ThoughtWorks®

Cabinet Office

# Tin Tulip - Blue team

Showcase #7 - June 2

# Agenda

What we achieved

What’s next?

# Summary

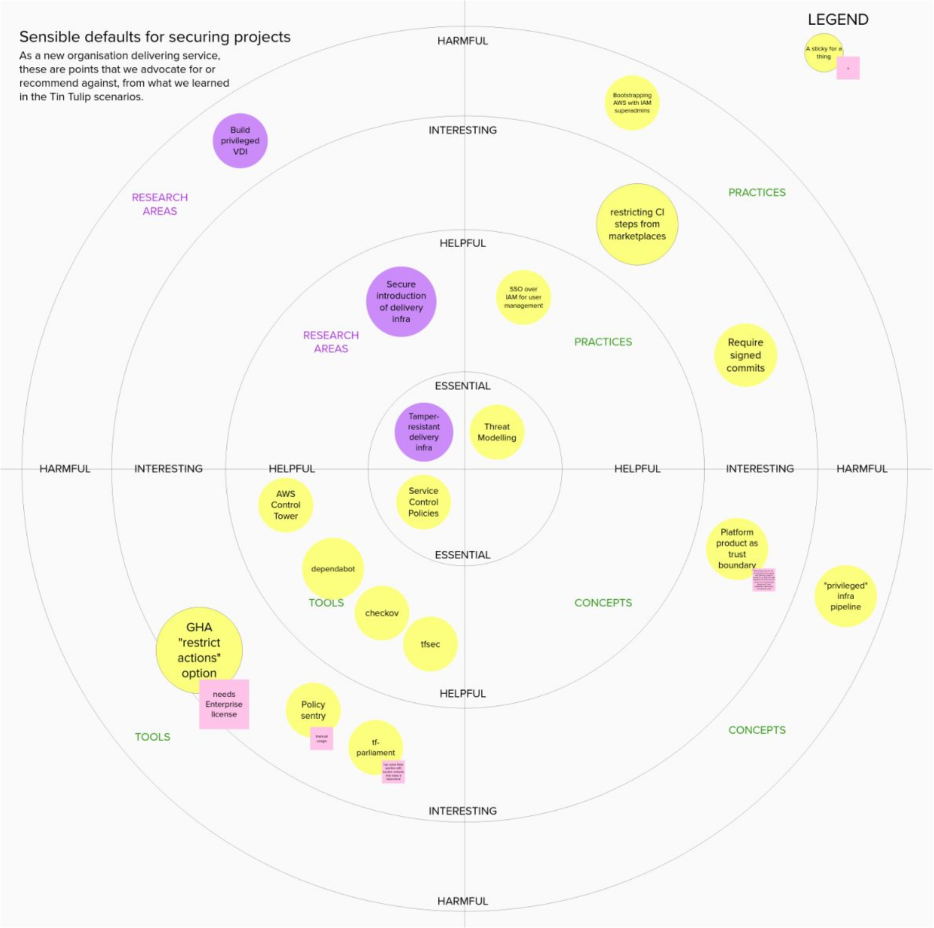
*The blue team are preparing for the beginning of red team engagement next week*

*We are adding a dynamic workload and finishing the trusted pipeline*

# What we achieved

# What we worked on

- Running Terratest in the Sandbox
- Setting up CodePipeline
- Network setup



Sensible defaults for securing projects

As a new organisation delivering service, these are points that we advocate for or recommend against, from what we learned in the Tin Tulip scenarios.

*Zoomable diagram available on Mural at this link (signup required)*

# Running Terratest in sandbox

**What we built:**
Created a sandbox account as well as the Github actions pipelines to run terratest.

**Why we built it:**
To have a testing environment for team Dali that tests the infrastructure.

**What we learned from it:**

- Developers can test their work without impacting other environments.
- Terratest provides fast feedback and destroys after testing.

