Red Hat

So you want to use K8s at work...

Ryan Kraus

Cloud Specialist Solutions Architect

rkraus@redhat.com

https://www.linkedin.com/in/rmkraus/

Agenda

- Build the platform
- Harden the platform
- Patch the platform
- Operate the platform
- Get promoted
- There’s got to be a better way

Build the platform

Red Hat

Rip off the bandaid

Kubernetes is not PaaS.

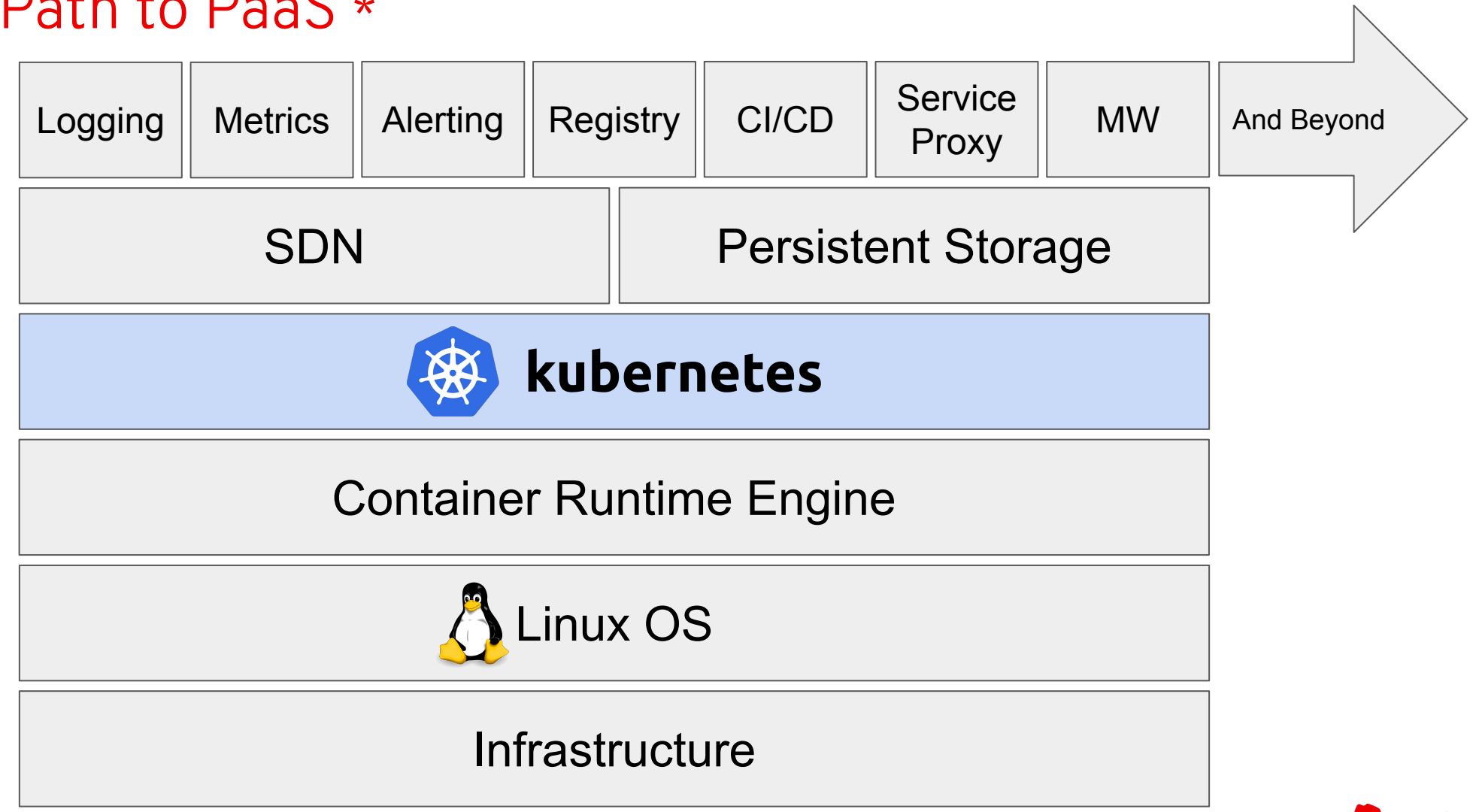
Source:

