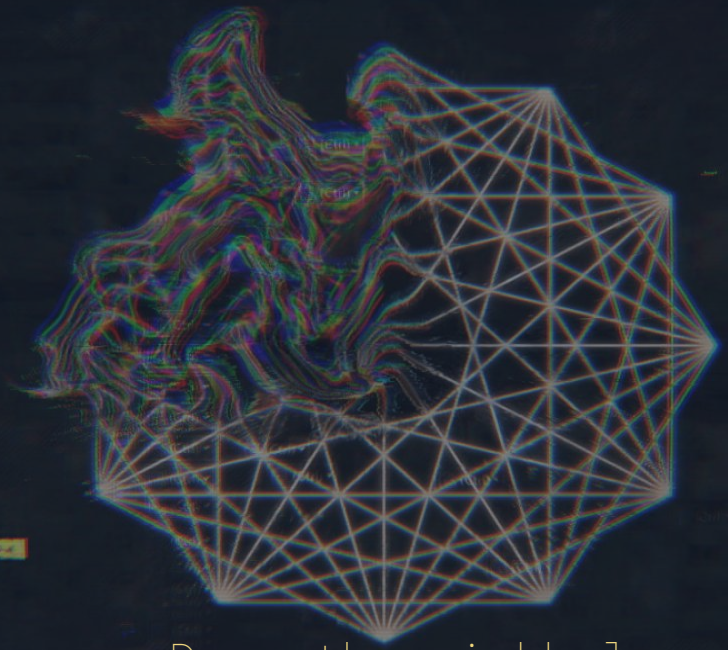


Down the sinkhole

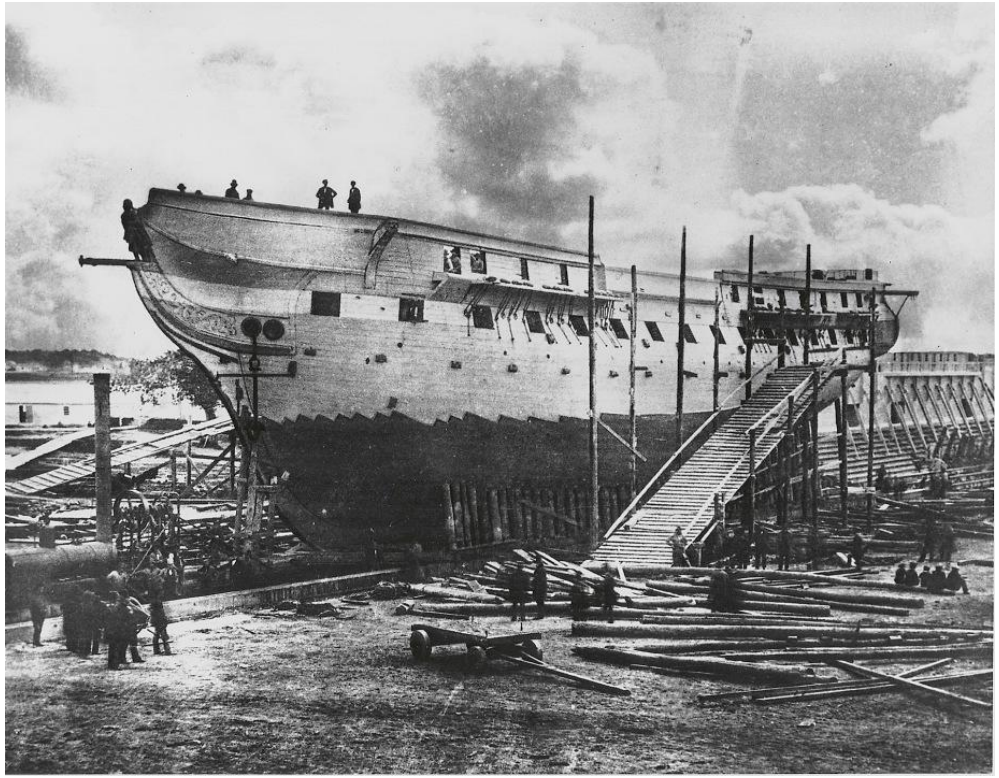
