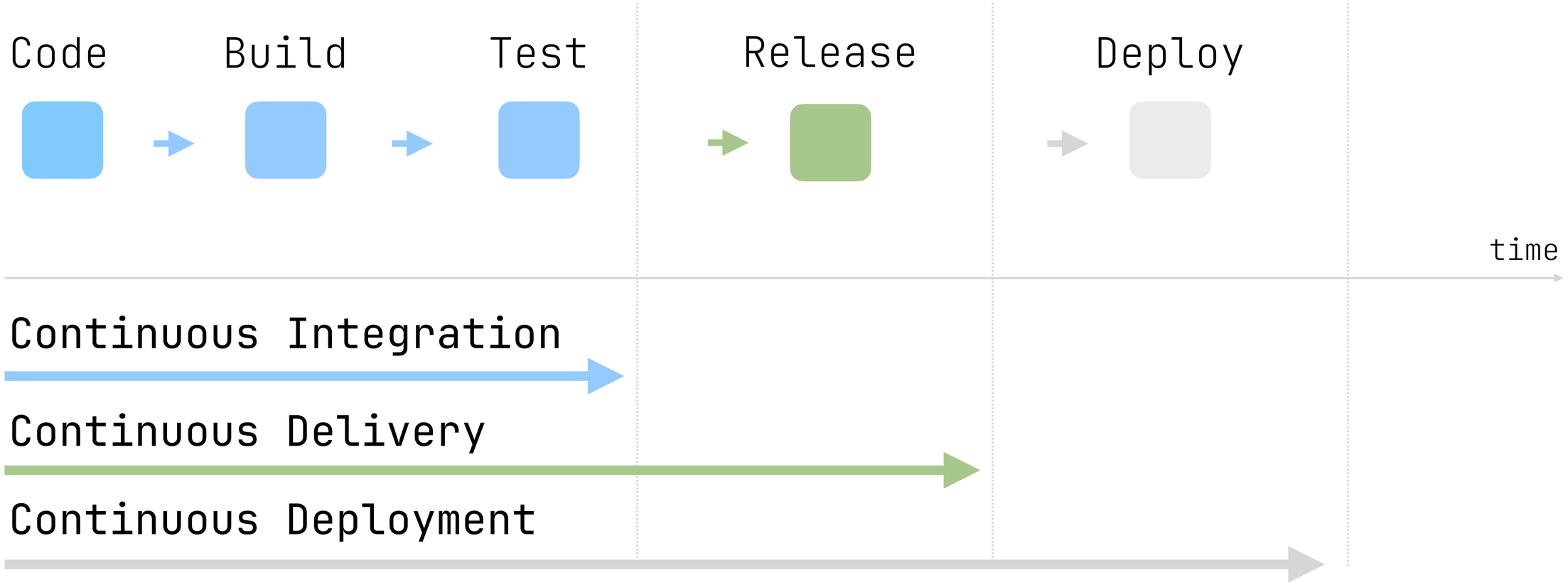
Streamlining Python Development: A Practical Approach to CI/CD with GitHub Actions

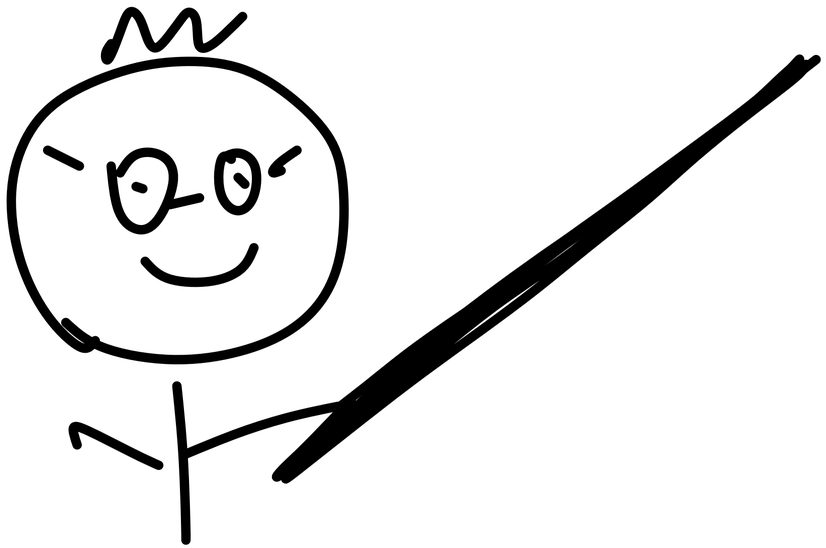
Artem Kislovskiy

Streamlining Python Development: A Practical Approach to CI/CD with GitHub Actions

Artem Kislovskiy

Kislovskiy/talks

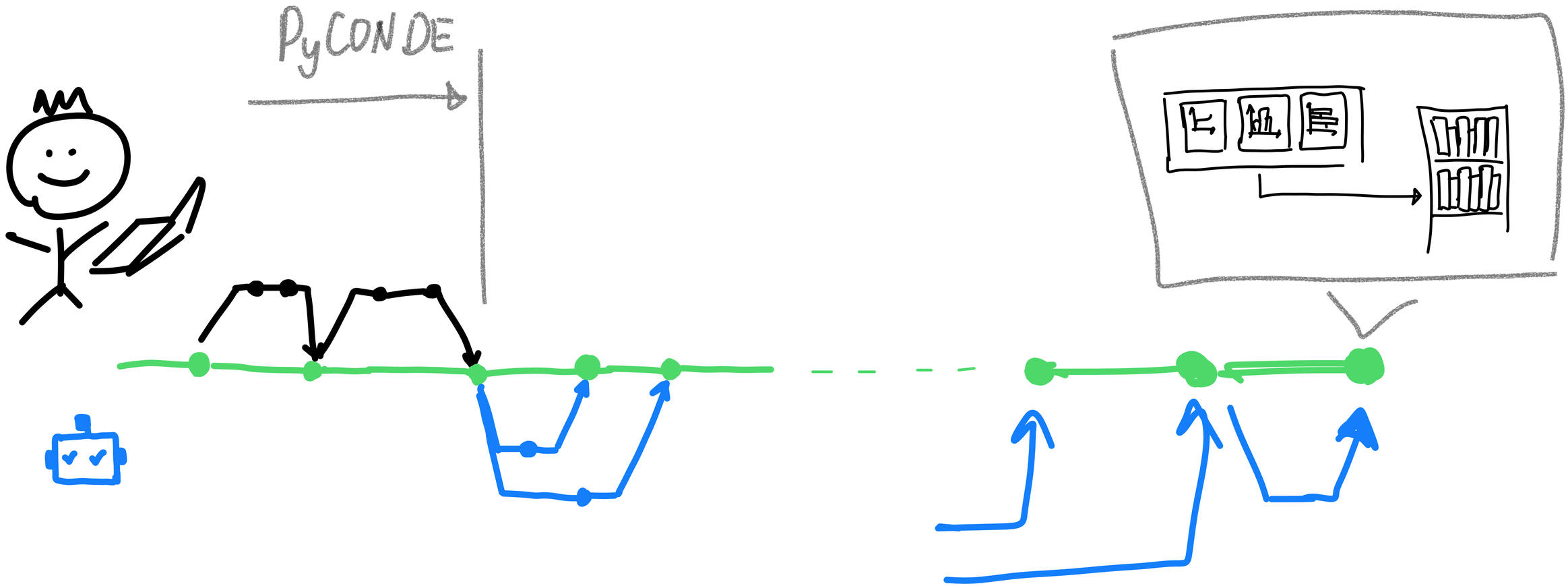

Code
Build
Test
Release
Deploy
time
Continuous Integration
Continuous Delivery
Continuous Deployment

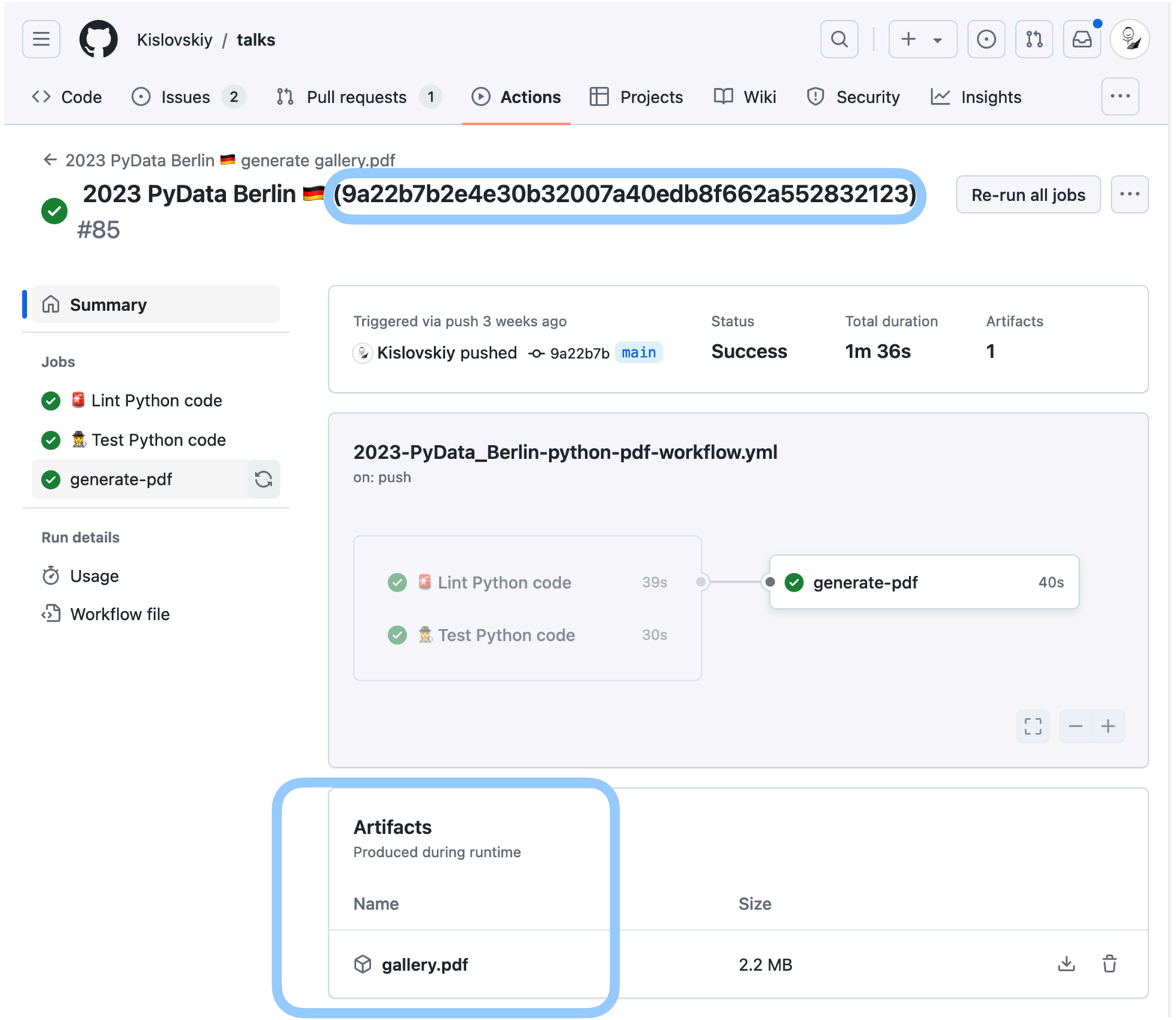


Continuous Integration

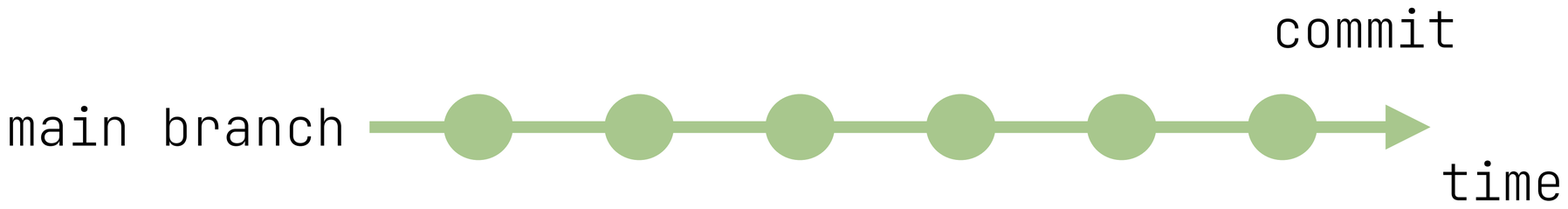
Process for speed, efficiency, reproducibility.

