DEV1123

Continuous Quality - Bringing CI/CD to Splunk App and Add-on Development

Ryan Faircloth

Principal Product Manager | Splunk, Inc

Ryan Faircloth

Splunk Inc.

Agenda

1) Demo – Broken TA detection

2) Testing your add-on code with pytest-splunk-add-on

3) Validating Best Practices with - AppInspect

4) Keep it consistent and track change – github.com

5) Automate workflow- with circleci.com

6) Analyize in Splunk

Pytest-splunk-add-on what does it cover?

Automation

Using data samples test every knowledge object to confirm use (no dead code) and correctness (produces a result)

1. Each regex report/extract will match at least one sample and produce a result
2. FIELDALIAS is based on a valid source field and will not cause a empty field
3. EVAL will produce a result that is not null
4. Lookups will match fields

Pytest-splunk-add-on what does it cover?

Automation

Using business rules documented by Splunk SME, confirm that CIM tagged events contain correct values such as

1. Authentication events must have a user destination and an action
2. Network Communication events must have source and dest address/port pairs
3. If fields are related the set must exist when used such as bytes_in should exist with bytes_out
4. Malware events must have signature

Pytest-splunk-add-on what does it cover?

Automation

Test common index time operations

1. Check Linebreaker and timestamping for file based sources
2. Test normalization in Splunk Connect for Syslog

Standard Tools

All hammers are not equal but close enough for a skilled carpenter

1. VCS – git or die. We use github.com but there are other great options gitlabs and bitbucket are good choices as well. Github is free for “opensource” projects every add-on should be open source create community and reduce costs.
2. CI/CD – Cloud hosted CI is your friend. We use circleci other choices like Jenkins, GithubActions and gitlab are also good.
3. Appinspect CLI – Static testing
4. pytest-splunk-addon – Dynamic testing, its open source, used by Splunk and available for you
5. Docker – Splunk in a container

