


# Wprowadzenie do Policy-as-Code z Open Policy Agent



Wojciech Barczyński, VP of Engineering  
[wojciechb@spacelift.io](mailto:wojciechb@spacelift.io)

# Problem

Chasing the rabbit:

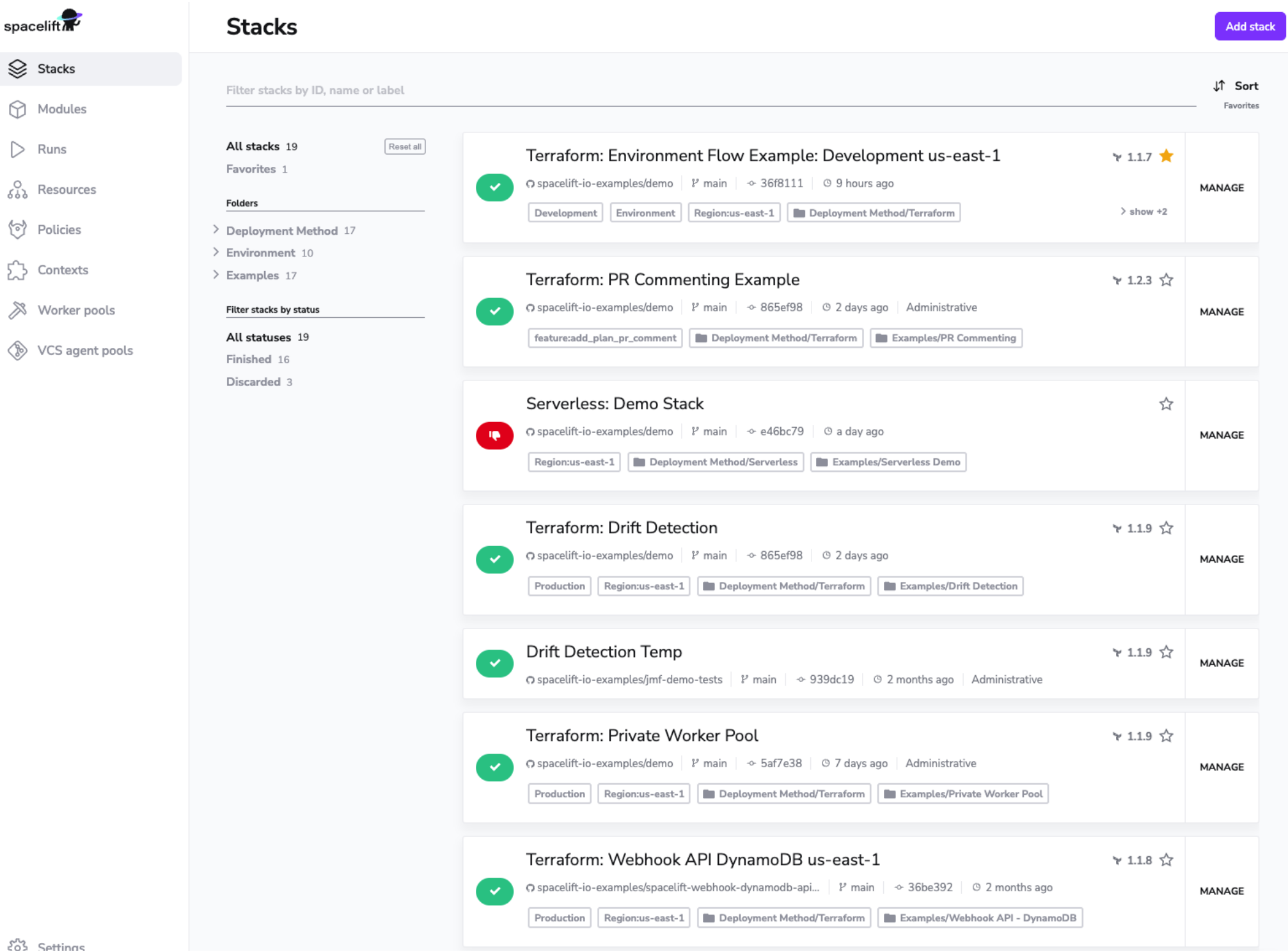
- Polityki
- Punkty decyzyjne
- Konfiguracje
- + bezpieczne 



# Building your own app

Spacelift.io:

