Securing DevOps

...

About Me

Matt Everson
Research Engineer

@matteverson
CISSP, OWASP Member

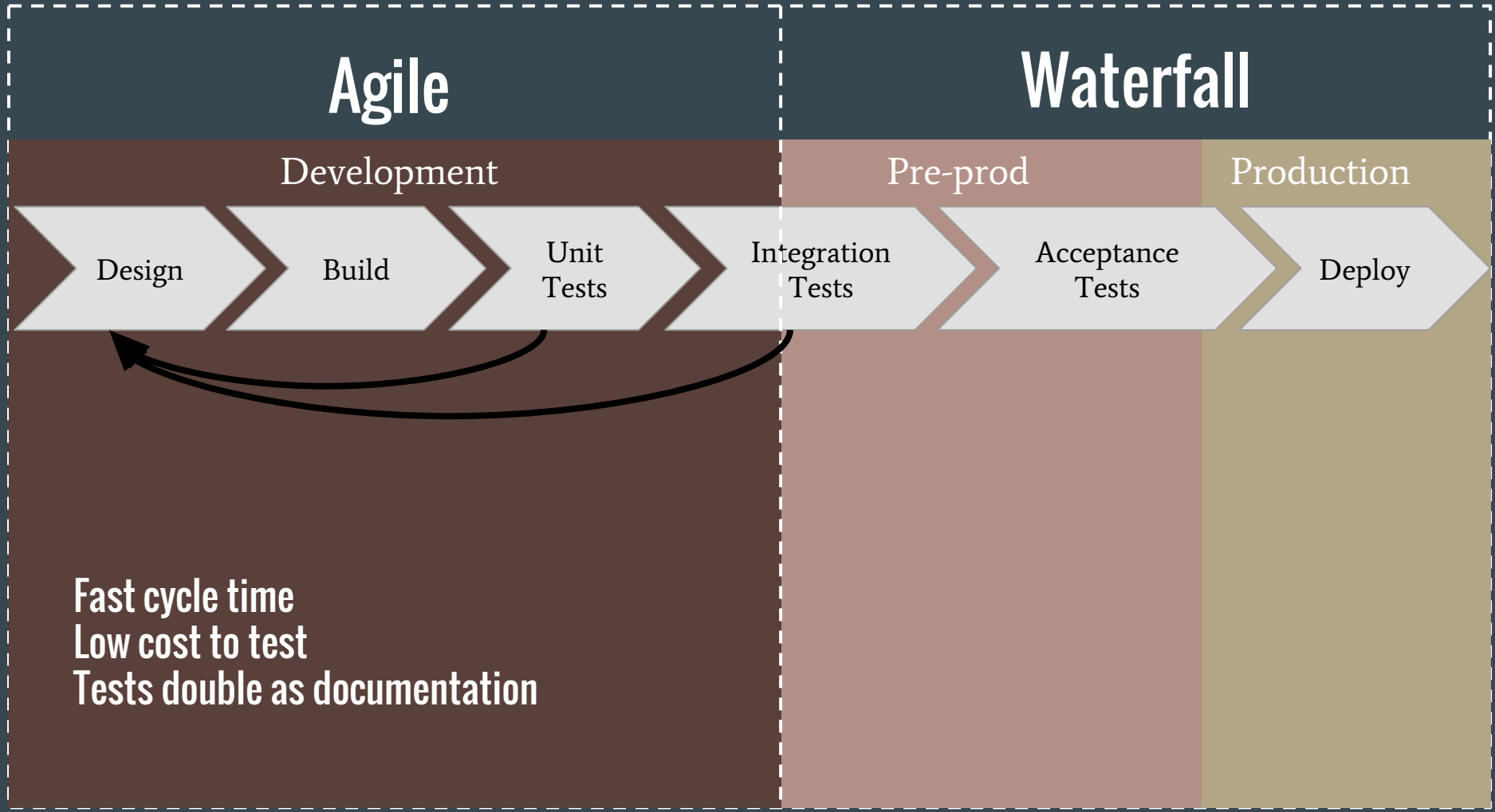
How many people here work in security?

