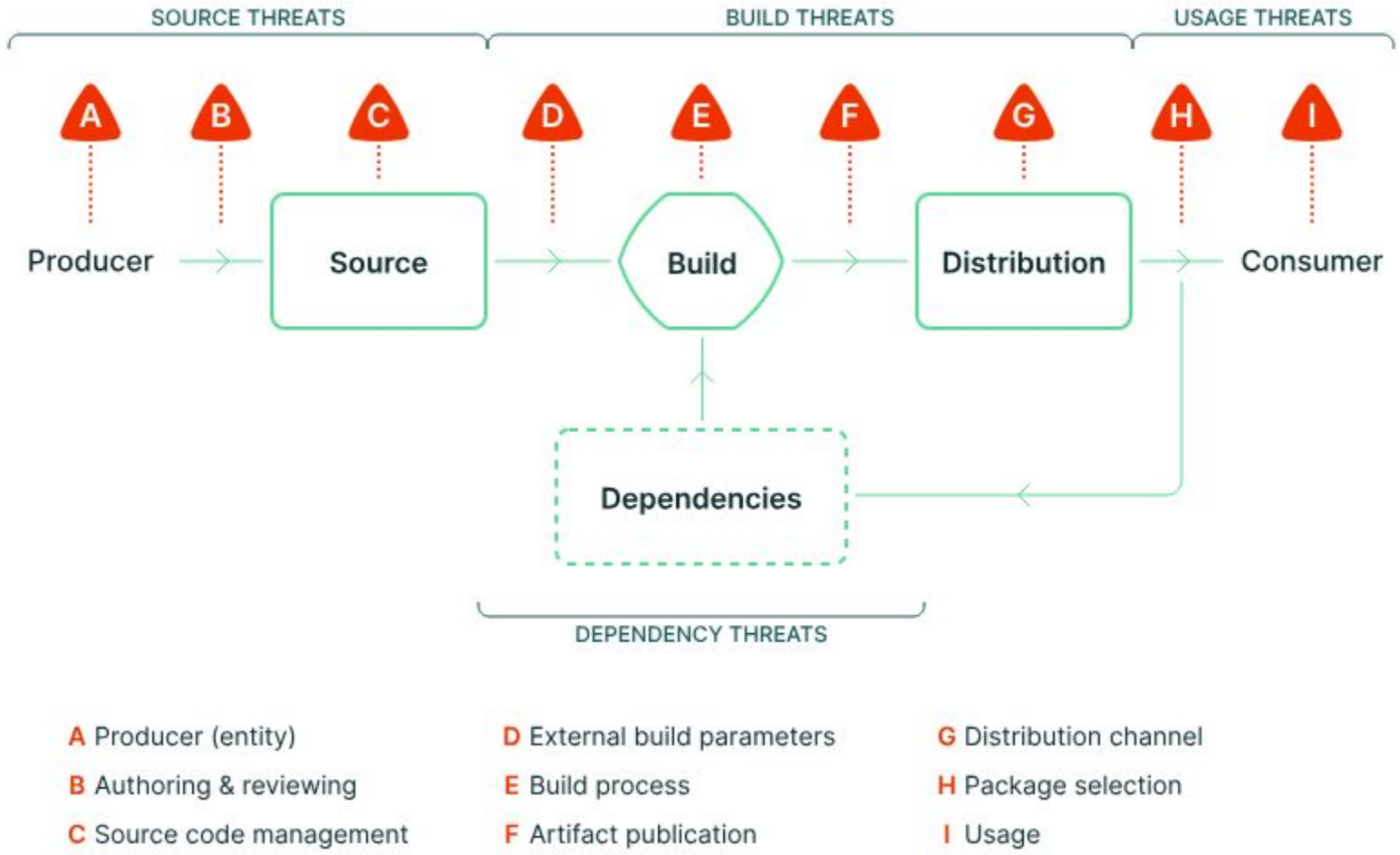
Let devs be devs without sacrificing security

Andrew McNamara; Red Hat

Devs need to be protected from threats



Source: https://slsa.dev/spec/v1.1-rc2/threats-overview

What does it mean to be a developer?

Build off of open source software

Troubleshoot their builds

Explore new problem spaces and solutions

Use tooling that is supportive not disruptive

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:
```

Devs want to troubleshoot builds

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

arewm update slsa provenance generator ✓

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

```
1   ---
2   name: Package
3
4   on:
5     push:
6     workflow_dispatch:
7
8   env:
9     IMAGE_REGISTRY: quay.io
10    IMAGE_REPO: arewm/festoji
11    IMAGE_TAGS: latest
12
13  jobs:
14    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

```
1   ---
2   name: Package
3
4   on:
5     push:
6     workflow_dispatch:
7
8   env:
9     IMAGE_REGISTRY: quay.io
10    IMAGE_REPO: arewm/festoji
11    IMAGE_TAGS: latest
12
13  jobs:
14    build:
```

Devs don’t need to be this unhappy

SLSA Build L3:

Harden the build platform

Generate provenance

Kubernetes is used to provide RBAC, containerization, namespace isolation etc.

