
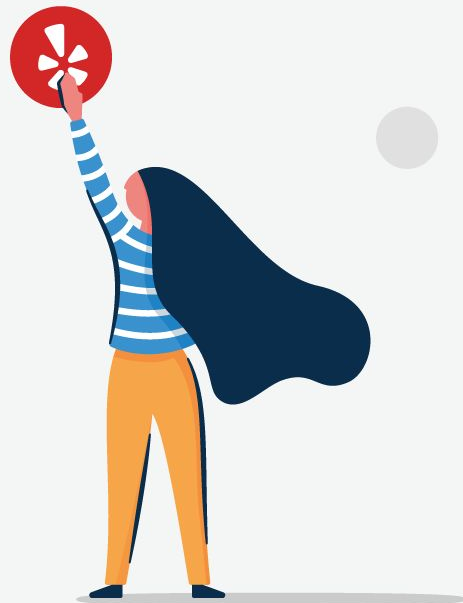


Securing the Docker Containers at the CI/CD Pipeline Level

Alina Radu

 @transcendentalia @BarcelonaBsides



About Yelp

Connecting people with **great local businesses**



[Write a Review](#)

[Events](#)

[Talk](#)



Find burgers, barbers, spas, handymen...

Near Barcelona, Spain



[Restaurants](#)

[Nightlife](#)

[Local Services](#)

[Delivery](#)

Tatte Bakery & Cafe
Photo by [Sophie P.](#)

