ThoughtWorks®

Cabinet Office

Tin Tulip - Blue team

Showcase #2 - April 28

Agenda

Our first retrospective!

What we achieved

What’s next?

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

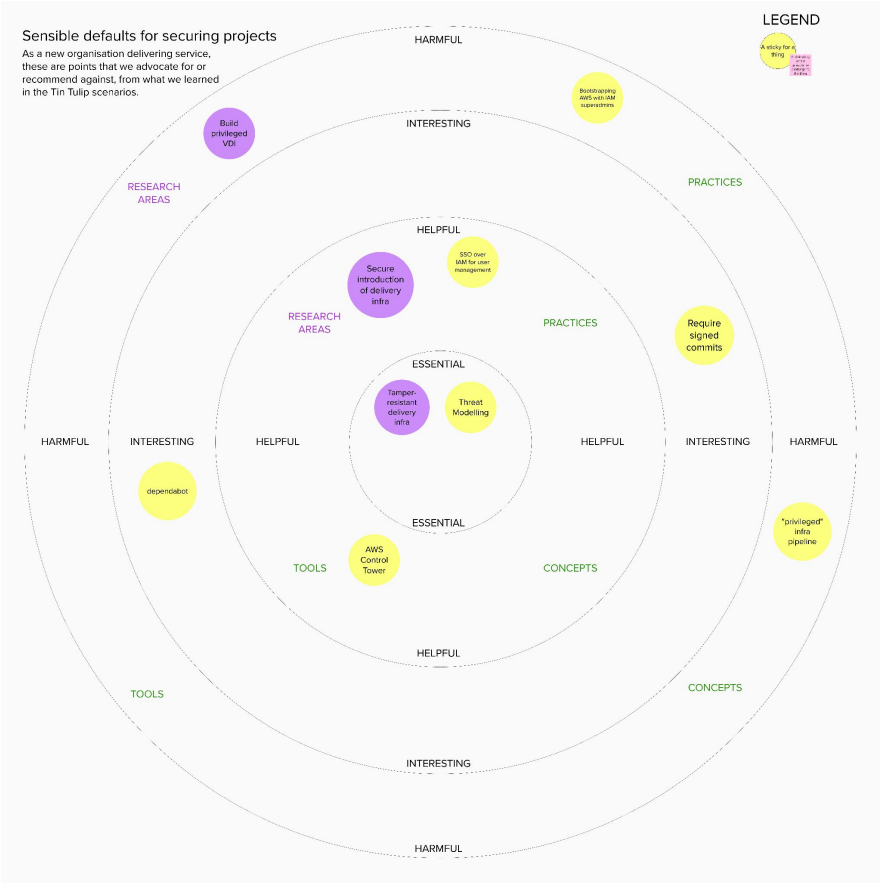
Guiding principle for communicating learnings

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

What we achieved

What we worked on

- GitHub Org Security Controls
- Control Tower
- Infra pipeline managed by platform team



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

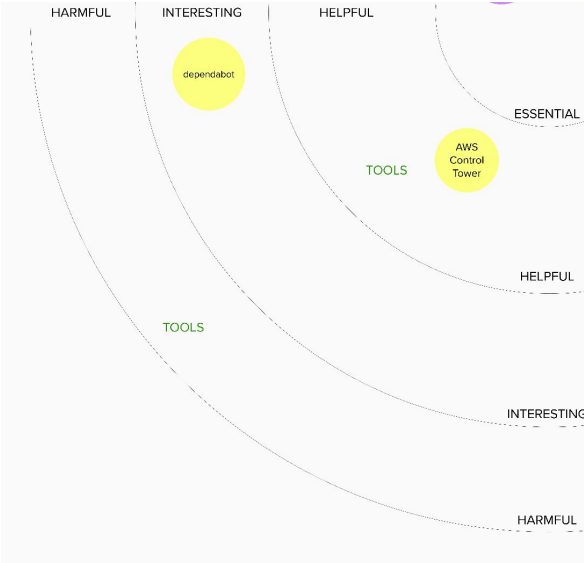
GitHub Org Security Controls

What we built:
Enabled various security settings within a GitHub Org

Why we built it:
To implement NCSC principle of secure development and deployment