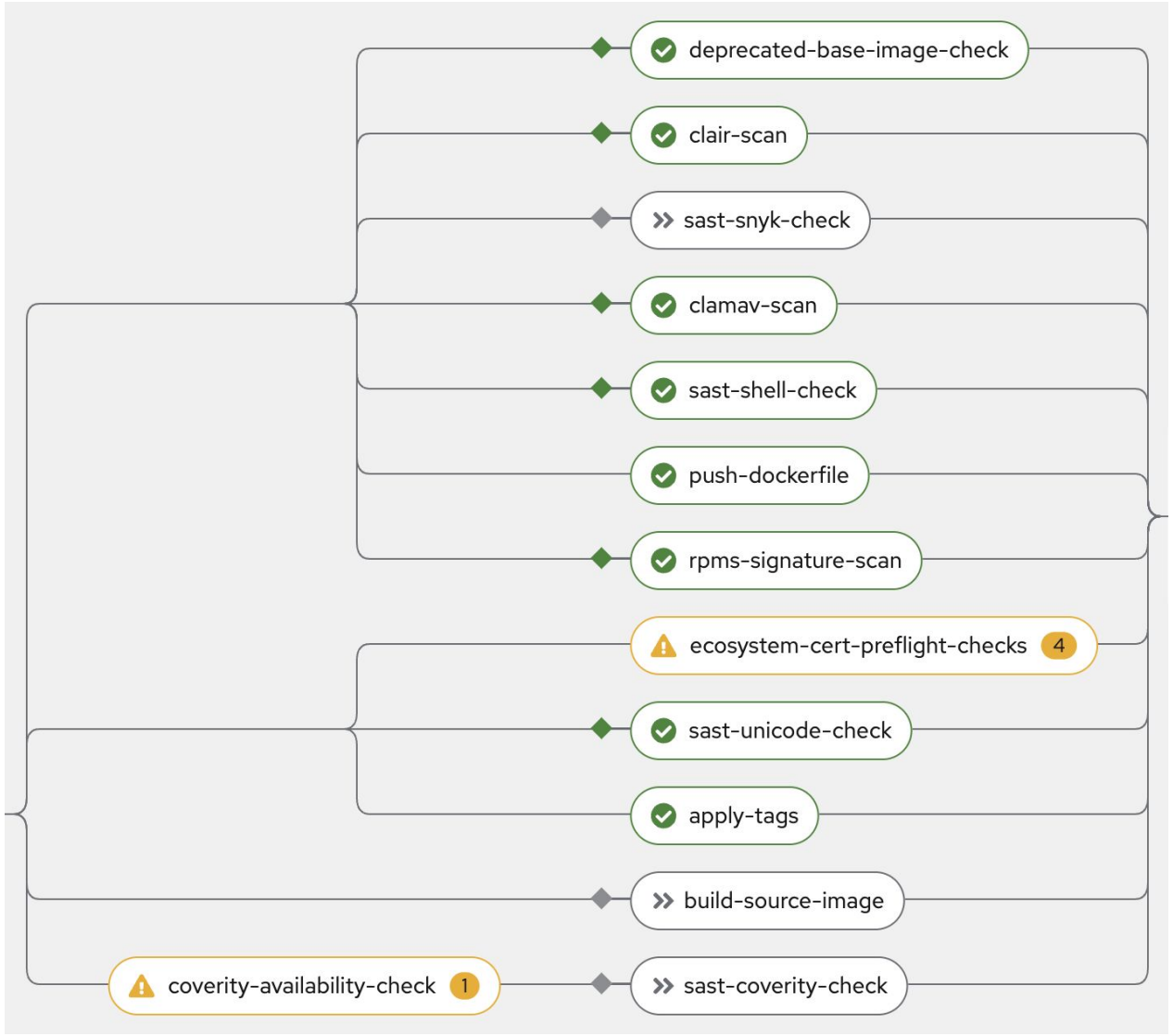
k8s + tekton

trusted task library

k8s + tekton

A library of tasks providing common and critical functions which need to be secure and auditable.