https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/#what-kubernetes-is-not

https://twitter.com/kelseyhightower/status/935252923721793536?lang=en

Red Hat

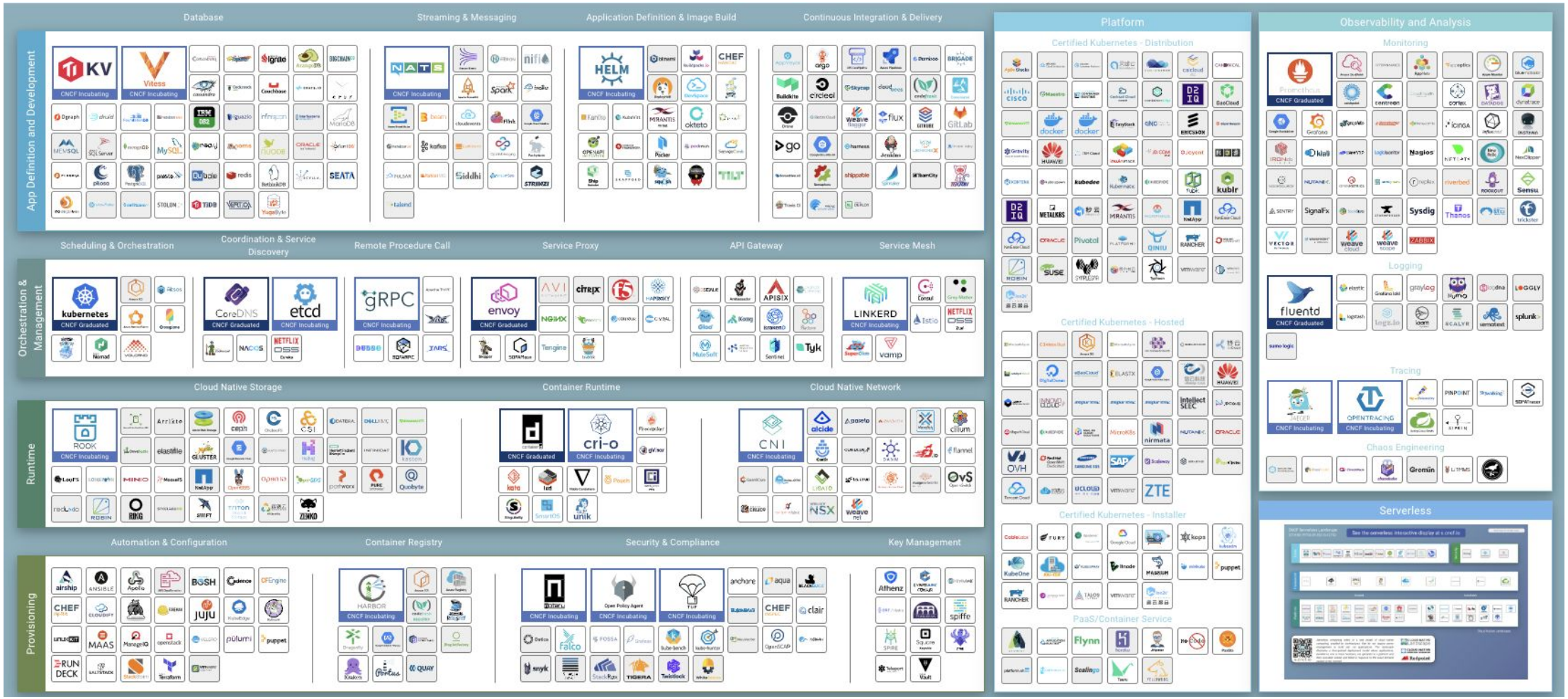
Path to PaaS *



* Not Inclusive. Not even close.

