DEFECTDOJO

introduced to you by

Matt Tesauro
@matt_tesauro

Fred Blaise
@FredBlaise
(madchap)

Matt - Who is this guy?

- Reformed programmer and AppSec engineer
- 13+ years in the OWASP community
  - OWASP AppSec Pipeline Leader
  - OWASP Defect Dojo Maintainer
  - OWASP WTE Leader
  - Former Global Board Member, employee
- 20+ years using FLOSS and Linux
- Currently a Golang fanboy
- Ee Dan in Tang Soo Do Mi Guk Kwan (2nd degree black belt)

Lac
miroir →

← Fred

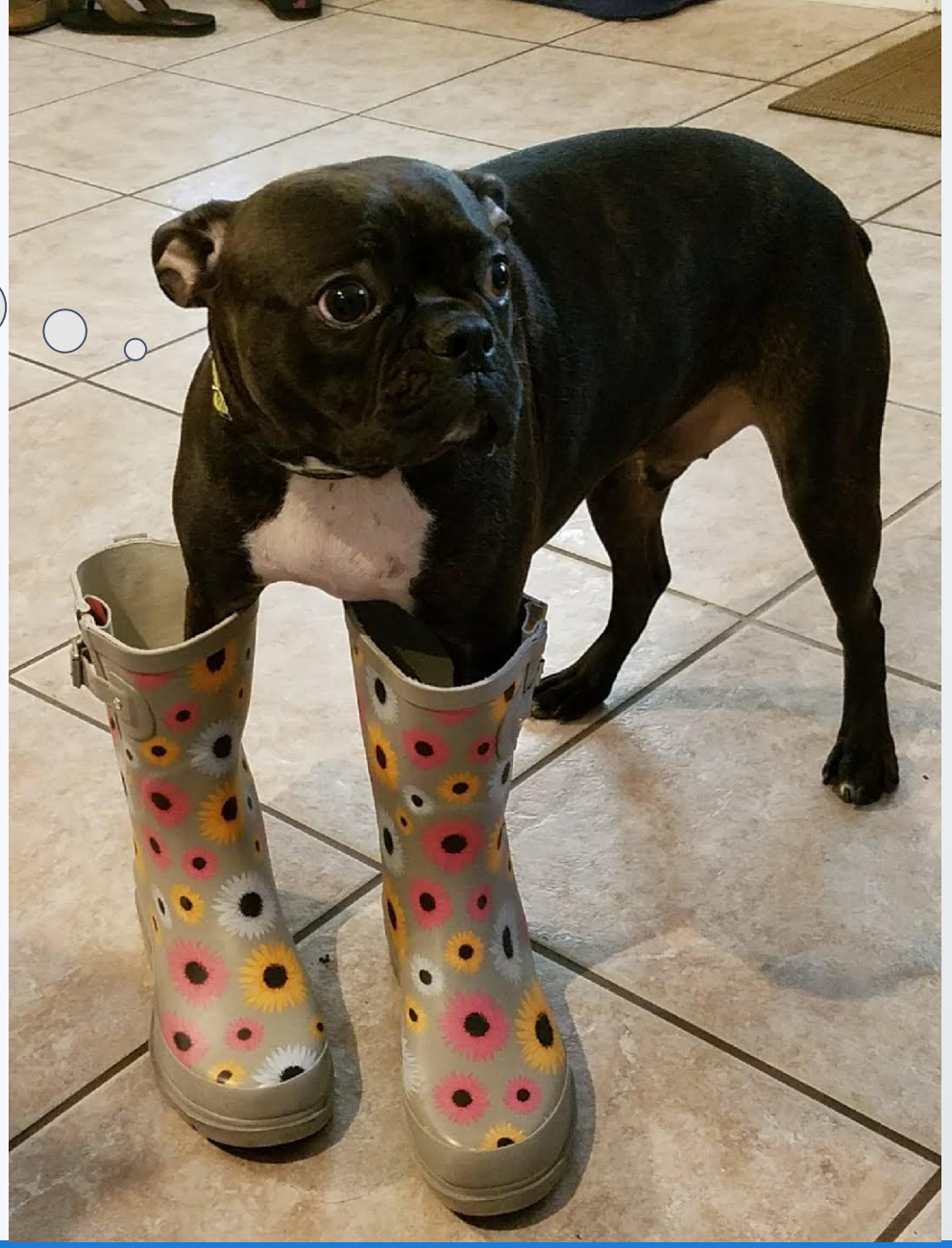
- Ops guy at heart, manager who wants to remain reasonably technical ;-)
- Crossed the french Alps by foot (autonomous - Leman lake to Mediterranean sea)
- Product Security leader
- DefectDojo core moderator

This is how I feel when I log into the Nth security tool web console…

And when I have to combine multiple tool's output for reporting

90% of Enterprise Vulnerability programs

But WHY!



OWASP DefectDojo

An open-source application vulnerability correlation and security orchestration tool.

