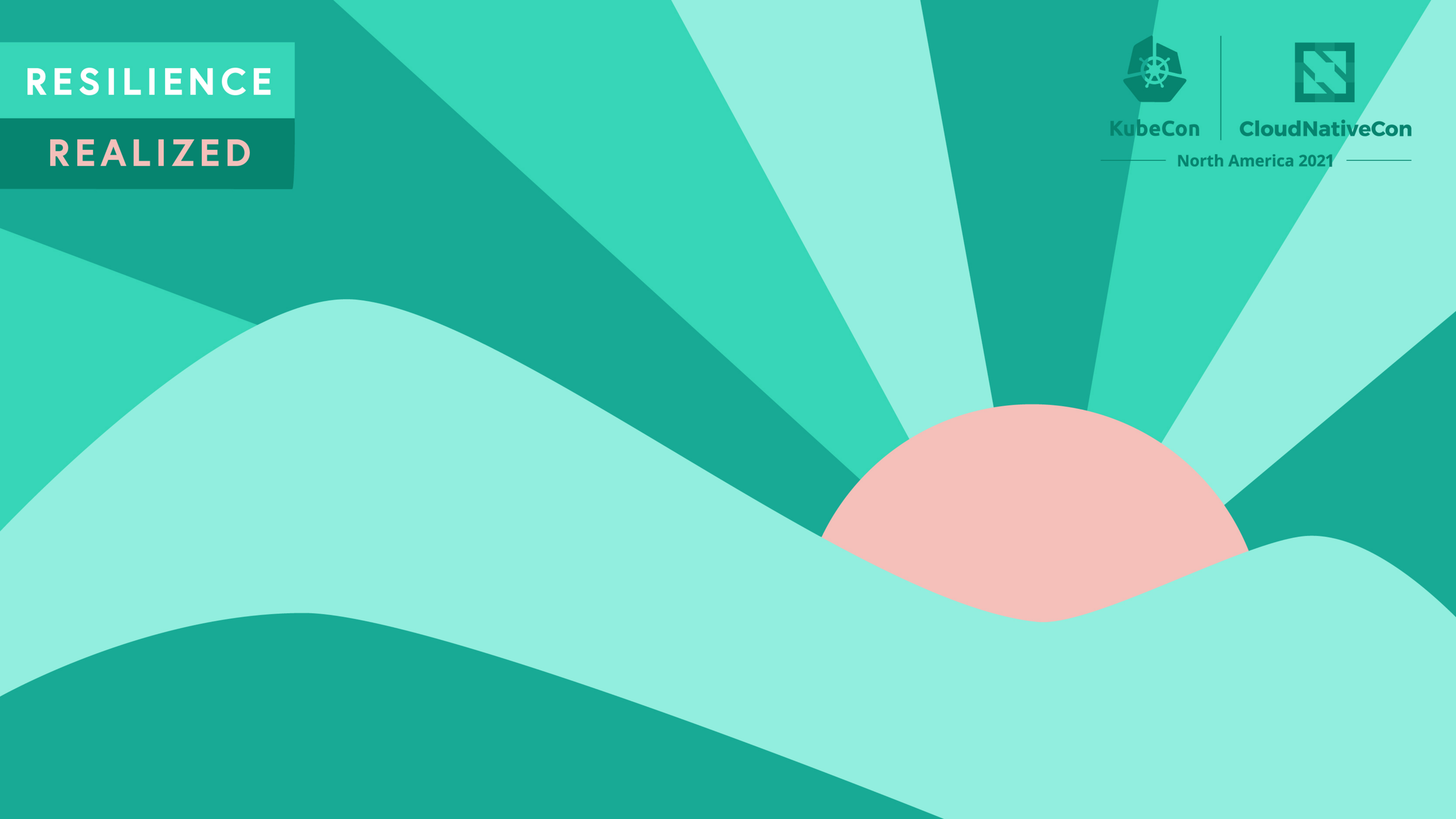
RESILIENCE REALIZED



KUBERNETES EXPOSED!

