Move Fast, Be Safe

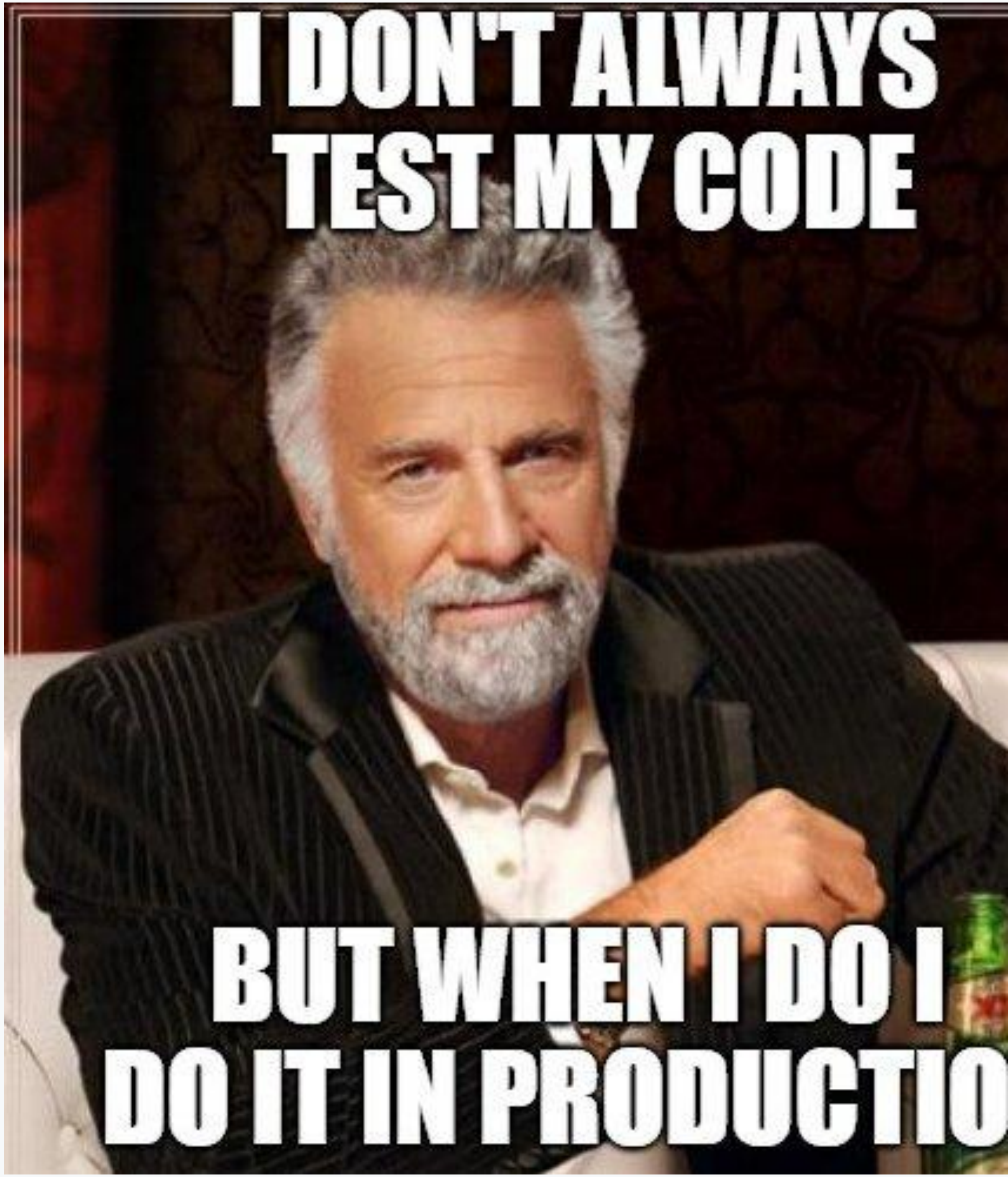
What if I told you you can write code fast without causing security vulnerabilities?

