DevSecCon | SINGAPORE 22-23 FEB 2018

REMOVE DEVELOPERS' SHAMEFUL SECRETS

OR SIMPLY REMOVE SHAMEFUL DEVELOPERS...

BY Fabian Lim

Join the conversation #DevSecCon

First thing First!

Materials can be found at:

github.com/DevSecOpsSG/devseccon2018

Do the Prerequisite!

Disclaimer

This presentation may or may not contain information about services under GovTech. The information contained in this presentation is classified as Public.

This presentation and its contents does not represent the views of GovTech, or any other entities. They are the sole views of the author. I take full responsibility for my work and any errors fall on my shoulders.

Be happy and awesome; and help others to be happy and awesome.

whoami - about.me/fabian.lim

missions:
- **energetic DevSecOps Engineer and Evangelist**
- physical and cyber security educator

education:
- Singapore Management University, BS Info System
- Carnegie Mellon University, MS Info Security Policy Mgmt

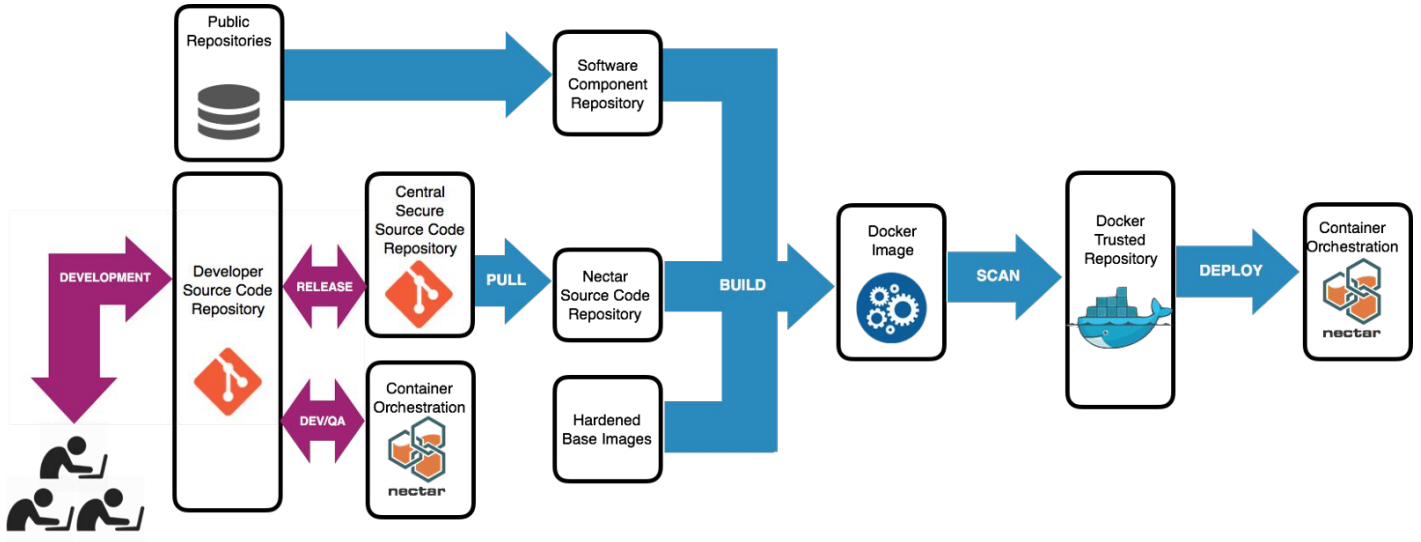
employers:
- Intuit Inc.
- **GovTech [Formerly known as IDA] check out tech.gov.sg for more**
  - **Nectar PaaS, security features, etc.**

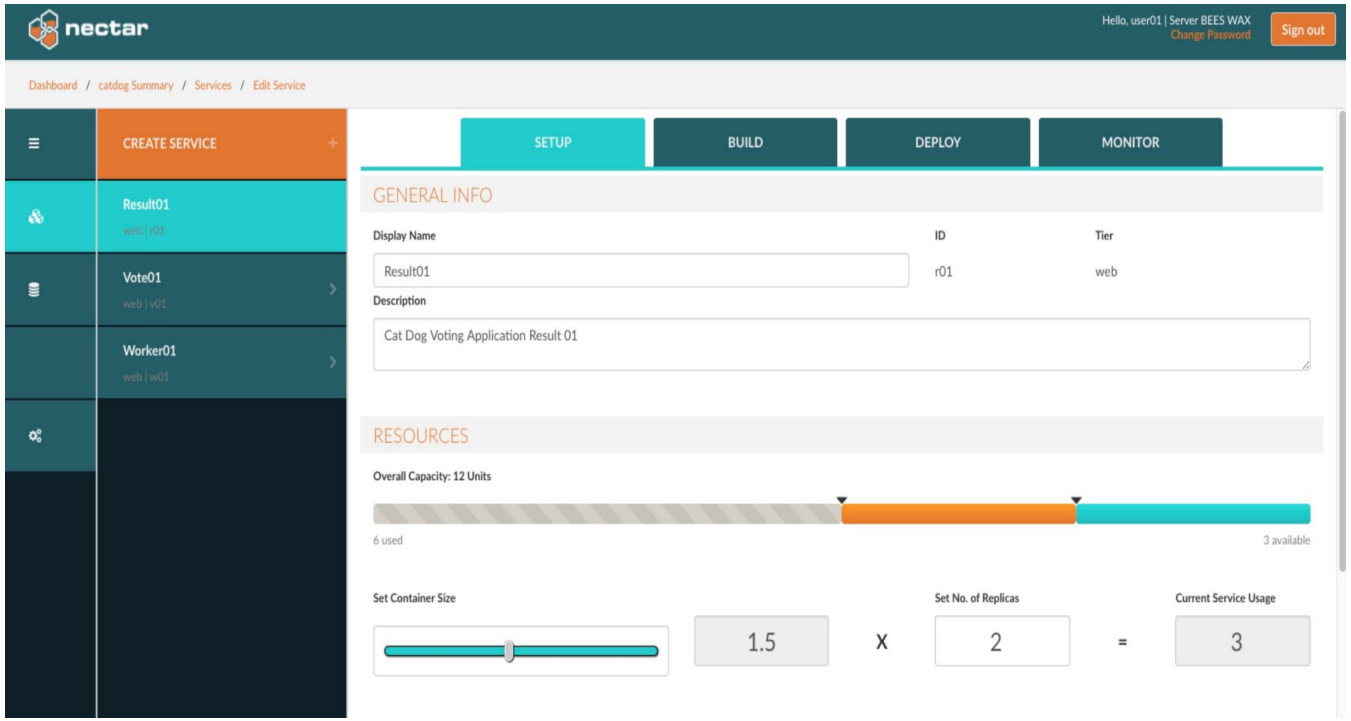
presentations:
- ADDO 2016 [Blue-Green Deployment] http://bit.ly/2fLfHqr
- RSA APJ 2017 [PaaS] http://bit.ly/2ylUyB9

