

Securing Shopify's PaaS on GKE

Jonathan Pulsifer



\$ 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

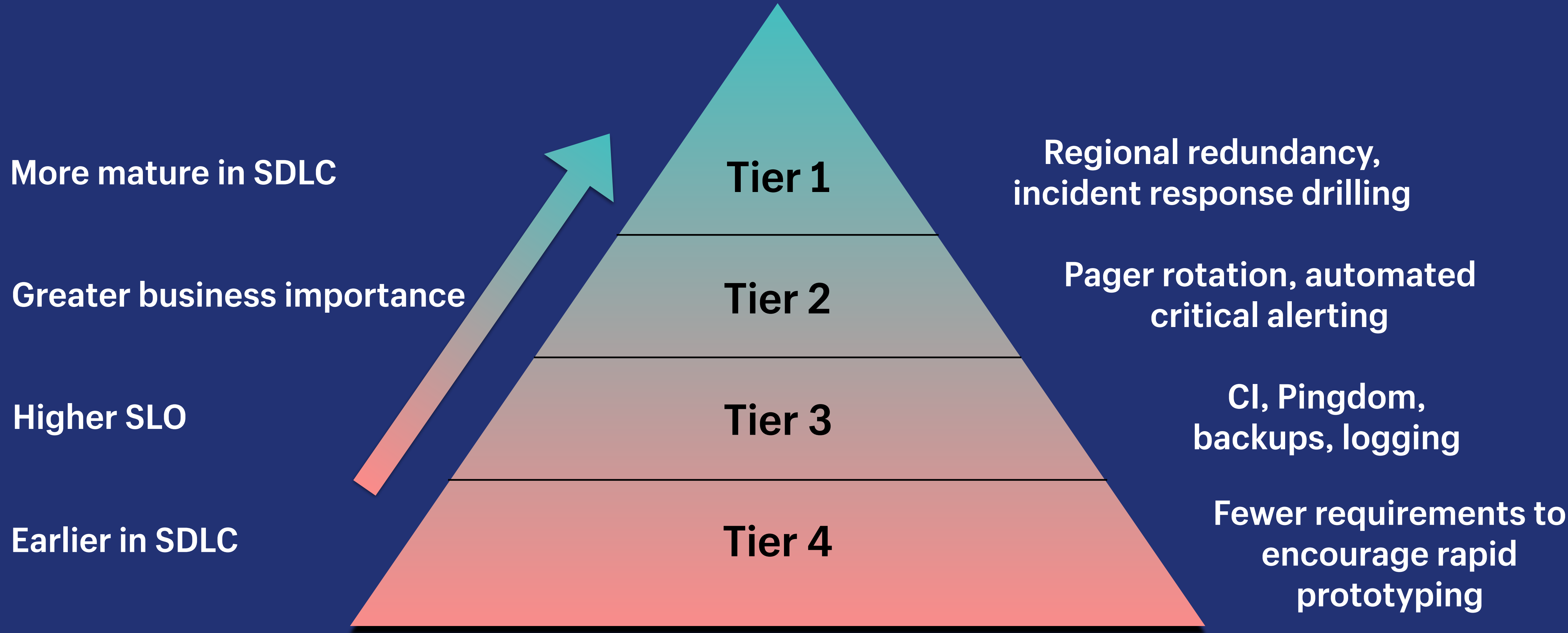
Find me dropping container capabilities and working on  security @Shopify || IT guy for @LawNeedsFem || CKA, GCIA, GSEC #kubernetes #cloudnative #treatyoself

