Securing Shopify's PaaS on GKE

Jonathan Pulsifer

shopify

$ whoami

- Infrastructure Security Engineer @ Shopify
- Certified Kubernetes Administrator
- twitter.com/JonPulsifer
- github.com/JonPulsifer

Previously

- Team Lead at CFNOC
- Network Defense Instructor at CFSCE
- SANS Mentor / Co-instructor (GCIA, GSEC)

Jonathan Pulsifer

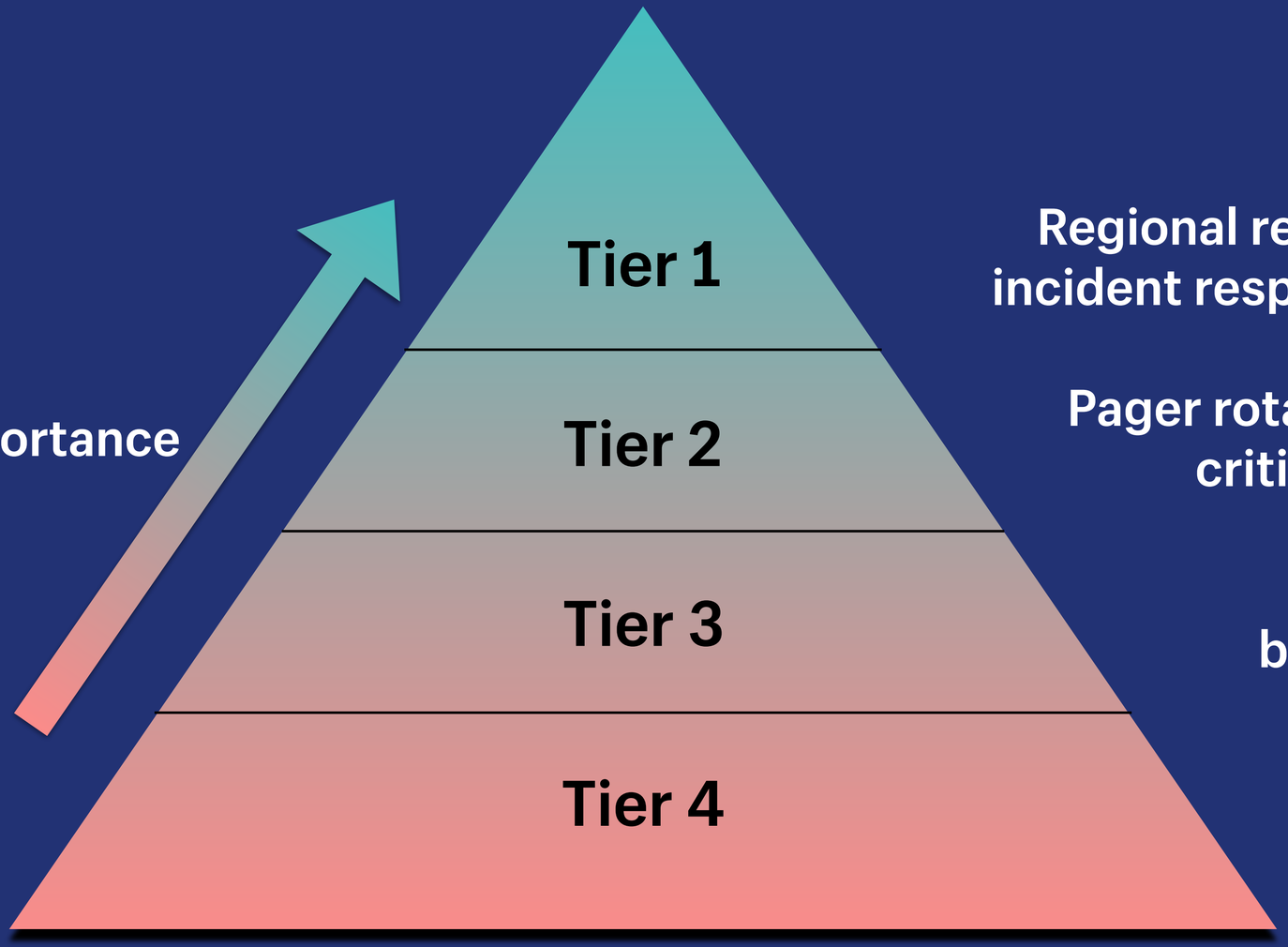
@JonPulsifer

Find me dropping container capabilities and working on security @Shopify || IT guy for @LawNeedsFem || CKA, GCIA, GSEC #kubernetes #cloudnative #treatyoself

