ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Running FaaS with Scissors

Matt Tesauro
@matt_tesauro

Who is this guy?

- Reformed programmer and AppSec engineer
- 11+ years in the OWASP community
  - OWASP AppSec Pipeline
  - OWASP Defect Dojo
  - OWASP WTE
  - 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)

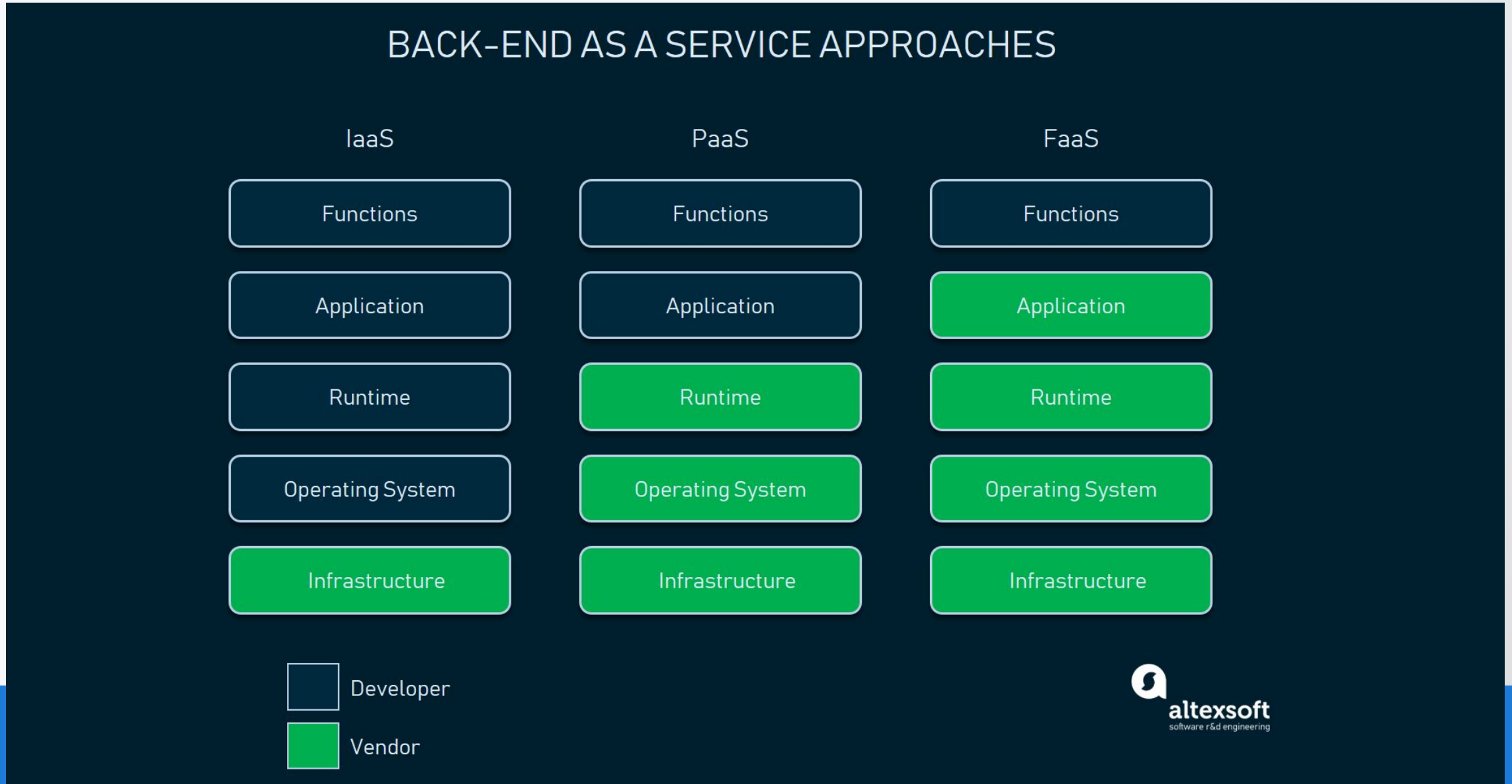
Not everything about completing a goal is sunshine and roses...

Serverless, what is it?

What is serverless?

- “Someone else’s computer”
- Remember xinetd ?
- Serverless aka Functions
  - Move the boilerplate of handling connections to the provider
  - “Focus on business value” for us ***focus on security problems***
- Serverless == Functions + Events + Managed Services
  ^ this is most of the work

Understanding what you're getting



More on Serverless

- Common Use-cases
  - REST APIs
    - Function per method/resource fronted by an API Gateway
  - Data Pipeline
    - Event happens, process something about that event, move on
- Gotchas
  - Use trigger URLs for early testing
  - Observability is really important
    - most of your ‘stack’ is already a black box
  - Watch DB connections, limit them to 1 idle and 1 max connections
  - These are called and killed - cattle not pets

Should I be scared of Serverless?

What's security's traditional answer to using new tech...

NO!

