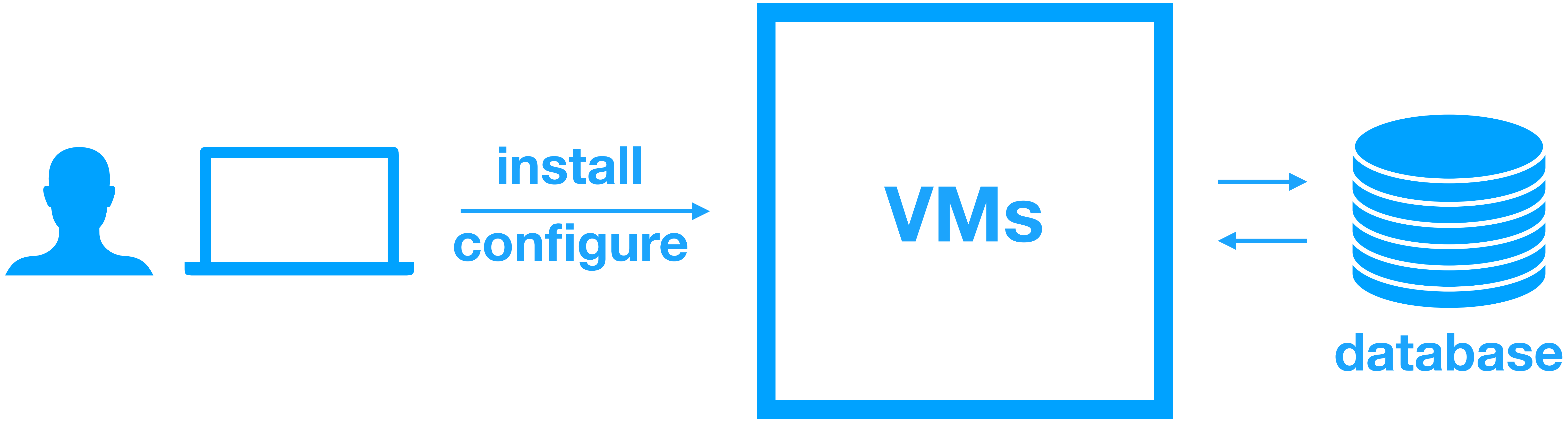
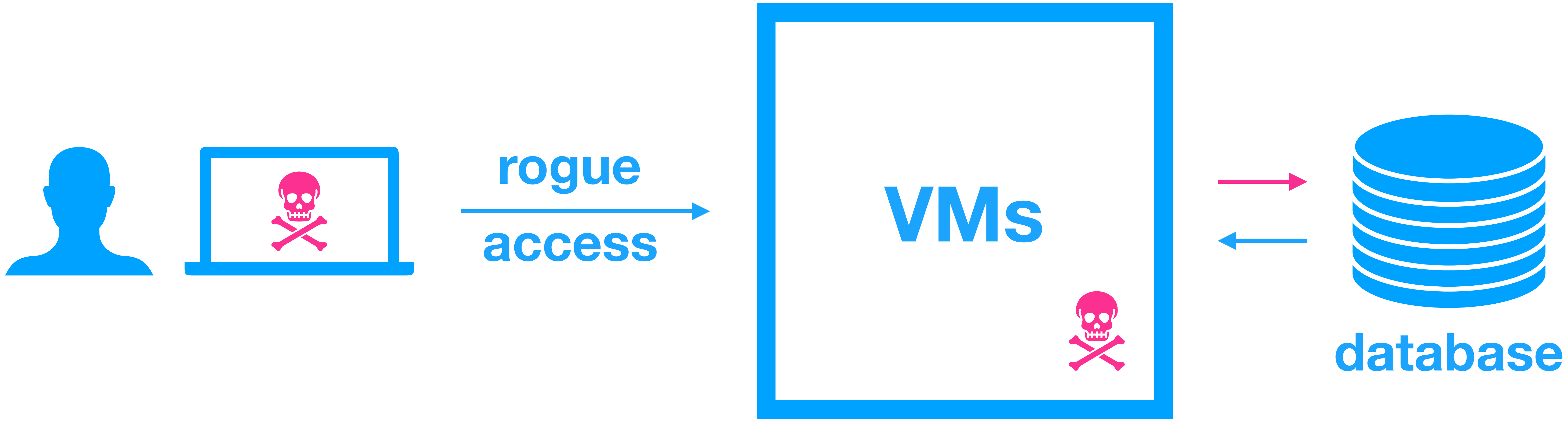
Know your ☸ deployments

