ThoughtWorks®

Cabinet Office

Tin Tulip - Blue team

Showcase #8 - June 9

Agenda

What we achieved

What’s next?

Summary

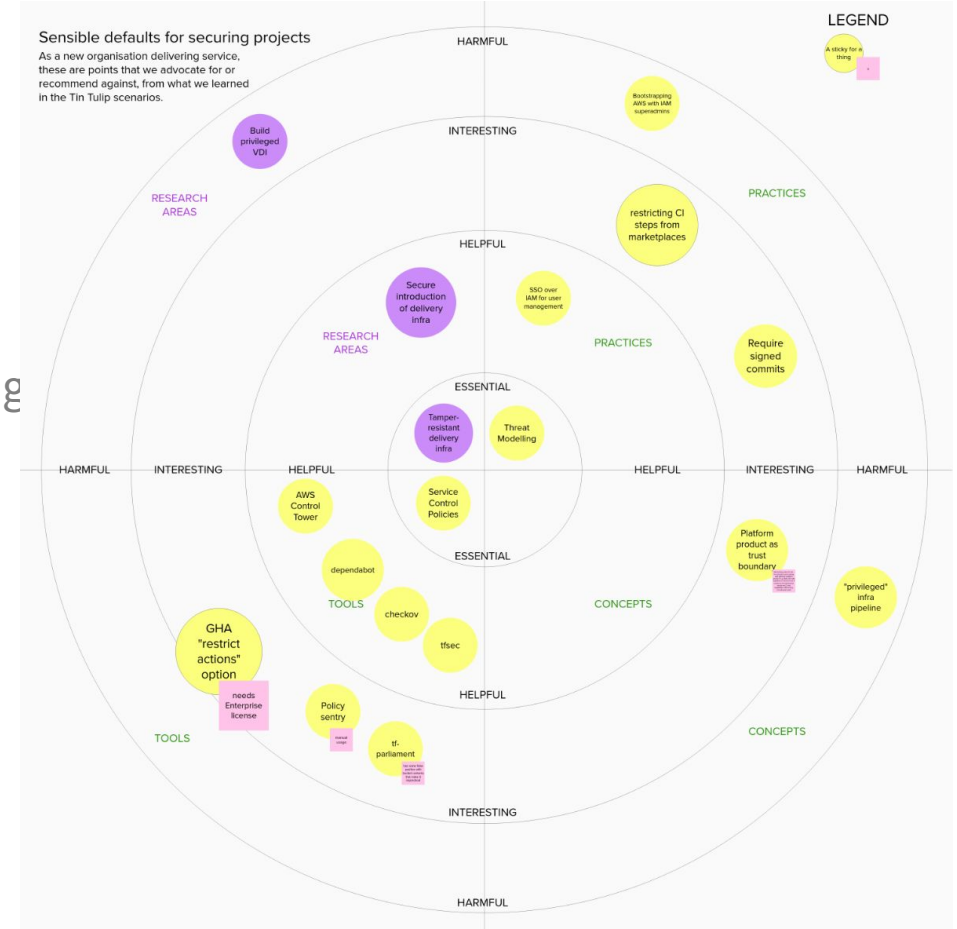
Blue team deployed a dynamic workload via trusted pipelines.

We are now focussing on enabling the Red team to start testing.

What we achieved

What we worked on

- Configure IaC pipeline
- Configure webapp pipeline
- Build & Deploy skeleton webapp
- Setup public-facing webapp networking
- Initial kickoff with Red Team
- First Red Team findings!



Zoomable diagram available on Mural at [this link](#) (signup required)

Configure IaC pipeline

What we built:

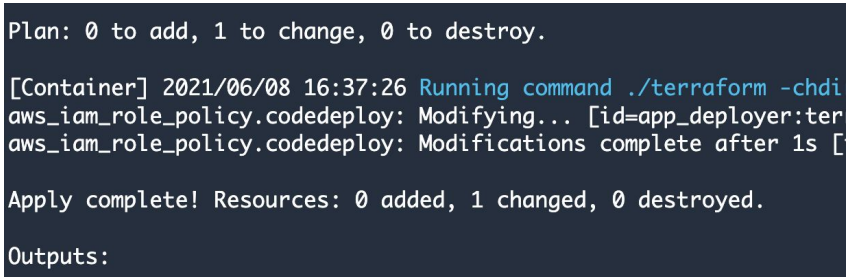
A trusted pipeline with terraform commands that starts after a commit from github.