init
clone-repository
prefetch-dependencies
build-container
build-image-index

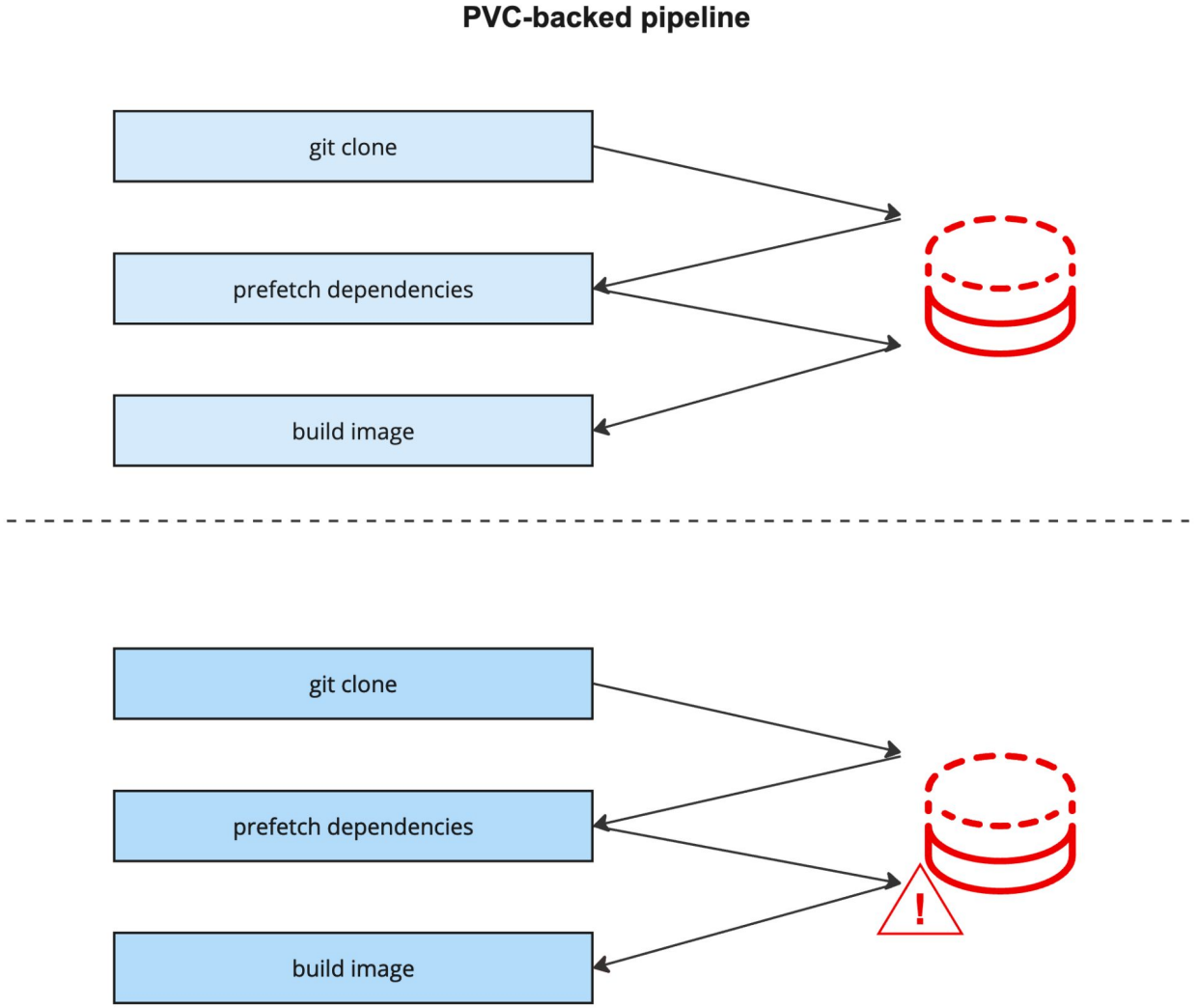

deprecated-base-image-check
clair-scan
sast-snyk-check
clamav-scan
sast-shell-check
push-dockerfile
rpms-signature-scan
ecosystem-cert-preflight-checks
4
sast-unicode-check
apply-tags
build-source-image
coverity-availability-check
1
sast-coverity-check