Seven of Nine Hidden Secrets That Will Give You Pause

@IanColdwater
@bradgeesaman

@IanColdwater

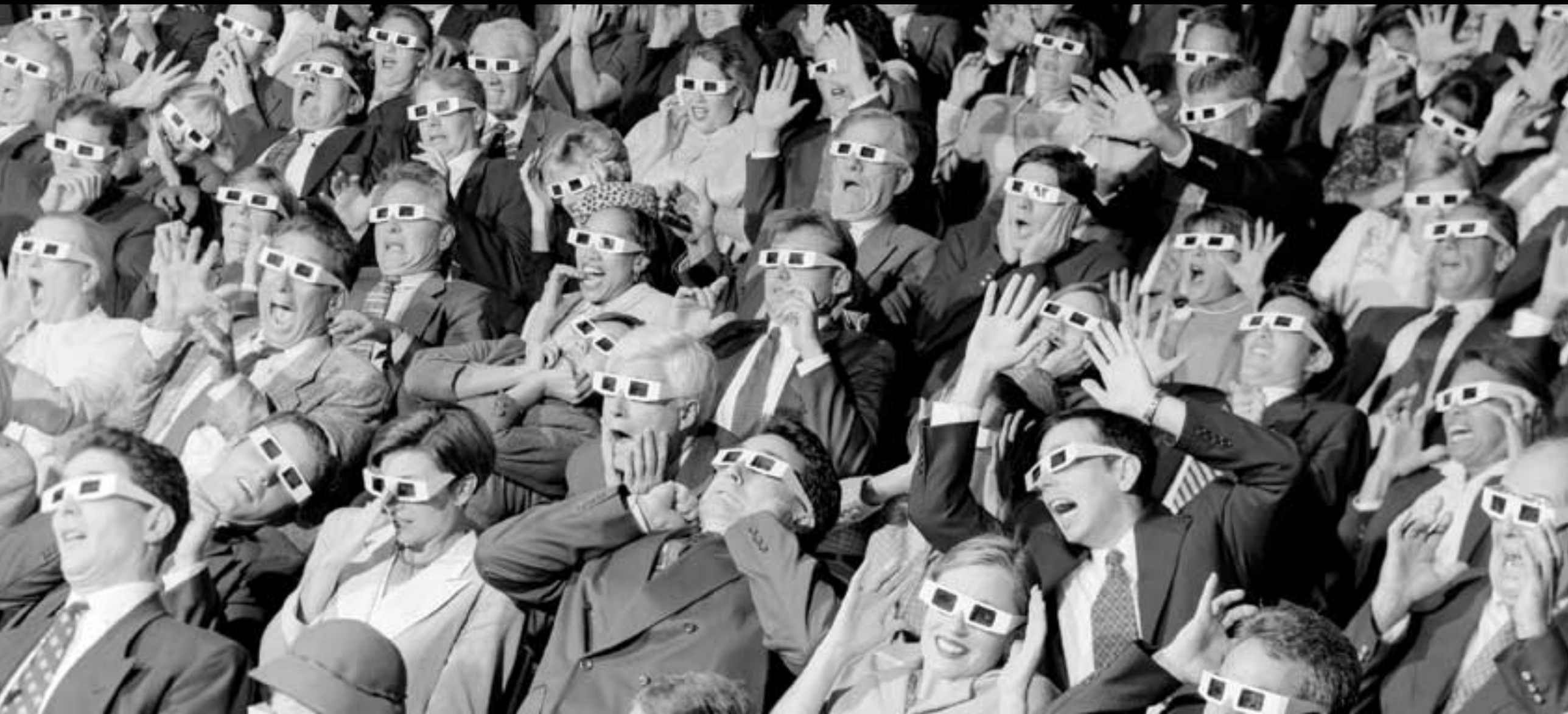
@bradgeesaman

- Ian is a leading expert on containers and container security.

- Brad is a leading expert on containers and container security.

GRAB SOME POPCORN!

@IanColdwater
@bradgeesaman



REVOKING CERTIFICATES

@IanColdwater
@bradgeesaman

DEFAULT SECCOMP?

