

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>



GET STARTED WITH CONTRAST COMMUNITY EDITION...

1. Sign up for a Free account

2. Add the Contrast agent to your app

3. Secure your software!

Register now to get Zero-day attack protection and OWASP Top 10 Coverage in a platform that integrates with IDEs, CI/CD tools and more!

Looking for more information? Explore our [Contrast Community Edition](#) page to learn more.

First Name

Last Name

Phone Number

Company Name

Company Email

Job Title

Company Employees

HQ Country

I am interested in a free demo

GET STARTED

Welcome to Contrast Security! What brought you here to check us out?

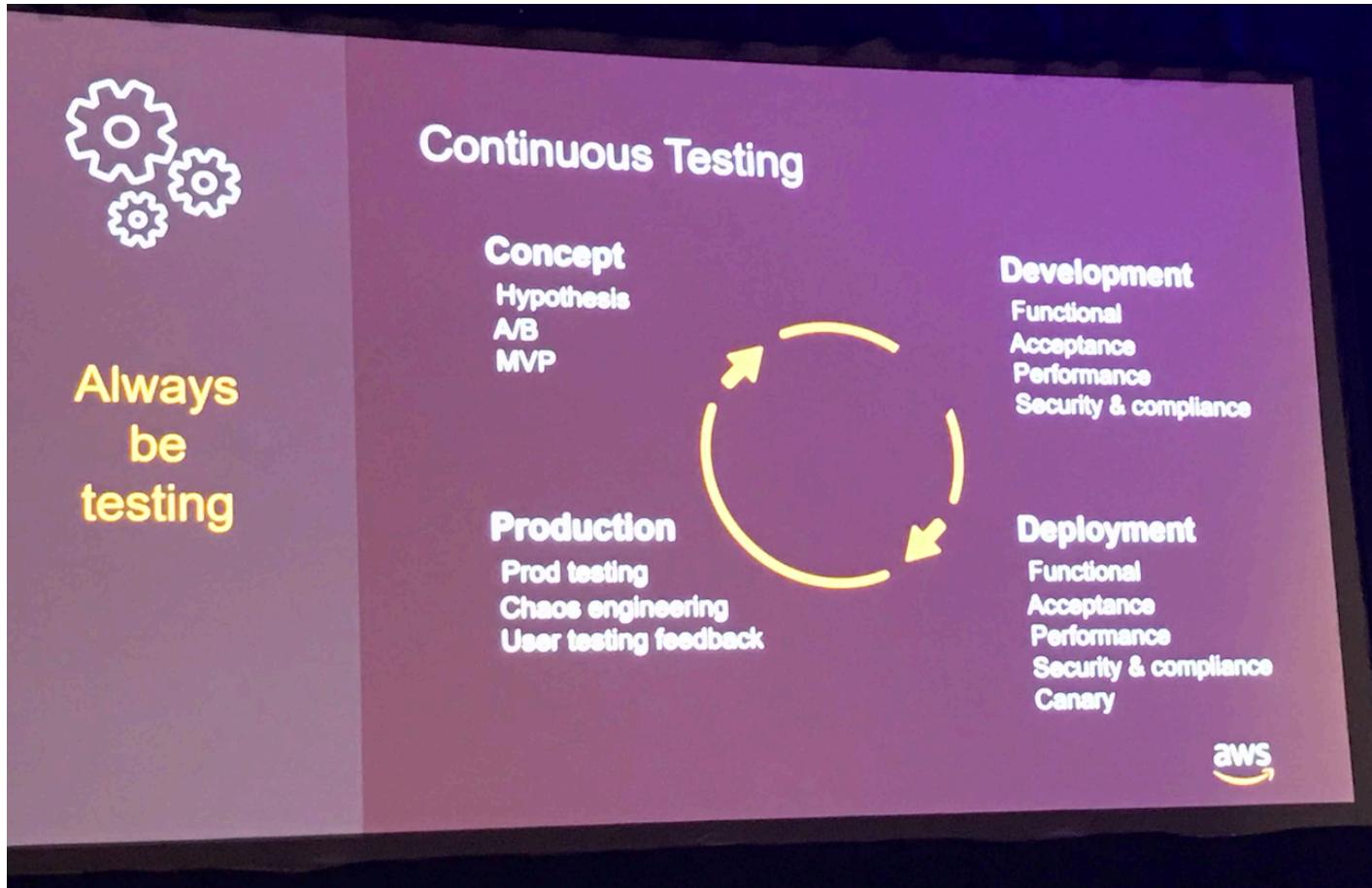
Thank you for registering for your free Contrast Community Edition account!