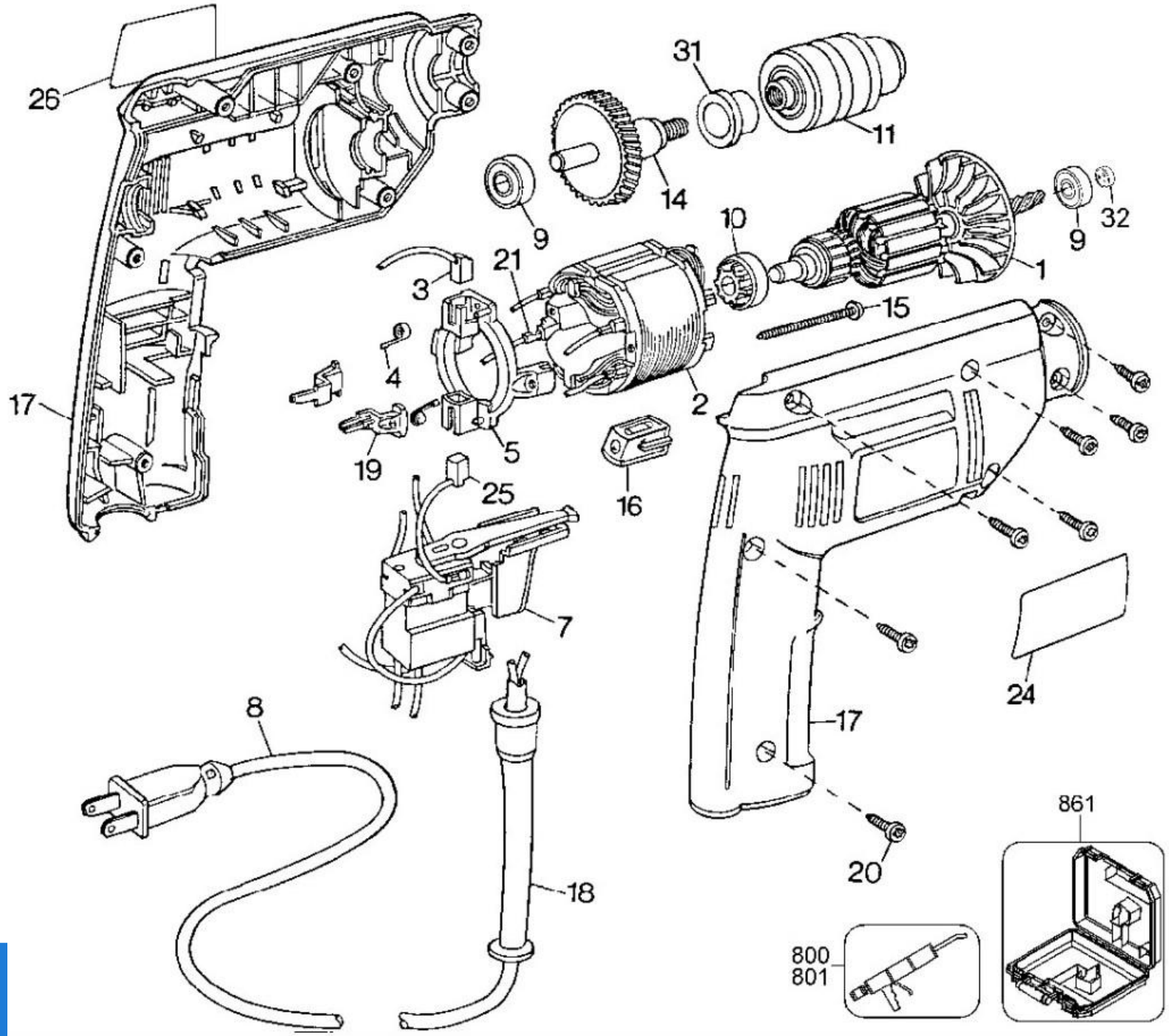
Let’s get real

- Mistakes can be made in any language using any technology
- Most of the ~infrastructure~ is run by your provider
  - hopefully better than you’d run it
- Easy path from throw-away scripts to security automation
  - you ***are*** writing some code currently, right?
- If nothing else…
  bug counts will be less since you’re writing less code [*]

The Big Picture

Thinking in Serverless

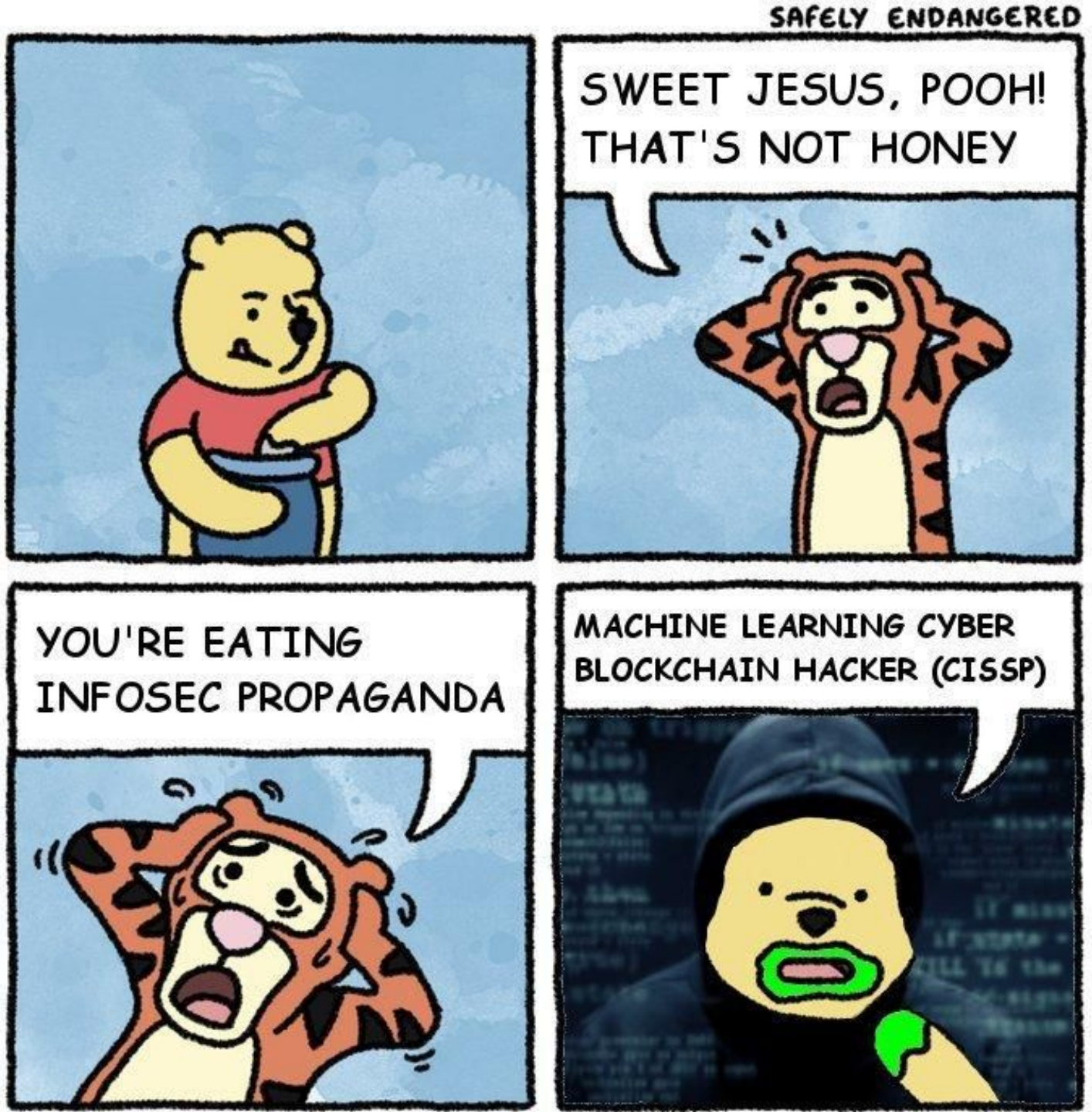
When all you have is a drill...