@IanColdwater
@bradgeesaman

NO GODS, NO SYSTEM:MASTERS

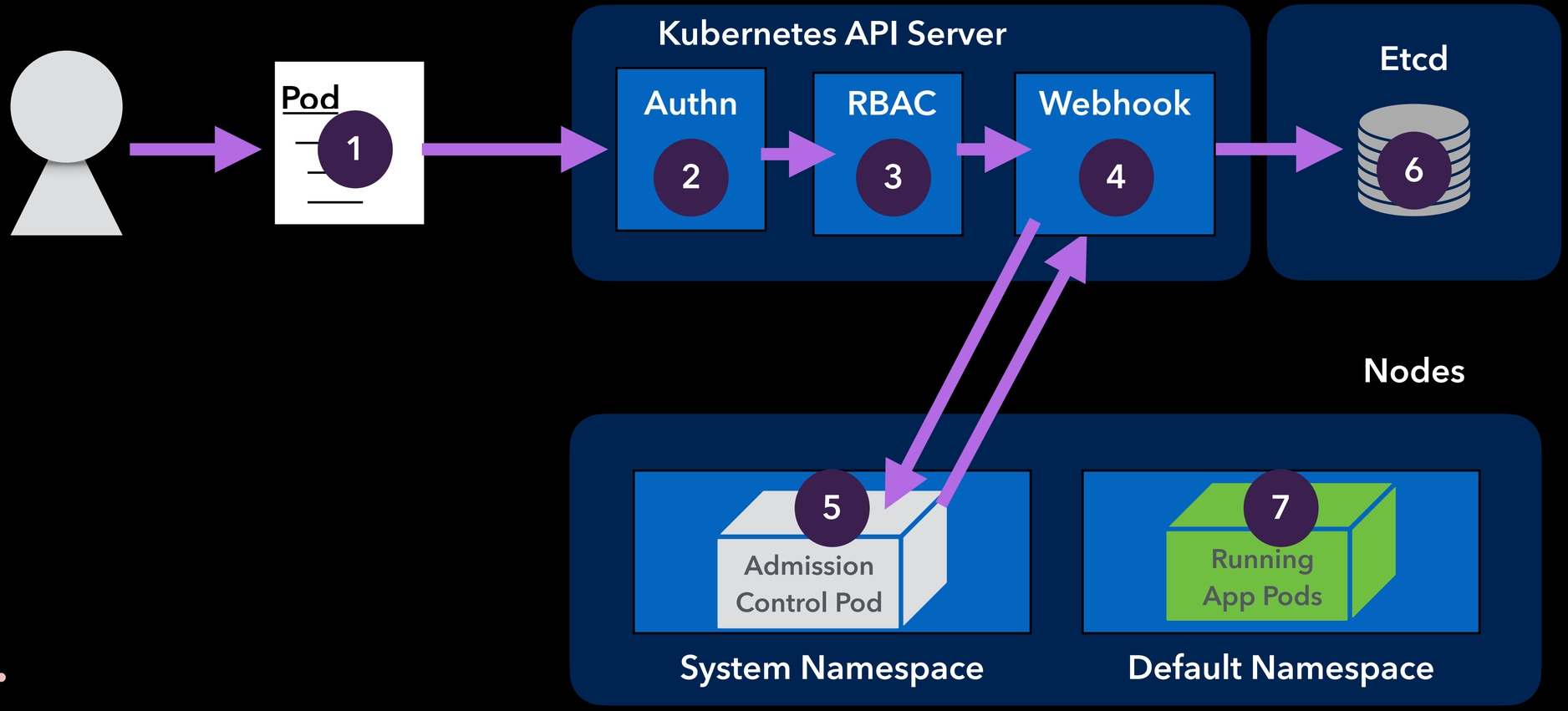
@IanColdwater
@bradgeesaman