The source of truth for a security program that makes vulnerability management work by

- **Consolidating** and **deduplicating** findings from multiple tools
- **Create** findings and **reconcile status** with defect trackers (e.g. JIRA)
- **Enabling automation** with its REST API
- Maintain products and applications information

Use cases - ingest all the things

Ad-hoc / manual

- Ad-hoc tools report upload, centralize
- Keep track of internal security assessments
- Leverage for your 3rd party pentests
- Track findings from your teams threat models

Complianc'ish

- Map and enforce your SLAs
- Keep track of your risk acceptances

CI

- Call DefectDojo directly from your CI pipelines
- Or from whatever abstraction/framework

Tech stack

Hope for a ReactJS front-end soonish...

Features ‘Bullet list’

- Manages AppSec program
- Application inventory + metadata
  - e.g., compliance, regulations
- Metrics / dashboards / reporting
- OWASP ASVS built in
- Tagging on multiple levels
- Historical knowledge of past assessments
- Calendar of security activities
- Export to Google Sheets
- REST API / Swagger-ified
- SSO (Okta, Google, SAML, ...)
- Notifications to JIRA, slack, MS teams, email
- Ingest reports from multiple tools

And more...

How many different tools do you use?

- DAST tools
- SAST tools
- Composition analysis/3rd party library tools
- Infrastructure tools
- Cloud tools
- Docker tools
- ...

How many of these can DefectDojo import?

100

and growing

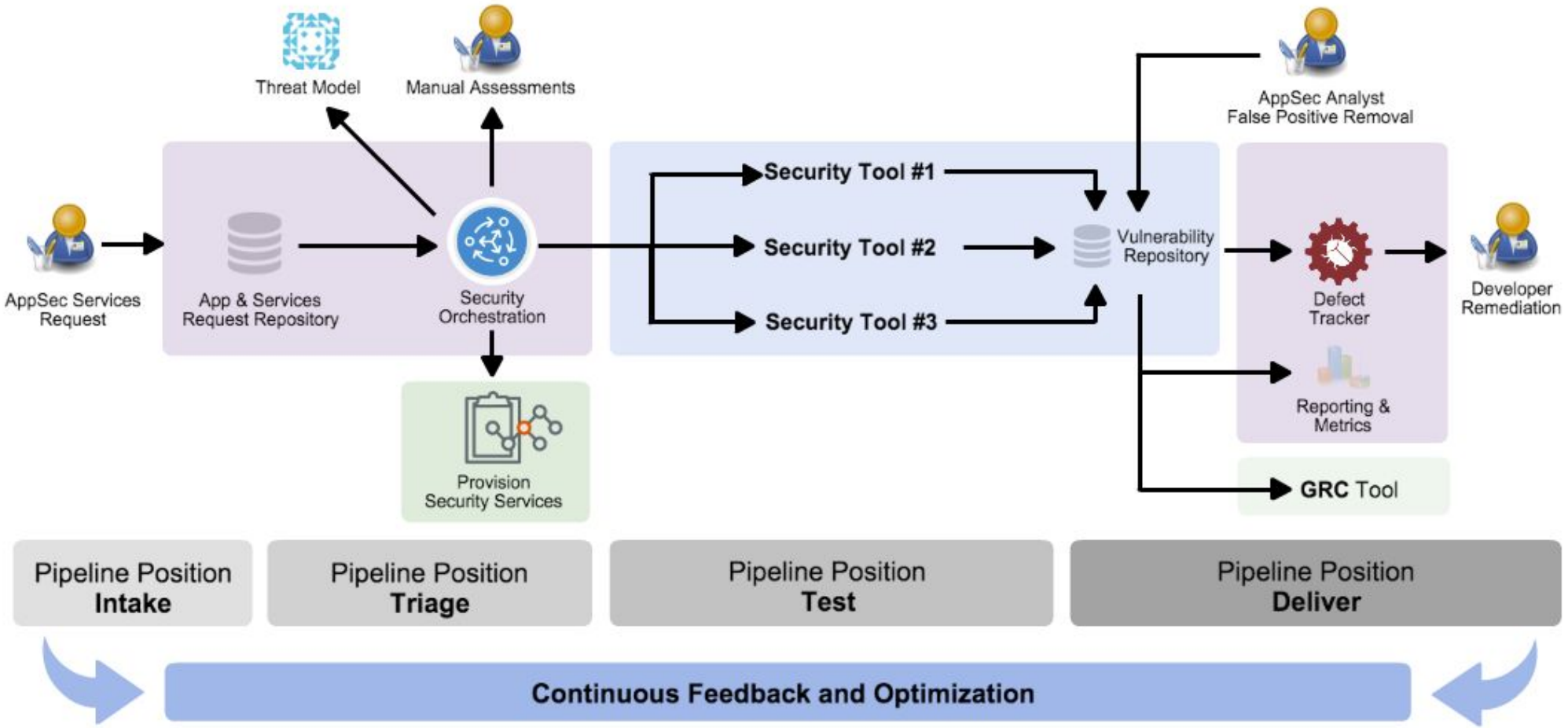
Automation

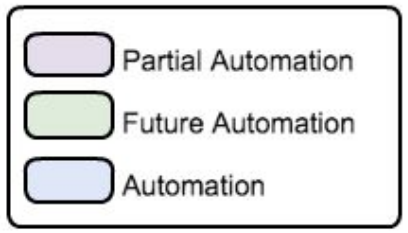
where DefectDojo shines

There’s never enough people or time...

