Bulletproof Kubernetes - Learn by Hacking!

whoami

KubeCon

CloudNativeCon

Europe 2019

Ana Calin

Systems Engineer @Paybase

Twitter: @AnaMariaCalin

Luke Bond

Co-founder @ControlPlane

Twitter: @lukeb0nd

The plan...

- Intro to security
- Team allocation
- Some hacking

User

Master

etcd (key-value DB, SSOT)

Controller Manager
(Controller Loops)

API Server (REST API)

Scheduler
(Bind Pod to Node)

Nodes

Networking
Kubelet
Container Runtime
OS
Node 1

Networking
Kubelet
Container Runtime
OS
Node 2

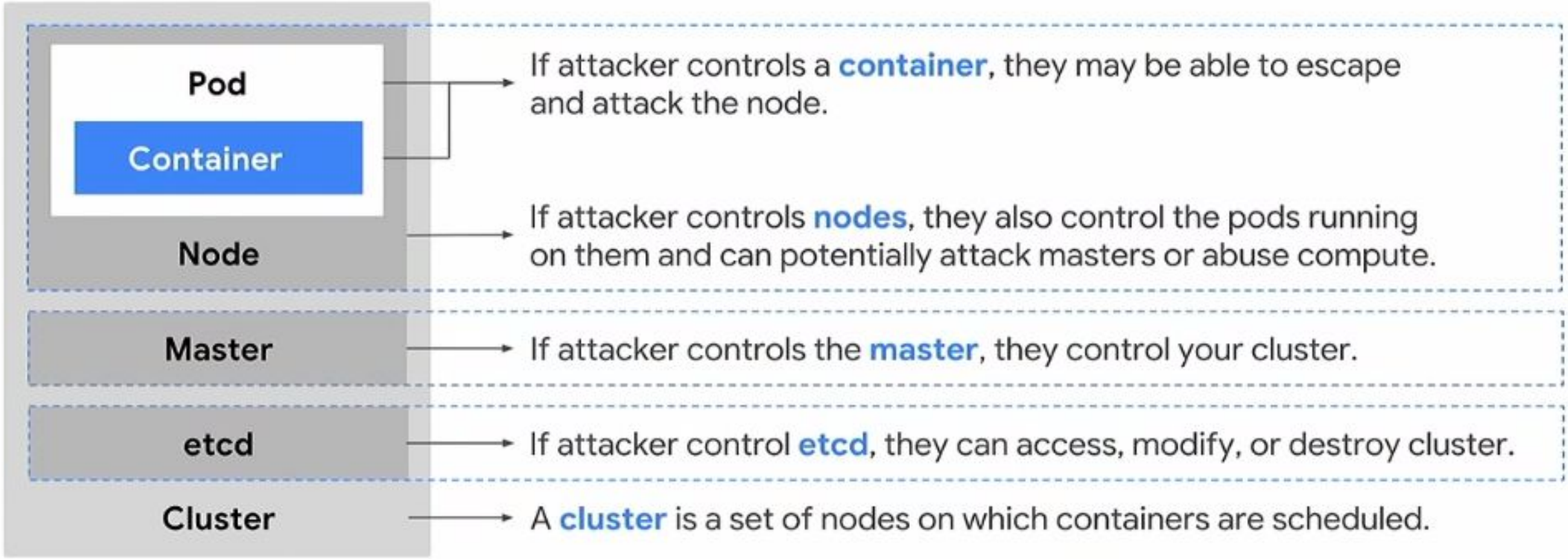
Networking
Kubelet
Container Runtime
OS
Node 3

Legend:

CNI
CRI
OCI
Protobuf
gRPC
JSON

By Lucas Käldström

Kubernetes architecture



What Can Go Wrong?

- **CVE-2016-9962** - docker: insecure opening of file-descriptor allows privilege escalation
- **CVE-2017-1000056** - PodSecurityPolicy admission plugin authorizes incorrectly
- **CVE-2017-1002100** - Azure PV should be Private scope not Container scope
- **CVE-2017-1002102** - atomic writer volume handling allows arbitrary file deletion in host filesystem
- **CVE-2019-5736** - when running a process as root (UID 0) inside a container, that process can exploit a bug in runc to gain root privileges on the host.
- **CVE-2019-1002100** - denial of service of the K8s API Server on versions prior to 1.13.4 by running `kubectl patch --type json`

