



DevOps All The Things:

Creating a Pipeline to Validate Your OPA Policies

Goran Osim
Karpagam Balan

Intro



KubeCon



CloudNativeCon

North America 2020

Virtual



Karpagam Balan

Senior Lead Technologist
Booz Allen Hamilton

Likes: Spy movies, spicy food
and everything Open Source



Goran Osim

Senior Lead Technologist
Booz Allen Hamilton

Likes: Corgis, Ramen,
sometimes Kubernetes

Open Policy Agent

- Open Source, general-purpose policy engine
- Rego: High-level declarative language
 - Policy as Code
 - Decouple policy decision-making from policy enforcement



Open Policy Agent

```
package kubernetes.admission

deny[msg] {
  input.request.kind.kind == "Pod"
  image := input.request.object.spec.containers[_].image
  not startswith(image, "hooli.com/")
  msg := sprintf("image '%v' comes from untrusted registry", [image])
}
```

- DevOps **Every** Step of the Software Lifecycle
 - Development – On your Local
 - Testing – In the Pipeline
 - Deployment – In the cluster
- Our Toolbelt
 - Konstraint
 - Conftest
 - Pre-Commit Hooks

Demo



Recap

- Centralized Rego Policies
- Automating the creation of Constraints & Constraint Templates from Rego Policies
- Validating the Policies within the Cluster
- Pre-Commit Hooks validating input to source code repository

What's Next?

- Integrate with Software Development Environment
- Terratest – Ephemeral Clusters

Questions?

