



Tin Tulip - Blue team

Showcase #11 - July 7

Agenda

What we achieved

Threat modelling

What's next

Summary

Red team is testing Scenario 2 and 3.

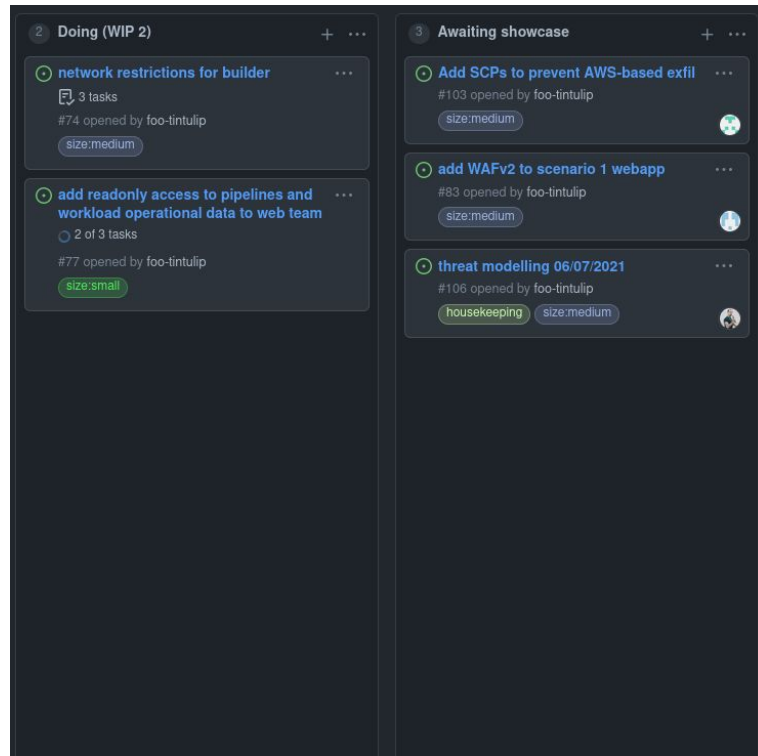
*Blue team is improving security controls in
builder account.*

What we achieved



What we worked on

- Preventing Data Exfil with SCPs
- Web Application Firewall



Preventing Data Exfil with SCPs

What we built:

A policy that prevents snapshots of the database being exported, modified or copied into external accounts.

Why we built it:

To prevent the snapshot from being used in the attackers account allowing them to steal data.

What we learned from it:

- RDS provides automated backups and manual backups which are the database snapshots.
- Can prevent EBS exfils by blocking modify-snapshot-attribute and create-volume permissions.

⊗ User: arn:aws:sts::961889248176:assumed-role/AWSReservedSSO_AWSAdministratorAccess_33b84988c90a5630/yusra.dahir+tintulip+protected@thoughtworks.com is not authorized to perform: rds:CopyDBSnapshot on resource: arn:aws:rds:eu-west-2:961889248176:snapshot:testinitalrules with an explicit deny ⊗

Web Application Firewall

What we built:

Added a second load balancer pointing to the same web application that is protected by WAF

Why we built it:

To do A/B testing and see if a WAF catches and blocks bad input

What we learned from it:

- Quick and easy to set up
- Can use AWS managed rules to cover a lot of cases
- Various attempts at probing the site have already been made

```
~ export TINTULIP_URL=https://waf.tintulip-scenario1.net
~ curl -X POST $TINTULIP_URL -F "user='AND 1=1;"
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
</body>
</html>
~ curl -X POST $TINTULIP_URL -F "user='<script><alert>Hello</alert></script>'"
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
</body>
</html>
~ curl -X GET $TINTULIP_URL
<!DOCTYPE html>
<html>
~ export TINTULIP_URL=https://www.tintulip-scenario1.net
~ curl -X POST $TINTULIP_URL -F "user='<script><alert>Hello</alert></script>'"
{"timestamp":"2021-07-07T09:27:06.487+00:00","status":405,"error":"Method Not Allowed"}
~ curl -X POST $TINTULIP_URL -F "user='AND 1=1;"
{"timestamp":"2021-07-07T09:27:28.857+00:00","status":405,"error":"Method Not Allowed"}
```