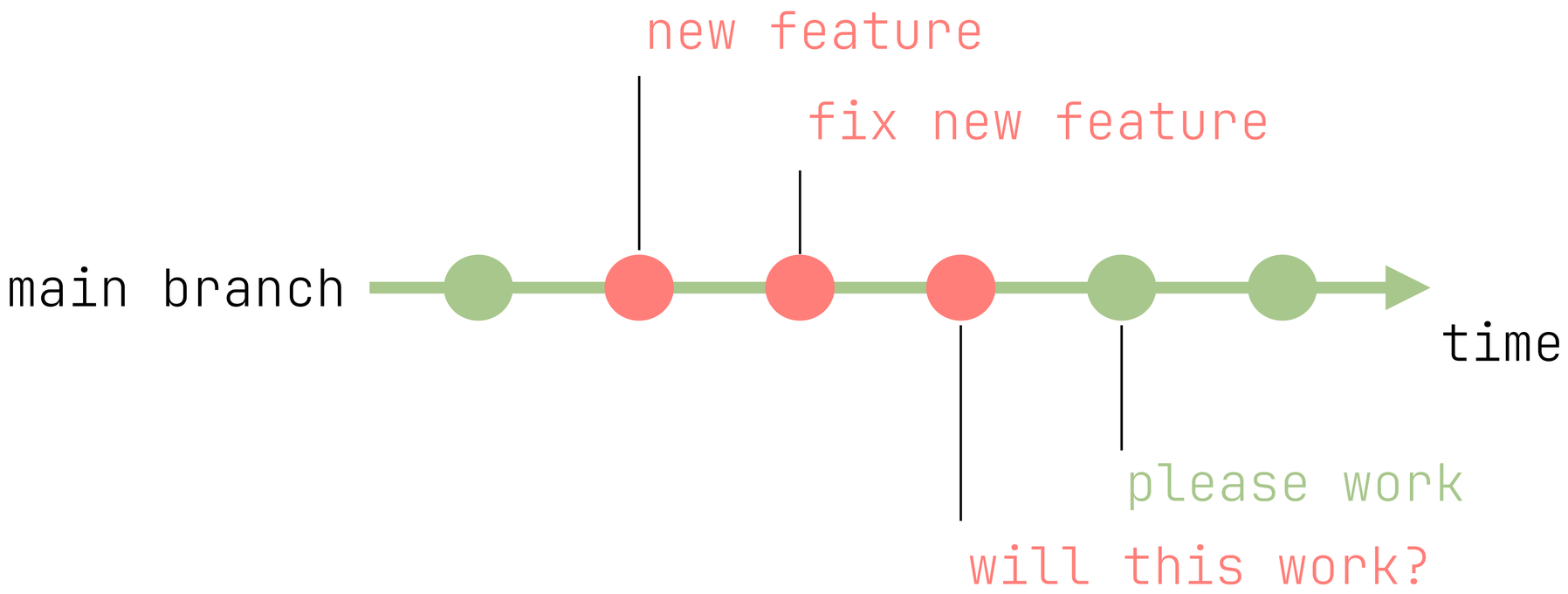

PyCon DE
2023 BERLIN
RETROSPECTIVE ON
MY DATA VIZ
MISTAKES
PyData
Berlin

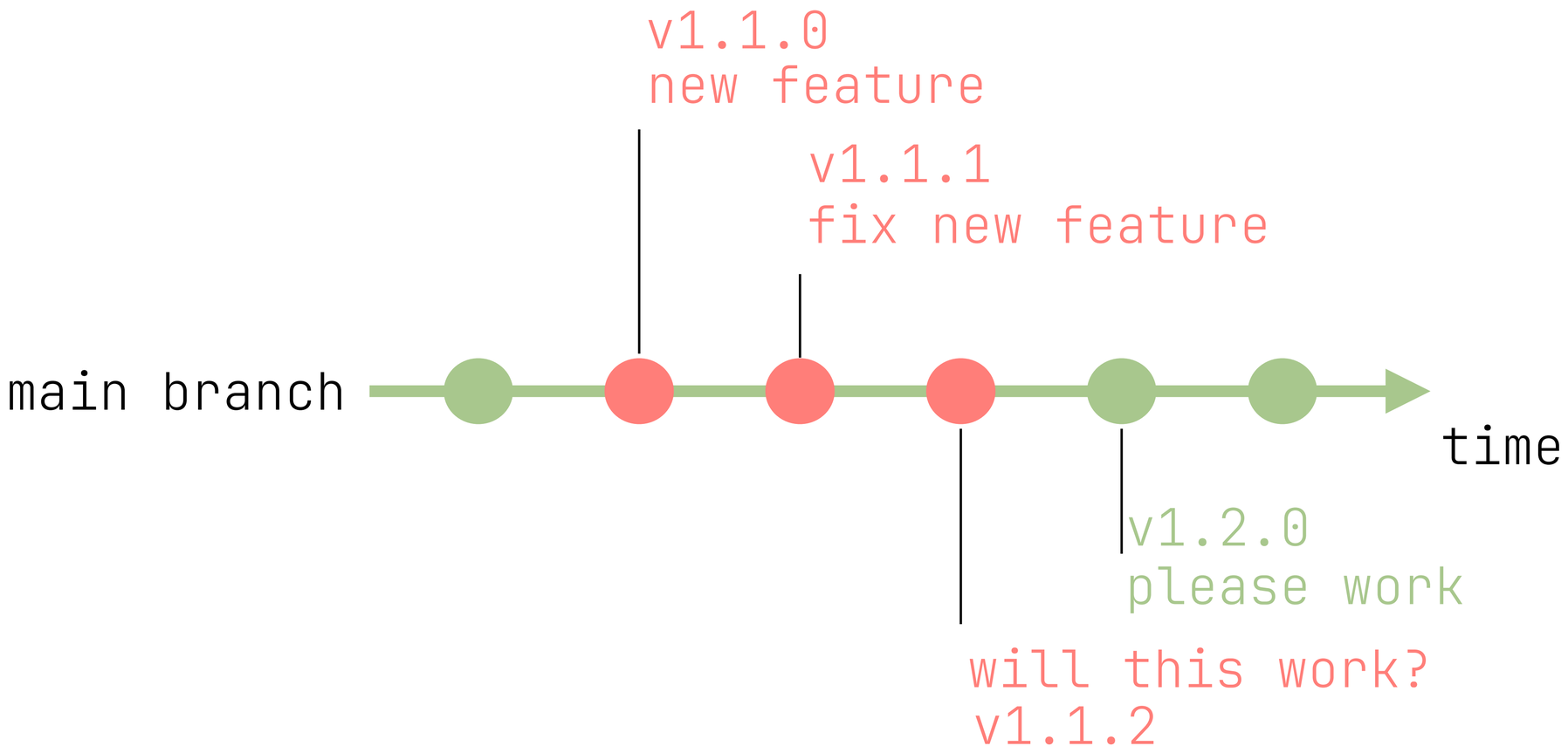

PyCONDE

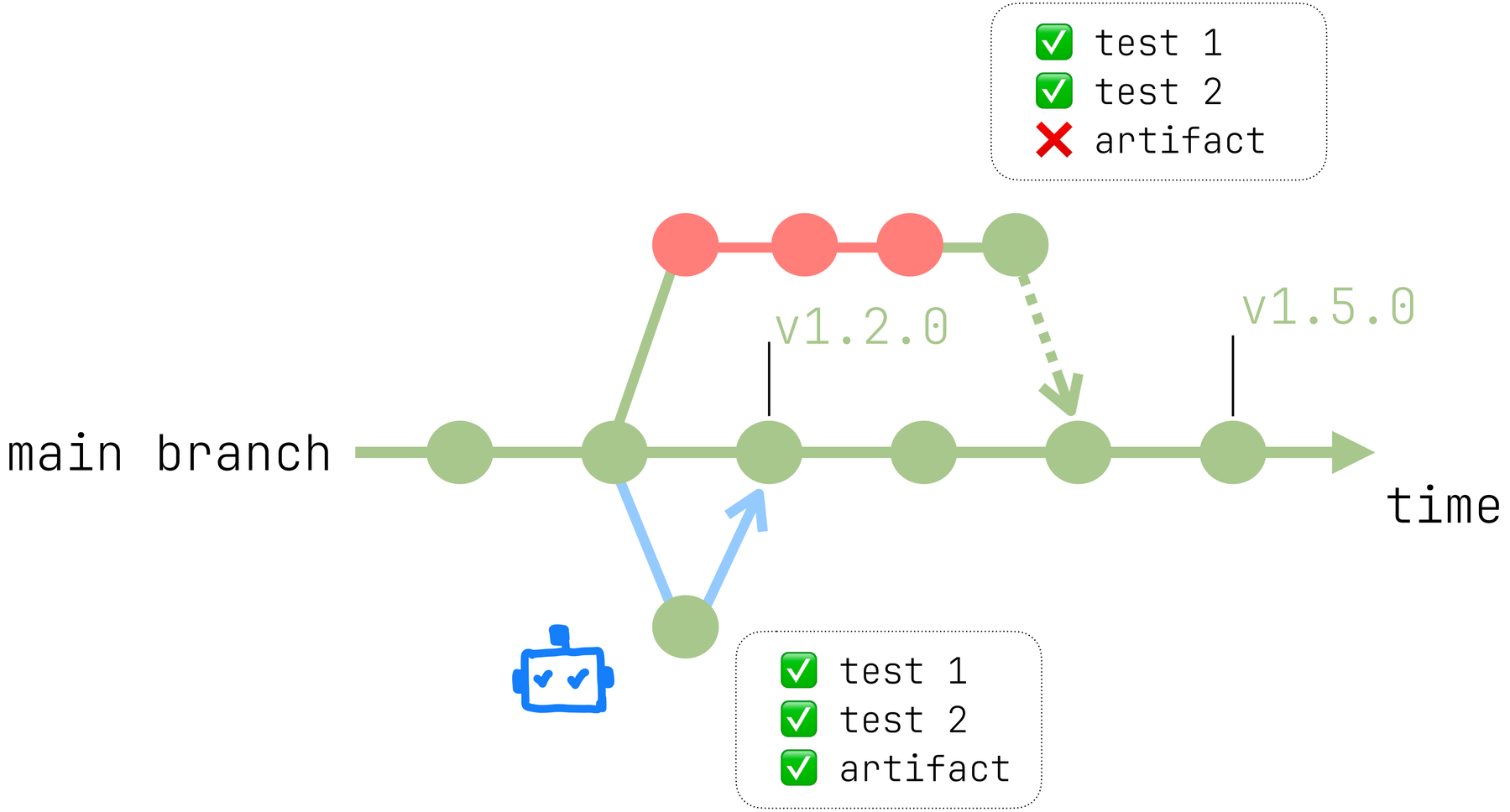


```
$ git show 9a22b7b2e4e30b32007a40edb8f662a552832123
commit 9a22b7b2e4e30b32007a40edb8f662a552832123
Author: renovate[bot] <29139614+renovate[bot]@users.noreply.github.com>
Date:   Sat Mar 23 11:28:11 2024 +0100

    Update dependency pandas to v2.2.1 (#59)

    Co-authored-by: renovate[bot]
<29139614+renovate[bot]@users.noreply.github.com>

diff --git a/2023_PyData_Berlin/requirements.txt b/2023_PyData_Berlin/
requirements.txt
index 4fad163..d29611e 100644
--- a/2023_PyData_Berlin/requirements.txt
+++ b/2023_PyData_Berlin/requirements.txt
@@ -1,5 +1,5 @@
 numpy==1.26.3
-pandas==2.2.0
+pandas==2.2.1
 matplotlib==3.8.2
 pytest==7.4.4
 flake8==7.0.0
```


commit
main branch
time


new feature
fix new feature
main branch
time
please work
will this work?


v1.1.0
new feature
v1.1.1
fix new feature
main branch
time
v1.2.0
please work
will this work?
v1.1.2


✅ test 1
✅ test 2
❌ artifact
v1.2.0
v1.5.0
main branch
time
✅ test 1
✅ test 2
✅ artifact

You just make a *.py* script, and it’s gravy, right? No need to install—just run the script in its directory!

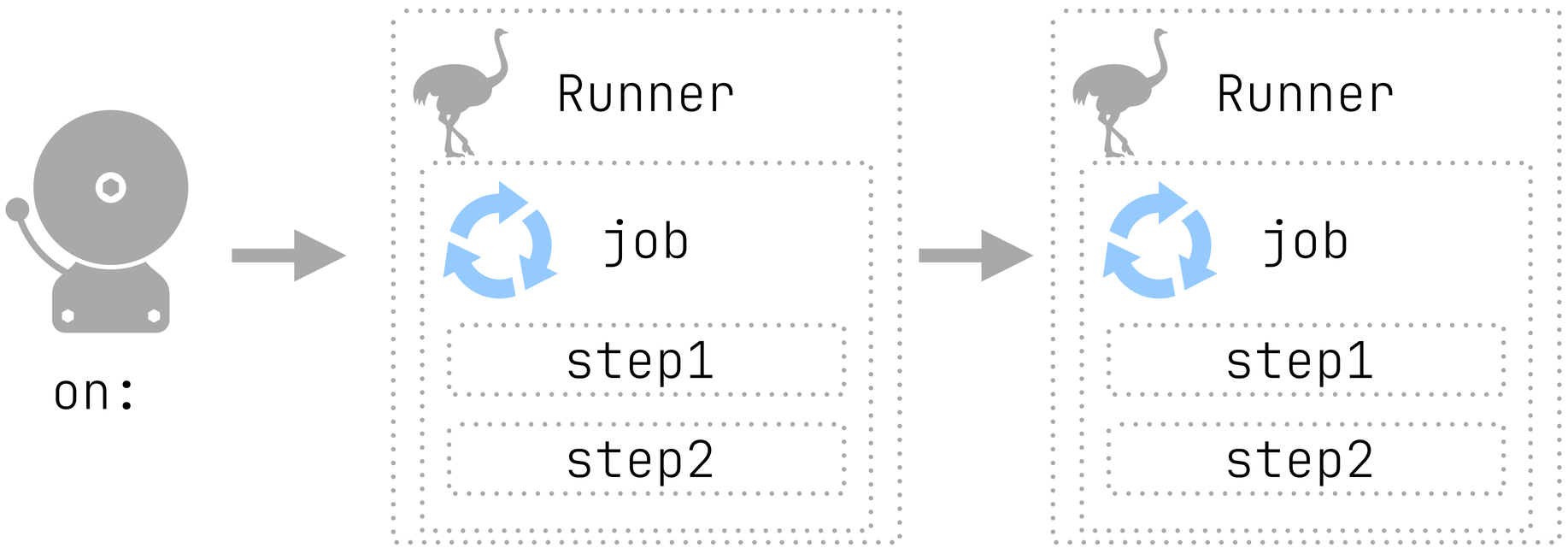
simplistic advice, overlooking crucial aspects of software development