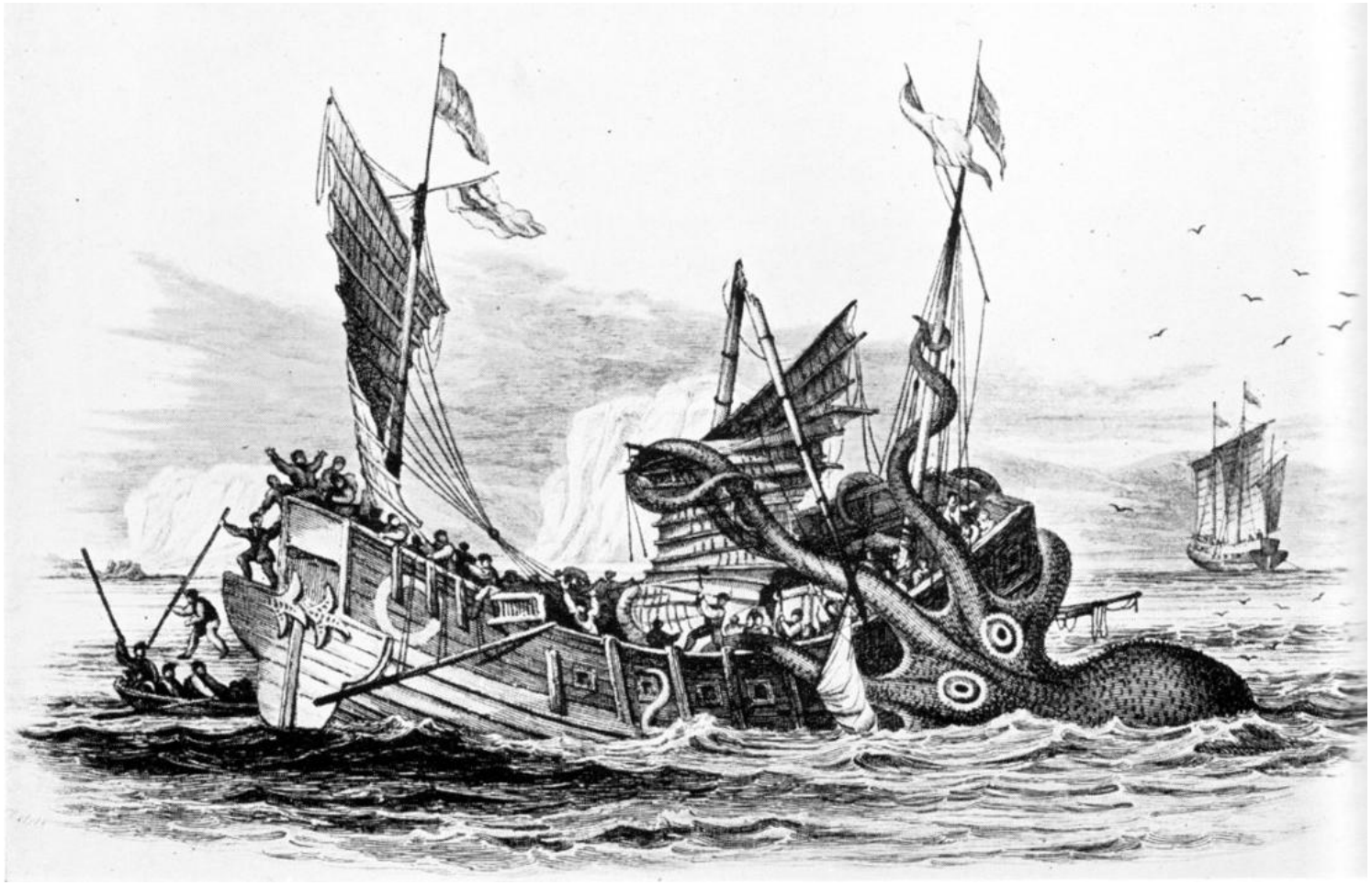
Container security

Application security — Are my applications secure?

Infrastructure security	Software supply chain	Container runtime security
Is my infrastructure **secure for developing** containers?	Is my container image **secure to build and deploy**?	Is my container **secure to run**?