Metric name	URI	Rule inside rule group	Action	Time
common-rule-set	/	AWS#AWSManagedRuleSet#CrossSiteScripting_BODY	BLOCK	Fri Jul 02 2021 11:58:31 GMT+0100 (British Summer Time)
sql-database-rule-set	/	AWS#AWSManagedRuleSet#SQL_BODY	BLOCK	Fri Jul 02 2021 11:58:33 GMT+0100 (British Summer Time)
sql-database-rule-set	/	AWS#AWSManagedRuleSet#SQL_BODY	BLOCK	Fri Jul 02 2021 11:58:22 GMT+0100 (British Summer Time)
sql-database-rule-set	/	AWS#AWSManagedRuleSet#SQL_BODY	BLOCK	Fri Jul 02 2021 11:51:14 GMT+0100 (British Summer Time)

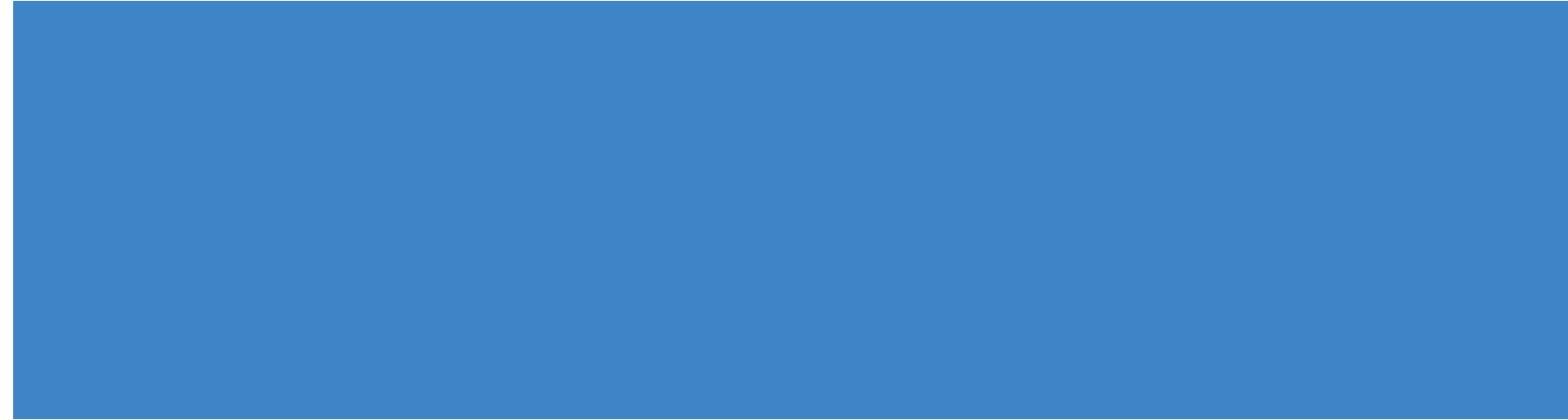
Resource available at this [Link](#)

Red team update

The image shows a Jira board with two columns: 'To do' and 'In progress'. Each column has a header with a number in a circle, a title, and icons for adding and more options. The 'To do' column has two tasks, and the 'In progress' column has one task. Each task card includes a title with a green circle icon, a description, and the text '#opened by jg-co'. The 'In progress' task also includes an assignee icon.

Column	Task ID	Task Description	Status
To do (2)	#100	Testing of scenario 3: Assume some bad terraform gets through the pipeline and deployed. What is the blast radius?	To do
	#99	Testing of Scenario 4: What if Rob from Red team was an evil developer on the Platform team? Add control to infra pipeline	To do
In progress (1)	#98	Testing of Scenario 2: Assume some bad code gets through the pipeline and into the web-application. What is the blast radius?	In progress

