS 4.1.5	CIS 4.1.6	CIS 4.1.7	CIS 4.1.8	CIS 4.1.9	CIS 4.1.10
FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL

Section 4.2: kubelet

CIS 4.2.1	CIS 4.2.2	CIS 4.2.3	CIS 4.2.4	CIS 4.2.5	CIS 4.2.6	CIS 4.2.7	CIS 4.2.8	CIS 4.2.9	CIS 4.2.10	CIS 4.2.11	CIS 4.2.12
PASS	PASS	PASS	PASS	PASS	FAIL	PASS	FAIL	PASS	FAIL	PASS	FAIL

CIS 4.2.13
FAIL

Operative System

Red Hat: free or paid?

Registry

atlas-applications

Search

Contents History

opsflow: PR#16211 Add CheckAvs option when Avs service is enabled b8a84653 Sergio López Mon at 3:35 PM	16211	succeeded
fraudgateway: PR#16199 Improvements of performance on database 2199b947 Juan Carlos Perez San Jose Mon at 12:19 PM	16199	succeeded
opsflow: PR#16162 fix allow unkown props in crm details 5cdbfee9 Gabriel Lima Fri at 2:46 PM	16162	failed
telemetry-reporter: PR#16153 Monitor Merchant Boarding Tool certificates e6187a6d Javier Revillas Garcia Fri at 9:58 AM	16153	succeeded
merchant-boarding: PR#16033: Added new cronjob e8e2892a Javier Garmon Feb 27 at 2:52 PM	16033	succeeded
Merged PR 16128: Update pre application nl pdf 180b2229 Álvaro Rivero Bablé Feb 27 at 2:05 PM	16128	failed
fraudgateway: PR#16125 Unify event processed logs 468ed053 Juan Carlos Perez San Jose Feb 27 at 12:45 PM	16125	succeeded
opsflow: PR#16122 fix checkout avs vars 28603bbc Gabriel Lima Feb 27 at 12:06 PM	16122	failed
fraudgateway: PR# 16116 Include AricOutput when appropiate 4929aaeb Juan Carlos Perez San Jose Feb 27 at 11:05 AM	16116	succeeded
chore: deploy web and gw to production 791e91c8 Manuel Navarro Pérez Feb 27 at 10:36 AM	16113	succeeded
opsflow: PR#16114 restore CheckAVS casing f1e01984 Sergio Amador Rodriguez Feb 27 at 10:34 AM	16114	succeeded
opsflow: PR#16107 fix card engine api url a6662900 Sergio López Feb 26 at 5:12 PM	16107	failed
Merged PR 16102: opsflow: PR#16102 add cardengine envs 2a09c788 Sergio López Feb 26 at 4:38 PM	16102	failed
opsflow: PR#15977 Create Opsflow.CardEngine.API 5ce3f47c Sergio López Feb 26 at 3:42 PM	15977	failed
telemetry-reporter: PR#16058 Fix URL in ConfigMap 7d9a6f8c Javier Revillas Garcia Feb 26 at 11:05 AM	16058	succeeded
telemetry-reporter: PR#15887 Watch Telemetry Reporter SSL certificate fd34d843 Javier Revillas Garcia Feb 26 at 8:02 AM	15887	succeeded
opsflow: PR#16002 update masker for tokens f2cc63e1 Sergio Amador Rodriguez Feb 25 at 10:58 AM	16002	succeeded
feat: mask logger for sme project 570ba8e6 Antonio Jesús Carmona Villegas Feb 24 at 3:19 PM	15975	failed
opsflow: setup signature key for aceprotect merchants	15919	succeeded

Support Devs & Ops

- Training about specific tech
- “Beyond Duty”

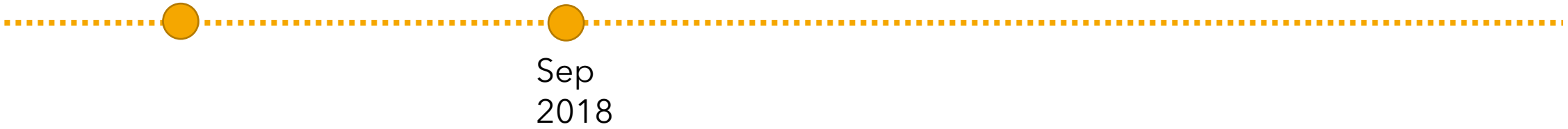
kops

- Why? We are just starting
- Where? AWS
- Pros/Cons
  - It works nicely out of the box
  - **Soooooo Outdated**
  - CIS Benchmark / Too many resources

Aug
2018

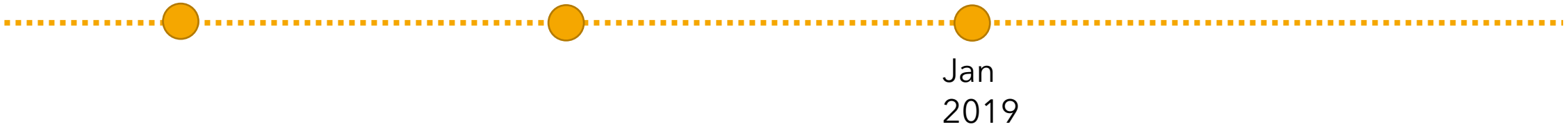
kubespray

- Bloated
- Too generic
- **kubeadm** to the rescue!