📍 Ottawa, ON

Services at Shopify



Service Tiers



More mature in SDLC

Greater business importance

Higher SLO

Earlier in SDLC

Tier 1

Tier 2

Tier 3

Tier 4

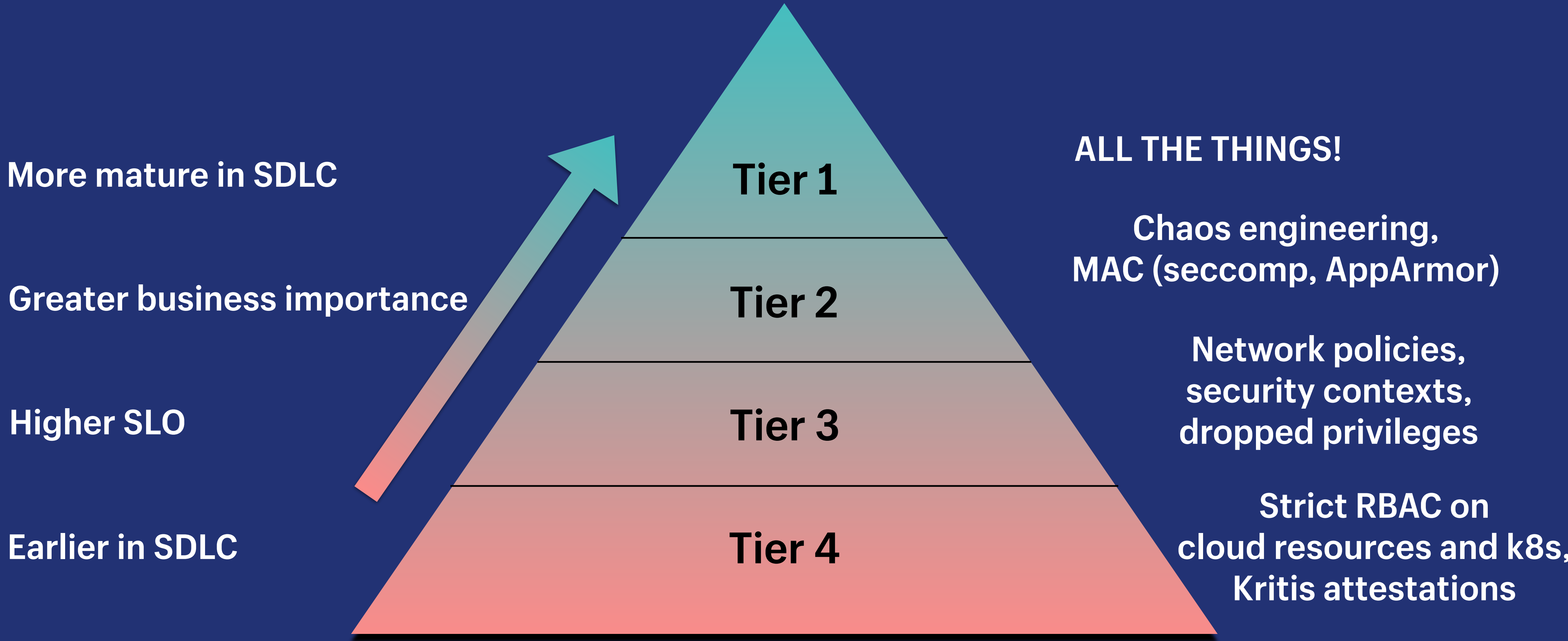
Regional redundancy,
incident response drilling