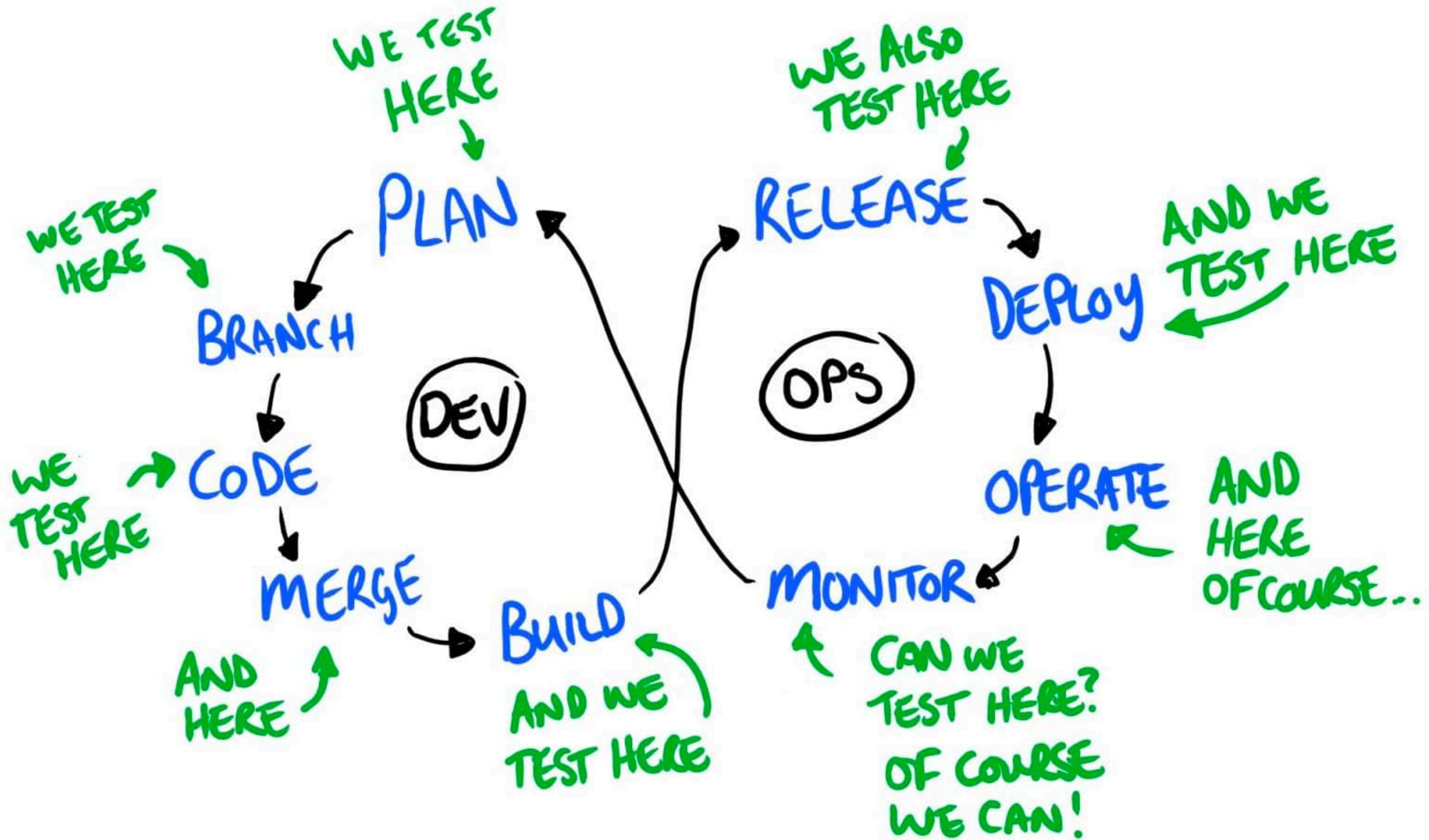
Please check your email to activate your account now.