DEMO: UNDELETABLE

@IanColdwater
@bradgeesaman

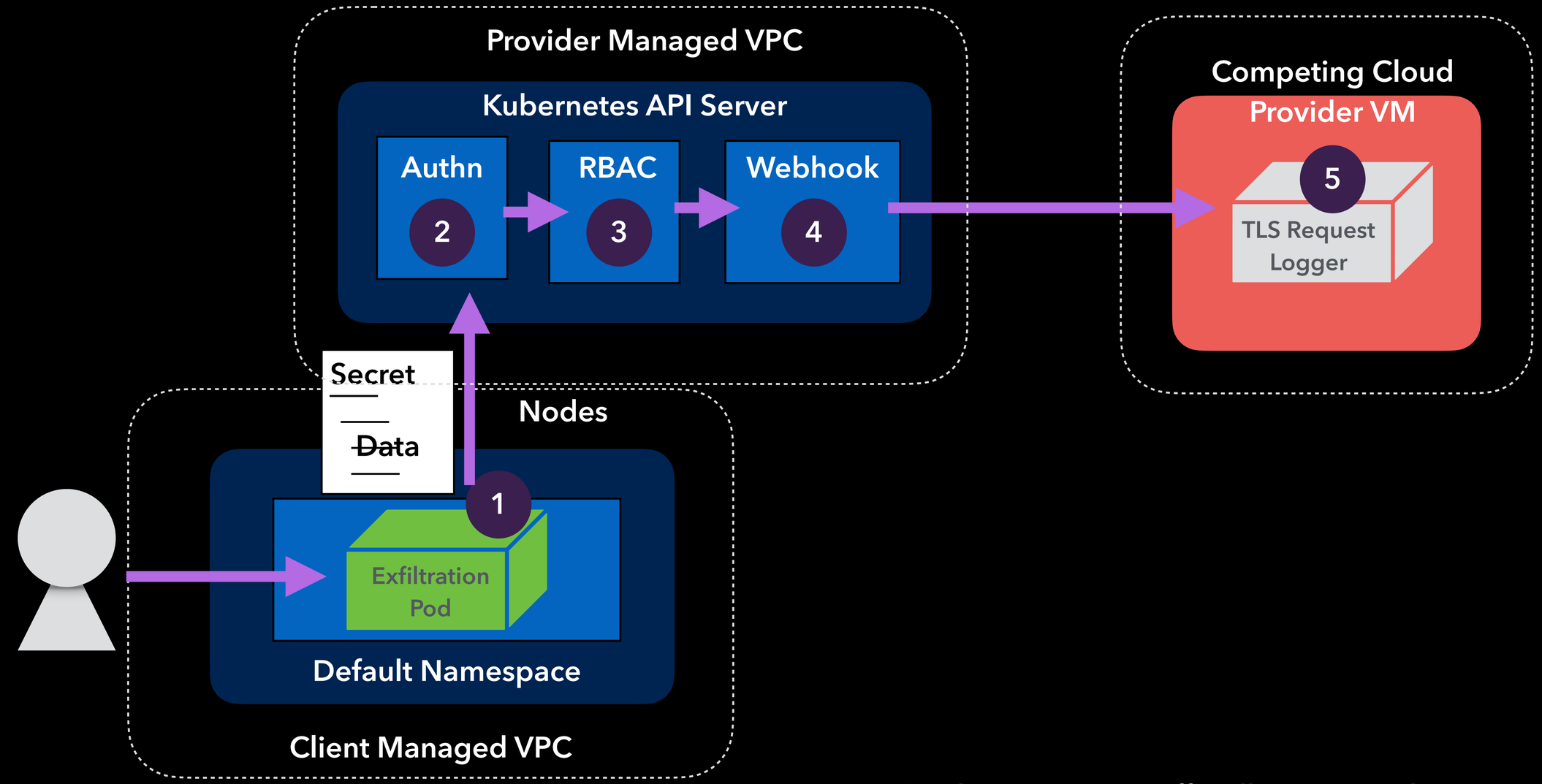
VALIDATING WEBHOOKS

@IanColdwater
@bradgeesaman