About Me

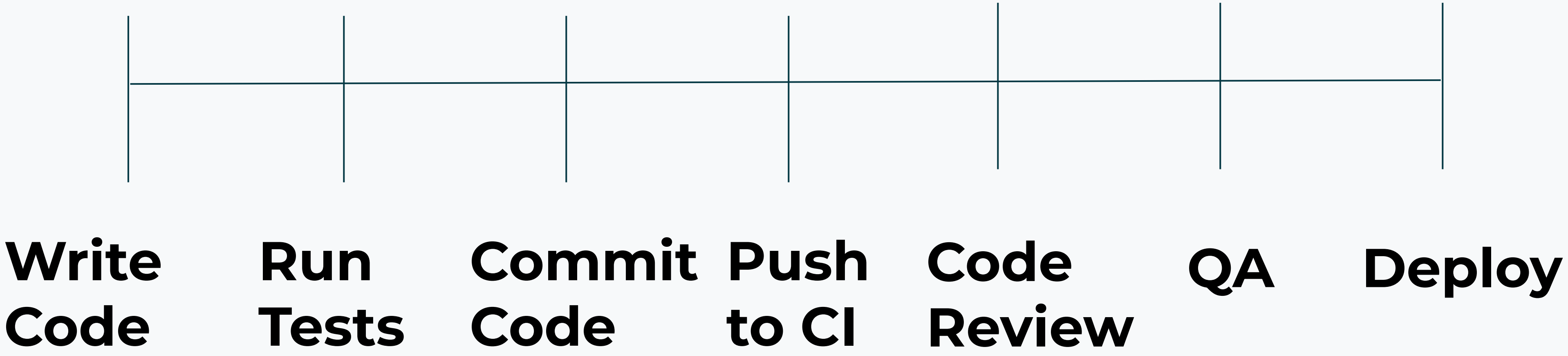
- My name is Esty Scheiner
- I’m from Boulder, Colorado
- Fun Fact: traveled/lived in 9 countries this year
- Security engineer @ Invoca
- Connect with me on Linkedin