Ottawa, ON

Services at Shopify

Service Tiers



More mature in SDLC

Greater business importance

Higher SLO

Earlier in SDLC

Regional redundancy, incident response drilling

Pager rotation, automated critical alerting

CI, Pingdom, backups, logging

Fewer requirements to encourage rapid prototyping

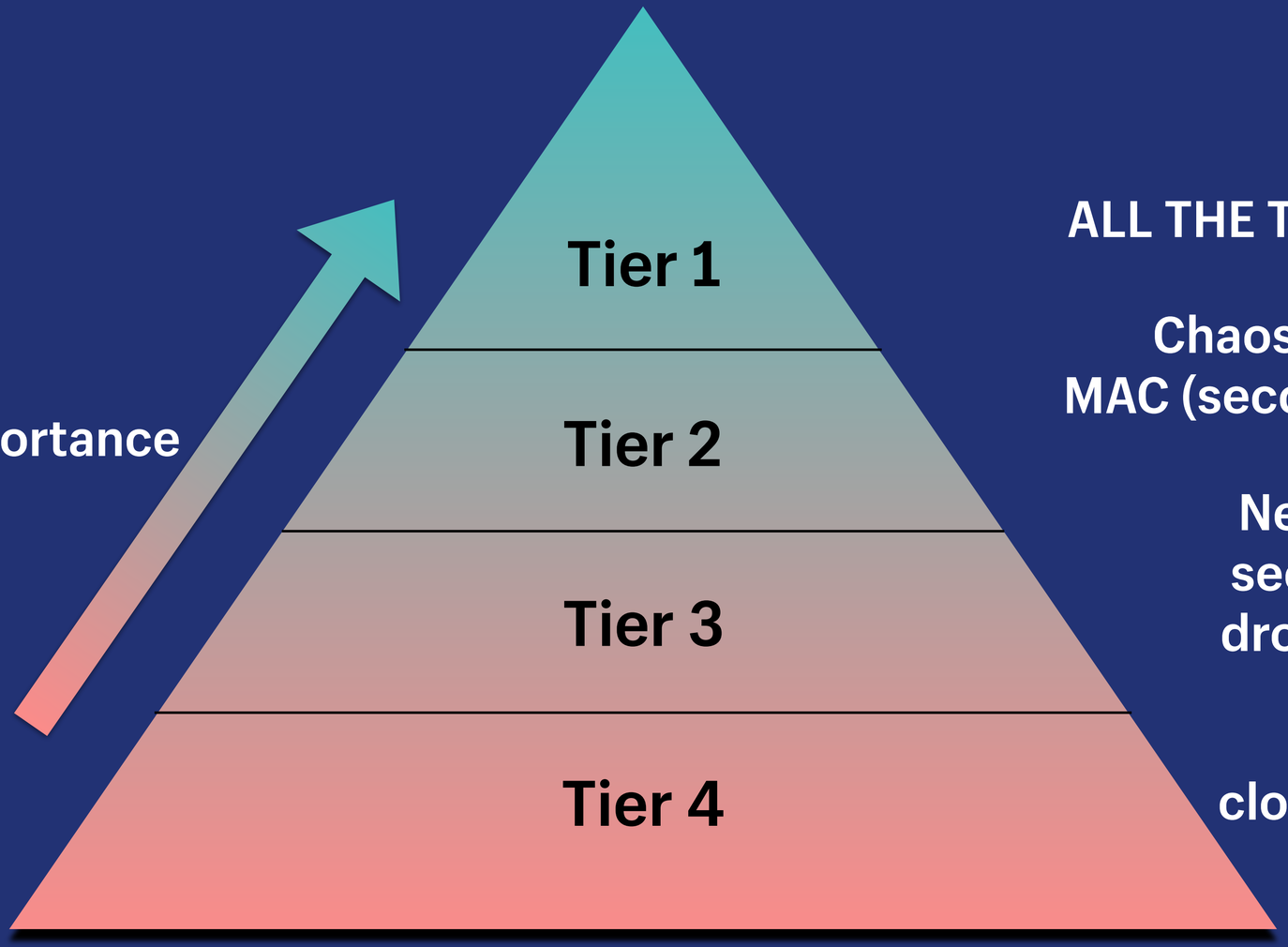
Security Tiers

More mature in SDLC

Greater business importance

Higher SLO

Earlier in SDLC



ALL THE THINGS!

Chaos engineering,
MAC (seccomp, AppArmor)