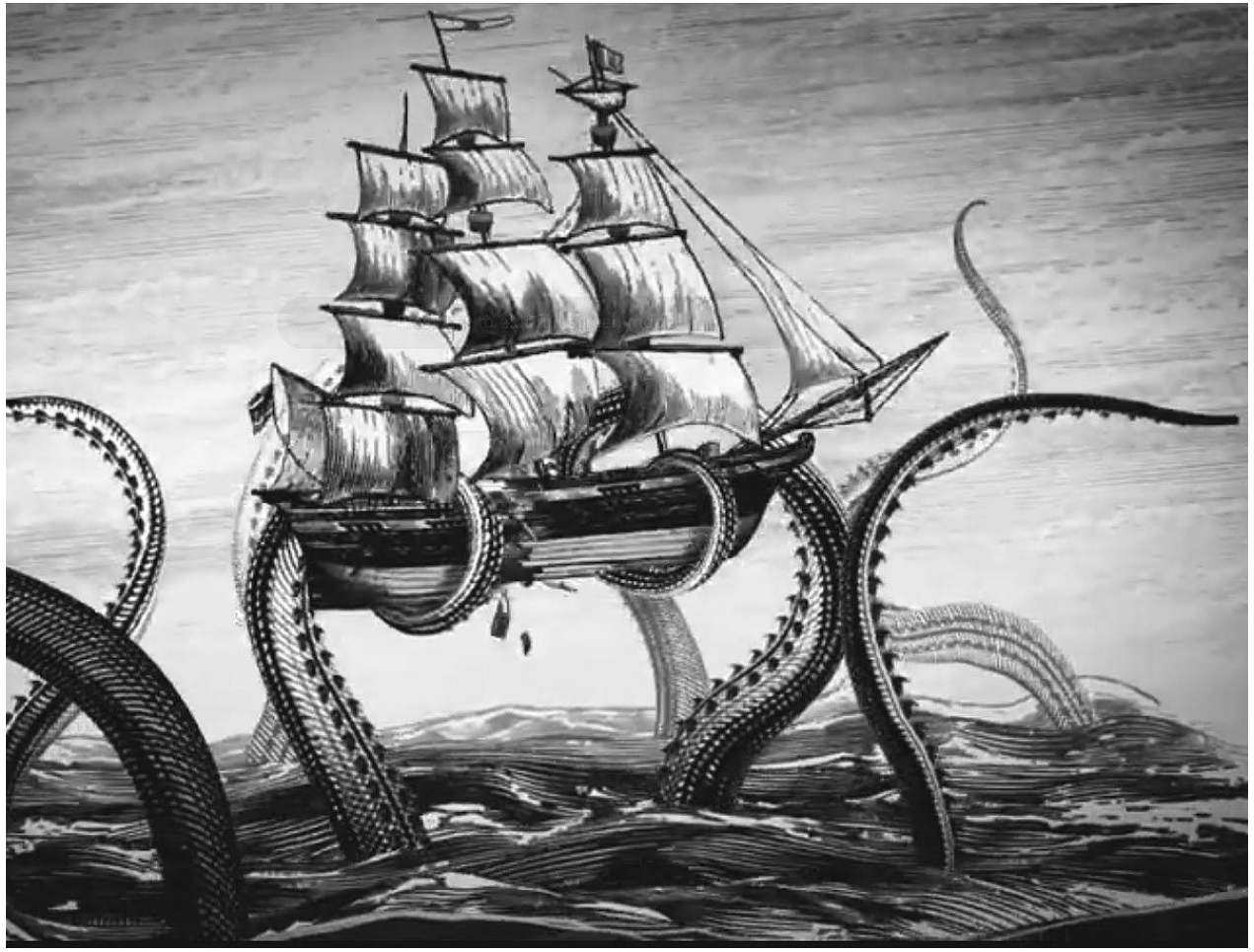
Platform security — Is my (cloud provider's) infrastructure secure?

Common Attacks on Kubernetes



- Can you name any?