Red Hat

You have some options



Source:

https://landscape.cncf.io/

Red Hat

And you can't work in a vacuum

Task: Pick a container runti

Considerations:

- Which version is c
- Is that version als
- Which storage dri n of my engine, that version of my
- Which versions a my chosen SDN?
- Are all of th

This is a journey

- CNCF - Cloud Native Trail Map

  https://raw.githubusercontent.com/cncf/trailmap/master/CNCF_TrailMap_latest.pdf

- Minimum viable product

- Industry Tested > New and Shiny

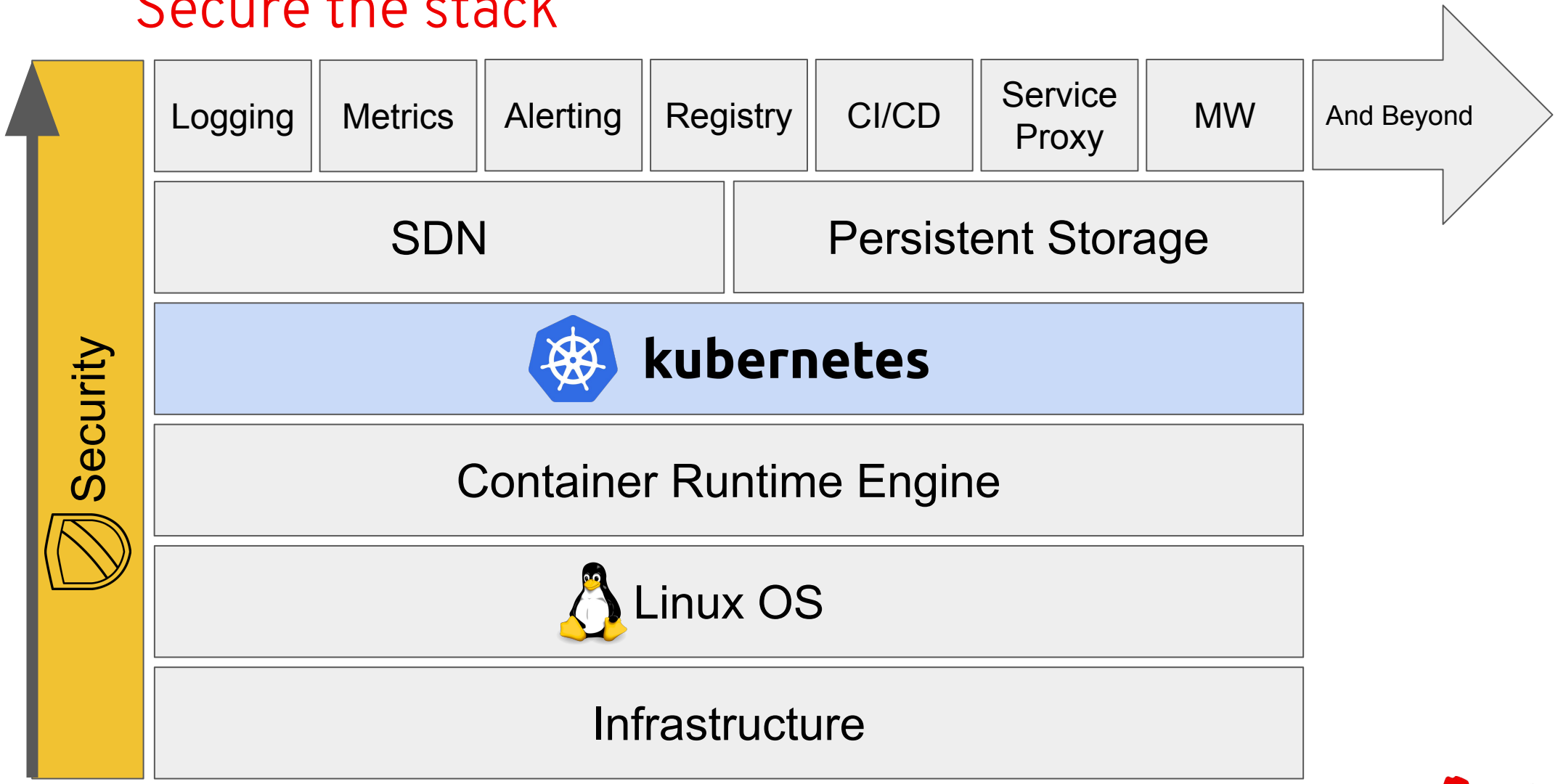
- Buy, don’t build

Harden the platform

Kubernetes is not secure

Red Hat

Secure the stack



Security resources *

- ## Infrastructure hardening

  VPC Design, IAM Roles, Data Security, Boundary Protection, Encryption Management

  AWS Best Practices | Azure Best Practices | GCP Best Practices | CIS Benchmarks

- ## Operating system hardening

  Patching Procedures, Exposed Services, Access Control, Auditing Control, General Configuration

  CIS Benchmarks

- ## Container runtime engine hardening

  Auditing/Logging, Configuration, Trusted Repos Configured. SELinux/AppArmor, Networking

  CIS Benchmarks

Red Hat

* Not Inclusive. Not even close.

Security resources *

- Kubernetes

  Default security policies, Encrypted cluster traffic, Secret names in logs, SECCOMP, RBAC, Component configuration

  CNCF Audit | kube-hunter | CIS Benchmarks

- Software defined network security

  Twistlock | Tigera | et al.

- … and friends
  - Helm Best Practices
  - Persistent Volumes
  - Jenkins Best Practices
  - Container Image Registry
  - Elasticsearch Security (GOTO 10)

Red Hat

* Not Inclusive. Not even close.

This is a journey

- This is hard: Don't be Tesla, WeightWatchers, or Monzo Bank
- Use all available resources and threat model
- Minimum viable product
- Industry Tested > New and Shiny
- Buy, don't build