Pager rotation, automated
critical alerting

CI, Pingdom,
backups, logging

Fewer requirements to
encourage rapid
prototyping

Security Tiers



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



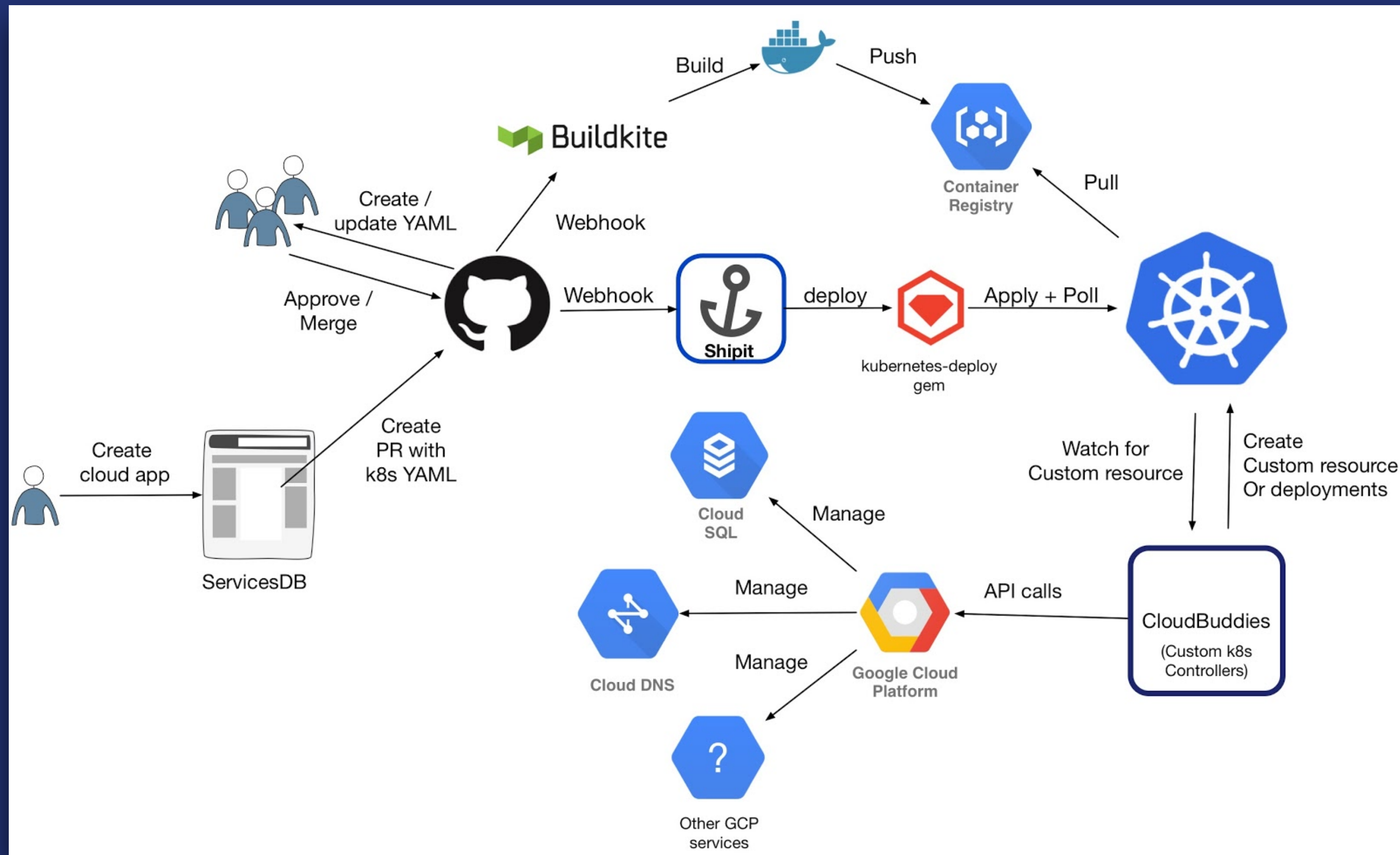
15

47

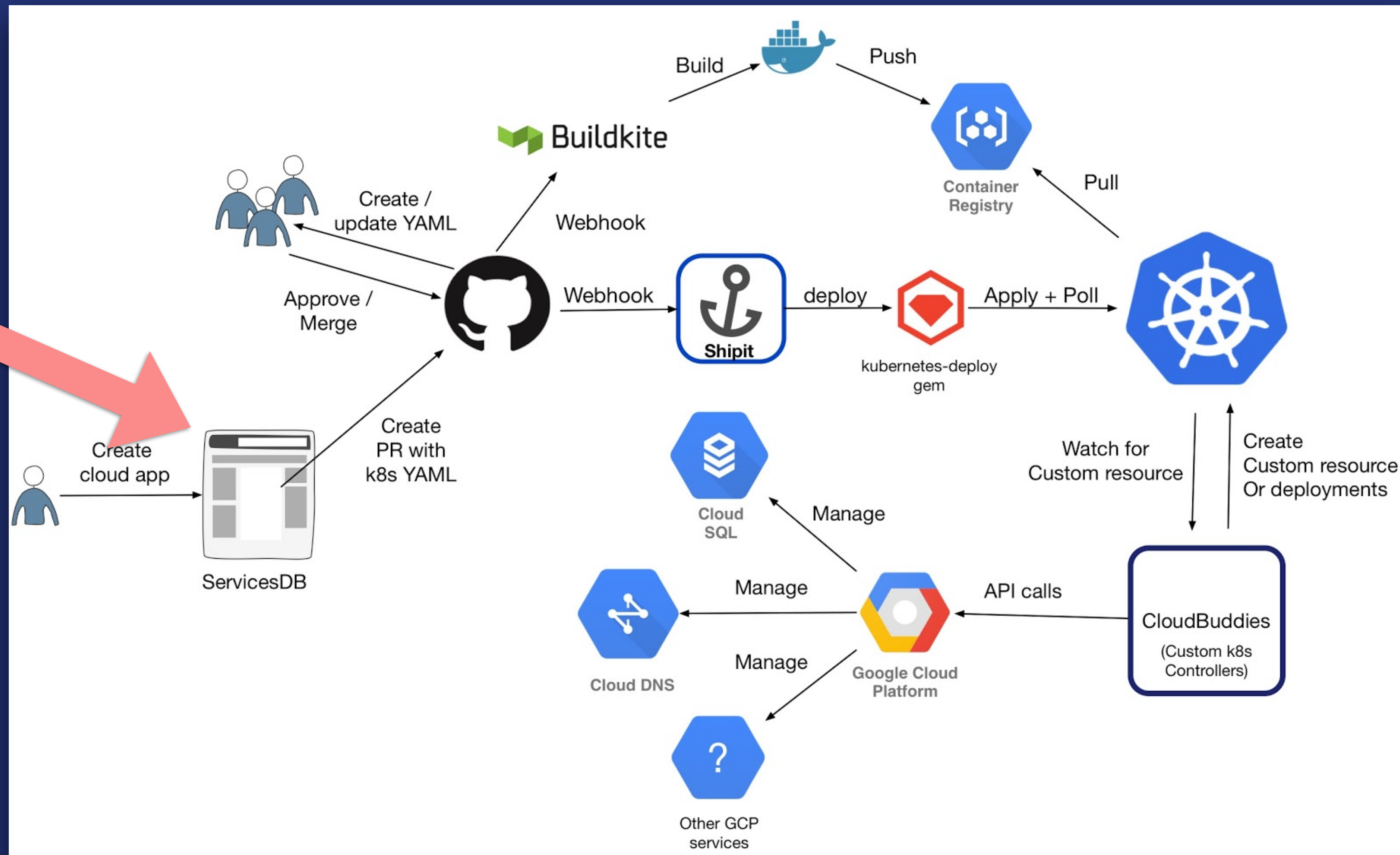
180



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

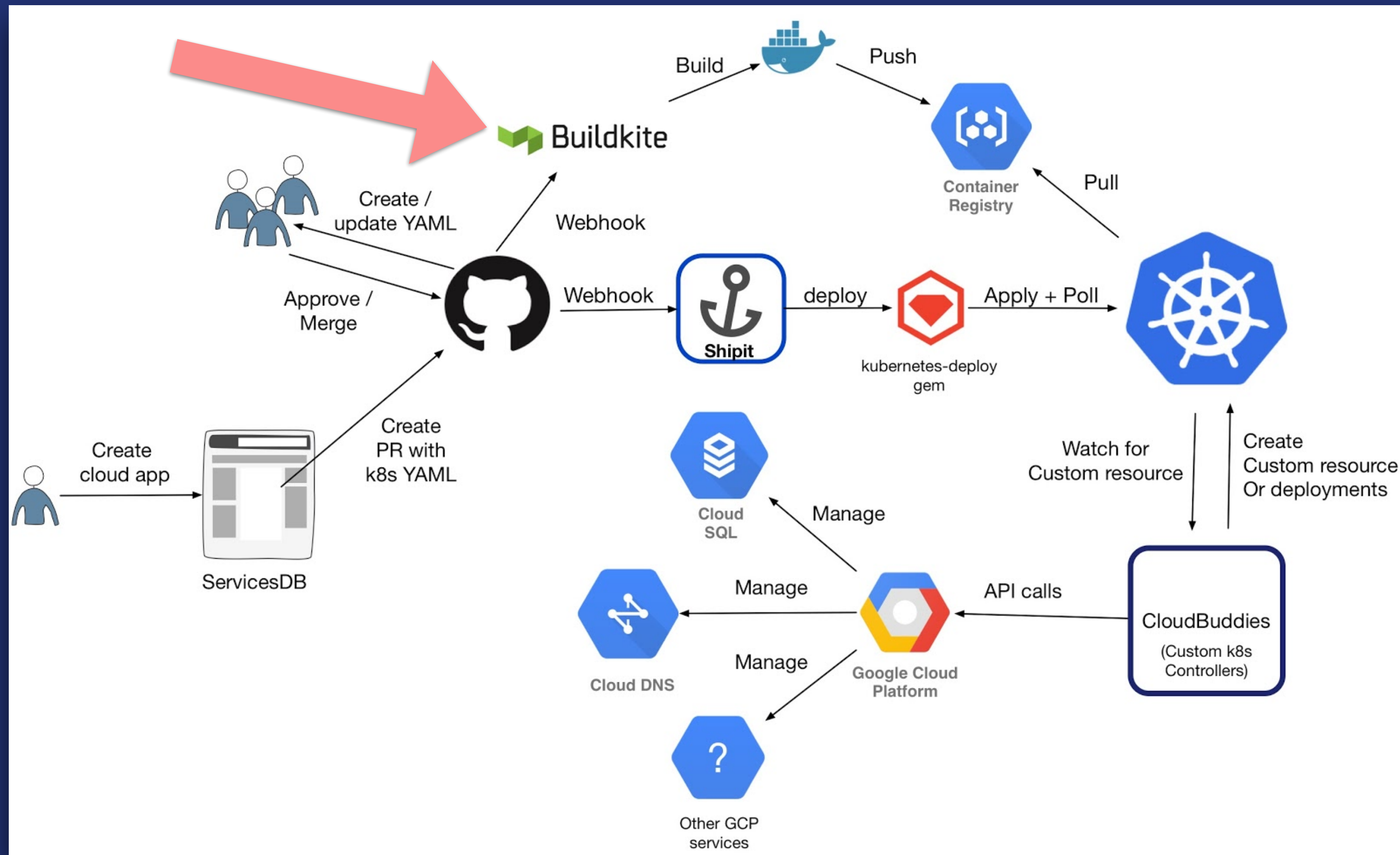
The screenshot shows a GitHub Pull Request titled "Update shopify-cloud #25". It indicates that "shopify-services" wants to merge 1 commit into the "master" branch from the branch "services-db/update-shopify-cloud-to-1.1.3". The PR has 0 conversations, 1 commit, and 1 file changed. A comment from "shopify-services" (with an "APPLAUSE" emoji) is visible, stating "commented 2 hours ago". The comment includes the following information:

- Owners: @JonPulsifer
- Service: [secure-the-paas/production](#)
- This PR updates the following gems:

gem name	version specification	old version	new version	changelog
shopify-cloud	>= 0	1.1.2	1.1.3	No changelog available

At the bottom of the PR, there is a commit entry: "Update shopify-cloud to 1.1.3" with a green checkmark and the commit hash "4a38ddd".