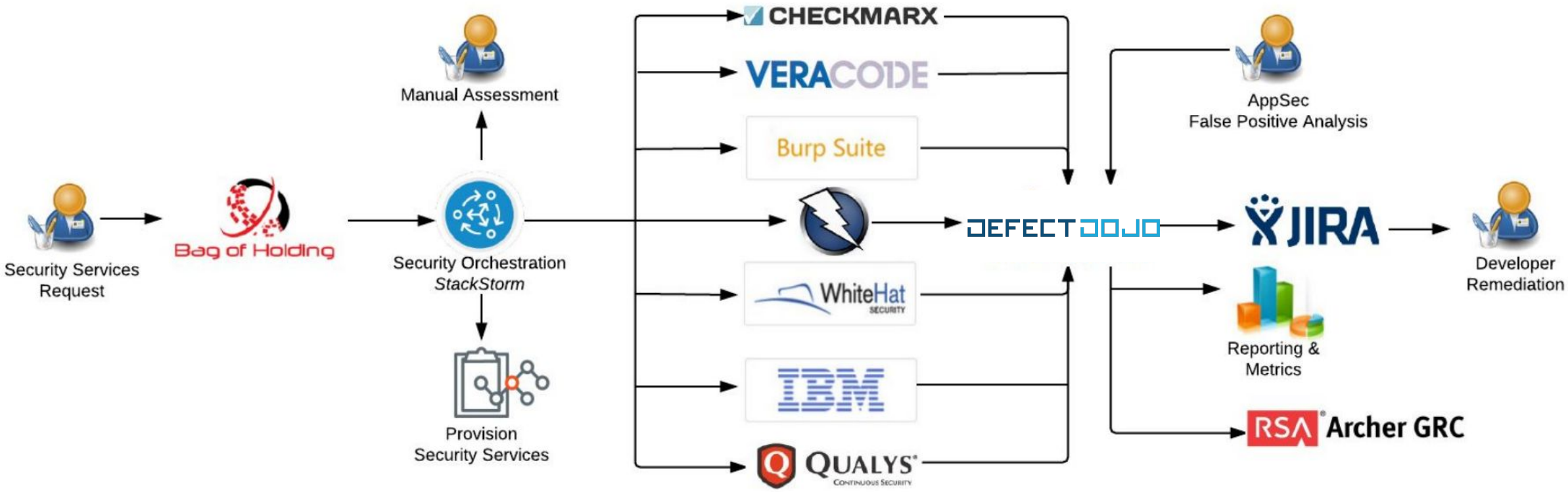
- AppSec teams size is small vs Dev teams size
- Automate all the things that don’t take a human brain
- DefectDojo (and its REST API) is the heart of AppSec automation

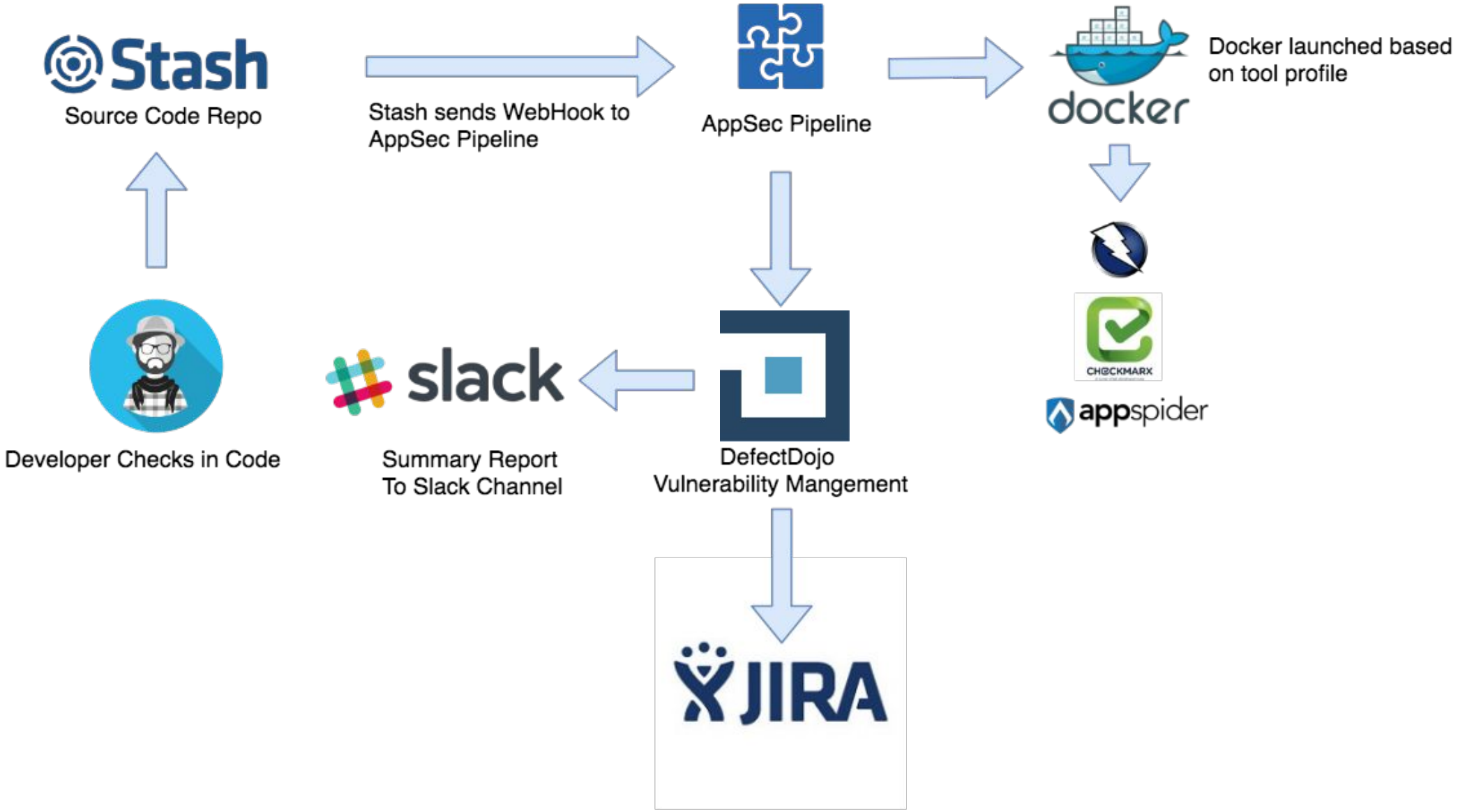
Rugged Devops - AppSec Pipeline Template





