Open Policy Agent

Philipp Krenn @xeraa

Example: Ansible

```
- name: TCP open port violation
  ansible.builtin.debug:
    msg: TCP port {{ item.port }} by pid {{ item.pid }} violates the list of open ports
  vars:
    tcp_listen_violations: >
        "{{ ansible_facts.tcp_listen | selectattr('port', 'in', tcp_list) | list }}"
    tcp_list:
      - 22
      - 25
  loop: "{{ tcp_listen_violations }}"
```


THIS IS FINE.

Decouple policy from change control or application

Run policies constantly

Manage as code

Gain insights into policy state

PS: Compliance & audits

Why?

Security incidents come in three levels

FYI, WTF, and OMG

Learn about a breach

From the press or users

Learn about a breach

Attackers asking for a ransom

Learn about a breach

Cloud provider's bill

Learn about a breach

Yourself after the fact

Learn about a breach

Yourself & you can prove no harm

Find security holes

Yourself before harm can happen

Tribal knowledge != security


TH-
THIS IS NOT FINE!!
OH MY GOD EVERY THINGS ON FIRE
WHAT THE HELL IS MY PROBLEM

No silver bullet 

Open Policy Agent

Started 2016

CNCF graduate

Widely used: Netflix, Cloudflare,...

Continuous Integration & Delivery

Cloud Native Network

Container Runtime

Coordination & Service Discovery

Container Runtime

Service Proxy

Coordination & Service Discovery

Logging

Continuous Integration & Delivery

Container Registry

Application Definition & Image Build

Service Mesh

Tracing

Scheduling & Orchestration

Scheduling & Orchestration

Service Mesh

Security & Compliance

Monitoring

Cloud Native Storage

Key Management

Key Management