trusted artifacts

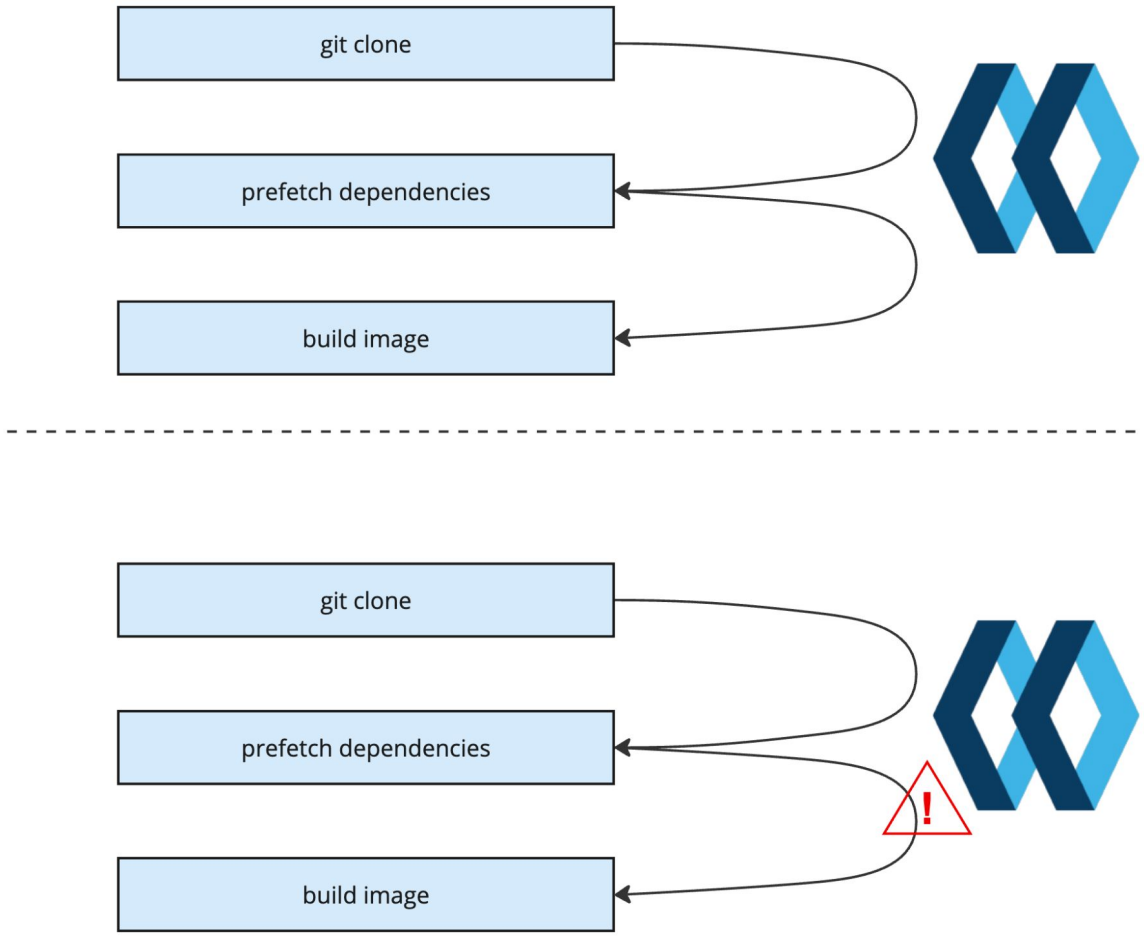
trusted task library

k8s + tekton

'Trusted artifacts' is a method of sharing data between tasks which allows detection of data alterations.


PVC-backed pipeline
git clone
prefetch dependencies
build image
git clone
prefetch dependencies
build image
!