Network policies,
security contexts,
dropped privileges

Strict RBAC on
cloud resources and k8s,
Kritis attestations

Kubernetes Namespaces by Tier

35

Tier 1

50

Tier 2

70

Tier 3

175

Tier 4

* not all services run on GKE

Cloud Platform

Google Cloud Platform

500

Projects

15

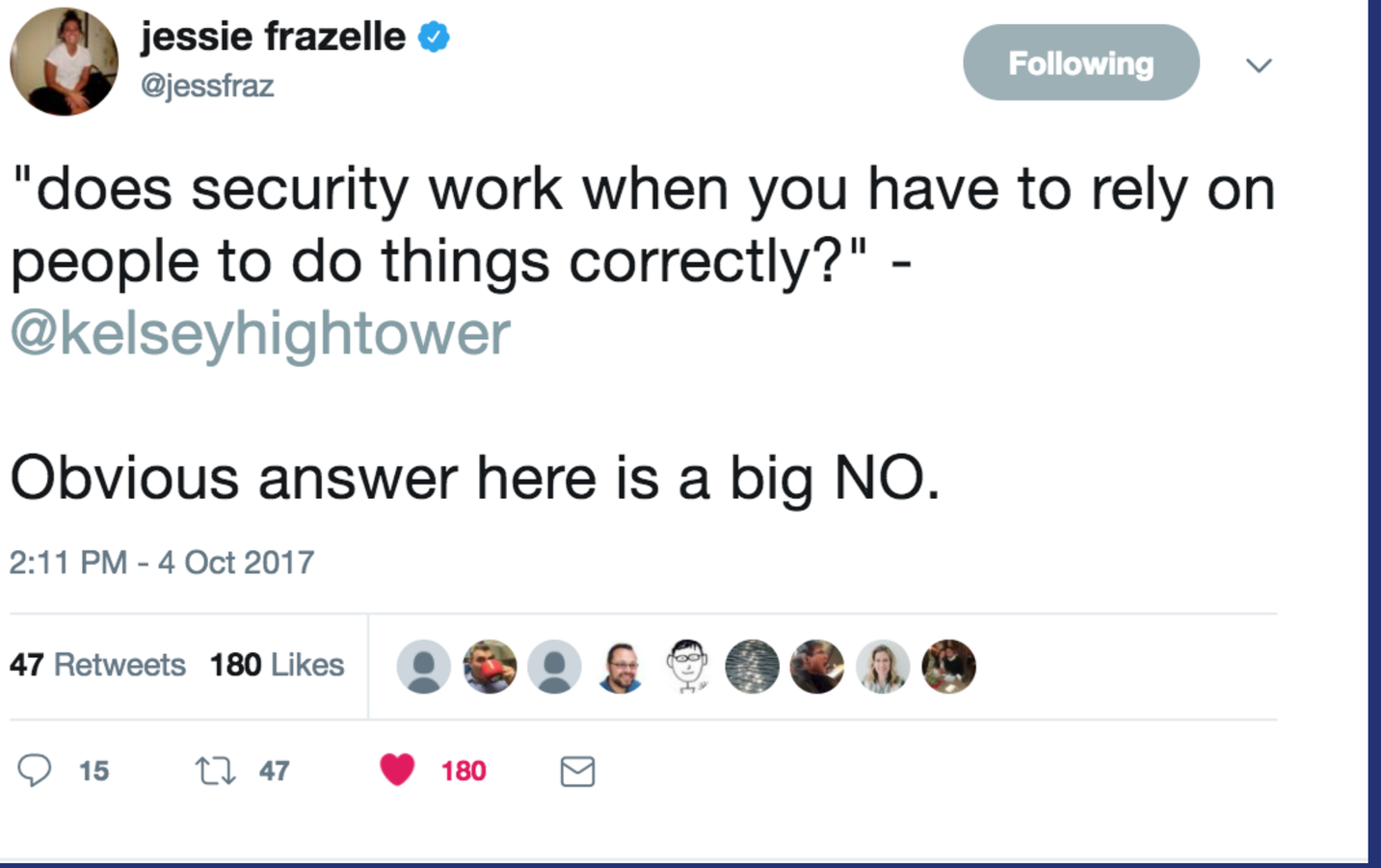
Folders