With Kubernetes

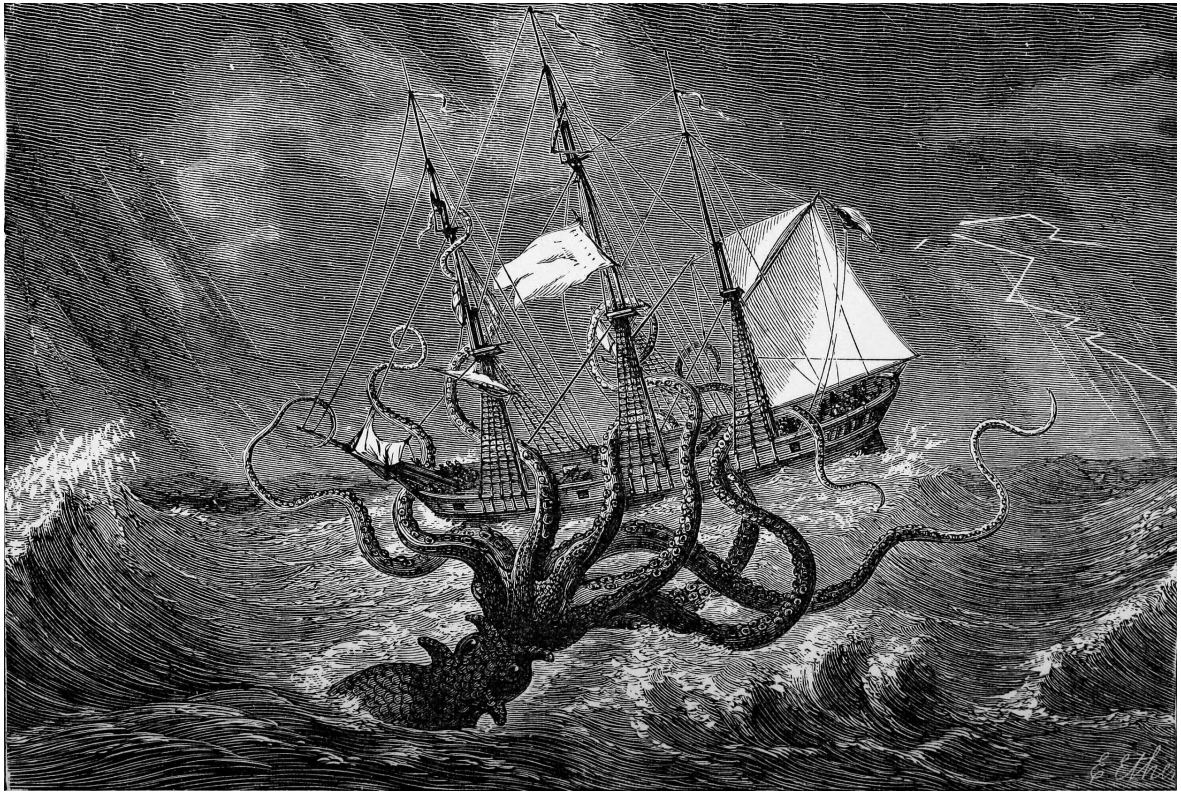
Kubernetes!

