ThoughtWorks®

Cabinet Office

Tin Tulip - Blue team

Showcase #6 - May 26

Agenda

What we achieved

Threat Modelling #4 recap

What’s next?

Summary

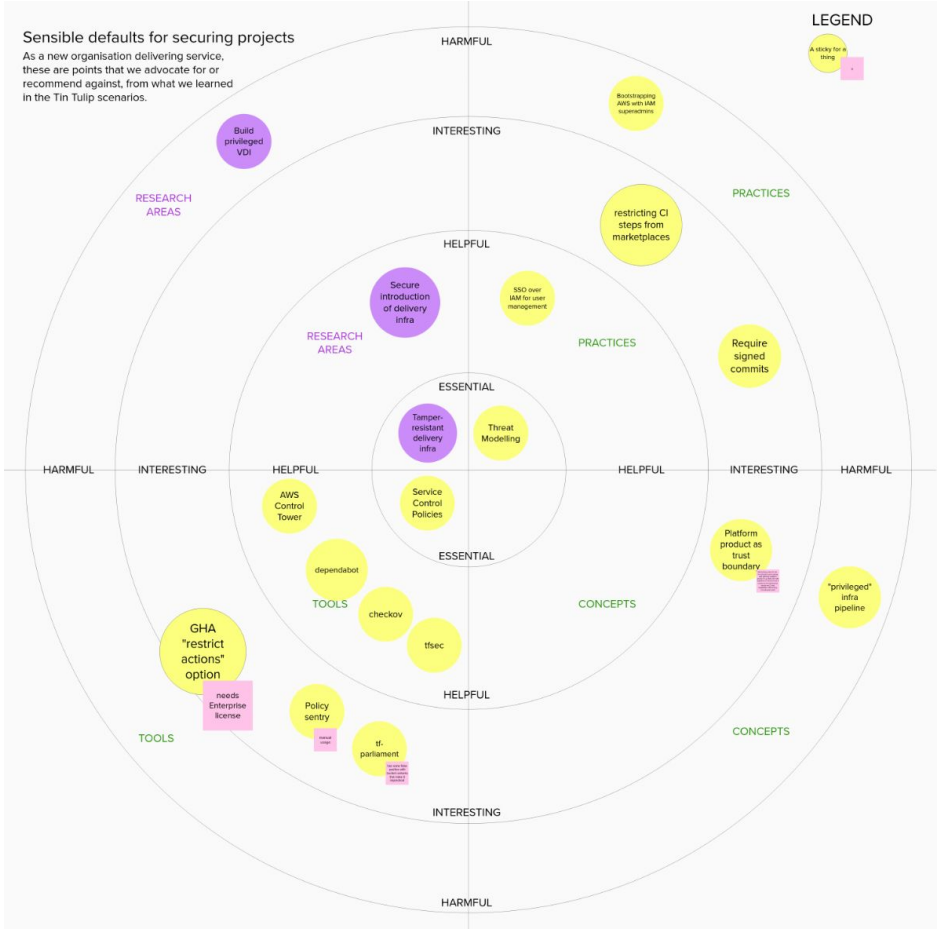
CLA's website is now available to the public.

The platform team improved security controls across the organisation and has now started working on pipeline security and the build of a "licensing service".

What we achieved

What we worked on

- Enabled GuardDuty in all regions
- Cross account log replication
- Groundwork for trusted pipeline



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

GuardDuty in all regions

What we built:

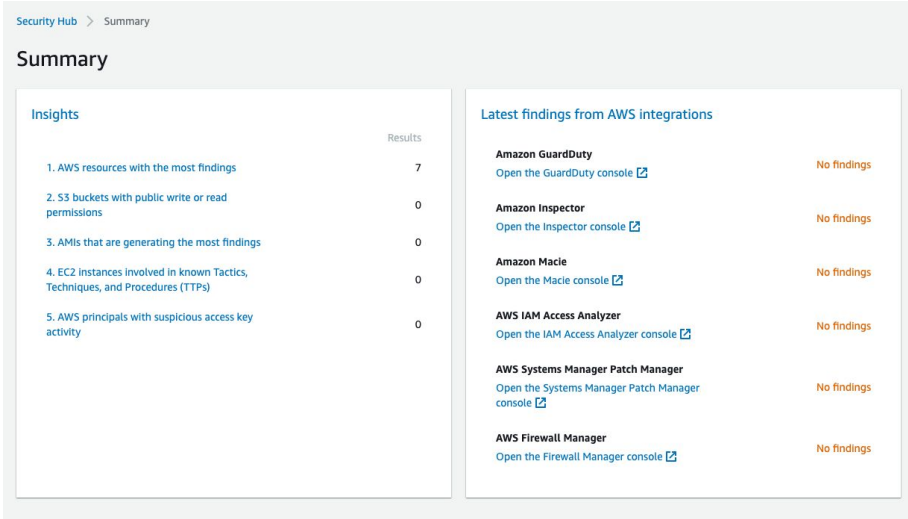
Enabled GuardDuty for all AWS accounts in all enabled regions in the organisation from a centralised security account.