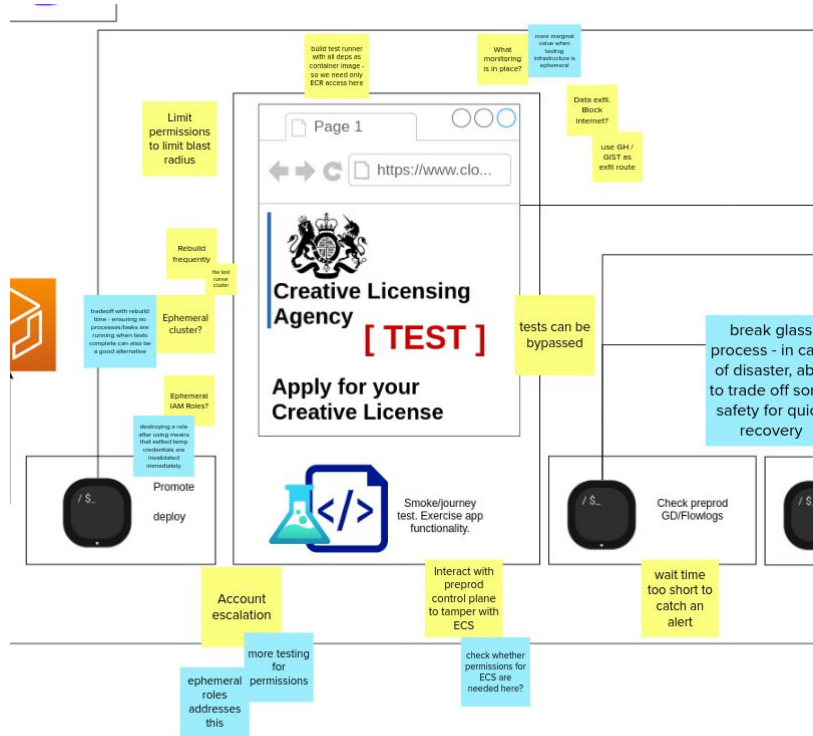
Threat modelling #3 - recap



Threat Modelling

On running tests in Trusted Pipelines:

- Networking restrictions remain strong control
- Pre-building a test runner container cuts some networking requirements
- Running tests on ephemeral compute and roles limits exposure



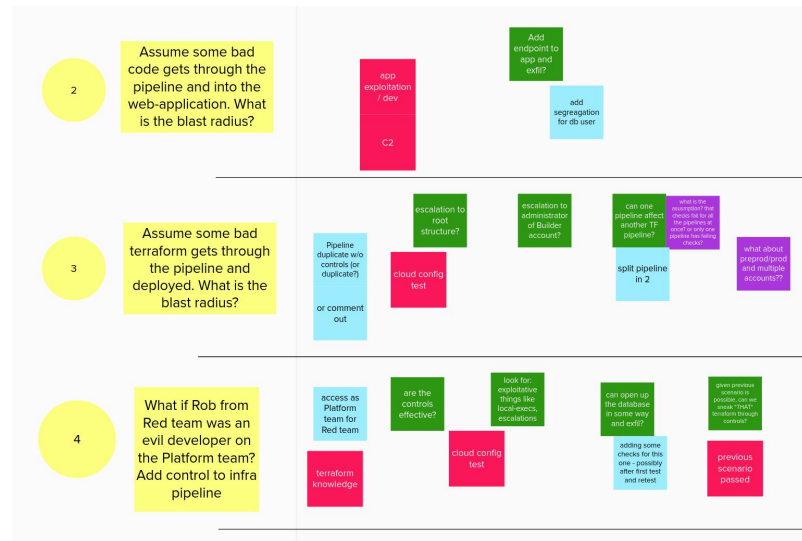
What's next



Next scenarios tested

In running order:

- IN PROGRESS
Assume some bad code gets through the pipeline and into the web-application. What is the blast radius?
- ☐ STARTING TODAY
Assume some bad terraform gets through the pipeline and deployed. What is the blast radius?
- Assume a Platform developer has malicious intent. Can they bypass automated checks and add malicious Terraform?