Me harty's guide fer all ye scallywags









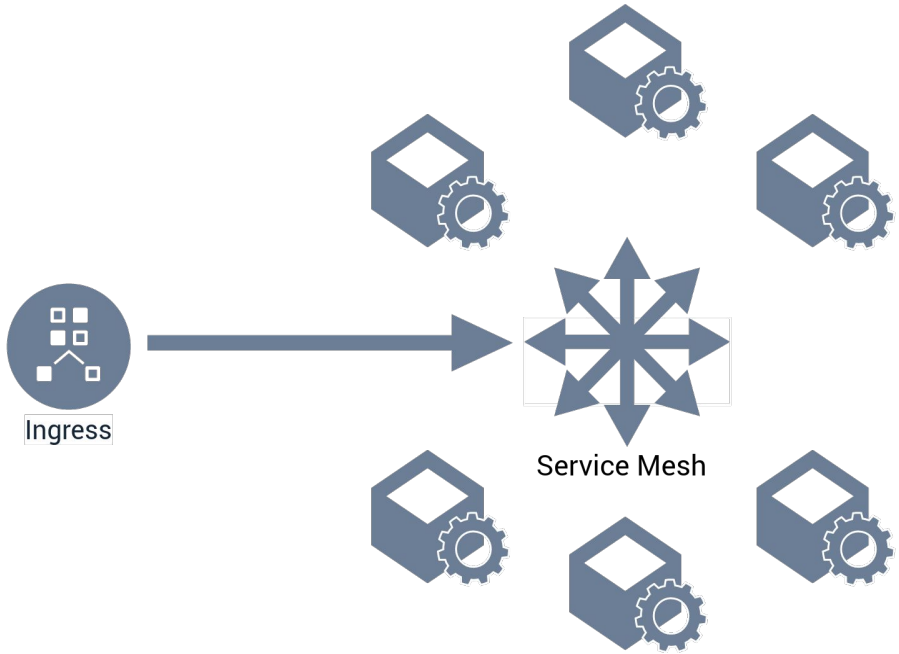


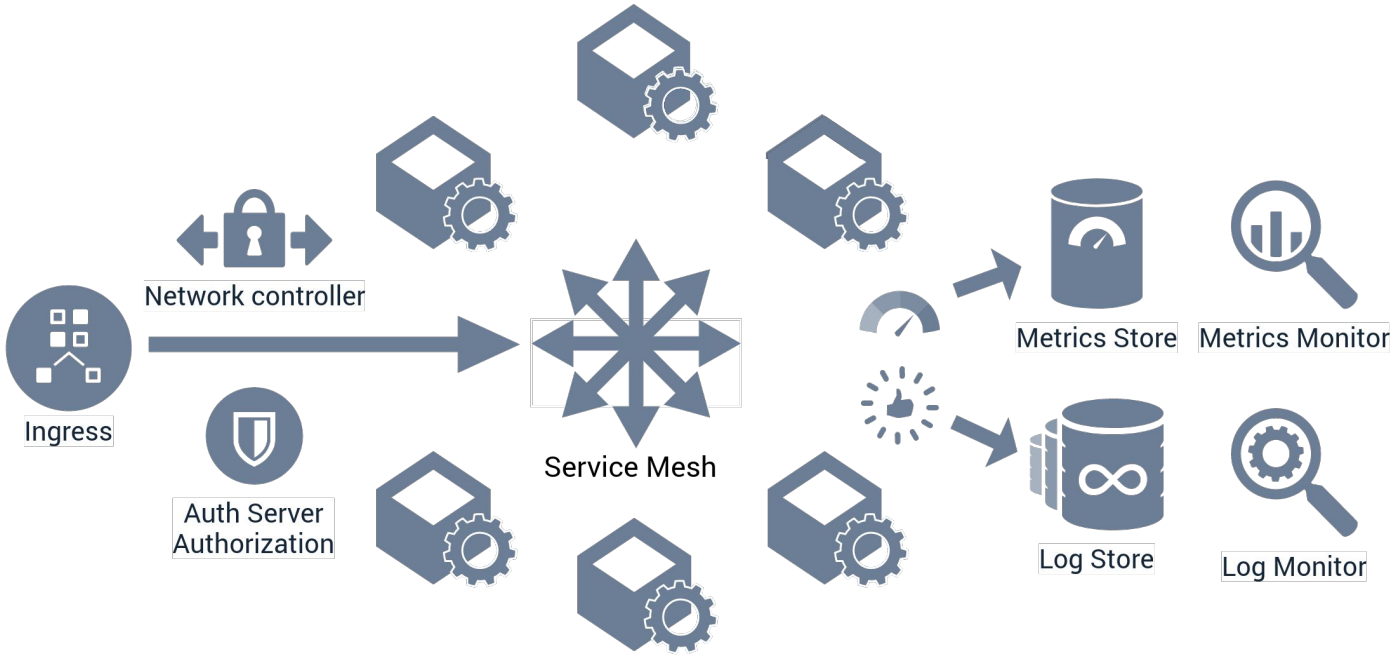
Ahoy!