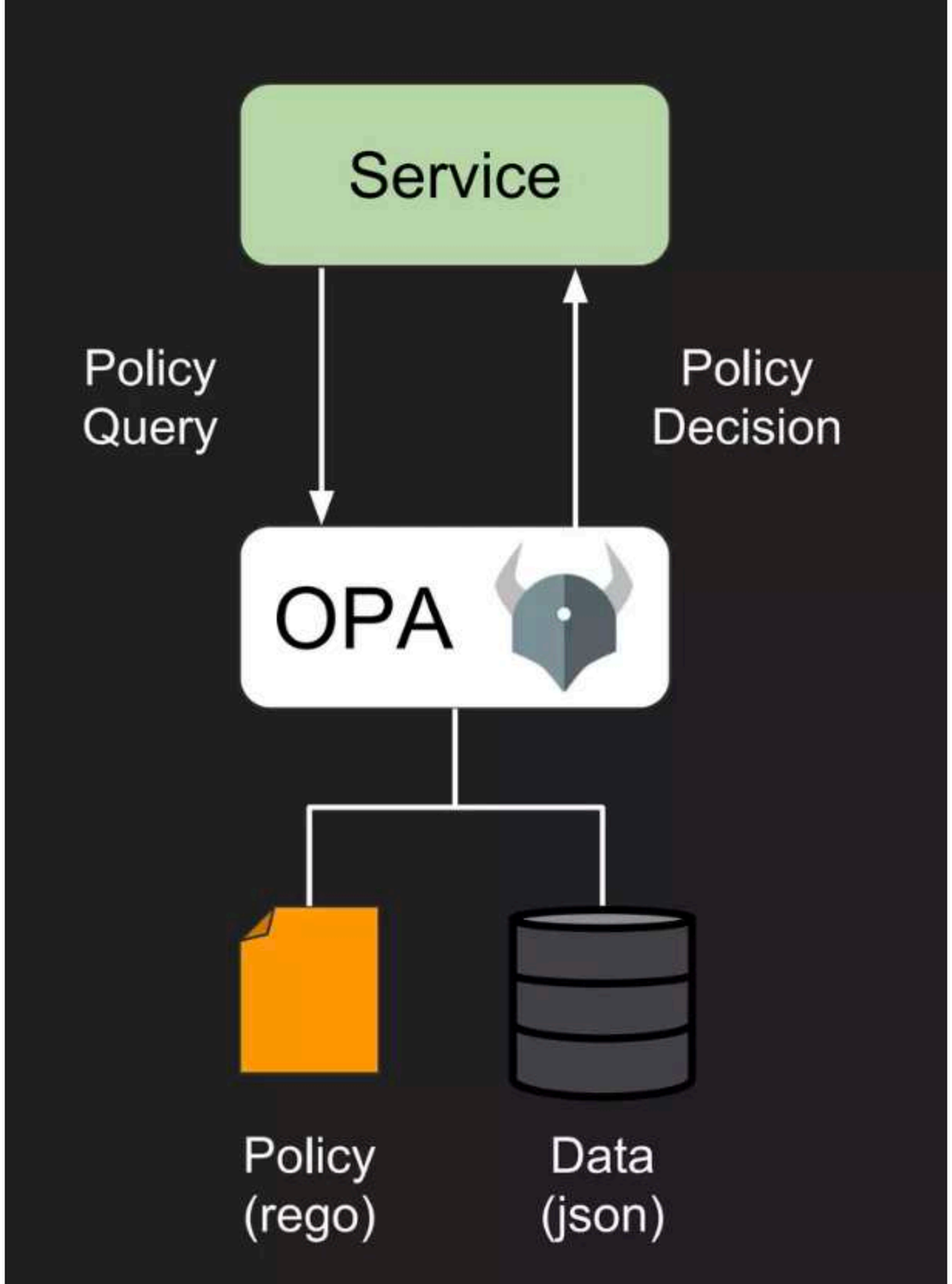
Security & Compliance

Database

Database


Container
API
UI
Host
Kubernetes
SSH
UI
Data
Servicemesh
CICD
API

OPA diagram


Service
Policy
Query
Policy
Decision
OPA
Policy
(rego)
Data
(json)

Read your own data

Policy

```
allow = true {
    input.method = "GET"
    input.path =["my-data", employee_id]
    input.user = employee_id
}
```

Input

```
{
    "method": "GET",
    "path":["my-data", "philipp"],
    "user": "philipp"
}
```

Policy

```
package play

default allow = false
allow = true {
    input.method = "GET"
      input.path = ["my-data", employee_id]
      input.user = employee_id
}
```

Input

```
{
    "method": "GET",
    "path":["my-data", "philipp"],
    "user": "peter"
}
```

Read your employee's data

Policy

```
allow = true {
    input.method = "GET"
    input.path =["my-data", employee_id]
    input.user = data.manager_of[employee_id]
}
```

Data (in-memory)

```
{
    "manager_of": {
        "philipp": "david",
        "matt": "philipp"
    }
}
```

Example: Kubernetes

```
package kubernetes.admission

import future.keywords

deny contains msg if {
    input.request.kind.kind == "Pod"
    some container in input.request.object.spec.containers
    image := container.image
    not startswith(image, "elastic.co/")
    msg := sprintf("image '%s' comes from untrusted registry", [image])
}
```

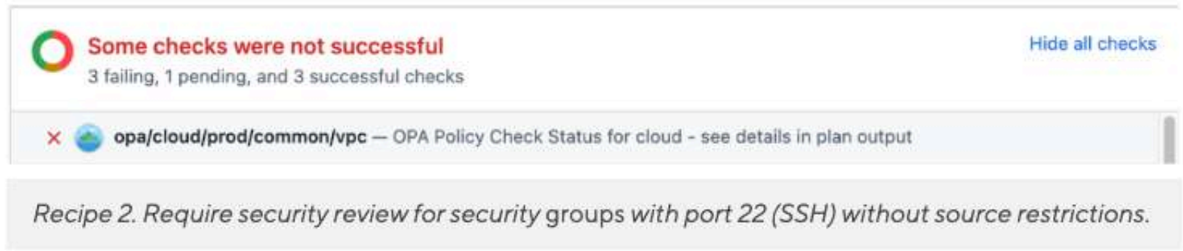
Example: Application

```
package application.authz
import future.keywords

default allow := false

allow if {
    input.method == "PUT"
    some petid
    input.path = ["pets", petid]
    input.user == input.owner
}
```