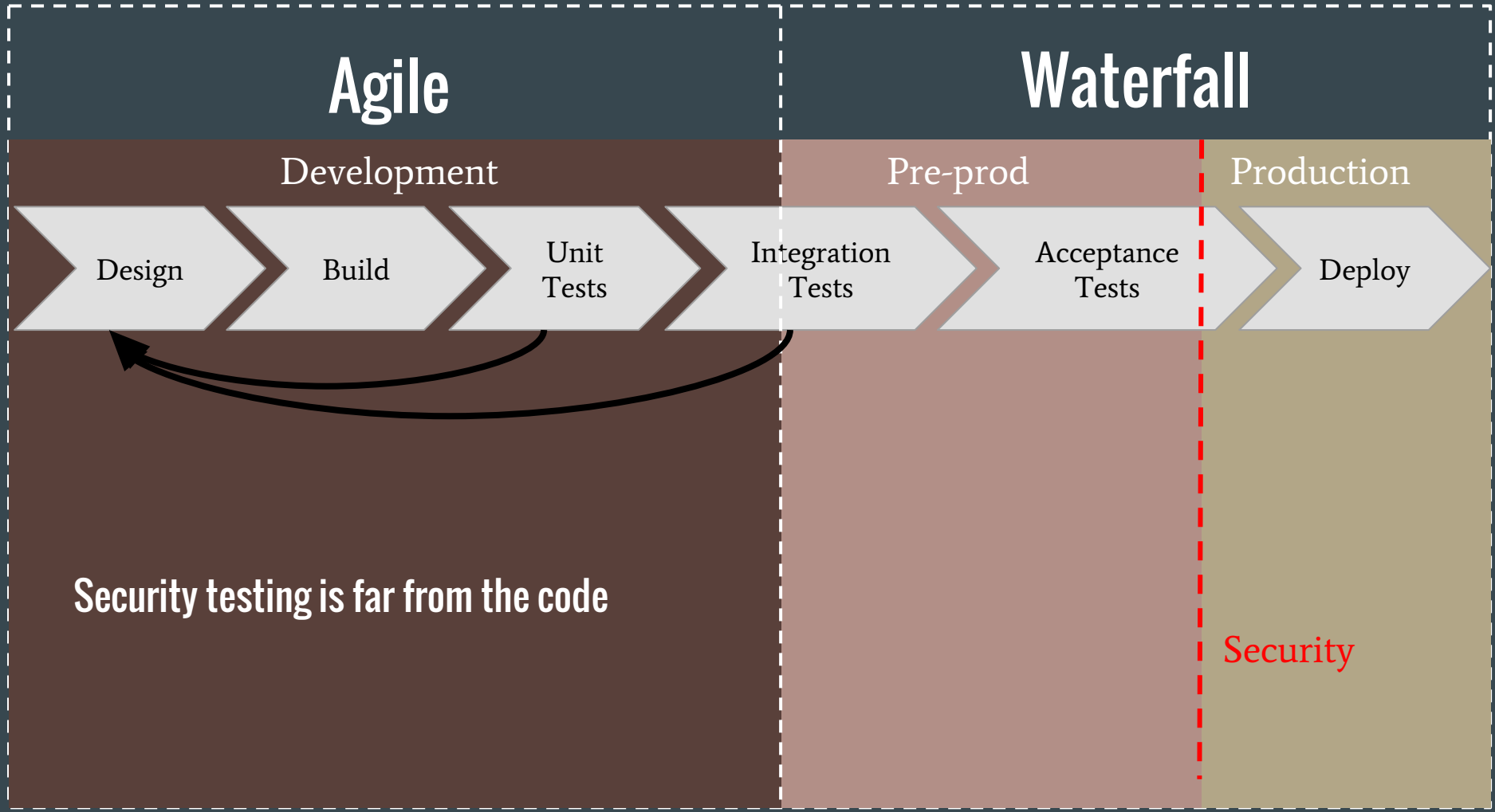
100%

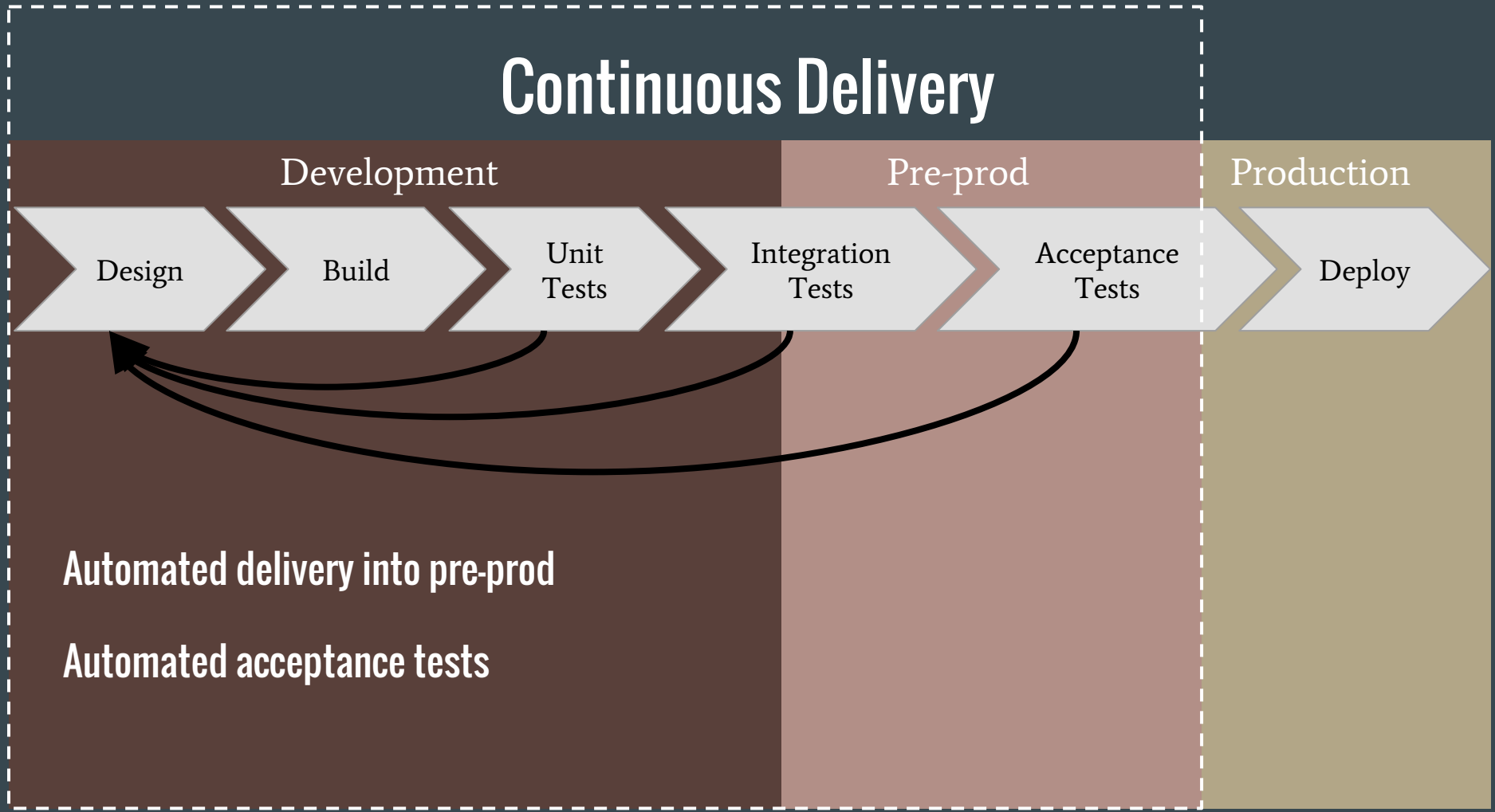
Everyone is responsible for security

How can we deliver value faster?

How can we deliver software faster?

