CONTRAST SECURITY

JUMPSTART DEVSECOPS WITH CONTRAST CE – HANDS ON

Robert Statsinger

Senior Solution Architect

Robert.Statsinger@ContrastSecurity.com

October 17, 2019

GOT DOCKER?

HANDS ON:

JUMPSTART DEVSECOPS FOR FREE USING CONTRAST COMMUNITY EDITION

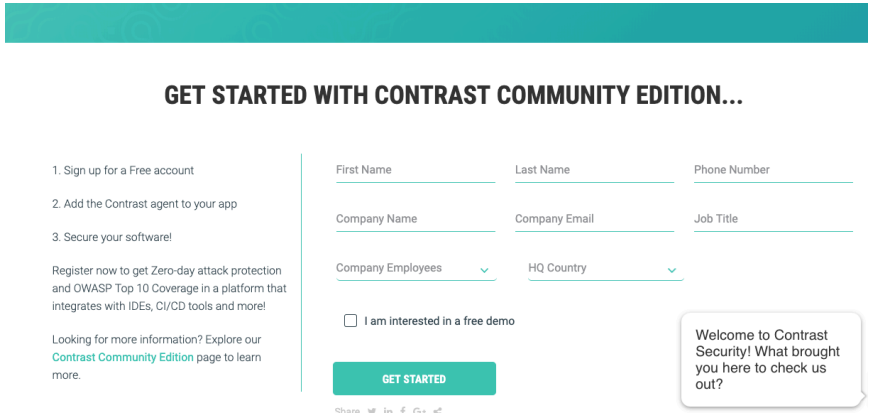
CLONE THIS REPO (OR JUST GRAB ALL THE FILES)

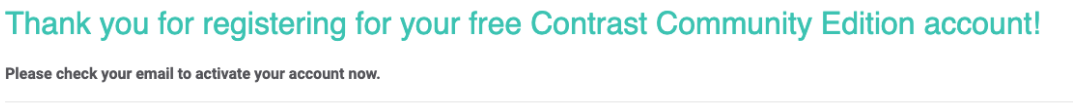
https://github.com/rstatsinger/iastraspworkshop

- Create a working directory
- Stash everything there
- Make a backup copy of the Dockerfile