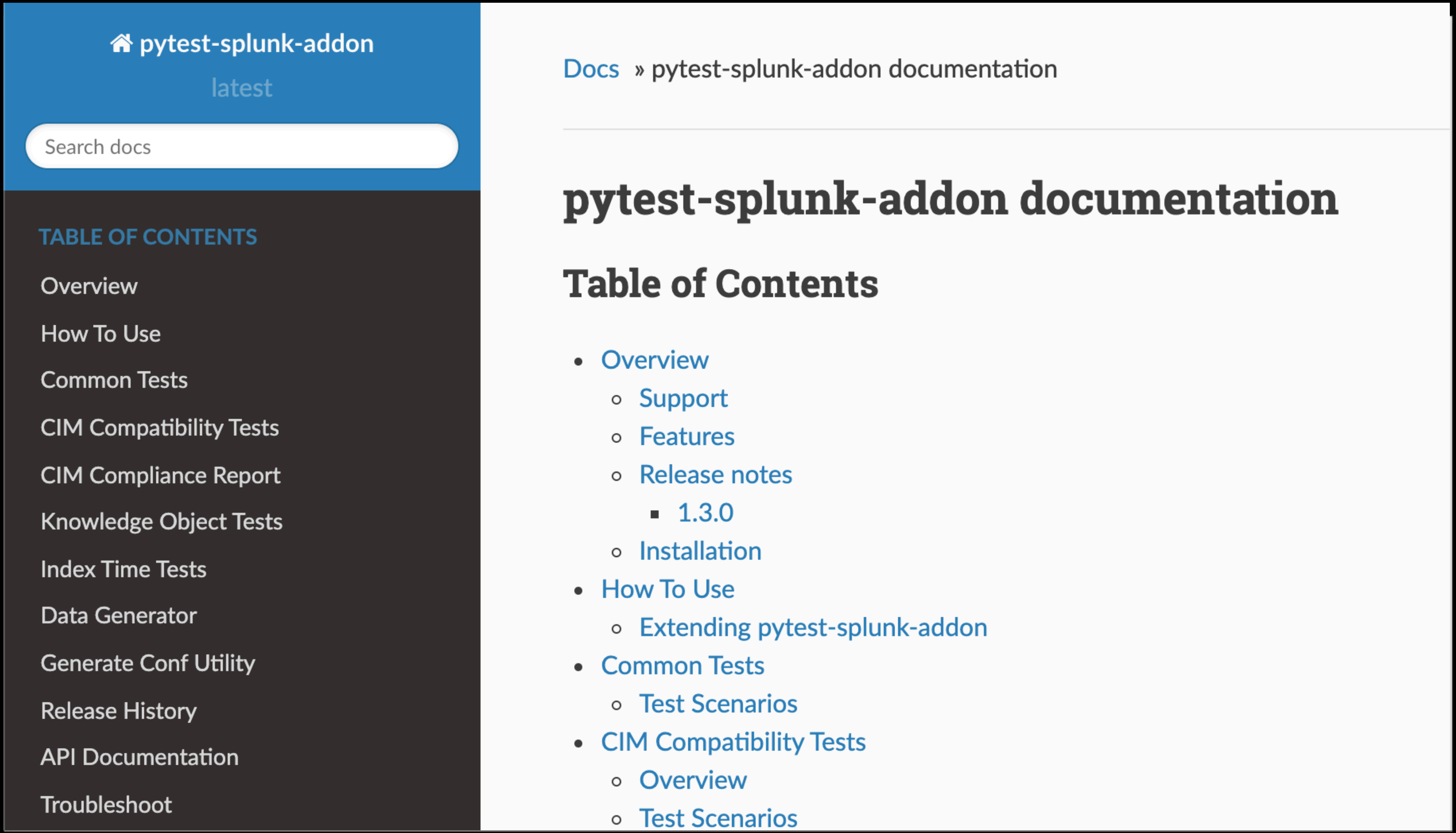


TABLE OF CONTENTS

Docs » pytest-splunk-addon documentation

pytest-splunk-addon documentation