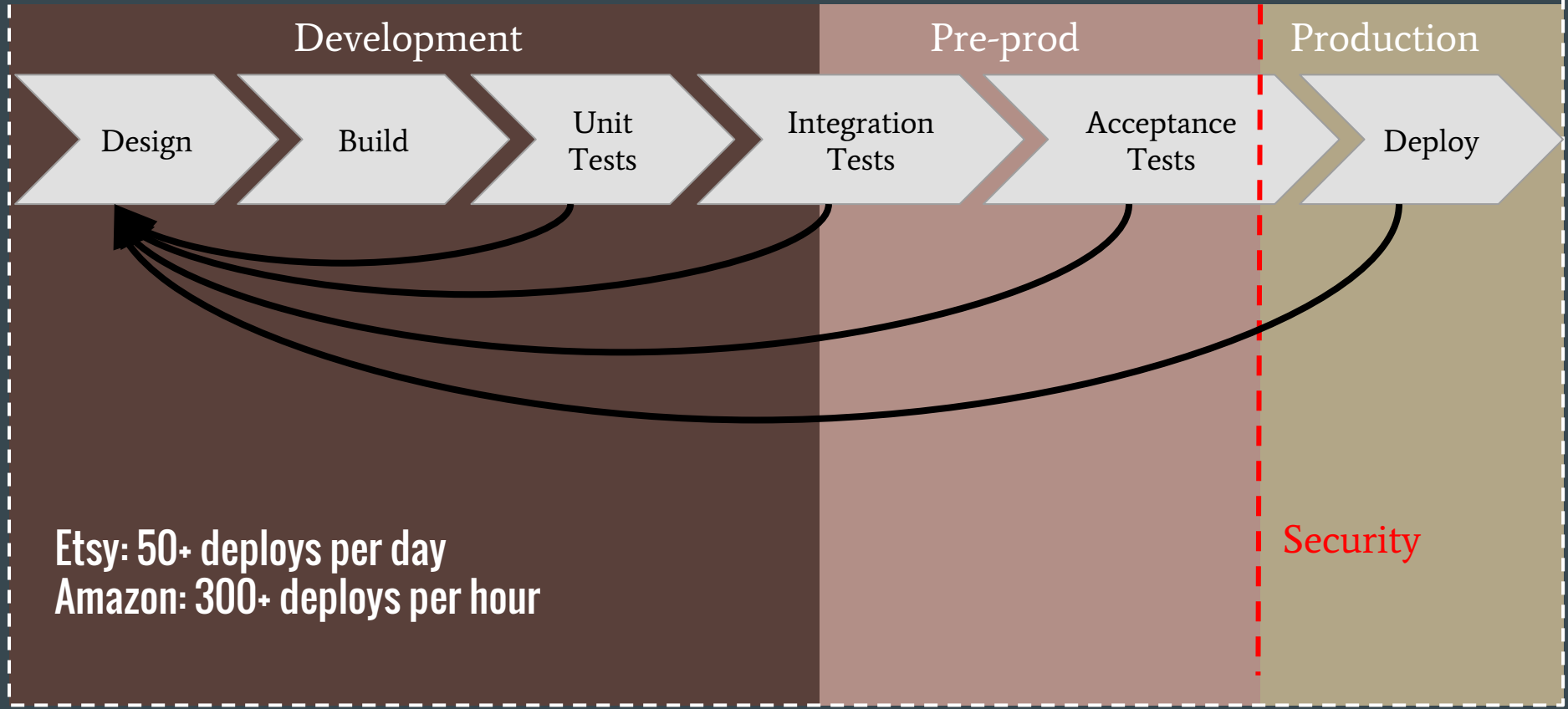

Agile
Waterfall
Development
Pre-prod
Production
Design
Build
Unit Tests
Integration Tests
Acceptance Tests
Deploy
Fast cycle time
Low cost to test
Tests double as documentation


Agile
Waterfall
Development
Pre-prod
Production
Design
Build
Unit Tests
Integration Tests
Acceptance Tests
Deploy
Security testing is far from the code
Security


Continuous Delivery
Development
Pre-prod
Production
Design
Build
Unit Tests
Integration Tests
Acceptance Tests
Deploy
Automated delivery into pre-prod
Automated acceptance tests

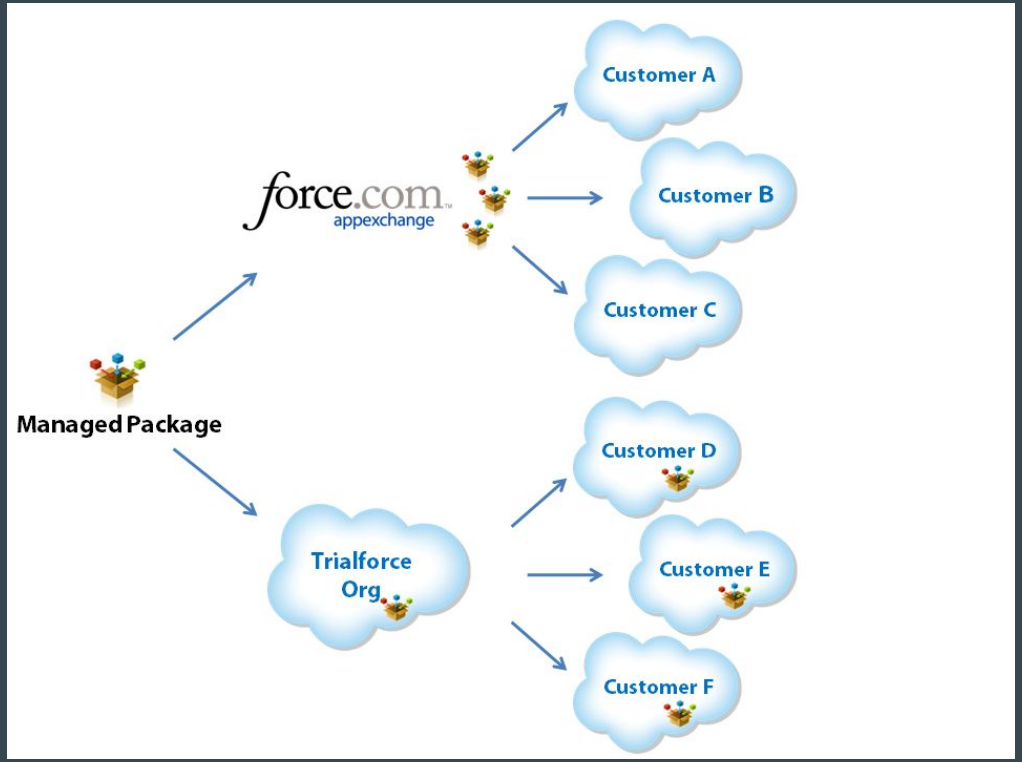
An example CI/CD workflow

Continuous Deployment



What can we do about security testing?