- SaaS
- IaC as a Code
- Power users



# **DX, Platform, infra teams**

- Wymuszenie najlepszych praktyk
- Zaproszenie zespołów do kontrybucji

# Potencjalne rozwiązania

- Endless forms
- Markup language

# Potencjalne rozwiązania

- Scripting language embedded

# Policy as-a-code

- Dedykowany język z gwarancjami bezpieczeństwa
- Działa na loosely structured data
- wsparcie dla JSONu



# Open Policy Agent



Created by



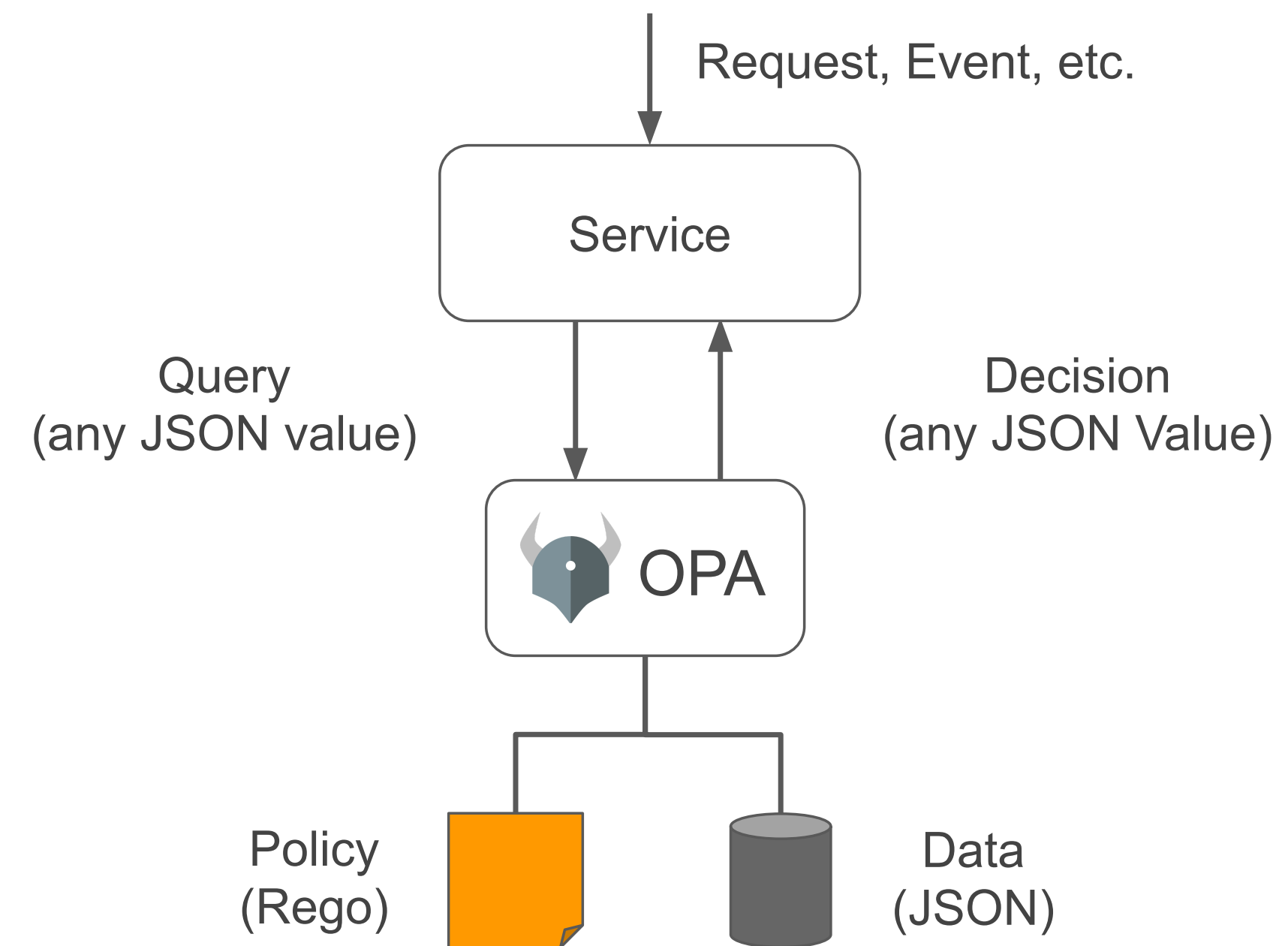
[openpolicyagent.org](https://openpolicyagent.org)





# Open Policy Agent

- 1. Rego ✓
- 2. loosely structured data ✓
- 3. JSON ✓



# Demo

[play.openpolicyagent.org](https://play.openpolicyagent.org)