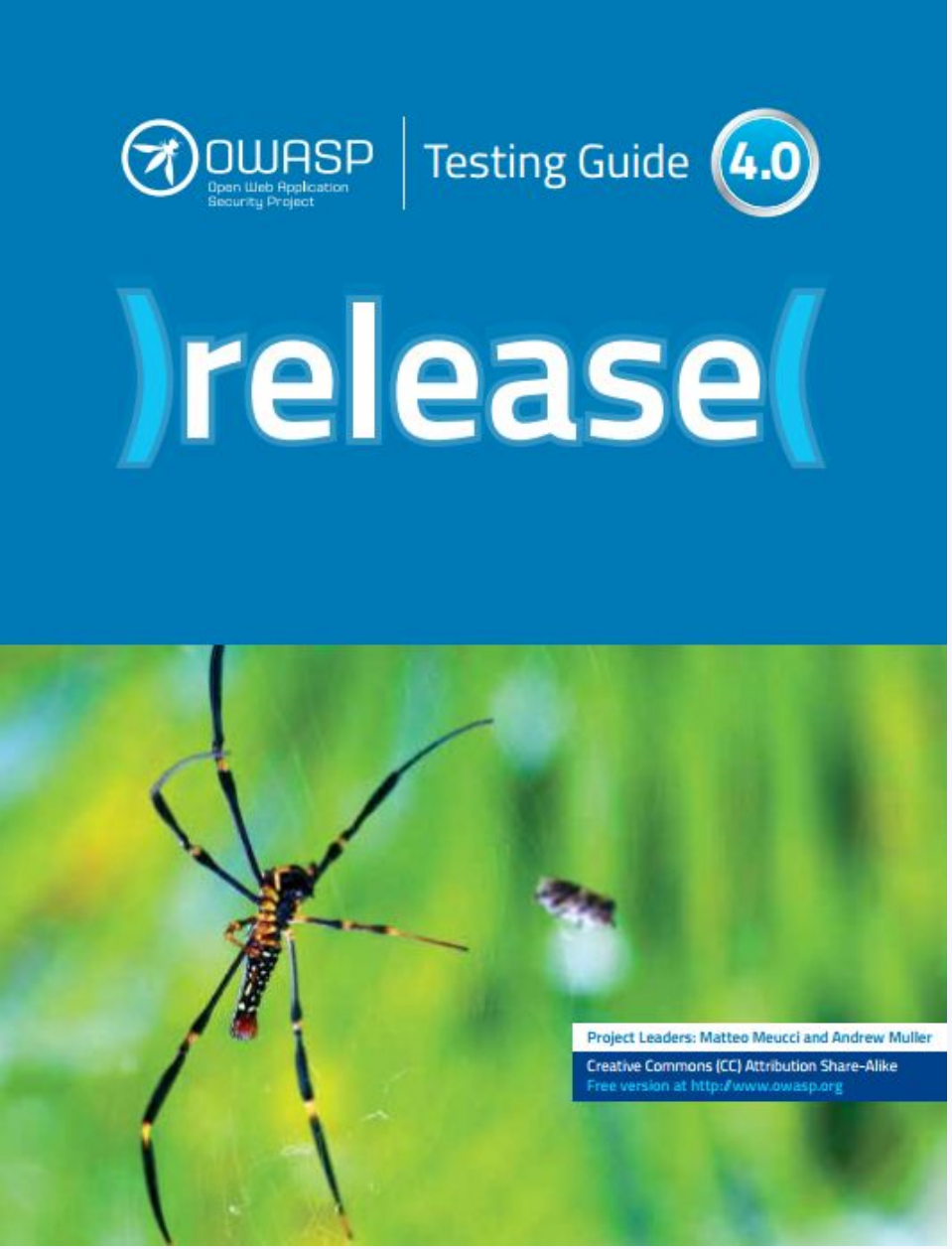


Explode your security processes

- There’s certain things you do every time
  - Something happens (Event)
    Code commit, deploy to UAT, …
  - You take some action (Function)
    SAST repo, security baseline the deploy…
  - You inform the Product team (Managed Service)
    Commit de0633 has an issue, security headers are missing in last deploy, drop a finding into the team Slack channel…

Using these powers for Good


SAFELY ENDANGERED
SWEET JESUS, POOH! THAT'S NOT HONEY
YOU'RE EATING INFOSEC PROPAGANDA
MACHINE LEARNING CYBER BLOCKCHAIN HACKER (CISSP)



How will this work for me?

Think about the sections of the OWASP Testing Guide…

Could those be turned into functions?

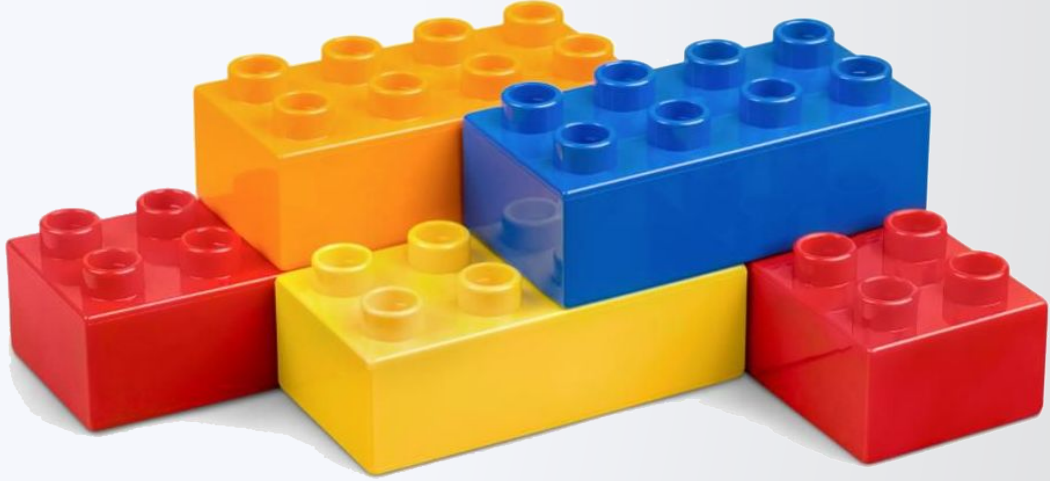
Getting real with serverless

- OTO-INFO-001 - Search engine discovery and recon
  - function to do your favorite ‘Google dorks’
- OTO-INFO-002 - Fingerprint web server
  - function to poll the server and any “X-Powered-By” headers
- OTO-INFO-003 - Review webserver meta files
  - function to pull robots.txt, crossdomain.xml, sitemap.xml…
- Other fun functions
  - HTTP header checks
  - HTTP method checks
  - TLS/SSL configuration checks
  - Custom checks for your apps
    e.g. grep web.config for mandatory settings in .Net apps

OK, AppSec, what else? DFIR

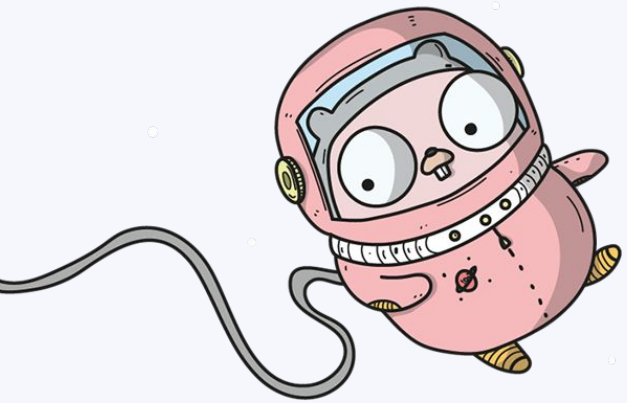
- Reverse IP Lookup
- IP reputation
- IP blacklist check
- Domain reputation
- Known IP (do we own it)
- Check IP against our cloud account(s)
- Who registered domain
- How long domain registered

- Shodan lookup
- Geolocate IP
- Whois
- Check against threat lists/APIs
- Virus Total



Building blocks

Any resemblance to actual toys, living or dead,
or actual trademarked items is purely coincidental.



Serverless options

SPARTA
gosparta.io

Providers / Projects

- AWS Lambda
- Google Cloud Functions
- Azure Functions
- IBM Cloud Functions
- Oracle Functions
- OpenFaaS
  - on/off prem

Languages / Frameworks

- Provider SDKs
  - for most popular languages
- “serverless framework”
  https://serverless.com/framework/
- Sparta (Golang for Lamba)
- Furnace (furnace.org)
- [Your programming language]
  - It's just handling HTTP requests so you language can do that, right?