Salesforce Chimera



Security issues are quality issues

Everyone is responsible for quality

Move quality testing closer to the code

Continuous automated testing

Tests are visible to the team

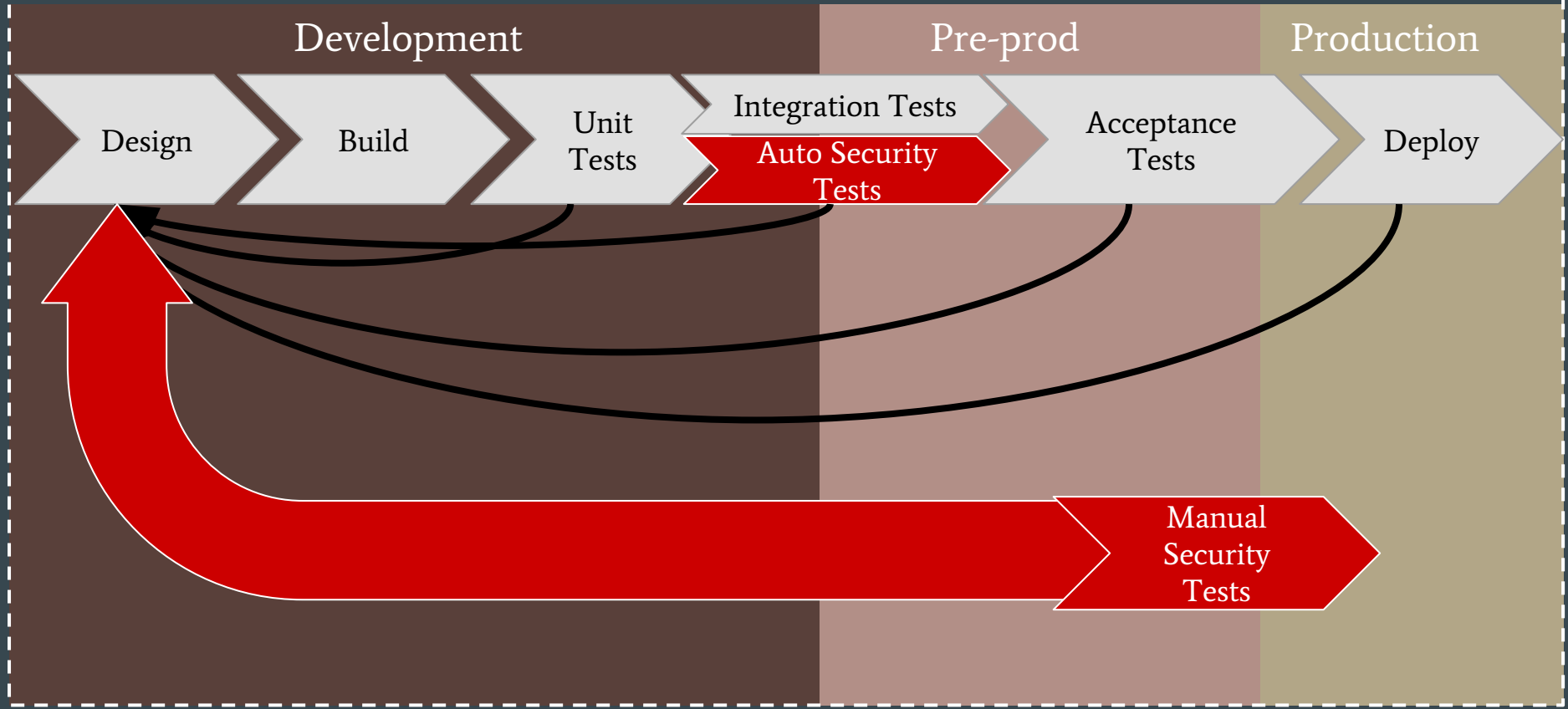
Everyone is responsible for security

Move security testing closer to the code

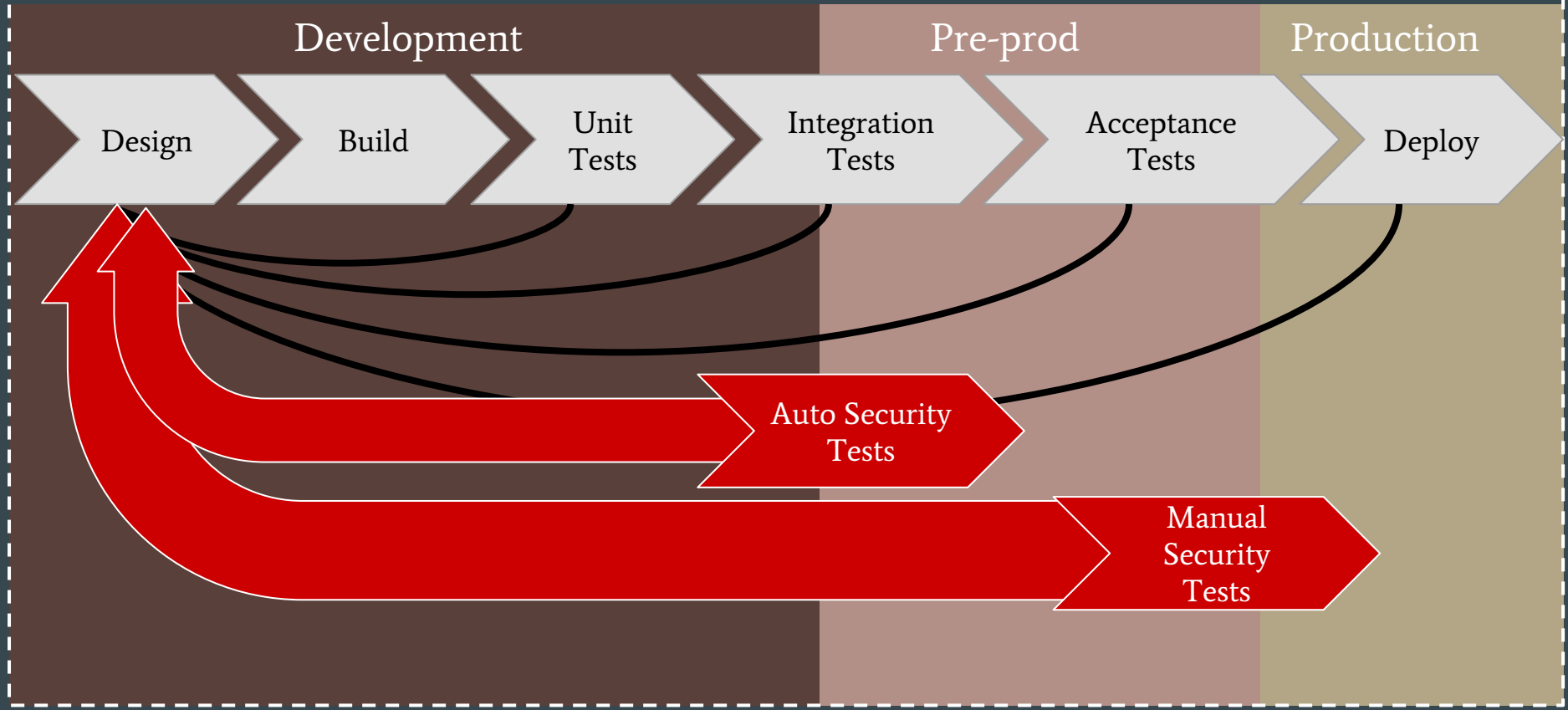
Continuous automated security testing

Security tests are visible to the team

Continuous Deployment with Blocking Tests



Continuous Deployment with Parallel Tests



Which do you prefer?