hobbies:
- krav maga; self defense & martial arts
- food

NECTAR

GovTech's Platform as a Service





Read more about it here:
https://blog.gds-gov.tech/nectar-10e0eb1581cf

Takeaways

1) Learned a thing about secret management
2) Learned a thing about design a secure workflow / pipeline
3) Learned a cool, new tool to integrate into your workflow
4) Or… Made a new friend :)

Tone

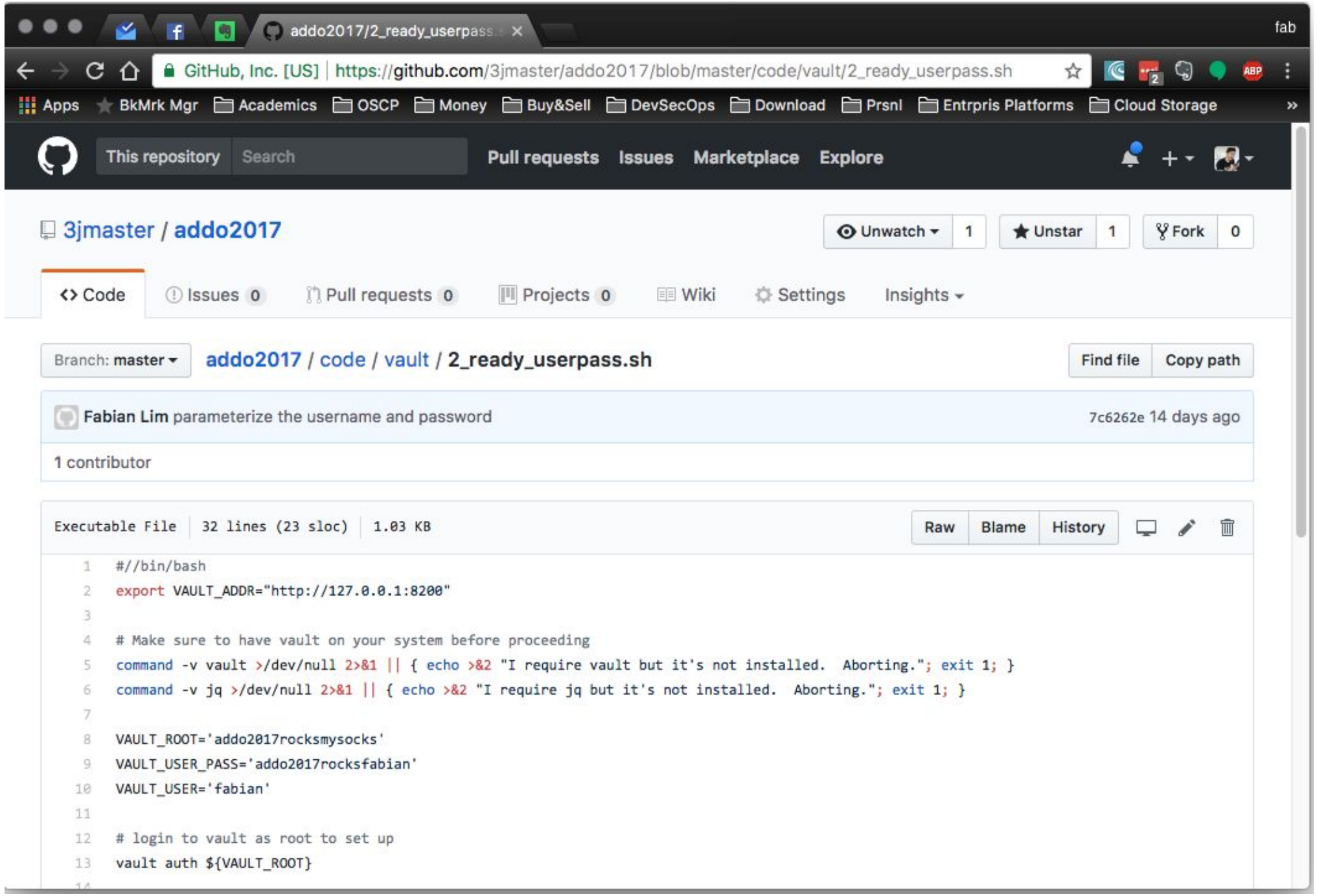
1) Interactive
2) Technical
3) Open

Agenda

1) Get to know each other, and the problems
2) Open discussion for designing a solution
3) Improve on current pipeline
4) Debrief and possible future integrations

My Mistakes!