Patch the platform

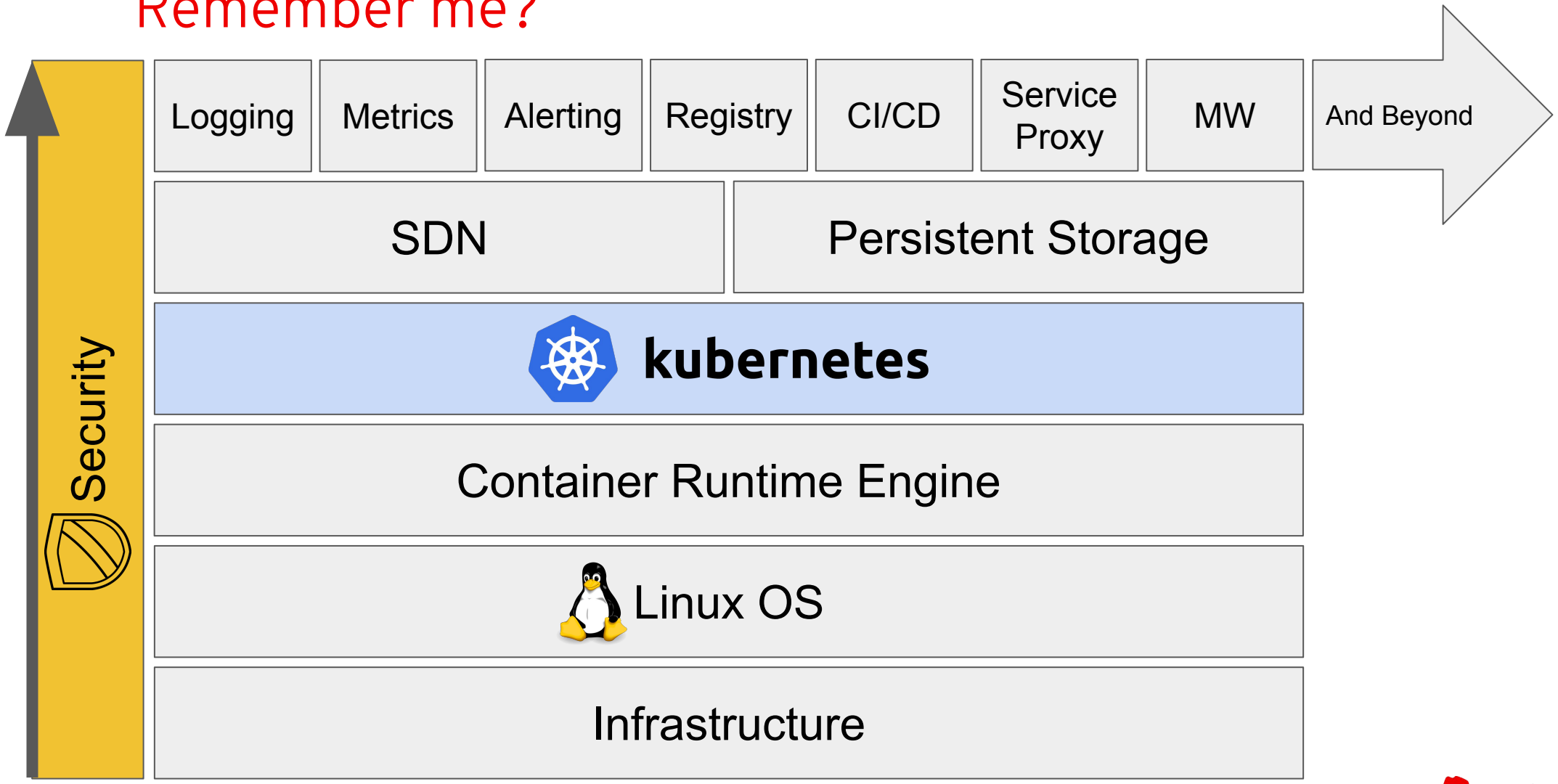
Kubernetes releases every 90 days

And you have to keep up.

Not all fixes are backported.

Only incremental upgrades are supported.

Remember me?



Patch all the things

- Repeat full stack compatibility exercise.
- Bring everything as up-to-date as possible.
- Remember Kubernetes API changes!

But wait... I use a managed service...

I'mma let you finish, but...

- Upgrading Amazon EKS Cluster
- Upgrading Azure Kubernetes Service
- Upgrading Google Compute Engine Clusters
- Upgrading Google Kubernetes Engine

Everybody else

- Upgrade cluster with kops
- Upgrading cluster with Kubespray
- However you deployed is how you will upgrade
- Manage downtime expectations

Patch the OS

```
# tell K8s you're begining node maintenance
kubectl get nodes  # list all available nodes
kubectl drain node-5.example.com  # empty the node, make unschedulable

# update the operating system
yum update -y  # or apt-get, dnf, etc
reboot

# once the node comes back up
kubectl get nodes  # verify node is reachable
kubectl uncordon node-5.example.com  # allow node to be scheduled
```

This is a journey

- Patch, patch, patch
- You will have out-of-sequence patches
- Minimum viable product
- Industry Tested > New and Shiny
- Buy, don’t build

Operate the platform

Red Hat

Now we can get started with Day 2

- Monitor cluster health statistics - There's an operator for that.

- Develop app onboarding policies - Some Red Hat docs

  Quota Management, Network Policy Management, SCC Management

- Keep IaaS costs in check - Autoscale cluster nodes

- Keep an eye on new trends and tools:
  - Serverless Landscape
  - Kubernetes Virtualization - KubeVirt
  - Service Meshes - Istio

Get promoted

Red Hat

I'll just leave this here…

Source:
https://enterprisersproject.com/article/2019/5/kubernetes-jobs-11-salary-statistics