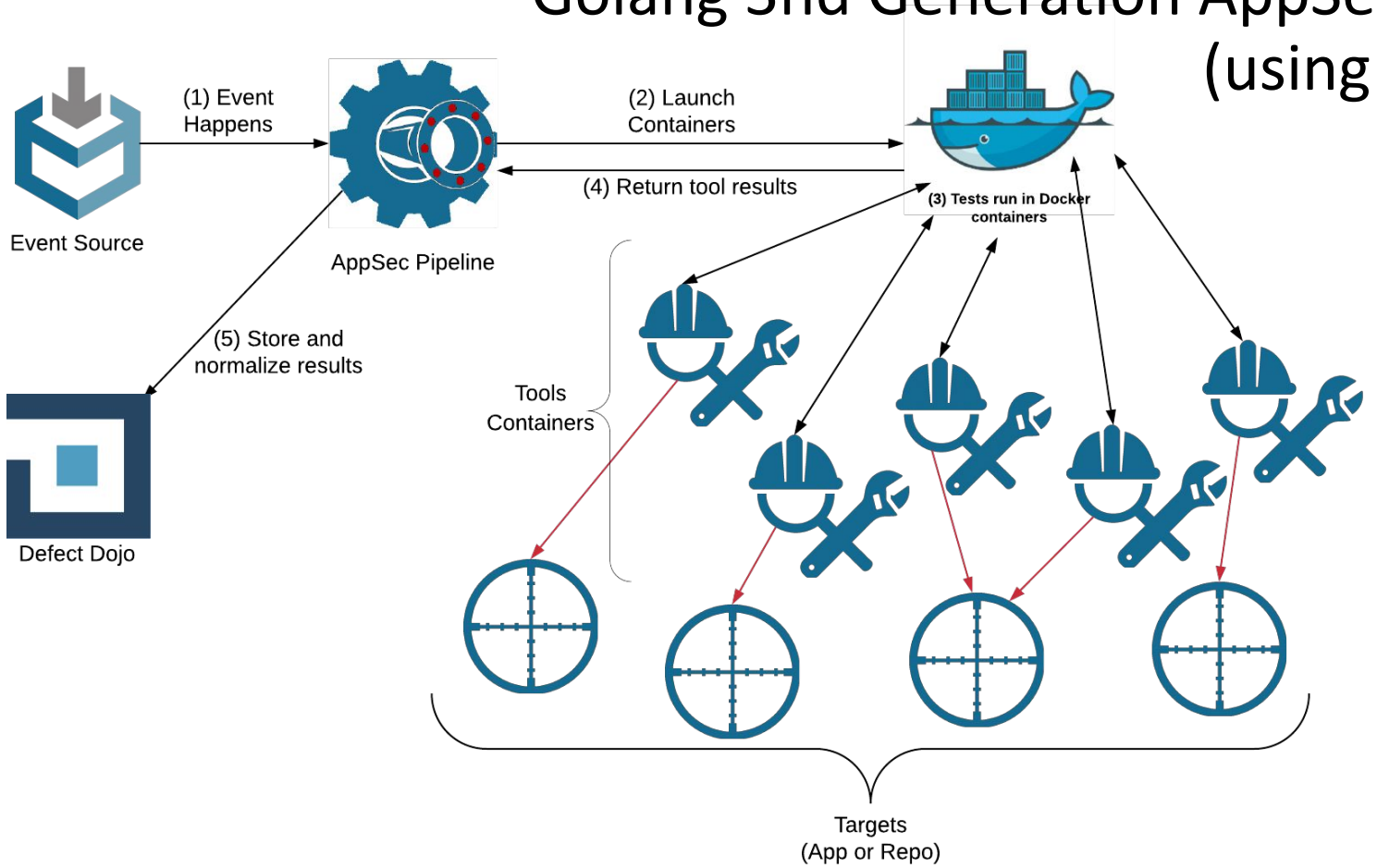
First Gen AppSec Pipeline




Stash
Source Code Repo
Stash sends WebHook to
AppSec Pipeline
AppSec Pipeline
docker
Docker launched based
on tool profile
CHECKMARX
appspider
Developer Checks in Code
slack
Summary Report
To Slack Channel
DefectDojo
Vulnerability Mangement
JIRA