What we learned from it:

- Enforcing MFA
- dependabot
- Branch Protection
- Signing Commits
- Verified Actions



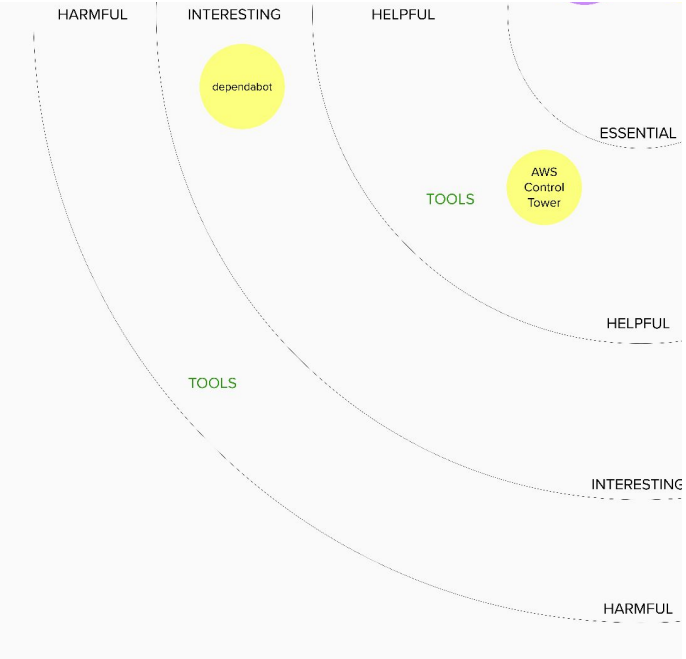
AWS Control Tower

What we built:
A best-practice AWS Org using Control Tower

Why we built it:
Adopting existing best practice for AWS security and scalability

What we learned from it:

- Control Tower is an excellent tool to "bootstrap" an AWS Org and have guardrails from day 1
- AWS SSO is recommended for user management
- CT enables less security tooling that we expected, more about compliance and configuration



Infra Pipeline managed by platform team

What we built:

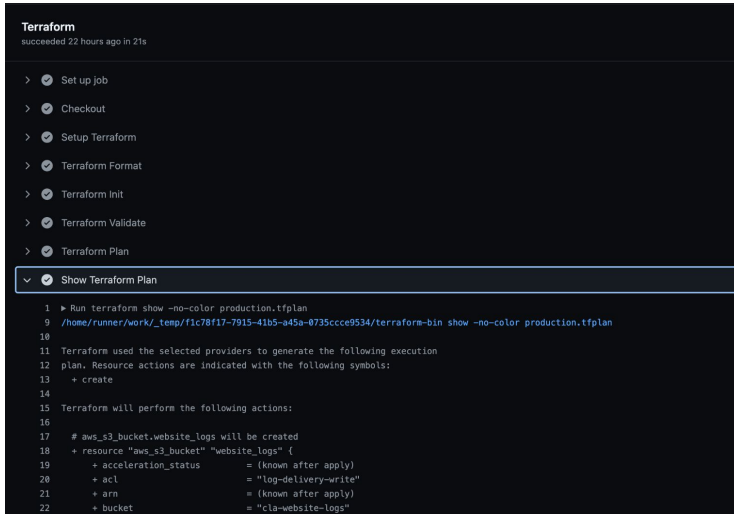
A CI/CD pipeline using github actions to deploy code.