Common layouts

```
helloworld/
├── .gitignore
├── helloworld.py
├── LICENSE
├── README.md
├── pyproject.toml
└── tests.py

├──.github
    └── workflows
        └── ci.yaml
```

```
helloworld/
├── helloworld/
│   ├── __init__.py
│   ├── helloworld.py
│   └── helpers.py
├── tests/
│   ├── helloworld_tests.py
│   └── helpers_tests.py
├── .gitignore
├── LICENSE
├── README.md
└── pyproject.toml
```

Anatomy of an Action



Anatomy of an Action

Workflow

```yaml
name: "2024 PyCON DE 🔬 Show Default Shell"
run-name: "MANUAL - 🔬 Show Default Shell (run by - ${{ github.triggering_actor }})"
on:
  workflow_dispatch:
```

Job

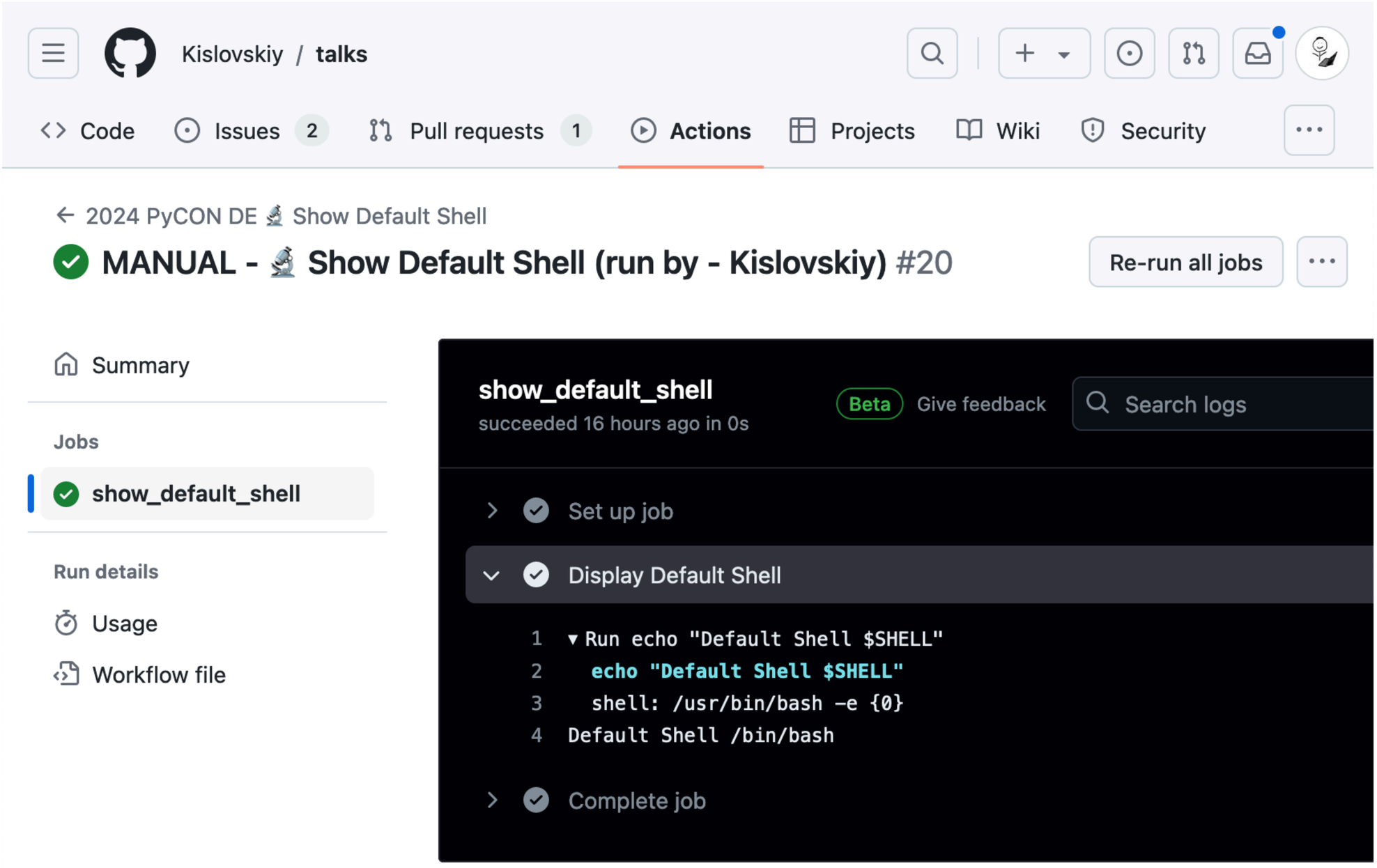
```yaml
jobs:
  show_default_shell:
    runs-on: ubuntu-latest
```

Step

```yaml
    steps:
```

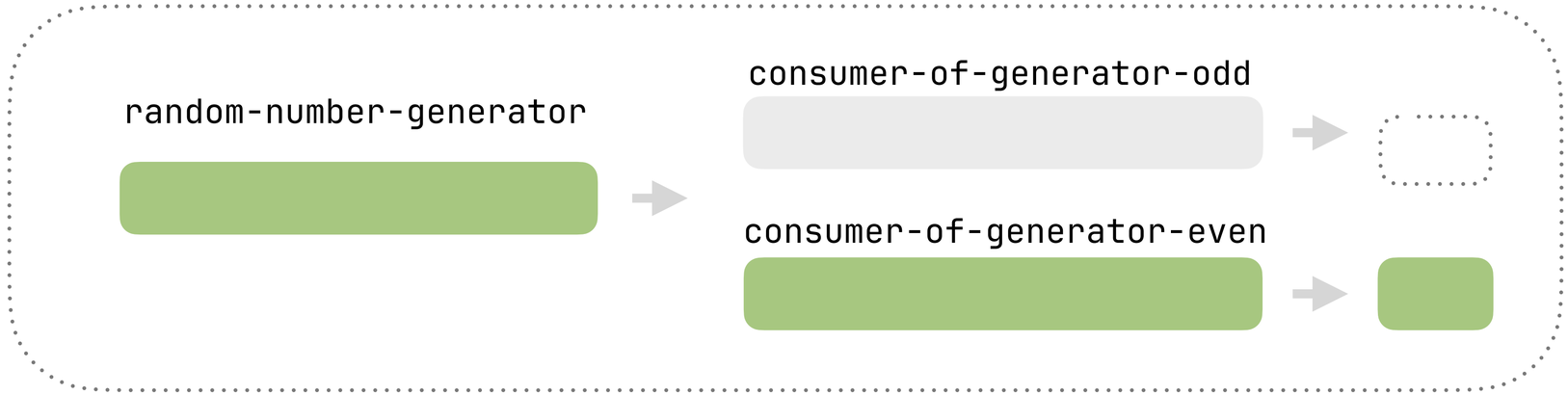
Action

```yaml
    - name: Display Default Shell
      run: echo "Default Shell $SHELL"
```

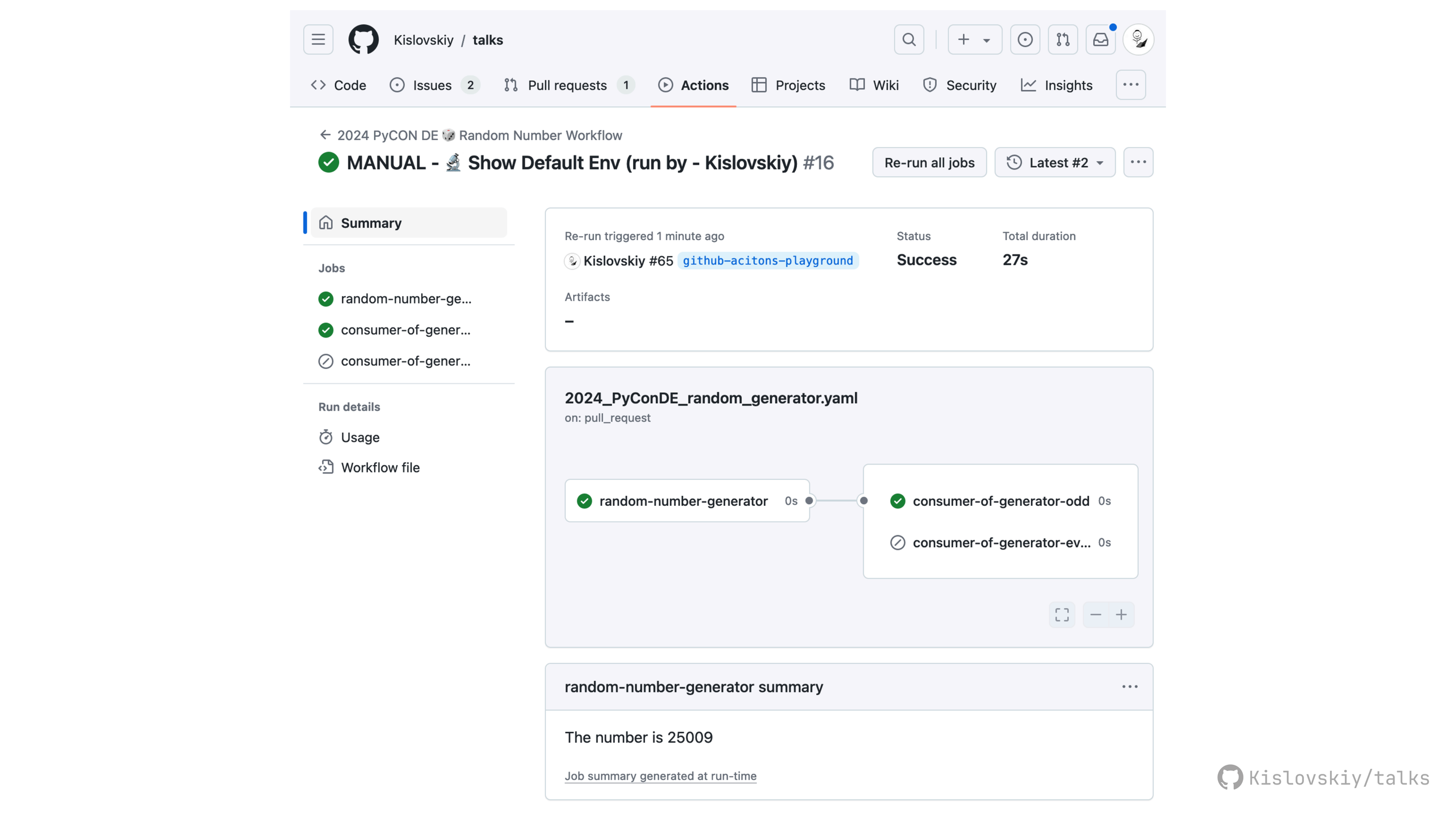

Kislovskiy / talks
Code
Issues 2
Pull requests 1
Actions
Projects
Wiki
Security
2024 PyCON DE Show Default Shell
MANUAL - Show Default Shell (run by - Kislovskiy) #20
Re-run all jobs
Summary
Jobs
show_default_shell
Run details
Usage
Workflow file
show_default_shell
succeeded 16 hours ago in 0s
Beta
Give feedback
Search logs
Set up job
Display Default Shell
1 ▼ Run echo "Default Shell $SHELL"
2 echo "Default Shell $SHELL"
3 shell: /usr/bin/bash -e {0}
4 Default Shell /bin/bash
Complete job

```yaml
name: "2024 PyCON DE ☠️ Show Environment"
run-name: "MANUAL - ☠️ Show Environment (run by - ${{ github.triggering_actor }})"

on:
 workflow_dispatch:

jobs:
  show_default_shell:
    runs-on: ubuntu-latest
    timeout-minutes: 1

    steps:
    - name: ☠️ Display Environment Variables Names
      run: |
        for var in $(printenv | cut -d "=" -f 1); do
          echo "$var"
        done >> $GITHUB_STEP_SUMMARY
```

2024_PyConDE_random_generator.yaml

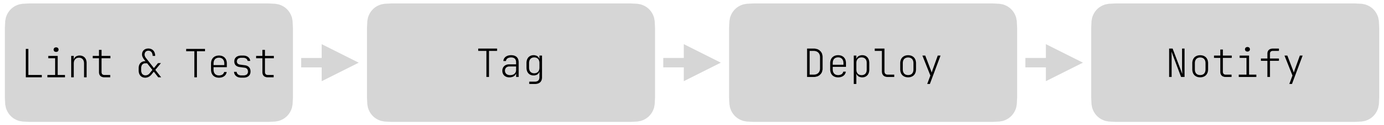


```yaml
jobs:
  random-number-generator:
   outputs:
      number: ${{ steps.generate-number.outputs.number }}
      is-even: ${{ steps.generate-number.outputs.is-even }}
   …

  consumer-of-generator-odd:
    needs: random-number-generator
    if: ${{ needs.random-number-generator.outputs.is-even == 0 }}
    …

  consumer-of-generator-even:
    needs: random-number-generator
    if: ${{ needs.random-number-generator.outputs.is-even == 1 }}
    …
```

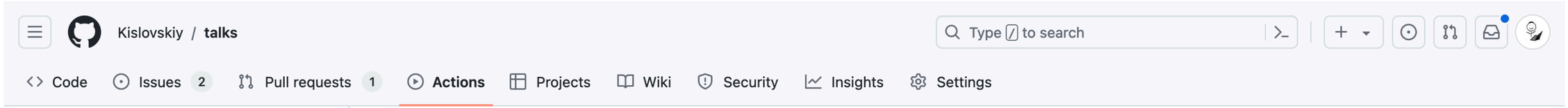


Good habits:

- Keep your CI blocks **atomic**



- Use **descriptive names**, and the **run-name** property
  - BUILD-
  - EVENT-
  - MANUAL-



Actions

New workflow

All workflows

Workflows

- .github/workflows/2023-PyData_Berlin-py...
- .github/workflows/2024_PyConDE_trigger...
- 2023 EuroSciPy 🇨🇭 Continuous Integration...
- 2023 PyConIT 🇮🇹 generate gallery.pdf
- 2024 PyCON DE 🎲 Random Number Work...
- 2024 PyCON DE 🔬 Show Default Env
- 2024 PyCON DE 🔬 Show Default Shell
- Show Default Shell
- Show Environemnt

Management

- Caches
- Deployments
- Runners

All workflows

Showing runs from all workflows

Filter workflow runs

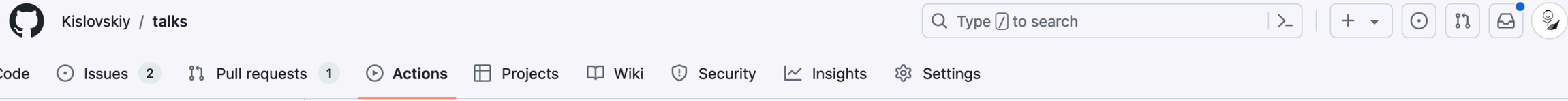
Help us improve GitHub Actions
Tell us how to make GitHub Actions work better for you with three quick questions.