Why we built it:

Securely deploy infrastructure changes to the pre-production environment.

What we learned from it:

- Connecting GH via webhook is non-trivial, and hard to debug when it doesn't work



Resource available at this Link

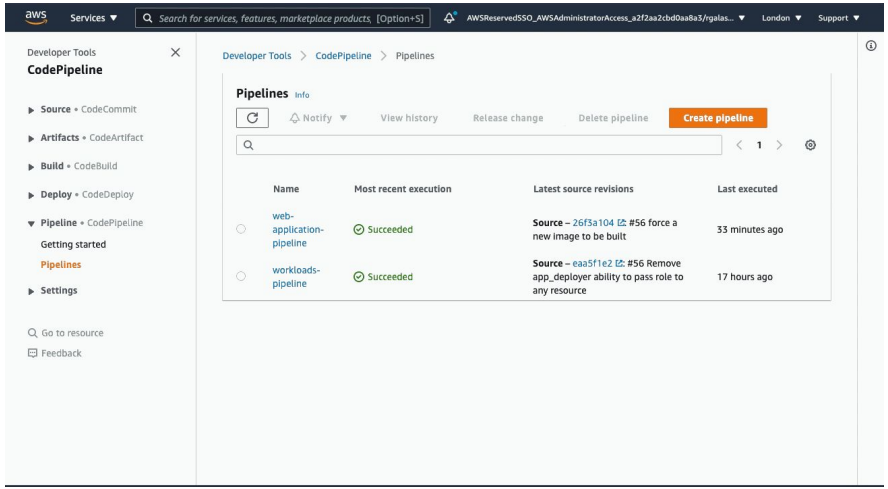
Configure Web App pipeline

What we built:
A trusted pipeline that starts after a commit from github, builds the image and deploys that image

Why we built it:
Securely deploy images to an ECS cluster without requiring knowledge of infrastructure

What we learned from it:

- Infrastructure for services are defined in the workloads repo (managed by the platform team)
- Small changes needed to the ReadOnly policy to allow developers to view pipeline or approve changes



Resource available at this Link

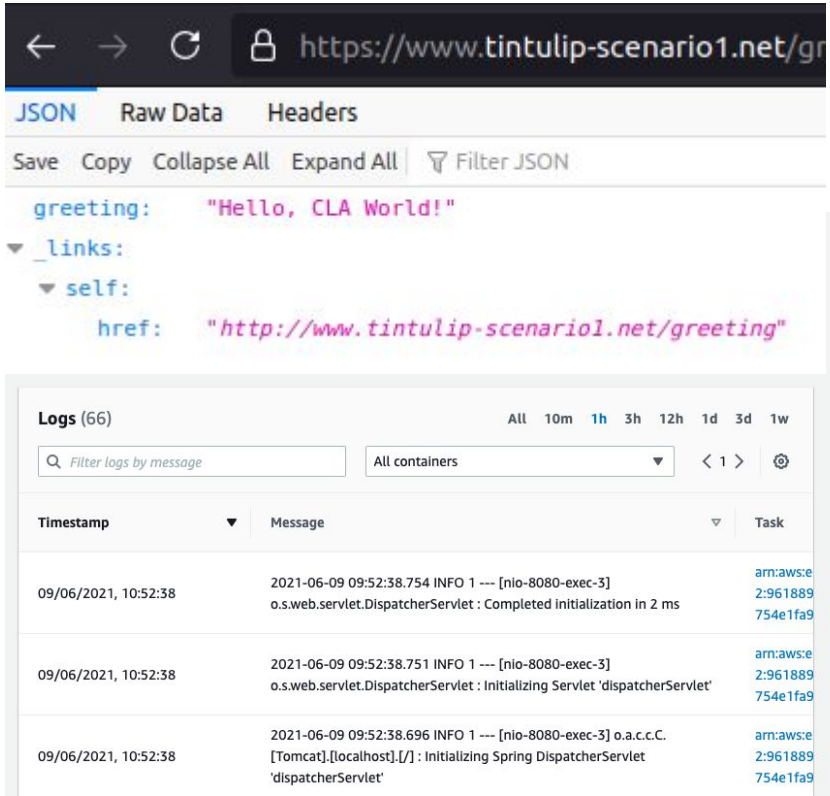
Build & Deploy skeleton webapp

What we built:
A simple microservice (SpringBoot, Java16) that returns a greeting