There’s got to be a better way

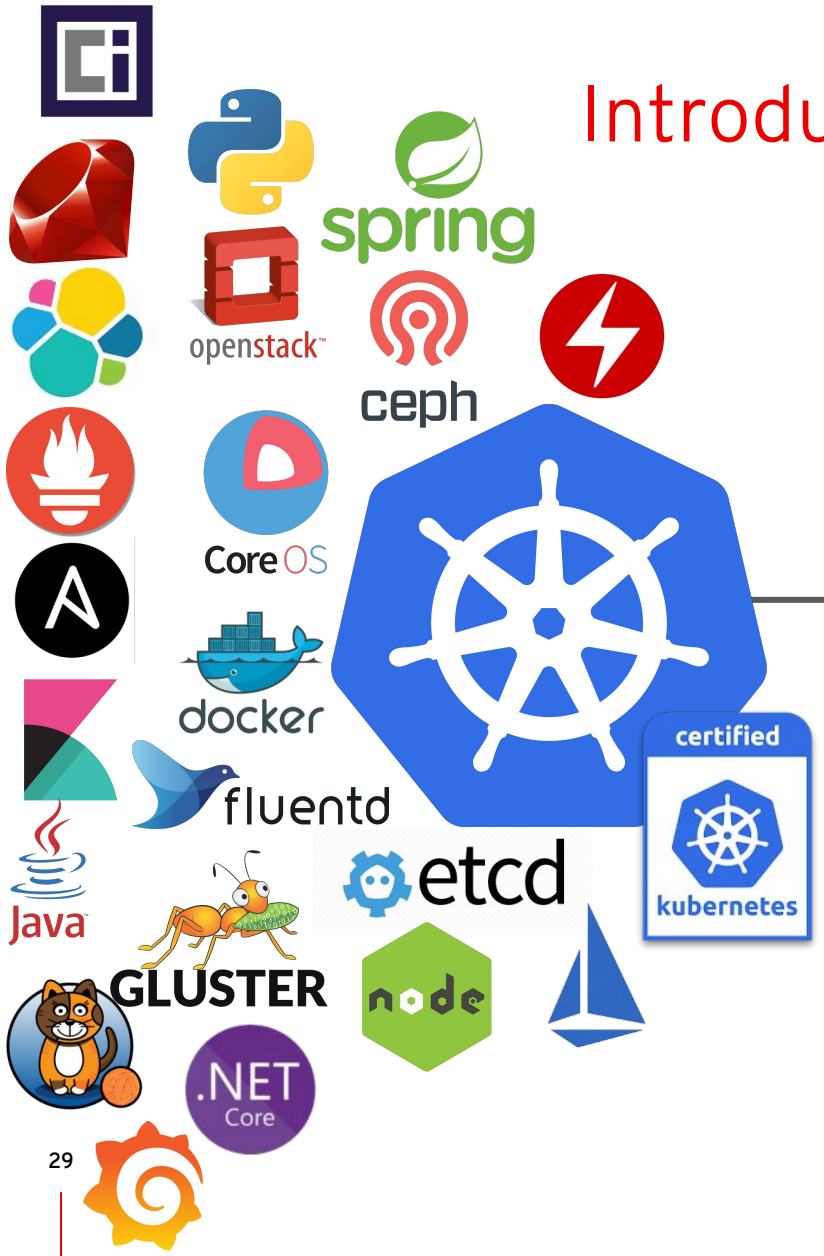
Red Hat

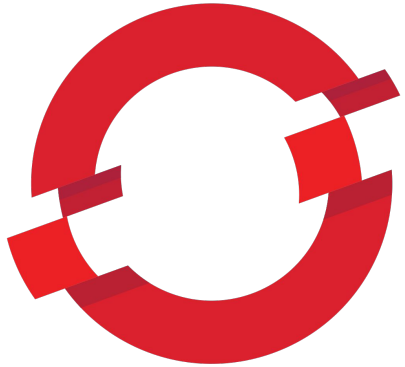
I just want to make some apps

Source:
https://enterprisersproject.com/article/2019/5/kubernetes-jobs-11-salary-statistics

Red Hat

Introducing the Kubernetes Distribution





OPENSHIFT

Enterprise product from multiple projects
Kubernetes is the core
Full PaaS for enterprise innovation
Secured, Supported, Trusted
Full stack of supported middleware and runtimes

Opinionated distributions

Source:
https://enterprisersproject.com/article/2019/5/kubernetes-jobs-11-salary-statistics

Unbiased information

- InfoWorld: 10 Kubernetes distributions leading the container revolution
- CNCF: Certified Kubernetes Distributions

Kelsey Hightower
@kelseyhightower

Follow

Kubernetes is for people building platforms. If you are a developer building your own platform (AppEngine, Cloud Foundry, or Heroku clone), then Kubernetes is for you.

Red Hat

THANK YOU