FREE EGRESS?*

@IanColdwater
@bradgeesaman



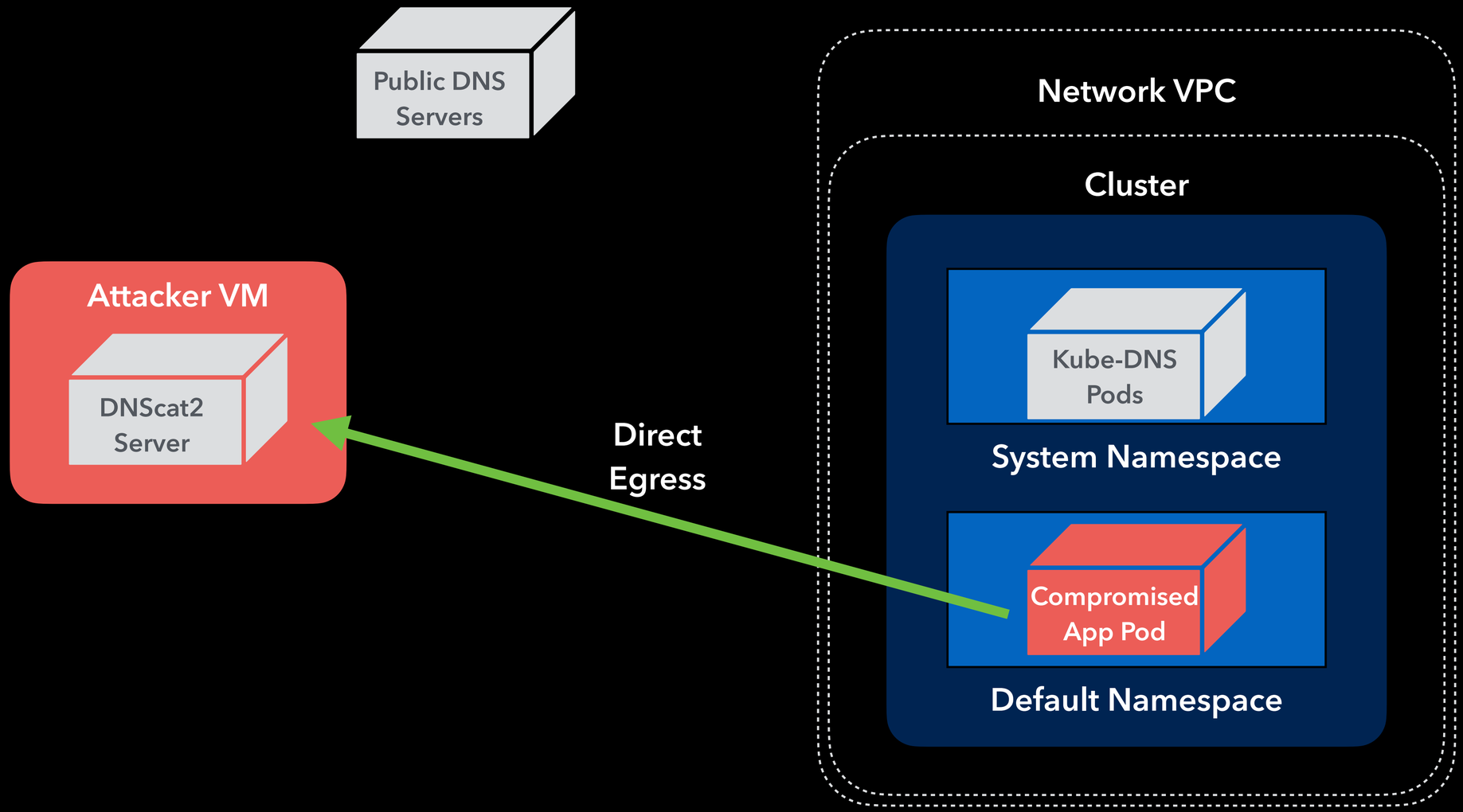
** Disclaimer: Not an officially supported use case*