Felix Glaser
Production Security Engineer
shopify

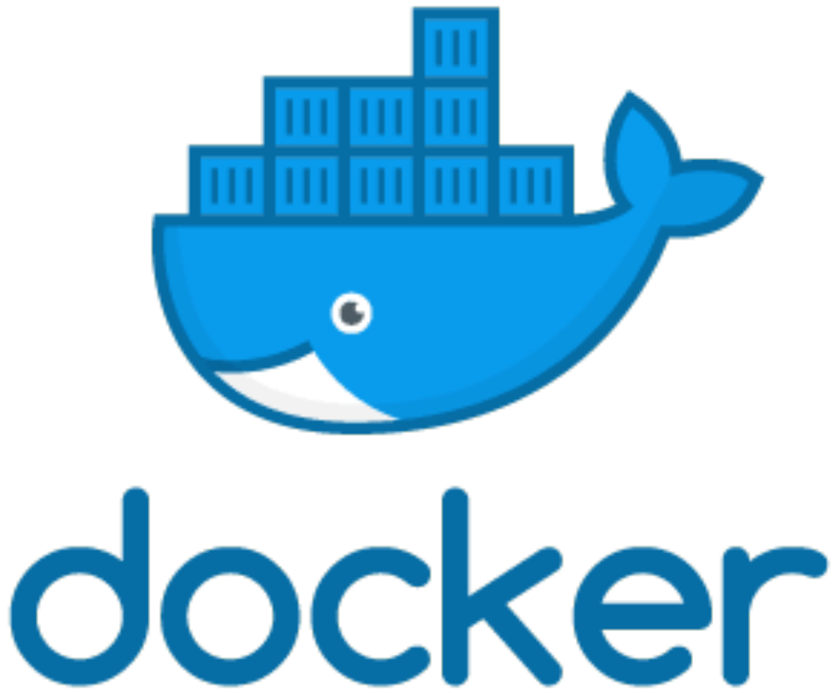
```
curl | sudo bash
```


install
configure
VMs
database

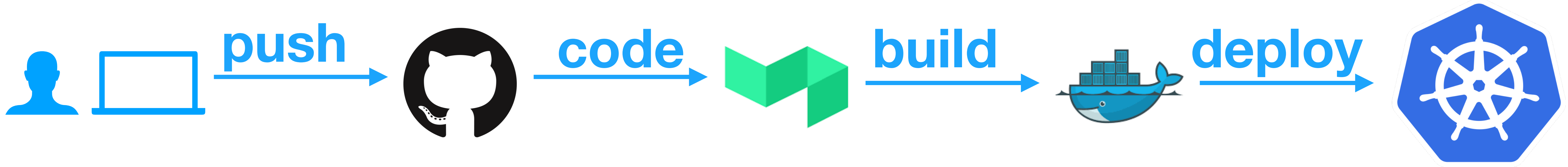
Mutability is the enemy.



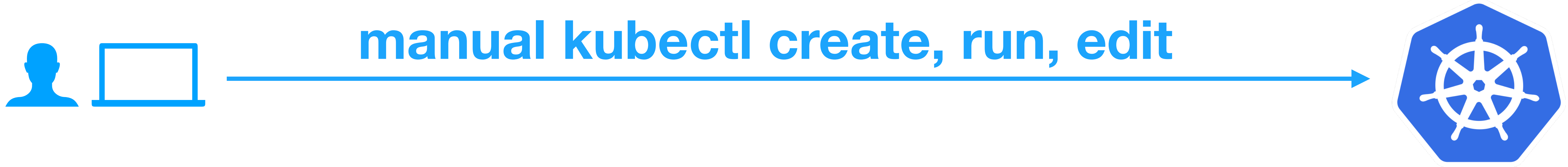
Mutability is no more!



Containerized infrastructure

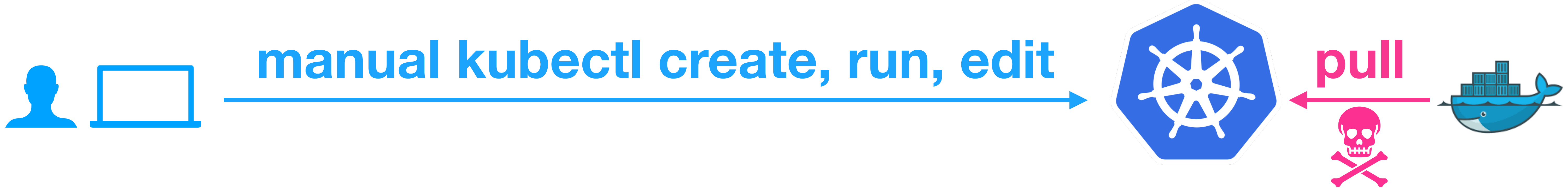


Still allows manual changes



manual kubectl create, run, edit

Runs containers outside your org



manual kubectl create, run, edit

pull

The new `curl|sudo bash`

```
FROM Ubuntu:14.04
COPY executable /usr/bin
CMD [“/usr/bin/executable"]
```