Give feedback

414 workflow runs Event Status Branch Actor

✅ **BUILD - 2023 PyConIT (pull_request)** **2023 PyConIT 🇮🇹 generate gallery.pdf** #28: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	13 hours ago 14s	...
✅ **MANUAL - 🔬 Show Default Env (run by - Kislovskiy)** **2024 PyCON DE 🎲 Random Number Workflow** #10: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	13 hours ago 23s	...
✅ **BUILD - 2023 EuroSciPy (pull_request)** **2023 EuroSciPy 🇨🇭 Continuous Integration Demo** #27: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	13 hours ago 11s	...
✅ **MANUAL - 🔬 Show Default Env (run by - Kislovskiy)** **2024 PyCON DE 🔬 Show Default Env** #20: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	13 hours ago 10s	...
✅ **MANUAL - 🔬 Show Default Shell (run by - Kislovskiy)** **2024 PyCON DE 🔬 Show Default Shell** #20: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	13 hours ago 10s	...
❌ **full path** **.github/workflows/2023-PyData_Berlin-python-pdf-workflow.yaml** #50: Commit 22c641b pushed by Kislovskiy	`github-acitons-playground`	13 hours ago *Failure*	...

Observability matters



Actions

New workflow

All workflows

Workflows

- 2023 EuroSciPy 🇨🇭 Continuous Integration...
- 2023 PyConIT 🇮🇹 generate gallery.pdf
- **2023 PyData Berlin 🇩🇪 generate gallery....**
- 2024 PyCON DE 🔬 Show Default Env
- 2024 PyCON DE 🔬 Show Default Shell
- Show Default Shell
- Show Environemnt

Management

- Caches
- Deployments
- Runners

2023 PyData Berlin 🇩🇪 generate gallery.pdf

2023-PyData_Berlin-python-pdf-workflow.yaml

workflow:

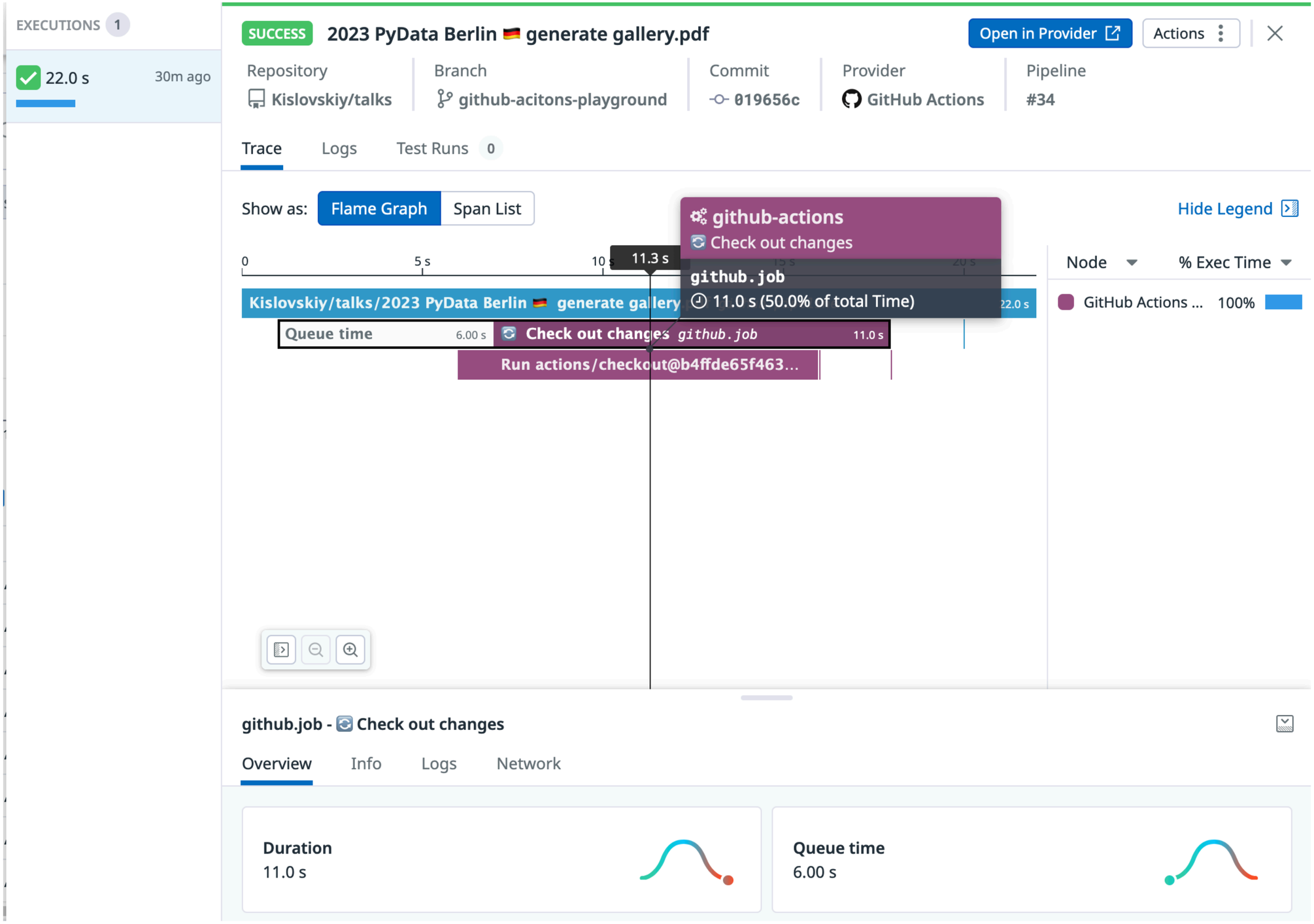
Help us improve GitHub Actions
Tell us how to make GitHub Actions work better for you with three quick questions.

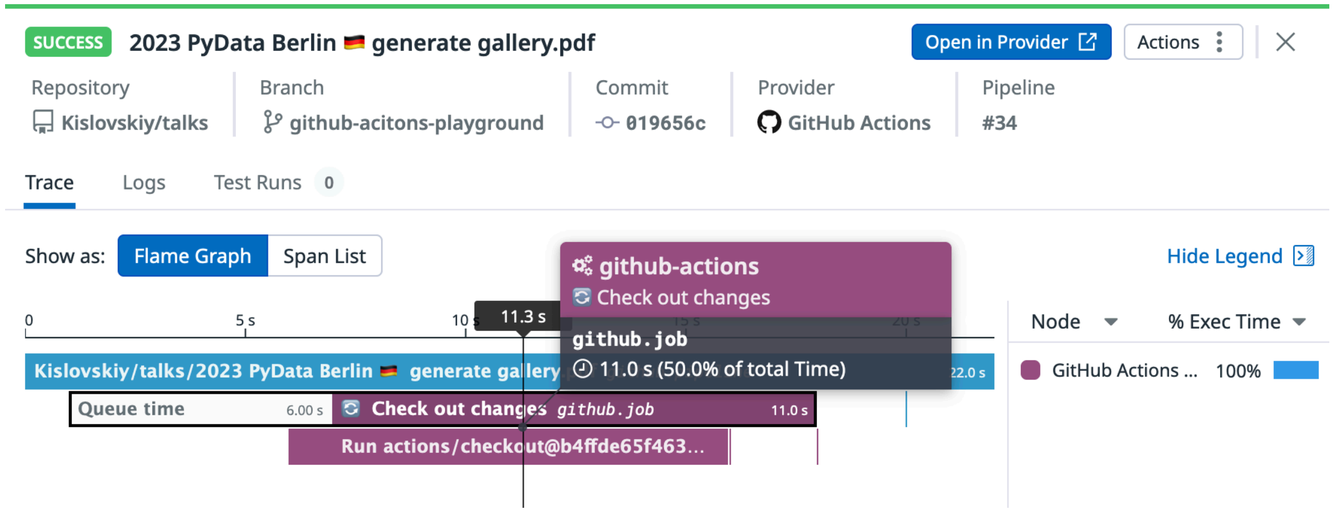
Give feedback

23 workflow run results

Event | Status | Branch | Actor

BUILD - 2023 PyData Berlin (pull_request) **2023 PyData Berlin 🇩🇪 generate gallery.pdf** #37: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	45 minutes ago	11s
BUILD - 2023 PyData Berlin (pull_request) **2023 PyData Berlin 🇩🇪 generate gallery.pdf** #36: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	48 minutes ago	14s
BUILD - 2023 PyData Berlin (pull_request) **2023 PyData Berlin 🇩🇪 generate gallery.pdf** #35: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	1 hour ago	15s
BUILD - 2023 PyData Berlin (pull_request) **2023 PyData Berlin 🇩🇪 generate gallery.pdf** #34: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	1 hour ago	22s
BUILD - 2023 PyData Berlin (pull_request) **2023 PyData Berlin 🇩🇪 generate gallery.pdf** #33: Pull request #65 synchronize by Kislovskiy	`github-acitons-playground`	1 hour ago	27s
BUILD - 2023 PyData Berlin (pull_request)	`github-acitons-playground`	1 hour ago	


EXECUTIONS 1
22.0 s
30m ago
SUCCESS
2023 PyData Berlin 🇩🇪 generate gallery.pdf
Open in Provider
Actions
Repository
Kislovskiy/talks
Branch
github-acitons-playground
Commit
019656c
Provider
GitHub Actions
Pipeline
#34
Trace
Logs
Test Runs 0
Show as:
Flame Graph
Span List
Hide Legend
github-actions
Check out changes
github.job
11.0 s (50.0% of total Time)
0
5 s
10 s
11.3 s
Kislovskiy/talks/2023 PyData Berlin 🇩🇪 generate gallery
22.0 s
Queue time
6.00 s
Check out changes
github.job
11.0 s
Run actions/checkout@b4ffde65f463...
Node
% Exec Time
GitHub Actions ...
100%
github.job - Check out changes
Overview
Info
Logs
Network
Duration
11.0 s
Queue time
6.00 s




```yaml
jobs:
  changes:
    name: 🔄 Check out changes
    runs-on: ubuntu-latest
    timeout-minutes: 1
    permissions:
      pull-requests: read
    steps:
    - uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4.1.1
    - name: Check for file changes in 2023_PyData_Berlin
      uses: dorny/paths-filter@de90cc6fb38fc0963ad72b210f1f284cd68cea36 #v3.0.2
      id: changes
      with:
        filters: |
          changes:
          - "2023_PyData_Berlin/**/*.py"
          - "2023_PyData_Berlin/**/*.ipynb"
          - "2023_PyData_Berlin/requirements.txt"
```