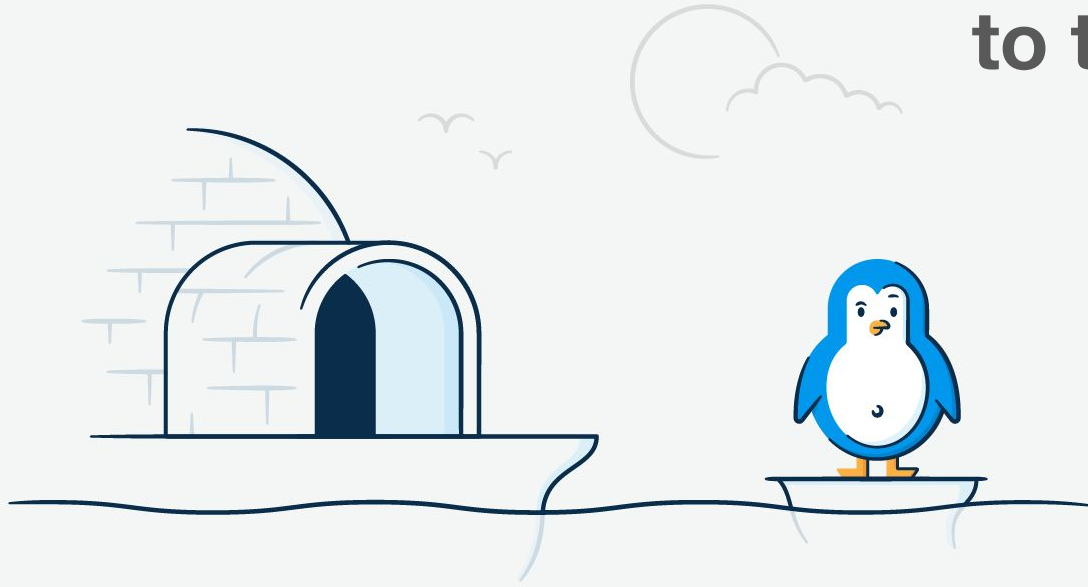


@transcendentalia

Agenda

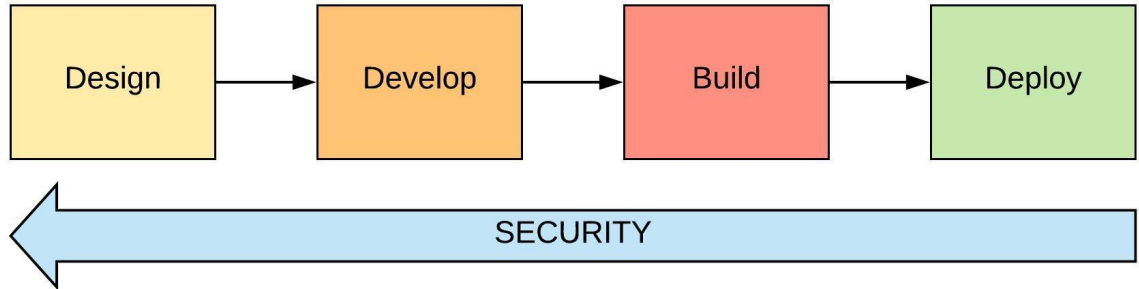
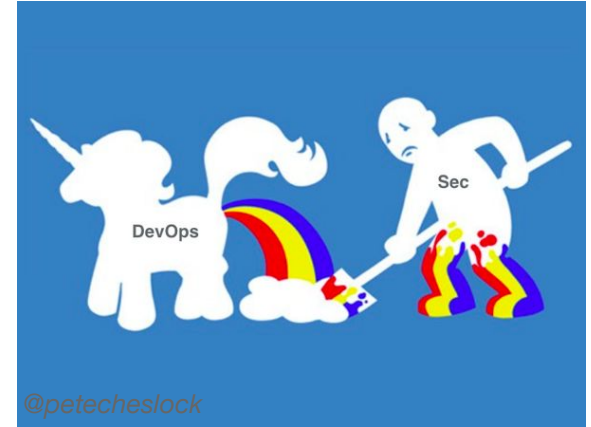
- ⚙️ Shifting security to the **left**
- ✓ Security at the **CI/CD pipeline** level
- 🔔 Failures and **actionable** alerts
- ❓ Q&A

Shifting security to the left



Shifting security to the left

- ✧ Security **by design**
- ✧ **Proactive** security
- ✧ Automation
- ✧ Increase team collaboration
 - Eliminating **silos**
- ✧ Reducing costs



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)[Yelp](#) / [paasta](#)[Unwatch](#)

101

[★ Star](#)

1,284

[Fork](#)

155

[Code](#)[Issues](#) 88[Pull requests](#) 7[Projects](#) 0[Insights](#)[Settings](#)

An open, distributed platform as a service

[Edit](#)[paasta](#) [mesos](#) [infrastructure](#) [smartstack](#) [sensu](#) [marathon](#) [chronos](#) [yelp](#)

8,680 commits

276 branches




881 releases

Apache-2.0

Branch: master

[New pull request](#)[Create new branch](#)[Upload files](#)[Clone or download](#) **chlgit** confirm affected cluster and instances before really start or stop (#...

Latest commit b8d8b70 2 days ago

 debian	Released 0.81.10 via make release	4 days ago
 docs/source	Released 0.81.10 via make release	4 days ago
 example_cluster	confirm affected cluster and instances before really start or stop (#...	2 days ago



@transcendentalia



Search or jump to...

Pull requests Issues Marketplace Explore



Yelp / paasta

Unwatch

101

★ Star

284

Fork

5

<> Code



Pull requests 7

Projects 0

Insights

Settings

An open, distributed service

paasta

smartstack

sensu

monitoring

chronos

yelp

8,6

276 branches

83 releases

Apache-2.0

Branch: master

request

Create

and file

Clone or download



chlgit confirm affected cluster and instances before really start or stop (#...

Latest commit b8d8b70 2 days ago

debian

docs/source

example_cluster

Released 0.81.10 via make release

Released 0.81.10 via make release

confirm affected cluster and instances before really start or stop (#...

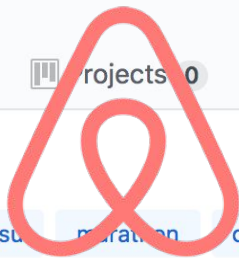
4 days ago

4 days ago

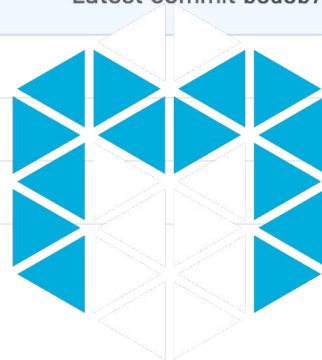
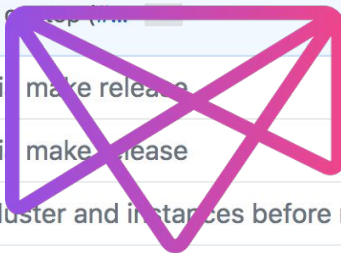
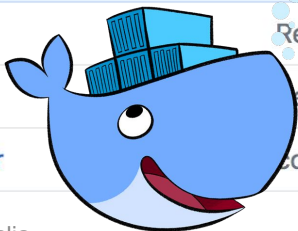
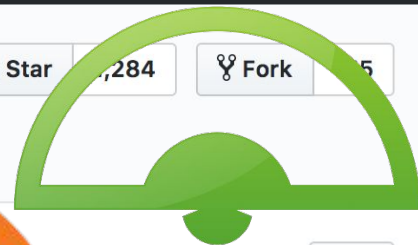
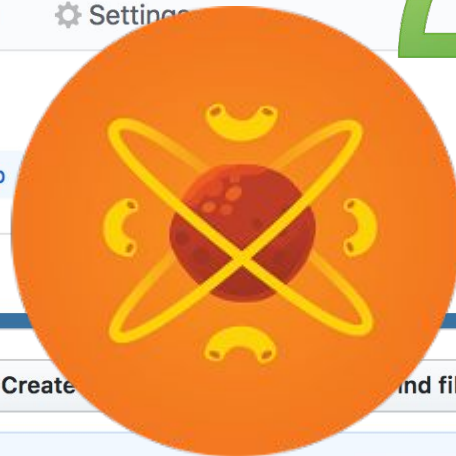
2 days ago