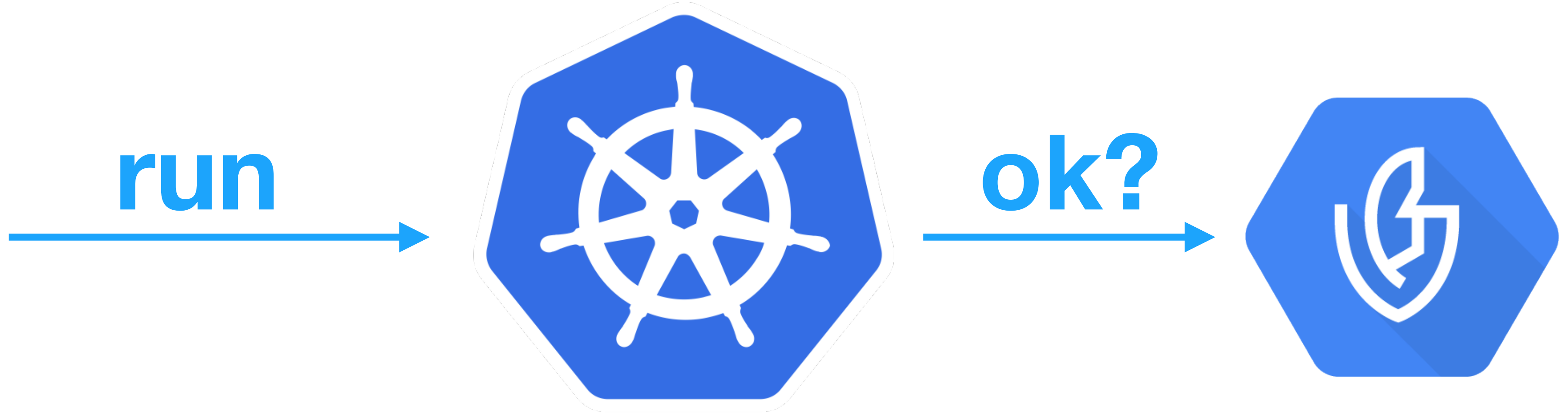
The new curl|sudo bash

```
FROM Ubuntu:14.04
COPY executable /usr/bin
CMD ["/usr/bin/executable"]
```

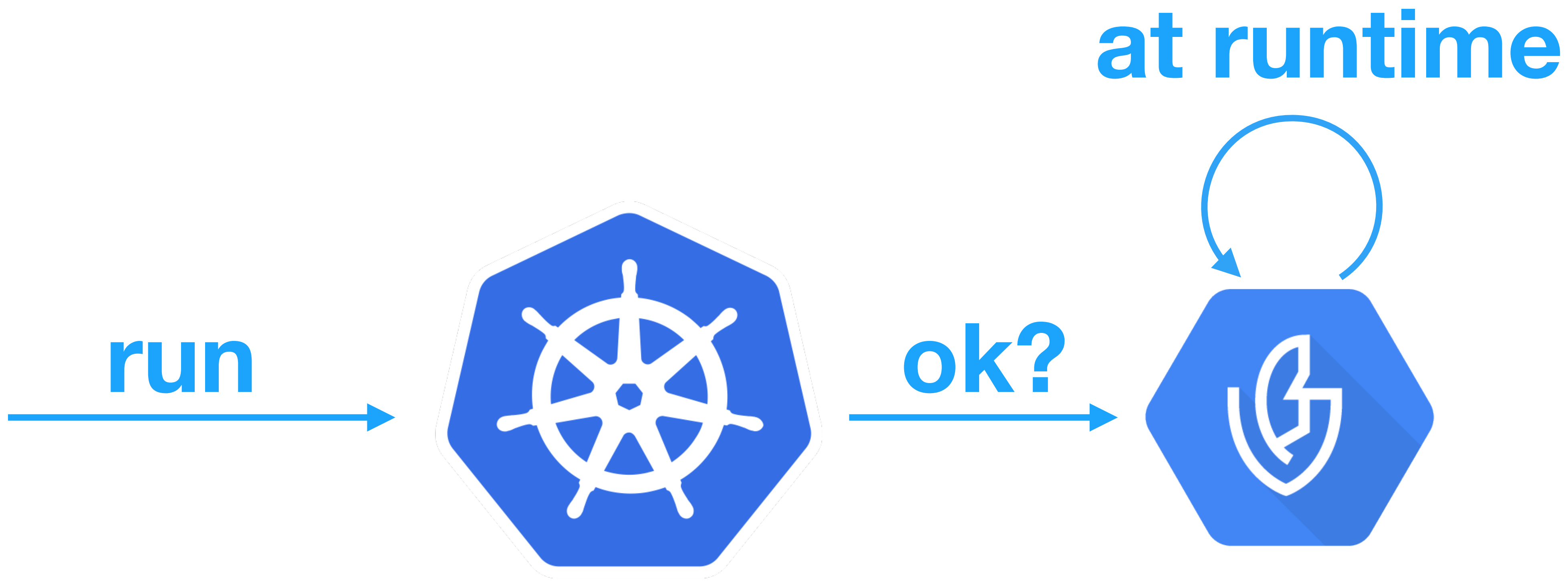
~~apt-get install unattended-upgrades~~

How do we fix this?