Why we built it:

Stand-up infrastructure for team Mozart (CLA web team)

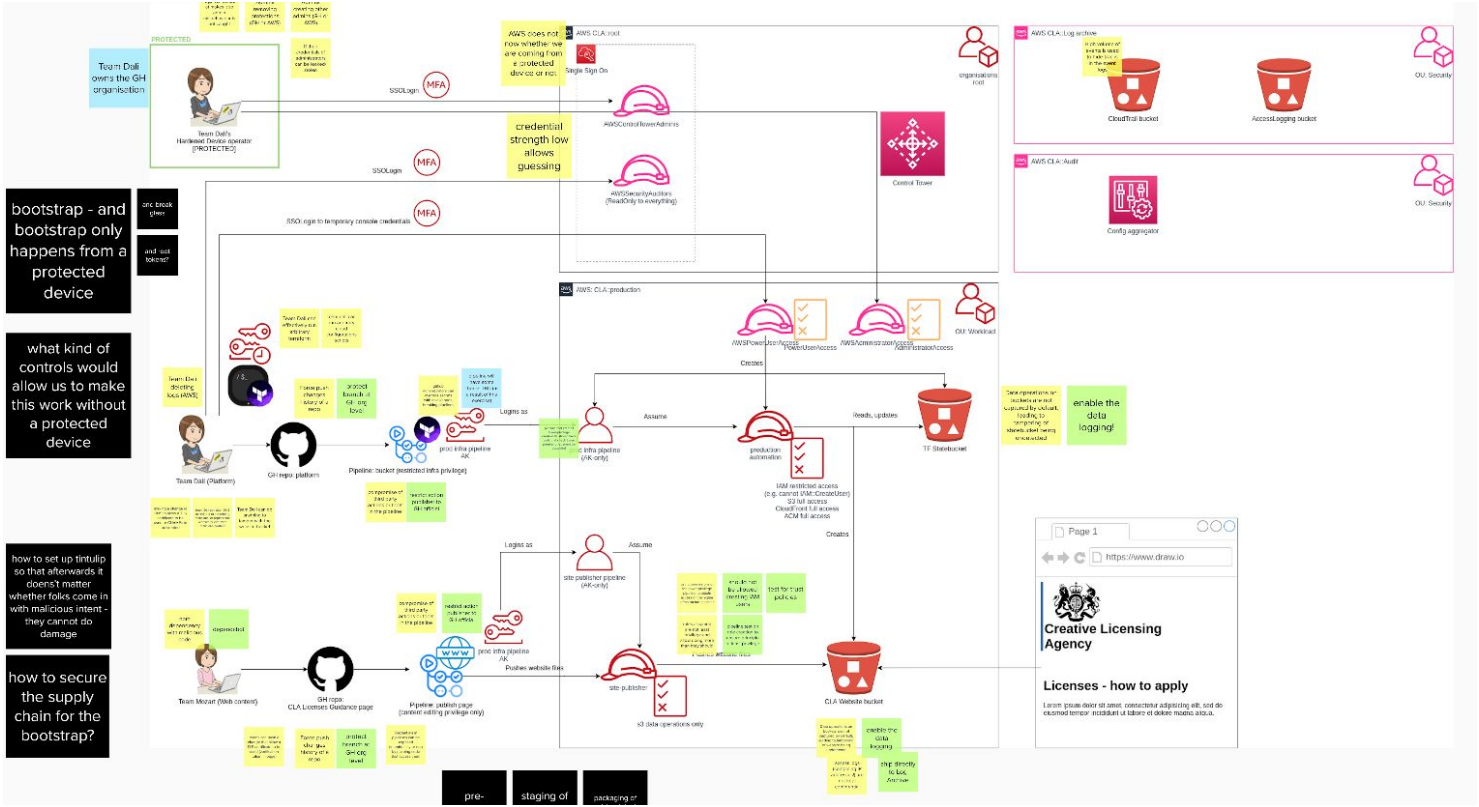
What we learned from it:

- To create the pipeline, there are four components required.
- Can restrict who can push to particular branches to trigger the pipeline.
- Static credentials stored in GitHub secrets need to be rotated every 90 days.