Trusted artifact pipeline



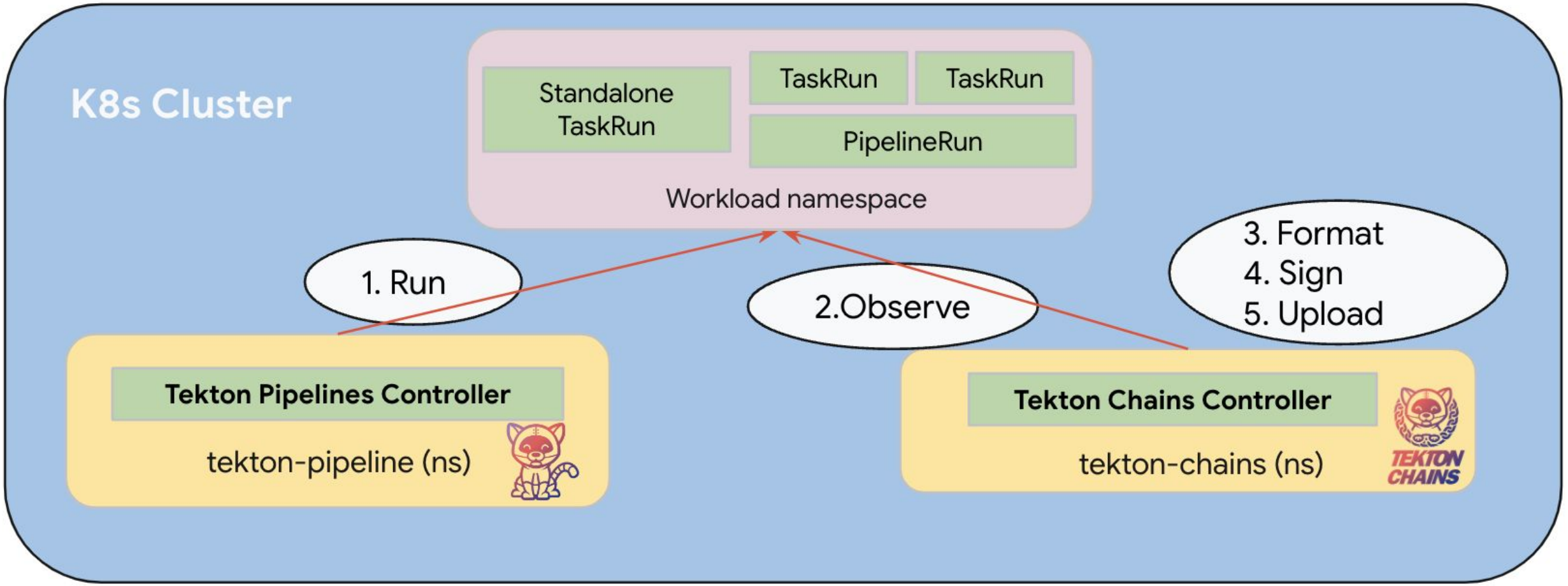
observer generated attestations

trusted artifacts

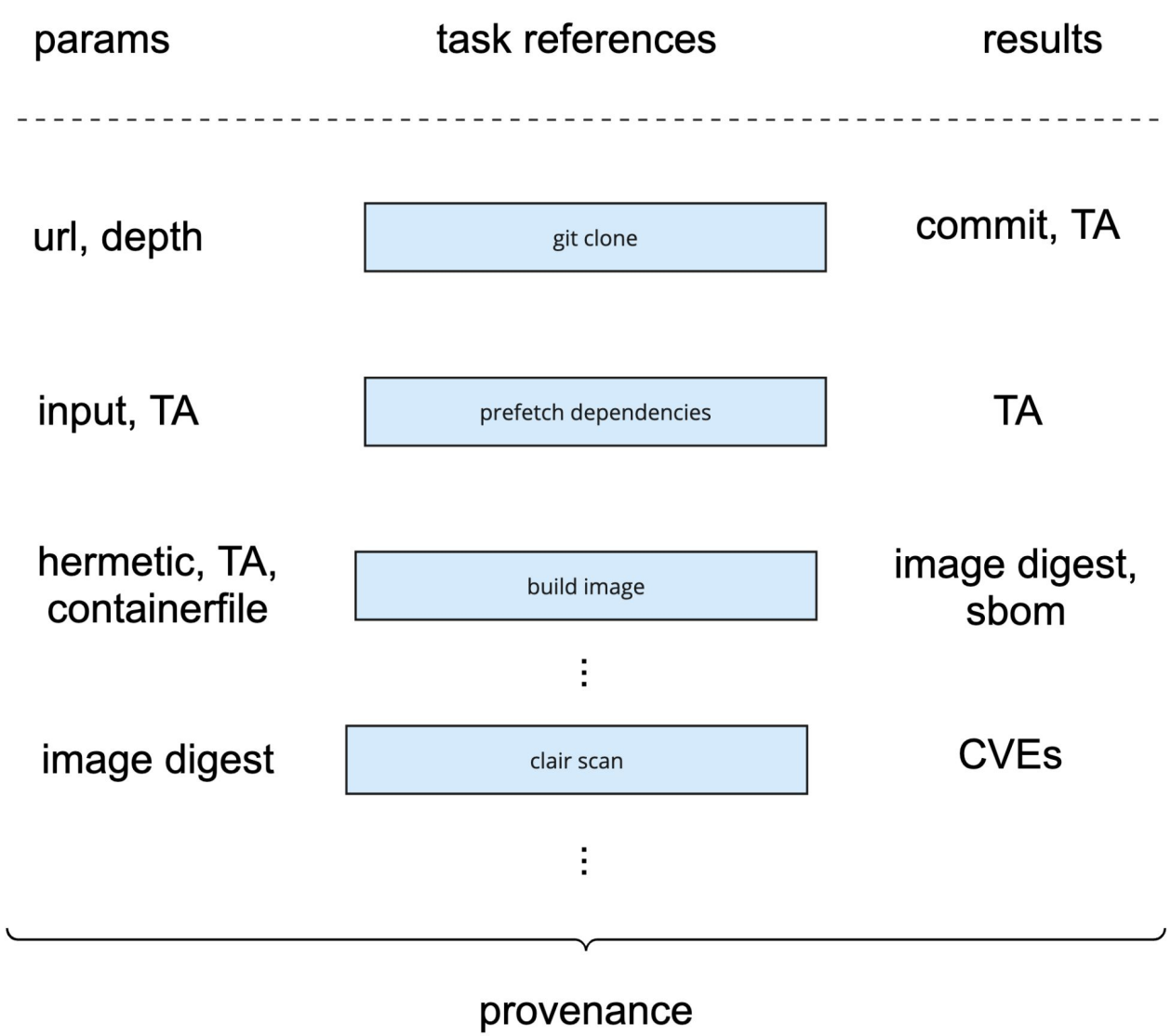
trusted task library

k8s + tekton

Attestations are generated separately from the pipeline (by an 'observer') so they cannot be influenced by the user.



https://tekton.dev/docs/chains/slsa-provenance/#how-does-tekton-chains-work


params
task references
results
url, depth
git clone
commit, TA
input, TA
prefetch dependencies
TA
hermetic, TA, containerfile
build image
image digest, sbom
image digest
clair scan
CVEs
provenance