DEMO: EXFILTRATING WEBHOOKS

@IanColdwater
@bradgeesaman

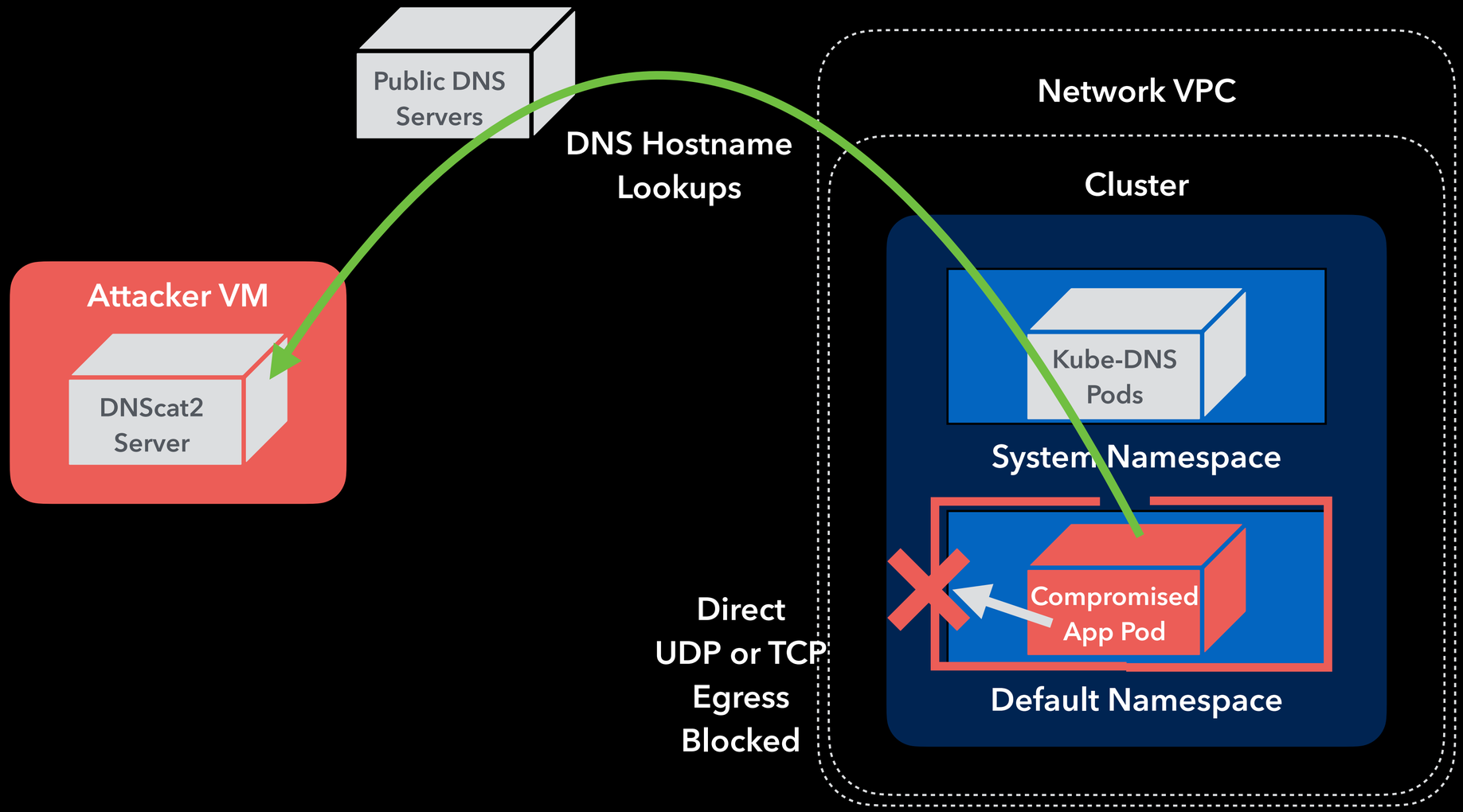
IT'S ALWAYS DNS

@IanColdwater
@bradgeesaman



EXFILTRATION VIA DNS

@IanColdwater
@bradgeesaman



DEMO: IT WAS DNS

@IanColdwater
@bradgeesaman

THE POWER OF SERVICES

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-evil-service
spec:
  selector:
    run: nginx
  type: LoadBalancer
  ports:
    - name: http
      protocol: TCP
      port: 80
      targetPort: 80
  externalIPs:
    - 23.185.0.3 #cncf.io
```

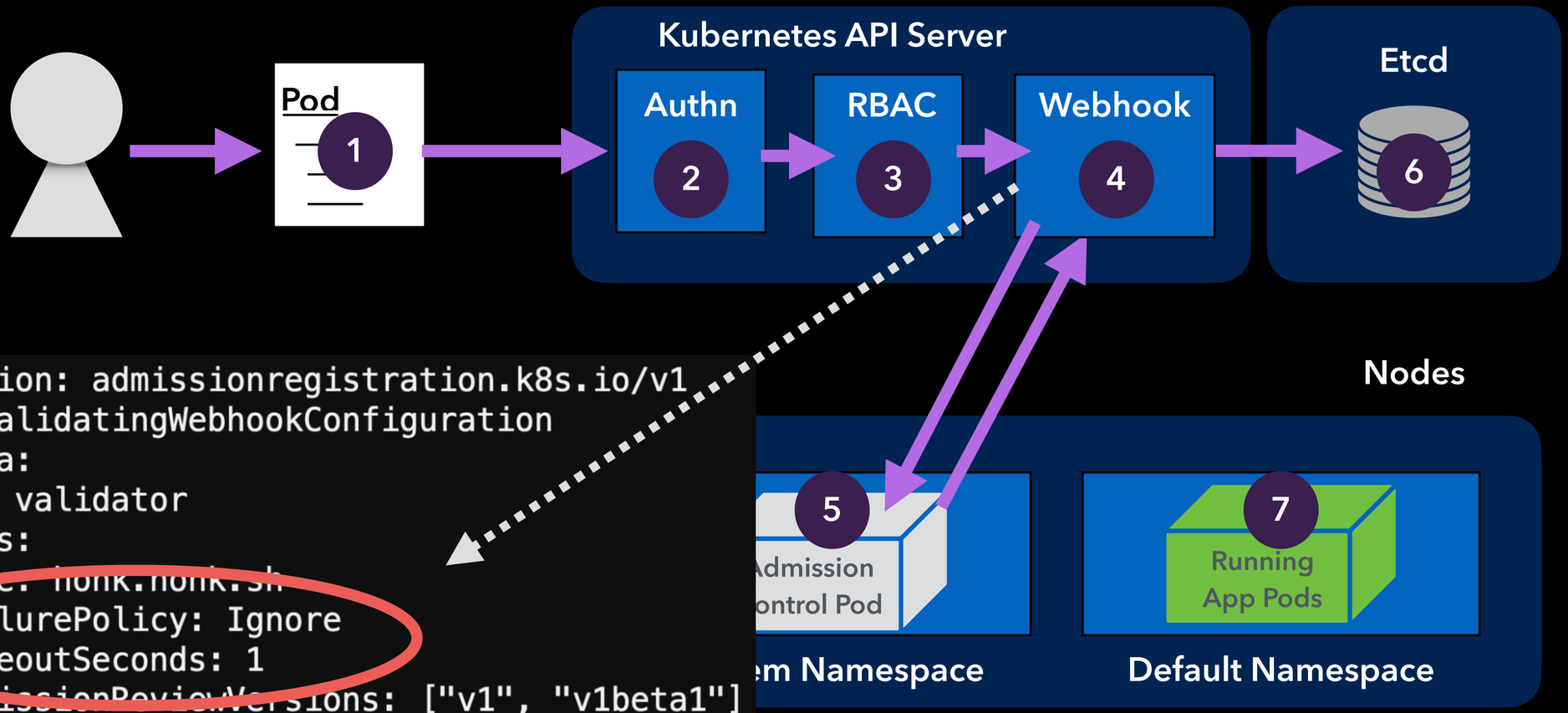
External IP Service