OOPS! Personal mistake -
commit secrets into repository...


addo2017/2_ready_userpass.
fab
GitHub, Inc. [US] | https://github.com/3jmaster/addo2017/blob/master/code/vault/2_ready_userpass.sh
Apps
BkMrk Mgr
Academics
OSCP
Money
Buy&Sell
DevSecOps
Download
Prsnl
Entrpris Platforms
Cloud Storage
This repository
Search
Pull requests
Issues
Marketplace
Explore
3jmaster / addo2017
Unwatch 1
Unstar 1
Fork 0
Code
Issues 0
Pull requests 0
Projects 0
Wiki
Settings
Insights
Branch: master
addo2017 / code / vault / 2_ready_userpass.sh
Find file
Copy path
Fabian Lim parameterize the username and password
7c6262e 14 days ago
1 contributor
Executable File | 32 lines (23 sloc) | 1.03 KB
Raw
Blame
History
#//bin/bash
export VAULT_ADDR="http://127.0.0.1:8200"
Make sure to have vault on your system before proceeding
command -v vault >/dev/null 2>&1 || { echo >&2 "I require vault but it's not installed. Aborting."; exit 1; }
command -v jq >/dev/null 2>&1 || { echo >&2 "I require jq but it's not installed. Aborting."; exit 1; }
VAULT_ROOT='addo2017rocksmysocks'
VAULT_USER_PASS='addo2017rocksfabian'
VAULT_USER='fabian'
# login to vault as root to set up
vault auth ${VAULT_ROOT}

ucdd2-sp15/sunlight – apikey.js — JavaScript

Showing the top two matches Last indexed on 19 Sep 2016

```
1  // api key
2  var apikey = {apikey: '6273aad657ed46168d96d5ac941597b8'}
```

ucdd2-sp15/sunlight – apikey.js — JavaScript

Showing the top two matches Last indexed on 19 Sep 2016

```
1  // api key
2  var apikey = {apikey: '6273aad657ed46168d96d5ac941597b8'}
```

marco-amoroso/images-app – sample.globals.js — JavaScript

Showing the top two matches Last indexed on 20 Sep 2016

```
1  /* exported apiKey */
2  var apiKey = '1234abcd';
```

asassu/game_talk – apikey.js — JavaScript

Showing the top two matches Last indexed on 19 Sep 2016

```
1  // api key
2  var apikey = {apikey_bomb: '293337dc0d93e1319cbcf7c424bf48e5b4c88347'}
```

asassu/game_talk – apikey.js — JavaScript

Showing the top two matches Last indexed on 19 Sep 2016

```
1  // api key
```

This repository Search Pull reque

andycall / VPN-Kicking

<> Code Issues 0 Pull requests 0 Proje

Tree: ef6f5314e8 VPN-Kicking / password.js

andycall add README

1 contributor

4 lines (2 sloc) 62 Bytes

```
1  var password = "dongtiancheng";
2
3
4  exports.password = password;
```

1 contributor

5 lines (3 sloc) 95 Bytes

```
1  CREDENTIALS = {}
2
3  CREDENTIALS['login'] = 'codingdojo'
4  CREDENTIALS['password'] = 'codingdojo15'
```

6 lines (5 sloc) 141 Bytes

```
1  const credentials = {
2          sid: 'ACcf5889a6dfd3bfbb298973ab1dc0baa0',
3          token: '2dc05cd146f749e9e41a56db3b64be85'
4  }
5
6  module.exports = credentials;
```

Tree: 71ba83a979 responsible / server / lib / config.js

JosephPena schme files changes updated

1 contributor

10 lines (8 sloc) 128 Bytes

```
1  var credentials = {
2    oauth: {
3      key: '63m5zj12b0yJe2k1MJKOEIz9Afs',
4    },
5  };
6
7  module.exports = {
8    credentials: credentials,
9  };
```