Problems?

Pitfalls

Results aren’t clear

Tests take too long

Parts of the application can’t be tested (signup, password reset)

Security team owns the tests

Automated security tests should...

return a pass or a fail

run quickly (about as long as acceptance tests)

exercise the high risk areas of the application

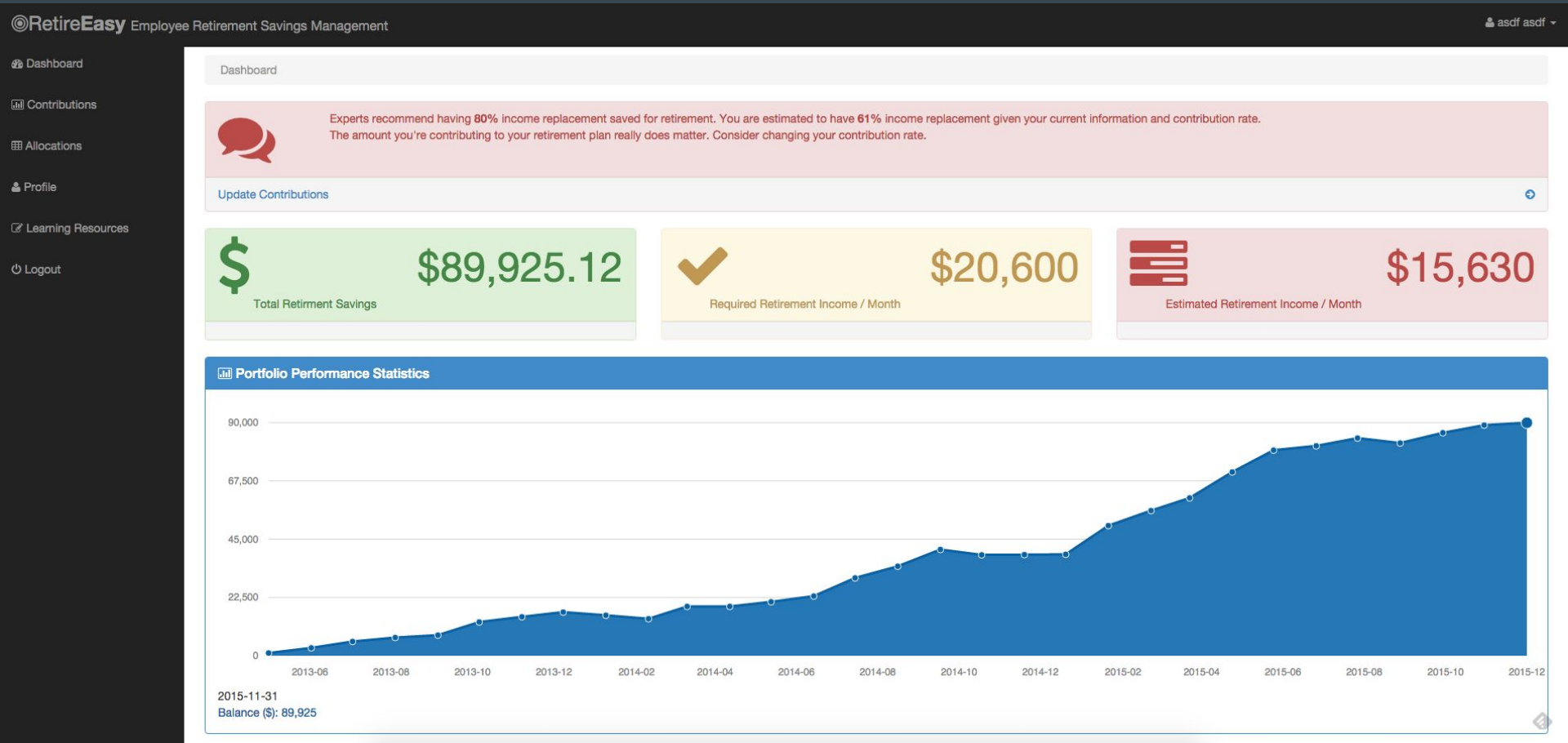
capture manual testing procedures and automate them (regression tests, yay)

be checked into source control next to the code

be understandable by the whole team

Where do we start?