- What this YAML says: “All traffic within the cluster going to 23.185.0.3 on port 80 gets sent to the nginx pod”
- This can cross namespaces!

@IanColdwater
@bradgeesaman

IGNORING FAILURES

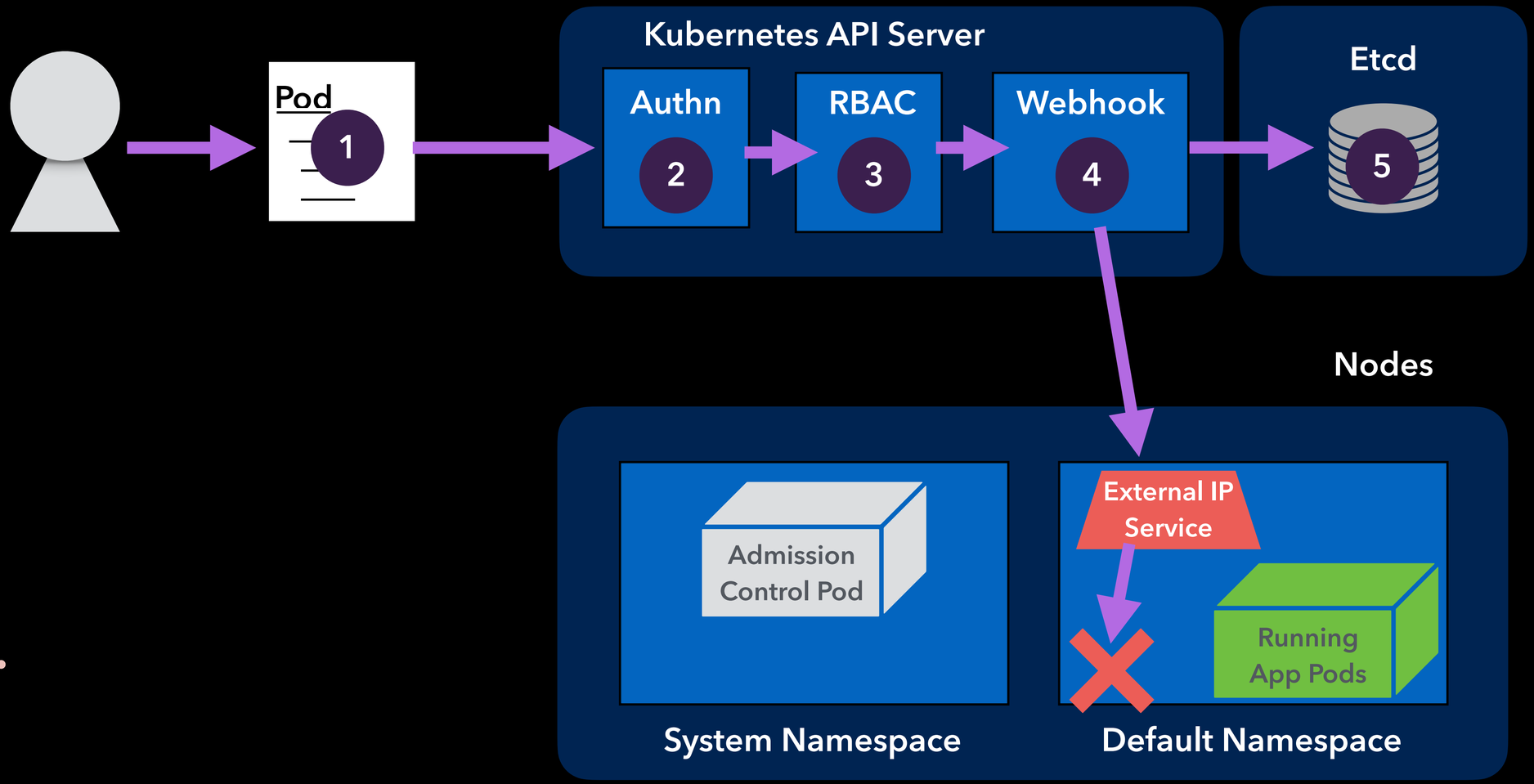
@IanColdwater
@bradgeesaman




```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  name: validator
webhooks:
  - name: honk.honk.sh
    failurePolicy: Ignore
    timeoutSeconds: 1
    admissionReviewVersions: ["v1", "v1beta1"]
    sideEffects: None
    rules:
      - operations: ["CREATE","UPDATE"]
```

FAILURE IS AN OPTION

@IanColdwater
@bradgeesaman



DEMO: WEBHOOK BYPASS

@IanColdwater
@bradgeesaman

THE MORE YOU KNOW

@IanColdwater
@bradgeesaman

RESOURCES

- Kubernetes Certificate Revocation: k8s.rip/cert-revocation
- Default Seccomp: k8s.rip/default-seccomp
- Service Account Token Volume Projection: k8s.rip/satvp
- Validating Webhooks: k8s.rip/validating-webhooks
- Kubernetes Static Pods: k8s.rip/static-pods
- Kubernetes Network Policies: k8s.rip/network-policies
- DNSCat2: k8s.rip/dnscat2
- The Path Less Traveled: k8s.rip/path
- https://k8s.io/security
- github.com/kelseyhightower/nocode - the best way to write secure and reliable applications!

@IanColdwater
@bradgeesaman