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



171 Builds

0 Running

0 Scheduled

New Build

Pipeline Settings

Merge pull request #111 from Shopify/edgescale/enable-auto-tls

Build #163 | master | 3e43842

Passed in 2m 49s



Pipeline Setup

Trigger validation build

buildpack - Build Contain...

Grafeas + Kritis



Jonathan Pulsifer

Created Mon 25th Sep at 10:43 AM

Triggered from Webhook

Rebuild

✓ Pipeline Setup pipa setup

9 seconds

pipa-agent-production-596776426-21wsc

✓ Trigger validation build pipa wrapper /buildkite/validations/k8s/run.sh

18 seconds

pipa-agent-production-596776426-6jg77

✓ buildpack - Build Container pipa build -x --push -- /buildkite/pipelines/buildpack/... 2 minutes, 13 seconds

pipa-agent-production-596776426-p1brl

Log

Artifacts

Agent

Environment

+ Expand groups - Collapse groups

Delete Download Follow

```
1 ▶ Running global environment hook 0s
3 ▶ Setting up Package Cloud Environment 3s
4 ▶ Applying environment changes 0s
8 ▶ Running global pre-checkout hook 0s
10 ▶ Preparing build directory 0s
13 ▶ Running global checkout hook 1s
46 ▶ Running global command hook 0s
48 ▶ Starting build 0s
49 ▶ Creating dummy DB containers 0s
50 ▶ Downloading cache 5s
55 ▶ buildpack 🐛🔔 1m 31s
416 ▶ Image layers 0s
432 ▶ Pruning cache 0s
433 ▶ Uploading cache 8s
438 ▶ Deleting local cache copy 1s
439 ▶ Deleting dummy DB containers 2s
441 ▶ Pushing to registry 17s
468 ▶ Applying environment changes 0s
470 ▶ Running global post-command hook 0s
472 ▶ Cleaning up stage 4s
497 ▶ Cleanup complete 0s
498 ▶ Running global pre-exit hook 0s
```