Get to know each other, and the problems

Get to know each other, and the problems

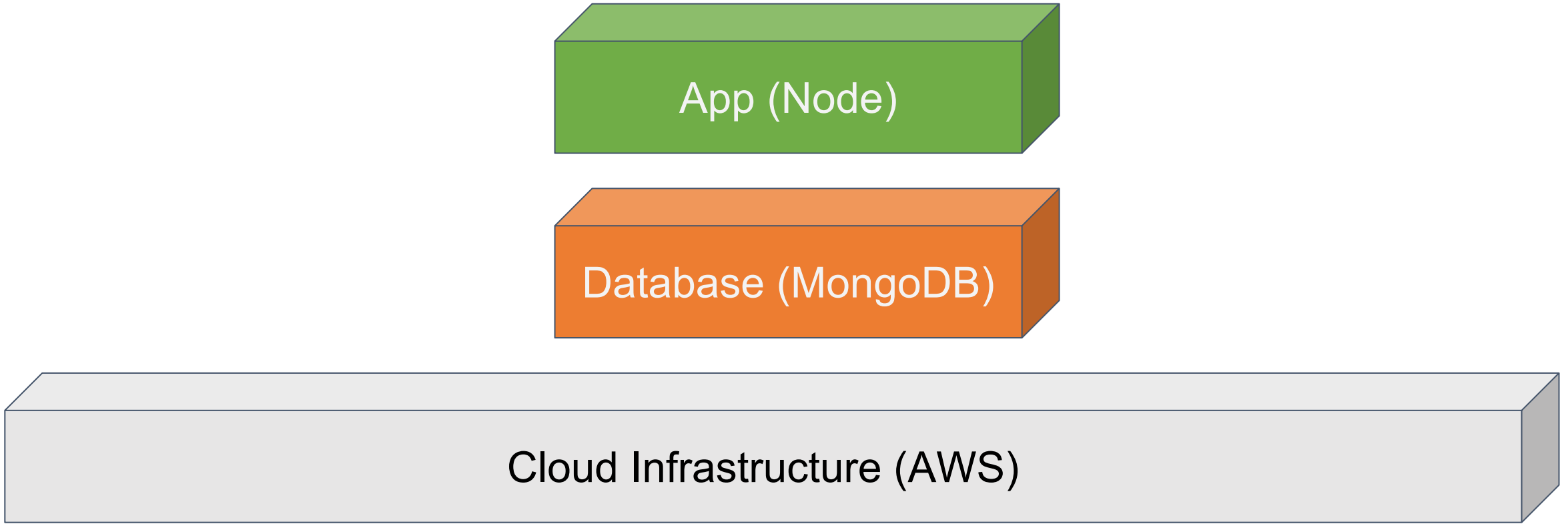
1) With 2 or 3 in a group, introduce and get to know each other

2) What are some common password problems?

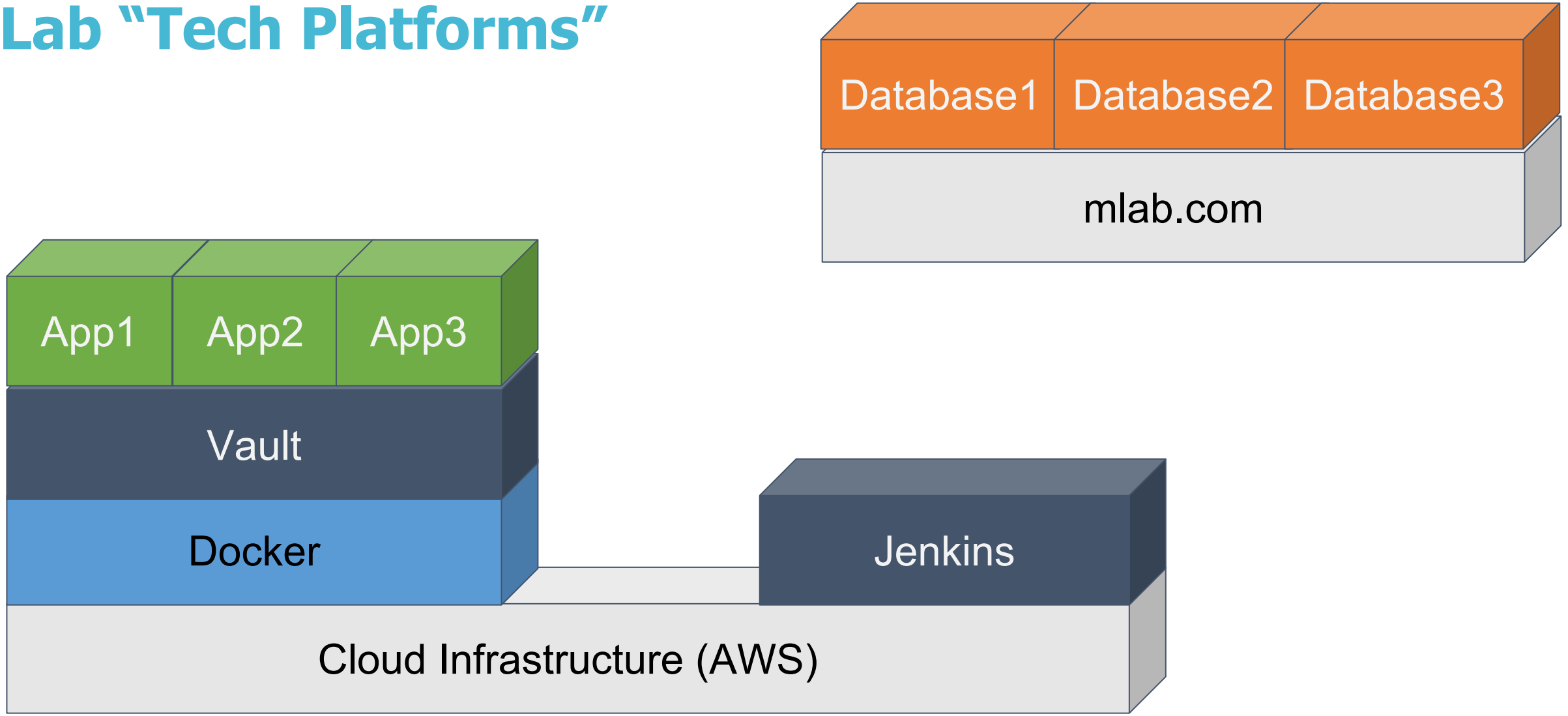
    a) What are the credentials for X database, Y API, etc?
    b) Where am I supposed to store these credentials?
    c) Who should have these credentials? Can I pass it to ABC?
    d) How do I rotate credentials for Y API because ABC left?
    e) How do I keep track of X secrets of Y apps?