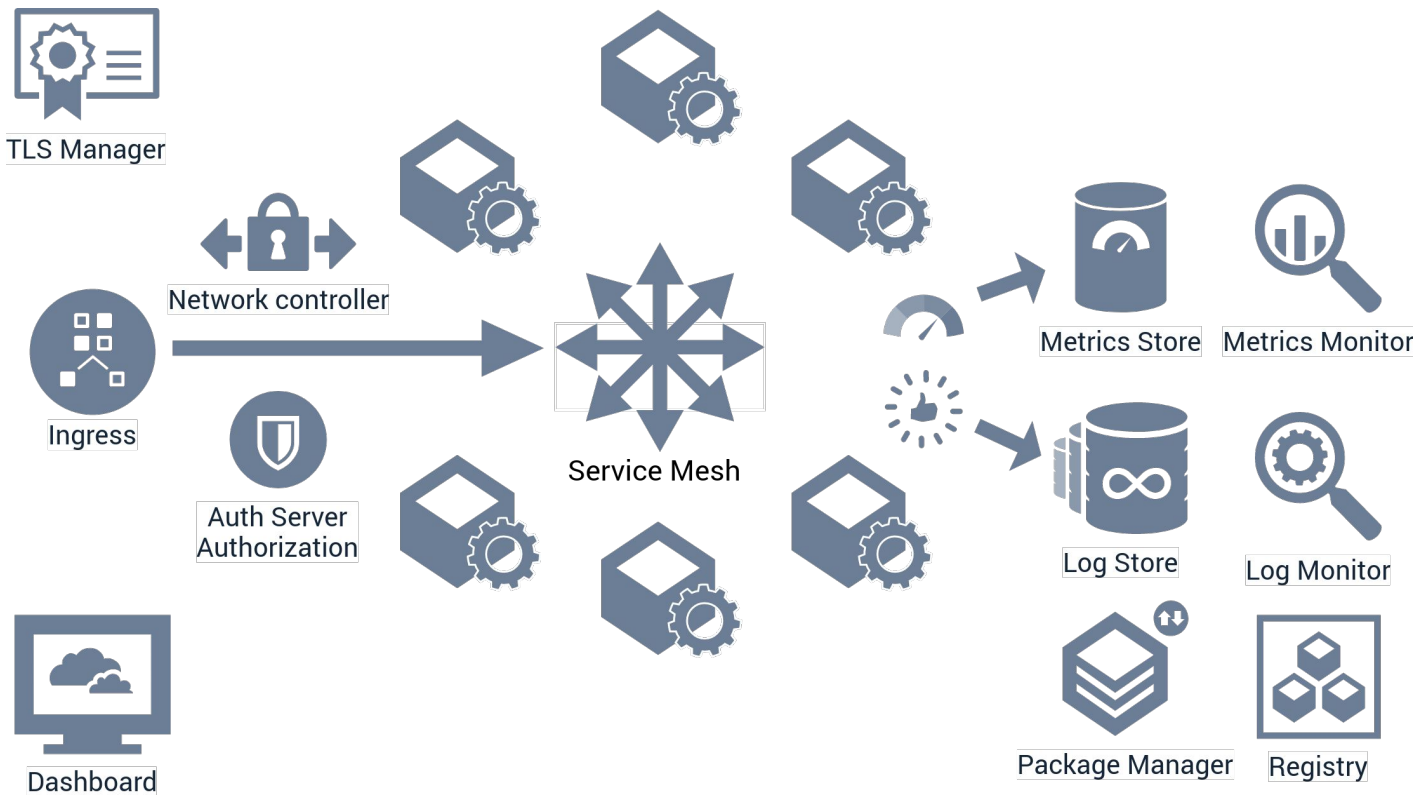
I am Alex Ivkin

I run solutions at Eclypsium

Portland, OR


Network controller
Ingress
Auth Server
Authorization
Service Mesh
Metrics Store
Metrics Monitor
Log Store
Log Monitor


TLS Manager
Network controller
Ingress
Auth Server
Authorization
Service Mesh
Metrics Store
Metrics Monitor
Log Store
Log Monitor
Package Manager
Registry
Dashboard