CNCF Serverless Landscape

2019-05-10T14:35:42Z 641871a

See the serverless interactive display at s.cncf.io

Greyed logos are not open source

Tools

CLOUDZERO, dashbird, Epsagon, event gateway, HASURA, IO|pipe, Iron.io, Kubeless, python-λ, SCAR, SIGMA, STACKERY, THUNDRA

Security

intrinsic, Protego, PURESEC, threat stack

Framework

APEX, Architect, aws Chalice, AWS SAM, Claudia.js, FLOGO, gun.io, serverless, SPARTA, Spring Cloud Function

Hosted

Installable

Platform

ALGORITHMIA, Alibaba Cloud Function Compute, AWS Lambda, Azure Functions, BINARIS, cloudboost, CLOUDFLARE Workers, Google Cloud Functions, HUAWEI FunctionStage, IBM Cloud Functions, kitchune, netlify, PubNub Functions, spotinst, stdlib, Tencent Cloud, twilio Functions, ZEIT

OpenWhisk, AppScale, DISPATCH, fission, fn, GALACTIC FOG, Knative, Kubeless, Kyma, LunchBadger, nuclio, OPENFAAS, PipelineAI, rff, Virtual Kubelet

s.cncf.io

Serverless computing refers to a new model of cloud native computing, enabled by architectures that do not require server management to build and run applications. This landscape illustrates a finer-grained deployment model where applications, bundled as one or more functions, are uploaded to a platform and then executed, scaled, and billed in response to the exact demand needed at the moment

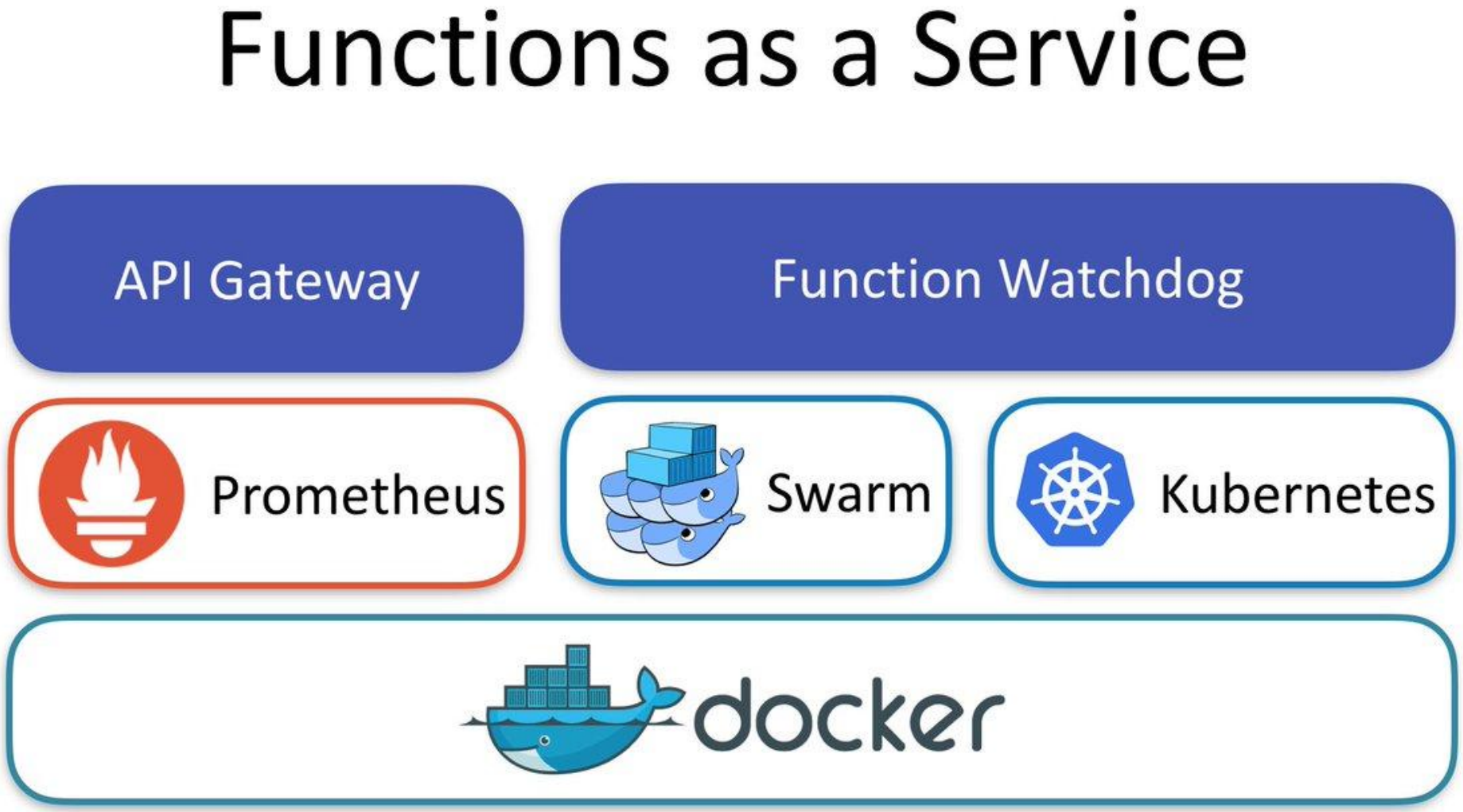
CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION

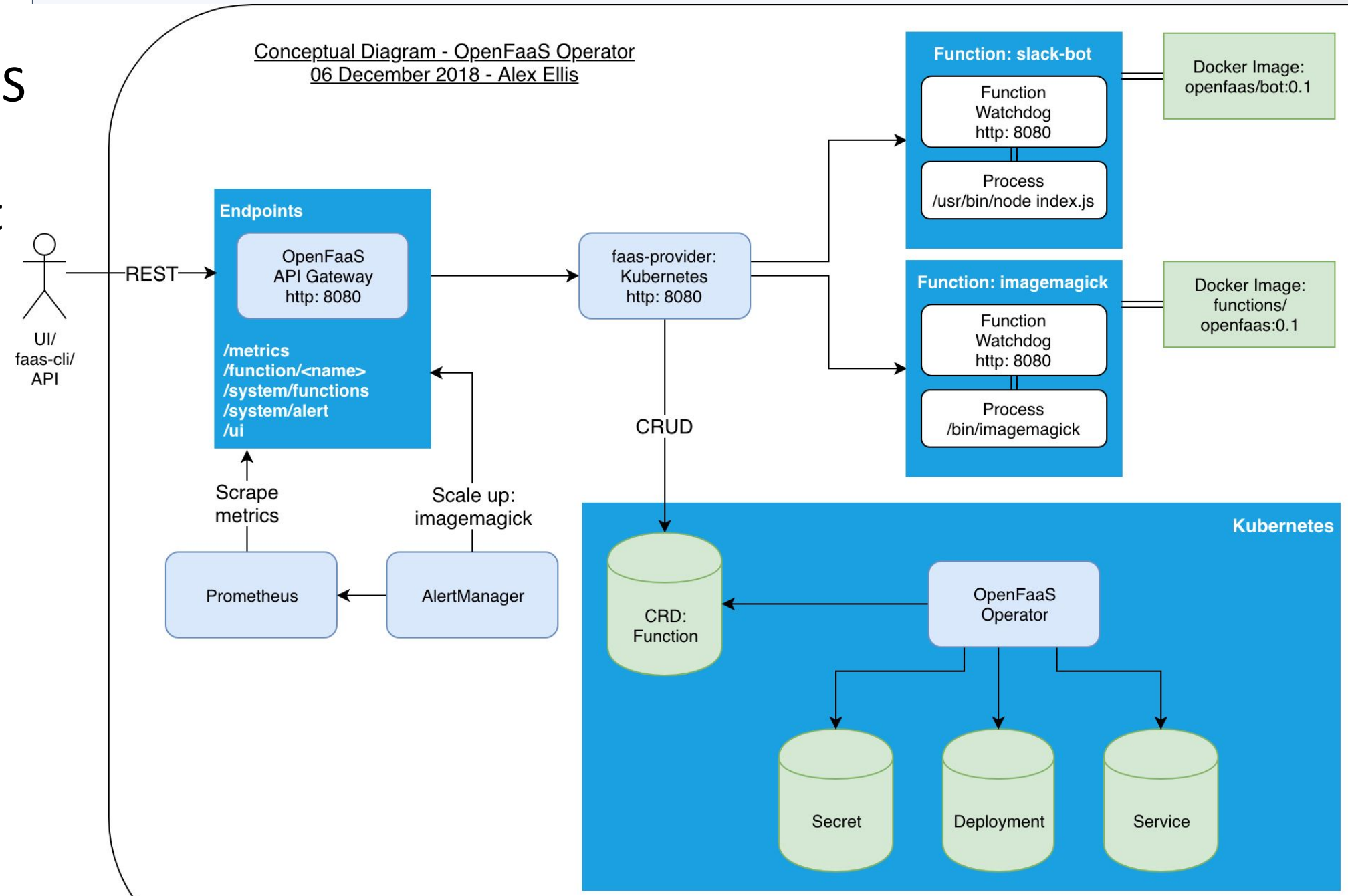
Redpoint

Cloud Native Landscape

Shout out to OpenFaaS



OpenFaaS has excellent docs and a very good tutorial!