Why we built it:

Provides a governance framework that monitors threats and issues detailed findings of affected resource.

What we learned from it:

- Only charged for usage so no findings = no cost.
- Combines well with SCP to restrict actions in every Region - use security hub for a centralised view



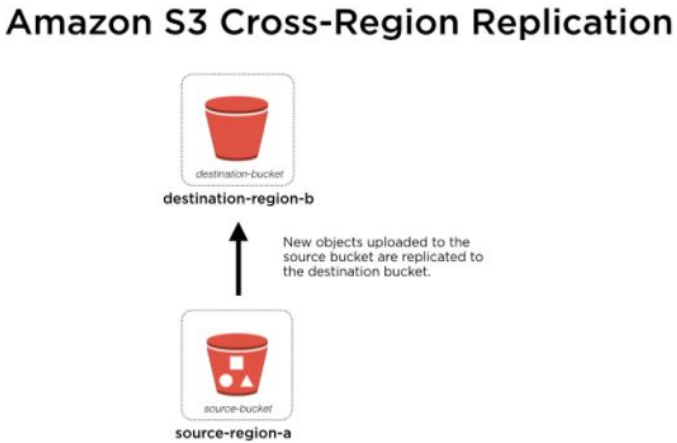
Cross Account log replication

What we built:
S3 bucket in the log-archive account containing replicated logs from the production logs bucket with lifecycle rules

Why we built it:
Central place for logging in the log archive account configured by Control Tower

What we learned from it:

- A role (created in the workload account) with cross-account abilities is required
- Using the default AWS Kms key for encryption resulted in cross account replication errors resolved by issuing our own key
- Objects are encrypted by an AWS Kms customer master key during replication



Zoomable diagram available on Github at [this link]

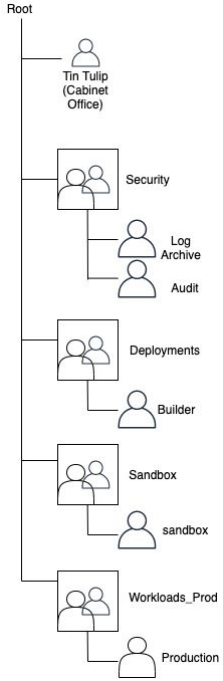
Groundwork for Trusted Pipeline

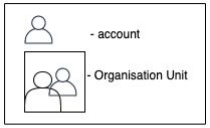
What we built:
Built foundation for Trusted pipeline including account, stub repo creation and OU structuring.

Why we built it:
Highly trusted environment to build infrastructure in workload environments.

What we learned from it:

- Nested OU not possible with Control Tower
- For CI/CD as a separate function AWS recommends a deployment OU

