



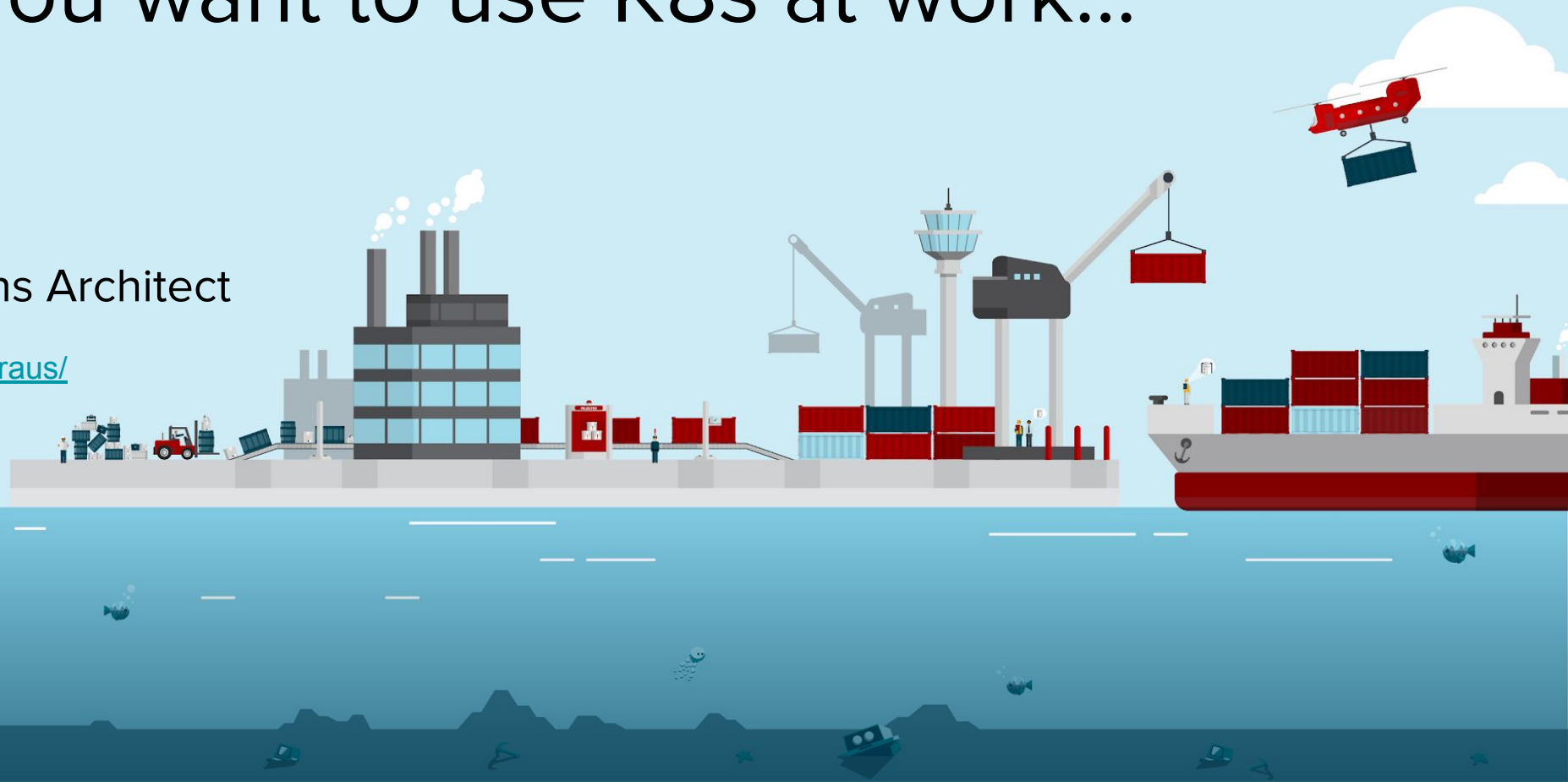
So you want to use K8s at work...