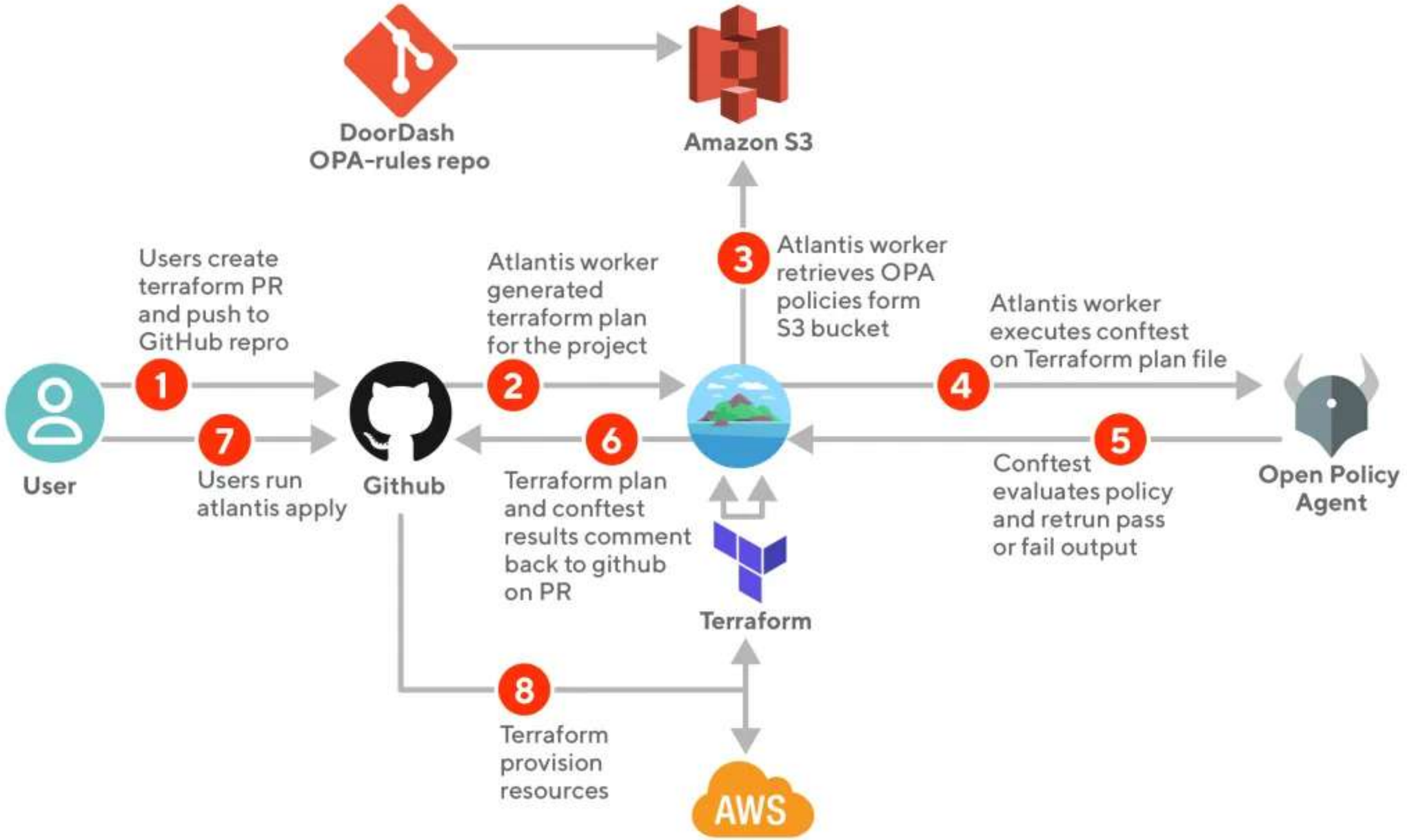
Example: Door Dash

https://thenewstack.io/how-doordash-governs-its-infrastructure-with-open-policy-agent/

```
Copy
Evaluating cloud
FAIL - /root/atlantis/.atlantis/repos/doordash/default.tfplan.json - Some of the resources actions
```