Why we built it:
To have an end-to-end flow built by the developer team from source to ECS

What we learned from it:

- Using AWS CodeDeploy for cross-account deployments is complex - easier to use awscli (ecs update-service)



Web-application source code available at this link

Setup public-facing webapp networking

What we built:
Public-facing LB with TLS for
www.tintulip-scenario1.net

Why we built it:
Make CLA's webapp available to public users

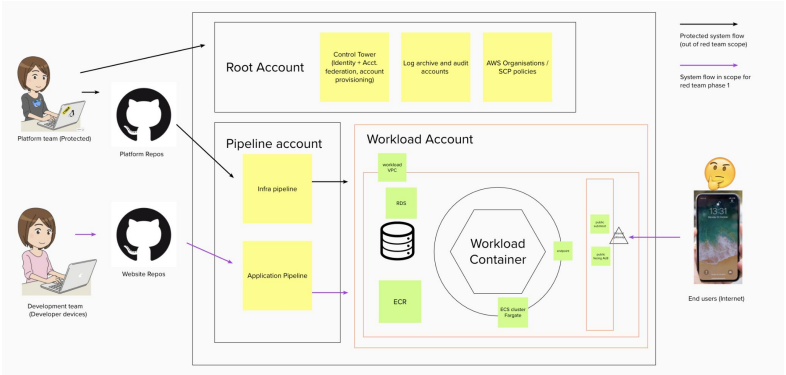
What we learned from it:

- NS for a domain bought via Route53 need to match the NS in the public hosted zone used for it

Website at https://www.tintulip-scenario1.net/greeting

Kickoff with Red Team

- Agreed next steps
  - Run "best practice" tooling against AWS
  - Set up shared spreadsheet for coordination
  - Catch up this week re logistics for attack from malicious developer (aim next week start)
- AWS Audit access for David configured via SSO



Red Team findings

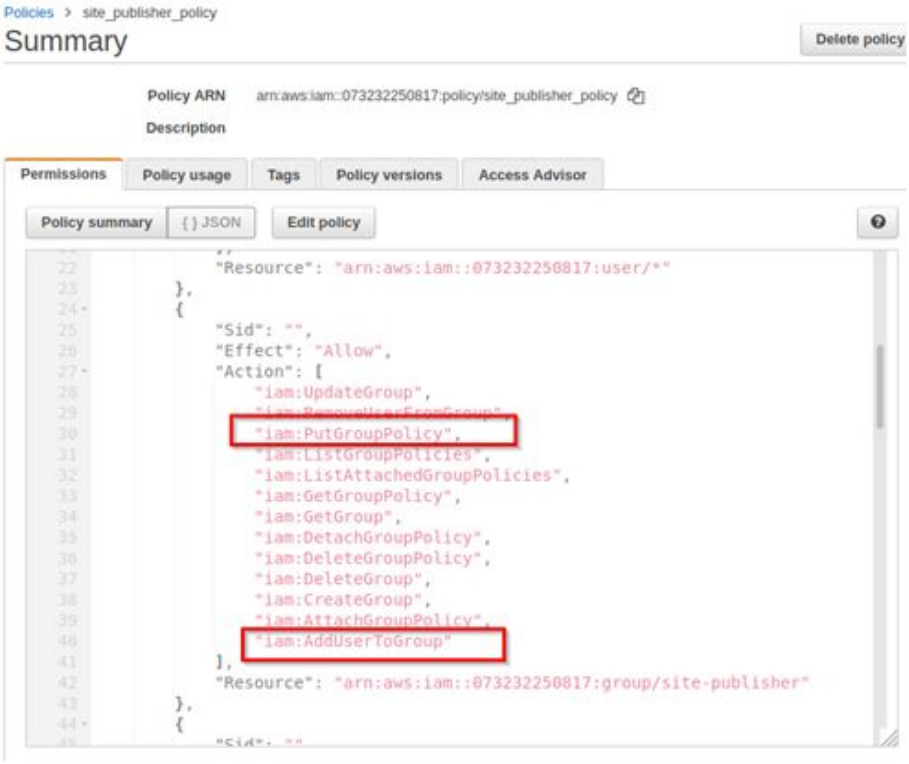
Scenario 0:

Permissions of website-infra role can be escalated to full admin.

```
aws sts assume-role \
  --role-arn arn:aws:iam::073232250817:role/website-infra \
  --role-session-name AssumeRole
```

```
aws iam add-user-to-group \
  --user-name website-infra \
  --group-name site-publisher
```

```
aws iam put-group-policy \
  --group-name site-publisher \
  --policy-name Admin \
  --policy-document file://<(cat <<EOF
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "Admin",
           "Effect": "Allow",
           "Action": "*",
           "Resource": "*"
       }]
}
EOF
)
```



What's next?