Ryan Kraus

Cloud Specialist Solutions Architect

✉ rkraus@redhat.com

in <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

Rip off the bandaid

Kubernetes is not PaaS.

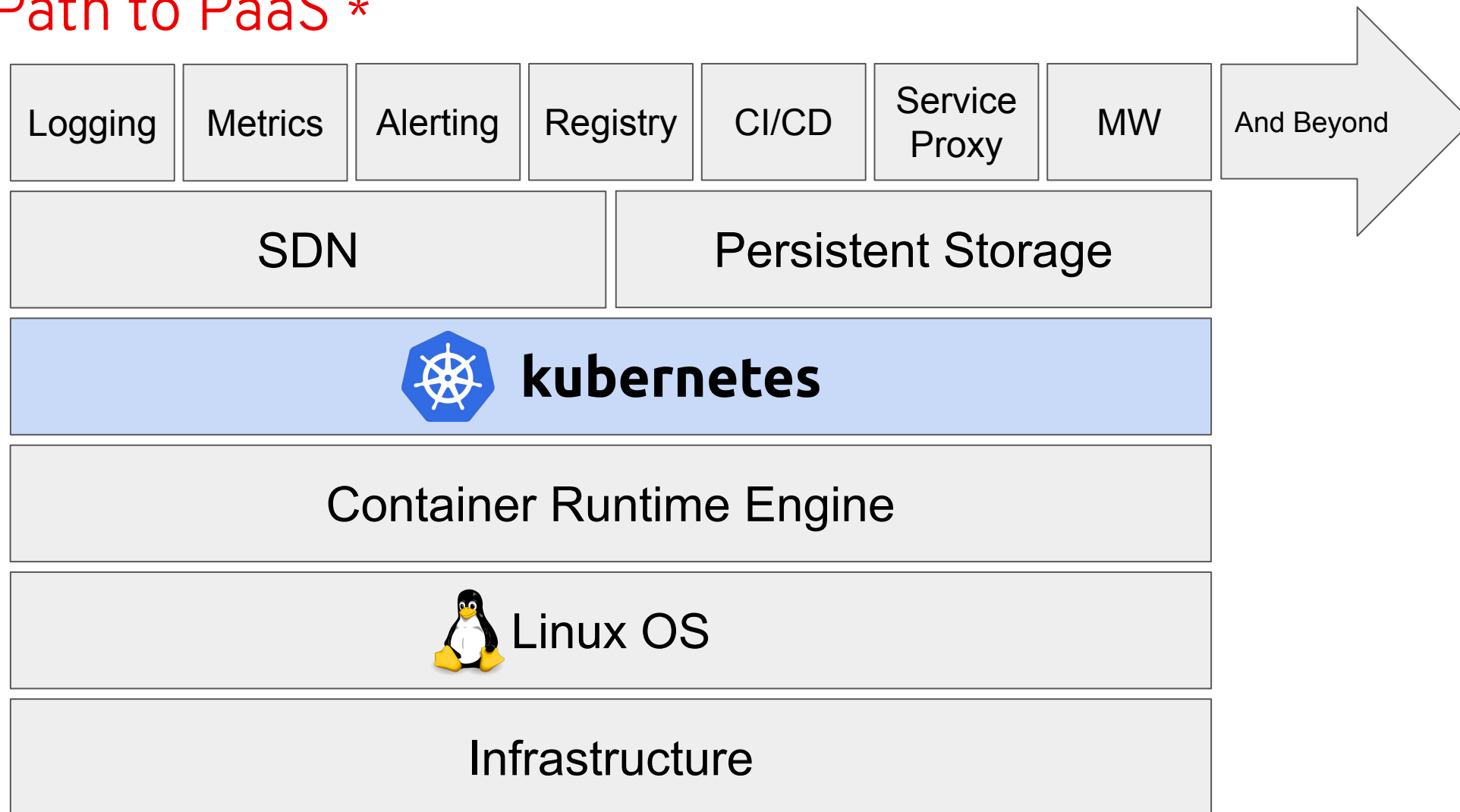


4 Source:

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

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

Path to PaaS *



You have some options

The image displays a detailed grid of logos for various CNCF projects, organized into several functional categories:

- App Definition and Development:** Includes Database (e.g., KV, V, CockroachDB), Streaming & Messaging (e.g., NATS, Spark), Application Definition & Image Build (e.g., HELM, Jenkins), and Continuous Integration & Delivery (e.g., Jenkins, GitLab).
- Orchestration & Management:** Includes Scheduling & Orchestration (e.g., Kubernetes), Coordination & Service Discovery (e.g., CoreDNS, etcd), Remote Procedure Call (e.g., gRPC), Service Proxy (e.g., Envoy), API Gateway (e.g., Kong), and Service Mesh (e.g., Istio, Linkerd).
- Runtime:** Includes Cloud Native Storage (e.g., Rook, Ceph), Container Runtime (e.g., cri-o, containerd), and Cloud Native Network (e.g., Cilium, Calico).
- Provisioning:** Includes Automation & Configuration (e.g., Ansible, Terraform), Container Registry (e.g., Harbor), Security & Compliance (e.g., Falco), and Key Management (e.g., Vault).
- Platform:** Divided into Certified Kubernetes - Distribution (e.g., OpenShift, Rancher) and Certified Kubernetes - Hosted (e.g., EKS, AKS).
- Observability and Analysis:** Includes Monitoring (e.g., Prometheus, Grafana), Logging (e.g., Fluentd, ELK), Tracing (e.g., Jaeger, Zipkin), and Chaos Engineering (e.g., Chaos Mesh).
- Serverless:** A dedicated section for serverless computing solutions.

And you can't work in a vacuum

Task: Pick a container runtime you can run

Considerations:

- Which version is compatible with my engine?
- Is that version also compatible with my chosen SDN?
- Which storage driver is supported by that version of my engine?
- Which versions are compatible with my chosen SDN?
- Are all of the above considerations met?