policy engine

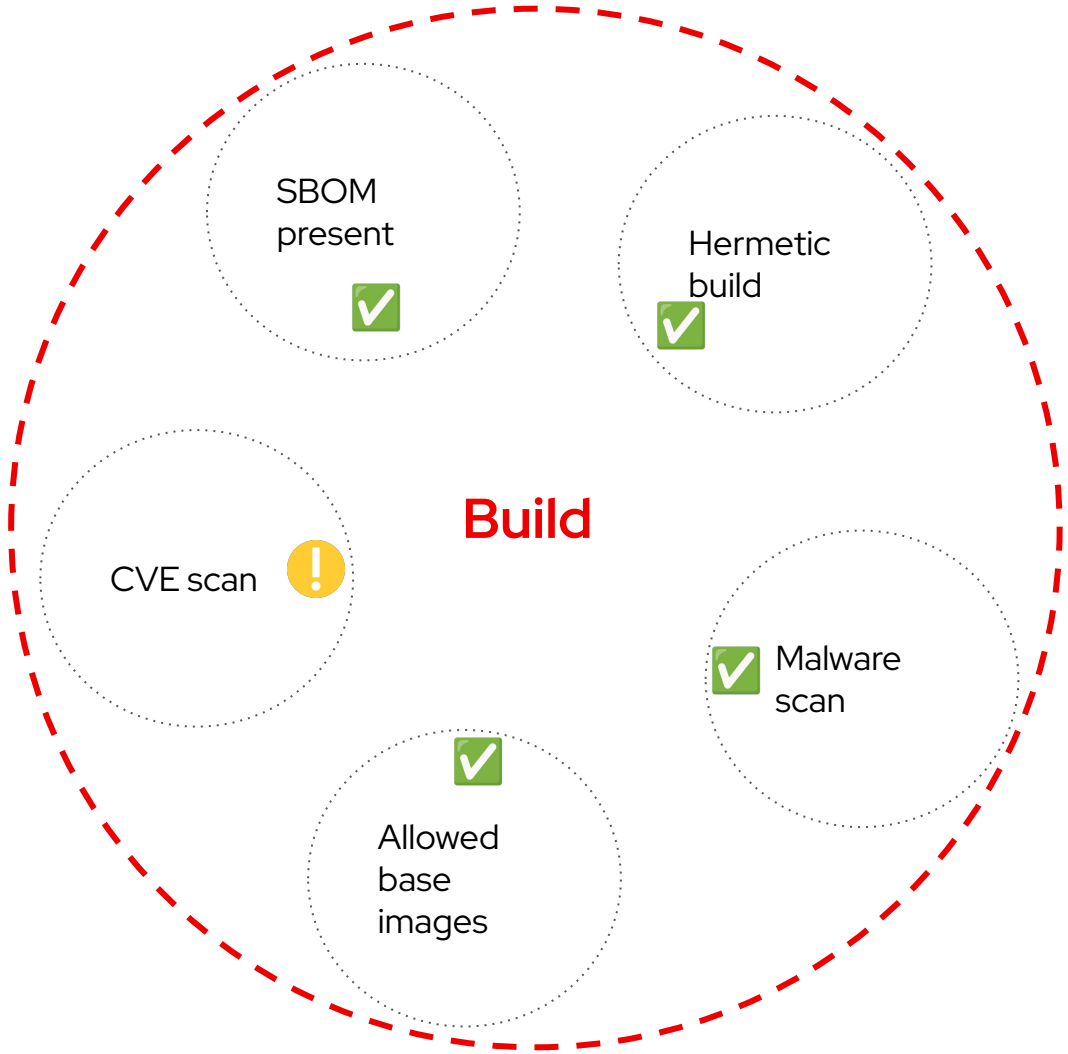
observer generated attestations

trusted artifacts

trusted task library

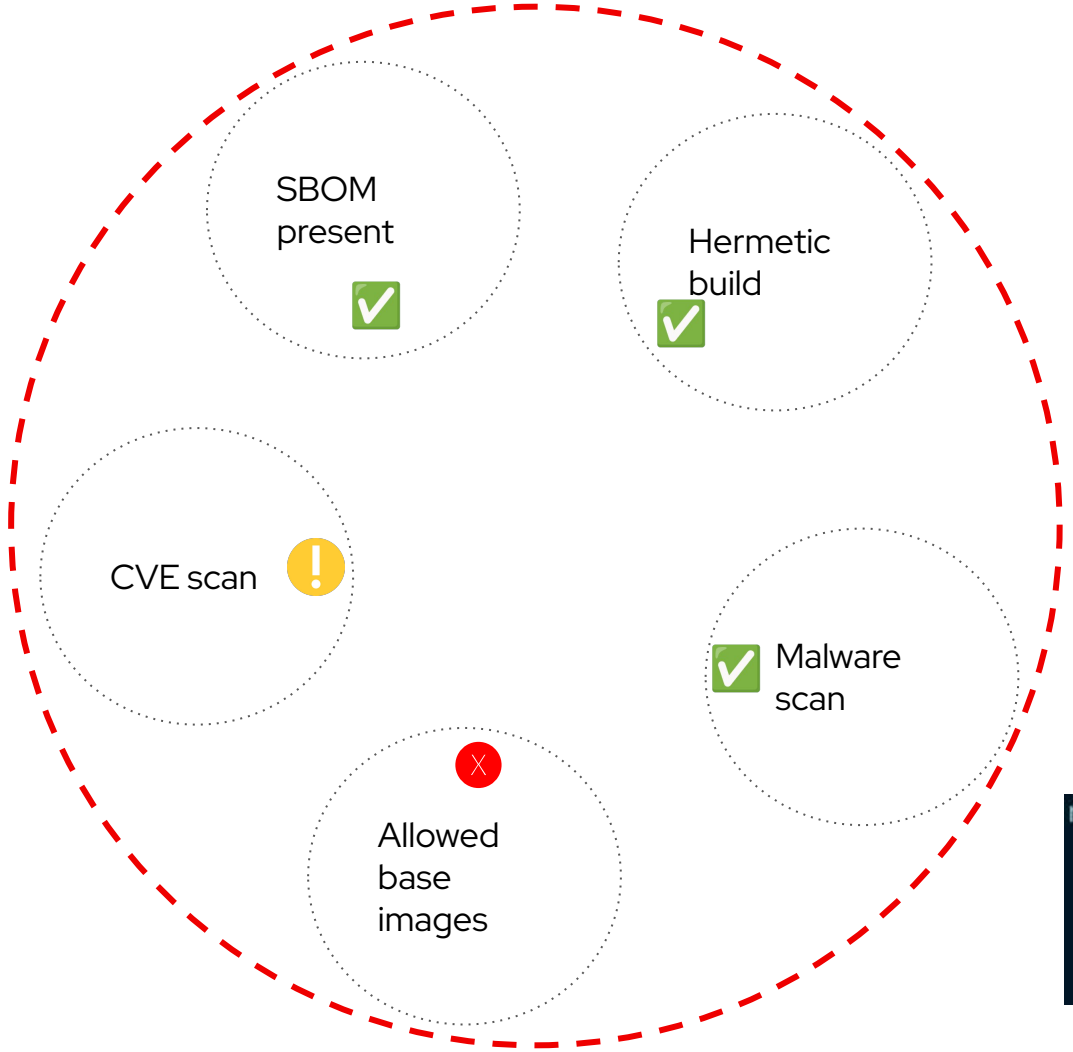
k8s + tekton

A policy engine is used to compare the attestations against required policy (we use Conforma).



conforma

verify artifacts, enforce policies



conforma

verify artifacts, enforce policies