Table of Contents

AppInspect CLI

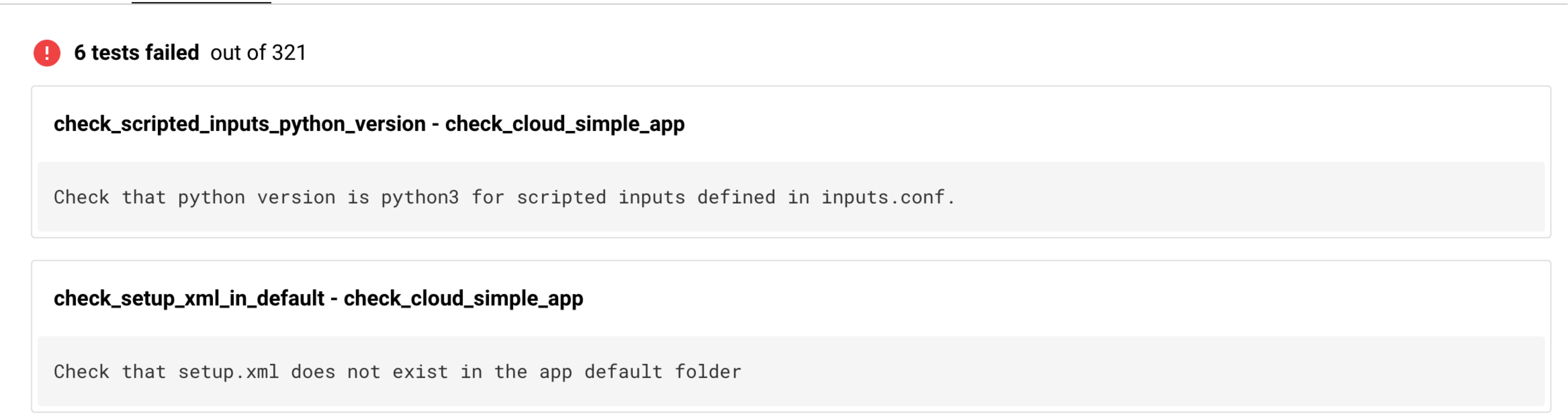
1) Static analysis of best practices and identification of worst behaviors