This is a journey

- CNCF - Cloud Native Trail Map

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

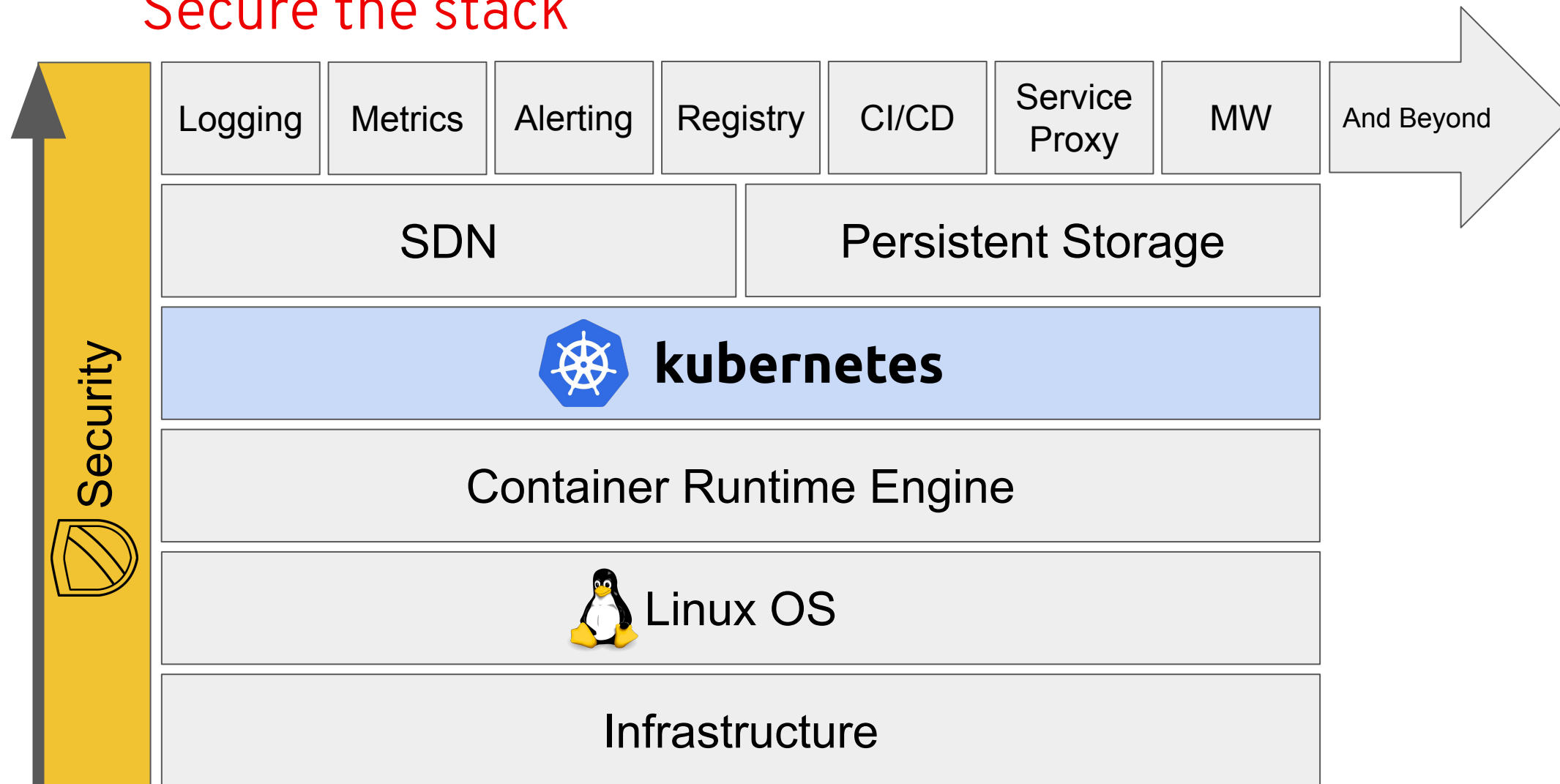
- Minimum viable product
- Industry Tested > New and Shiny
- Buy, don't build

Harden the platform

Kubernetes is not secure



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](#)

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)

