SOSS Community Day

EUROPE

SOSS Community Day
EUROPE

Let devs be devs without sacrificing security

Andrew McNamara; Red Hat

What does it mean to be a developer?

Build off of open source software

Explore new problem spaces and solutions

Use tooling that is supportive not disruptive

SOSS Community Day
EUROPE

Red Hat

Devs want to easily build artifacts

festoji / .github / workflows / **package.yaml**

arewm update slsa provenance generator ✓

Code | Blame | 90 lines (75 loc) · 2.67 KB

```yaml
---
name: Package

on:
  push:
  workflow_dispatch:

env:
  IMAGE_REGISTRY: quay.io
  IMAGE_REPO: arewm/festoji
  IMAGE_TAGS: latest

jobs:
  build:
```

SOSS Community Day
EUROPE

Red Hat

Devs want to troubleshoot builds

festoji / .github / workflows / **package.yaml**

arewm update slsa provenance generator ✓

Code | Blame | 90 lines (75 loc) · 2.67 KB

```yaml
---
name: Package

on:
  push:
  workflow_dispatch:

env:
  IMAGE_REGISTRY: quay.io
  IMAGE_REPO: arewm/festoji
  IMAGE_TAGS: latest

jobs:
  build:
```

Devs want to explore new tech

festoji / .github / workflows / **package.yaml**

arewm update slsa provenance generator ✓

Code | Blame | 90 lines (75 loc) · 2.67 KB

```yaml
---
name: Package

on:
  push:
  workflow_dispatch:

env:
  IMAGE_REGISTRY: quay.io
  IMAGE_REPO: arewm/festoji
  IMAGE_TAGS: latest

jobs:
  build:
```

Devs don’t need to be this unhappy

SLSA Build L3:

Harden the build platform

Generate provenance

Devs don’t need to be this unhappy

Focus on hardening the build platform

Focus on accurate (detailed) provenance

Provide templates for builds and tests

Red Hat

Devs don’t need to be this unhappy

Flexibility vs. risk

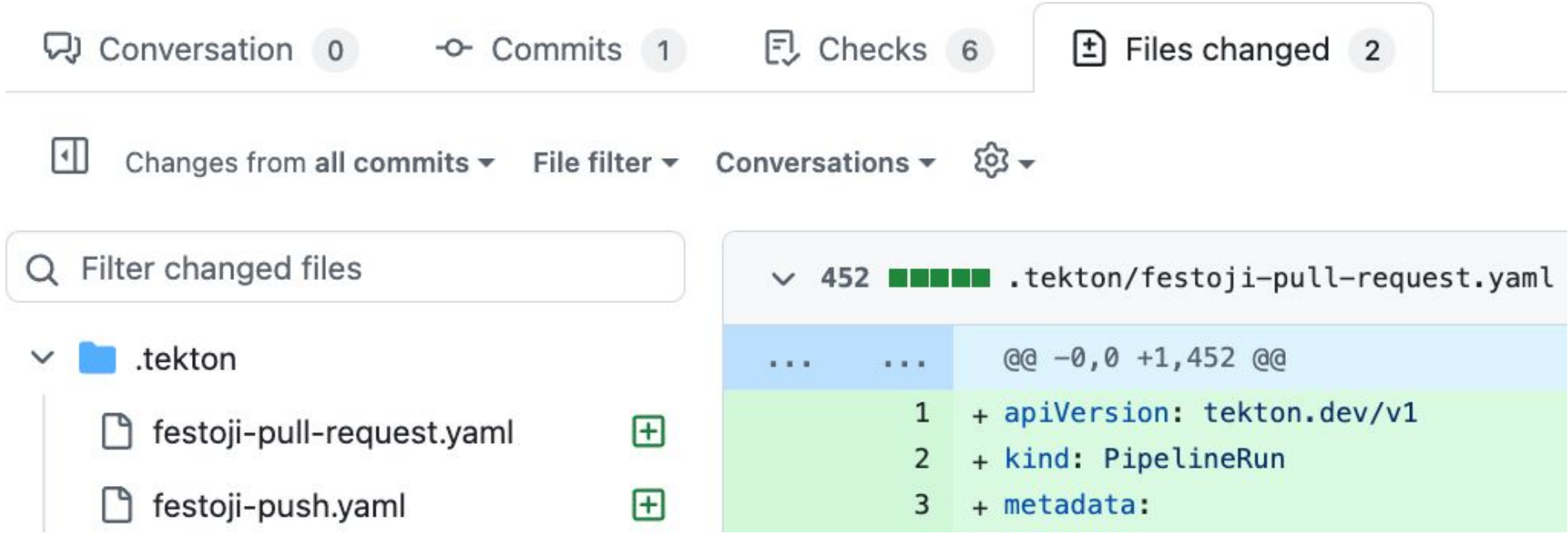
Sliding scale of risk

enterprise contract

SOSS Community Day
EUROPE

Red Hat

Devs can easily build artifacts



Devs can easily build artifacts

Results

Component ▾ | Status ▾ | Filter by rule...