@transcendentalia



airbnb
SmartStack



Build pipeline of a service

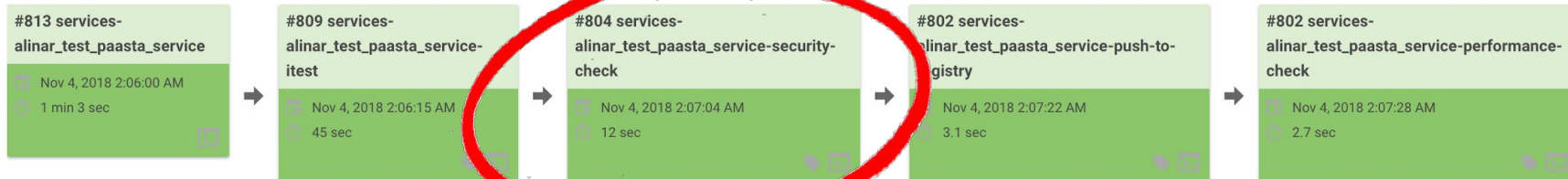
✱ Configuration repository

✱ **Jenkins**

- Orchestrates build and deployment
- Pipelines of sequential steps
- Security-check step



Pipeline
#813



PaaSTA security-check

✱ Set of **python tests**

✱ **High level** security status of the service