Discussion Time!

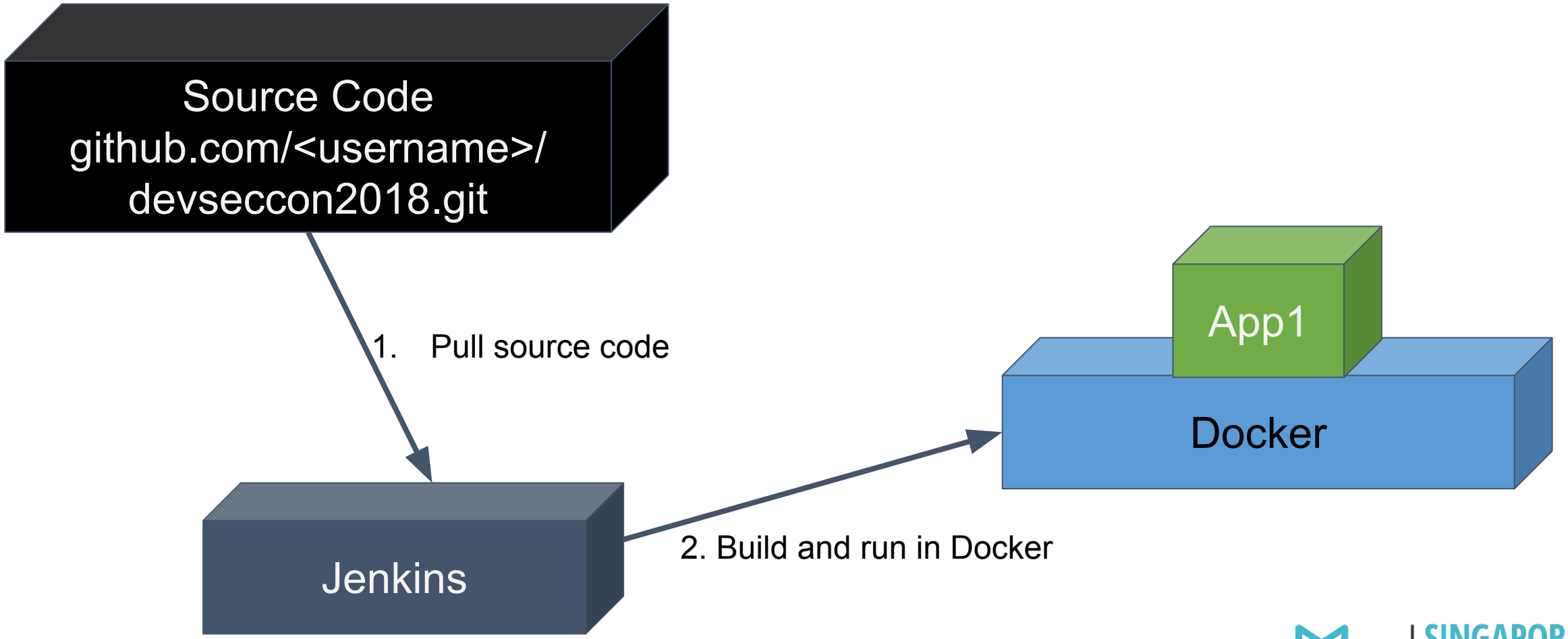
Lab "Tech Stack"



Lab "Tech Platforms"



Lab Workflow



LET’S GO!

Lab

https://docs.google.com/presentation/d/12qNpVXpSxNuOE4wG9CBSGINauc7cBjOmIiQo3w7w9AA/edit#slide=id.g31f475055f_0_238

Open discussion for designing a solution

How to retrieve secrets?

1. Environment variables (static)
    a. How do I manage the environment variables in dev, staging and prod?
2. Run-time API retrieval (pull)
    a. What API keys to use? Where do I store it?
3. Run-time deployment variable injection (push)
    a. How does the deployer trust THIS instance of build?
    b. How does the deployer know what secrets THIS instance need?