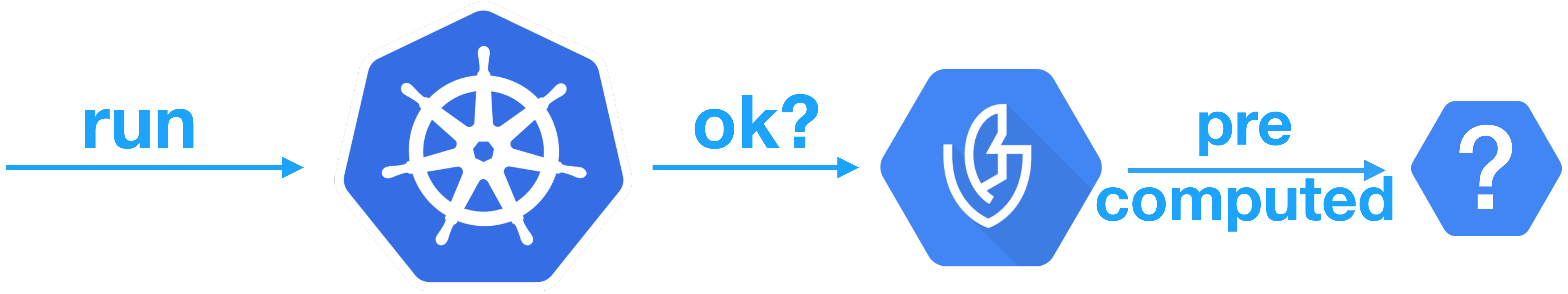
Gate which images can run



When to make the decision



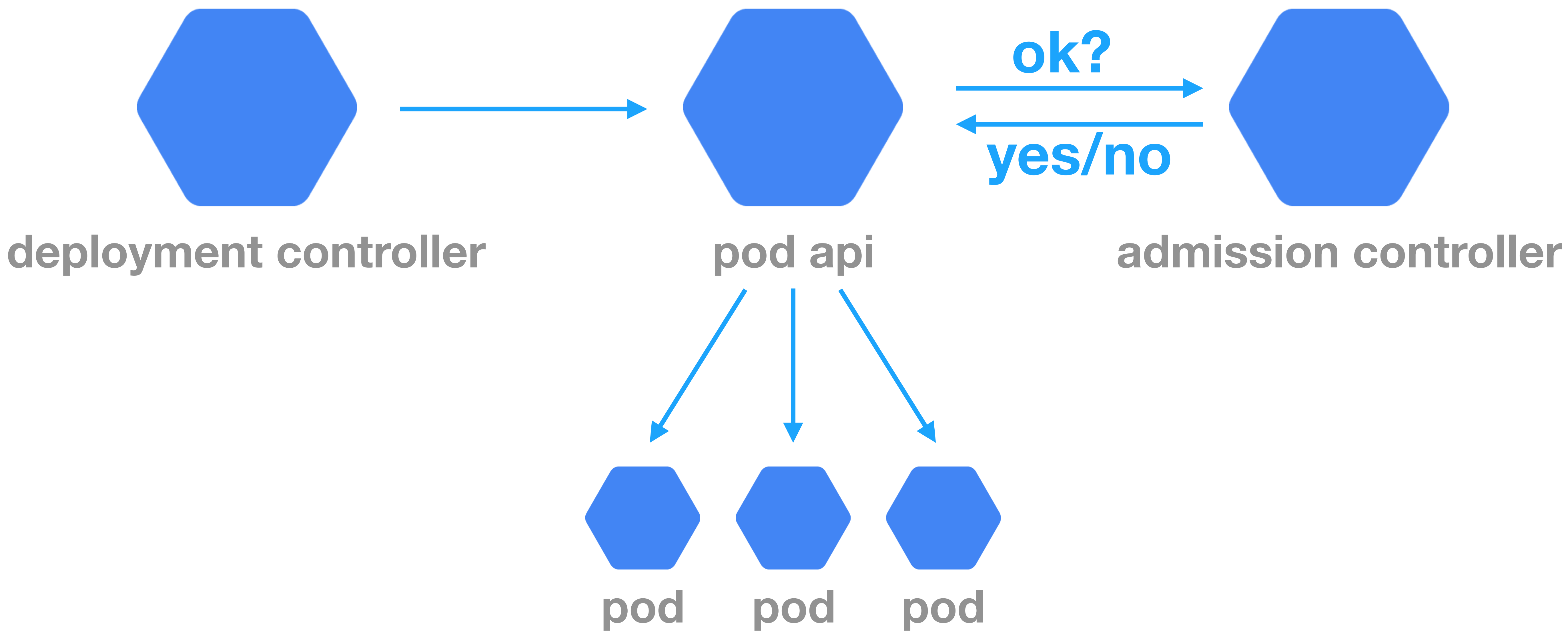
When to make the decision



Pre-computed signatures

```
PGP.sign({
  "critical": {
    "identity": {
      "docker-reference": "gcr.io/some/where"
    },
    "image": {
      "docker-manifest-digest": “sha256:462205…28c9fd945a”
    },
    "type": "Google cloud binauthz container signature"
  }
})
```