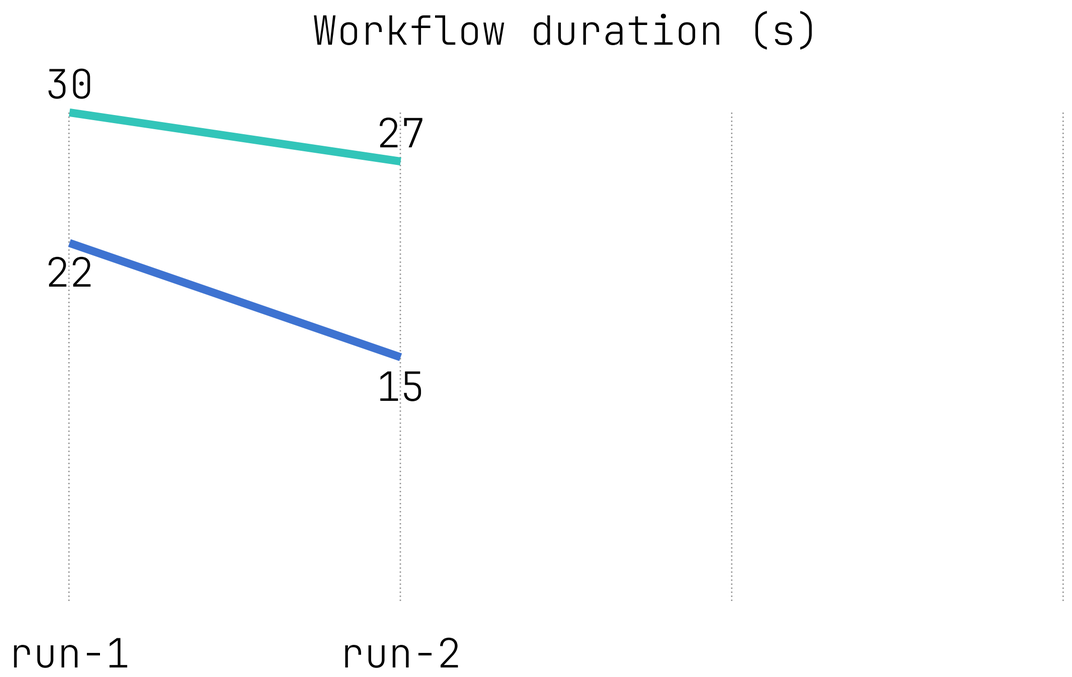
3

.github/workflows/2023-PyData_Berlin-python-pdf-workflow.yaml

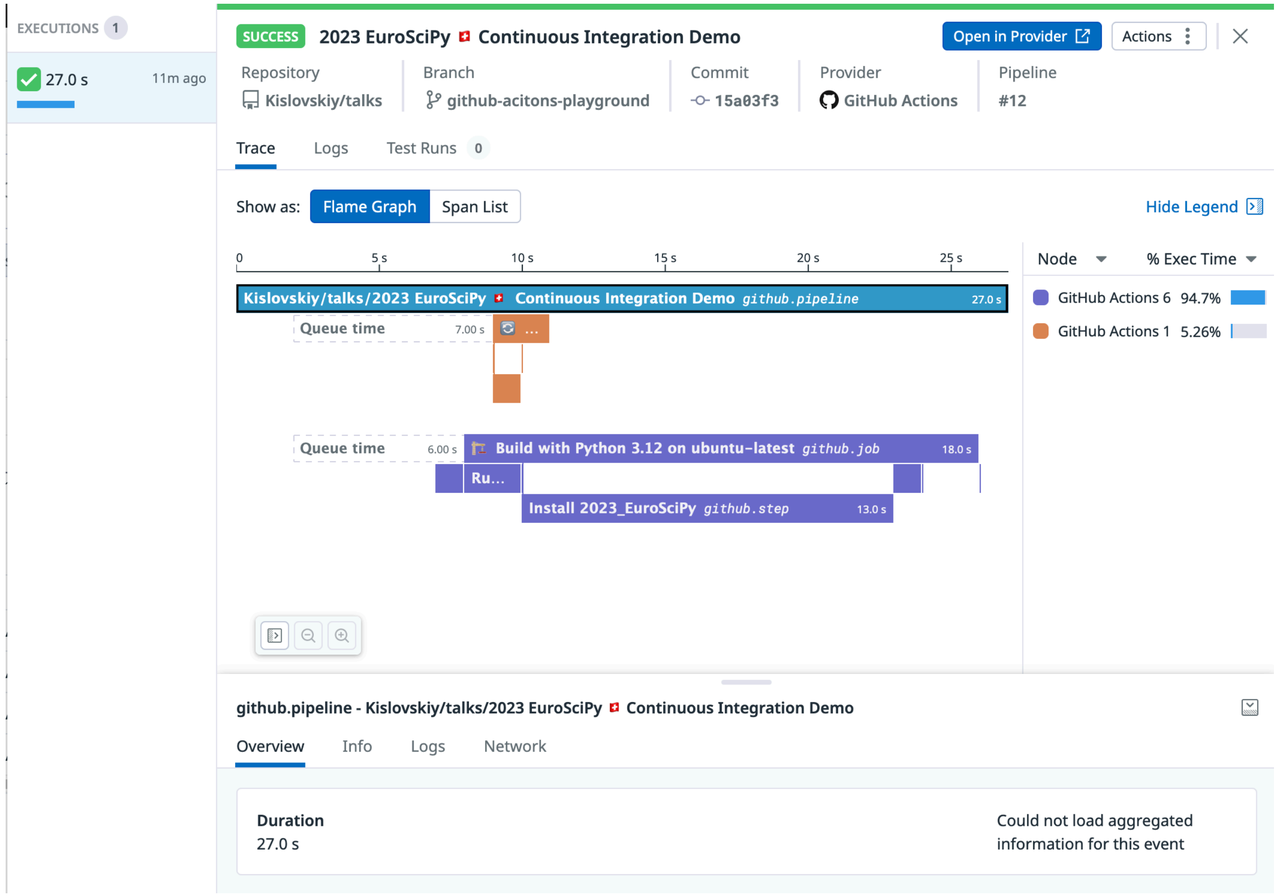
```
@@ -22,10 +22,9 @@ jobs:
22 22       timeout-minutes: 1
23 23       permissions:
24 24         pull-requests: read
27 25       steps:
28 26       - uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4.1.1
   27 +       if: github.ref == 'refs/heads/main'  # Only checkout when the branch is 'main'
29 28       - name: Check for backend file changes
30 29         uses: dorny/paths-filter@de90cc6fb38fc0963ad72b210f1f284cd68cea36 #v3.0.2
31 30         id: changes
```

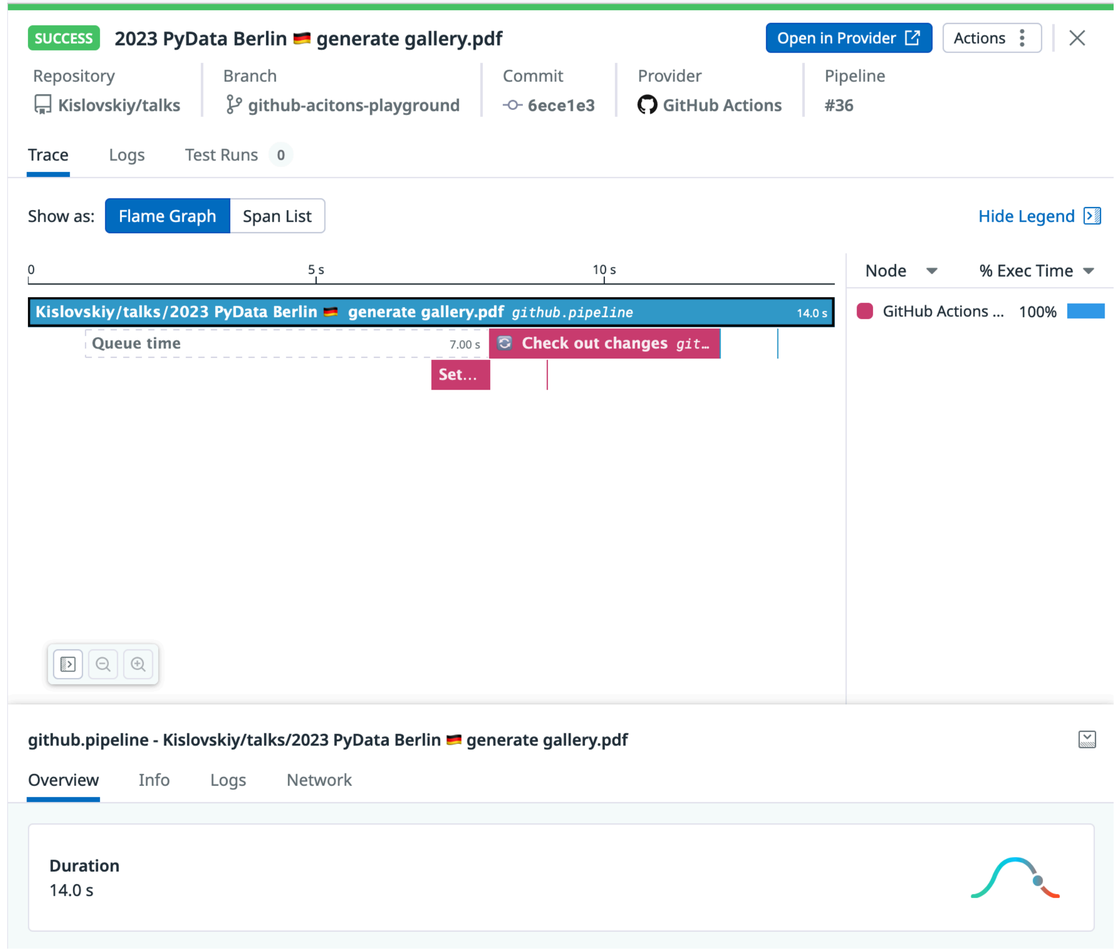
3 .github/workflows/2023_EuroSciPy_workflow.yaml

```
@@ -19,10 +19,9 @@ jobs:
19 19       timeout-minutes: 1
20 20       permissions:
21 21         pull-requests: read
24 22       steps:
25 23       - uses: actions/checkout@b4ffde65f46336ab88eb53be808477a3936bae11 # v4.1.1
   24 +       if: github.ref == 'refs/heads/main'  # Only checkout when the branch is 'main'
26 25       - name: Check for backend file changes
27 26         uses: dorny/paths-filter@de90cc6fb38fc0963ad72b210f1f284cd68cea36 #v3.0.2
28 27         id: changes
```



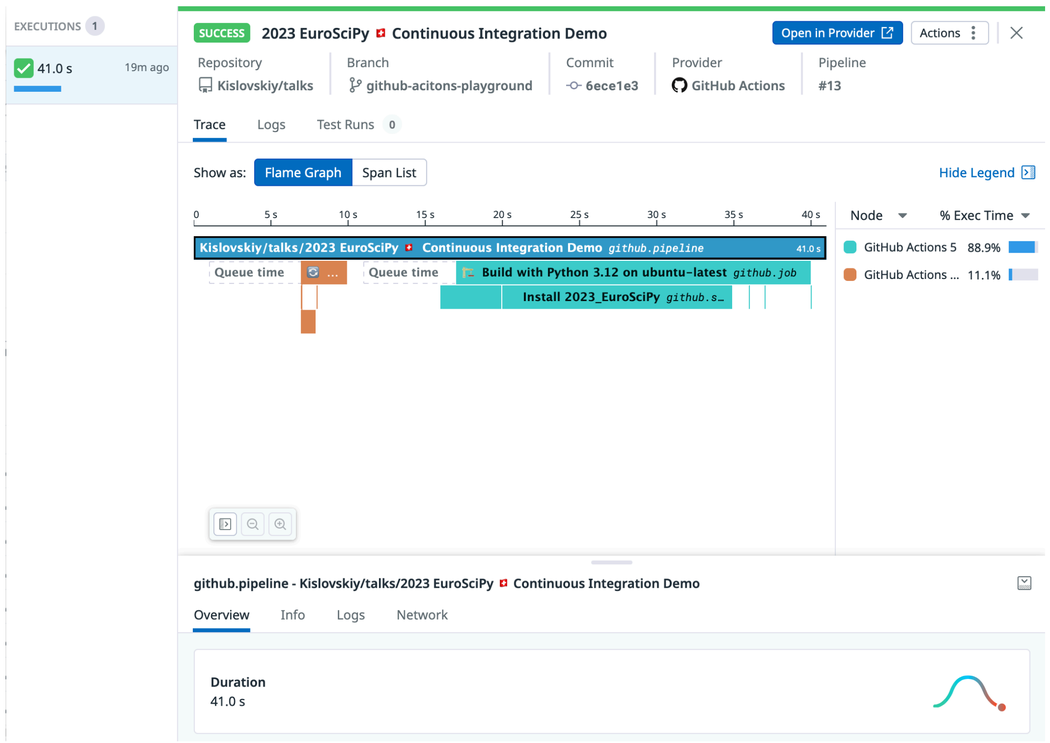
DATE	PIPELINE NAME	DURATION	PIPEL...	REPOSITORY N...	BRANCH	STAGE BR
Apr 13 16:44:50.000	2023 PyData Berlin 🇩🇪 generate gallery.pdf	15.0 s	#35	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:33:40.000	2023 PyData Berlin 🇩🇪 generate gallery.pdf	22.0 s	#34	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:45:01.000	2023 EuroSciPy 🇨🇭 Continuous Integration Demo	27.0 s	#12	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:33:48.000	2023 EuroSciPy 🇨🇭 Continuous Integration Demo	30.0 s	#11	Kislovskiy/talks	github-acitons-playground	

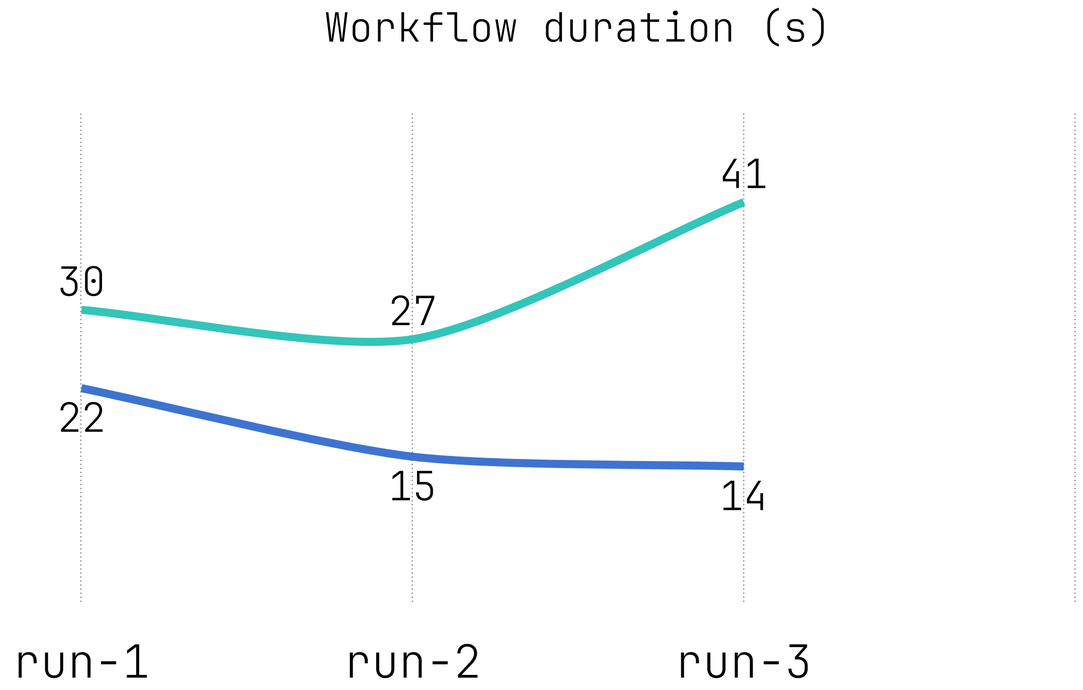




1 .github/workflows/2023_EuroSciPy_workflow.yaml

```
@@ -33,6 +33,7 @@ jobs:
33 33             - "2023_EuroSciPy/requirements.txt"
34 34       build:
35 35         name: 🏗 Build with Python ${{ matrix.python-version }} on ${{ matrix.os }}
36 +         needs: changes
36 37         runs-on: ${{ matrix.os }}
37 38
38 39         strategy:
```