Results summary

Failed 14 | Warning 3 | Success 94

	Rules	Status	Message	Component
>	Build task called with hermetic param set	Failed	Build task was not invoked with the hermetic parameter set	festoji
>	Required labels	Failed	The required "com.redhat.component" label is missing. La...	festoji
>	Required labels	Failed	The required "description" label is missing. Label descripti...	festoji
>	Exists	Failed	No source image references found	festoji
>	All required tasks were included in the pipeline	Failed	One of "source-build", "source-build-oci-ta" tasks is missi...	festoji
>	No tests erred	Failed	The Task "ecosystem-cert-preflight-checks" from the buil...	festoji
>	No tests were skipped	Failed	The Task "sast-snyk-check-oci-ta" from the build Pipeline...	festoji
>	Optional labels	Warning	The optional "maintainer" label is missing. Label descripti...	festoji

Devs can troubleshoot builds

```
taskRef:
  params:
  - name: name
    value: buildah-oci-ta
  - name: bundle
    value: quay.io/konflux-ci/tekton-catalog/task-buildah-oci-ta:0.2
  - name: kind
    value: task
  resolver: bundles
```

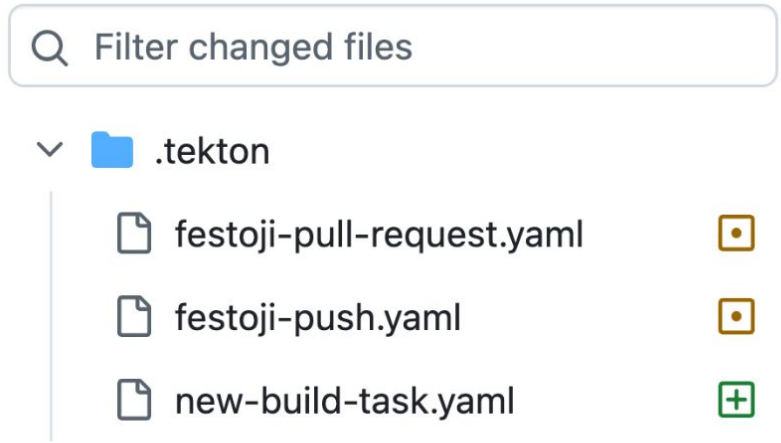
Devs can troubleshoot builds

```
$ tkn bundle list -o json quay.io/konflux-ci/tekton-catalog/task-buildah-oci-ta
:0.2 task buildah-oci-ta | jq
{
  "kind": "Task",
  "apiVersion": "tekton.dev/v1",
  "metadata": {
    "name": "buildah-oci-ta",
    "creationTimestamp": null,
    "labels": {
      "app.kubernetes.io/version": "0.2",
      "build.appstudio.redhat.com/build_type": "docker"
    },
    "annotations": {
      "tekton.dev/pipelines.minVersion": "0.12.1",
      "tekton.dev/tags": "image-build, konflux"
    }
  },
  "spec": {
[...]
```

SOSS Community Day
EUROPE

Red Hat

Devs can explore new tech

- 

6 ■■■■■ .tekton/festoji-pull-request.yaml

```
@@ -191,6 +191,12 @@ spec:
191  191            workspace: git-auth
192  192          - name: netrc
193  193            workspace: netrc
     194  +       - name: sample-new-build-task
     195  +         taskRef:
     196  +           kind: Task
     197  +           name: new-build-task
     198  +         runAfter:
     199  +           - clone-repository
194  200          - name: build-container
195  201            params:
196  202            - name: IMAGE
```

Devs don’t need to be this unhappy

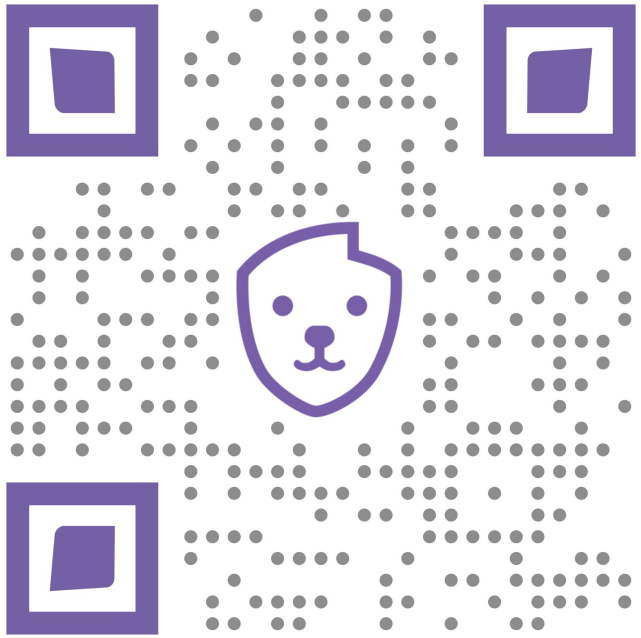



KONFLUX

Thank you!

@arewm

arewm@redhat.com



SOSS Community Day
EUROPE

Red Hat