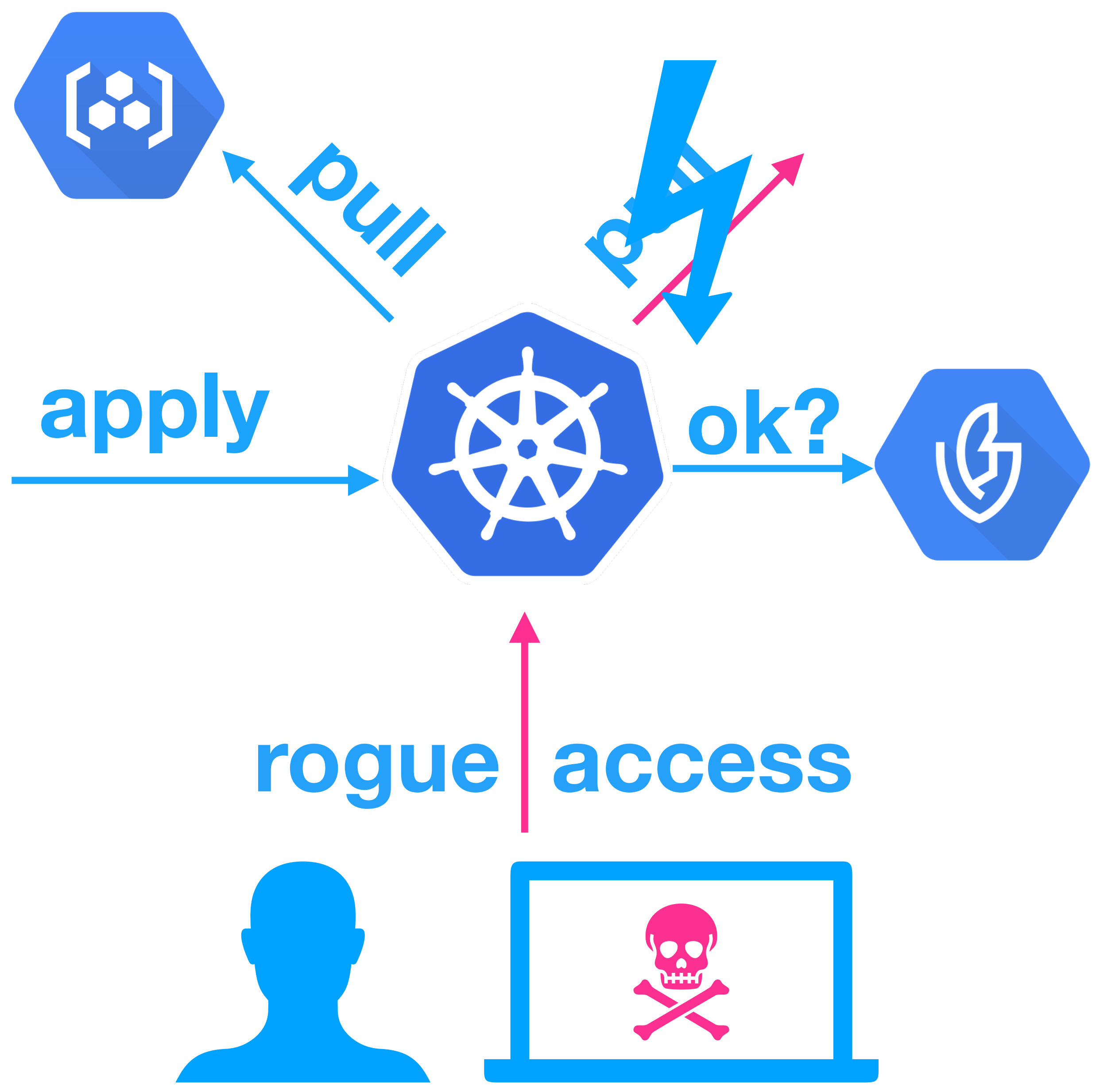
k8s admission controller



Kritis

github.com/grafeas/kritis

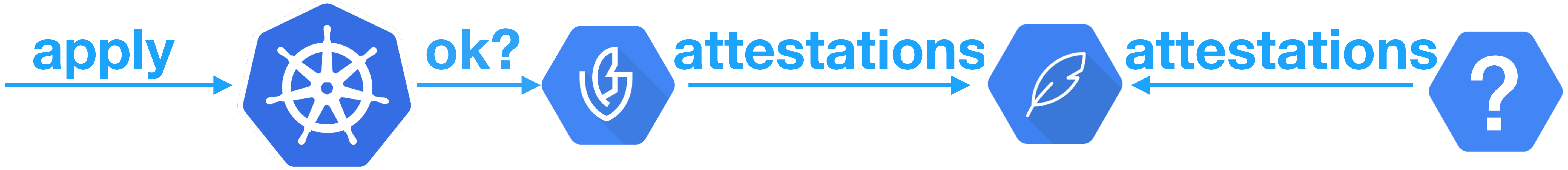
Kritis gating deploys



Grafeas

github.com/grafeas/grafeas