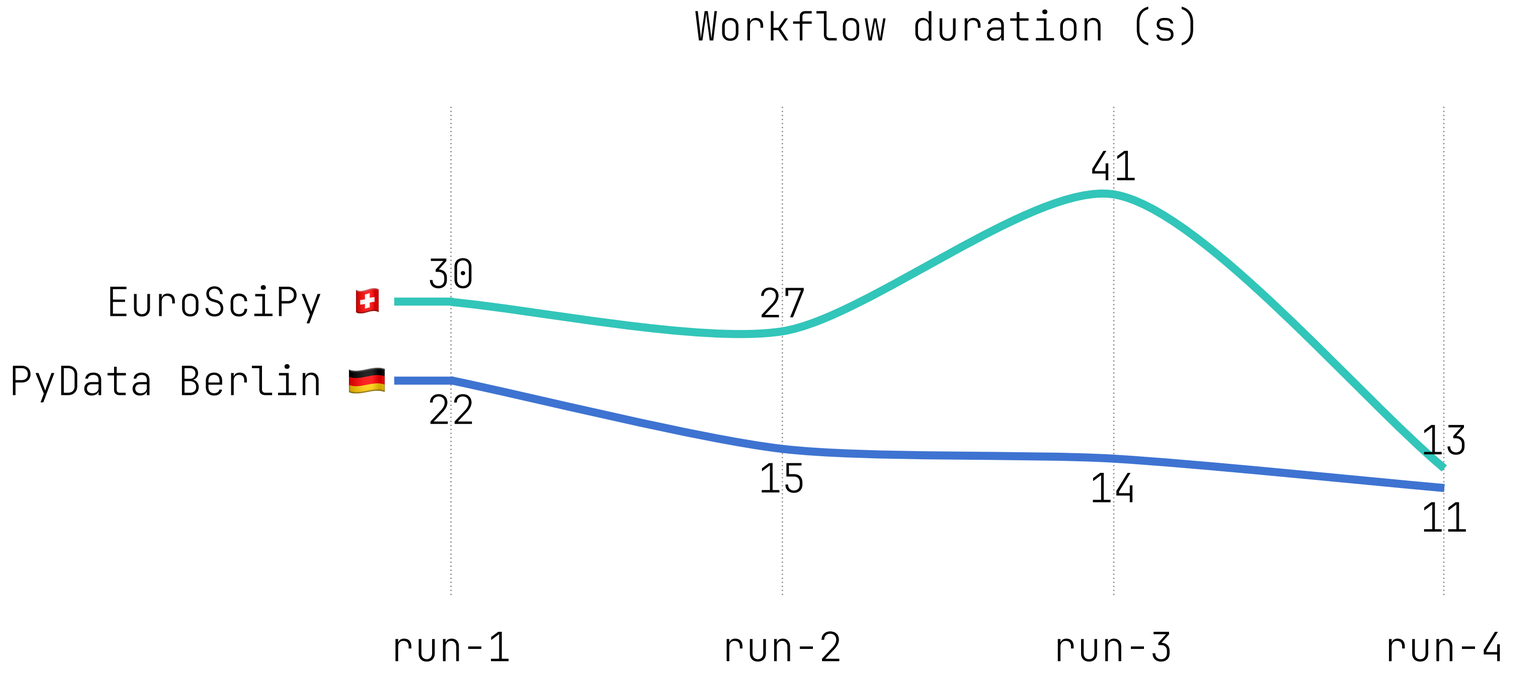


1 .github/workflows/2023_EuroSciPy_workflow.yaml

```
@@ -33,6 +33,7 @@ jobs:
33 33             - "2023_EuroSciPy/requirements.txt"
34 34       build:
35 35         name: 🏗 Build with Python ${{ matrix.python-version }} on ${{ matrix.os }}
   36 +       needs: changes
36 37         runs-on: ${{ matrix.os }}
37 38
38 39         strategy:
```

1 .github/workflows/2023_EuroSciPy_workflow.yaml

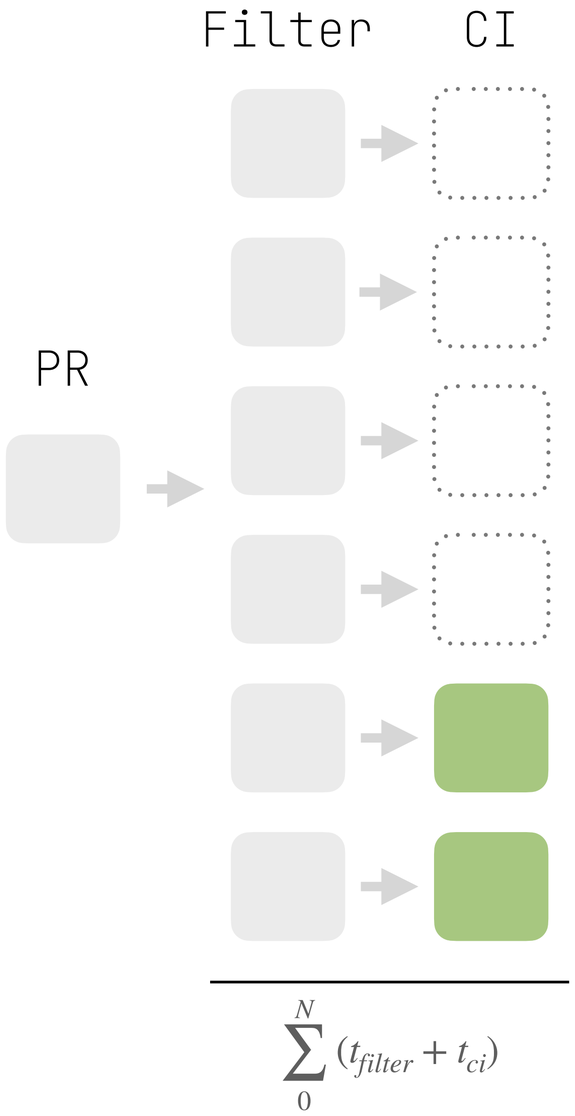
```
@@ -34,6 +34,7 @@ jobs:
34 34       build:
35 35         name: 🏗 Build with Python ${{ matrix.python-version }} on ${{ matrix.os }}
36 36         needs: changes
   37 +       if: needs.changes.outputs.changes == 'true'
37 38         runs-on: ${{ matrix.os }}
38 39
39 40         strategy:
```

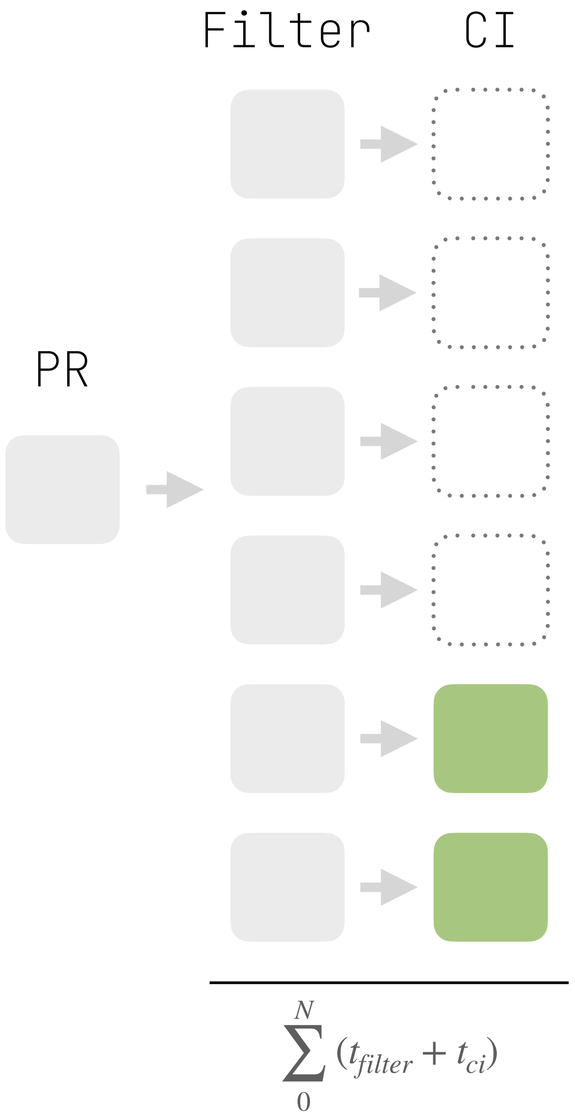


DATE	PIPELINE NAME	DURATION	PIPEL...	REPOSITORY N...	BRANCH	STAGE BREA
Apr 13 16:59:54.000	**2023 PyData Berlin 🇩🇪 generate gallery.pdf**	11.0 s	#37	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:56:38.000	**2023 PyData Berlin 🇩🇪 generate gallery.pdf**	14.0 s	#36	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:44:50.000	**2023 PyData Berlin 🇩🇪 generate gallery.pdf**	15.0 s	#35	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:33:40.000	**2023 PyData Berlin 🇩🇪 generate gallery.pdf**	22.0 s	#34	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:59:56.000	**2023 EuroSciPy 🇨🇭 Continuous Integration Demo**	13.0 s	#14	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:57:05.000	**2023 EuroSciPy 🇨🇭 Continuous Integration Demo**	41.0 s	#13	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:45:01.000	**2023 EuroSciPy 🇨🇭 Continuous Integration Demo**	27.0 s	#12	Kislovskiy/talks	github-acitons-playground	
Apr 13 16:33:48.000	**2023 EuroSciPy 🇨🇭 Continuous Integration Demo**	30.0 s	#11	Kislovskiy/talks	github-acitons-playground	

Why do I care?

```
./talks
├── .github
│   └── workflows
│       ├── 2023-PyConIT-workflow.yaml
│       ├── 2023-PyData_Berlin-python-pdf-workflow.yaml
│       ├── 2023_EuroSciPy_workflow.yaml
│       ├── 2024_PyConDE_explore_default_shell.yaml
│       ├── 2024_PyConDE_explore_environemnt.yaml
│       ├── 2024_PyConDE_random_generator.yaml
│       ├── 2024_PyConDE_reusable_workflow.yaml
│       └── 2024_PyConDE_trigger_workflow.yaml
├── .gitignore
├── .pre-commit-config.yaml
├── 2023_EuroSciPy
│   ├── src
│   └── tests
├── 2023_PyConIT
│   ├── src
│   └── tests
├── 2023_PyData_Berlin
│   ├── README.md
│   ├── requirements.txt
│   ├── src
│   └── tests
├── LICENSE
├── README.md
└── renovate.json
```






```yaml
name: "2023 PyData Berlin 🇩🇪 generate gallery.pdf"
run-name: "BUILD - 2023 PyData Berlin (${{ github.event_name }})"
on:
  pull_request:
  …
jobs:
  changes:
    …
    steps:
    …
    - name: Check for 2023_PyData_Berlin file changes
      uses: dorny/paths-filter@de90cc6fb38fc0963ad72b210f1f284cd68cea36 #v3.0.2
      id: filter
      with:
        filters: |
          PyDataBerlinChanges:
          - "2023_PyData_Berlin/**/*.py"
          - "2023_PyData_Berlin/**/*.ipynb"
          - "2023_PyData_Berlin/requirements.txt"
  lint:
    name: 🚨 Lint Python code
    if: ${{ needs.changes.outputs.PyDataBerlinChanges == 'true' }}
    needs: changes
```

DATADOG

Go to... ⌘ + K

Recent
Dashboards
Monitors
Watchdog
Service Mgmt
Infrastructure
APM
Digital Experience
Software Delivery
Security
Metrics
Logs
Integrations

artem.kislovskiy...
unk

Invite Support Help

CI Visibility - Pipelines dashboard

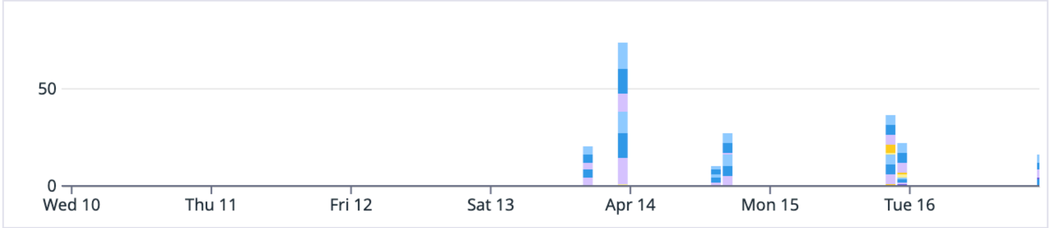
Share Show Overlays Configure Clone

provider_name: * | pipeline_name: * | branch_name: * | is_default_branch: * | provider_instance: * | env: *