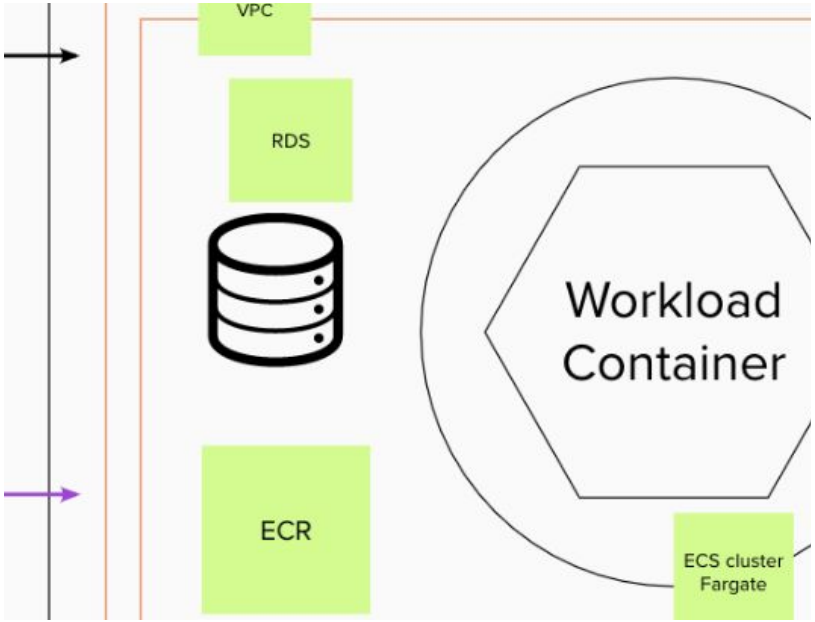
What's next

What we are working on:

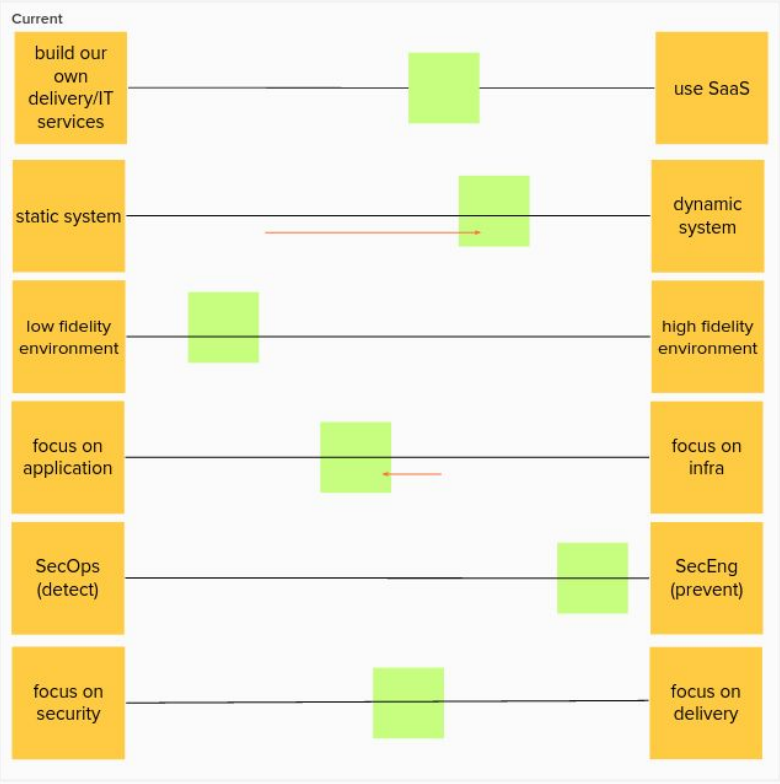
- Adding a database to Scenario 1
- Tighten controls around Scenario 1

Next steps to enable Red Team

- Login as a Development team user
- Agree flags
- Agree wash up calls
- *Any other logistics ?*



Tradeoff Sliders review



- Focussed on enabling red team engagement
- Will expand the application to make use of a database
- Introducing a database will make the system more dynamic

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