Agenda

- ✓ SLDC
- ✓ Devops Culture
- ✓ Project {SSAAS}
- ✓ Q & A



Software development life cycle



Write Code

Run Tests

Commit Code

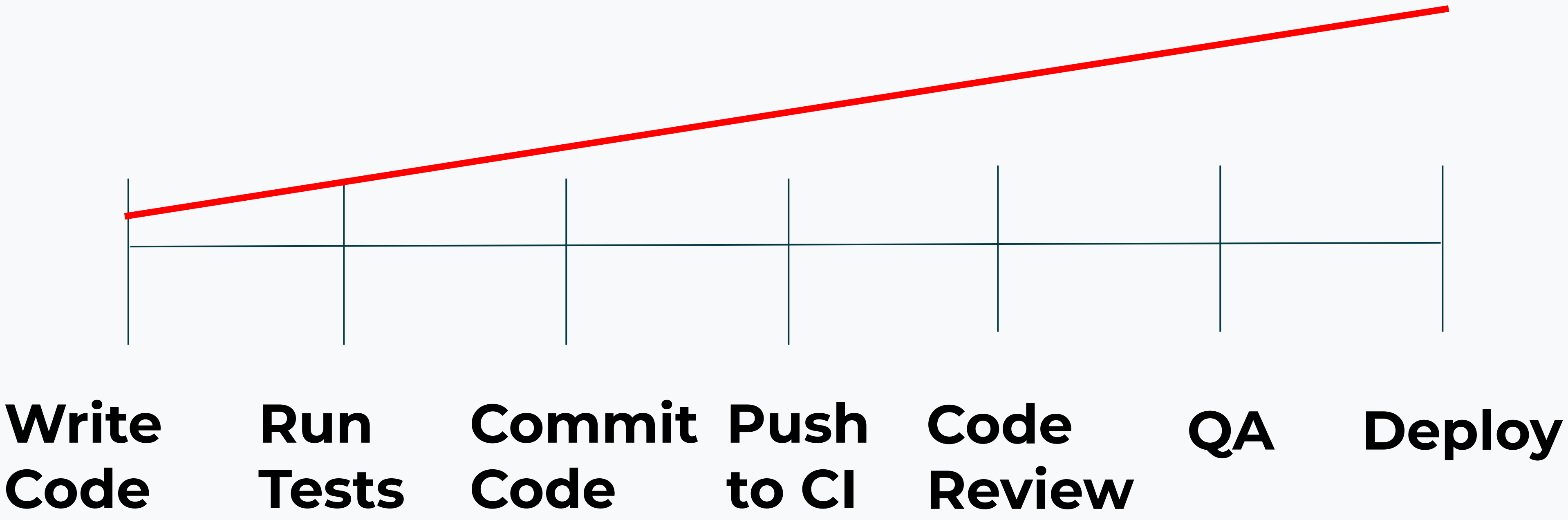
Push to CI

Code Review

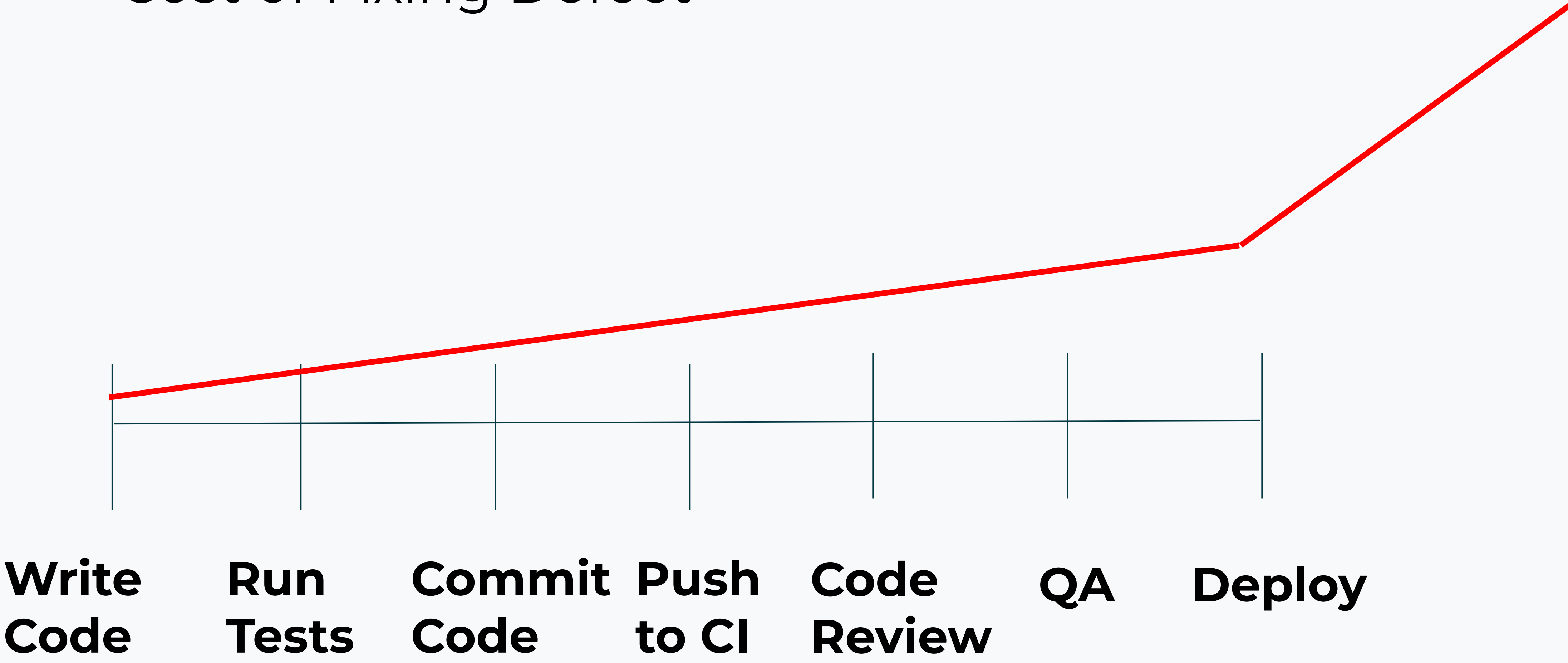
QA

Deploy