Demo: gasp-docker

Golang 3nd Generation AppSec Pipeline (using docker)



AppSec Pipeline Stats

15 Repos

5,100 Runs

4 Months

25,000+
Container Executions

Automation Results

	2014	2015	2016
Number of Assessments	**44**	**224**	**414**
Headcount	**N/A**	**-3.5**	**-2**
Percentage Increase	**N/A**	**450%**	**107%**

Deployment options

docker-compose

- As easy as *docker-compose pull && docker-compose up*
- Can override the profiles for easy development
- Can also be used for some (semi) prod-like workloads
  - Still run the database somewhere dedicated
- Probably the most tested way of deploying
  - And all our tests run on docker

Real world docker-compose

- 1 EC2 instance t2.large (2 vCPUs, 8GB of RAM)
- Database running on AWS RDS (MySQL)
- DefectDojo app overall settings
  - uWSGI: 4 processes / 6 threads (24 concurrent connections per “django” pod)
  - Celery: prefork mode, custom prefetch multipliers with autoscaling.

⟶ Good for up to ~200K findings

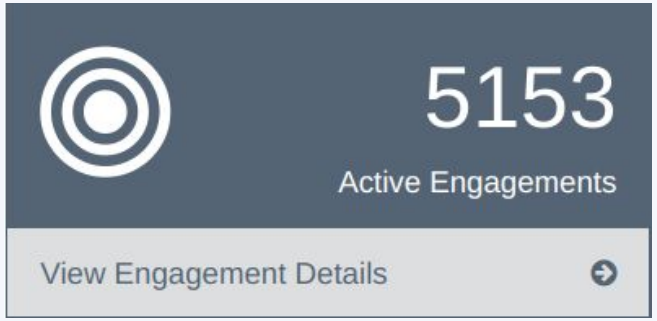
⟶ Running full dedupe computation may likely kill you (celery workers will not cope need more CPU)

kubernetes / helm

- Packaged with Helm 3
- Run locally with minikube (or else, but we've done local minikube)
- Can run with minimal changes on your favorite cloud provider
- Do not yet support file uploads

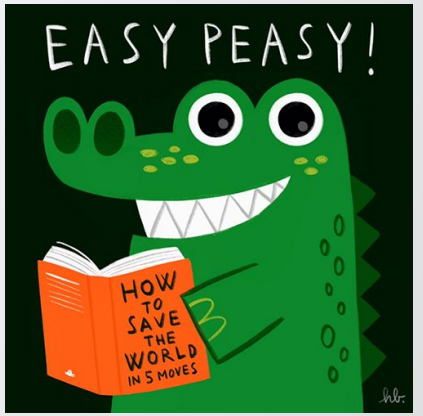
Real world k8s example

- GKE cluster, 5 nodes (n1-standard-4) (also includes all ops related pods, not just defectdojo)
  - 3 “django” pods (uWSGI), 6 celery pods by default -> auto-scaling
  - Allows for HA and seamless rolling upgrades
    - if the django database migration do not take too long…
- Database running on Google’s Cloud SQL (Postgres)
  - 21GB in size - we had to disable audit mode for now :-(
- DefectDojo app overall settings
  - uWSGI: 4 processes / 6 threads (24 concurrent connections per “django” pod)
  - Celery: prefork mode, custom prefetch multipliers with autoscaling.