*Resource available at this Link*

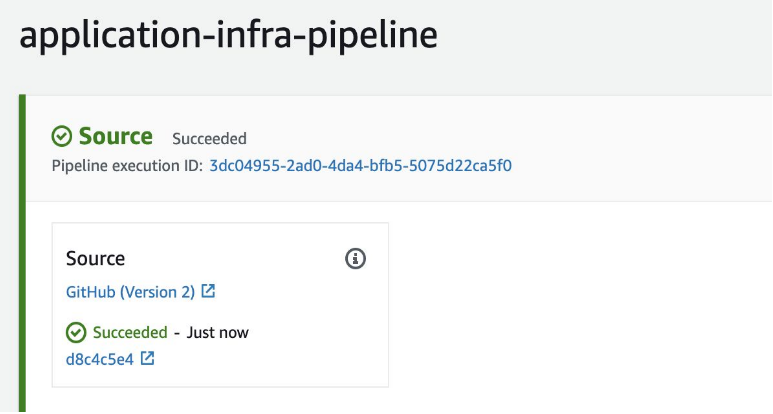
# Setting up CodePipeline

**What we built:**
A pipeline for the builder account that is triggered when a commit is made to the CI (GitHub Actions).

**Why we built it:**
To have a secondary pipeline in a highly trusted environment to reduce the blast radius of a malicious user.

**What we learned from it:**

- IAM user can trigger CodePipeline from GitHub actions.
- Alternatively GitHub actions can be integrated with CodePipeline using a webhook.