↑ Back to top

✓ Grafeas + Kritis /buildkite/grafeas/kritis

7 seconds

pipa-agent-production-596776426-p1brl



Grafeas

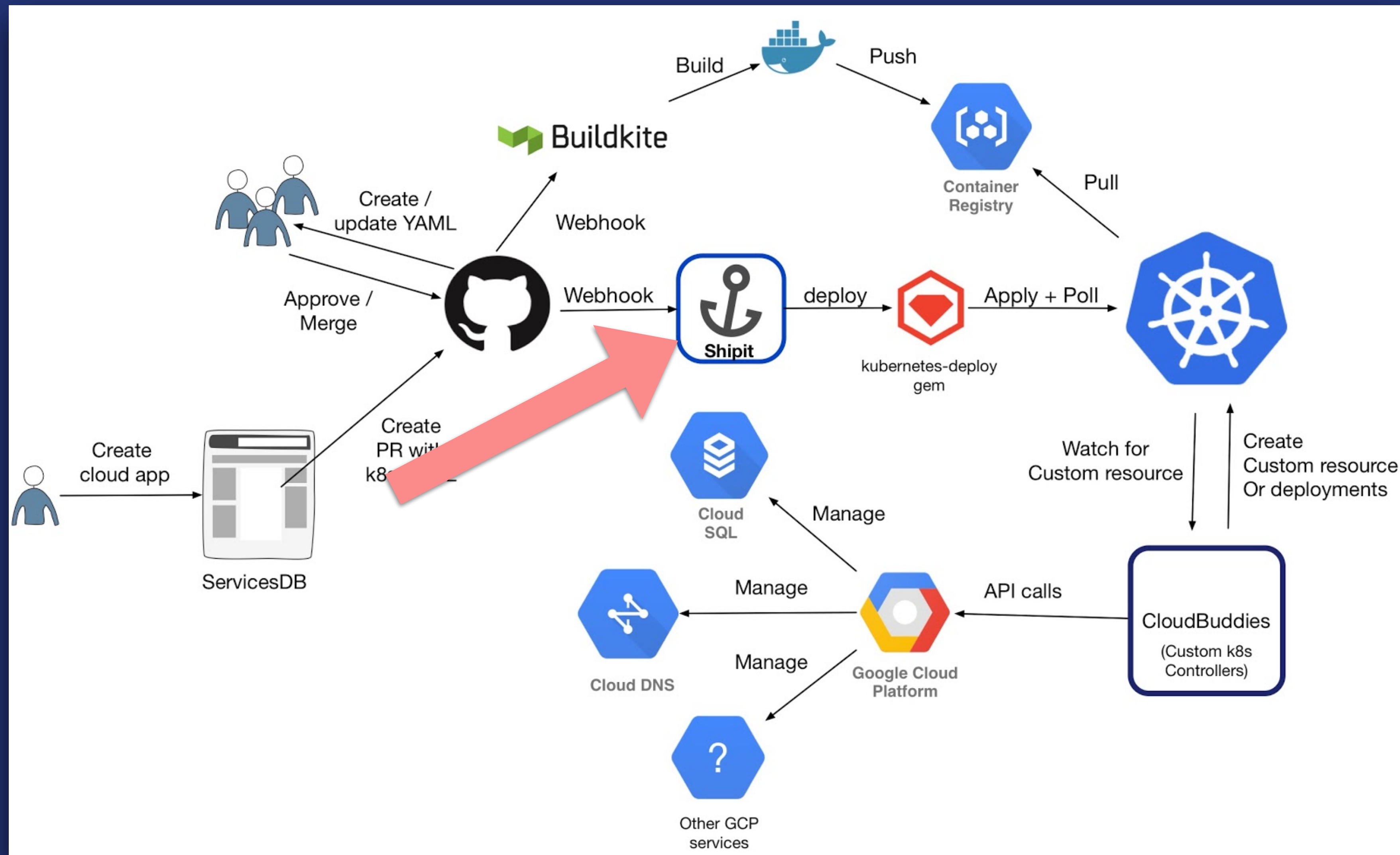
- <https://github.com/Grafeas/Grafeas>
- Central source of truth for software component metadata
- my.regist.ry/image@sha256:hash as key for containers
- Container notes produced at build
- See GCP's or Shopify's Engineering blog for more

