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

Tier 1
- More mature in SDLC
- Greater business importance
- Higher SLO
- Regional redundancy, incident response drilling
- Pager rotation, automated critical alerting
- CI, Pingdom, backups, logging
- Fewer requirements to encourage rapid prototyping

Tier 2

Tier 3

Tier 4
- Earlier in SDLC

Security Tiers

Tier 1
- More mature in SDLC
- ALL THE THINGS!
  - Chaos engineering,
  - MAC (seccomp, AppArmor)

Tier 2
- Greater business importance
- Network policies,
  - security contexts,
  - dropped privileges

Tier 3
- Higher SLO
- Strict RBAC on
  - cloud resources and k8s,
  - Kritis attestations

Tier 4
- Earlier in SDLC
Kubernetes Namespaces by Tier

Tier 1: 35
Tier 2: 50
Tier 3: 70
Tier 4: 175

* not all services run on GKE
Cloud Platform
Google Cloud Platform

500
Projects

700
Google Groups

15
Folders

17
GKE Clusters
"does security work when you have to rely on people to do things correctly?" - @kelseyhightower

Obvious answer here is a big NO.
Cloud Platform Architecture
Cloud Platform Architecture

[Diagram showing the architecture of a cloud platform, including components such as Buildkite, Webhook, Shiptt, Container Registry, Kubernetes, and various services like Cloud SQL, Cloud DNS, and Google Cloud Platform.]
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](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](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
Cloud Platform Architecture

- Buildkite
  - Create / update YAML
  - Approve / Merge
  - Webhook

- Build
  - Push
  - Container Registry
  - Pull

- Webhook
  - Shipt
  - deploy
  - kubernetes-deploy
  - Apply + Poll
  - Watch for Custom resource
    - Create Custom resource
    - Or deployments

- Cloud SQL
- Manage

- Cloud DNS
- Manage

- Google Cloud Platform
- API calls

- CloudBuddies
  - (Custom k8s Controllers)

- ServicesDB
- Create cloud app

- Other GCP services
kubernetes-deploy

- [github.com/Shopify/kubernetes-deploy](https://github.com/Shopify/kubernetes-deploy)
- [github.com/Shopify/shipit-engine](https://github.com/Shopify/shipit-engine)

**Features:**
- clear, actionable pass/fail result for each deploy
- pre-deploy certain types of resources
- decryption of EJJSON to k8s secrets
- protected namespaces
Cloudbuddies

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

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

```bash
$ kubectl get image -l nginx:1.13.5-alpine
ERR[0000] Image tag was incorrect secure-the-paas/demo tag=1.3.3-alpine type=deployment

$ kubectl get image -l sc privileged
ERR[0000] kube-system/calico-node-vertical-autoscaler type=deployment
ERR[0000] kube-system/calico-typo type=deployment
ERR[0000] kube-system/calico-typha type=deployment
ERR[0000] kube-system/calico-typha-horizontal-autoscaler type=deployment
ERR[0000] kube-system/calico-typha-vertical-autoscaler type=deployment
ERR[0000] kube-system/calico-node type=daemonSet
ERR[0000] kube-system/fluentd-gcp-v2.0 type=daemonSet
ERR[0000] kube-system/ip-masq-agent type=daemonSet
ERR[0000] kube-system/event-exporter type=deployment
ERR[0000] kube-system/heapster-v1.4.2 type=deployment
ERR[0000] kube-system/kube-dns type=deployment
ERR[0000] kube-system/kube-dns-autoscaler type=deployment
ERR[0000] kube-system/kube-state-metrics type=deployment
ERR[0000] kube-system/kube-proxy-gke-cloudlab-main-b3a19cf7-sh8p type=pod
ERR[0000] kube-system/kube-proxy-gke-cloudlab-tini-4a6b7e3e-xz31 type=pod
ERR[0000] secure-the-paas/demo type=deployment

$ kubectl get image -f deployment.yaml -l 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!