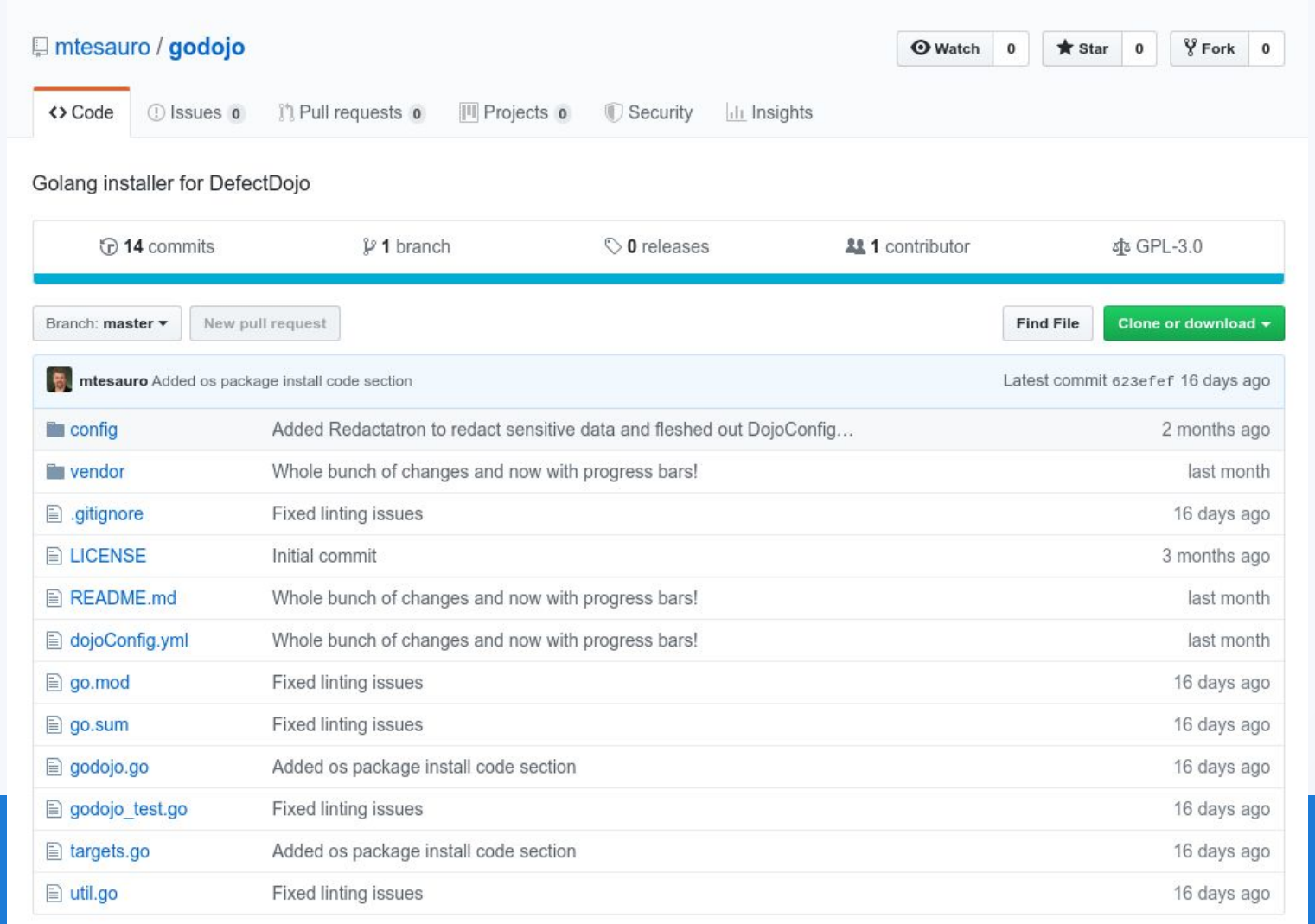
~75 products

~in DB: 1.2M findings (half are dups),
150K findings ingested per month /
5000 per day



godojo (setup.bash was EOL'ed!)

New stand-alone installer



mtesauro / godojo

Watch 0 | Star 0 | Fork 0

Code | Issues 0 | Pull requests 0 | Projects 0 | Security | Insights

Golang installer for DefectDojo

14 commits | 1 branch | 0 releases | 1 contributor | GPL-3.0

Branch: master | New pull request | Find File | Clone or download

mtesauro Added os package install code section — Latest commit 623efef 16 days ago

config	Added Redactatron to redact sensitive data and fleshed out DojoConfig…	2 months ago
vendor	Whole bunch of changes and now with progress bars!	last month
.gitignore	Fixed linting issues	16 days ago
LICENSE	Initial commit	3 months ago
README.md	Whole bunch of changes and now with progress bars!	last month
dojoConfig.yml	Whole bunch of changes and now with progress bars!	last month
go.mod	Fixed linting issues	16 days ago
go.sum	Fixed linting issues	16 days ago
godojo.go	Added os package install code section	16 days ago
godojo_test.go	Fixed linting issues	16 days ago
targets.go	Added os package install code section	16 days ago
util.go	Fixed linting issues	16 days ago

Features

- Single binary installer
- 160+ configurable options with sane defaults (yaml)
- All options can be overridden with ENV vars
- Non-interactive (optional)
- Multiple logging levels
- Install a release, a specific commit, or branch

Recent improvements and next up

Recent improvements

- Refactoring
  - Parser code
  - JIRA handling code
- Tests
  - Way more unit and integration tests FTW
- Release governance
- Re-import (also refactored)
  - Now keep tracks of delta in-band
  - Dedupe algorythm now matching the regular import one
- Findings grouping to push as one to JIRA
- Performance improvements
- Many more: Over 120 PRs merged every month!

Up next

- Coming soon: new authorization model (kudos to StefanFI!)
  - Right now behind feature flag, testing welcome!
  - Should be the default authorization model coming in autumn/winter.
- APIv1 or APIv2?
  - v1 has been EOL'ed (end of 2020)
  - v2 set to get more love, better swagger
- GSoC
  - First attempts to build something with ReactJS
- Helm chart published with every release starting with 1.15.0

```
$ helm search repo defectdojo

NAME                            CHART VERSION     APP VERSION DESCRIPTION
helm-charts/defectdojo      1.5.1         1.14.0-dev  A Helm chart for Kubernetes to install DefectDojo
```