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

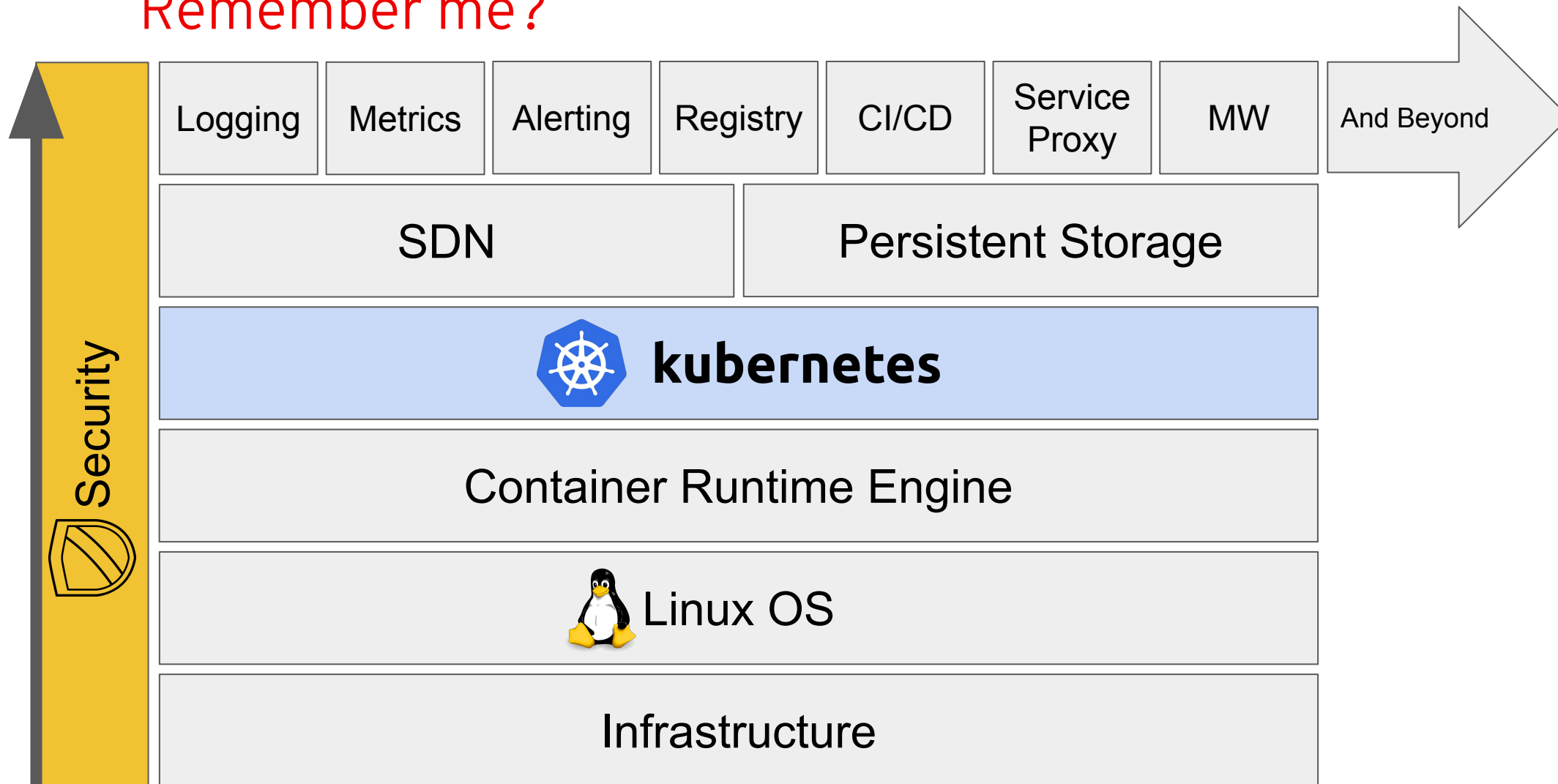
And you have to keep up.