Kritis

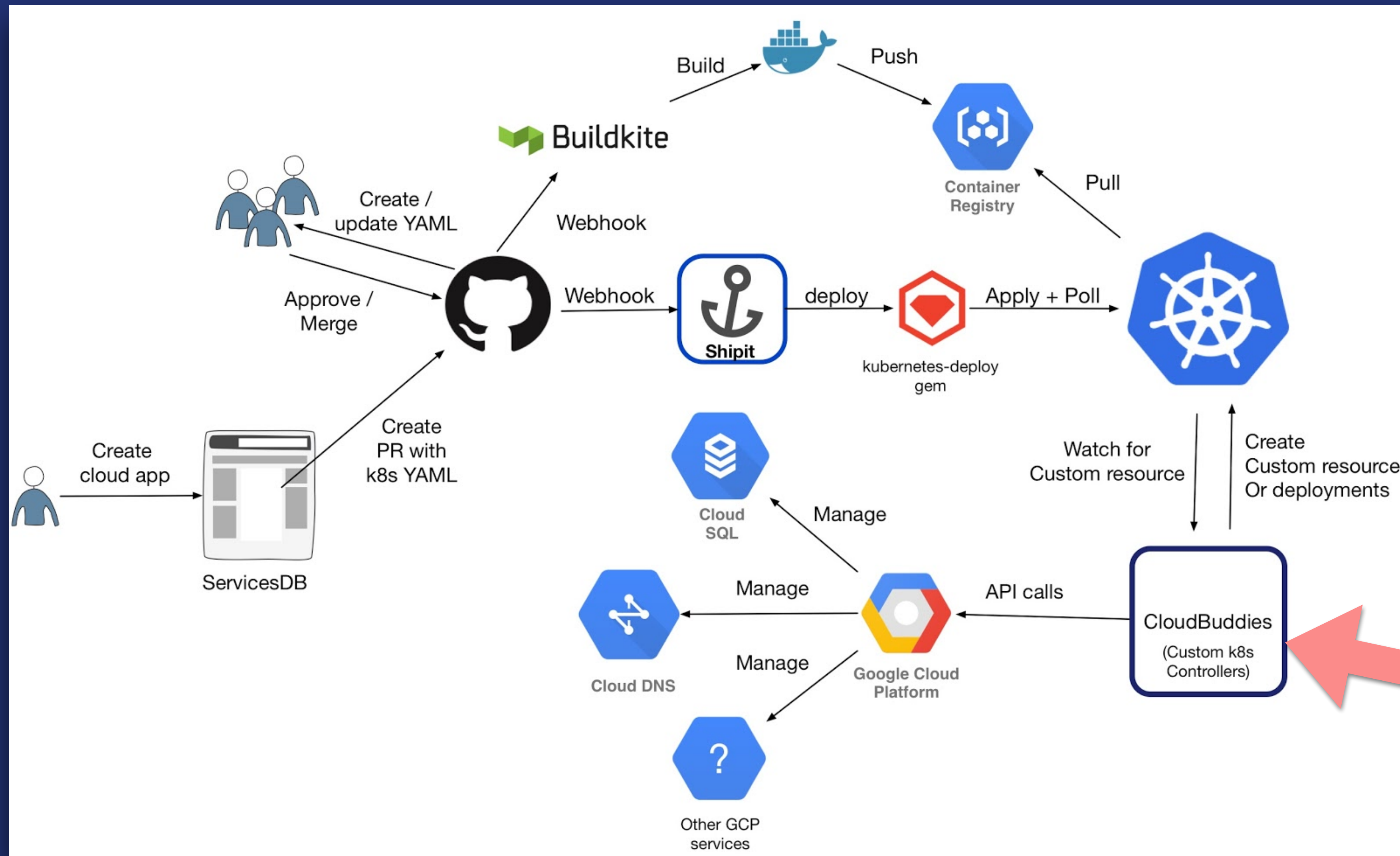
- Use metadata stored in Grafeas to create policies
- Real-time enforcement of policies on Kubernetes

```
1  {
2  "createTime": "2017-09-14T04:34:47.777125Z",
3  "kind": "PACKAGE_VULNERABILITY",
4  "name": "projects/myproject/occurrences/randomID",
5  "noteName": "providers/myscanner/notes/CVE-2017-13036",
6  "resourceUrl": "https://gcr.io/myproject/image@sha256:hash",
7  "updateTime": "2017-09-14T04:34:47.777125Z",
8  "vulnerabilityDetails": {
9    "cvssScore": 7.5,
10   "packageIssue": [
11     {
12       "affectedLocation": {
13         "cpeUri": "cpe:/o:canonical:ubuntu_linux:16.04",
14         "package": "tcpdump",
15         "version": {
16           "name": "4.9.0",
17           "revision": "1ubuntu1~ubuntu16.04.1"
18         }
19       },
20       "fixedLocation": {
21         "cpeUri": "cpe:/o:canonical:ubuntu_linux:16.04",
22         "package": "tcpdump",
23         "version": {
24           "name": "4.9.2",
25           "revision": "0ubuntu0.16.04.1"
26         }
27       },
28       "severityName": "LOW"
29     }
30   ],
31   "severity": "HIGH"
32 }
33 }
```


Cloud Platform Architecture



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!

```
~ 🌩️ kubesecc/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

~ 🌩️ kubesecc/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

~ 🌩️ kubesecc/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?

RENA
MONROVIA

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!