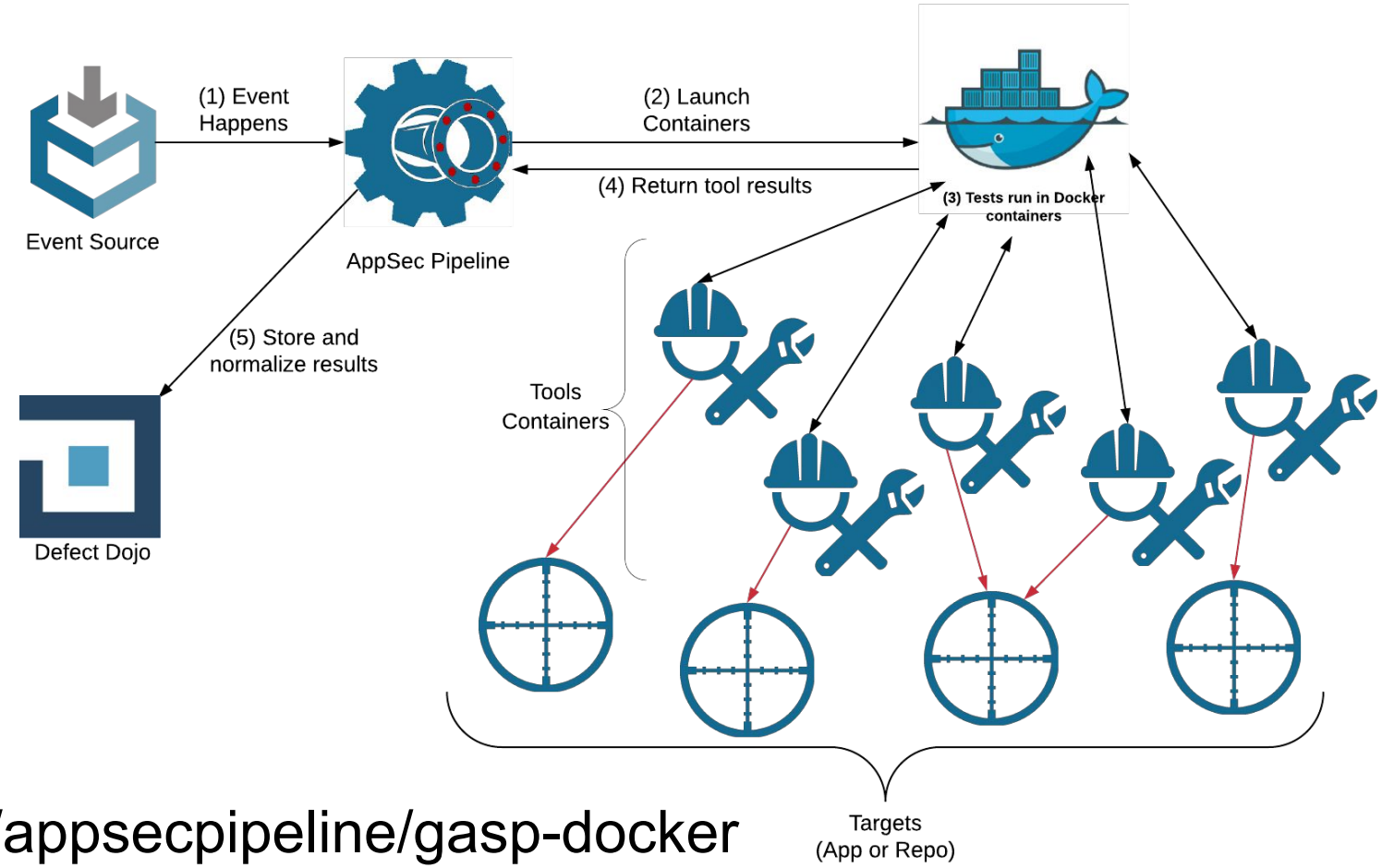
3x Demo Time...

So, that worked...

Maybe this will too...