Recipe 2. Require security review for security groups with port 22 (SSH) without source restrictions.


DoorDash
OPA-rules repo
Amazon S3
Users create terraform PR and push to GitHub repro
1
Atlantis worker generated terraform plan for the project
2
3
Atlantis worker retrieves OPA policies form S3 bucket
Atlantis worker executes conftest on Terraform plan file
4
User
7
Users run atlantis apply
Github
6
Terraform plan and conftest results comment back to github on PR
5
Conftest evaluates policy and retrun pass or fail output
Open Policy Agent
Terraform
8
Terraform provision resources
AWS

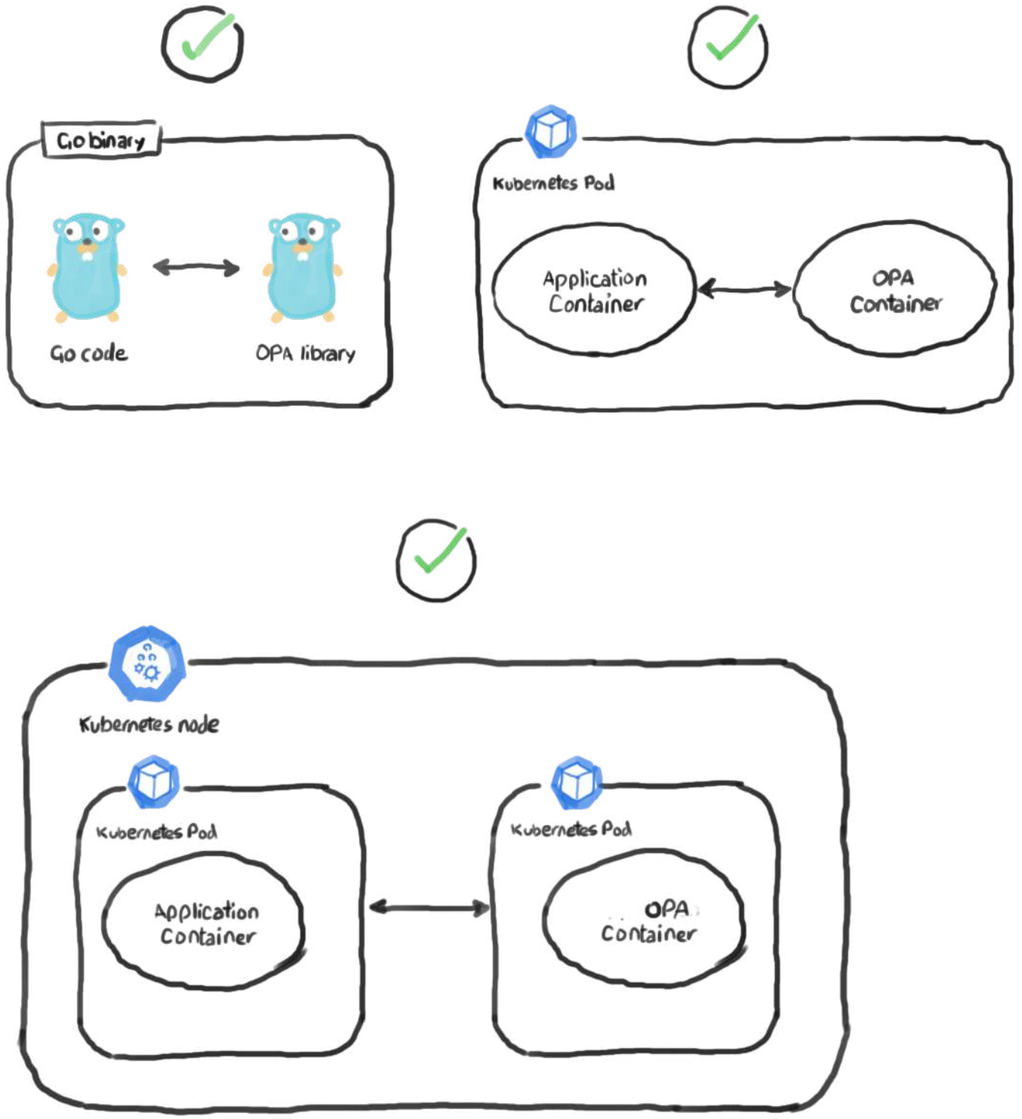
Getting started

https://play.openpolicyagent.org

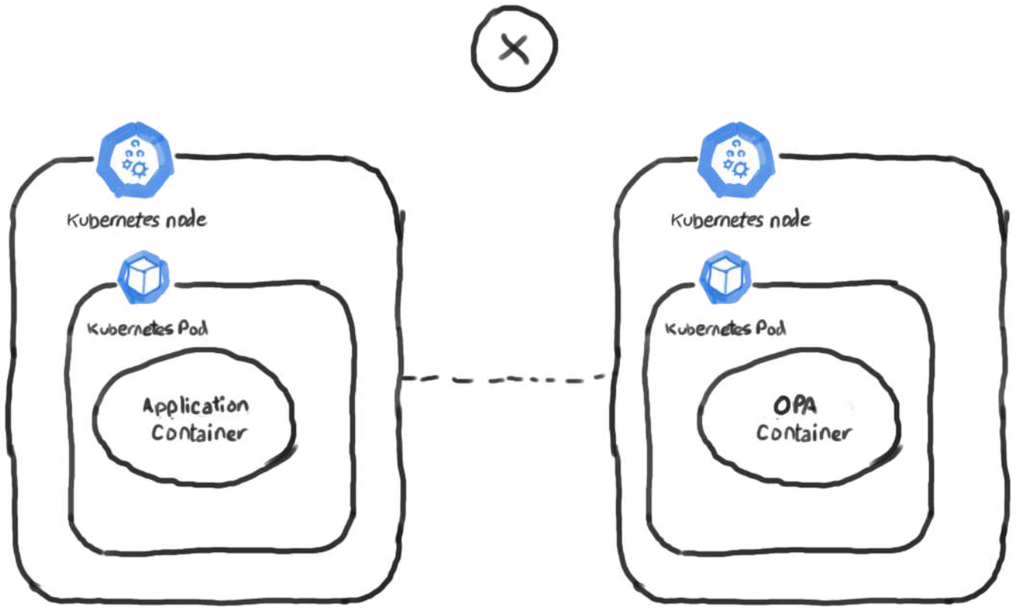
Deployment Options

Go library

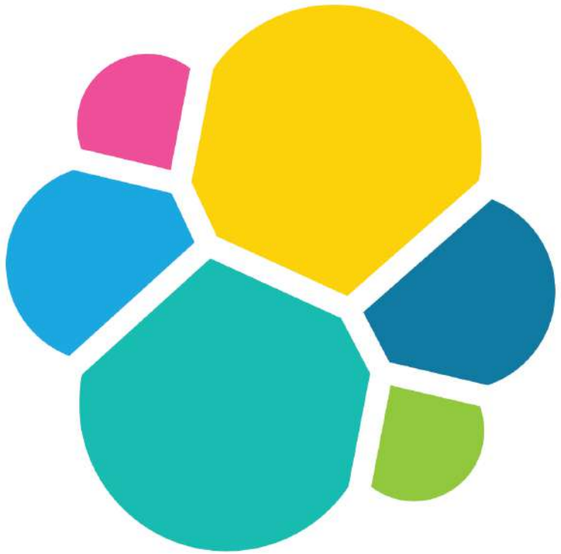
Daemon (co-located)



https://www.weave.works/blog/introducing-policy-as-code-the-open-policy-agent-opa



https://www.weave.works/blog/introducing-policy-as-code-the-open-policy-agent-opa



elastic

Developer 🥑

Why does Elastic care?