700

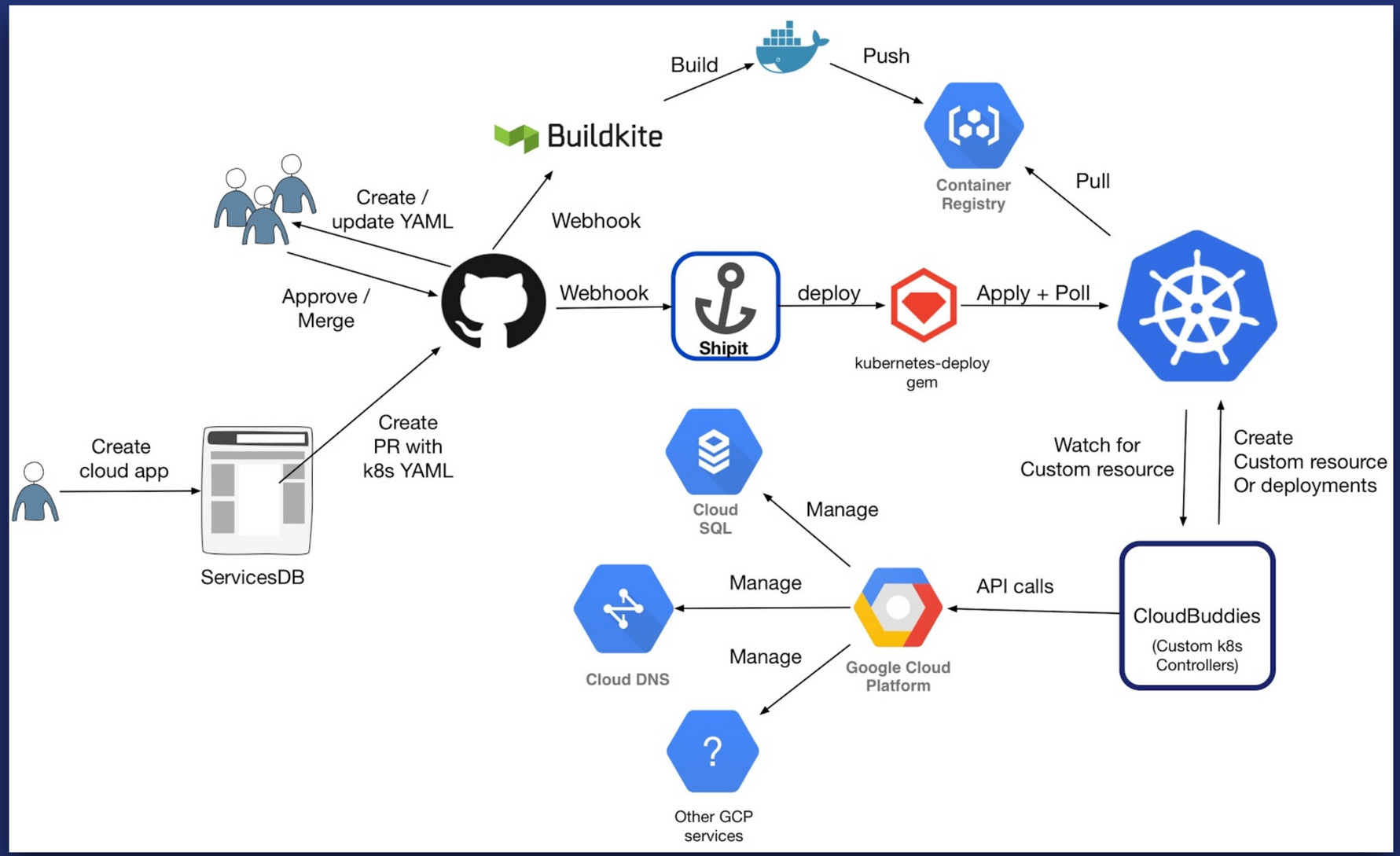
Google Groups

17

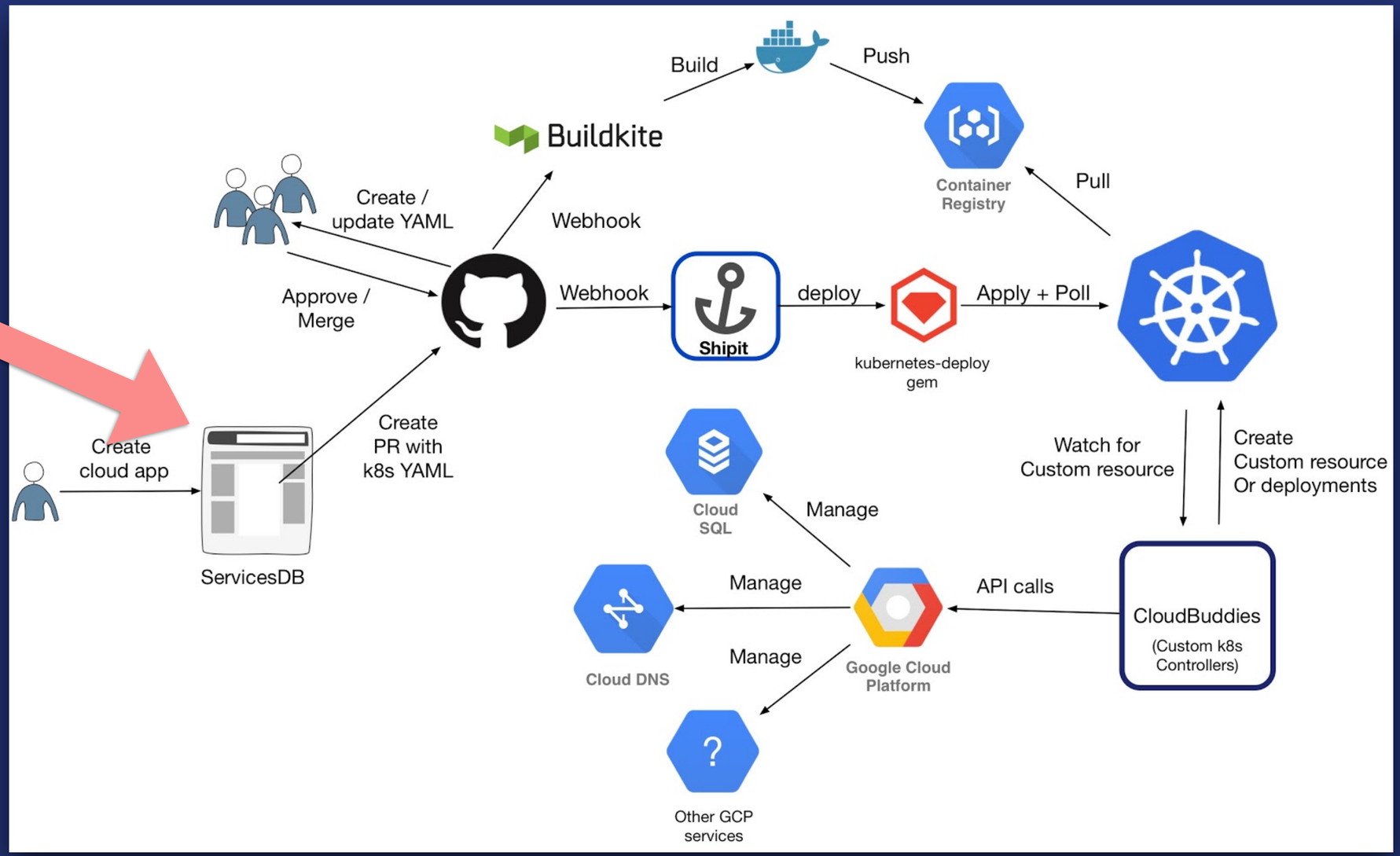
GKE Clusters


jessie frazelle
@jessfraz
Following
"does security work when you have to rely on people to do things correctly?" - @kelseyhightower
Obvious answer here is a big NO.
2:11 PM - 4 Oct 2017
47 Retweets 180 Likes
15
47
180