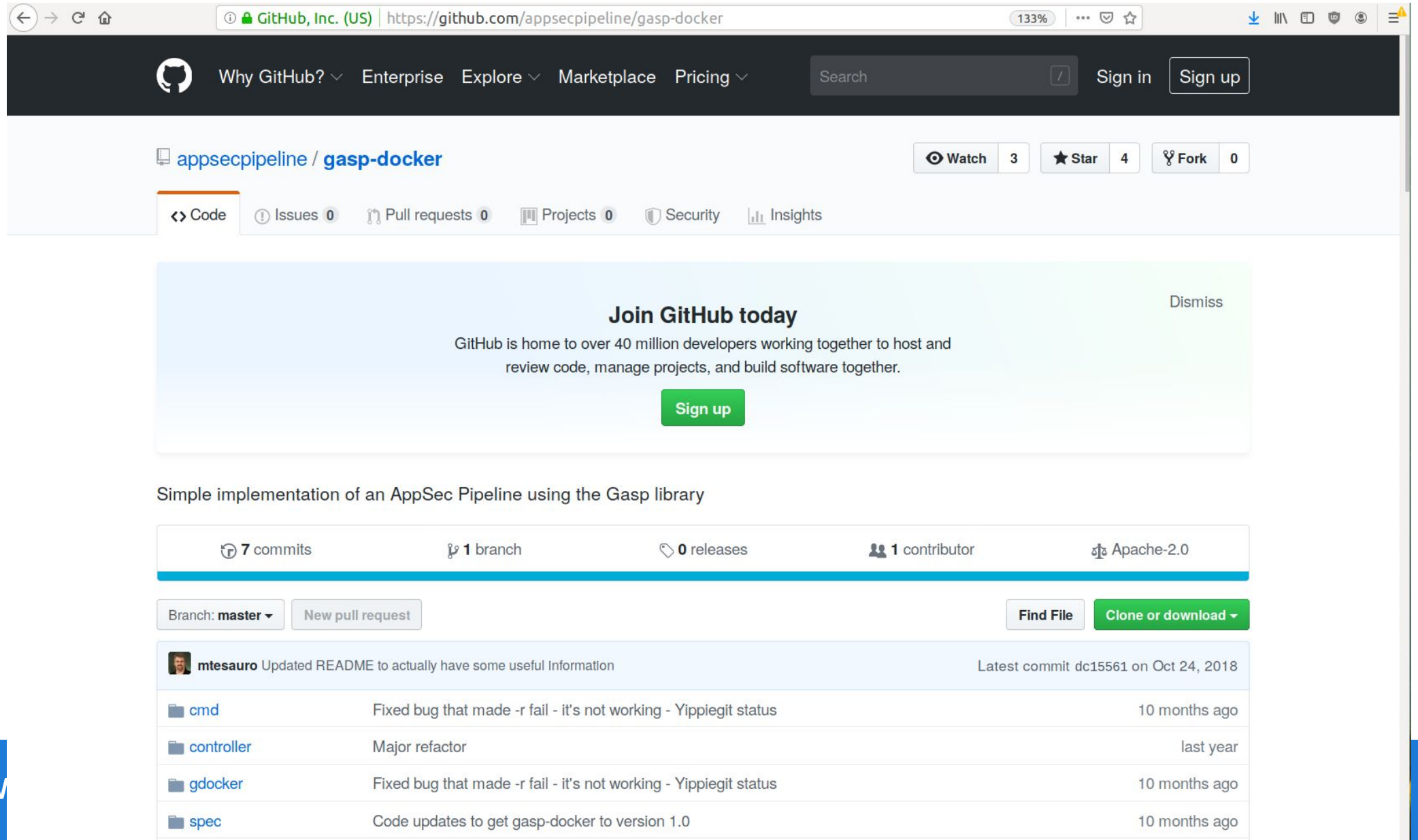
gasp-docker

Golang AppSec Pipeline (using docker)

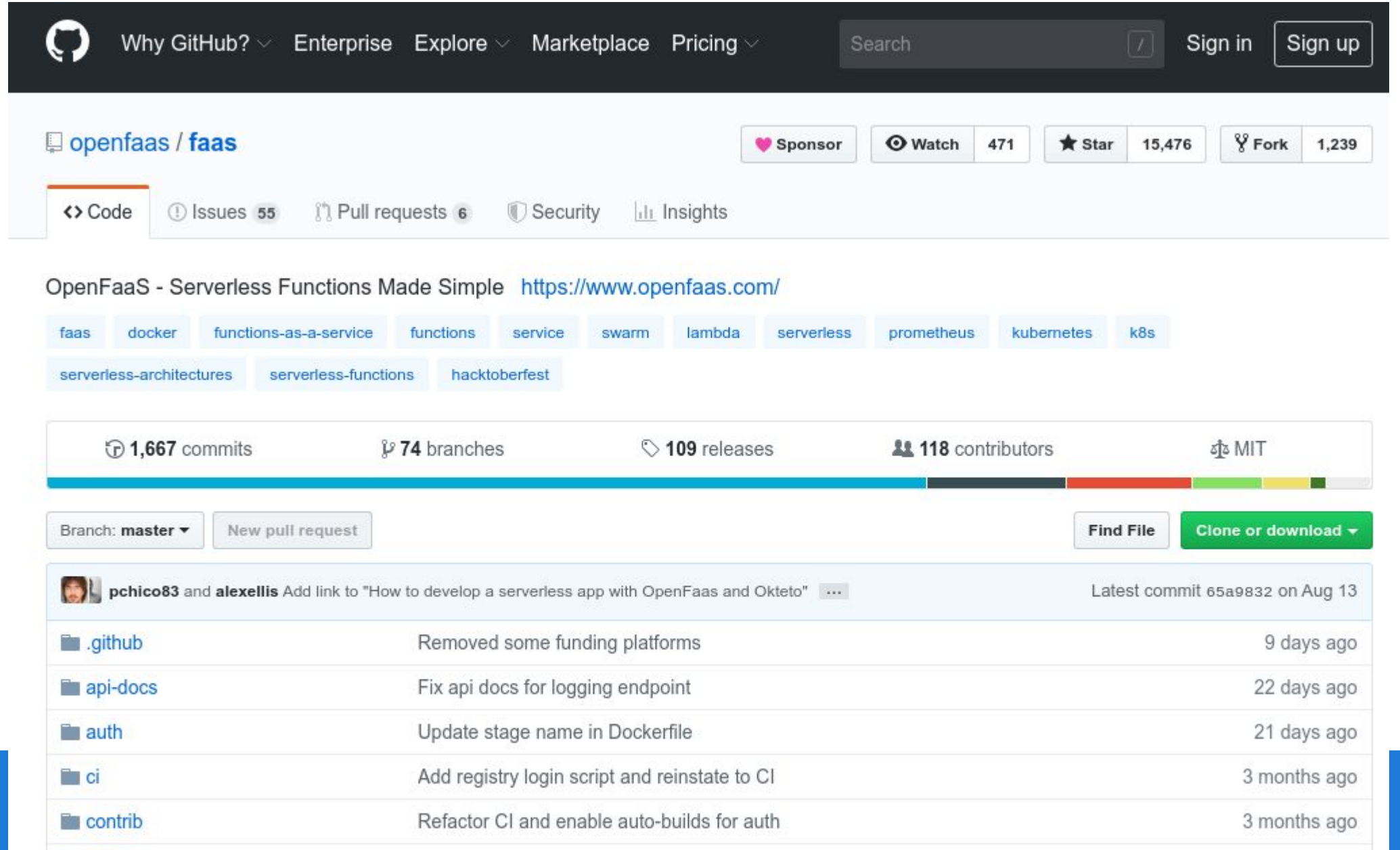


https://github.com/appsecpipeline/gasp-docker

Under the “appsecpipeline” GH Org



OpenFaaS on Github



alfred

https://github.com/kcmerrill/alfred

alfred

A simple go/yaml powered make file/task runner with a bit of a twist and a ton of flexibility.

Features

- Extendable + Plugins
- Watch files for modifications
- Retry/Rerun tasks based on failures before giving up
- Logging
- Success/Failure decision tree
- Run tasks asynchronously or synchronously
- Arguments
- Loops
- Static webserver
- Many more!

For more information RTFM.

Sample Usage

Create a file named: `alfred.yml`

```
say.hello:
    summary: I will say hello!
    usage: alfred say.hello
    command: echo "Hello!"

say.howareyou:
    summary: I will ask how you are
    usage: alfred say.howareyou
    command: |
        echo "How"
        echo "Are"
        echo "You?"
```

Serverless Security Automation is

- Not in-depth testing
  but ‘you must be this high’
- Allows some testing to be ‘pre-calculated’ for assessments
- Creates a baseline of security