Threat modelling #2

Threat Modelling

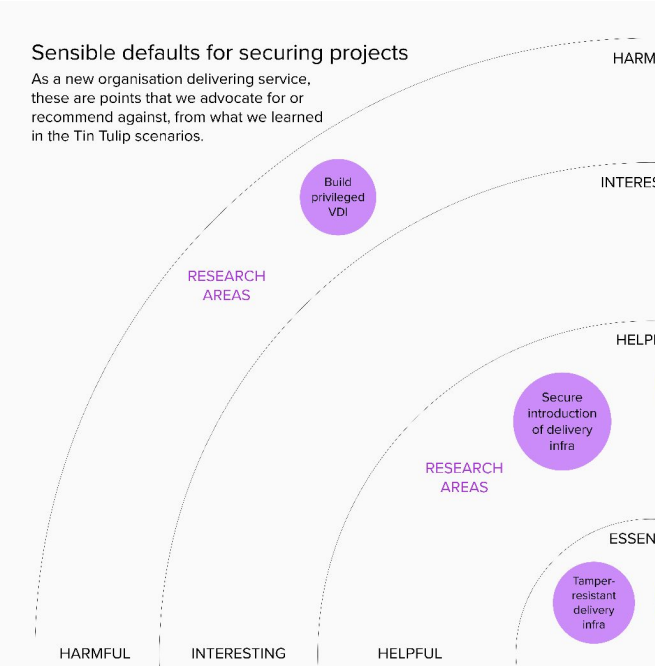


View full article [on GitHub]

Threat Modelling

Key takeaways:

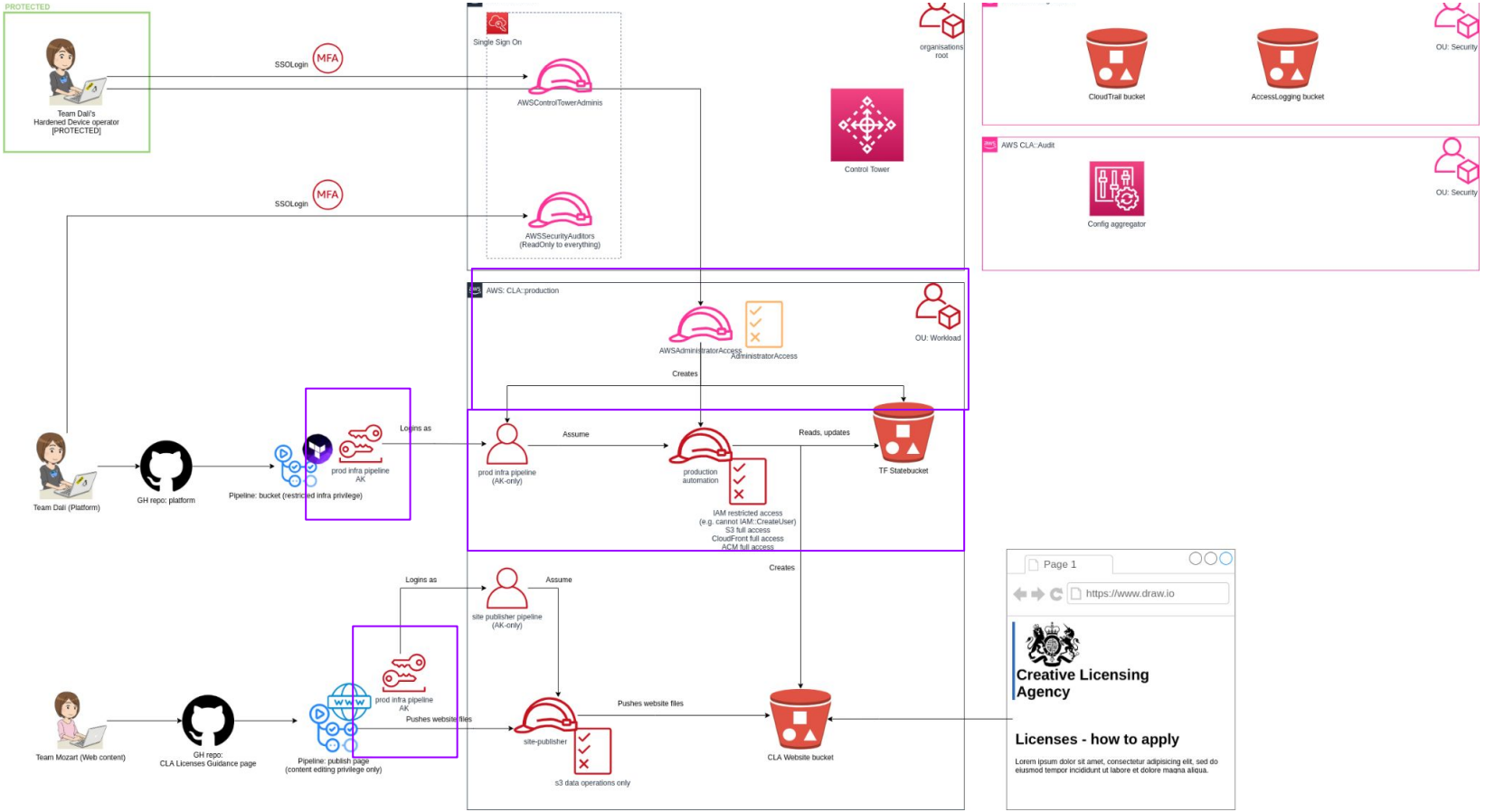
- Modelling Protected devices on Rosa would make learnings too specific
- Main interest is how to make CLA's delivery infrastructure resistant to compromised engineers
- Second main interest is secure introduction of the delivery infrastructure