NodeGoat - http://nodegoat.herokuapp.com



Travis CI

Let's add a scan using OWASP ZAP in our CI

Branch: **master** ▾ **NodeGoat** / **.travis.yml** | **Find file** | **Copy path**

matteverson Update .travis.yml — a60ba75 a day ago

1 contributor

15 lines (14 sloc) | 247 Bytes | **Raw** | **Blame** | **History**

```
1  language: node_js
2  node_js:
3    - '0.12'
4  services:
5    - mongodb
6    - docker
7  cache:
8    directories:
9      - node_modules
10 before_script:
11   - npm install -g grunt-cli
12   - grunt db-reset:development
13   - chmod +x .travis-script.sh
14 script: ./.travis-script.sh
```

Let's add a scan using OWASP ZAP in our CI

Branch: **master** ▾ **NodeGoat** / **.travis-script.sh** | **Find file** | **Copy path**

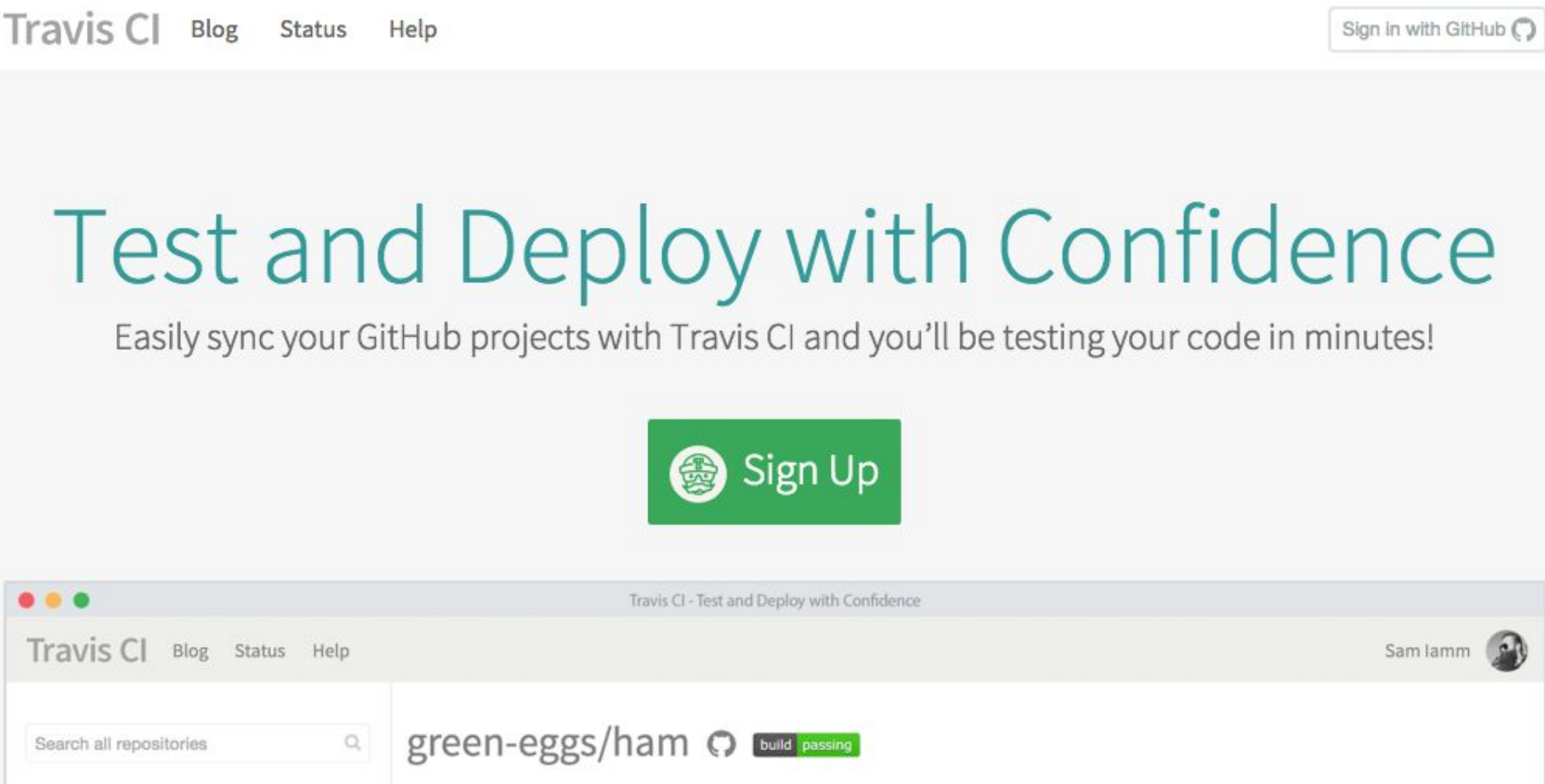
matteverson Update .travis-script.sh — 174302d just now

1 contributor

9 lines (8 sloc) | 353 Bytes — **Raw** | **Blame** | **History**

```
1  #!/bin/bash
2  npm start &
3  sleep 5
4  curl http://127.0.0.1:4000/login
5  hostip=$(docker run -u zap -it owasp/zap2docker-stable bash -c 'ip route show' | awk '/default/ {print$3}')
6  echo Scanning $hostip
7  docker run -u zap -i owasp/zap2docker-stable zap-cli --verbose quick-scan --self-contained \
8  -o "-config api.disablekey=true" --spider -r http://$hostip:4000
```

Travis CI - https://travis-ci.org



ME

Matt Everson
Repositories 23

Token:

Organizations

Tenable Network Security Inc.
Repositories 11

Is an organization missing?
Review and add your authorized organizations.