Deduplication and jira groups

Community

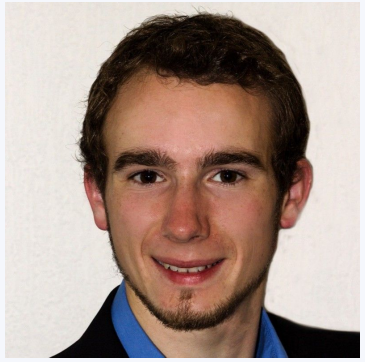
The nucleus

Aaron Weaver

Greg Anderson

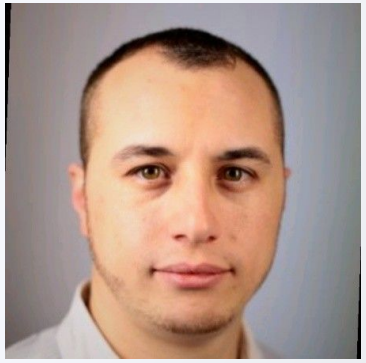
Valentijn Scholten

Jannik Jürgens

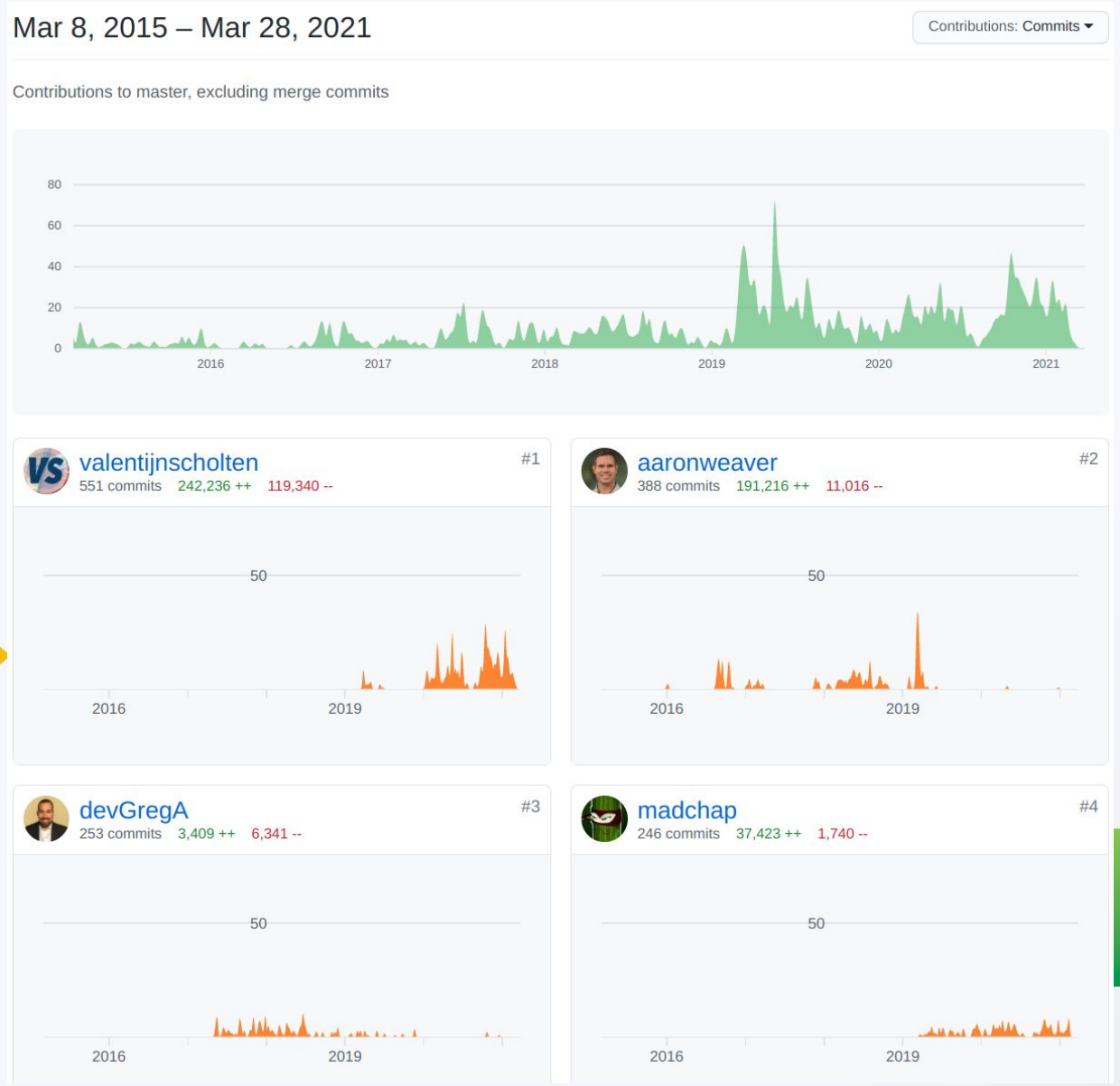


Cody Maffucci

Damien Carol



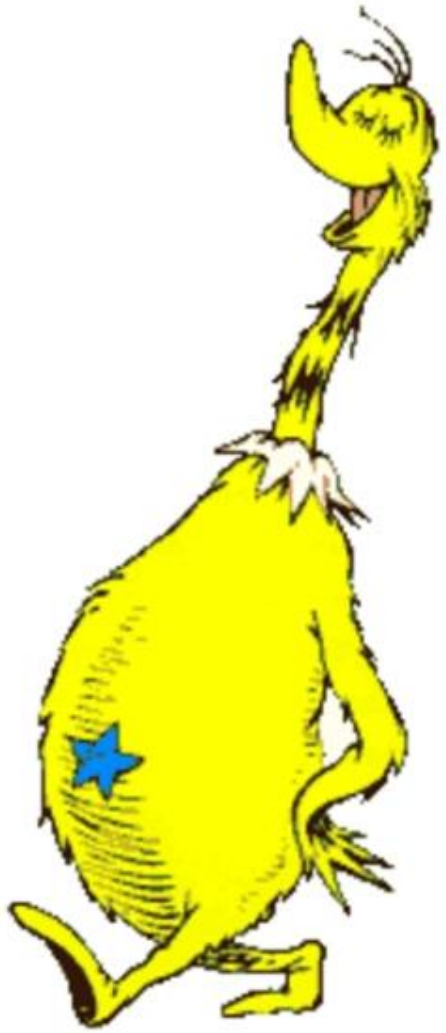
An active project



2021 Google Summer of Code

FLAGSHIP

We got stars on ours



Unwatch 200 | Unstar 1.6k | Fork 755

February 28, 2021 – March 28, 2021

Period: 1 month

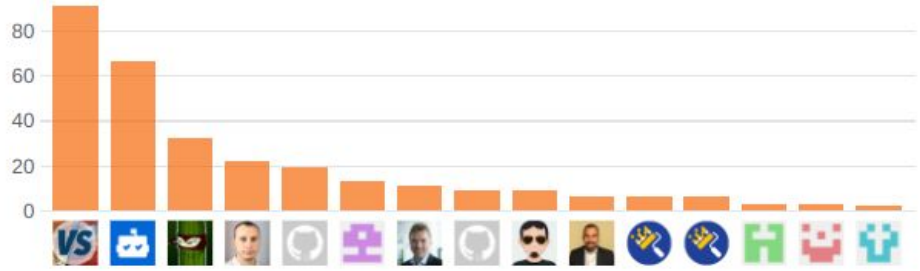
Overview

144 Active Pull Requests

88 Active Issues

124 Merged Pull Requests	**20** Open Pull Requests	**61** Closed Issues	**27** New Issues

Excluding merges, **31 authors** have pushed **12 commits** to master and **249 commits** to all branches. On master, **1 file** has changed and there have been **1 additions** and **1 deletions**.



How can you help?

- Write some code (e.g. a parser) / submit a PR