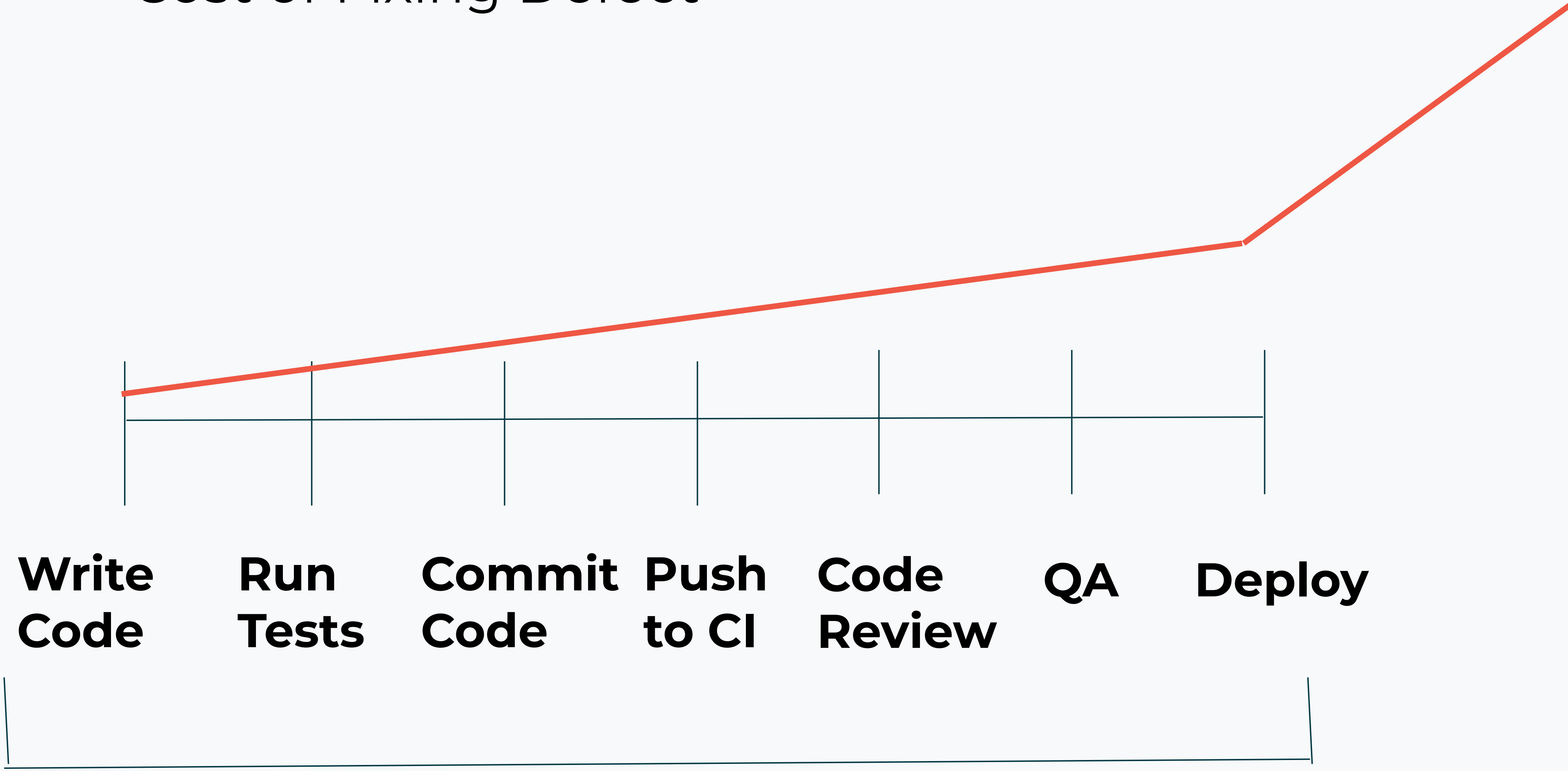
Cost of Fixing Defect



Cost of Fixing Defect



Cost of Fixing Defect



Let’s do security here!

How this played out for us.

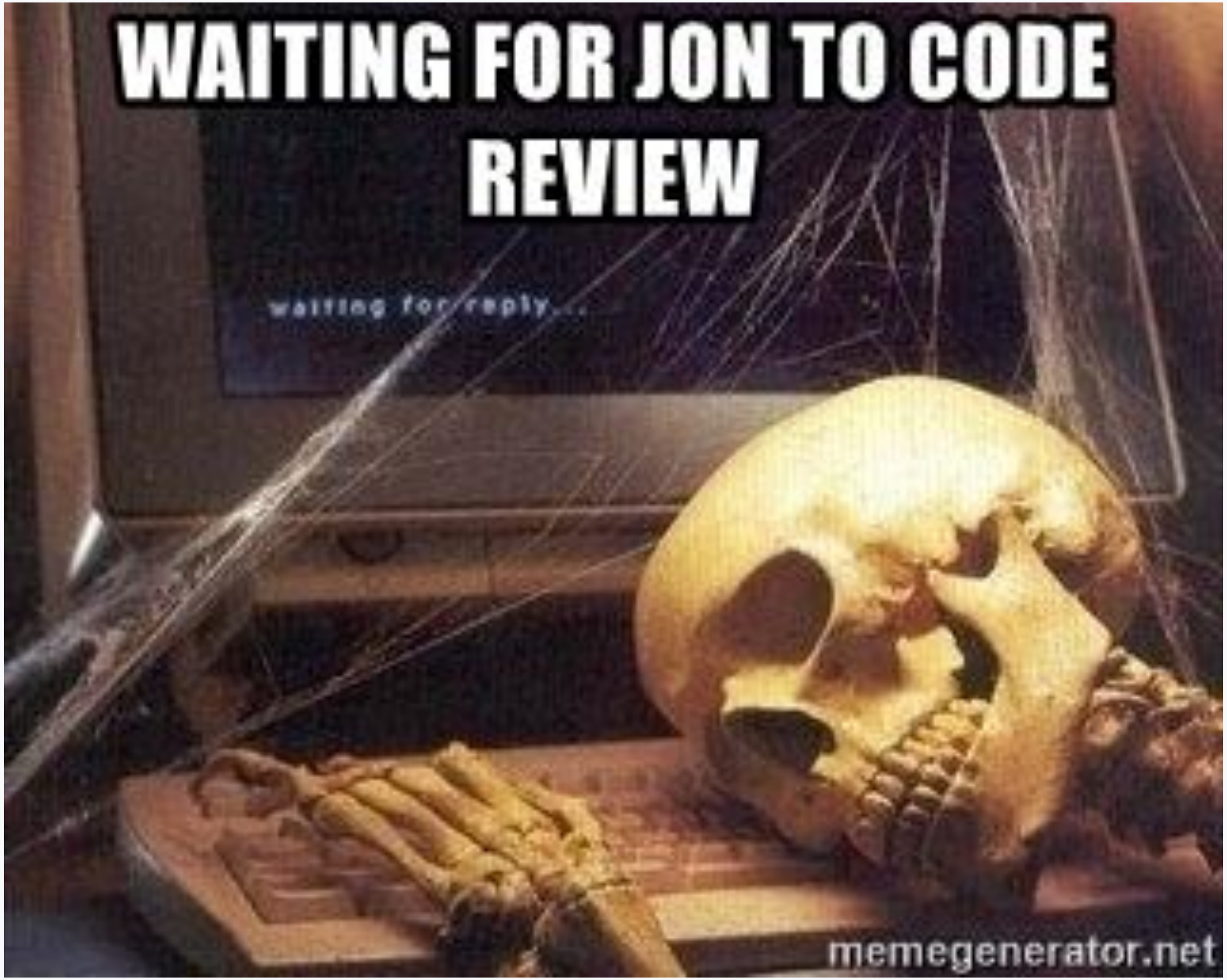
A Developer Story

As a developer I am creating a new service.