What’s next?

Options for prioritisation

- How to make an infra pipeline on GH Actions resistant to spoofing
  - Assuming secure introduction of delivery infra
  - Reusable on any other CI/CD that uses Access Keys to interact with AWS
- How to make an infra pipeline for a website tamper-resistant
  - Assuming secure introduction of delivery infra
- How to have secure introduction of a delivery infra for a pipeline
  - Assuming we have protected devices that can run tooling
  - No assumptions around security of the supply chain of dev tooling and code on said devices
- How to make updates to delivery infrastructure tamper-resistant
  - Assuming we have an automated, secure introduction of the delivery infrastructure


PROTECTED
Team Dali's
Hardened Device operator
[PROTECTED]
SSOLogin
MFA
Single Sign On
AWSControlTowerAdminis
organisations root
Control Tower
CloudTrail bucket
AccessLogging bucket
OU: Security
AWS CLA::Audit
Config aggregator
OU: Security
SSOLogin
MFA
AWSSecurityAuditors
(ReadOnly to everything)
AWS: CLA::production
OU: Workload
AWSAdministratorAccess
AdministratorAccess
Creates
Team Dali (Platform)
GH repo: platform
Pipeline: bucket (restricted infra privilege)
prod infra pipeline
AK
Logins as
prod infra pipeline
(AK-only)
Assume
production
automation
Reads, updates
TF Statebucket
IAM restricted access
(e.g. cannot IAM::CreateUser)
S3 full access
CloudFront full access
ACM full access
Creates
Logins as
site publisher pipeline
(AK-only)
Assume
Team Mozart (Web content)
GH repo:
CLA Licenses Guidance page
Pipeline: publish page
(content editing privilege only)
prod infra pipeline
AK
Pushes website files
site-publisher
Pushes website files
s3 data operations only
CLA Website bucket
Page 1
https://www.draw.io
Creative Licensing
Agency
Licenses - how to apply
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do
eiusmod tempor incididunt ut labore et dolore magna aliqua.