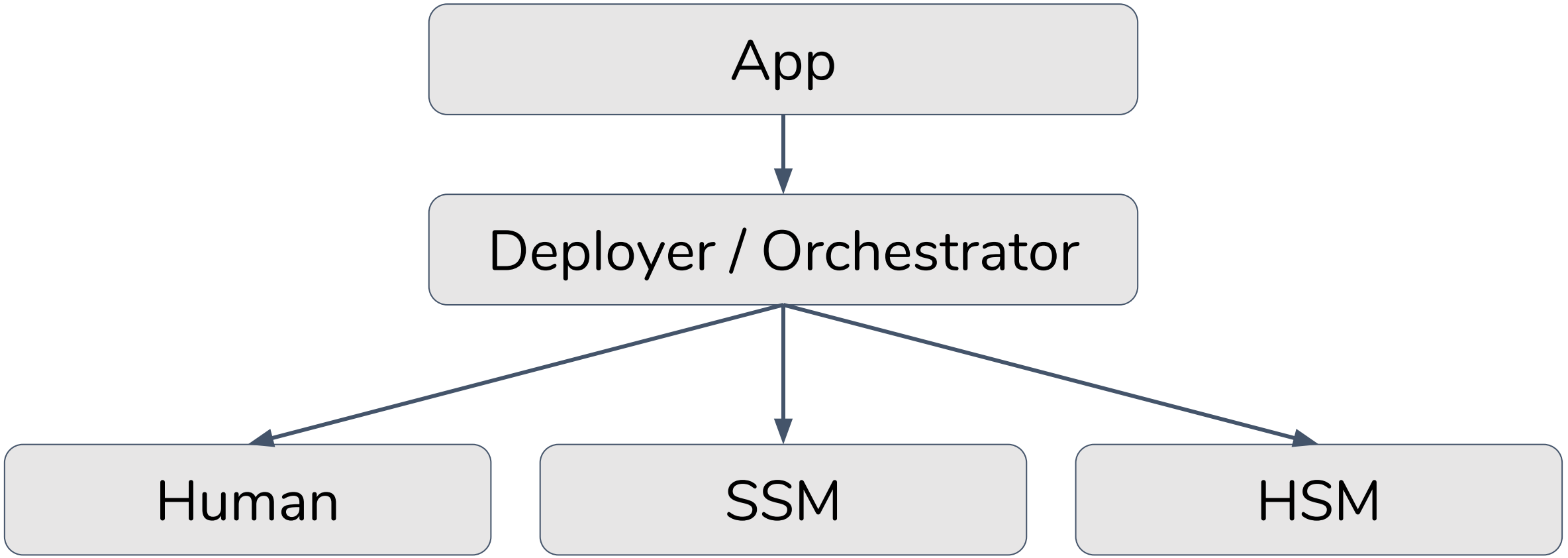
Chain of Trust

Manage Trust in workflow / pipeline

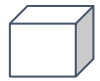
secret[0]

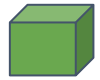
The idea of secret[0] is the first piece of credential, or the first entity of trust, needed to initiate a trusted chain of actions like producing the second piece of secret, etc.

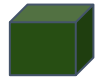
Shift of Responsibility to Hold secret[0]