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

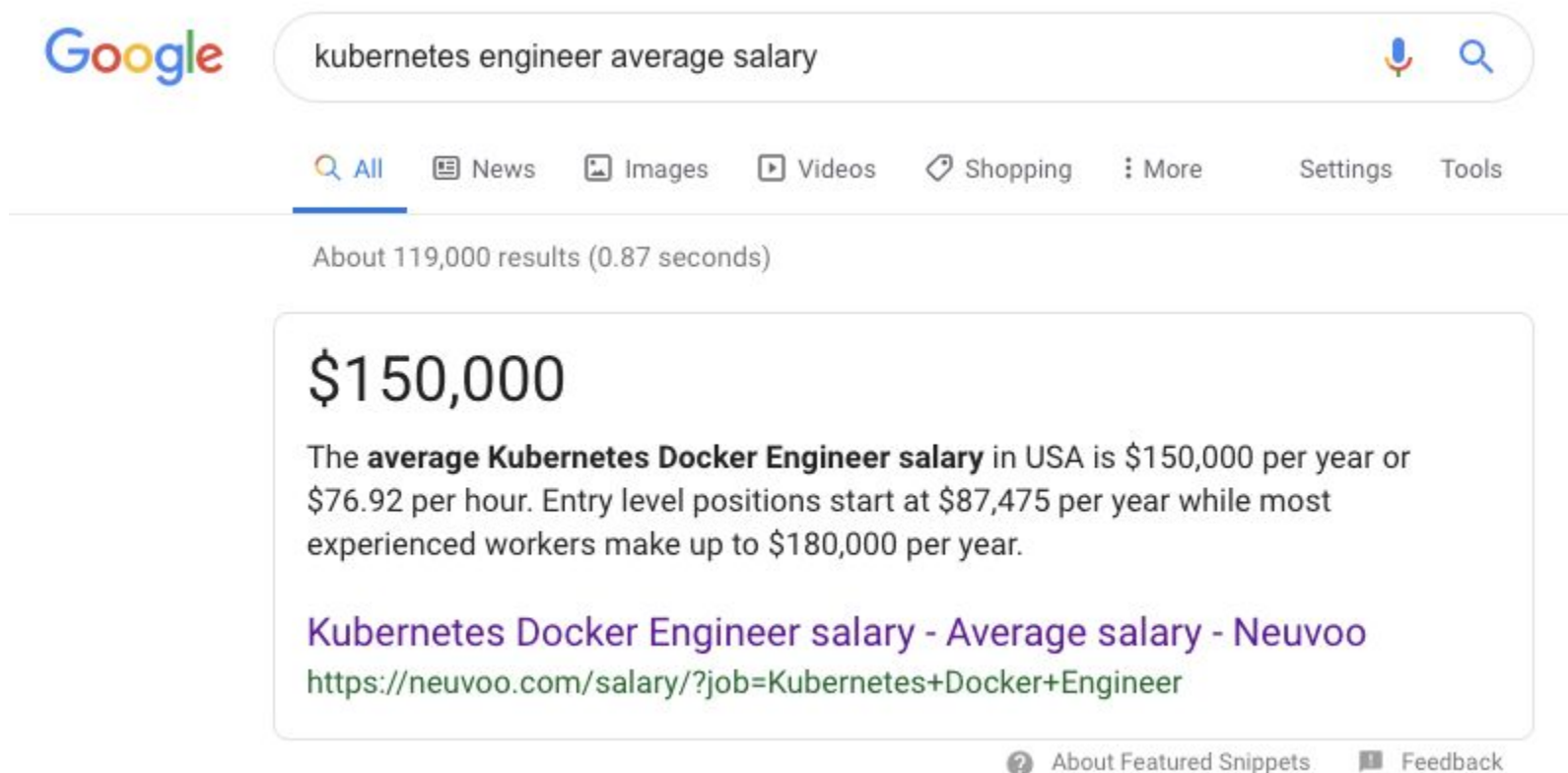
Operate the platform

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

I'll just leave this here...



A screenshot of a Google search interface. The search bar contains the text "kubernetes engineer average salary". Below the search bar, the results are displayed. The first result is a featured snippet showing a salary of \$150,000. The snippet text states: "The **average Kubernetes Docker Engineer salary** in USA is \$150,000 per year or \$76.92 per hour. Entry level positions start at \$87,475 per year while most experienced workers make up to \$180,000 per year." Below this, there is a link to "Kubernetes Docker Engineer salary - Average salary - Neuvo" with the URL "https://neuvo.com/salary/?job=Kubernetes+Docker+Engineer". At the bottom right of the snippet, there are links for "About Featured Snippets" and "Feedback".

Google

kubernetes engineer average salary

All News Images Videos Shopping More Settings Tools

About 119,000 results (0.87 seconds)

\$150,000

The **average Kubernetes Docker Engineer salary** in USA is \$150,000 per year or \$76.92 per hour. Entry level positions start at \$87,475 per year while most experienced workers make up to \$180,000 per year.

Kubernetes Docker Engineer salary - Average salary - Neuvo
<https://neuvo.com/salary/?job=Kubernetes+Docker+Engineer>

About Featured Snippets Feedback

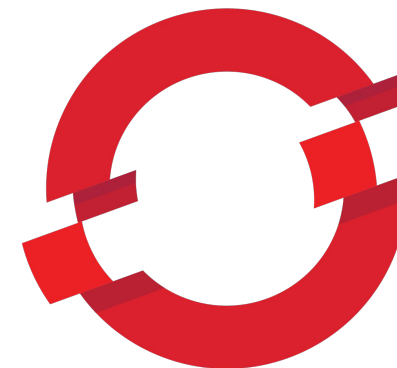
There's got to be a better way

I just want to make some apps



THERE'S GOT TO BE A BETTER WAY

Introducing the Kubernetes Distribution



OPENSIFT

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



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.



THANK YOU