# Demo

Input (aplikacja):

```
{  
  "session": {  
    "login": "natalia@example.com",  
    "teams": ["DevOps"],  
    "member": true  
  }  
}
```

# Demo

## Policy:

```
package talk_opa
teams := input.session.teams

admin { teams[_] == "DevOps" }
allow { teams[_] == "Engineering" }
deny  { not input.session.member }
```

# Rego

- Czytelny i łatwiejszy do pracy dla nie-programistów\*;
- Deklaratywny;
- Zainspirowany **Datalog**

# Rego

- Rozbudowany ze wsparciem dla dowolnych ustrukturyzowanych dokumentów;
- Build-in functions;



# Rego

- Obcy kod uruchamiany w bezpieczny sposób:
  - nie Turing-complete (nie ma pętli ani instrukcji warunkowych);
  - gwarancja zakończenia;
  - zapewnia, że zapytania są poprawne i nie wieloznaczne.

# Demo

Data - global values:

```
{  
  "maintenance": false,  
  "region": "eu-west-1"  
}
```

# Ecosystem



Kubernetes  
Admission Control



HashiCorp  
**Terraform**

Terraform Policy



Container Network  
Authorization with  
Envoy



Authorization for Java  
Spring Security



Styra Declarative  
Authorization Service



Container Network  
Authorization with  
Istio (at the Edge)



Strimzi (Apache Kafka  
on Kubernetes)



**kafka**

Kafka Topic  
Authorization



Custom Application  
Authorization



Permit.io



HTTP API  
Authorization in PHP



Fairwinds Insights  
Configuration  
Validation Software



**Kubescape**  
By ARM0

Kubescape  
Kubernetes security  
posture scanner



Kubernetes  
Authorization



**ceph**

Ceph Object Storage  
Authorization



OPAL (Open Policy  
Administration Layer)



**SPIRE**

SPIRE



AWS CloudFormation  
Hook

# Checkers & linters

Kubernetes, Terraform, i wile innych:

- [conftest](#)
- [kics.io](#)

# Checkers & linters

## conftest

```
package main

import data.kubernetes

name = input.metadata.name

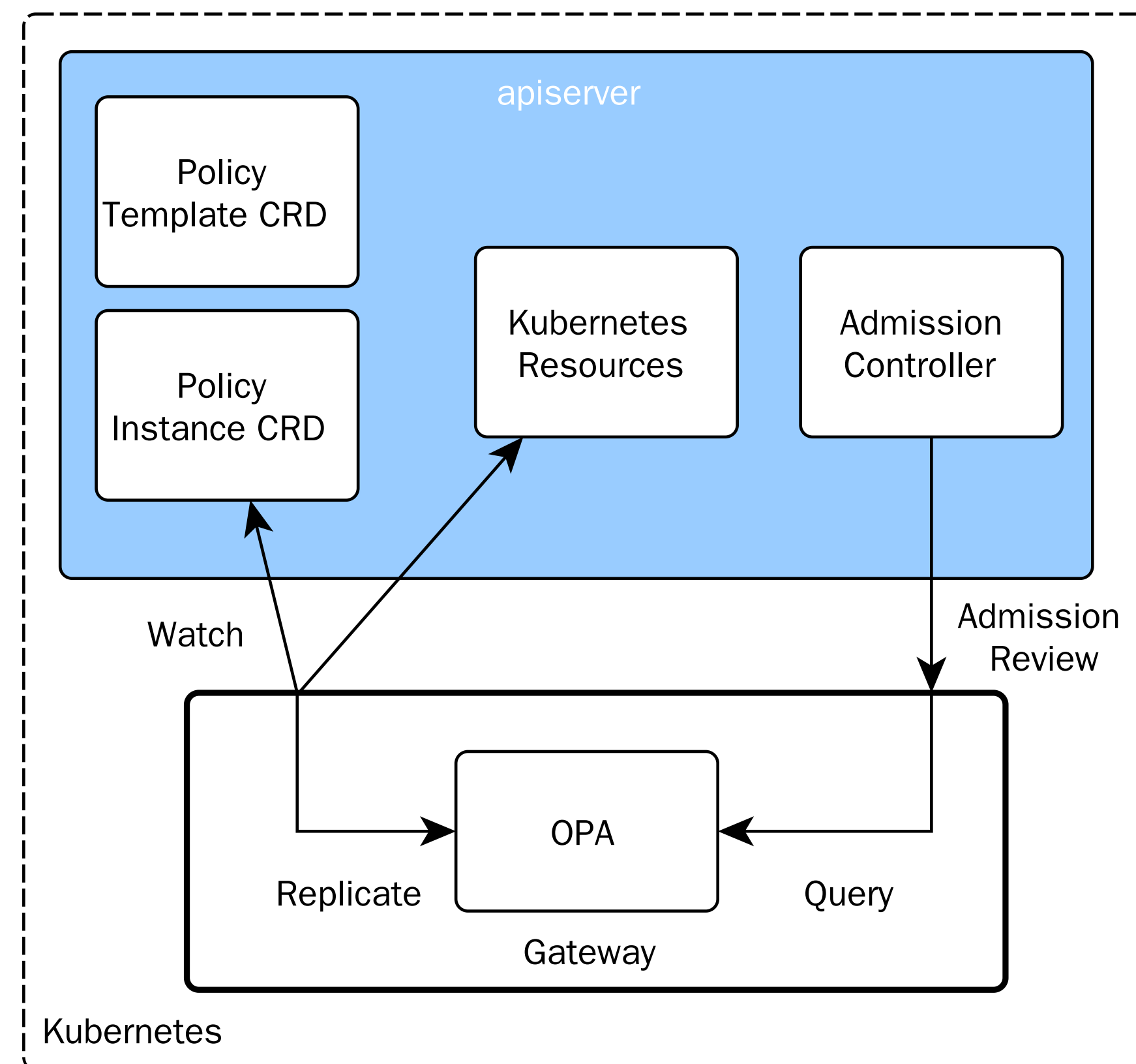
deny[msg] {
    kubernetes.is_deployment
    not input.spec.template.spec.securityContext.runAsNonRoot

    msg = sprintf("must not run as root in Deploy %s", [name])
}
```