Ingress - **Istio**, ingress-nginx

Package manager - **Helm/Tiller**, Kustomize

Service meshes - Linkerd, **Envoy**

Data collectors - Fluentd, Loki

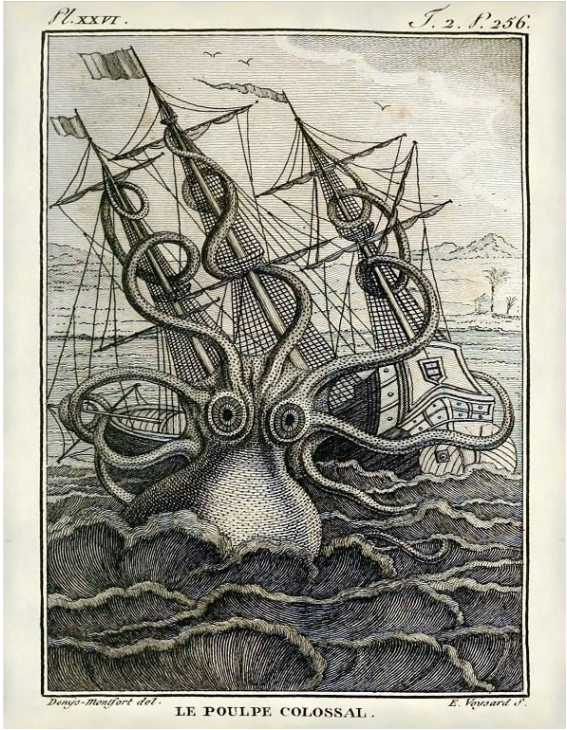
Metrics collectors - **Promethius**, Grafana

Network controller - Flannel, Falco, **Calico**

TLS manager - **Cert-manager**, Istio SDS

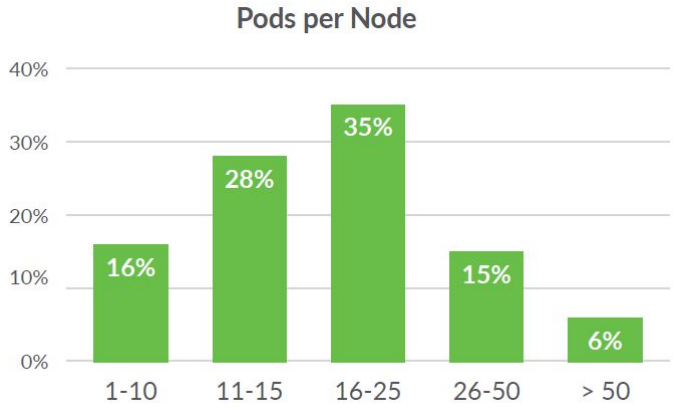
Image store - Docker **registry**, Notary

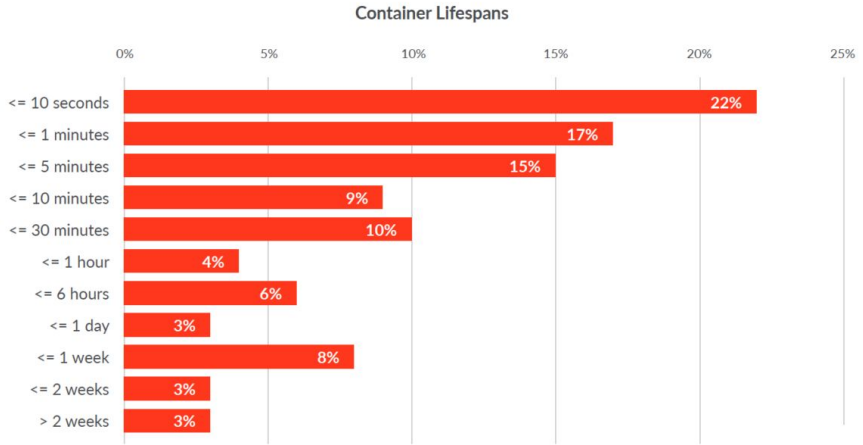
Auth/Azn - Hydra, OPA, **SPIRE**, RBAC-mgr