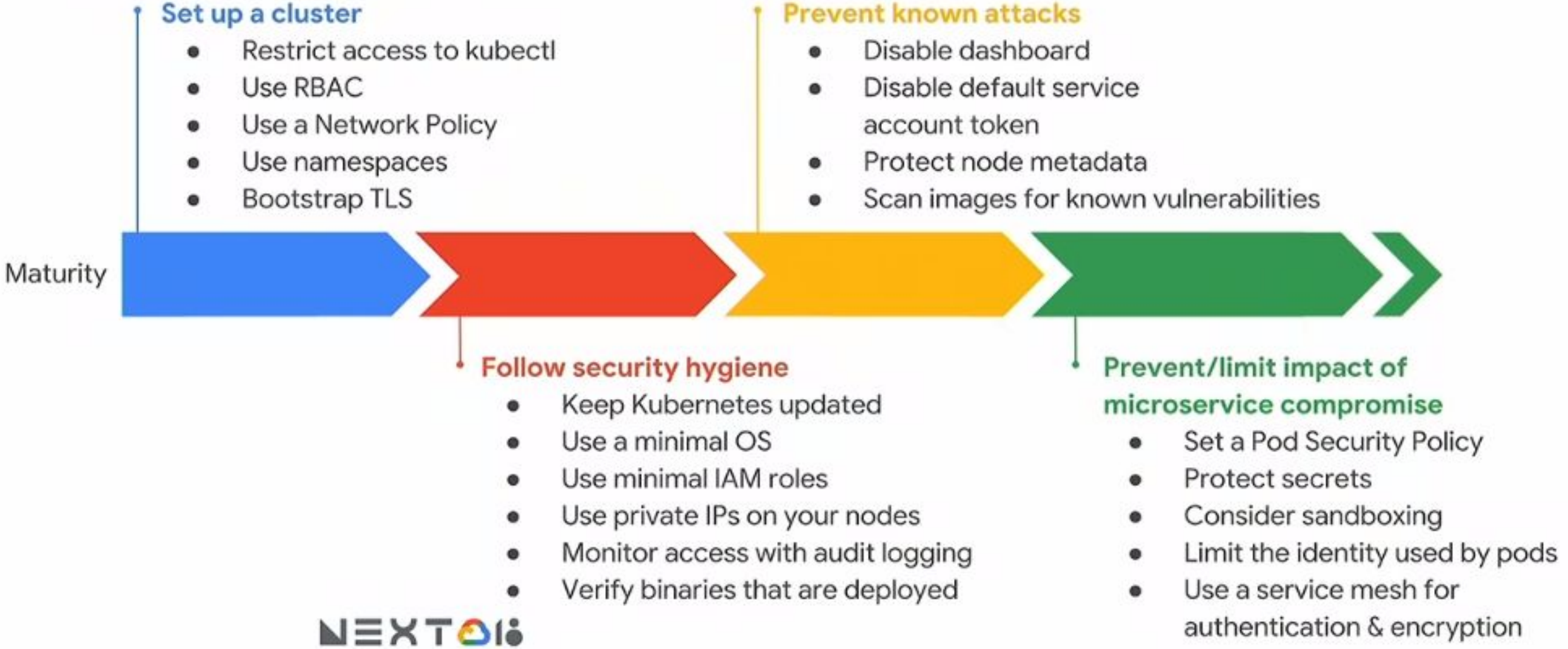
Where is Kubernetes vulnerable?



- Application workloads
- Workload configuration
- Cluster configuration - developer
- Cluster configuration - operations
- Cluster deployment

Pivoting from a Compromised Pod/Container

- Kernel exploit
  - Dirtycow, 0days
- Container runtime exploit
  - CVE-2016-9962 (insecure opening of file-descriptor allows privilege escalation)
- Orchestrator misconfiguration
  - Shared namespaces
  - Lack of user namespace for shared resources
  - Host mounts
  - Insecure pods
  - Privileged containers
- Application
  - Datastore access
  - Secrets and roles
- Network
  - Sniffing/brute forcing other entities (pods, control plane, datastores)
  - TLS/cert/downgrade attacks


Set up a cluster
Restrict access to kubectl
Use RBAC
Use a Network Policy
Use namespaces
Bootstrap TLS
Prevent known attacks
Disable dashboard
Disable default service account token
Protect node metadata
Scan images for known vulnerabilities
Maturity
Follow security hygiene
Keep Kubernetes updated
Use a minimal OS
Use minimal IAM roles
Use private IPs on your nodes
Monitor access with audit logging
Verify binaries that are deployed
Prevent/limit impact of microservice compromise
Set a Pod Security Policy
Protect secrets
Consider sandboxing
Limit the identity used by pods
Use a service mesh for authentication & encryption

Some ports you can explore

Port	Process	Description
443/TCP	kube-apiserver	Kubernetes API port
2379/TCP	etcd	
4194/TCP	cAdvisor	Container metrics
6443/TCP	kube-apiserver	Kubernetes API port
6666/TCP	etcd	etcd
6782-4/TCP	weave	Metrics and endpoints
8443/TCP	kube-apiserver	Kubernetes API port
8080/TCP	kube-apiserver	Insecure API port
9099/TCP	calico-felix	Health check server for Calico
10250/TCP	kubelet	HTTPS API which allows full node access
10255/TCP	kubelet	Unauthenticated read-only HTTP port: pods, runningpods, node state
10256/TCP	kube-proxy	Kube Proxy health check server

Kubernetes Cheat-sheet

A cheatsheet to help you out:

https://github.com/calinah/learn-by-hacking-kccn/blob/master/k8s_cheatsheet.md

Accessing the cluster

1. You will be allocated a team name
2. Go to

   https://github.com/calinah/learn-by-hacking-kccn/blob/master/teams.md and get you cluster details
3. Good luck!

Capture the flag

Write a flag to `**/tmp/flag**` on one of the worker nodes and let us know when you've done it. Good luck!

Solution

Further reading on other attacks

- ✓ https://www.4armed.com/blog/hacking-kubelet-on-gke/
- ✓ https://www.4armed.com/blog/kubeletmein-kubelet-hacking-tool/
- ✓ https://itnext.io/how-a-naughty-docker-image-on-aks-could-give-an-attacker-access-to-your-azure-subscription-6d05b92bf811
- ✓ https://kubernetes.io/blog/2018/07/18/11-ways-not-to-get-hacked/