Devs: Data filtering with OPA

https://github.com/open-policy-agent/contrib/tree/main/data_filter_elasticsearch

Ops: Checking infrastructure

Kubernetes

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for Kubernetes

CIS Benchmarks are freely available in PDF format for non-commercial use:

DOWNLOAD LATEST CIS BENCHMARK →

Included in this Benchmark

FREE DOWNLOAD

CIS Benchmark

Safeguard IT systems against cyber threats with

Recent versions available for CIS Benchmark:

CIS Benchmarks™

Discover the CIS Benchmarks

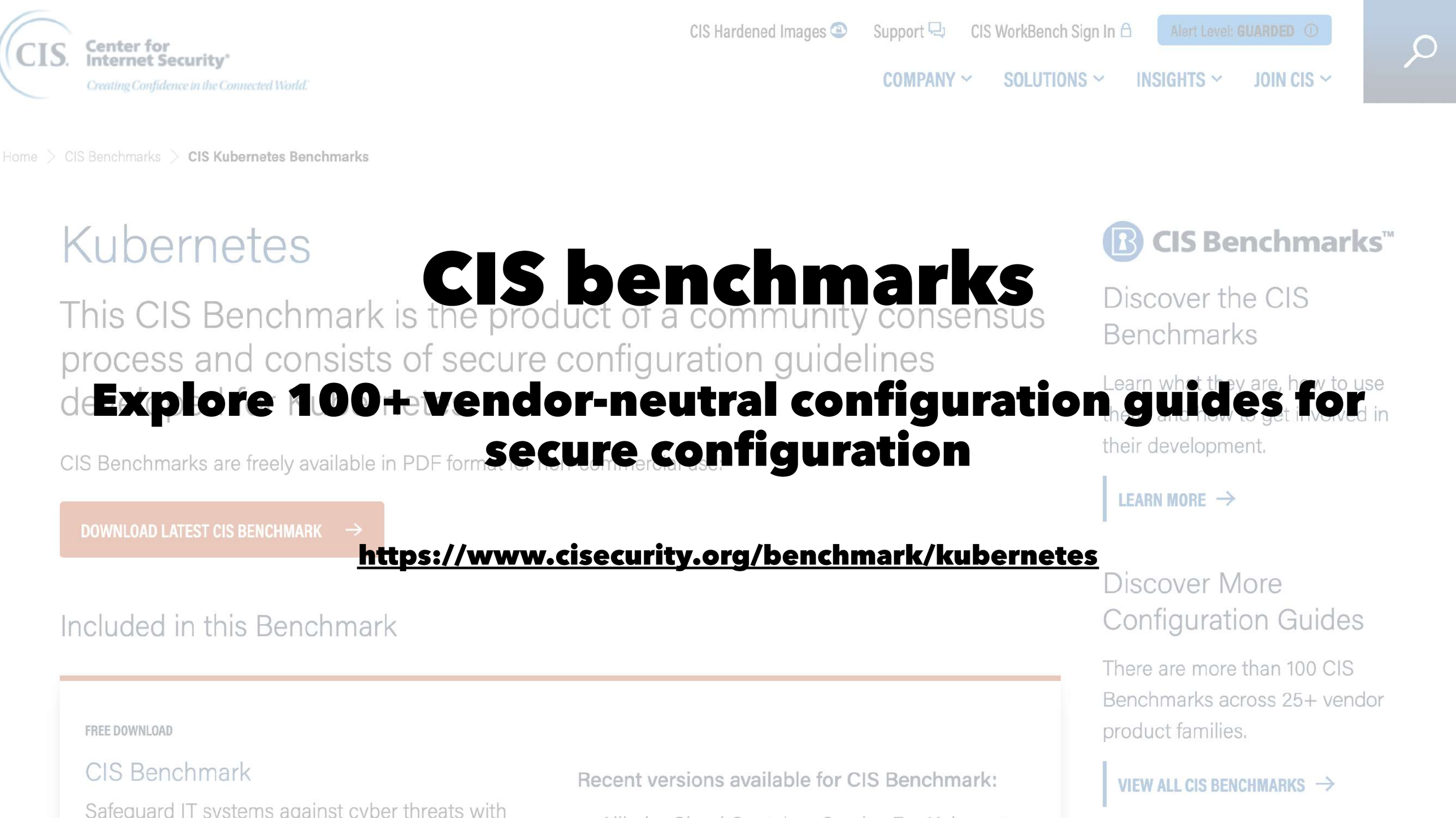
Learn what they are, how to use them, and how to get involved in their development.