https://sysdig.com/blog/sysdig-2019-container-usage-report/

Increased surface, decreased lifespan





@alexivkinx

Load Balancer

Control Plane

API Server

etcd

Scheduler

Controller Manager

DNS Management

Nodes

kubelet

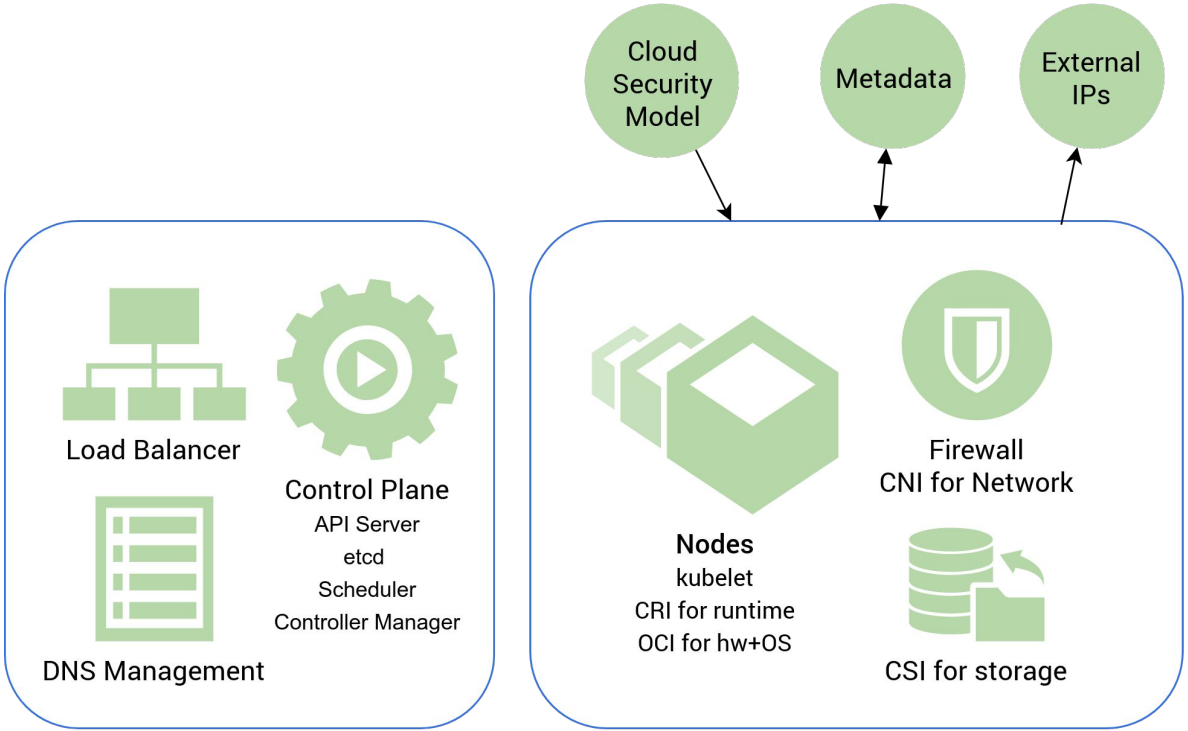
CRI for runtime

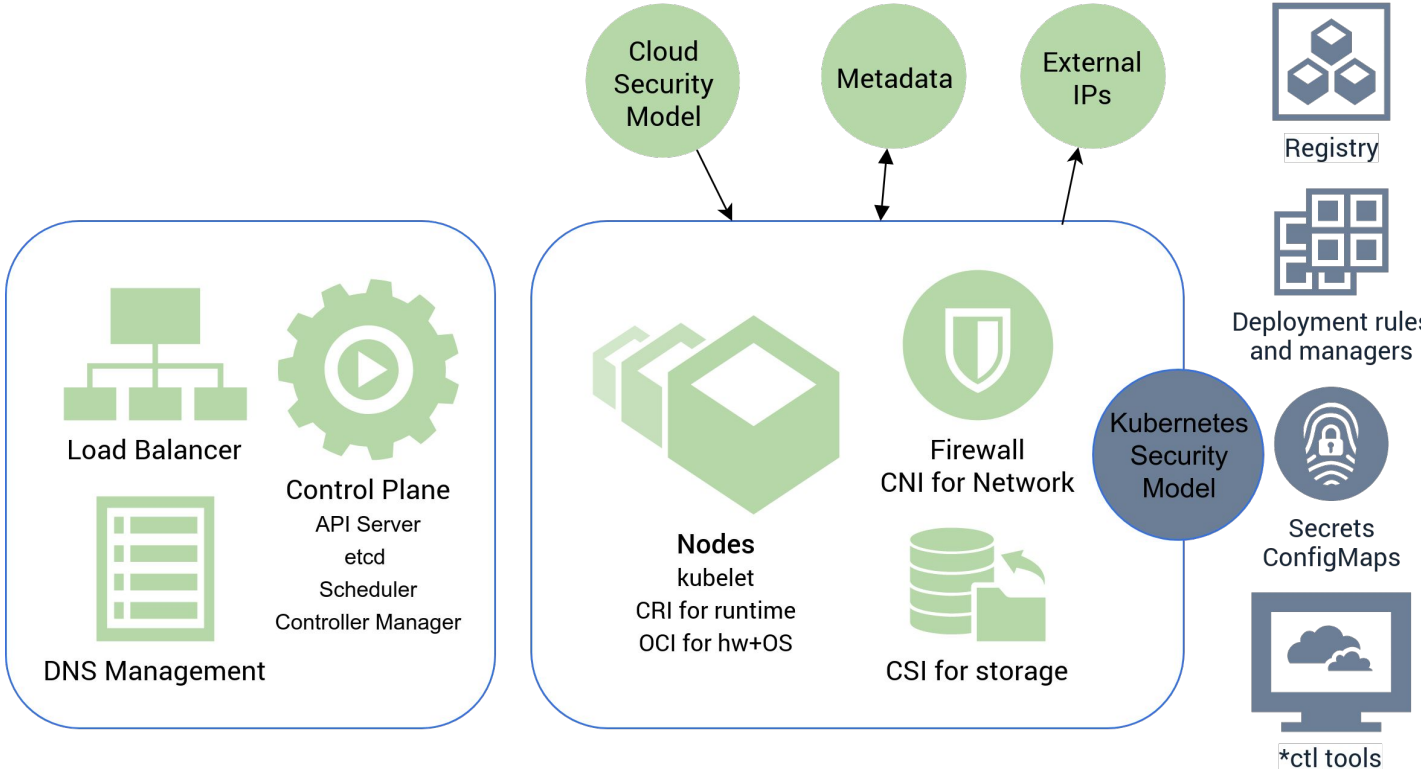
OCI for hw+OS

Firewall

CNI for Network

CSI for storage


Cloud Security Model
Metadata
External IPs
Load Balancer
Control Plane
API Server
etcd
Scheduler
Controller Manager
DNS Management
Nodes
kubelet
CRI for runtime
OCI for hw+OS
Firewall
CNI for Network
CSI for storage


Cloud Security Model
Metadata
External IPs
Registry
Deployment rules and managers
Load Balancer
Control Plane
API Server
etcd
Scheduler
Controller Manager
DNS Management
Nodes
kubelet
CRI for runtime
OCI for hw+OS
Firewall
CNI for Network
CSI for storage
Kubernetes Security Model
Secrets
ConfigMaps
*ctl tools

Containment models

	dockerd	minikube	K3s	GCP Kubernetes	DO Kubernetes	AWS AKS
AppArmor	default	unconfined	cri-containerd.apparmor.d	default	unconfined	unconfined
Seccomp	filtering	disabled	disabled	disabled	disabled	disabled
Blocked syscalls	56	19	30	18	21	20

Kubernetes defaults

Inside a Kubernetes cluster network is a complete **free-for-all HTTP by default**.