application-infra-pipeline

Source Succeeded
Pipeline execution ID: 3dc04955-2ad0-4da4-bfb5-5075d22ca5f0

Source
GitHub (Version 2)
Succeeded - Just now
d8c4c5e4

*Resource available at this Link*

# What’s next?

# Readiness for Red team start

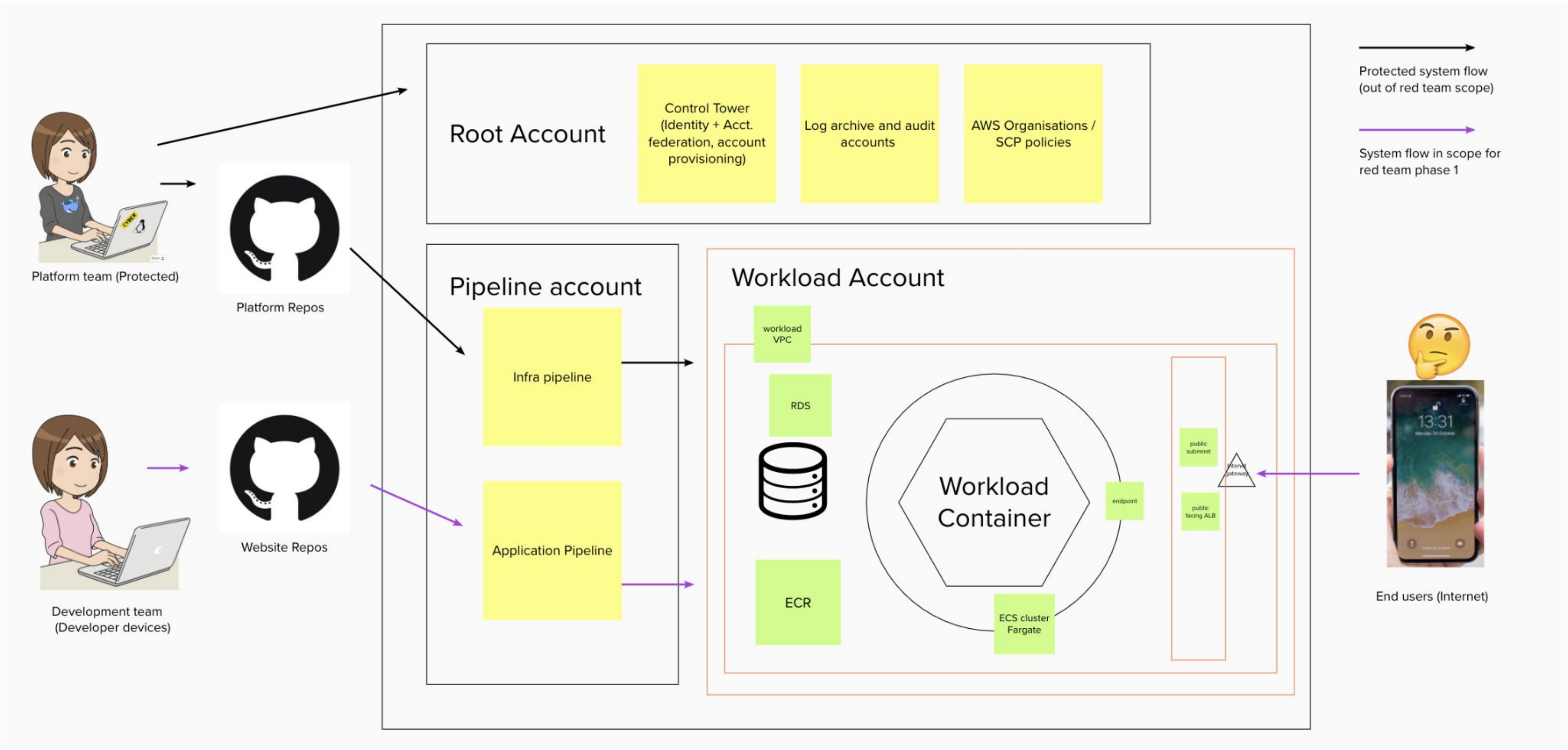

Platform team (Protected)
Platform Repos
Development team (Developer devices)
Website Repos
Root Account
Control Tower (Identity + Acct. federation, account provisioning)
Log archive and audit accounts
AWS Organisations / SCP policies
Pipeline account
Infra pipeline
Application Pipeline
Workload Account
workload VPC
RDS
ECR
Workload Container
ECS cluster Fargate
endpoint
public submnet
public facing ALB
Intenet gateway
13:31
End users (Internet)
Protected system flow (out of red team scope)
System flow in scope for red team phase 1

*Diagram available on Mural Link*

# Readiness for Red team start

## What we are working on:

- Completion of pipelines
- Completion of ECS workload

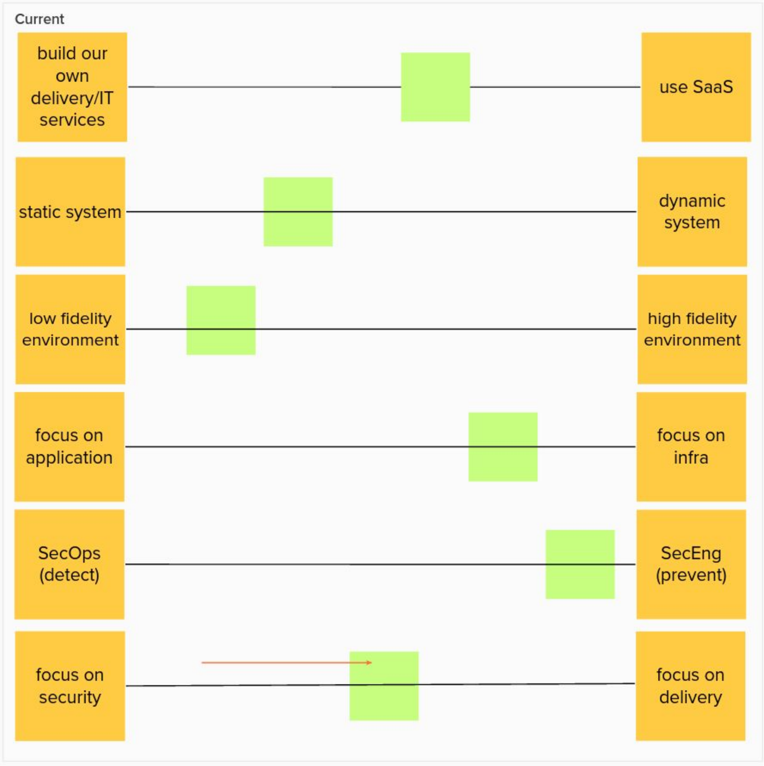
## What we will give the red team:

- Login as a Development team user
- URL for workload on Internet

## What we need to do with red team to prepare

- Agree flags
- Share credentials
- Agree daily wash up calls
- *Any other logistics ?*

# Tradeoff Sliders review



- Focussed on starting red team engagement

Sliders tracker (link requires access):

https://app.mural.co/t/thoughtworksclientprojects1205/m/thoughtworksclientprojects1205/1620729955822

# Appendix: Guiding Principles

# Guiding principle for the project

*Does this teach us something new about a security control, or how to defeat it?*

## Guiding principle for platform implementation

*In order to research the known security boundaries, the blue team will implement a test platform based on published best practices, including those published by the NCSC*

# Guiding principle for communicating learnings

*The key audience for learnings are government departments, who want to empower their local technology teams to deliver secure systems*