LEARN MORE →

Discover More Configuration Guides

There are more than 100 CIS Benchmarks across 25+ vendor product families.

VIEW ALL CIS BENCHMARKS →



CIS benchmarks

Explore 100+ vendor-neutral configuration guides for secure configuration

https://www.cisecurity.org/benchmark/kubernetes

Load OPA bundle from FS #380

Code

Merged **uri-weisman** merged 29 commits into `elastic:main` from `uri-weisman:fs_bundle` on Sep 17, 2022

Conversation 18 Commits 29 Checks 49 Files changed 13 +102 −383

uri-weisman commented on Sep 8, 2022 • edited Member

1. Release - package opa bundle with cloudbeat.
2. Load opa bundle from FS and remove bundle-server logic.
3. Update CI.

- [CSP Rules] Cloudbeat consumption of bundle from FS security-team#4496

uri-weisman added 2 commits 5 months ago

`load from fs works` `f7b3bfc`

`delete bundle test` `f3ba1ce`

uri-weisman added 8.5 candidate Team:Cloud Security labels on Sep 8, 2022

mergify bot assigned **uri-weisman** on Sep 8, 2022

mergify bot commented on Sep 8, 2022

Reviewers

DaveSys911

eyalkraft

csp-automation

gurevichdmitry

Assignees

uri-weisman

Labels

8.5 candidate backport-skip Team:Cloud Security

Projects

None yet

Milestone

No milestone

https://github.com/elastic/csp-security-policies

Cloud Security Posture - Rego policies

CIS Kubernetes (74%) CIS Amazon EKS (60%) CIS AWS (70%)

coverage 99.25

▶ Project structure

Local Evaluation

`input.json`

should contain a beat/agent output and the `benchmark` (not mandatory - without specifying benchmark all benchmarks will apply), e.g. k8s eks aws

```
{
  "type": "file",
  "benchmark": "cis_k8s",
  "sub_type": "file",
  "resource": {
    "mode": "700",
    "path": "/hostfs/etc/kubernetes/manifests/kube-apiserver.yaml",
    "owner": "etc",
    "group": "root",
    "name": "kube-apiserver.yaml",
    "gid": 20,
    "uid": 501
  }
}
```

Used by 6

Contributors 13

+ 2 contributors

Languages

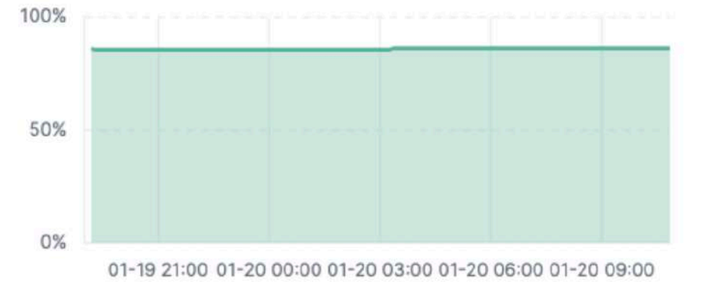
- Open Policy Agent 92.9%
- Python 6.9%
- Go 0.2%