✱ Run at every build

✱ **Actionable** alerts

02:07:15 [✓] DebianSystemPackageCheck

02:07:15 [✓] DockerRootCheck

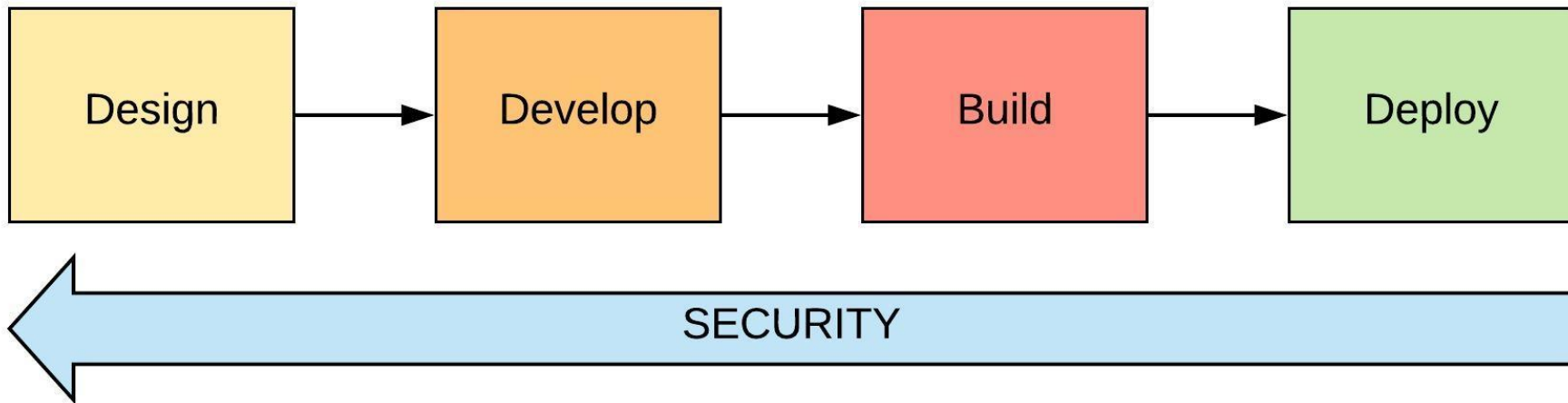
02:07:15 [✓] DockerfileCheck

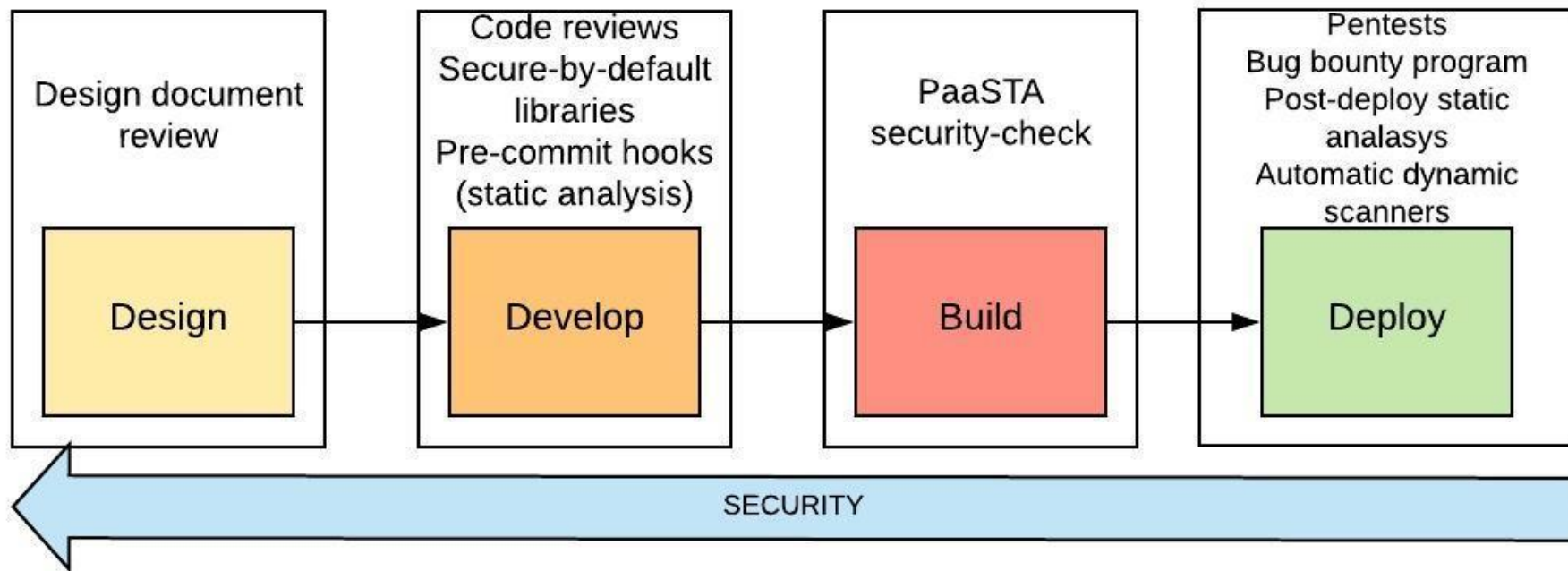
02:07:15 [✓] NpmDependencyCheck

02:07:15 [✓] PhpDependencyCheck

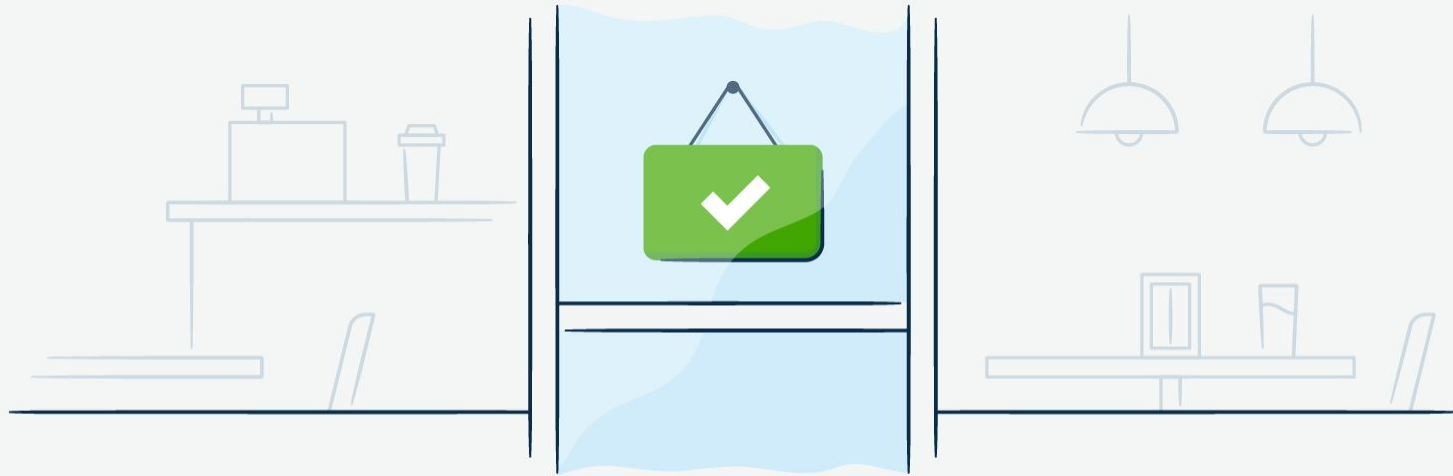
02:07:15 [✓] PythonDependencyCheckCustom