Cloud Platform Architecture



Cloud Platform Architecture



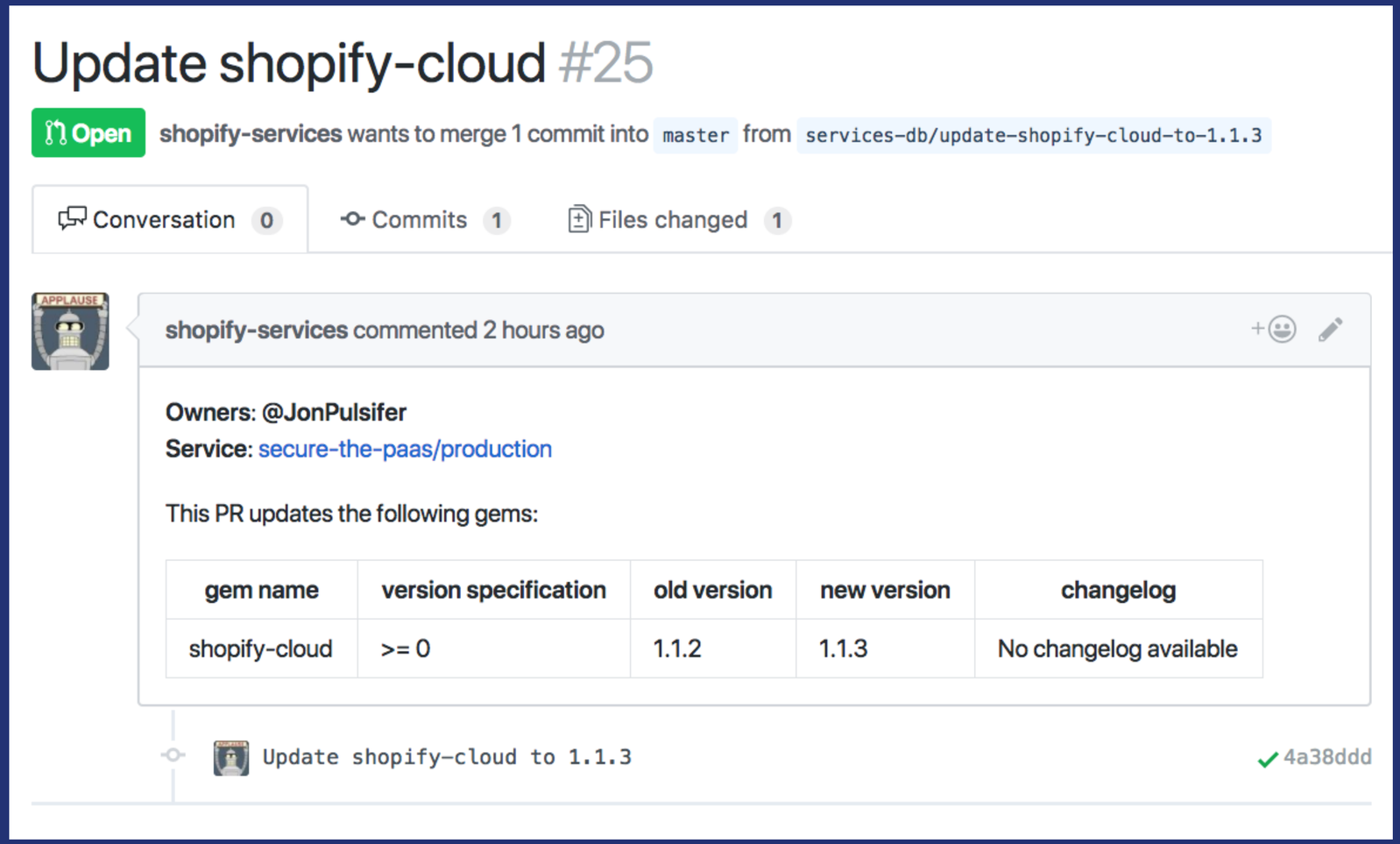
Services Automation

Services DB

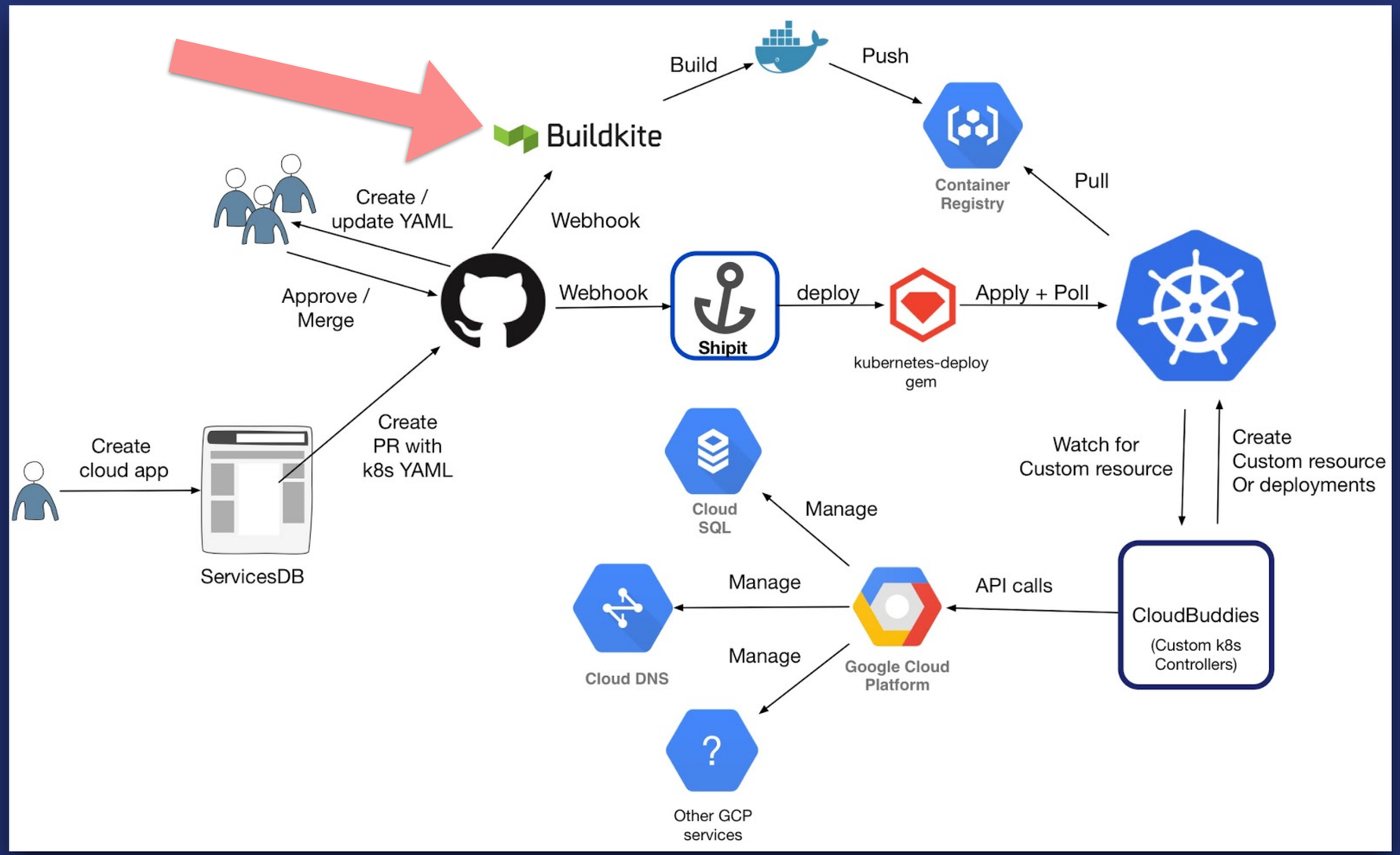
- Automatic patching!
- Generation and auditing of Kubernetes manifests
- Configures CI

Groundcontrol

- Creation and annotation of Kubernetes namespaces
- https://github.com/Shopify/ejson key pair creation
- GCP service account creation