Cloud Posture BETA

Cloud Posture Score

86%

326/378 Findings passed



Failed Findings

CIS Section	Findings
Pod Security Standards	23/90
API Server	12/28
RBAC and Service Accou...	9/184
Kubelet	4/13
Controller Manager	2/6

View all failed findings

Open Cases

Coming soon

CIS Kubernetes V1.23
Cluster ID 4d43fe

4 hours ago

Compliance Score

86%

326/378 Findings passed

Failed Findings

CIS Section	Findings
Pod Security Standards	23/90
API Server	12/28
RBAC and Service Accounts	9/184

View all failed findings

cluster_id: "4d43fe71-fa75-44cd-8e25-4fc473bdfae8" and rule.section: "Pod

Findings BETA

Group by None

Showing **1**-**10** of **23** Findings

Resource ID	Result	Resource Type	Resource Name	Rule
068ca4b5-d5d...	Fail	Pod	kube-scheduler-...	Minimize
068ca4b5-d5d...	Fail	Pod	kube-scheduler-...	Minimize
875f5ace-734...	Fail	Pod	kindnet-5kshf	Minimize
875f5ace-734...	Fail	Pod	kindnet-5kshf	Minimize
875f5ace-734...	Fail	Pod	kindnet-5kshf	Minimize
01bbabd9-528...	Fail	Pod	kube-apiserver-c...	Minimize
01bbabd9-528...	Fail	Pod	kube-apiserver-c...	Minimize
49fc748f-ac9e...	Fail	Pod	local-path-provis...	Minimize

Fail

Minimize the admission of containers with t...

Overview Rule Resource JSON

Details

Rule Name

Minimize the admission of containers with the NET_RAW capability (Automated)

Rule Tags

CIS Kubernetes CIS 5.2.8 Pod Security Standards

Evaluated at

January 20, 2023 @ 11:11:33.694

Resource Name

kube-apiserver-cspm-control-plane

Framework Sources

CIS Section

Pod Security Standards

Index

logs-cloud_security_posture.findings_latest-default

Remediation

elastic

@xeraa

AWS, GCP, Azure & Kubernetes supported

No custom rules (yet)

Improve process evaluation performance #137

Edit | Code

Merged **jeniawhite** merged 1 commit into `elastic:main` from `jeniawhite:evgb-RegoPerformance` on Nov 15, 2022

Conversation 4 | Commits 1 | Checks 2 | Files changed 79 | +1,220 −952

jeniawhite commented on Nov 9, 2022 • edited — Member

Changed parsing logic of process arguments and improved evaluation time for process resources by ~3.23x (faster).
Prior to change:

```
"timer_rego_query_eval_ns": 47741250
```

After the change:

```
"timer_rego_query_eval_ns": 14774584
```

- Policy performance degradation #134

2

jeniawhite requested a review from **elastic/csp-security-policies** as a code owner 4 months ago

Reviewers

oren-zohar

Still in progress? Learn about draft PRs

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Conclusion

Application: Why not?

Change management: Why not?

OPA: Why?

OPA: Why not?

How to express OR in Rego

Anders Eknert

10 min read **Published** September 21, 2023

One of the most common questions people new to Open Policy Agent (OPA) and Rego ask is about how to express logical "OR" in the language. While there is no "OR" operator, Rego has no shortage of ways to express that, with some being more obvious than others. In this blog, we'll take a look at the most common ways to express OR, and weigh the virtues of each method against the others. Hopefully you'll learn a few tricks along the way. One thing is certain — if you make it through to the end, there's no way you'll wonder how to express OR in Rego!

https://www.styra.com/blog/how-to-express-or-in-rego/

Tradeoff

limited vs complex

Open Policy Agent

Philipp Krenn @xeraa