```
ruleData:
  rule_data_custom:
    allowed_registry_prefixes:
      - trusted-registry.io/trusted-images/
```

release service

policy engine

observer generated attestations

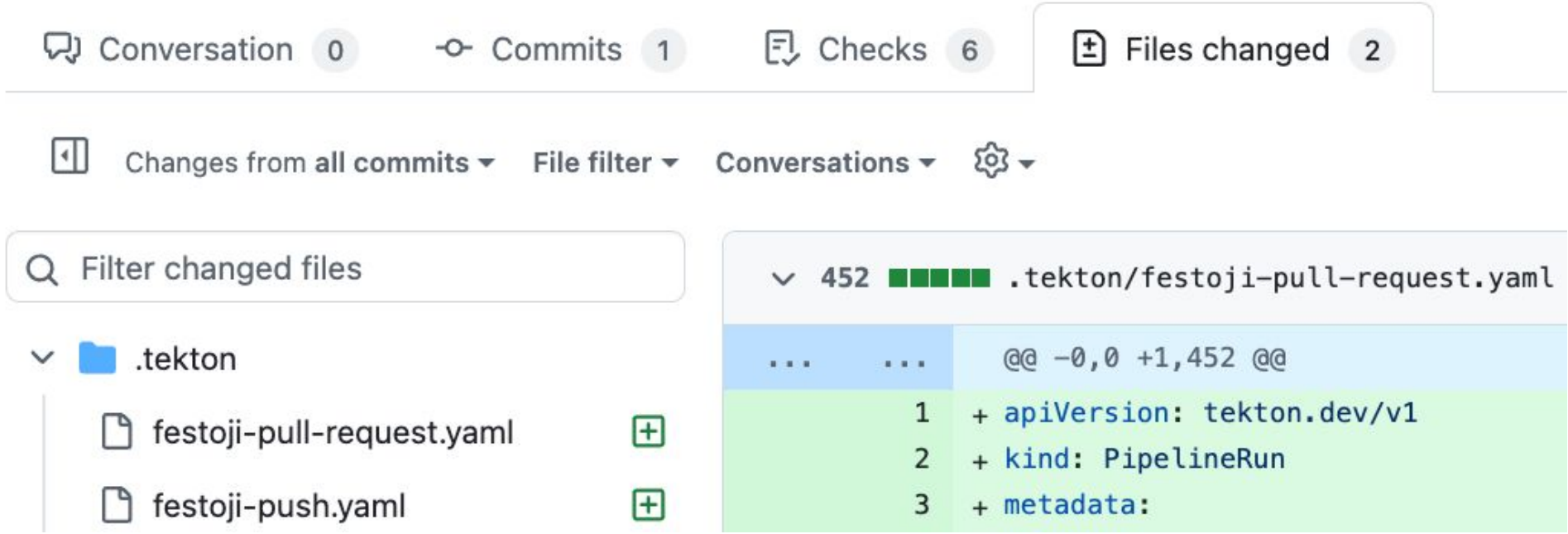
trusted artifacts

trusted task library

k8s + tekton

Release service gates access to protected destinations based on policy evaluation.