02:07:15 [✓] ShellShockCheck





Security tests



Debian packages up to date



- ✿ Check is the latest packages are **up to date** against upstream repositories

```
class DebianSystemPackageCheck(BasePlugin):  
  
    def perform_check(self, docker, **kwargs):  
        # -qq: Do it super-quietly and say yes to  
        everything  
        # update: Update the package index, but do not  
        install && get all the things we would theoretically  
        install  
  
        dist_upgrade_print = docker.run(  
            'apt-get -qq update && apt-get --just-print  
            dist-upgrade', root=True).decode('utf-8')
```

07:45:18 DebianSystemPackageCheck:

07:45:18 Package libudev1 needs to be updated from 229-4ubuntu21.4 to 229-4ubuntu21.5

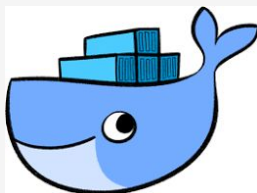
07:45:18 Package systemd-sysv needs to be updated from 229-4ubuntu21.4 to 229-4ubuntu21.5

07:45:18 Package systemd needs to be updated from 229-4ubuntu21.4 to 229-4ubuntu21.5

07:45:18 Package libsystemd0 needs to be updated from 229-4ubuntu21.4 to 229-4ubuntu21.5



Docker best practices



19:08:15 DockerRootCheck:

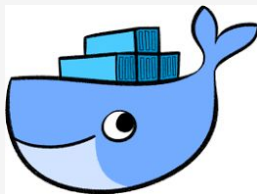
19:08:15 The default user in this container is root. Please add a USER statement, see y/dockerbestpractices

✱ Container **not** running as **root** (default)

```
class DockerRootCheck(BasePlugin):  
  
    def perform_check(self, docker, **kwargs):  
        output =  
        docker.run('whoami').decode('utf-8').strip()  
        if output == 'root':  
            self.messages.append('The default user in  
this container is root. '  
'Please add a USER statement, see  
y/dockerbestpractices')  
            return SecurityCheckResult. FAIL  
  
        self.messages.append(  
            'The default user in this container is: ' +  
output)  
        return SecurityCheckResult. PASS
```



Docker best practices



Dockerfile

- Yelp maintained Docker images
- latest images
- no packages pinned to certain versions
- .dockerignore contains .git

```
class DockerfileCheck(BasePlugin):  
  
    def check_dockerignore(self):  
        dockerignore = self.get_dockerignore()  
        if dockerignore is None:  
            self.messages.append('No .dockerignore  
file exists. Create one and add .git to it.')  
            return False  
  
        if not any([line.startswith('.git') for  
line in dockerignore]):  
            self.messages.append('A .dockerignore  
file exists but .git is not in it; please add it.')  
            return False  
  
        return True
```

19:08:15 DockerfileCheck:

19:08:15 This Dockerfile's base image is pinned to something other than `latest` (8.9.1).

19:08:15 Consider using the latest version.

19:08:15 A .dockerignore file exists but .git is not in it; please add it.



Well known vulnerabilities



* Bash Shellshock

```
class ShellShockCheck(BasePlugin):  
    COMMAND = "env x='() { :; }; echo vulnerable' bash -c 'echo  
this is a test'"  
  
    def perform_check(self, docker, **kwargs):  
        output = docker.run(self.COMMAND).decode('utf-8').strip()  
  
        if output == 'this is a test':  
            self.messages.append('Bash is safe. It is not  
vulnerable to shellshock.')  
            return SecurityCheckResultPASS  
  
        self.messages.append('!! Bash is vulnerable to shellshock  
!!')  
        return SecurityCheckResultFAIL
```

19:08:15 ShellShockCheck:

19:08:15 Bash is safe. It is not vulnerable to shellshock.