1. Write some code.. and some tests
2. Push code to CI
3. Open a PR against mainline branch
4. Peer reviews and approves PR
5. Merge code

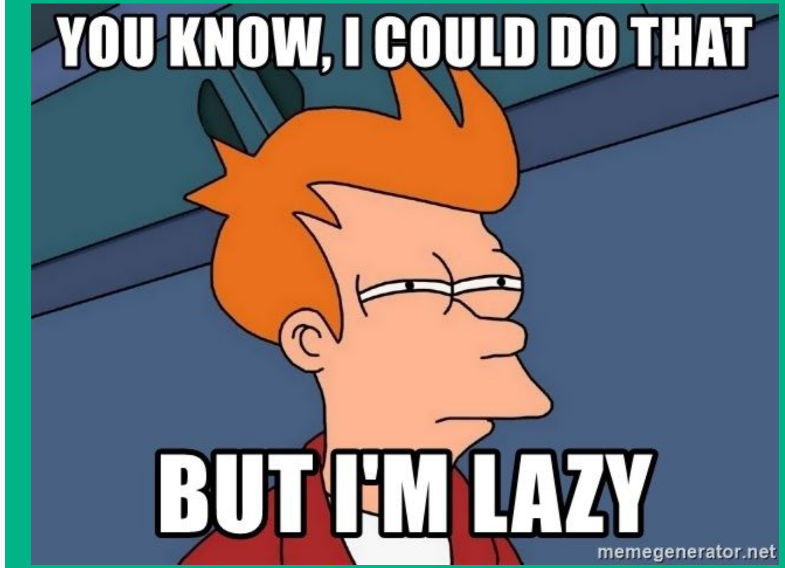
When critical vulnerabilities are identified by security team or when audit time rolls around....

6. Repeat steps 1-5 to resolve security defects


WAITING FOR JON TO CODE REVIEW
waiting for reply...
memegenerator.net

My Security Trajectory

- Passed CISSP
- Security engineering @ SecureSet (only female)
- Youngest engineer at Invoca
- Hacker enthusiast - just passed my OSCP(!! ?)
- My problem.. (I’m kinda lazy)