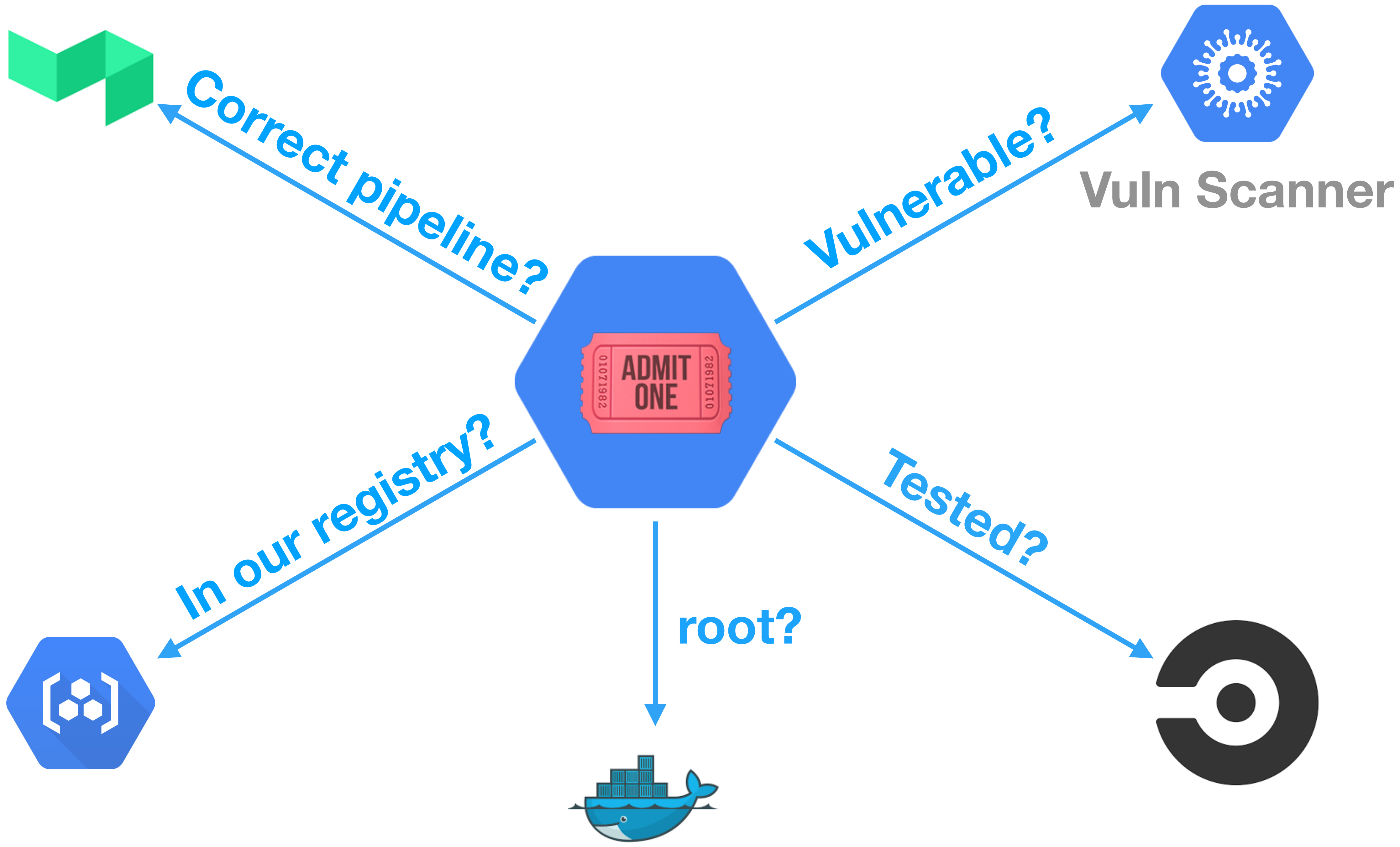
Who creates the attestations?



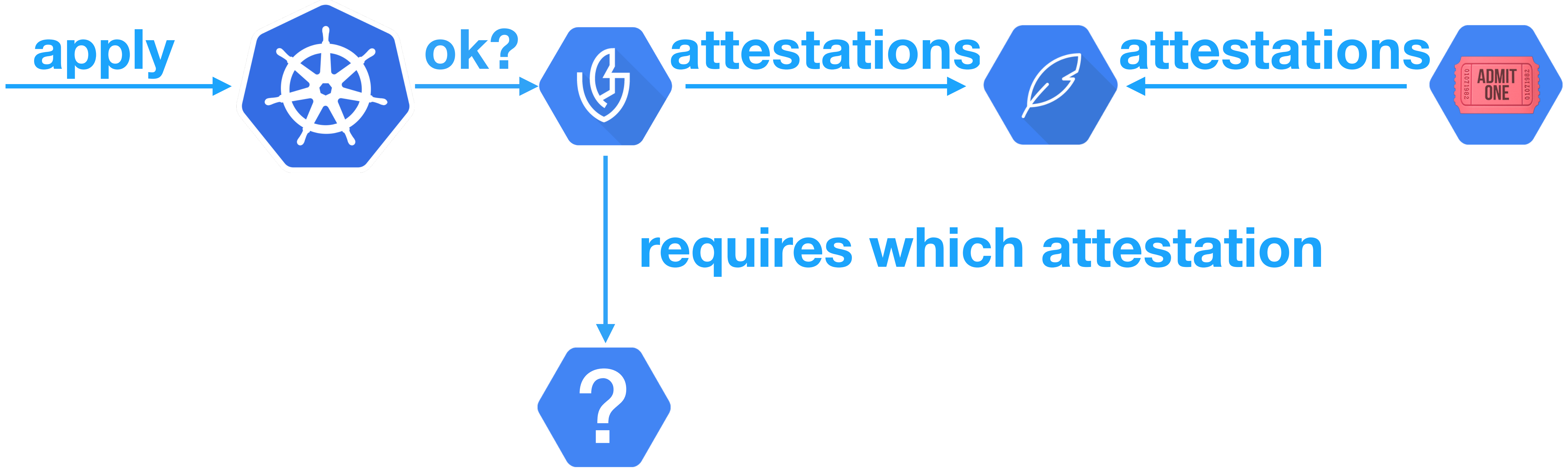
🎟️Voucher

github.com/shopify/voucher

Voucher runs checks



Which attestations are required?