2) Gives your developers confidence via the AppInspect badge your add-on is safe to deploy

3) Gives your users confidence with Cloud Ready validation of best practices

AppInspect

Early identification of standards based issues



❗ **6 tests failed** out of 321

check_scripted_inputs_python_version - check_cloud_simple_app

```
Check that python version is python3 for scripted inputs defined in inputs.conf.
```

check_setup_xml_in_default - check_cloud_simple_app

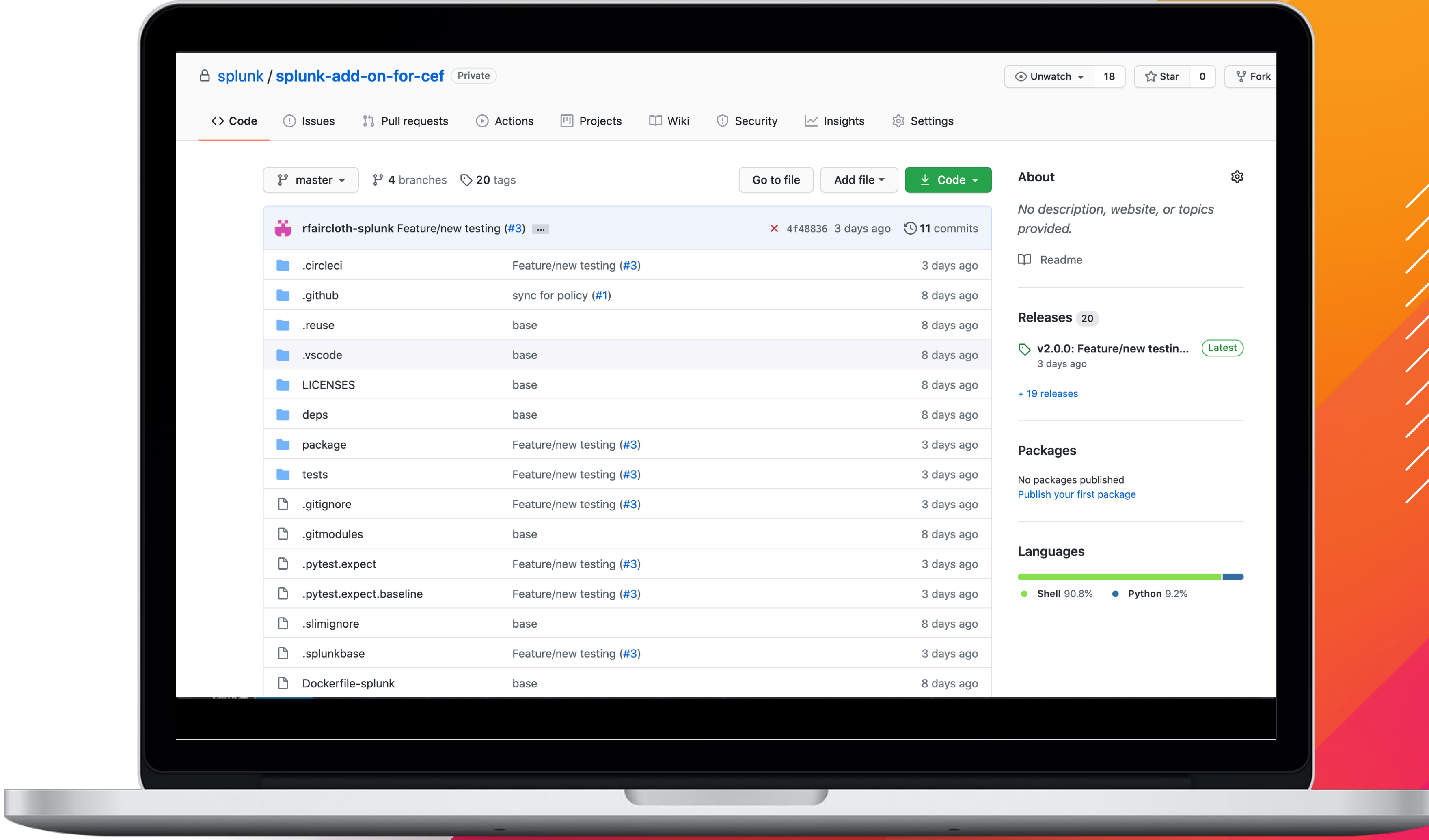
```
Check that setup.xml does not exist in the app default folder
```