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

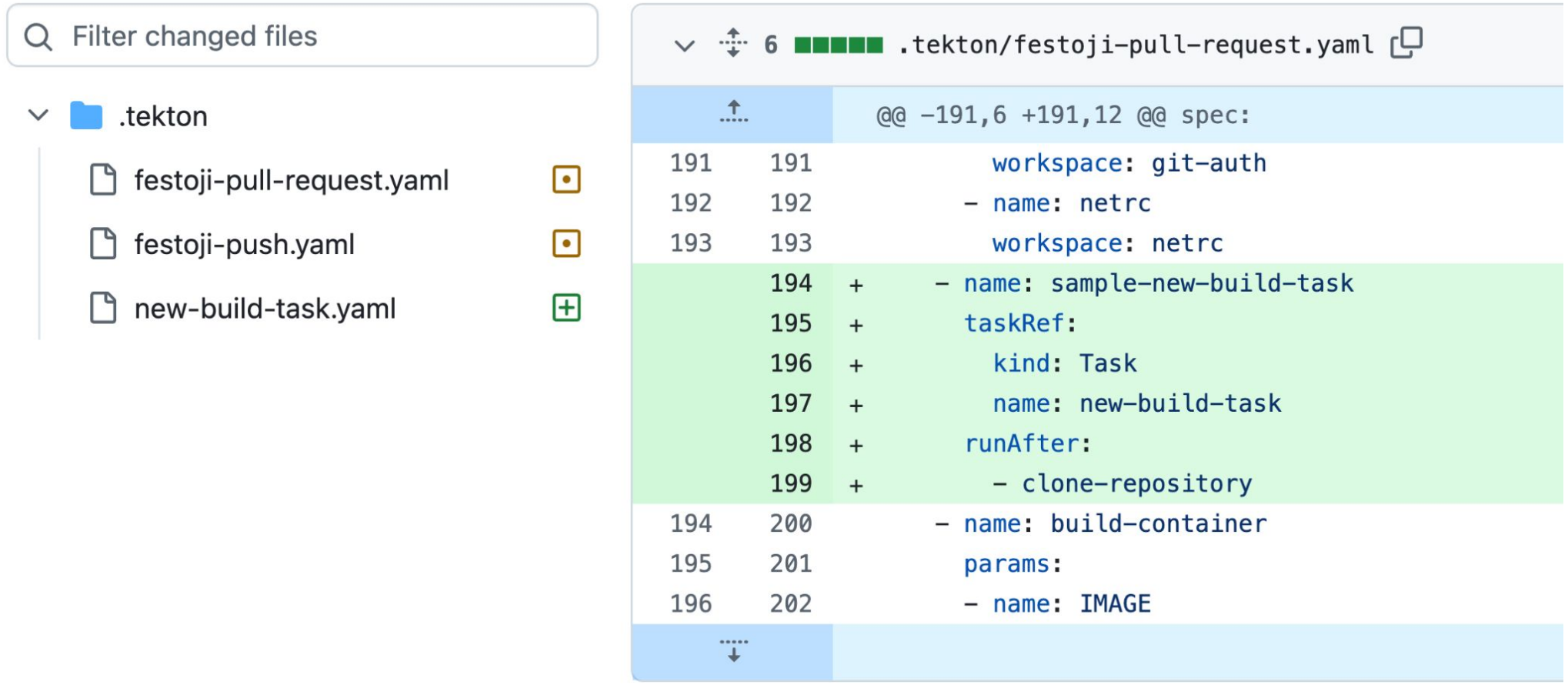
Devs can troubleshoot builds

```
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

```
$ oras manifest fetch --pretty
quay.io/konflux-ci/tekton-catalog/task-buildah-remote-oci-ta:0.4 | jq .annotations
{
  "dev.konflux-ci.task.previous-migration-bundle": "",
  "org.opencontainers.image.description": "Buildah task builds source code into a
container image and pushes the image into container registry using buildah tool.",
  "org.opencontainers.image.documentation":
"https://github.com/konflux-ci/build-definitions/tree/75741ae0dbd0e3ffa0414acc7fbc950740
e889ae/task/buildah-remote-oci-ta/0.4/README.md",
  "org.opencontainers.image.revision": "75741ae0dbd0e3ffa0414acc7fbc950740e889ae",
  "org.opencontainers.image.source": "https://github.com/konflux-ci/build-definitions",
  "org.opencontainers.image.url":
"https://github.com/konflux-ci/build-definitions/tree/75741ae0dbd0e3ffa0414acc7fbc950740
e889ae/task/buildah-remote-oci-ta/0.4",
  "org.opencontainers.image.version": "0.4"
}
```

Devs can explore new tech

- 

Devs don’t need to be this unhappy




Thank you!

@arewm

arewm@redhat.com

konflux-ci.dev

conforma.dev

hermetoproject.github.io/hermeto