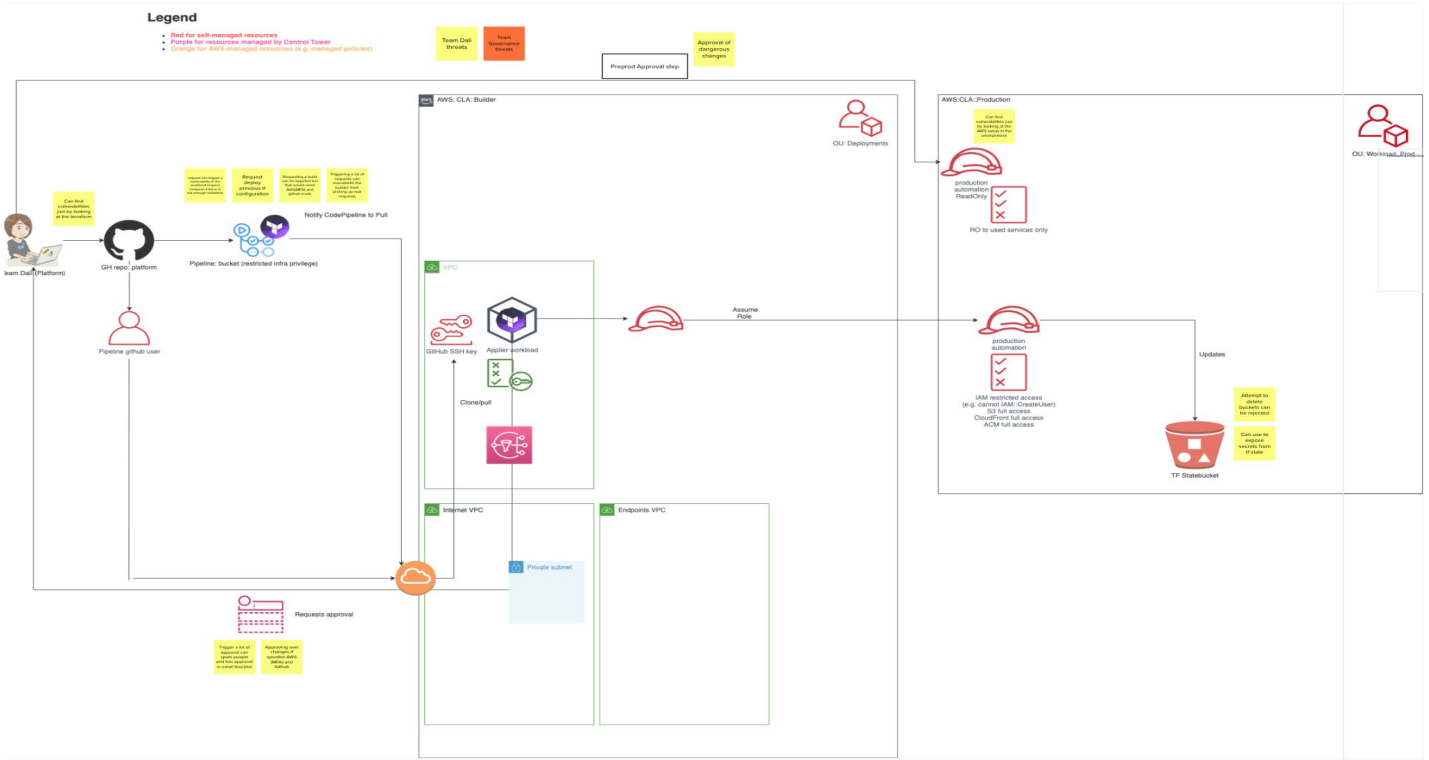




Zoomable diagram available on Github at [this link]

Threat Modelling #4 - recap

Threat Modelling



View full article [on Github]

Threat Modelling

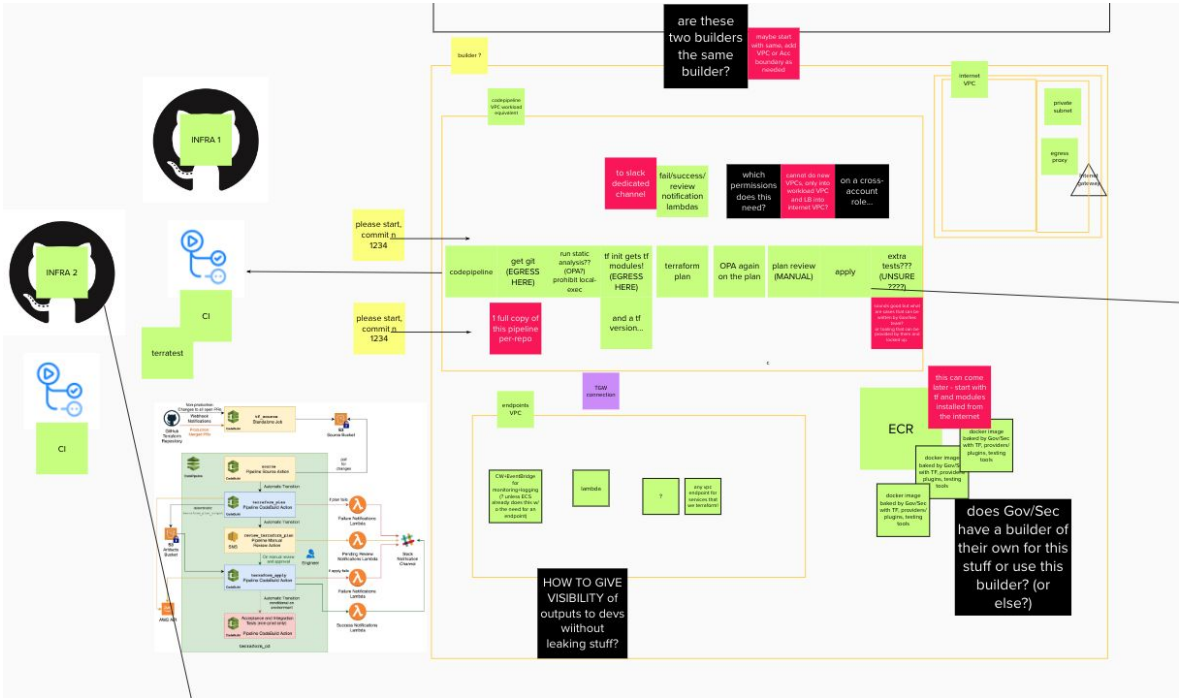
Key takeaways:

- Approval of dangerous changes being made to production prevented by using
  - a pre-prod account for validation
  - having a two person approval mechanism in place
- Attempt to delete state buckets from the workloads environment should be rejected.
- Account isolation from production to builder mitigates many pipeline threats identified in scenario 0

What's next?

Scenario 1 Architecture Session

[Mural Board]



Tradeoff Sliders review

- Laying the foundation for trusted pipeline

Sliders tracker (link requires access):

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

Options for prioritisation

1 - Trustable pipelines:

Follow ups from Threat Modelling - improve scenario 0 pipelines - improve tamper-resistance.

2 - Scenario 1:

Build towards CLA's "Apply for a Creative License" service

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