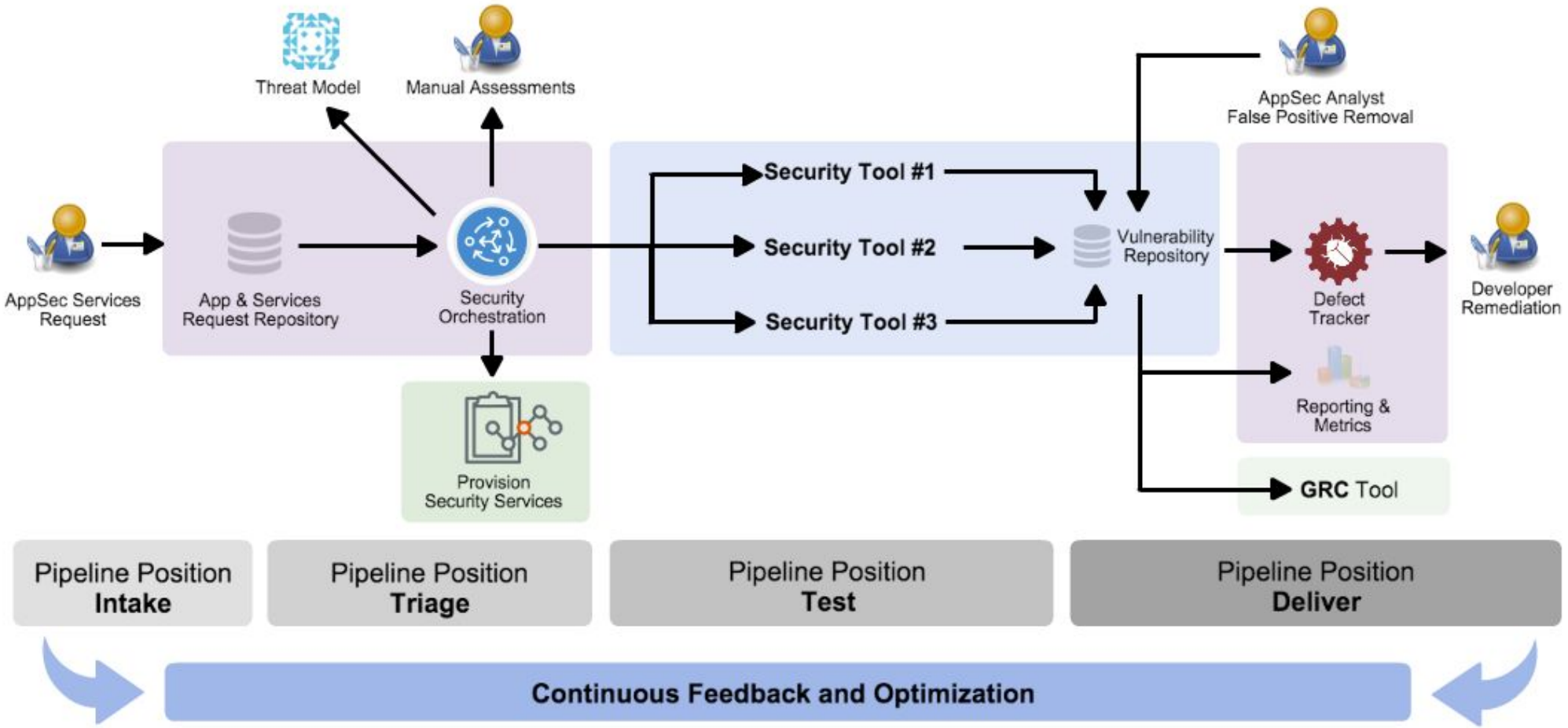
Welcome to the world of severless security automation

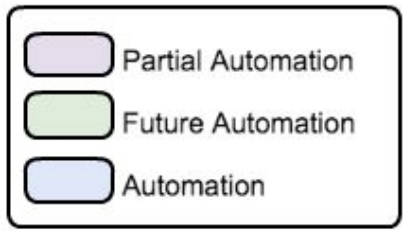
THANKS!

Questions?

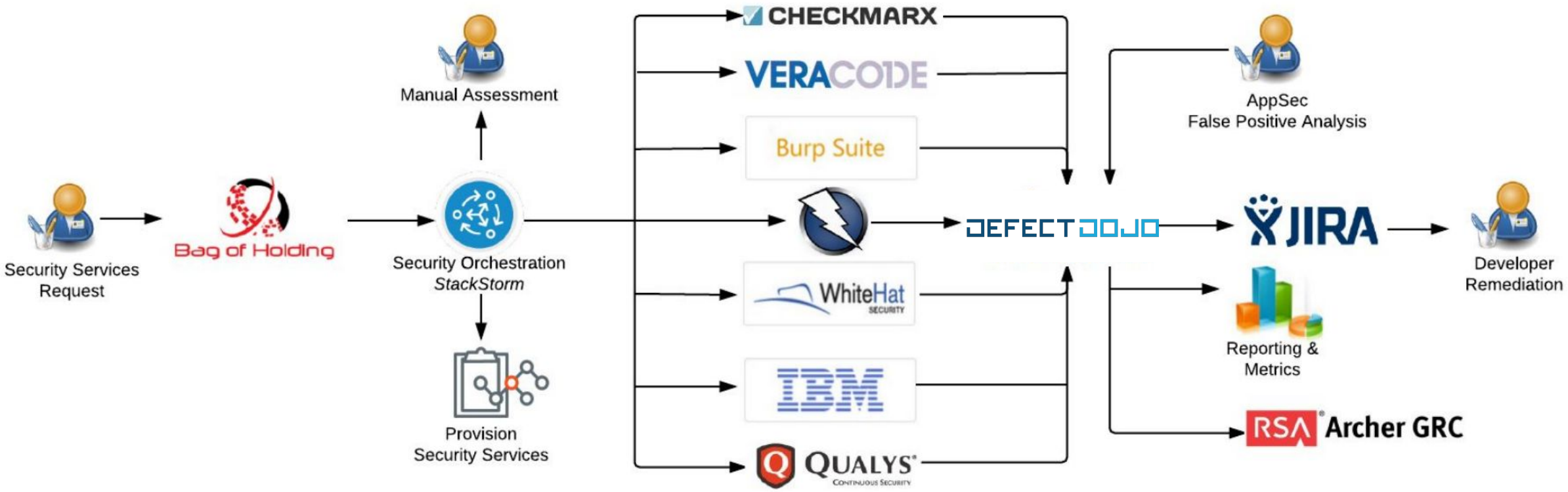
or do you need a nap?

Rugged Devops - AppSec Pipeline Template





First Gen AppSec Pipeline



OWASP Projects
AppSec Pipeline

Weaponized
Jenkins

3) Push Findings

DEFECTDOJO

Source of Truth

4) Validated
Findings

JIRA

Project Jira

Optional
Notifications

Project Slack
Channel

2) Launch Docker(s)