Check your email for confirmation

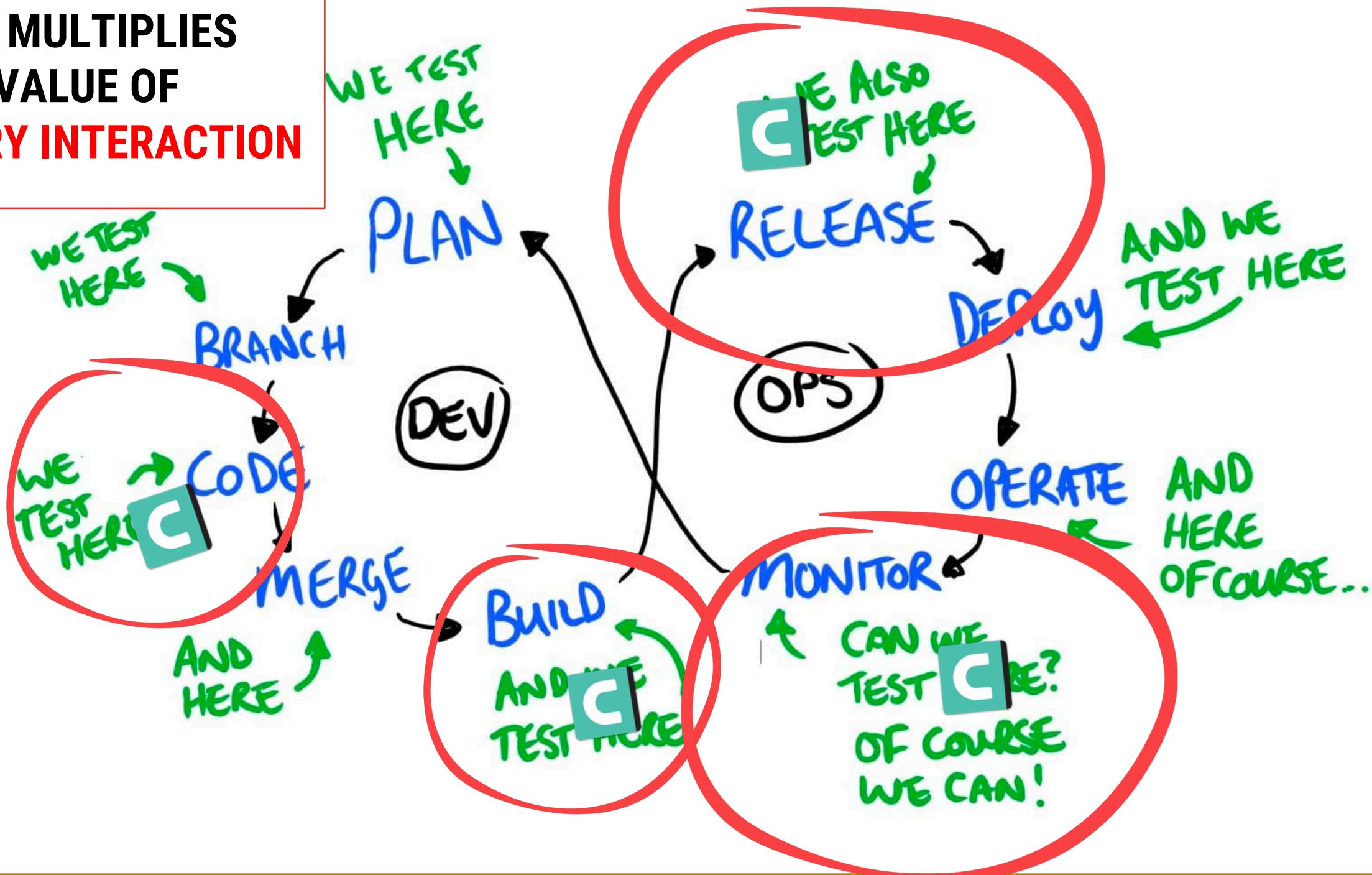
A BRIEF SOAPBOX...

CT (Continuous Testing)



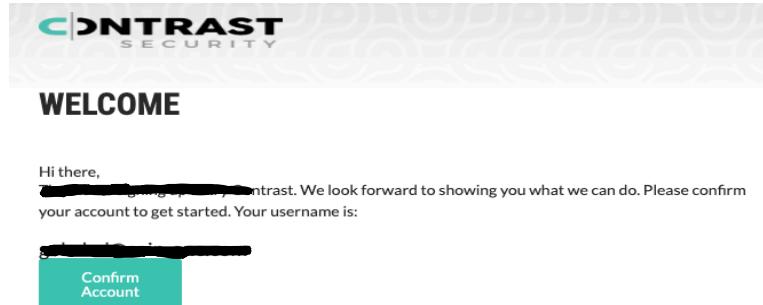


IAST MULTIPLIES THE VALUE OF EVERY INTERACTION



CONFIRM YOUR ACCOUNT....