SIGN UP FOR A CONTRAST COMMUNITY EDITION ACCOUNT

Sign up at https://www.contrastsecurity.com/contrast-community-edition



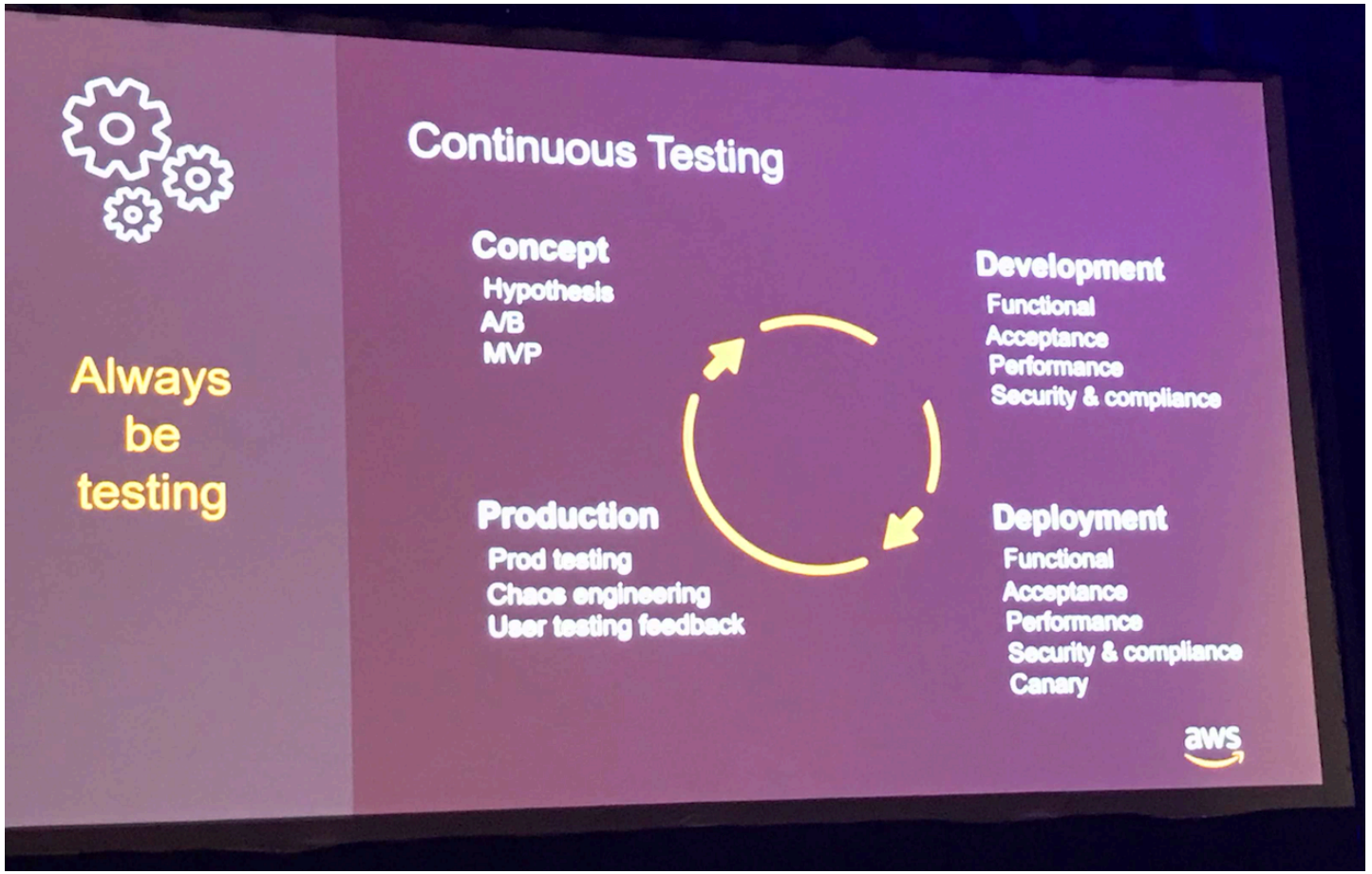


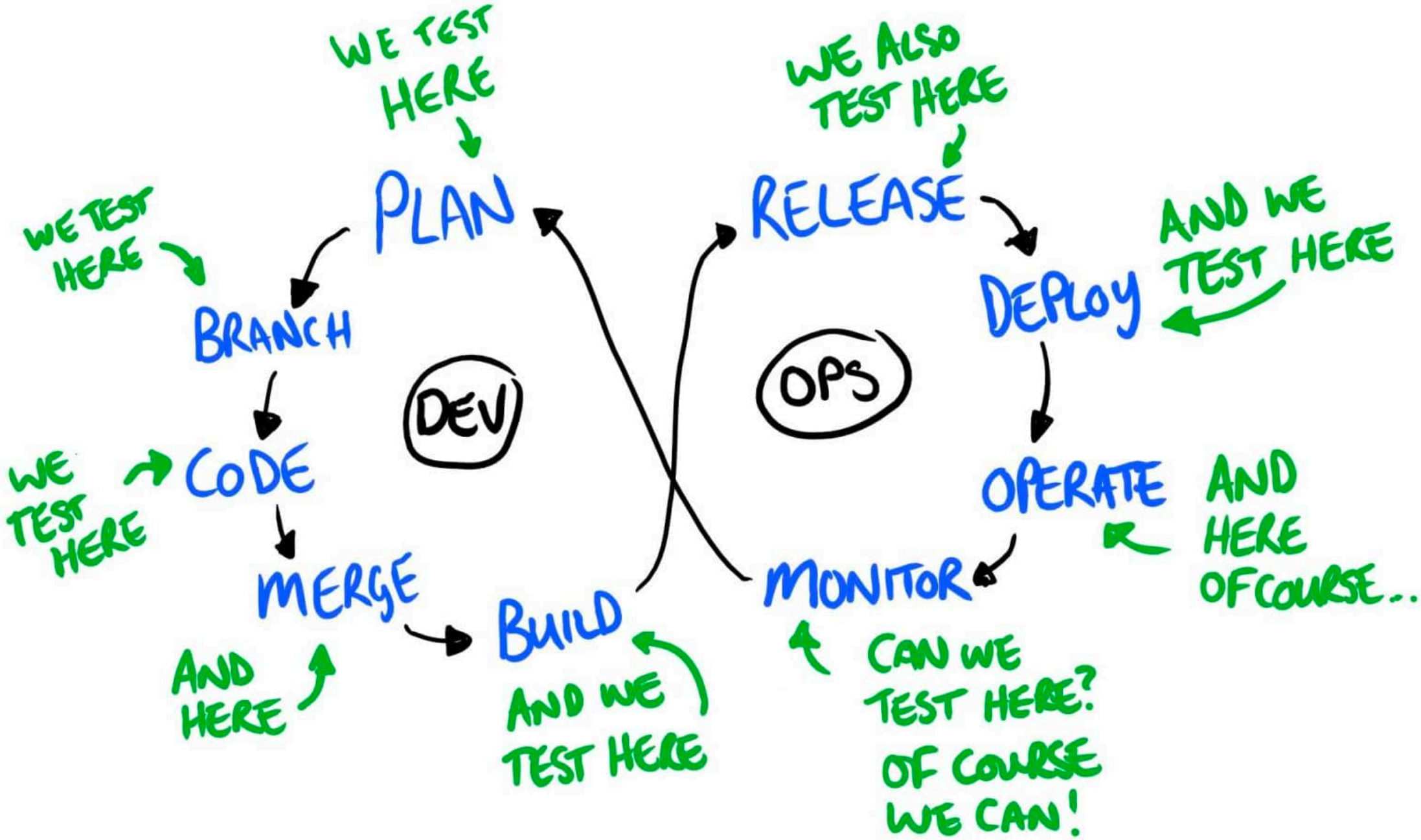
