Marc-Philipp Knechtle

Going public

Tips for publishing your own code

Table of contents

Sensitive data in git

- Problem: (Accidental) commits of secrets
- e.g. passwords, application secret keys, OAuth secret keys, SSH keys
- The file is still accessible in history, even if the original file was deleted
- Security risk, even in private repositories

Removing sensitive data

- git filter-repo
- BFG Repo-Cleaner

Encrypt sensitive data

Methods for encrypting and storing sensitive data:

- ■ Why shouldn't I store the secrets separate from the repository?
- ■ Methods for encrypting and storing sensitive data:
  - ► git-secret CLI
  - ► github encrypted secrets
  - ► technology specific encryption tool (e.g. ansible-vault)

Points of interaction with the community

community-
specific
forum

|

**Interaction
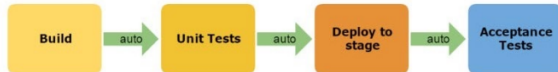Points** — Issues

|

Pull
Requests
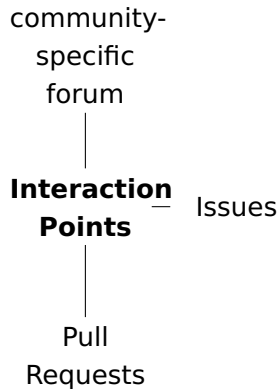
Code of Conduct

- Content: set of rules, with norms, responsibilities and proper parties
- defines the actions of a single person in a organisation
- Goal: healthy, constructive community behaviour
- CODE_OF_CONDUCT file (in the git repository)
- e.g. Contributor Covenant [1], Django Code of Conduct [2]

Continuous Integration overview

Github Actions

- ■ CI/CD platform, used for testing Pull Requests
- ■ Reactions on other events such as an issue beeing created
- ■ workflows can run on VMs or a self-hosted instance
- ■ workflows consist of jobs, which is a shell script or an action
- ■ actions are custom github actions applications (e.g. pulling a repository, setting up the toolchain)
- ■ runners are the servers on which the process is performed

Ideas for promoting your code

- Cross-promoting projects through their documentation
- Writing a blog with shareable posts for each major release
- Monitor new mentions of your project e.g. through bots [3]

References