GIT

Practice Safe Dev Workflow

Commit a Change

1. Test a change
2. Review a change
3. Release a change



splunk / splunk-add-on-for-cef Private

4 branches 20 tags

rfaircloth-splunk Feature/new testing (#3) ... 4f48836 3 days ago 11 commits

.circleci	Feature/new testing (#3)	3 days ago
.github	sync for policy (#1)	8 days ago
.reuse	base	8 days ago
.vscode	base	8 days ago
LICENSES	base	8 days ago
deps	base	8 days ago
package	Feature/new testing (#3)	3 days ago
tests	Feature/new testing (#3)	3 days ago
.gitignore	Feature/new testing (#3)	3 days ago
.gitmodules	base	8 days ago
.pytest.expect	Feature/new testing (#3)	3 days ago
.pytest.expect.baseline	Feature/new testing (#3)	3 days ago
.slimignore	base	8 days ago
.splunkbase	Feature/new testing (#3)	3 days ago
Dockerfile-splunk	base	8 days ago

About

No description, website, or topics provided.

Readme

Releases 20

v2.0.0: Feature/new testin... Latest
3 days ago

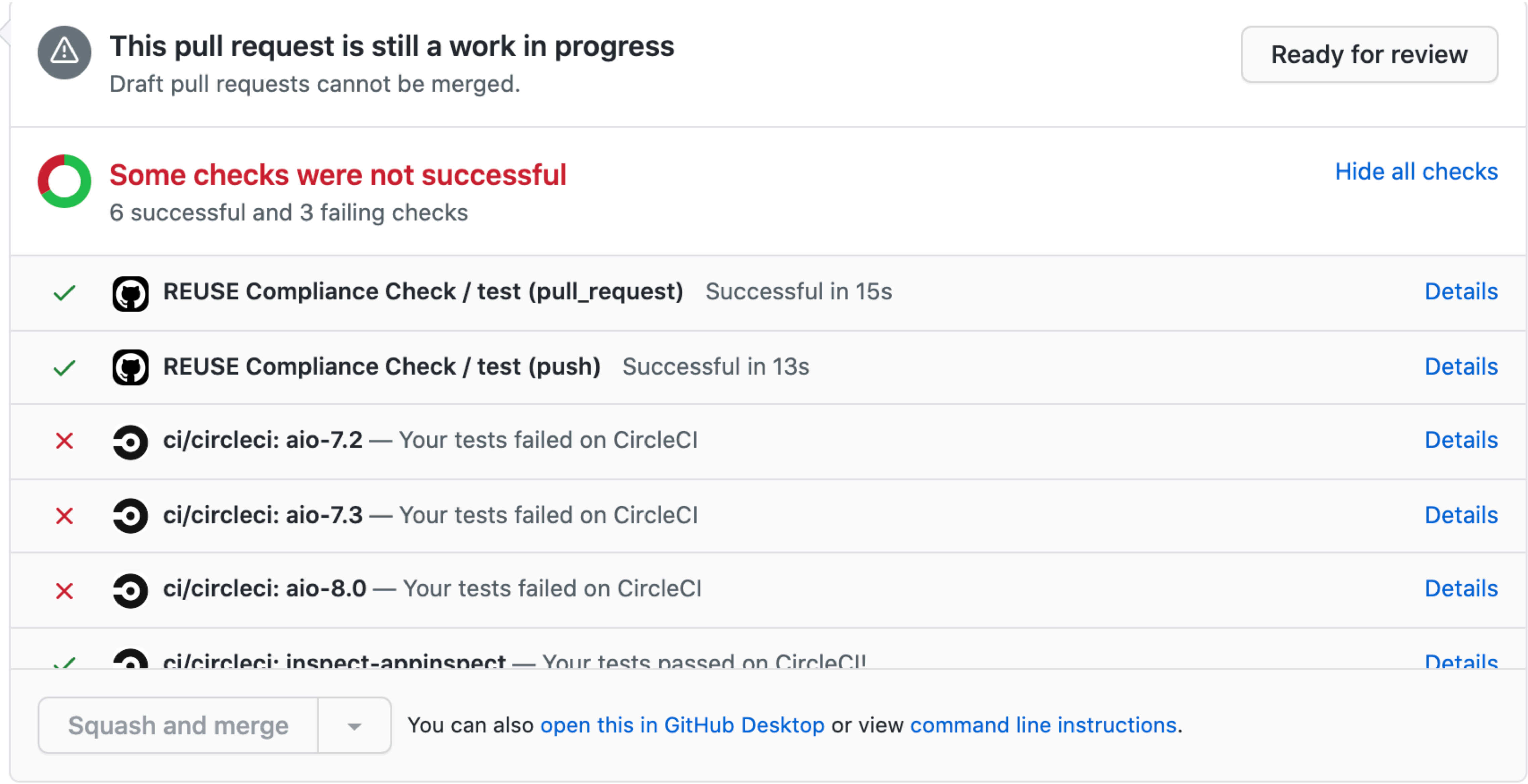
+ 19 releases

Packages

No packages published
Publish your first package

Languages

Shell 90.8% Python 9.2%



This pull request is still a work in progress

Draft pull requests cannot be merged.