CISSP® Certified Information Systems Security Professional

Invoca Security Team Core Values

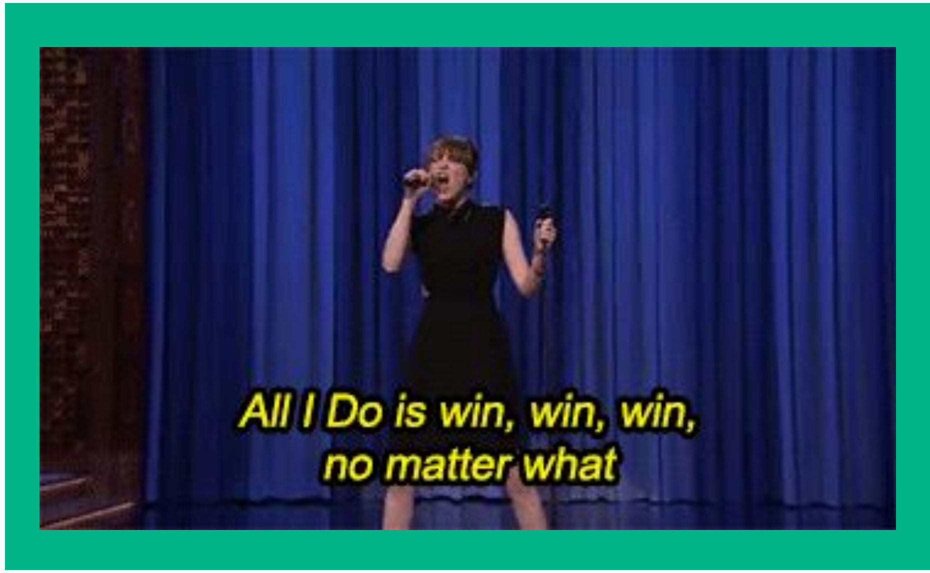
DevOps Culture

- Loosely Coupled
- Highly Cohesive
- Autonomy
- Faster Innovation

Why

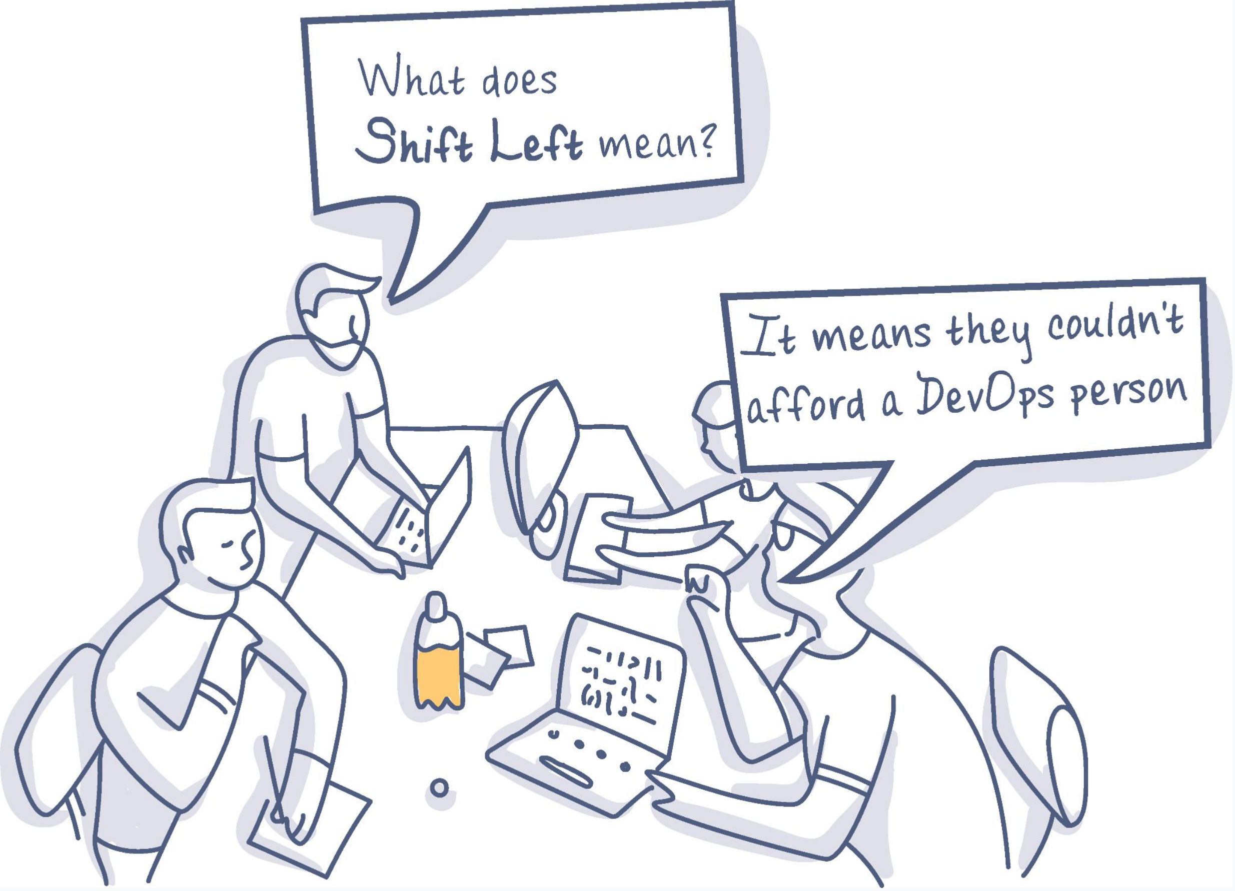
- Beat out the competition
  - Studies show that fast and nimble teams are more successful
    - https://puppet.com/blog/introducing-2018-state-devops-survey-new-research-focus

- Companies that are disrupting markets
  - Tesla broke into a very static market
  - Netflix overtook Disney in media market
  - Facebook crushed Myspace
  - Invoca dethroned Marchex



Shift Left

- Embed the knowledge with the people doing the work
- The people closest to the work have the context and knowledge to be autonomous to make the best decisions


What does Shift Left mean?
It means they couldn't afford a DevOps person

GuardRails

- ✓ Increase productivity
- ✓ Increase speed of production
- ✓ Increase autonomy

What if I told you you can write code fast without causing security vulnerabilities?

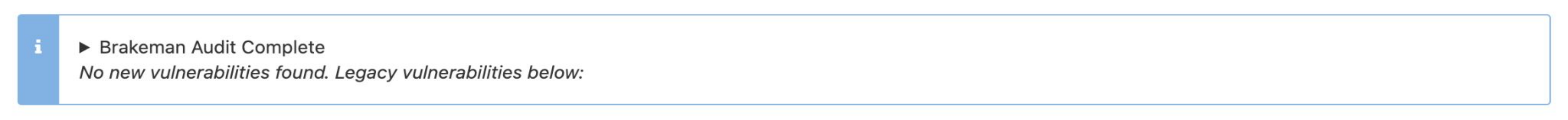
Automating Security Audits

Github action

Buildkite

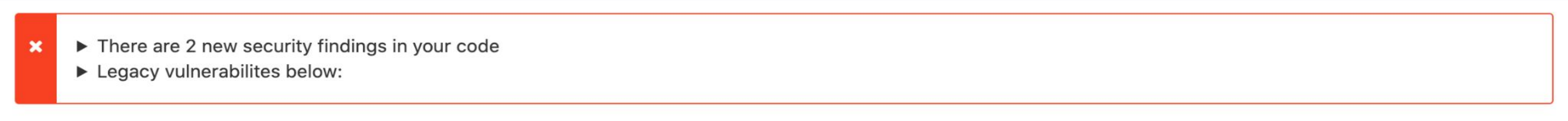
Brakeman

CVE Audit



▶ Brakeman Audit Complete

No new vulnerabilities found. Legacy vulnerabilities below:



▶ There are 2 new security findings in your code

▶ Legacy vulnerabilites below:

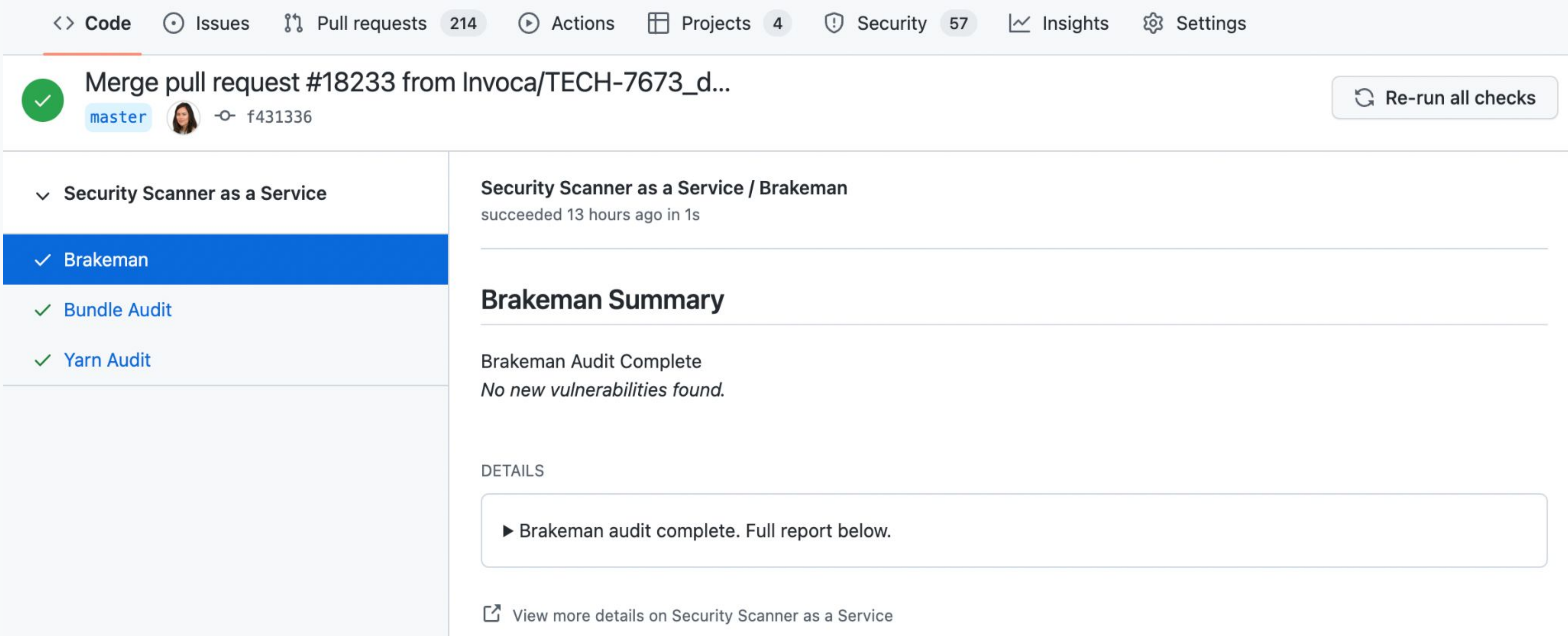
Resolving Legacy Vulnerabilities

- Legacy Vulnerabilities Comparison reduced noise
- Brakeman Open Source Contribution
- Service owning teams were responsible for investigating and resolving remaining vulnerabilities

Problem Statement:

How do we build **Security by default** into our services while keeping up with a fast pace of innovation?

Project {{SSAAS}}



Merge pull request #18233 from Invoca/TECH-7673_d...