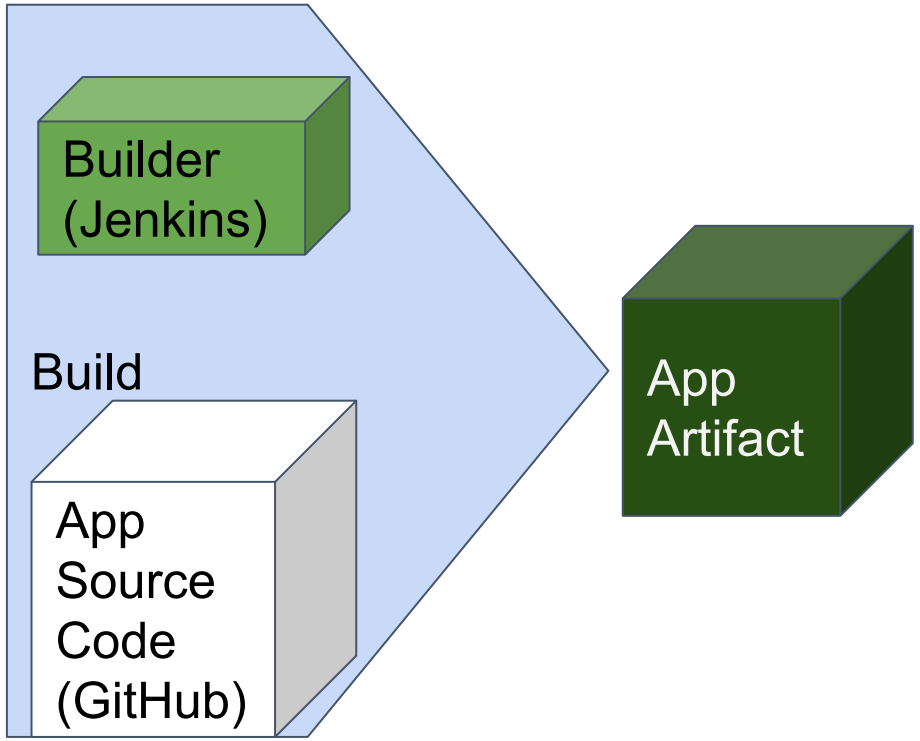


The App is a Box, in a Pipeline

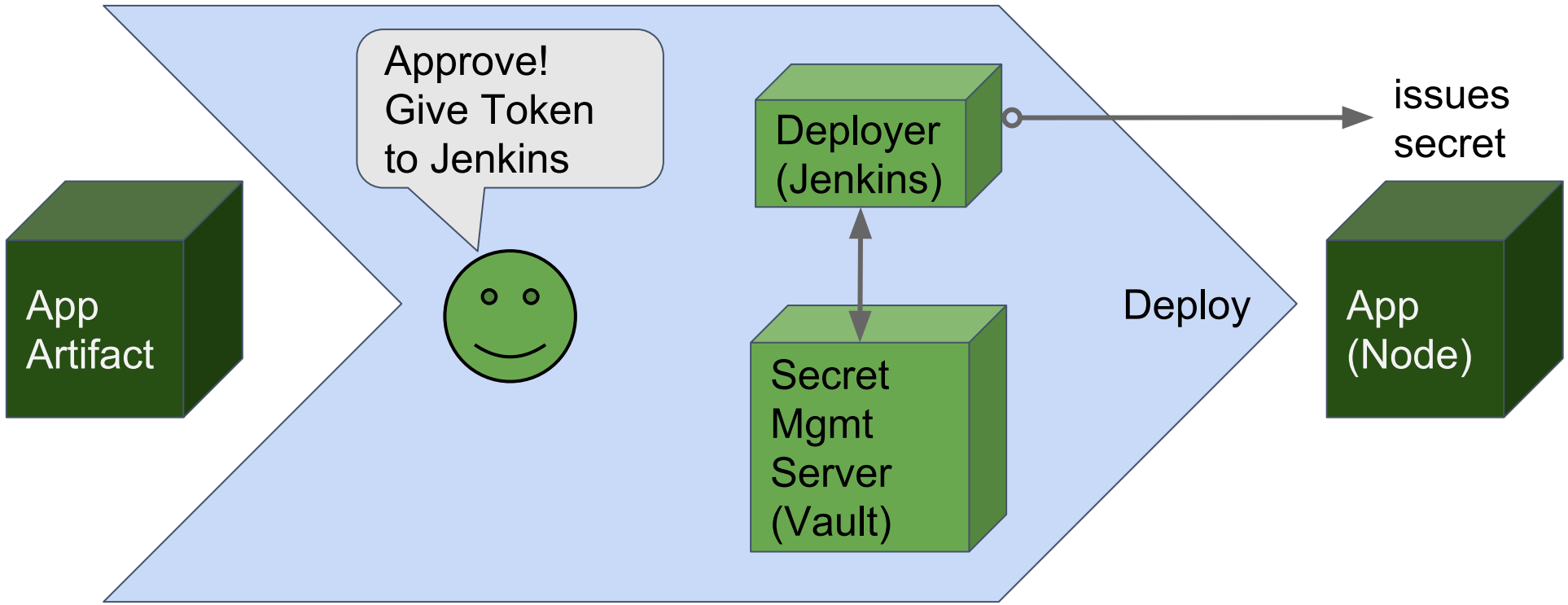

= Neutral Entity


= Trusted Entity


= Trusted Child Entity



The App is a Box, in a Pipeline

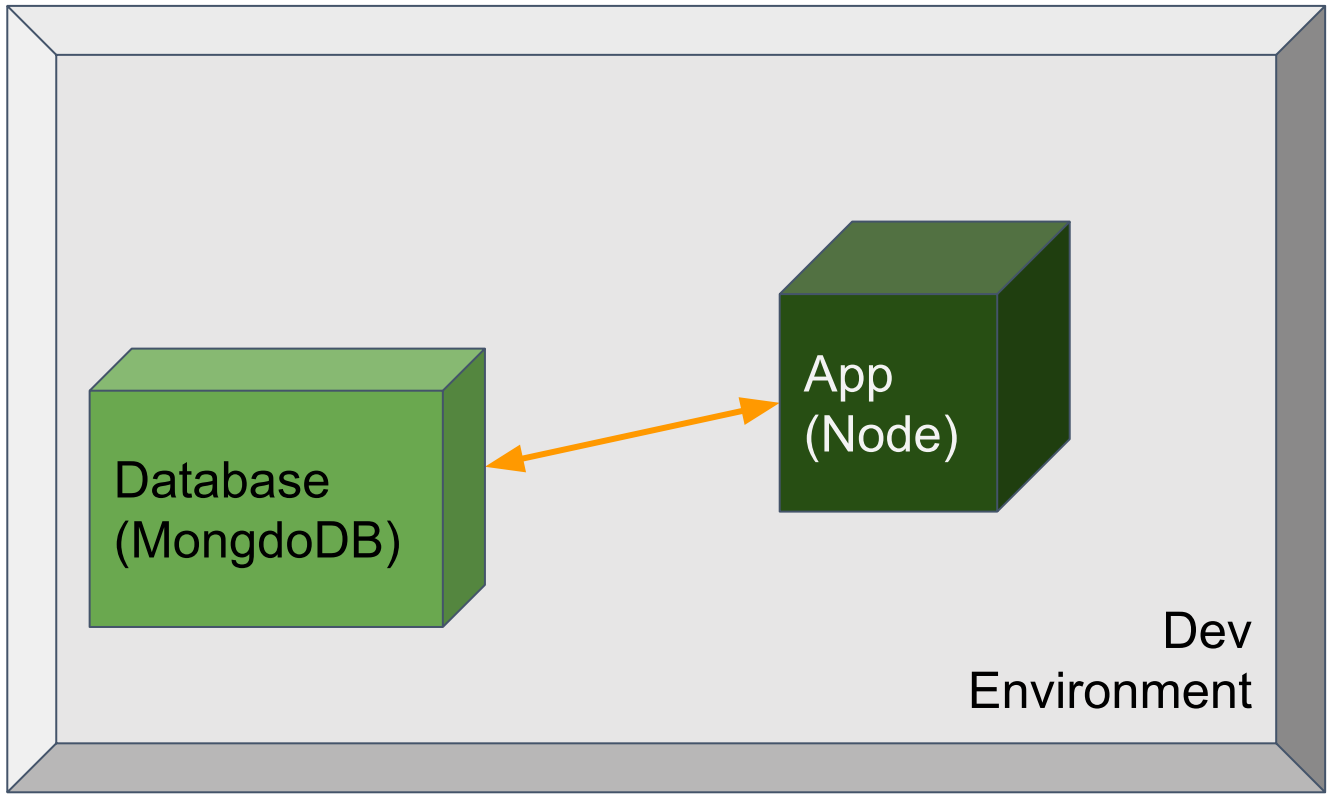


The App is a Box, in a Pipeline

= Neutral Entity

= Trusted Entity

= Trusted Child Entity



Improve on current pipeline

Open discussion for designing a solution

Put on the Security Architect's hat:

1) What's a good technical solution that removes (or the risk of storing) secrets in code repositories?