- Submit issues
- Help with the documentation
- Provide an example of scanner output
- Write code / docs for a deployment method
- Join the Slack channel and answer questions
- Donate / Sponsor a feature enhancement

Latest from contributors, not moderators!

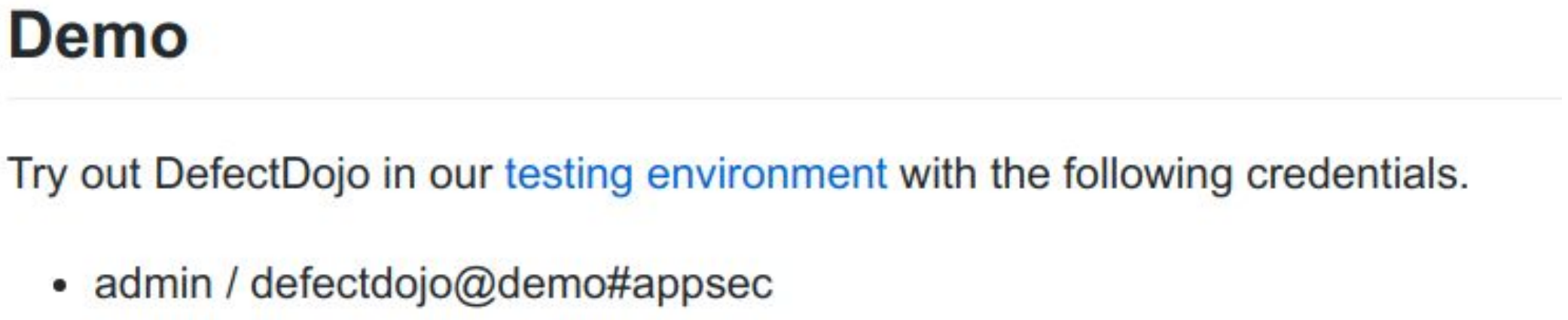
Only examples, for all contribs see the release notes or merged PRs

- Brand new authorization model - by StefanFI
- Performance improvements - by Daniel Naab
- GitHub Actions - Kubernetes/Helm related - dsever, bgoareguer
- New importers/parsers - SPoint42, jis0324, hasantayyar, bp4151, mohcer and quite a few others!
- API enhancements - RomainJufer, xens

Try it yourself anytime

Many things we have not talked about...

https://demo.defectdojo.org



Or clone and *docker-compose up -d*

Rate this Session

SCAN THE QR CODE TO COMPLETE THE SURVEY

Or
https://forms.gle/b55Uget61YWXPV1y8

Thank you

See around on the OWASP Slack \o/

Thank You!