Matt Everson

Sync account

Flick the repository switch on

Add .travis.yml file to your repository

Trigger your first build with a git push

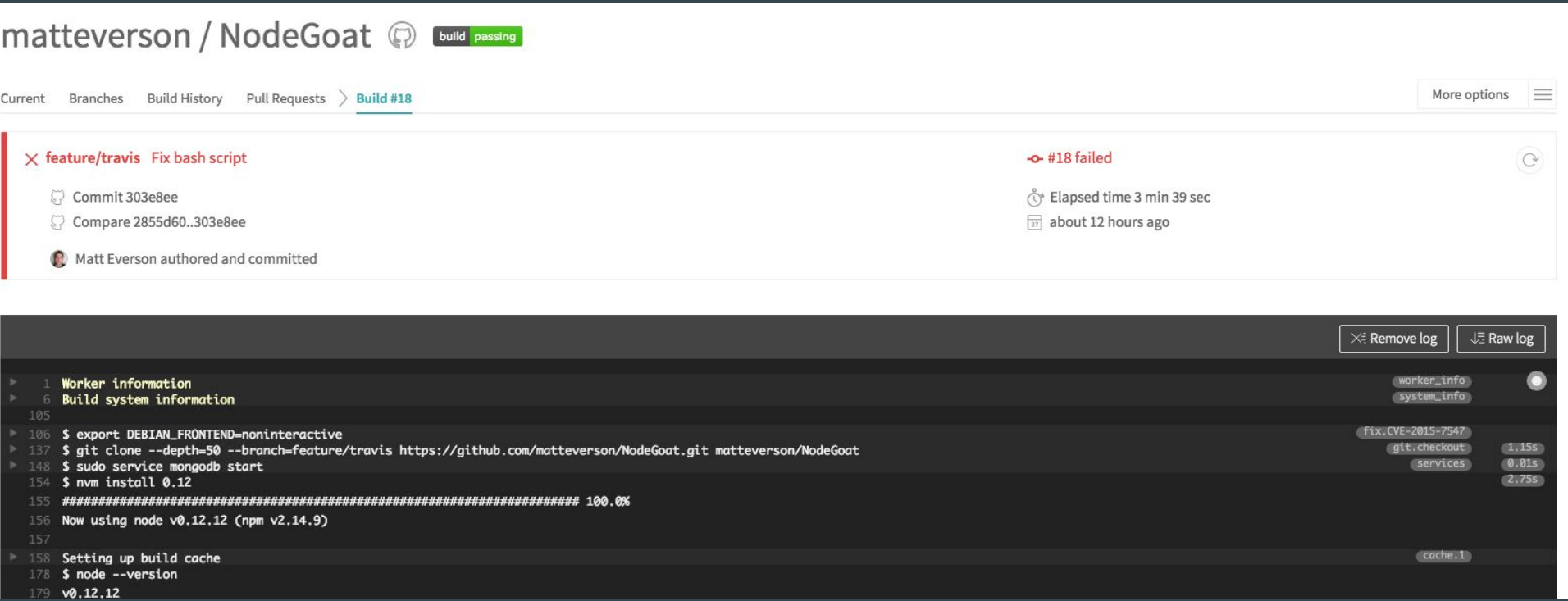
matteverson/angular-cart-demo

matteverson/appletonapi

matteverson/Balzac-for-Jekyll

matteverson/docker

The results

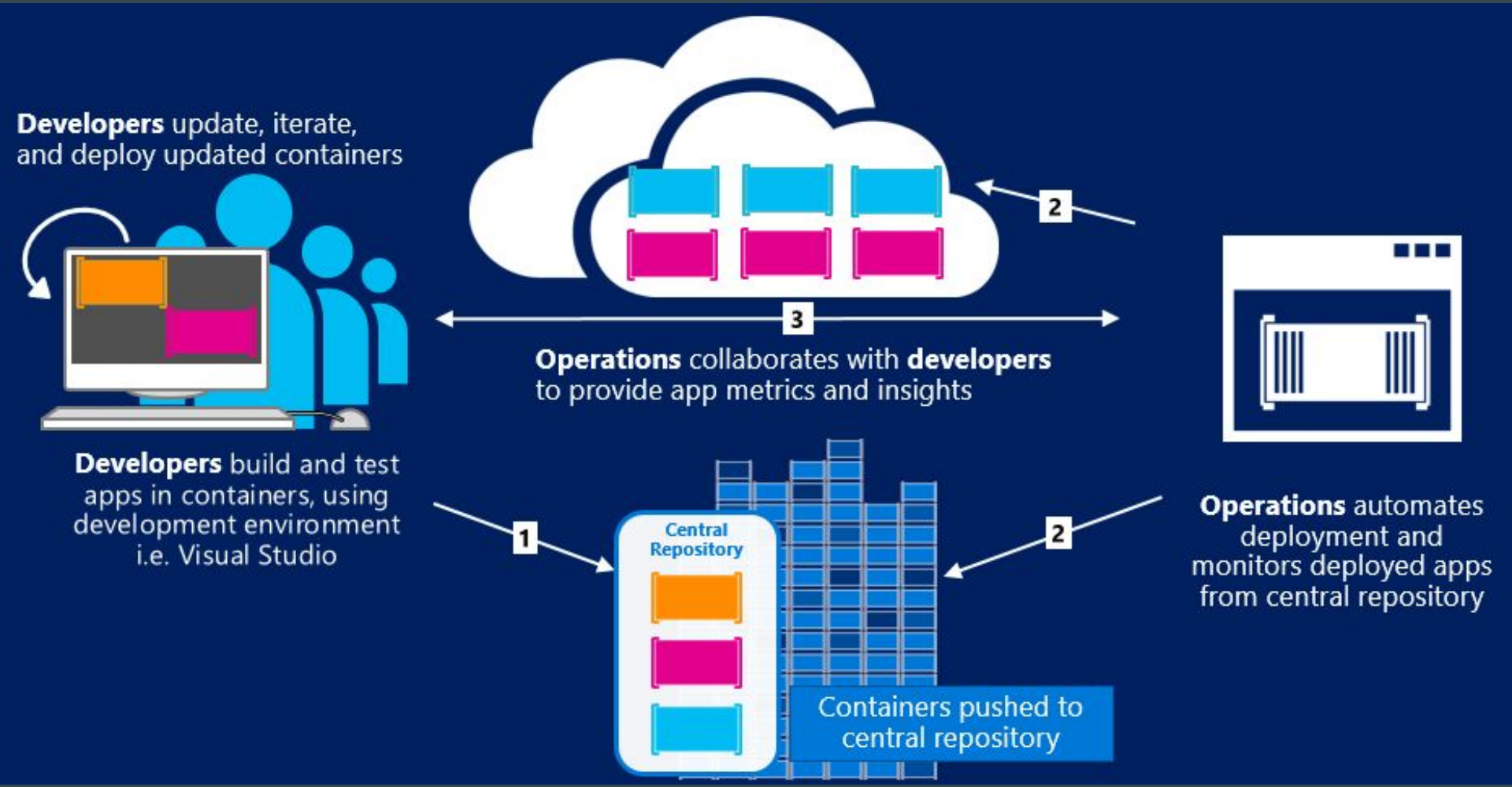

matteverson / NodeGoat
build passing
Current
Branches
Build History
Pull Requests
Build #18
More options
feature/travis Fix bash script
Commit 303e8ee
Compare 2855d60..303e8ee
Matt Everson authored and committed
#18 failed
Elapsed time 3 min 39 sec
about 12 hours ago
Remove log
Raw log
1 Worker information
6 Build system information
105
106 $ export DEBIAN_FRONTEND=noninteractive
137 $ git clone --depth=50 --branch=feature/travis https://github.com/matteverson/NodeGoat.git matteverson/NodeGoat
148 $ sudo service mongodb start
154 $ nvm install 0.12
155 ## 100.0%
156 Now using node v0.12.12 (npm v2.14.9)
157
158 Setting up build cache
178 $ node --version
179 v0.12.12
worker_info
system_info
fix.CVE-2015-7547
git.checkout
1.15s
services
0.01s
2.75s
cache.1

The results

```
1520 [DEBUG]           Scan progress %: 98
1521 [DEBUG]           Scan #0 completed
1522 [INFO]            Issues found: 3
1523 +---------------------------------+--------+----------+-------------------------------+
1524 | Alert                           | Risk   |   CWE ID | URL                           |
1525 +=================================+========+==========+===============================+
1526 | Cross Site Scripting (Reflected) | High   |       79 | http://172.17.42.1:4000/signup |
1527 +---------------------------------+--------+----------+-------------------------------+