1w Past 1 Week

Pipelines

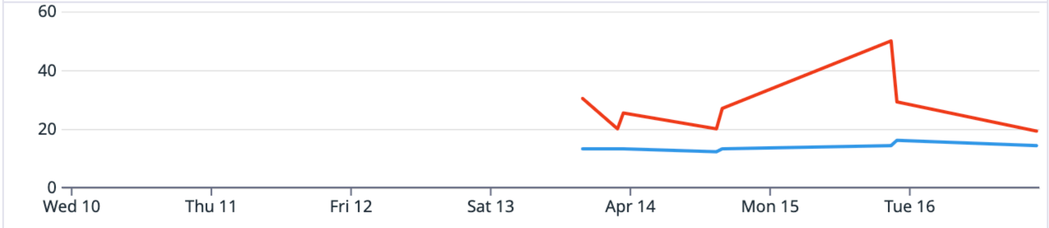
Pipeline executions



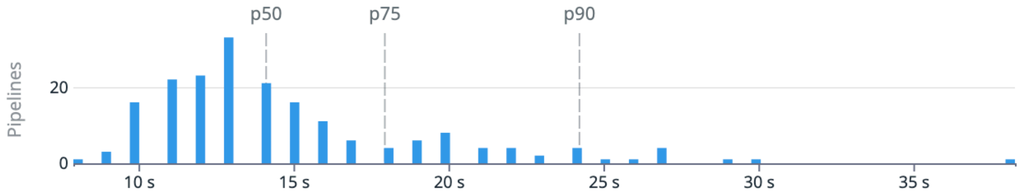
Pipeline overall success rate

98.04%

Pipeline duration



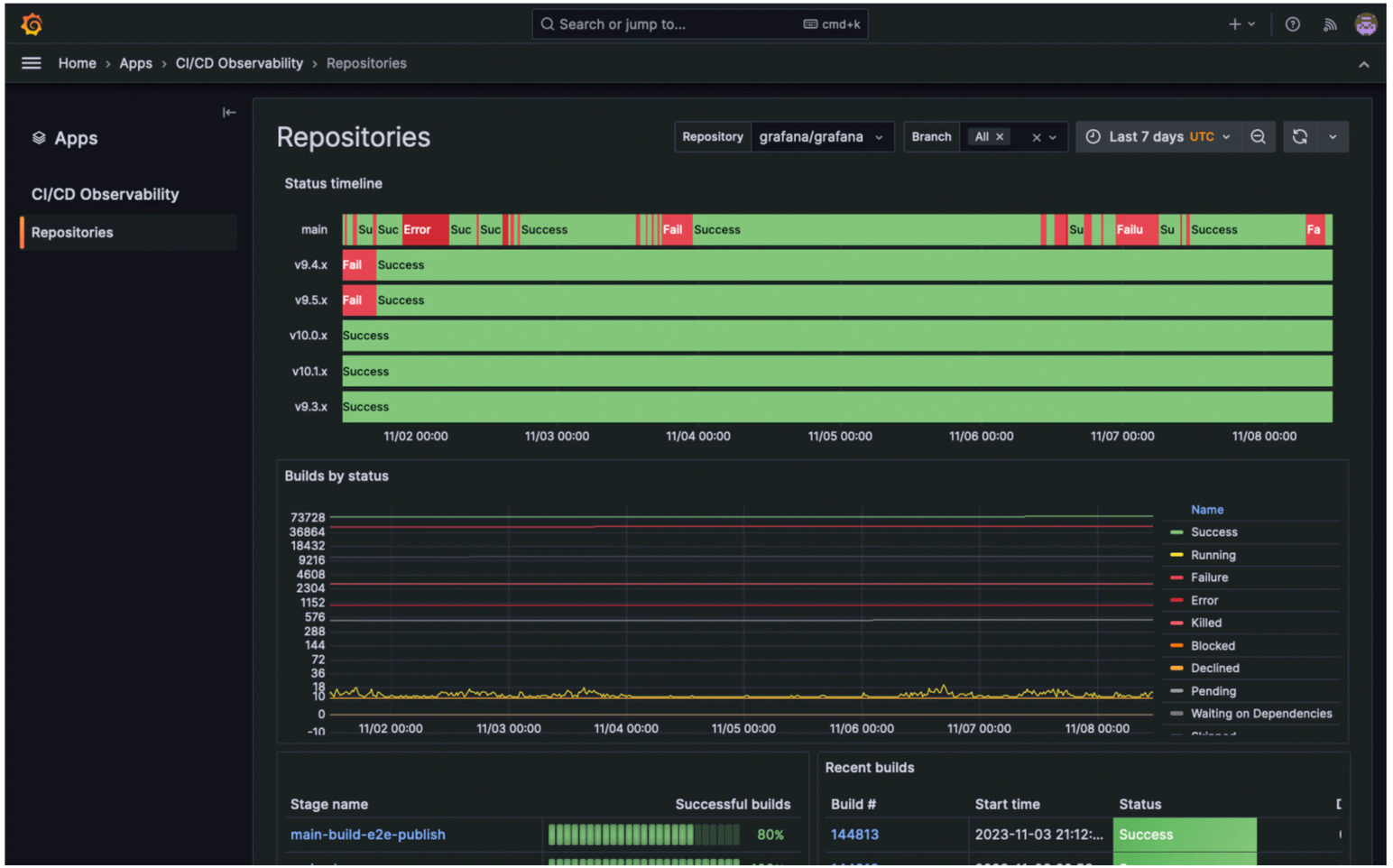
Pipeline duration distribution



Top slowest pipelines

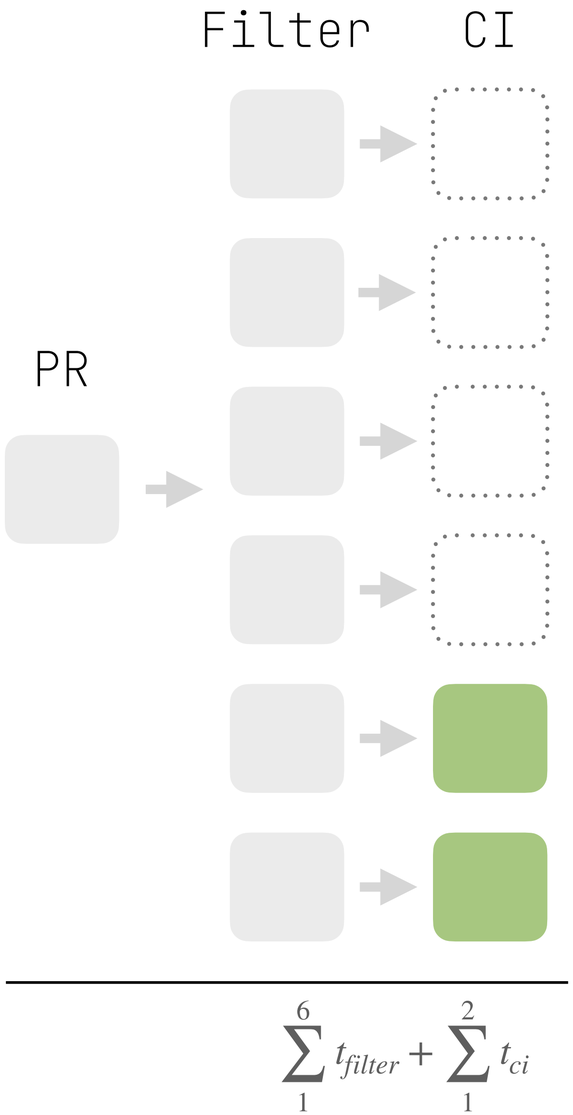
PIPELINE NAME	COUNT[CI_LEVEL:PIPELINE @CI.STAT...	MEDIAN:@DURATION[CI_LEVEL:PIPELIN...	PC95:@DURATION[CI_LEVEL:PIPELINE ...	SUM:@DURATION[CI_LEVEL:PIPELINE @...
2023 PyConIT 🇮🇹 generate gallery.pdf	38	14.1 s	19.8 s	9.65 min
2023 EuroSciPy 🇨🇭 Continuous Integra...	37	14.1 s	26.8 s	9.52 min
2024 PyCON DE 🔬 Show Default Shell	30	12.0 s	14.1 s	6.17 min
2023 PyData Berlin 🇩🇪 generate galler...	26	15.0 s	49.8 s	10.1 min
2024 PyCON DE 🎲 Random Number ...	25	21.9 s	26.8 s	9.35 min
2024 PyCON DE ♻️ My Reusable Work...	5	11.1 s	13.0 s	3.43 min

What is CI/CD observability, and how are we paving the way for more observable pipelines?

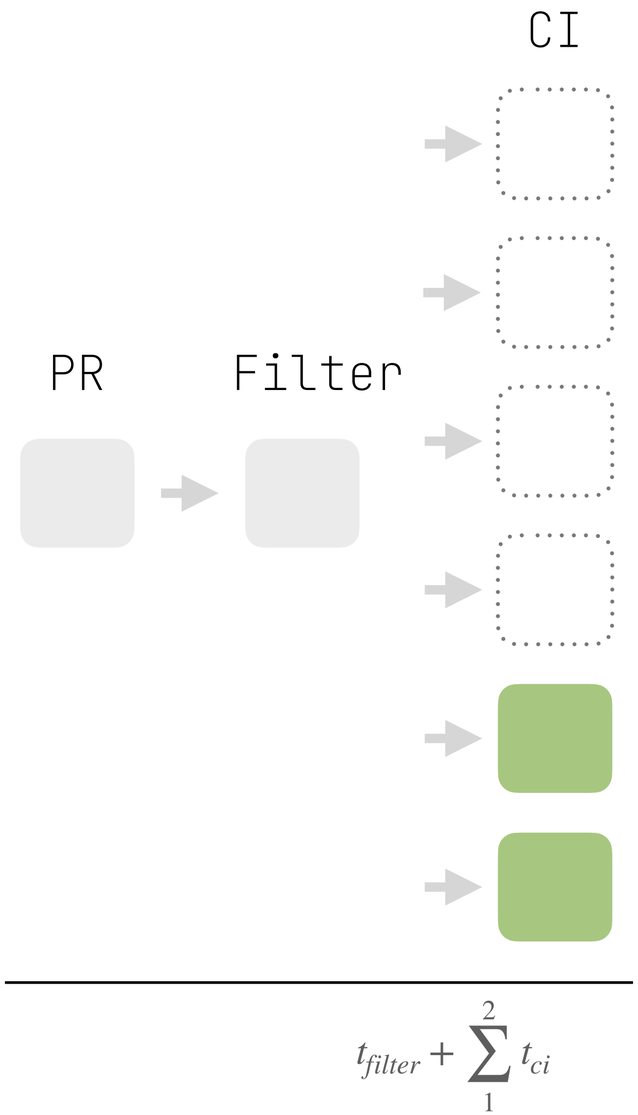


Source: https://grafana.com/blog/2023/11/20/ci-cd-observability-via-opentelemetry-at-grafana-labs/#empowering-cicd-observability-within-grafana