Check your email for confirmation

CONTRAST SECURITY

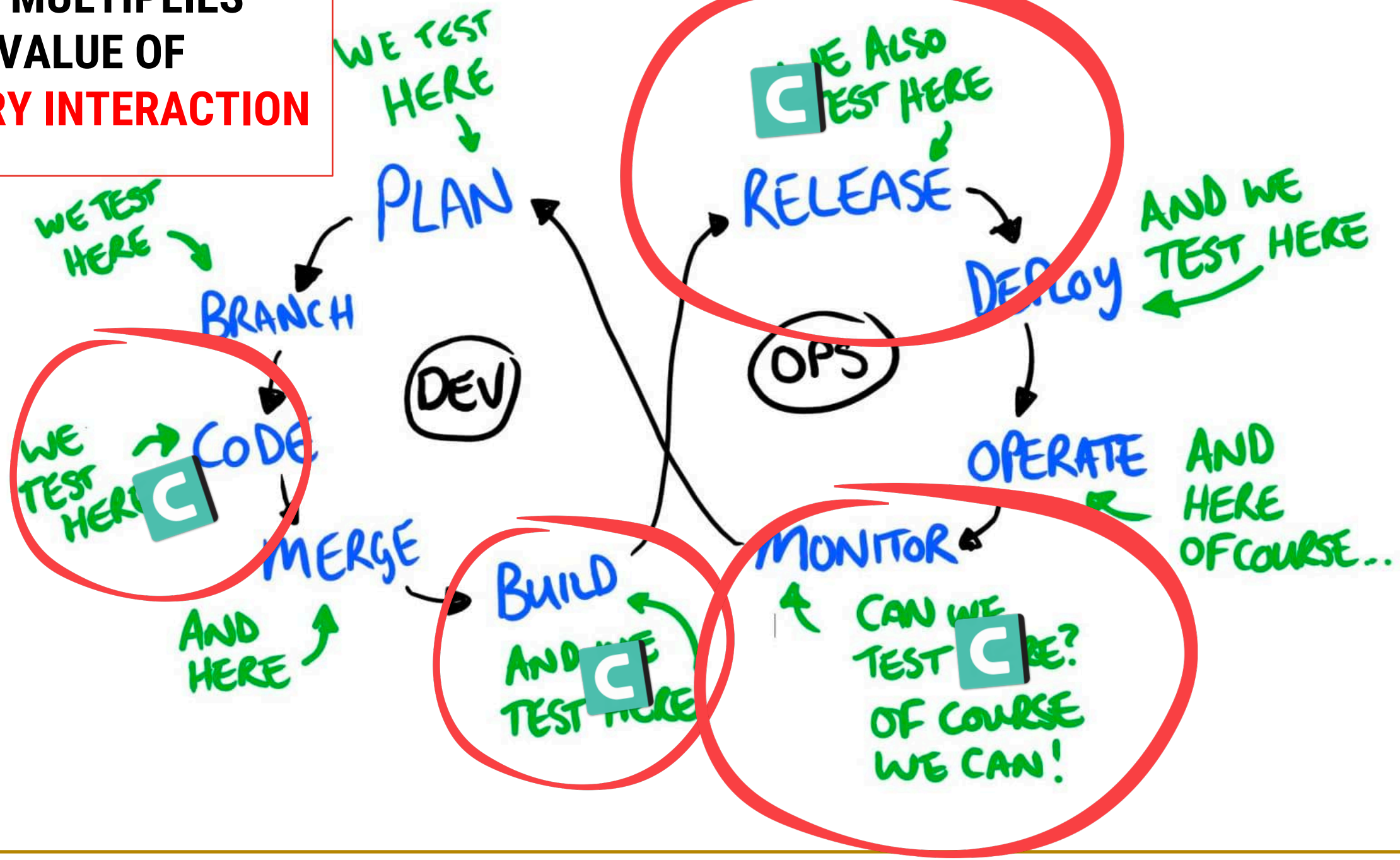
A BRIEF SOAPBOX…

CT (Continuous Testing)



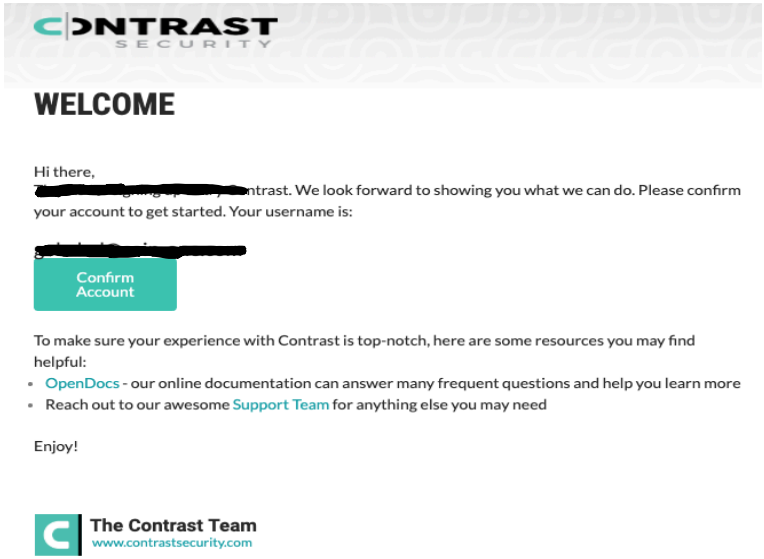

WE TEST HERE
PLAN
WE TEST HERE
BRANCH
DEV
WE TEST HERE
CODE
MERGE
AND HERE
BUILD
AND WE TEST HERE
WE ALSO TEST HERE
RELEASE
DEPLOY
AND WE TEST HERE
OPS
OPERATE
AND HERE OF COURSE..
MONITOR
CAN WE TEST HERE? OF COURSE WE CAN!