2) How do you establish trust in a workflow?

3) How does a good development pipeline or workflow look like?

Discussion Time!

Scenario

- You are a new security developer in the team
- Audit flagged a high risk in the plaintext secrets that was checked in t the code repository

Objectives

Task #1: Remove secrets in code repository, but still run
Task #2: Prevent secrets from exposing in build environment (logs)

LET’S GO!

Lab

https://docs.google.com/presentation/d/12qNpVXpSxNuOE4wG9CBSGINauc7cBjOmIiQo3w7w9AA/edit#slide=id.g31f475055f_0_238

Debrief, and possible future integrations

Pipelines are Fundamental in DevSecOps

Because it:

- Supports SDLC; and Agile

By:

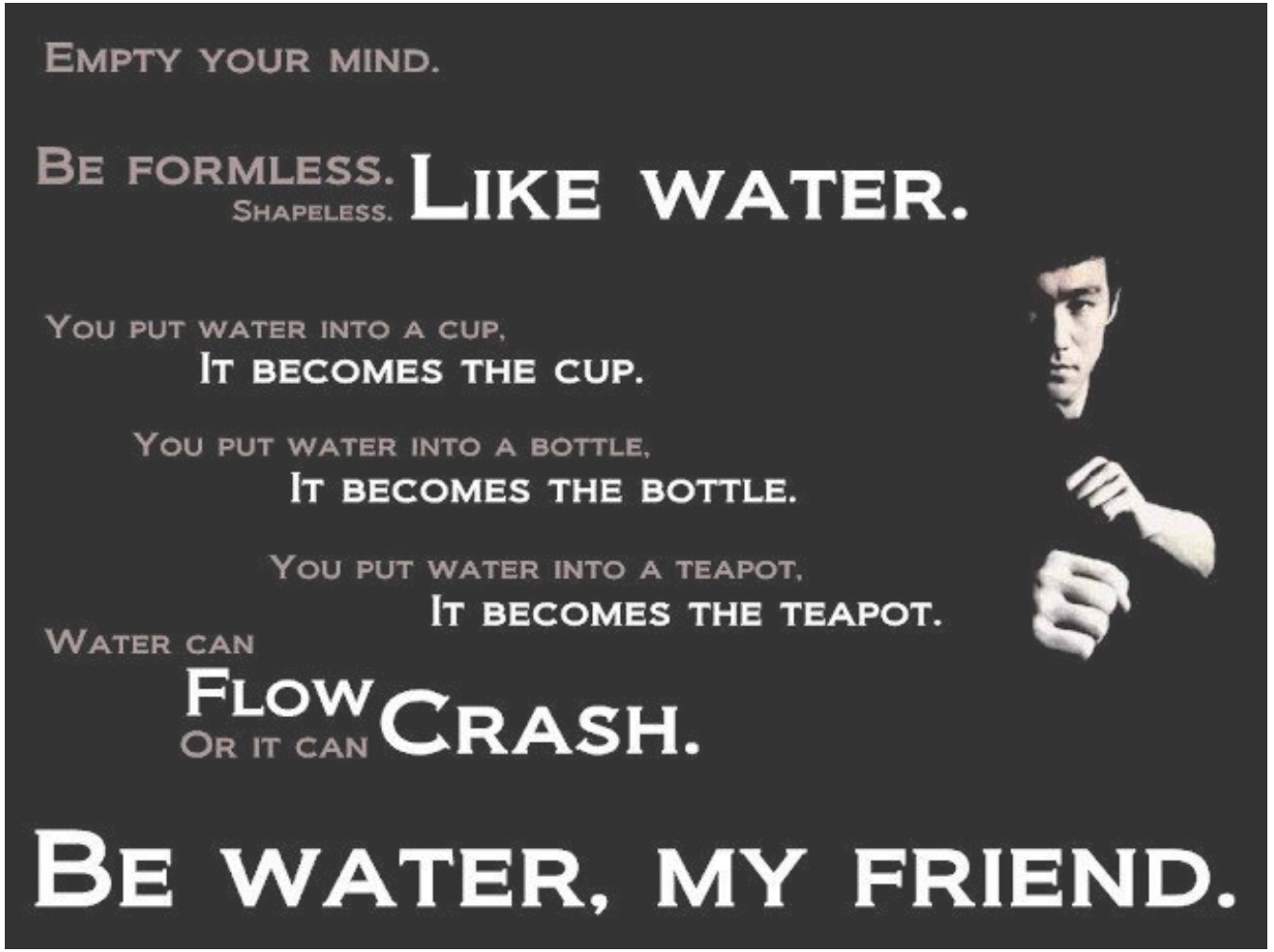
- Thinking like water pipelines engineers
- Building as modular as possible - API
- Building resilience

Doing so, benefits are:

- Security is built-in by design
- Containment; Blast Radius
- It can scale healthily!
- It has the ability to be re-build

Find your recipe

1)



Debrief, and possible future integrations

1) What are your takeaways?
   a) Find # of hard-coded secrets
   b) "Variablize" found secrets
   c) Remove habits of checking in secrets
   d) Remove guilty developers [optional]

2) How would you start to embark this journey and start to communicating this with your developers?

3) What are possible integrations improvements to this workflow?

DevSecCon | SINGAPORE 22-23 FEB 2018

Thank you for your attention, patience, and enthusiasm during the workshop!

Happy Lunar New Year!
Cheers!

Join the conversation #DevSecCon