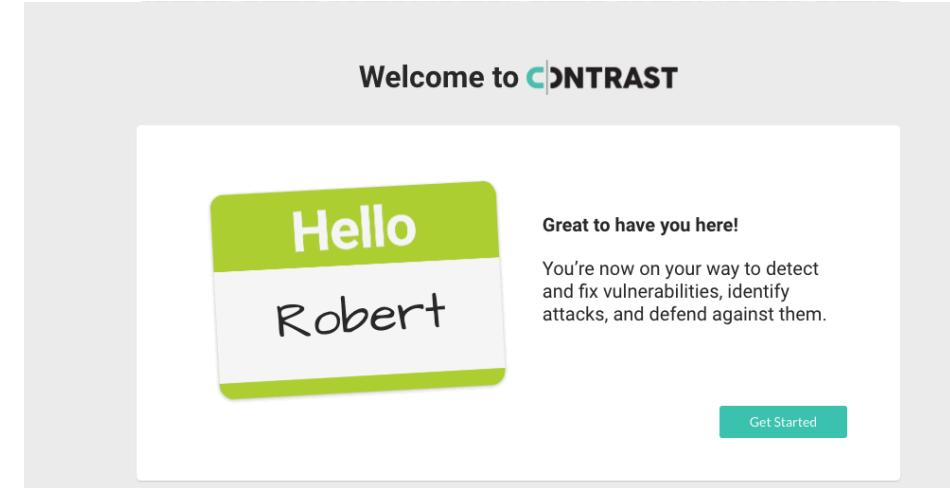
Confirm your new account from registration email:



Click Confirm Account to set your password

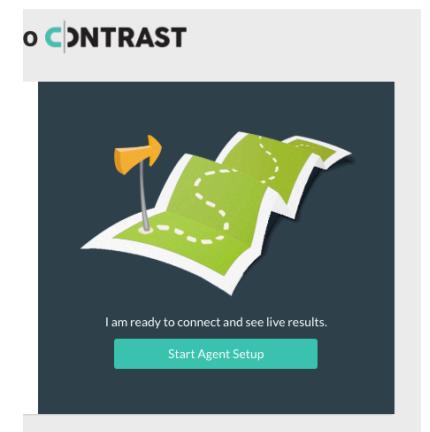
GET STARTED...

Click Get Started



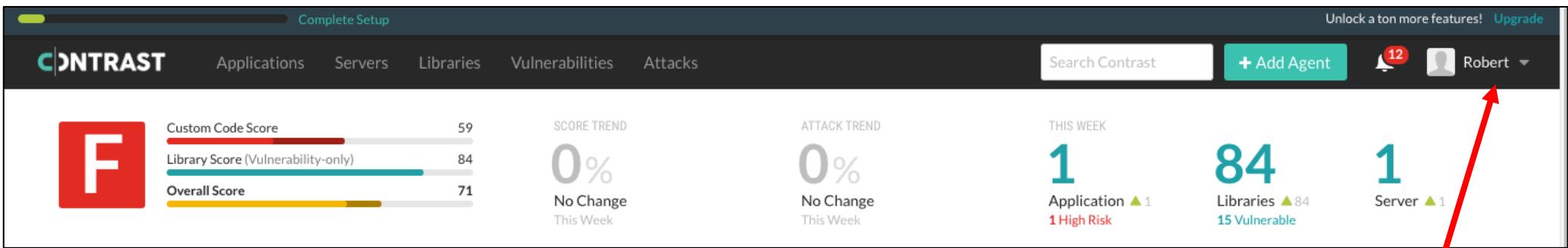
 The Contrast Team
www.contrastsecurity.com

Agree to the Ts & Cs
Click Start Agent Setup



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:



This is a screenshot of the 'Your Account' settings page. It includes sections for 'GENERAL INFORMATION' (Profile, First Name: Robert, Last Name: Statsinger, Date Format: MM/dd/yyyy, Time Format: hhmm a, Time Zone: (GMT-05:00) Eastern Time), 'YOUR KEYS' (Organization Keys and Personal Keys sections, both containing API keys and service keys), and a 'Contrast URL' field (https://ce.contrastsecurity.com/Contrast/).

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>
```



GO!

```
% docker build `pwd` -t dockerwebgoat
```

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

The screenshot displays two browser windows side-by-side. The left window shows the Contrast security tool interface, specifically the 'Applications' view, with one application named 'WebGoatDocker' listed. The right window shows the 'login.mvc' page of the WebGoat application, which is a Java web application designed for penetration testing. The WebGoat logo is visible at the top of the page. The login form contains fields for 'Username' and 'Password', and a 'Sign in' button. Below the form, a message states: 'The following accounts are built into Webgoat'. A table lists two accounts:

Account	User	Password
Webgoat User	guest	guest
Webgoat Admin	webgoat	webgoat

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](#)

**NEED HELP? GOT QUESTIONS? USE
THE WEBINAR CHAT**