Cloud Platform Architecture



Builder Stats

6,000

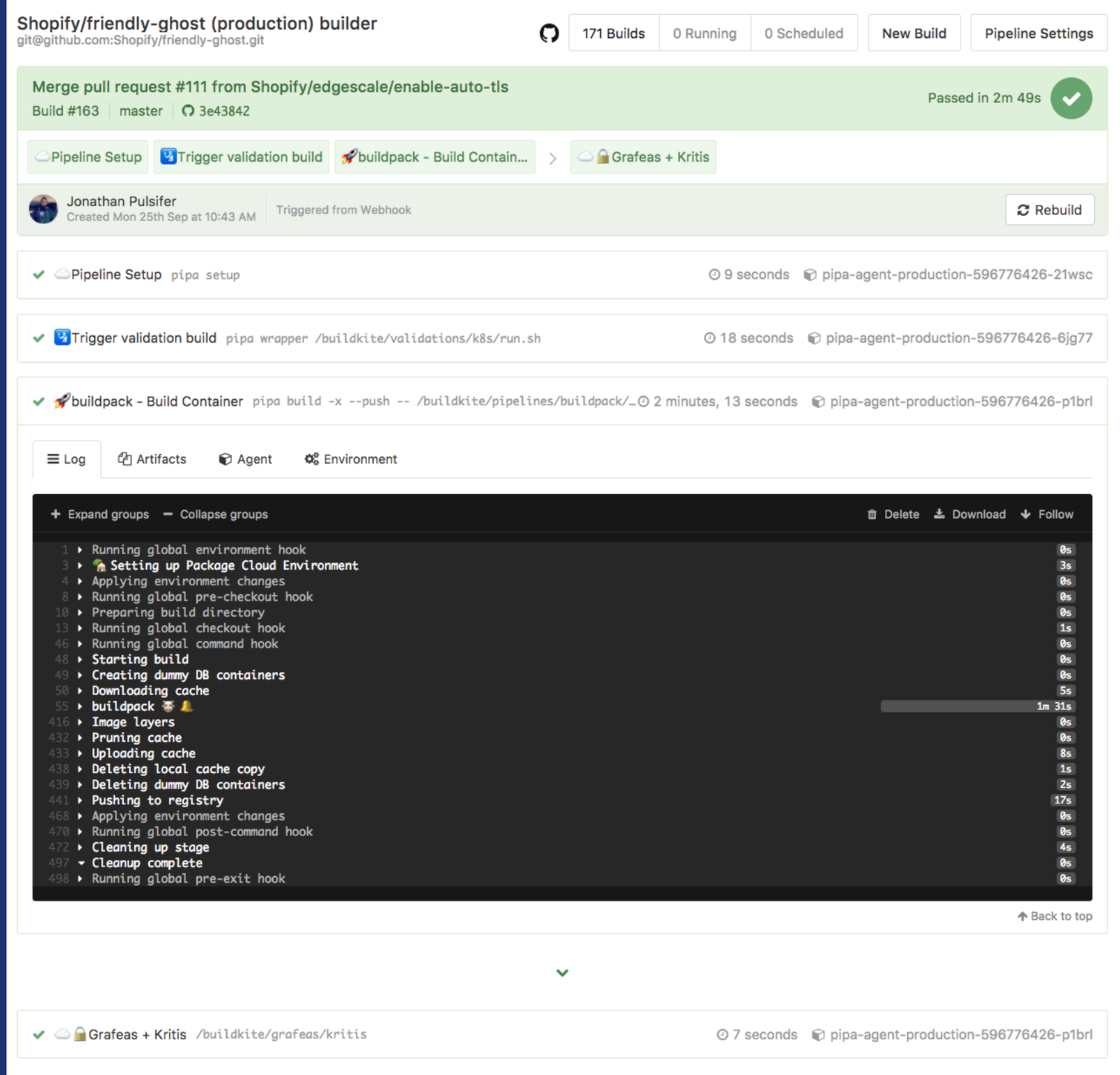
average builds per weekday

330,000

images in GCR

PIPA

- Buildpack, Dockerfile, or custom build pipelines
- Kubernetes template validation
- Container Audits:
  - does this image run as root?
  - does this image contain any vulnerable packages?
  - container attestations



Grafeas

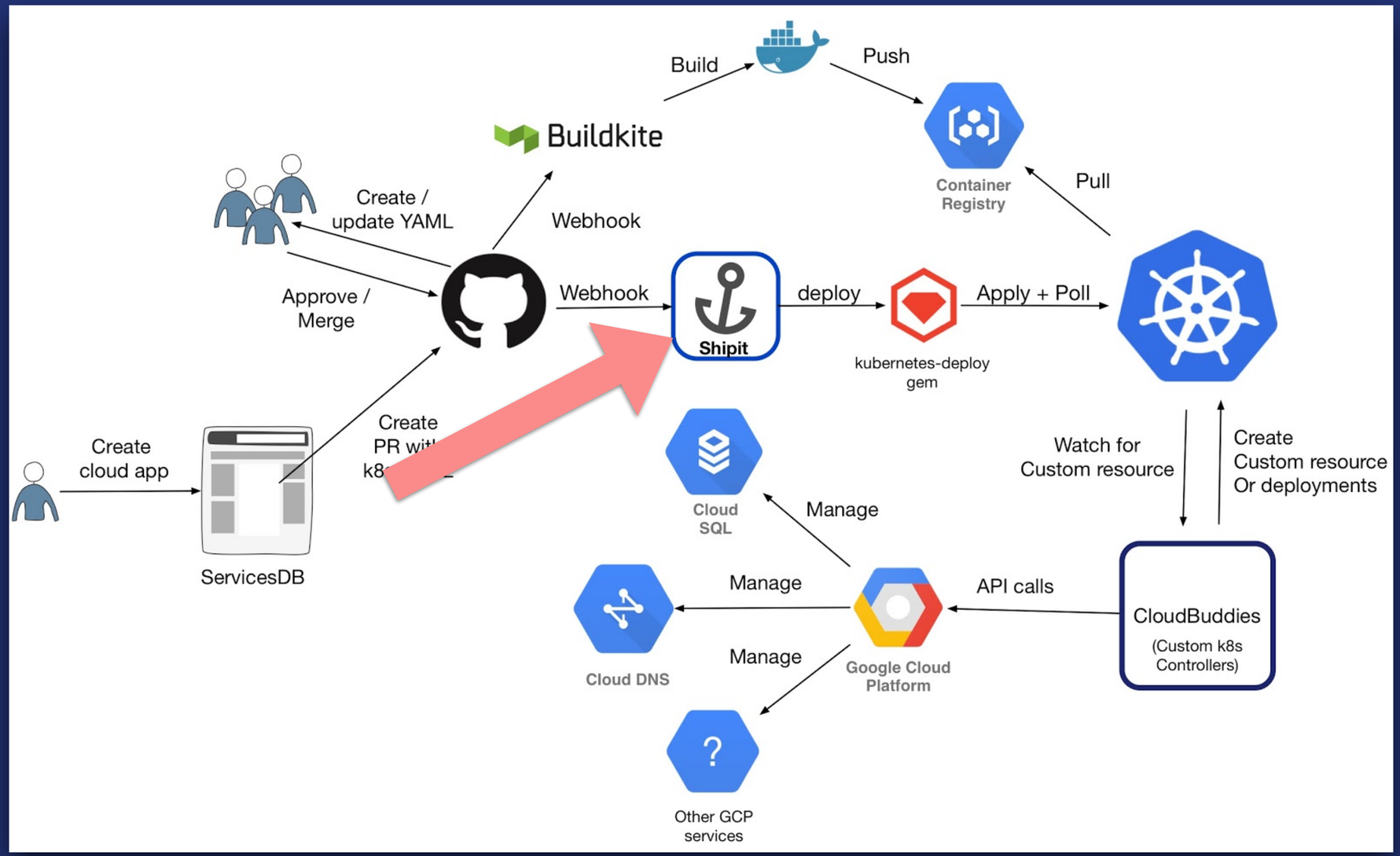
- https://github.com/Grafeas/Grafeas
- Central source of truth for software component metadata
- my.regist.ry/image@sha256:hash as key for containers
- Container notes produced at build
- See GCP's or Shopify's Engineering blog for more