Etcd is **open to the tubes**, with internal RBAC off
Kube-controller-manager by default **auto-approve** certificate signing requests for system:nodes:
CoreDNS **will not verify** if records correspond to reality
Kubelet default authorization mode is **AlwaysAllow** for all requests

Kubernetes Dashboard runs with **full admin rights**
Tiller is deployed with **allow unauthenticated users**
Istio installation **policy enforcement is disabled**.
Cert-manager runs with **validation disabled**
Envoy listens **everywhere** on port 15020
istio-sidecar-injector would inject anything

@alexivkinx

Pillage!

@alexivkinx

Me be needin some toolz

Mess with the sidecar injection

```
curl -sL https://github.com/istio/istio/releases/download/1.4.0-beta.0/istioctl-1.4.0-beta.0-linux.tar.gz | tar xzf -
```

Kubectl

```
curl -sLO https://storage.googleapis.com/kubernetes-release/release/v1.16.0/bin/linux/amd64/kubectl; chmod u+x kubectl
```

GCP and DO metadata for easy kube pwnage

```
curl -sL https://github.com/4ARMED/kubeletmein/releases/download/v0.6.5/kubeletmein_0.6.5_linux_amd64 -o kubeletmein; chmod u+x kubeletmein
```

Manage private registries

```
curl -sL https://github.com/genuinetools/reg/releases/download/v0.16.0/reg-linux-amd64 -o reg; chmod u+x reg
```