Some checks were not successful

6 successful and 3 failing checks

✓ **REUSE Compliance Check / test (pull_request)** Successful in 15s Details

✓ **REUSE Compliance Check / test (push)** Successful in 13s Details

✕ **ci/circleci: aio-7.2** — Your tests failed on CircleCI Details

✕ **ci/circleci: aio-7.3** — Your tests failed on CircleCI Details

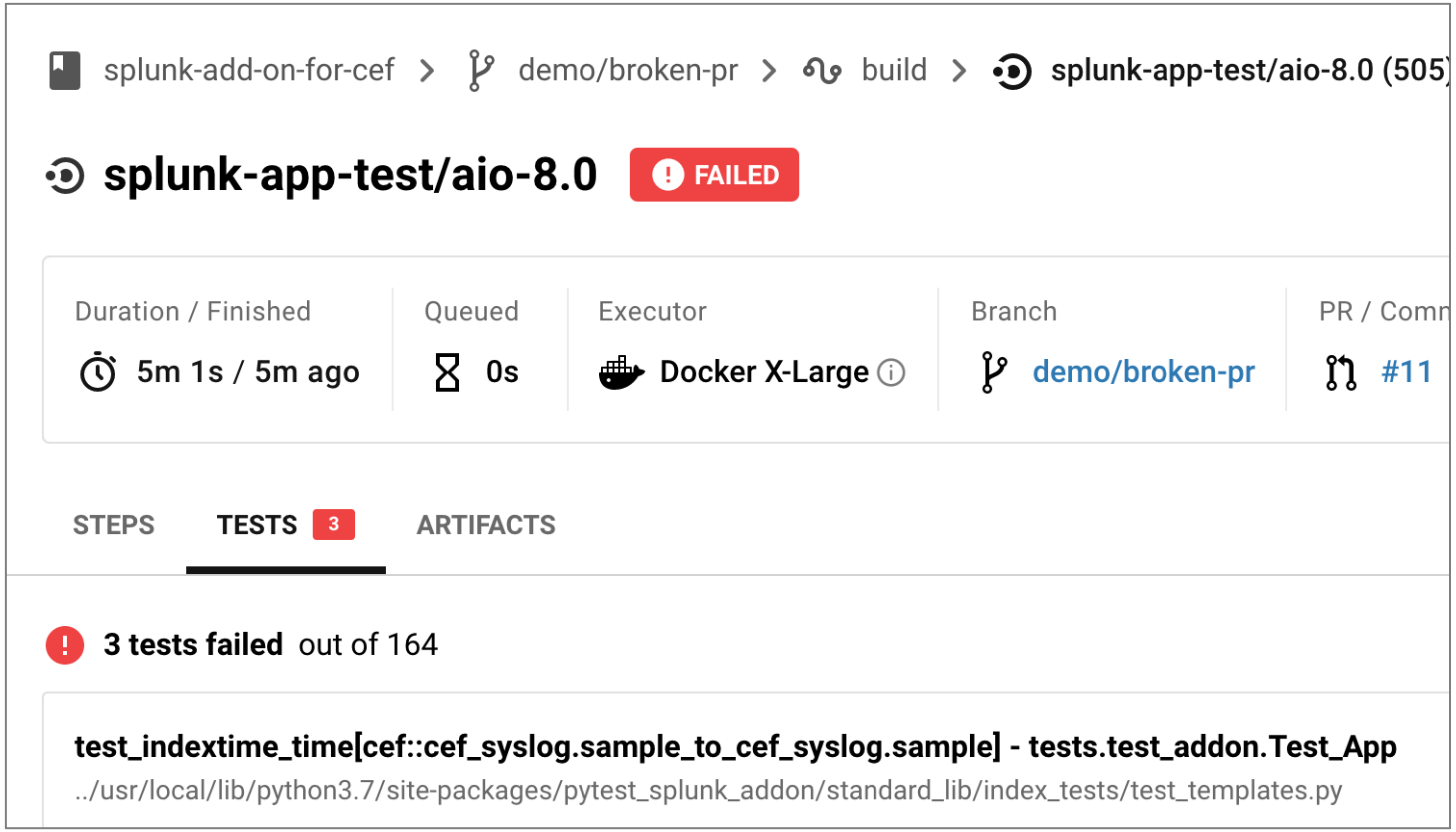
✕ **ci/circleci: aio-8.0** — Your tests failed on CircleCI Details

✓ **ci/circleci: inspect-appinspect** — Your tests passed on CircleCI! Details

You can also open this in GitHub Desktop or view command line instructions.