Code dependency check

✿ Packages with **known vulnerabilities**

✿ Database of vulnerable packages

- e.g. npmjs.com/advisories for node.js
- e.g. pyup.io/safety for python

```
10:45:25 NpmDependencyCheck:
```

```
10:45:25 This service has NPM dependencies with known vulnerabilities:
```

```
10:45:25
```

```
10:45:25 base64url@2.0.0 Out-of-bounds Read (CVSS: 7.1) https://nodesecurity.io/advisories/658
```

```
10:45:25 debug@2.1.3 Regular Expression Denial of Service (CVSS: 3.7) https://nodesecurity.io/advisories/534
```



Image vulnerability scanning



- ✱ **Clair** open source project
- ✱ Scan base image
- ✱ CVEs, classified by severity
- ✱ **Anti-pattern:** patch running containers
 - rebuild the base image

The screenshot shows the GitHub repository page for `coreos/clair`. The repository is a Vulnerability Static Analysis for Containers. It has 201 watchers, 4,354 stars, and 552 forks. The repository is licensed under Apache-2.0. The page shows the repository's history, including a recent pull request merge by jzelinskie and a commit by jzelinskie adding stale and issue template enforcement.

coreos / clair

Watch 201 Star 4,354 Fork 552

Code Issues 54 Pull requests 8 Insights

Vulnerability Static Analysis for Containers

containers static-analysis go kubernetes docker oci oci-image vulnerabilities clair

798 commits 6 branches 26 releases 71 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

jzelinskie Merge pull request #650 from Katee/add-ubuntu-cosmic Latest commit 93e7a4c 4 days ago

.github: add stale and issue template enforcement a month ago

Documentation *: remove bzz dependency 4 months ago

No secrets in the service repository

- ✱ Detect and prevent **high entropy** strings from entering the code base
- ✱ Assume existing code has no secrets
- ✱ Check only the new code
- ✱ Loosely based off **truffleHog**

The screenshot shows the GitHub repository page for `Yelp / detect-secrets`. The repository has 29 watchers, 601 stars, and 44 forks. It contains 8 issues, 1 pull request, 0 projects, and 0 wiki pages. The repository description is "An enterprise friendly way of detecting and preventing secrets in code." It has 284 commits, 11 branches, 18 releases, 9 contributors, and is licensed under Apache-2.0. The current branch is `master`. The repository is pinned to the pre-commit 1.11.2 hook. The latest commit is 411a865, made 5 days ago. The repository contains two files: `detect_secrets` and `test_data`. The `detect_secrets` file has a commit message "Don't suggest .secrets.baseline for 'please create baseline' msg" made 6 days ago. The `test_data` file has a commit message "Add whitelist to Keyword plugin, fix the rest of the tests" made 2 months ago.

Yelp / detect-secrets

Watch 29 Star 601 Fork 44

Code Issues 8 Pull requests 1 Projects 0 Wiki Insights

An enterprise friendly way of detecting and preventing secrets in code.

284 commits 11 branches 18 releases 9 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

KevinHock Pin pre-commit to 1.11.2 Latest commit 411a865 5 days ago

detect_secrets	Don't suggest .secrets.baseline for 'please create baseline' msg	6 days ago
test_data	Add whitelist to Keyword plugin, fix the rest of the tests	2 months ago



Failures and alerts

✿ Security-check **failed?**

- Email
- Jira ticket
- Sensu alert

✿ **Runbook**



10:45:25 Summary

10:45:25 -----

10:45:25 [✓] DebianSystemPackageCheck

10:45:25 [x] DockerRootCheck

10:45:25 [✓] DockerfileCheck

10:45:25 [x] NpmDependencyCheck

10:45:25 [✓] PhpDependencyCheck

10:45:25 [✓] PythonDependencyCheckCustom

10:45:25 [✓] ShellShockCheck

10:45:26 The security-check failed. Please visit [y/security-check-runbook](#) to learn how to fix it (including whitelisting safe versions of packages and docker images).



Takeaways

- ✱ Shifting security to the **left**
- ✱ Security **tests** run at every build
- ✱ Service owners
 - more **aware** of the service security
 - **involved** in keeping it safe

Q&A