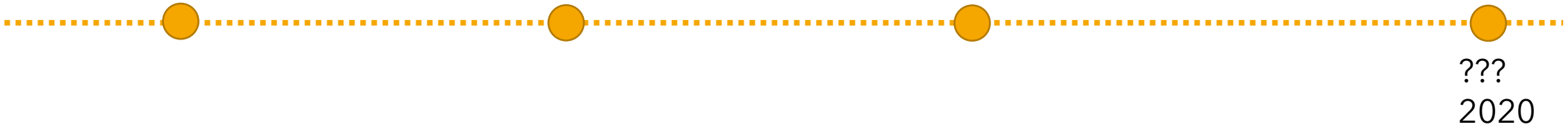
kubeadm

- In production, now



ClusterAPI?

- vSphere PoC
- Not there yet, for us



Private Registry

- We’ve tried:
  - Docker Trusted Registry
  - Harbor
- Both have authentication issues

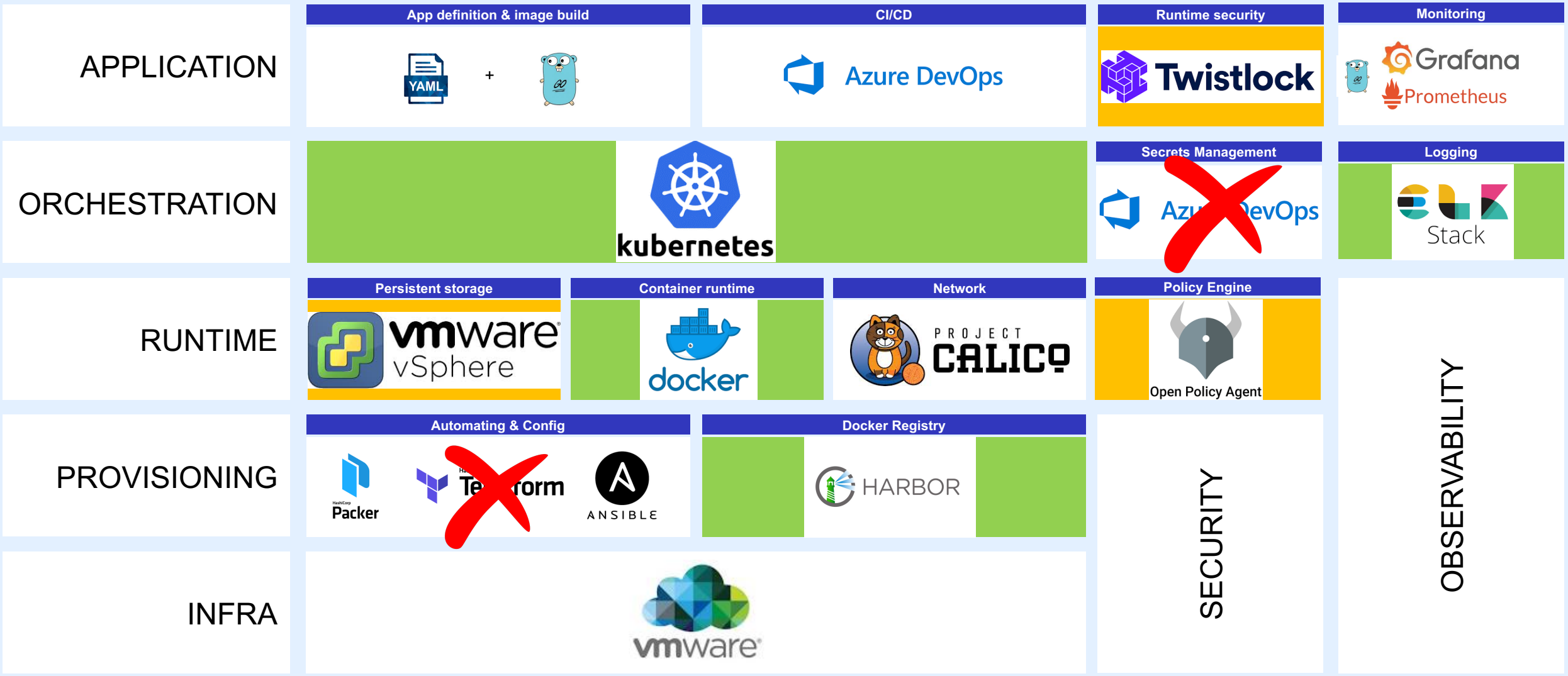
CNI

- DNS-aware network policies!
- Perfect for our use case!

- **Requires unsupported kernel version by RedHat**
  - RHEL 7 = 3.10 (vs 4.9.17)

cilium

And many many more…



To be determined or implemented

System

2018

- Jun: “GitOps”
- Aug:
  - Kubernetes AWS
  - 1 team
- Sep: Kubernetes ON-PREM

2019

- 7 teams, 10+ apps
- Bumpy road
- Beyond Duty
- Monitor all the things!

2020

- January: DTR -> Harbor

tech problems don't exist.
people problems exist.

@gapingvoid

That's all Folks!

Thanks!

@toqueteos

- GitHub
- GitLab
- Twitter