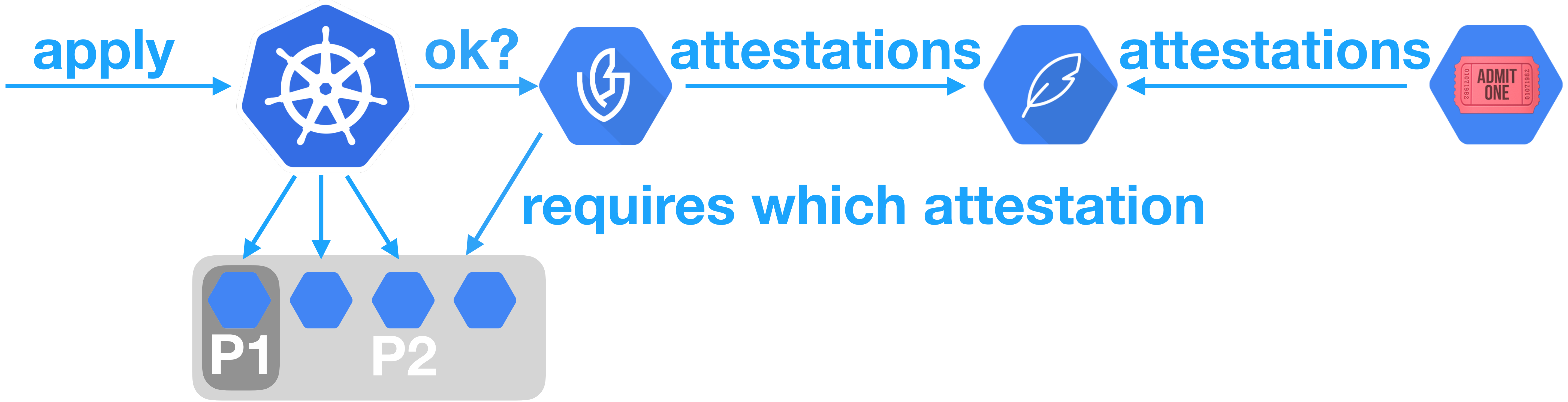
Policies

```
admissionWhitelistPatterns:
- namePattern: nginx/image:sha256…
defaultAdmissionRule:
  enforcementMode: ENFORCED_BLOCK_AND_AUDIT_LOG
  evaluationMode: REQUIRE_ATTESTATION
  requireAttestationsBy:
  - projects/binauthz/attestors/name
name: projects/shopify-security/policy
```

Policies

```
admissionWhitelistPatterns:
– namePattern: nginx/image:sha256…
clusterAdmissionRules:
  us-east1-a.cluster:
    evaluationMode: REQUIRE_ATTESTATION
    enforcementMode: ENFORCED_BLOCK_AND_AUDIT_LOG
    requireAttestationsBy:
    - projects/name/attestors/name
defaultAdmissionRule:
  enforcementMode: ENFORCED_BLOCK_AND_AUDIT_LOG
  evaluationMode: REQUIRE_ATTESTATION
  requireAttestationsBy:
  - projects/binauthz/attestors/name
name: projects/shopify-security/policy
```

Policies per project/cluster



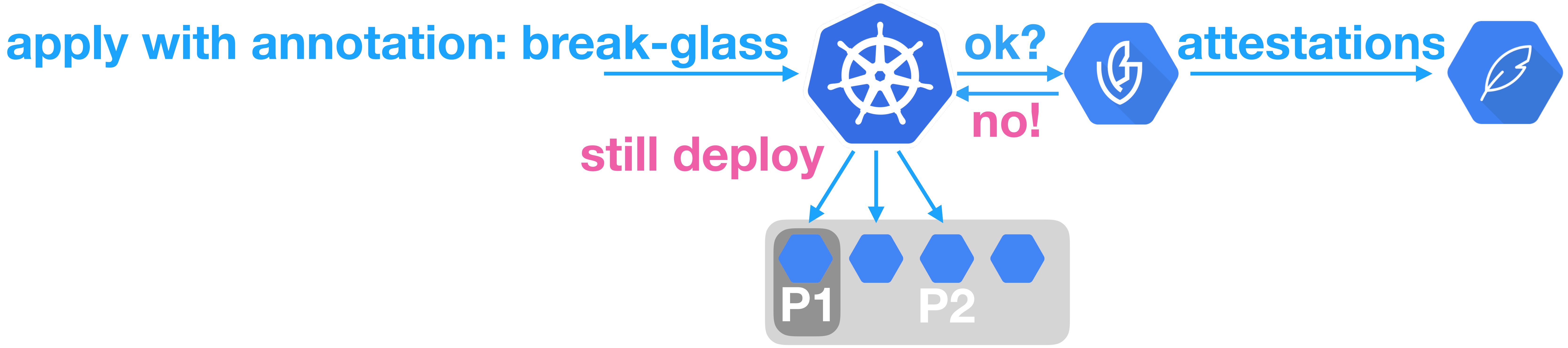
But what about emergencies?

That require changes right now!