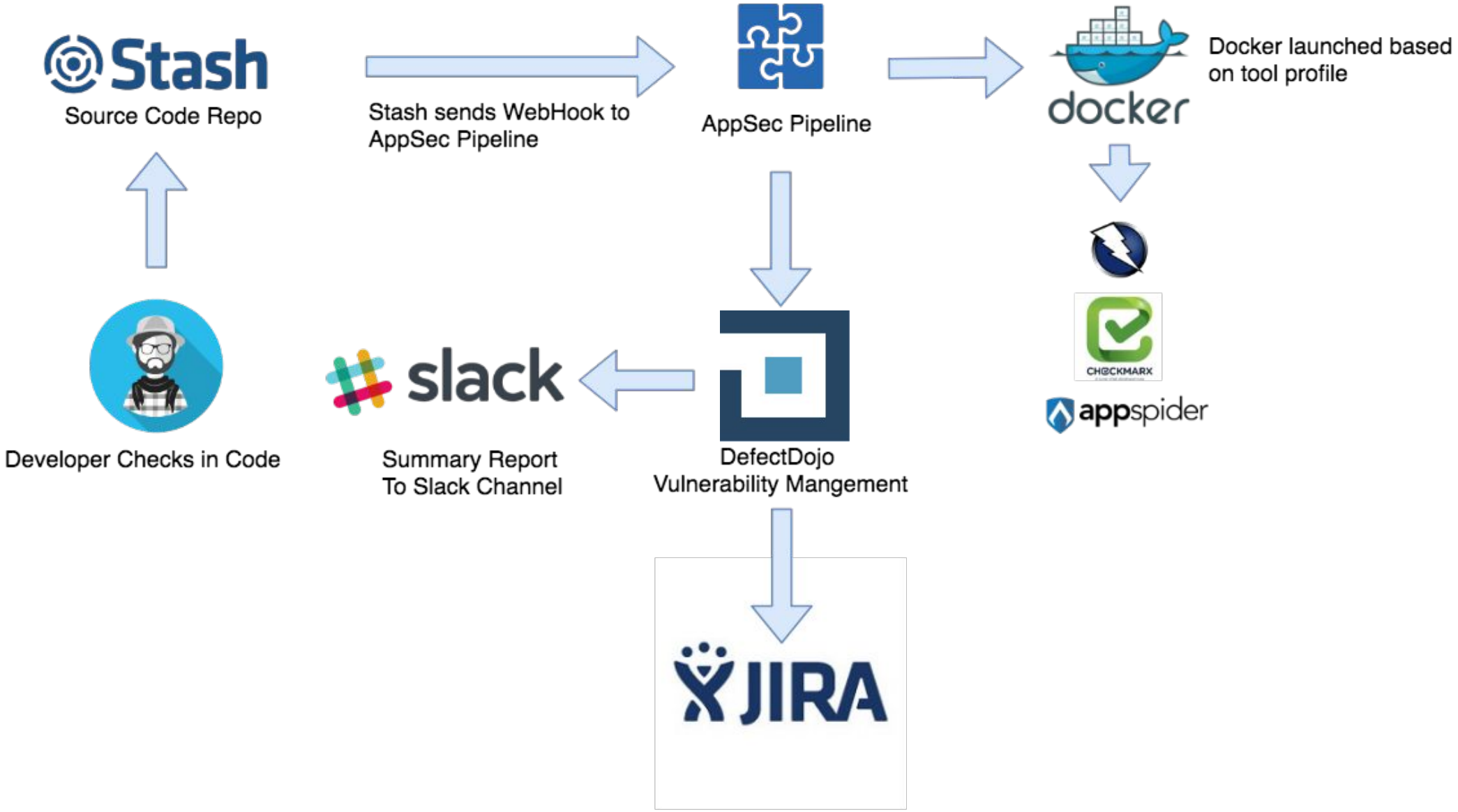
1) Pull Project Code

Project Repo

Tests run in Docker
containers

Test Web App
Projects

Zap Docker


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

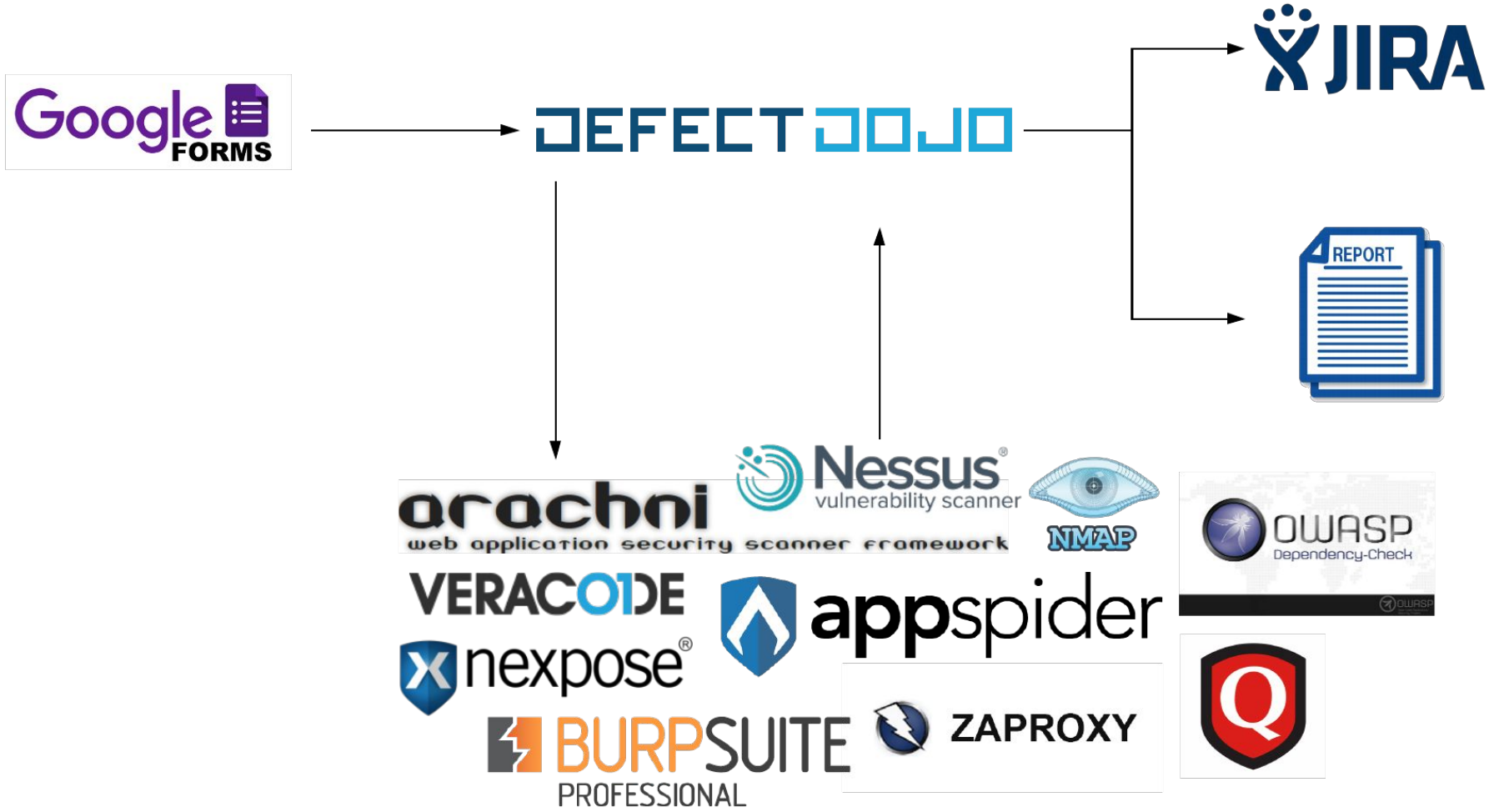
AppSec Pipeline Stats

15 Repos

5,100 Runs

4 Months

25,000+
Container Executions


Google FORMS
DEFECTDOJO
JIRA
REPORT
arachni
web application security scanner framework
Nessus
vulnerability scanner
NMAP
OWASP
Dependency-Check
VERACODE
appspider
nexpose
BURPSUITE
PROFESSIONAL
ZAPROXY

Automation Results

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

840.91%

Percentage Increase

From 2014 - 2016

References

- https://en.wikipedia.org/wiki/Running_with_Scissors_(company) (sign on title page)
- Kelsey Hightowers Serverless Talk at Gopher Con 2018 https://www.youtube.com/watch?v=U7glyWYj4qg
- Exploded view images: http://www.johngrimwade.com/blog/2017/08/21/taken-apart/
- L*g* blocks image (mildly edited by me): https://www.forbes.com/sites/scottlenet/2018/11/08/the-building-blocks-of-corporate-innovation%E2%80%8A/#476f45841697
- Chart of X-aaS approaches: https://dzone.com/articles/comparing-serverless-architecture-providers-aws-az
- Line of turtles image: https://www.trekearth.com/gallery/Asia/Japan/photo54378.htm
- Alfred images: https://en.wikipedia.org/wiki/Alfred_Pennyworth
- Serverless landscape image https://s.cncf.io