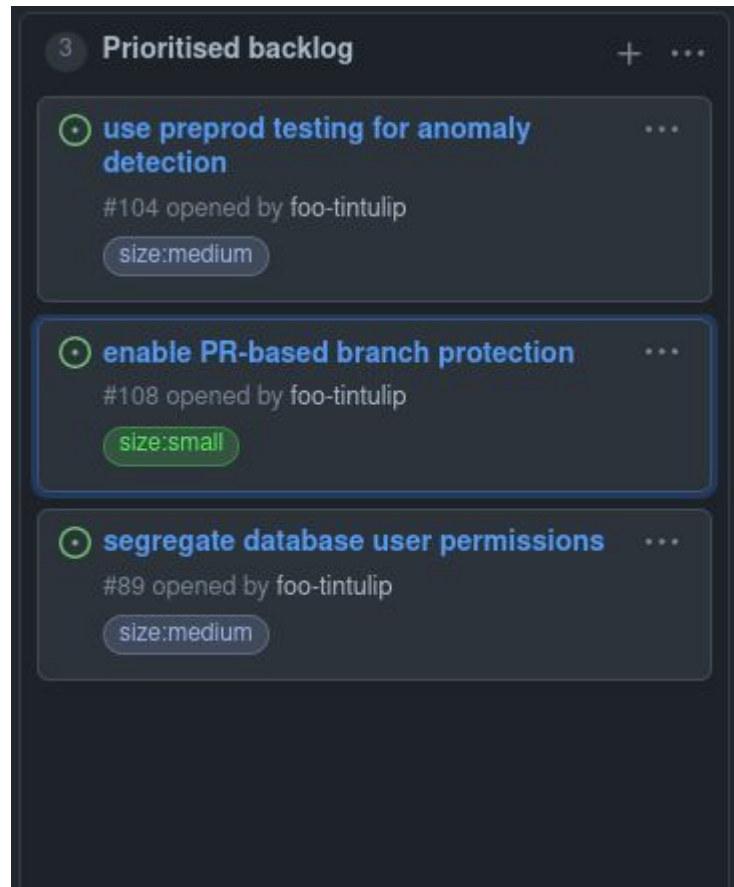
Public showcase next week

- **3pm Wednesday 14th July**
- **Progress update**
- **Planning next week**
 - **Phil / Foo / Breandan availability?**
- **Invite**
 - **73 invited**
 - **Can invite others**
 - **19 yes so far (only send this morning)**
 - **4 maybe**
 - **47 awaiting**

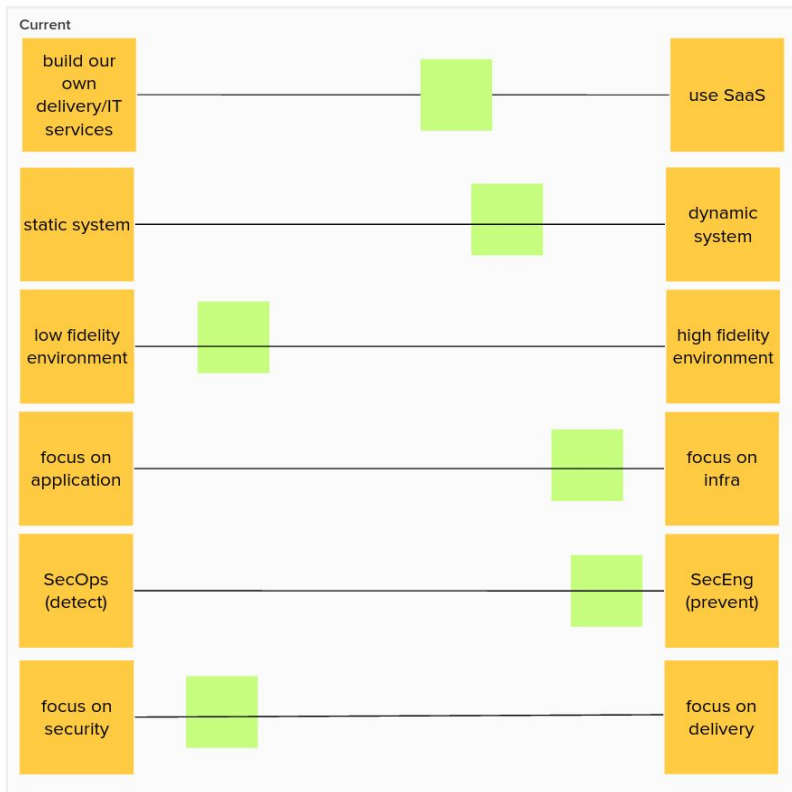
Next priorities for Blue team

In order:

- Limit egress from builder to a SaaS artifact repository
- Introduce technical controls around two pairs of eyes
- Introduce anomaly detection in preproduction application testing
- Something else?



Tradeoff Sliders review



- Stable since last 2 weeks
 - Focus on security controls on existing infra

Sliders tracker (link requires access):

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

Thank you!