master f431336

Security Scanner as a Service

- ✓ Brakeman
- ✓ Bundle Audit
- ✓ Yarn Audit

Security Scanner as a Service / Brakeman

succeeded 13 hours ago in 1s

Brakeman Summary

Brakeman Audit Complete

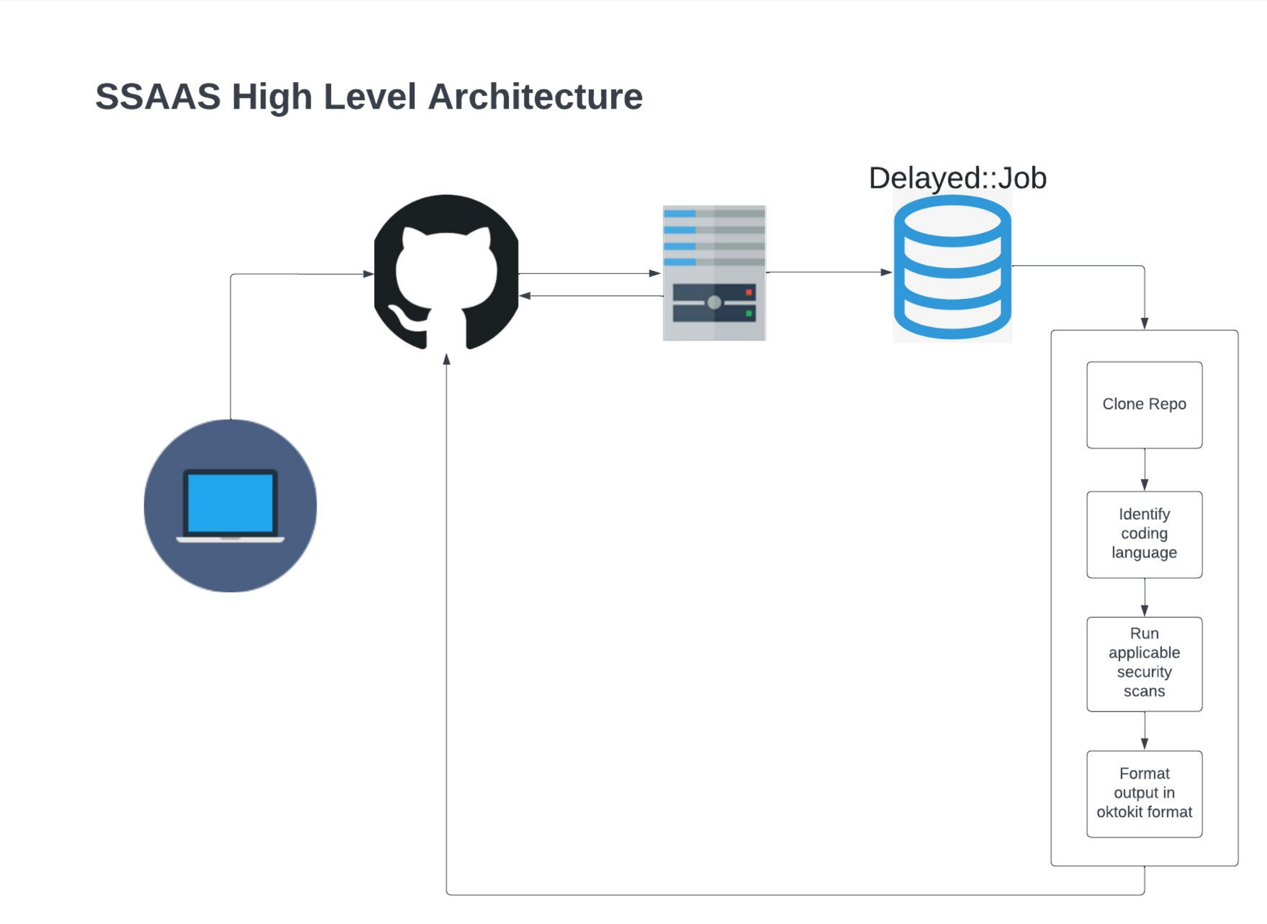
No new vulnerabilities found.

DETAILS

▶ Brakeman audit complete. Full report below.

View more details on Security Scanner as a Service

High Level Architecture



SSAAS High Level Architecture

Delayed::Job
Clone Repo
Identify coding language
Run applicable security scans
Format output in oktokit format

Techstack

Delayed::Job

A Developer Story

As a developer I am creating a new service.

1. Write some code.. and some tests
2. Push code to CI
3. Open a PR against mainline branch
4. Peer reviews and approves PR
5. Merge code

When critical vulnerabilities are identified by security team or when audit time rolls around....

6. Repeat steps 1-5 to resolve security defects

A Developer Story [NEW]

As a developer I am creating a new service.

1. Write some code.. and some tests
2. Push code to CI
3. SSAAS identifies the coding language and runs applicable security scans
4. Are there any vulnerabilities? If yes.. fix them now! (PR is blocked until security checks are green)
5. Open a PR against mainline branch
6. Peer reviews and approves PR

A Developer Story [NEW]

As a developer I am creating a new service.

1. Write some code.. and some tests
2. Push code to CI
3. SSAAS identifies the coding language and runs applicable security scans
4. Are there any vulnerabilities? If yes.. fix them now! (PR is blocked until security checks are green.
5. Open a PR against mainline branch
6. Peer reviews and approves PR

Merge It!!

Results

- Security team is not a blocker
- Tighter feedback loops
- Barely any findings from external pentesting
- Automated part of my job away :)

What’s to come?

- Support for more coding languages
- Continuous Monitoring
- Upgrading the project from MVP/POC to Production ready service
- Making SSAAS open source
- Dynamic security suggestions in the souce code editor

Q & A

Thank You