IAST MULTIPLIES THE VALUE OF EVERY INTERACTION



CONFIRM YOUR ACCOUNT….

Confirm your new account from registration email:



CONTRAST SECURITY

WELCOME

Hi there,
[redacted]ntrast. We look forward to showing you what we can do. Please confirm your account to get started. Your username is:

[redacted]

Confirm Account

To make sure your experience with Contrast is top-notch, here are some resources you may find helpful:

- OpenDocs - our online documentation can answer many frequent questions and help you learn more
- Reach out to our awesome Support Team for anything else you may need

Enjoy!

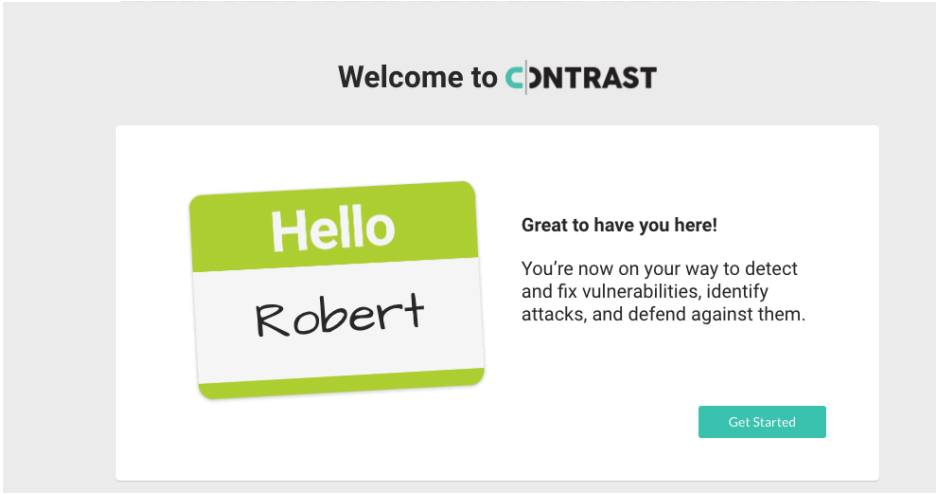
The Contrast Team
www.contrastsecurity.com