## przykłady

# Kubernetes

## Admission hooks:





# Kubernetes

```
package kubernetes.admission
operations = {"CREATE", "UPDATE"}

input_container[c] {
  c := input.request.object.spec.template.spec.containers[_]
}

deny[reason] {
  input.request.kind.kind == "Deployment"
  operations[input.request.operation]
  input_container[container]
  not container.resources.limits.cpu
  reason := sprintf("no cpu limit for container %v", [container])
}
```

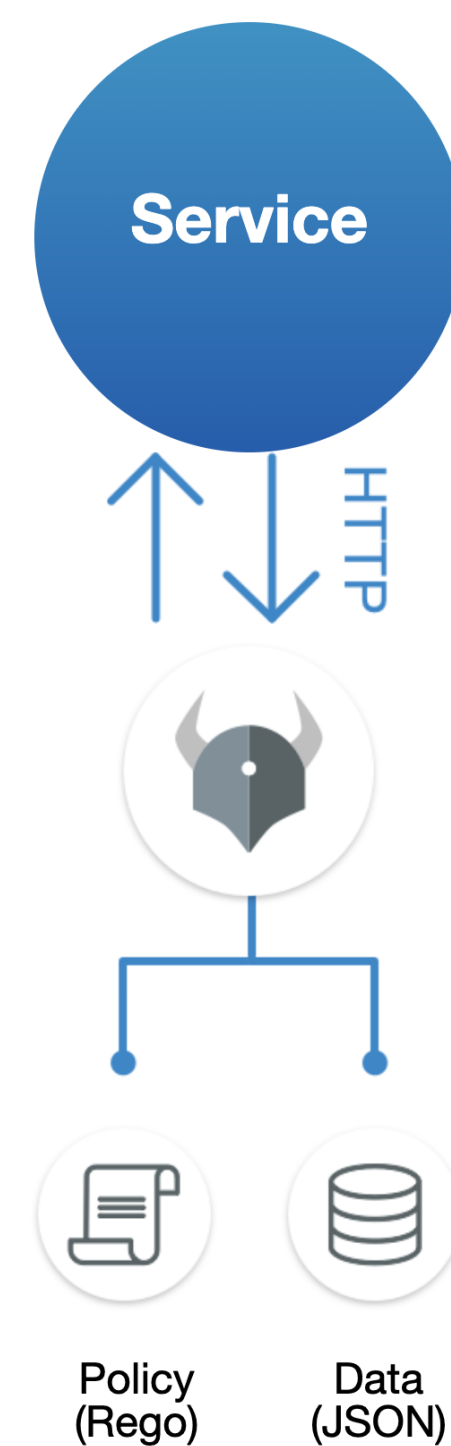
# Kubernetes

Integracje OPA:

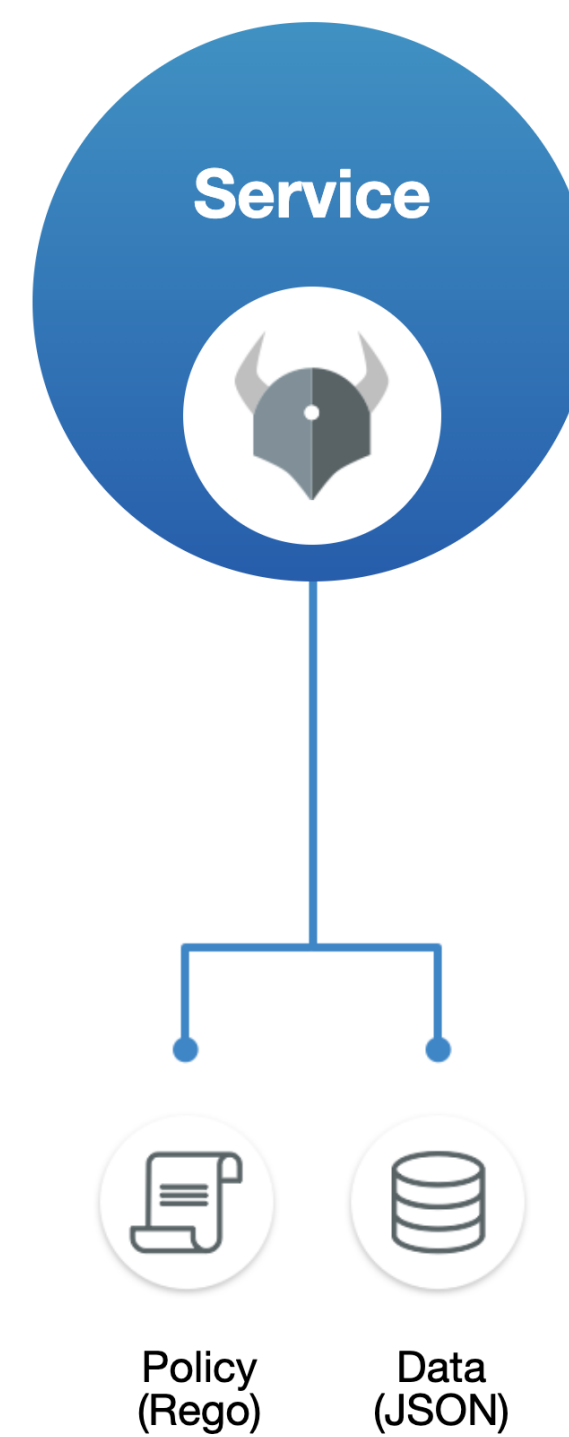
- Istio
- Envoy

# Twoja aplikacja/narzędzie

## Daemon



## Library



# Golang & OPA

- Golang lib - embed OPA
- Golang SDK - high level API

Patrz [dokumentacja](#)

# Golang & OPA

Przejdźmy do [kodu](#).

# Golang & OPA

```
var (  
    unsafeBuiltins = map[string]struct{}{  
        "http.send":      {},  
        "opa.runtime":      {},  
        "rego.parse_module": {},  
        "time.now_ns":      {},  
        "trace":             {},  
    }  
)
```

```
rego.UnsafeBuiltins(unsafeBuiltins)
```



# Golang & OPA

Możesz również dodać dla użytkownika dodatkowe funkcje rozszerzające rego, więcej w [dokumentacji](#).

# Lessons learnt

## Open Policy Agent:

- łatwo integruje się z Golangiem
- policy-as-a-code w bezpieczny sposób
- nie tylko do polityk ([przykład](#))

# Lessons learnt

Rego requires some time to master:

1. Policy workbench with samples
2. Przykłady dla użytkowników and dokumentacja
3. Testowanie Rego

# Lessons learnt

Styra, na przykład, dostarcza interaktywny edytor do budowania polityk:

- [Policy Builder](#)

# Alternatywy

- [cuelang](#)
- [kyverno](#)
- [Sentinel](#)



Dziękuję. Pytania?

Wojciech Barczynski  
wojciechb@spacelift.io

[github.com/wojciech12/talk\\_intro\\_OpenPolicyAgent](https://github.com/wojciech12/talk_intro_OpenPolicyAgent)





## Hiring

(Go) Backend and Frontend developers  
with a passion for building tools  
for other engineers.