Break-glass

```yaml
apiVersion: v1
kind: ReplicationController
metadata:
  name: break-glass
spec:
  replicas: 1
  selector:
    role: binary-authorization
  template:
    metadata:
      labels:
        role: binary-authorization
      annotations:
        alpha.image-policy.k8s.io/break-glass: "true"
    spec:
      containers:
      - name: binary-authorization
        image: gcr.io/somewhere/image@sha256:...
```

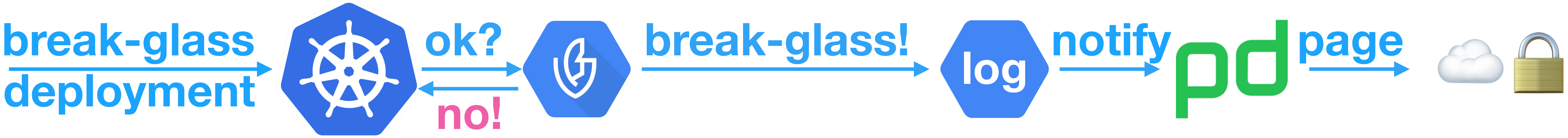
Break-glass


apply with annotation: break-glass
ok?
no!
attestations
still deploy
P1
P2

If everyone can just add break-glass…

… what is it good for?!

Page @cloudsec

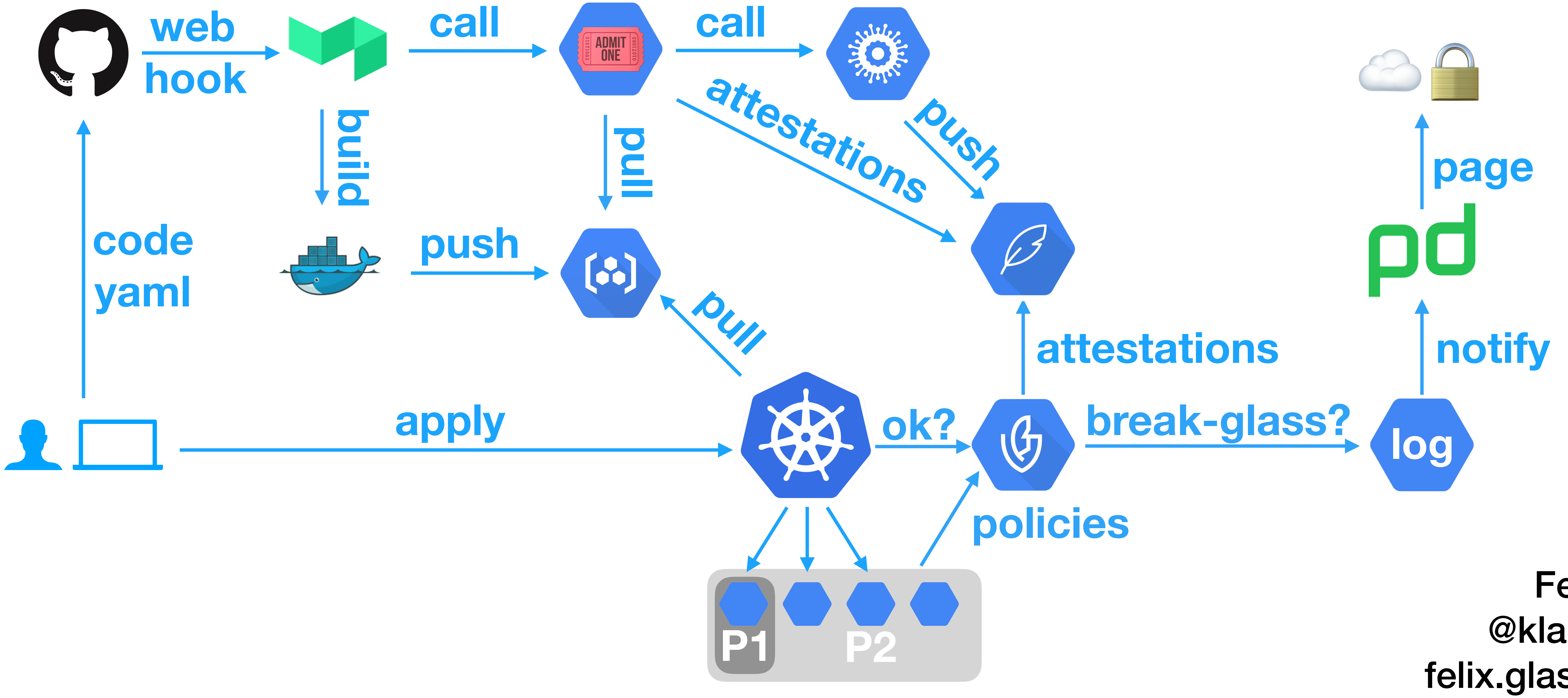


Are we secure yet?

Are we secure yet?

No, but we are much more secure!

Do you have any questions?



Felix Glaser
@klautcomputing
felix.glaser@shopify.com

Resources:

- https://github.com/Shopify/voucher
- https://github.com/grafeas/grafeas
- https://github.com/grafeas/kritis
- https://cloud.google.com/binary-authorization/docs/
- https://cloud.google.com/blog/products/identity-security/deploy-only-what-you-trust-introducing-binary-authorization-for-google-kubernetes-engine