Kritis

- Use metadata stored in Grafeas to create policies
- Real-time enforcement of policies on Kubernetes

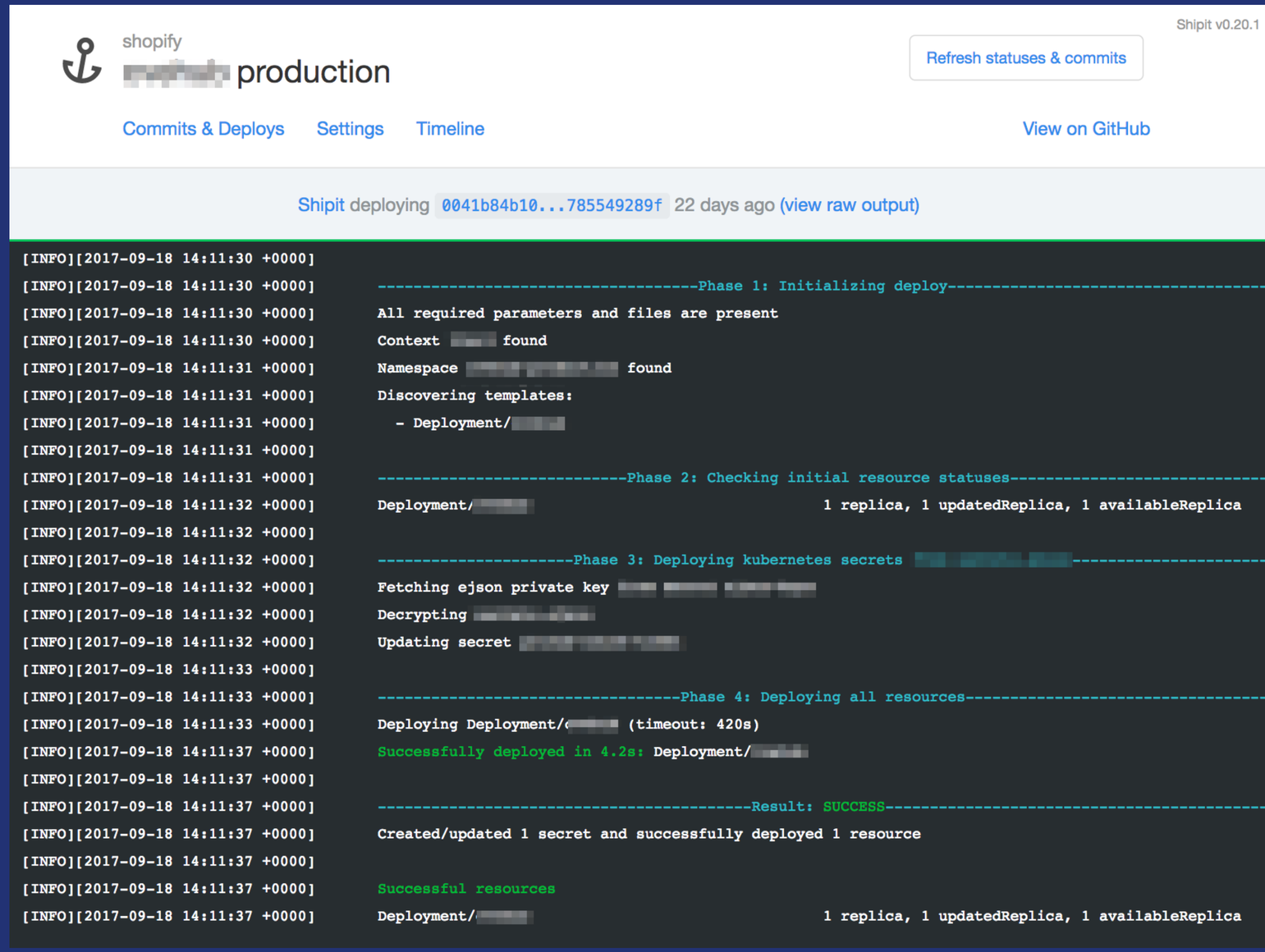

```
{
    "createTime": "2017-09-14T04:34:47.777125Z",
    "kind": "PACKAGE_VULNERABILITY",
    "name": "projects/myproject/occurrences/randomID",
    "noteName": "providers/myscanner/notes/CVE-2017-13036",
    "resourceUrl": "https://gcr.io/myproject/image@sha256:hash",
    "updateTime": "2017-09-14T04:34:47.777125Z",
    "vulnerabilityDetails": {
        "cvssScore": 7.5,
        "packageIssue": [
            {
                "affectedLocation": {
                    "cpeUri": "cpe:/o:canonical:ubuntu_linux:16.04",
                    "package": "tcpdump",
                    "version": {
                        "name": "4.9.0",
                        "revision": "1ubuntu1~ubuntu16.04.1"
                    }
                },
                "fixedLocation": {
                    "cpeUri": "cpe:/o:canonical:ubuntu_linux:16.04",
                    "package": "tcpdump",
                    "version": {
                        "name": "4.9.2",
                        "revision": "0ubuntu0.16.04.1"
                    }
                },
                "severityName": "LOW"
            }
        ],
        "severity": "HIGH"
    }
}
```