Circle CI

No testing left behind



splunk-add-on-for-cef > demo/broken-pr > build > splunk-app-test/aio-8.0 (505

splunk-app-test/aio-8.0 FAILED

Duration / Finished: 5m 1s / 5m ago

Queued: 0s

Executor: Docker X-Large

Branch: demo/broken-pr

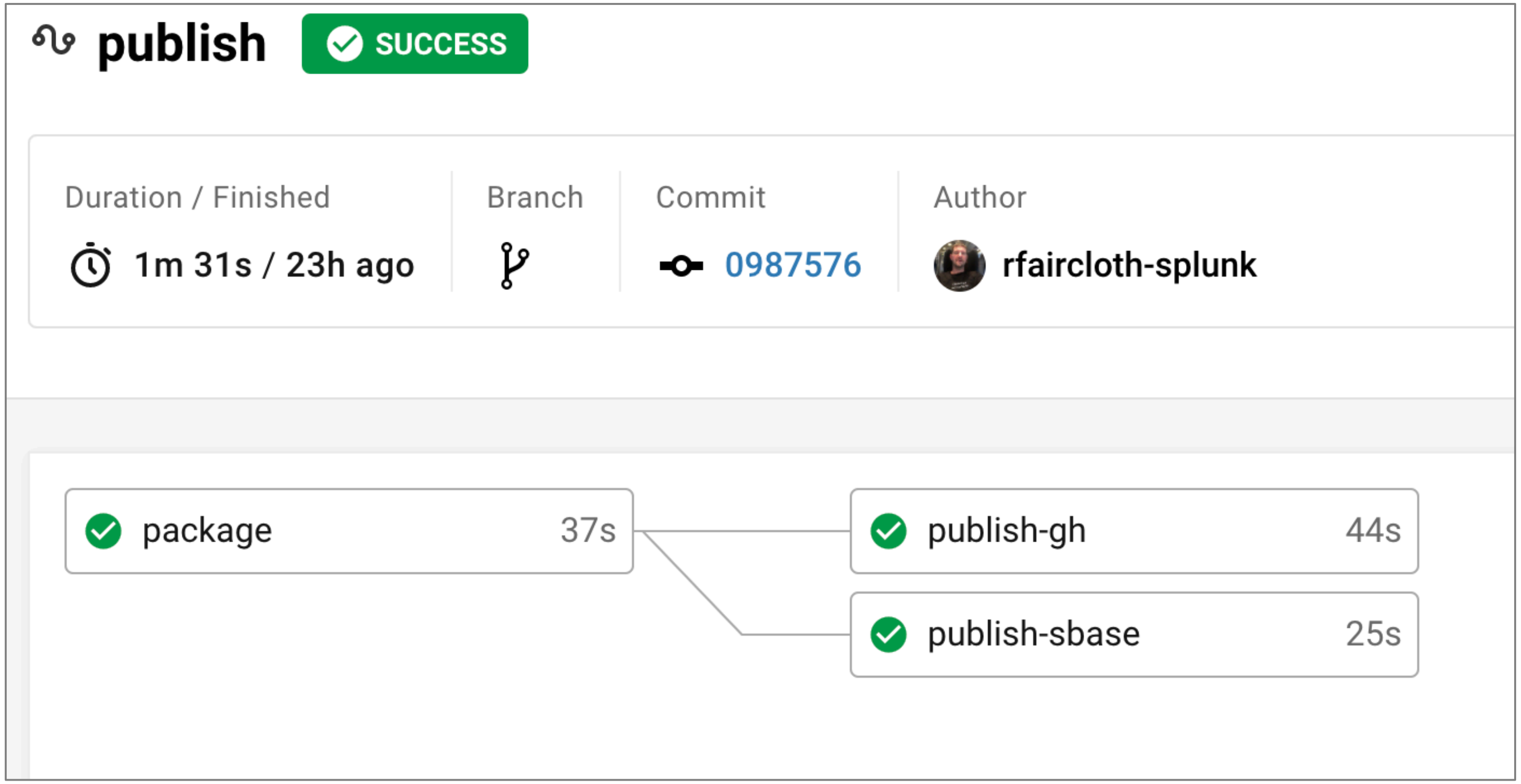
PR / Comm: #11

STEPS TESTS 3 ARTIFACTS

3 tests failed out of 164

test_indextime_time[cef::cef_syslog.sample_to_cef_syslog.sample] - tests.test_addon.Test_App
../usr/local/lib/python3.7/site-packages/pytest_splunk_addon/standard_lib/index_tests/test_templates.py

Automate Release



publish ✓ SUCCESS

Duration / Finished: 1m 31s / 23h ago

Branch

Commit: 0987576

Author: rfaircloth-splunk

Thank You

Please provide feedback via the

SESSION SURVEY

Resources

1) Splunk Community Slack #add-on-devs

2) Pytest-splunk-add-on docs

3) Pytest-splunk-add-on github

4) Demo Project github

5) Template Project github