Click Confirm Account to set your password

CONTRAST SECURITY

GET STARTED…

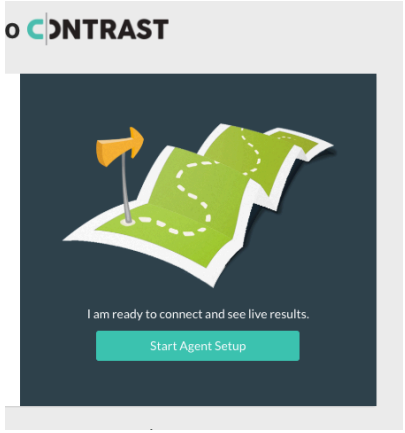
Click Get Started



The Contrast Team
www.contrastsecurity.com

Agree to the Ts & Cs

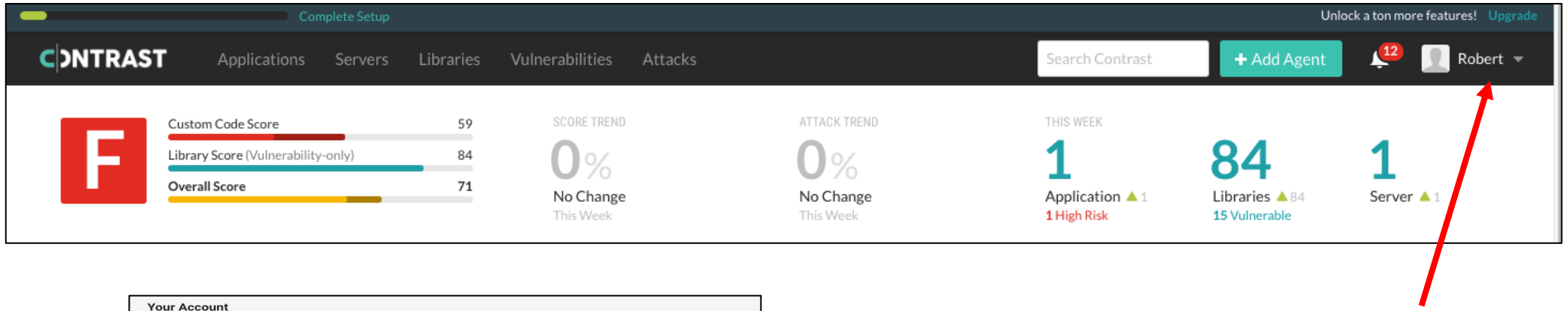
Click Start Agent Setup

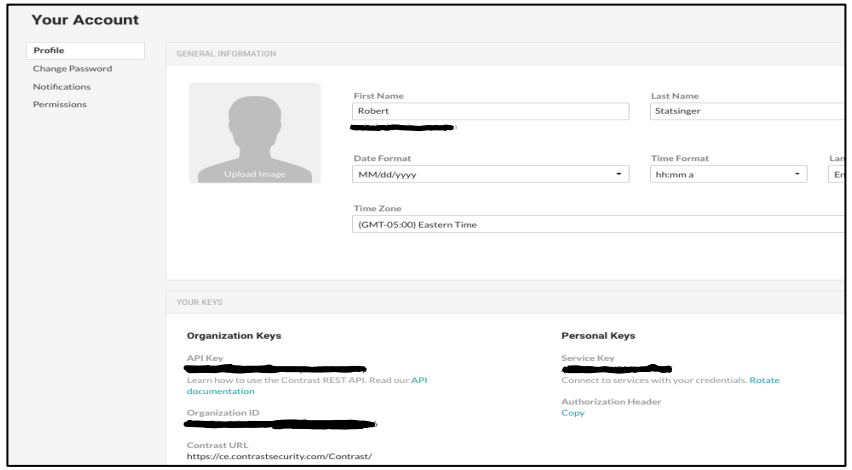


CONTRAST SECURITY

GET READY…

- Click the x at the top right so that you see the main dashboard
- Click the dropdown next to your name and go to the Your Account page:





CONTRAST SECURITY

GET SET…

- Plug the Organization ID, Authorization Token, and API Key from the Your Account page into the Dockerfile
  - Note: this is not best practice but we want to be expedient
- Doublecheck for correctness

```
# Dockerfile to run WebGoat 7.1 with Contrast Security Community Edition

FROM anapsix/alpine-java:jdk8

# TODO Edit the following three lines and substitute the keys from your Contrast Security CE Your Account page

ENV OrgID=<Replace with your Organization ID>

ENV Auth=<Replace with your Authorization Header>

ENV APIKey=<Replace with your API Key>
```