Cloud Platform Architecture

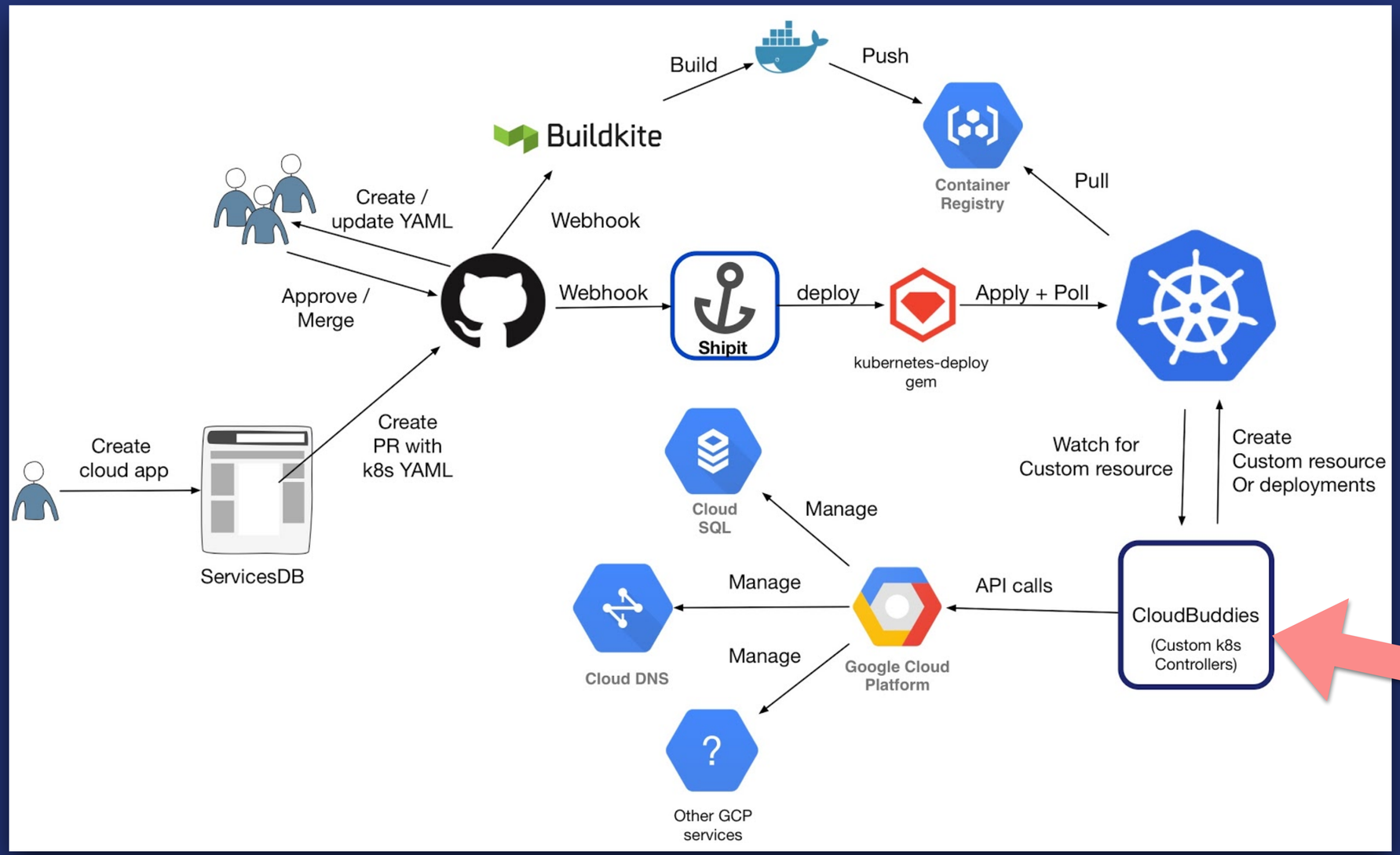


kubernetes-deploy

- github.com/Shopify/kubernetes-deploy
- github.com/Shopify/shipit-engine
- **Features:**
  - clear, actionable pass/fail result for each deploy
  - pre-deploy certain types of resources
  - decryption of EJSON to k8s secrets
  - protected namespaces



Cloud Platform Architecture



Cloudbuddies

- "Friendly Kubernetes controllers keeping the cloud fluffy"
- ~10 buddies per cluster
- Security automation!
- accountabilibuddy, bucketbuddy, netpolbuddy, rbacbuddy

kubeaudit

- github.com/Shopify/kubeaudit
- Audit Kubernetes security controls
- **Audits:**
  - automountServiceAccountToken
  - container images
  - network policies
  - security contexts
    - privileged containers
    - container capabilities too!

```
~  ☁  kubesec/cloudlab/secure-the-paas
› kubeaudit -l image -i nginx:1.13.5-alpine
ERRO[0000] Image tag was incorrect secure-the-paas/demo  tag=1.13.3-alpine type=deployment

~  ☁  kubesec/cloudlab/secure-the-paas
› kubeaudit -l sc privileged
ERRO[0000] kube-system/calico-node-vertical-autoscaler   type=deployment
ERRO[0000] kube-system/calico-typha                      type=deployment
ERRO[0000] kube-system/calico-typha-horizontal-autoscaler  type=deployment
ERRO[0000] kube-system/calico-typha-vertical-autoscaler  type=deployment
ERRO[0000] kube-system/calico-node                       type=daemonSet
ERRO[0000] kube-system/fluentd-gcp-v2.0                  type=daemonSet
ERRO[0000] kube-system/ip-masq-agent                     type=daemonSet
ERRO[0000] kube-system/event-exporter                    type=deployment
ERRO[0000] kube-system/heapster-v1.4.2                   type=deployment
ERRO[0000] kube-system/kube-dns                          type=deployment
ERRO[0000] kube-system/kube-dns-autoscaler               type=deployment
ERRO[0000] kube-system/kube-state-metrics                type=deployment
ERRO[0000] kube-system/kube-proxy-gke-cloudlab-main-b3a19cf7-sh8p  type=pod
ERRO[0000] kube-system/kube-proxy-gke-cloudlab-tini-4a6b7e3e-xz3l  type=pod
ERRO[0000] secure-the-paas/demo                          type=deployment

~  ☁  kubesec/cloudlab/secure-the-paas
› kubeaudit -f deployment.yaml sc
WARN[0000] Capabilities added to secure-the-paas/demo    caps="[NET_ADMIN SYS_PTRACE]" type=deployment
```

Continuous Security Monitoring

- **Nosy Bastard**
  - Scheduled scanning (Nessus, NMap, ZMap)
  - Discovery of cloud resources (AWS, Heroku, GCP)
  - Maps Kubernetes service accounts to RBAC roles
- **Forseti Security**
  - Comprehensive GCP inventorying
  - Enforcement of IAM policies
- **sshjanitor**
  - Discovery and deletion of stale project wide ssh keys (> 1h)

What's Missing?

Missing :(

- ~~API server logs~~ -- available in GKE >1.7.3 with Cloud Audit Logging
- ~~Network Policies~~ -- available in GKE >1.7.6 with Tigera's Calico
- PodSecurityPolicies + other admission control?
- IAM and RBAC synchronization
- GLBC configuration options for Identity Aware Proxy
- Container Identity (provisioning of identity by pod/container)

Thanks!

shopify