1528 | Cross Site Scripting (Reflected) | High   |       79 | http://172.17.42.1:4000/login  |
1529 +---------------------------------+--------+----------+-------------------------------+
1530 | Cross Site Scripting (Reflected) | High   |       79 | http://172.17.42.1:4000/signup |
1531 +---------------------------------+--------+----------+-------------------------------+
1532 [INFO]            Shutting down ZAP daemon
1533 [DEBUG]           Shutting down ZAP.
1534 [DEBUG]           ZAP shutdown successfully.
1535
1536
1537 The command "./.travis-script.sh" exited with 3.
```

Use your e2e tests

Containers


Developers update, iterate, and deploy updated containers
2
3
Operations collaborates with developers to provide app metrics and insights
Developers build and test apps in containers, using development environment i.e. Visual Studio
1
Central Repository
2
Operations automates deployment and monitors deployed apps from central repository
Containers pushed to central repository

What if ZAP doesn’t do what I want?

GauntIt

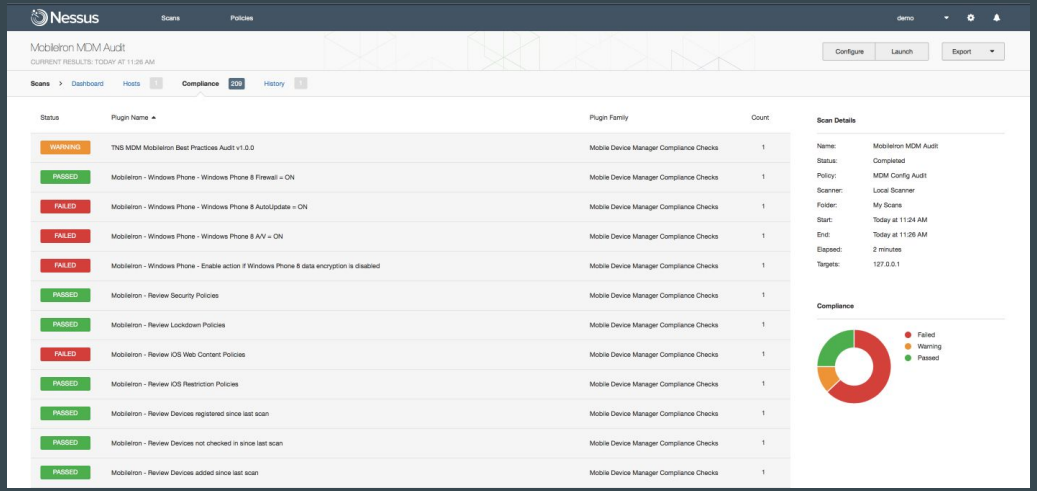
- nmap
- sslyze
- heartbleed
- sqlmap
- garmr
- generic command line

GauntIt

```
1  Feature: Run sslyze against a target
2
3  Background:
4    Given "sslyze" is installed
5    And the following profile:
6      | name     | value      |
7      | hostname | google.com |
8
9  Scenario: Ensure no anonymous certificates
10   When I launch an "sslyze" attack with:
11     """
12     python <sslyze_path> <hostname>:443
13     """
14   Then the output should not contain:
15     """
16     Anon
17     """
```

Nessus

- Nessrest - Python API client



Everyone is responsible for security

Move security testing closer to the code

Continuous automated security testing

Security tests are visible to the team

Questions