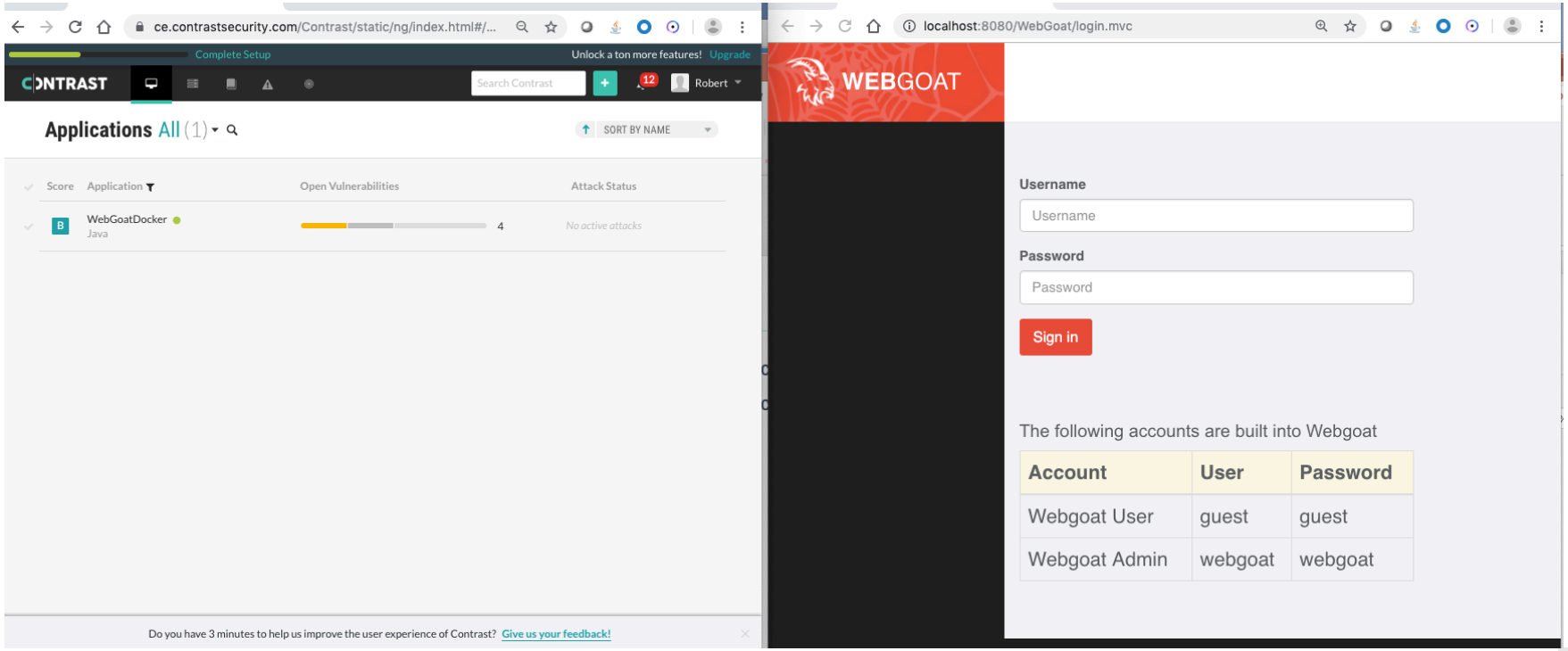
docker

CONTRAST SECURITY

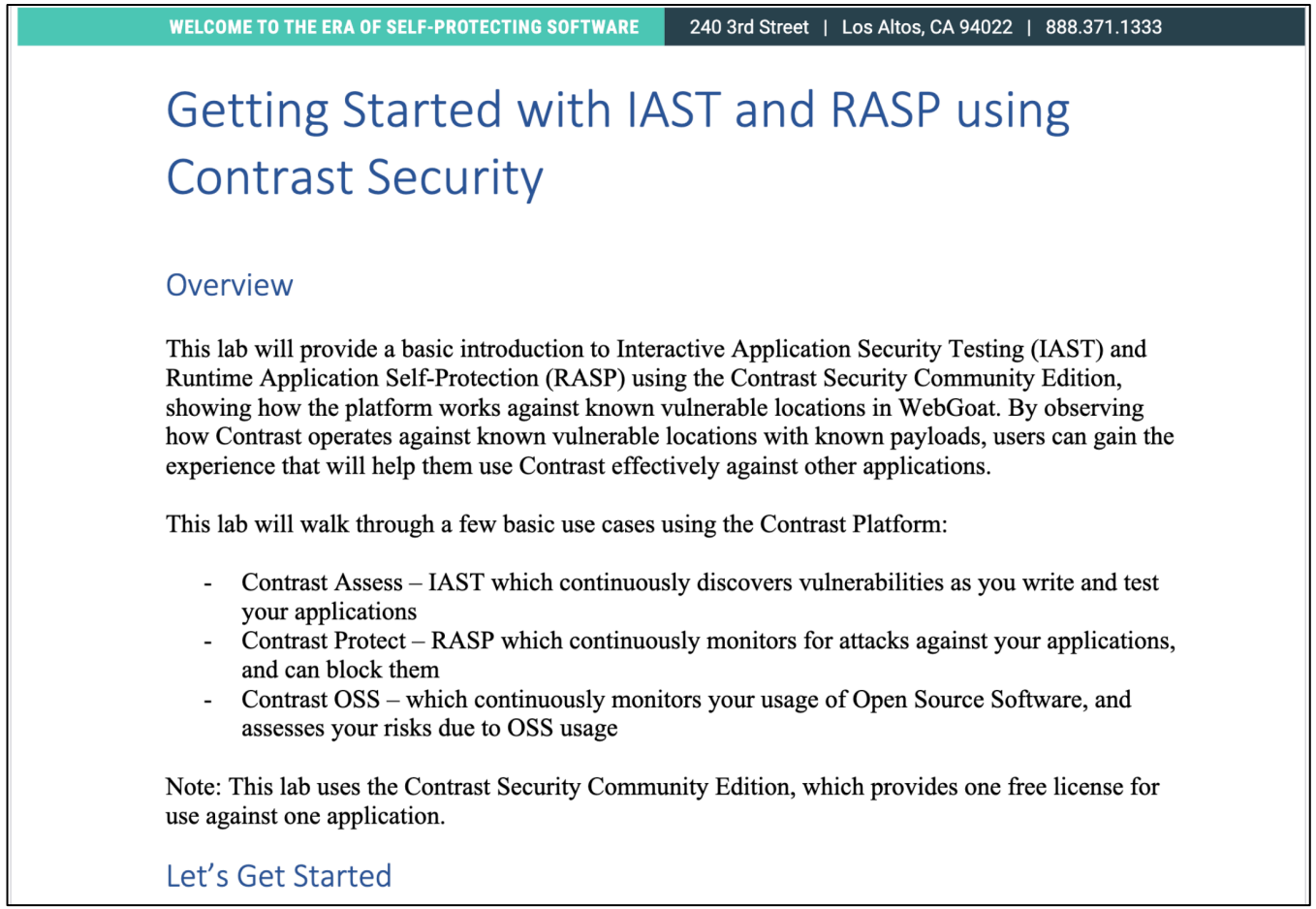
GO!

% docker build `pwd` -t dockerwebgoat

% docker run --rm –p 8080:8080 –t dockerwebgoat



CRACK OPEN THE PDF LAB GUIDE (IASTRASPWEBINARLAB.PDF)



WELCOME TO THE ERA OF SELF-PROTECTING SOFTWARE | 240 3rd Street | Los Altos, CA 94022 | 888.371.1333

Getting Started with IAST and RASP using Contrast Security

Overview

This lab will provide a basic introduction to Interactive Application Security Testing (IAST) and Runtime Application Self-Protection (RASP) using the Contrast Security Community Edition, showing how the platform works against known vulnerable locations in WebGoat. By observing how Contrast operates against known vulnerable locations with known payloads, users can gain the experience that will help them use Contrast effectively against other applications.

This lab will walk through a few basic use cases using the Contrast Platform:

- Contrast Assess – IAST which continuously discovers vulnerabilities as you write and test your applications
- Contrast Protect – RASP which continuously monitors for attacks against your applications, and can block them
- Contrast OSS – which continuously monitors your usage of Open Source Software, and assesses your risks due to OSS usage

Note: This lab uses the Contrast Security Community Edition, which provides one free license for use against one application.

Let's Get Started

CONTRAST SECURITY

NEED HELP? GOT QUESTIONS? USE THE WEBINAR CHAT