Better alternative to the docker CLI

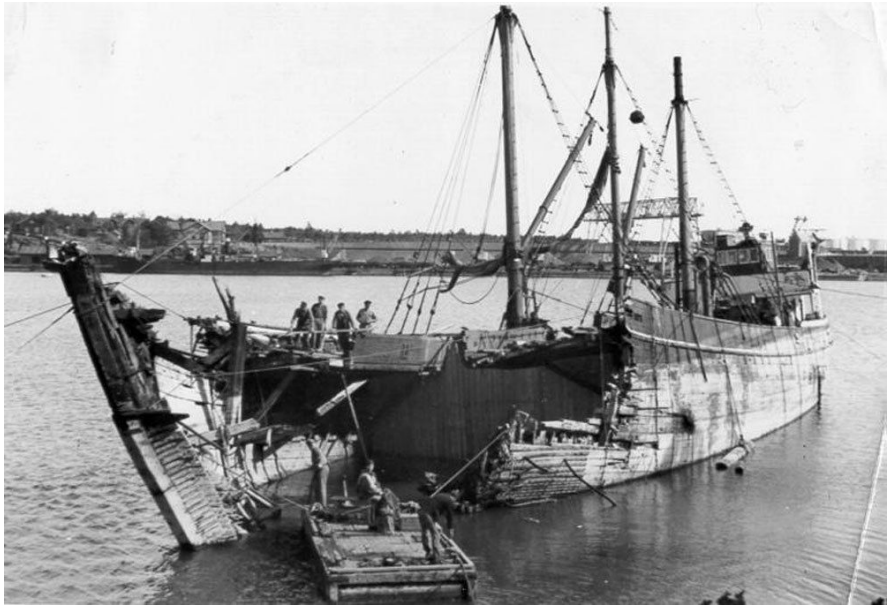
```
curl -sL https://github.com/kubernetes-sigs/cri-tools/releases/download/v1.16.1/crictl-v1.16.1-linux-amd64.tar.gz | tar zxf -
```

Etcd client

```
curl -sL https://github.com/etcd-io/etcd/releases/download/v3.4.3/etcd-v3.4.3-linux-amd64.tar.gz | tar zxf -
```

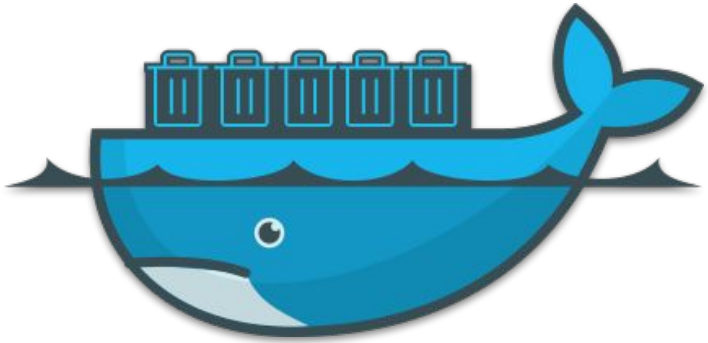
Helm chart allowing all to nodes

```
curl -sLO https://github.com/alexivkin/kubepwn/releases/download/0.1/bootychart.tgz
```



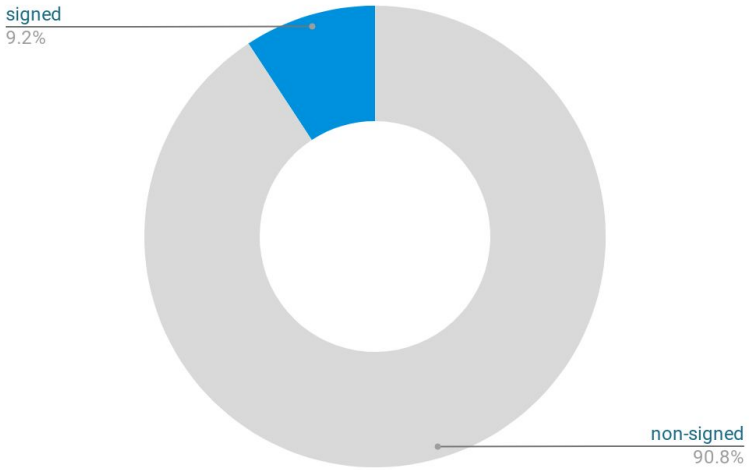
Yer front fell off!

@alexivkinx



@alexivkinx

@alexivkinx



@alexivkinx

Hide yo' ~~shit~~ metadata

Enable Istio Egress Gateway to limit metadata access

@alexivkinx

Errors, not vulnerabilities, lead to a lot of breaches *
Steep learning curve, mistakes will be made
Secure by default

** (Verizon 2019 data breach investigations report)*


Thank you!
back to regularly scheduled programming
@alexivkinx

EOF