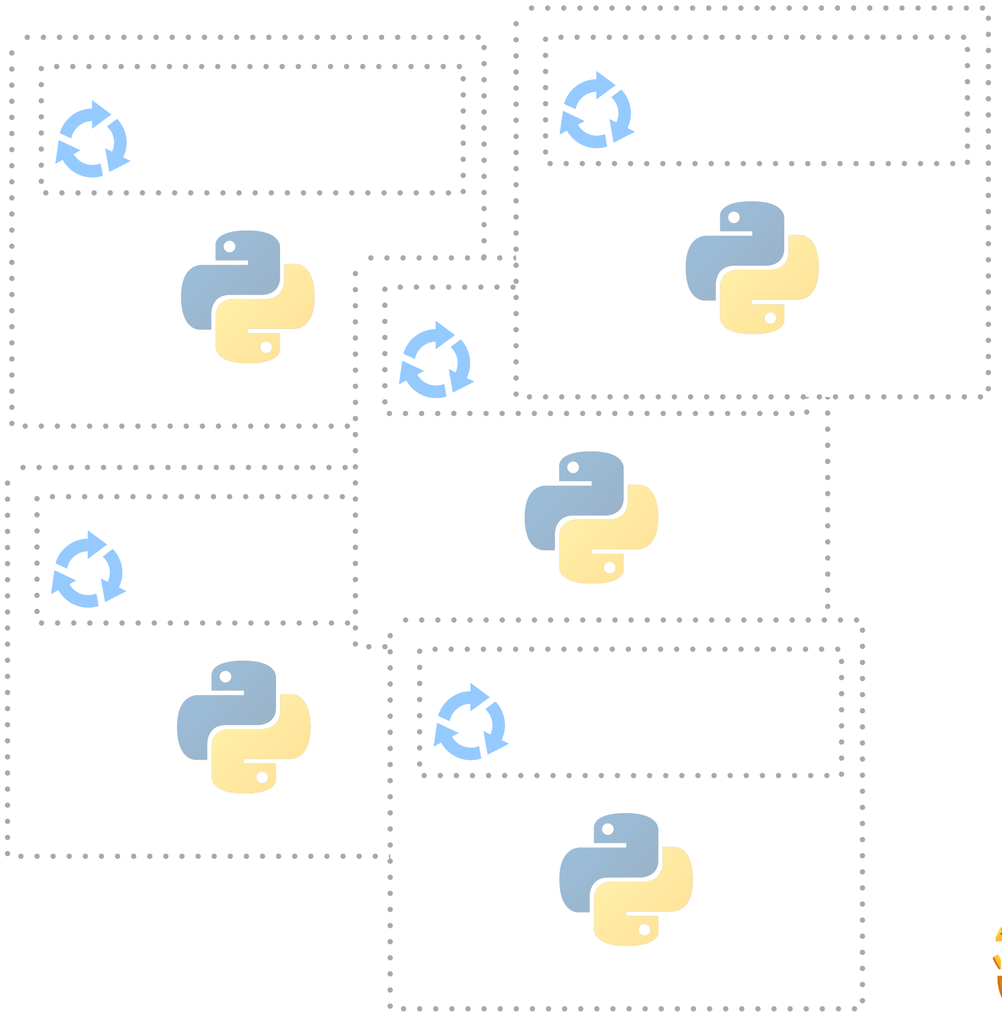
Reusable Workflows

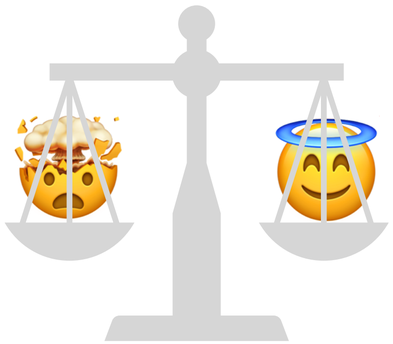


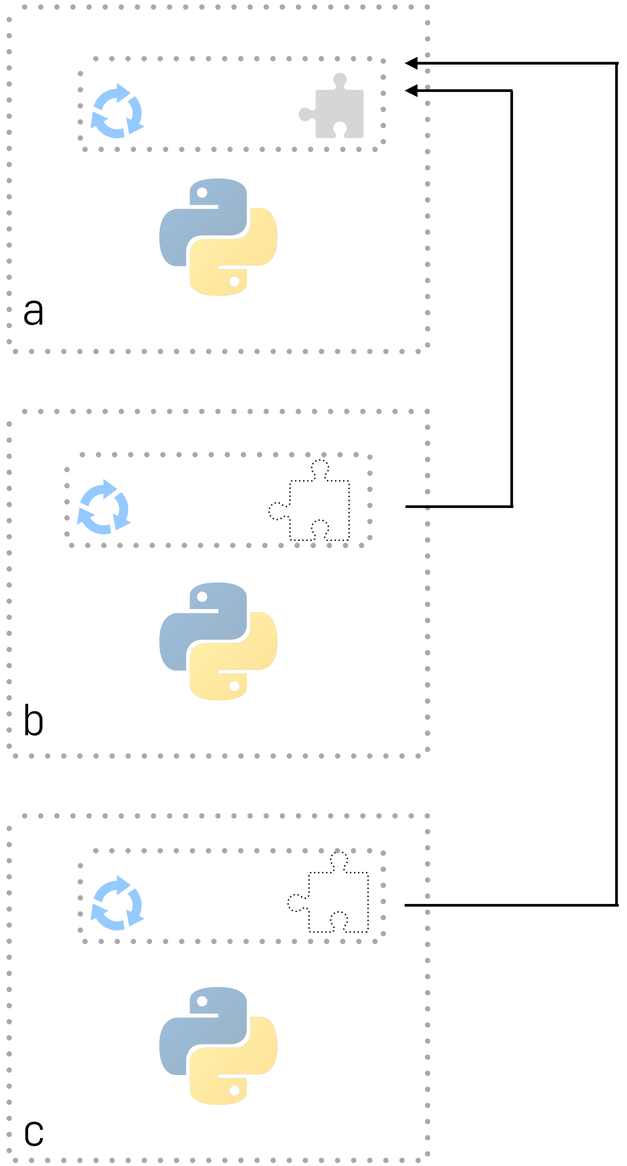
$$\sum_{1}^{6} t_{filter} + \sum_{1}^{2} t_{ci}$$



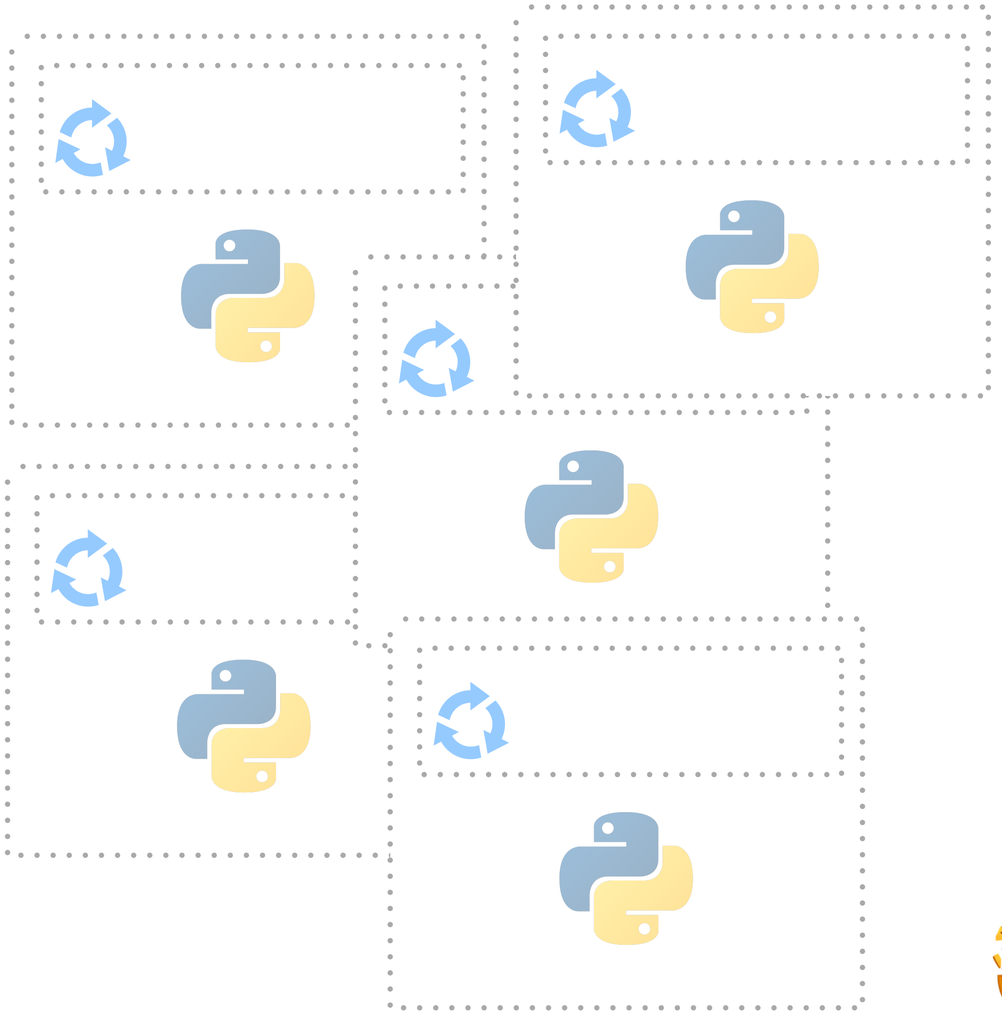
$$t_{filter} + \sum_{1}^{2} t_{ci}$$

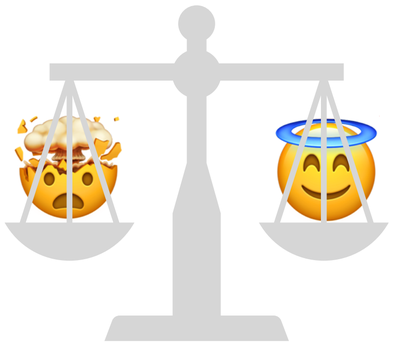




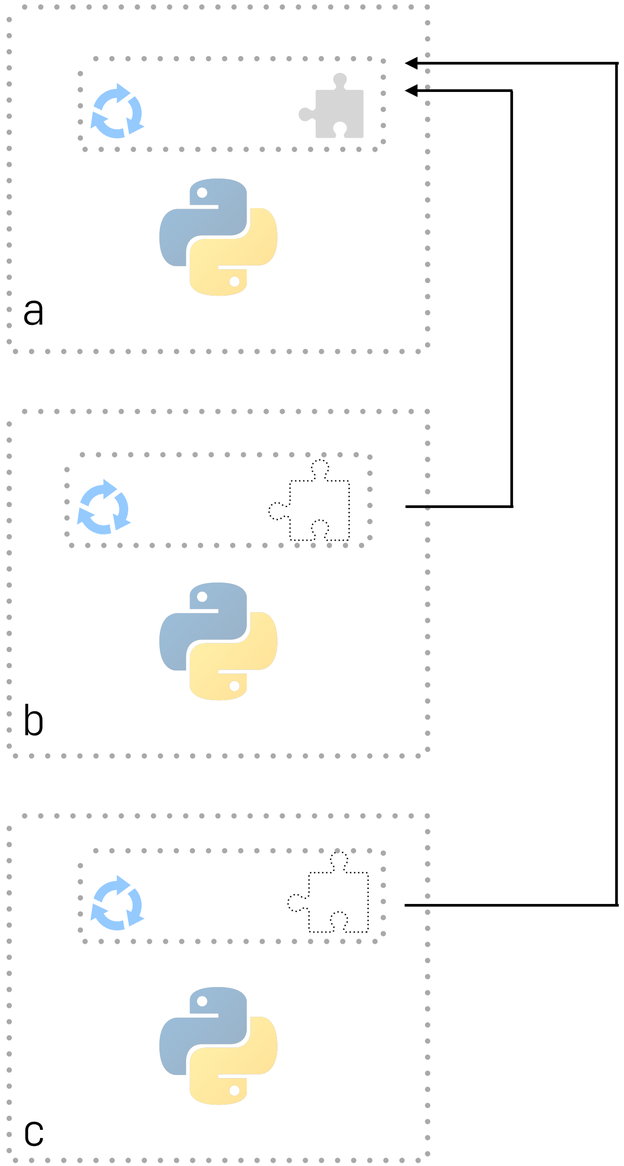


WET (we enjoy typing)





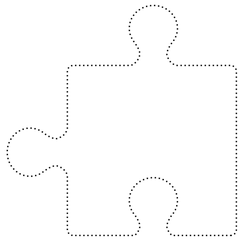
DRY (don’t repeat yourself)



```yaml
name: "2024 PyCON DE ♻️ My Reusable Workflow"
run-name: "MANUAL - ♻️ My Reusable Workflow (run by - ${{ github.triggering_actor }})"

on:
  workflow_call:
    inputs:
      example_param:
        description: 'An example input parameter'
        required: true
        default: 'Hello, World! (default) 😞'
        type: string

jobs:
  my_job:
    runs-on: ubuntu-latest
    steps:
      - name: Output Input Parameter
        run: echo "The input parameter value is ${{ inputs.example_param }}"
```


Kislovskiy/talks

```yaml
name: "2024 PyCON DE ♻️ Trigger Reusable Workflow"
run-name: "MANUAL - ♻️ Trigger Reusable Workflow (run by - ${{ github.triggering_actor }})"

on:
  workflow_dispatch:

jobs:
  trigger_workflow:
    uses: Kislovskiy/talks/.github/workflows/2024_PyConDE_reusable_workflow.yaml@main
    with:
      example_param: 'Hello, World! 😀'
```



Kislovskiy/talks

Nice things to add to your pipeline

```yaml
name: "2024 PyCON DE ☠️ Show Environment"
run-name: "MANUAL - ☠️ Show Environment (run by - ${{ github.triggering_actor }})"

on:
 workflow_dispatch:

jobs:
  show_default_shell:
    runs-on: ubuntu-latest
    timeout-minutes: 1

    steps:
    - name: ☠️ Display Environment Variables Names
      run: |
        for var in $(printenv | cut -d "=" -f 1); do
          echo "$var"
        done >> $GITHUB_STEP_SUMMARY
```

Regularly review and update workflows

```
uses: action@<commit-sha> #v3.0.2
```

```
# renovate.json
{
  …
 "extends": [
    …
    "helpers:pinGitHubActionDigests"
  ],
  …
 }
```

source: https://docs.renovatebot.com/

Top 10 CI/CD Security Risks

CICD-SEC-1 Insufficient Flow Control Mechanisms

CICD-SEC-2 Inadequate Identity and Access Management

CICD-SEC-3 Dependency Chain Abuse

CICD-SEC-4 Poisoned Pipeline Execution (PPE)

CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)

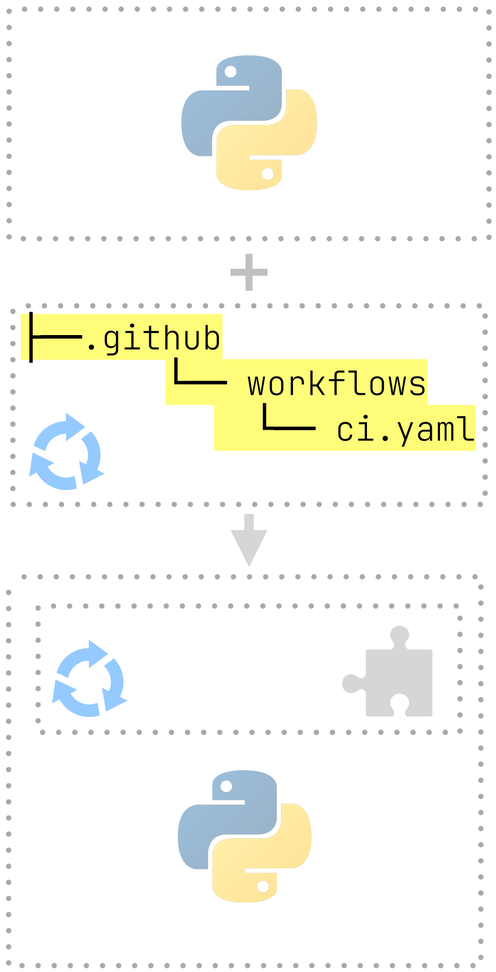
CICD-SEC-6 Insufficient Credential Hygiene

CICD-SEC-7 Insecure System Configuration

CICD-SEC-8 Ungoverned Usage of 3rd Party Services

CICD-SEC-9 Improper Artifact Integrity Validation

CICD-SEC-10 Insufficient Logging and Visibility



Tools and resources I recommend:

- GitHub Actions + GitLab + JetBrains Docs / Blog
- Microsoft Learn (GitHub Actions Collection)
- “Mastering GitHub Actions" by Eric Chapman
- Security: https://owasp.org/
- https://github.com/bsommardahl/anyhasher
- Observability: datadoghq.com
- Debugging: https://github.com/nektos/act
- Pre-commit: `id: check-yaml`

🤓 **GitHub.com/Kislovskiy/talks**