ThoughtWorks®

Cabinet Office

Tin Tulip - Blue team

Showcase #12 - July 21

Agenda

What we achieved

What's next

Summary

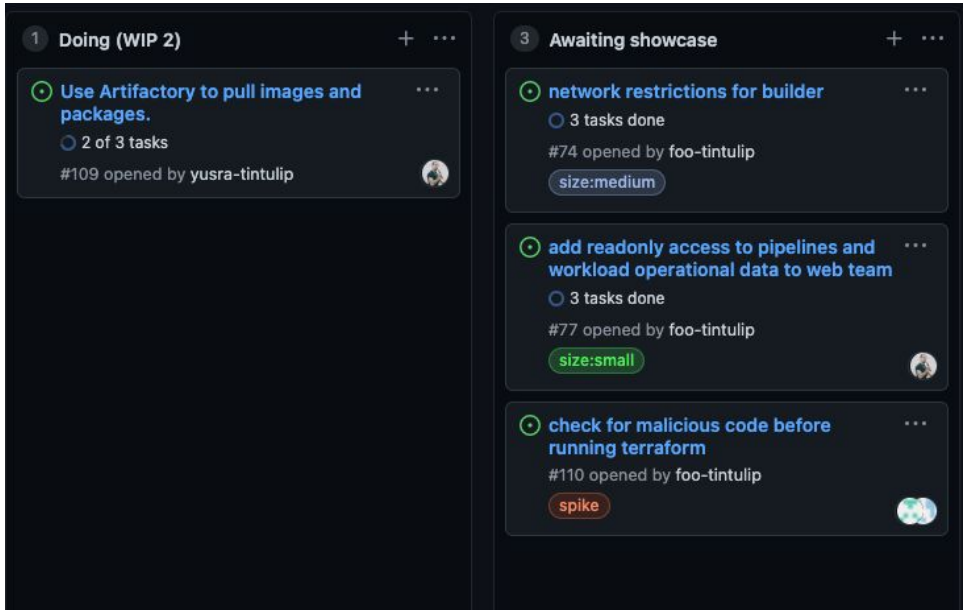
Red team is testing Scenario 2 and 3.

Blue team is improving security controls in builder account.

What we achieved

What we worked on

- Network Restrictions for Builder Account
- Read-only access for web team
- Checking for malicious code



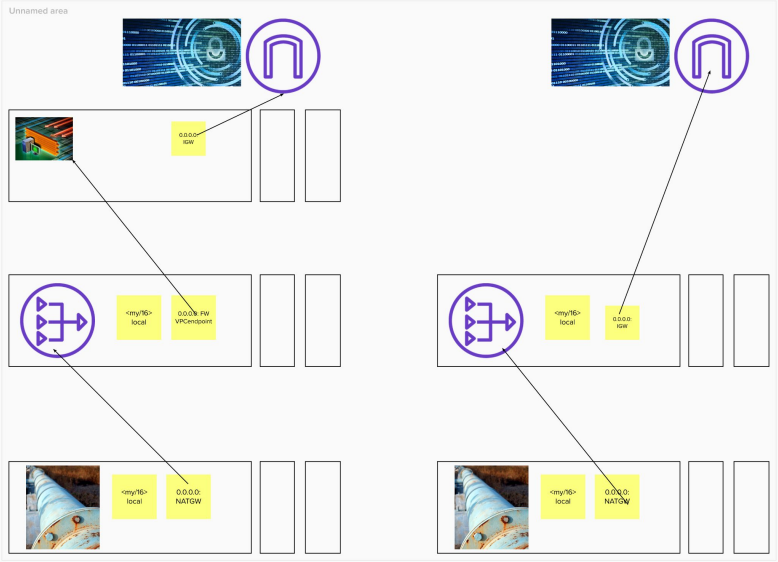
Network Restrictions for the Builder Account

What we built:
A network firewall which permits or block traffic from the VPC to the external Internet

Why we built it:
Prevent C2 from happening e.g. exfil data from the builder or attempt to escalate from within

What we learned from it:

- The Terraform VPC module needs to be modified due to the additional subnets required
- The Network Firewall has an allowlist for domains - this would need to be modified everytime there is a new supply chain




```
[Container] 2021/07/08 16:19:40 Running command wget -nv https://github.com/open-policy-
agent/conftest/releases/download/v0.25.0/conftest_0.25.0_Linux_x86_64.tar.gz
2021-07-08 16:19:41 URL:https://github-releases.githubusercontent.com/178249461/20a5a000-af4d-11eb-9830-dba4340a6b2c?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210708%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20210708T161940Z&X-Amz-Expires=300&X-Amz-Signature=f1f19dd3a033653cbf9a8577d09217a7a2f1fb671e318c51fa33f3b25615571a&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=178249461&response-content-
disposition=attachment%3B%20filename%3Dconftest_0.25.0_Linux_x86_64.tar.gz&response-content-type=application%2Foctet-stream
[11731631/11731631] -> "conftest_0.25.0_Linux_x86_64.tar.gz" [1]

[Container] 2021/07/08 16:19:41 Running command tar xzf conftest_0.25.0_Linux_x86_64.tar.gz

[Container] 2021/07/08 16:19:42 Running command wget -nv
https://gist.githubusercontent.com/brandonb927/3195465/raw/0c0b99dca7bd3ca43ba33e8f0a659d9841b0a2ed/osx-for-hackers.sh
Unable to establish SSL connection.
```

Resource available at this Link

Checking for malicious code

```
Status: Downloaded newer image for tintulip.jfrog.io/docker-remote/returntocorp/semgrep:latest
using config from https://semgrep.dev/p/java. Visit https://semgrep.dev/registry to see all public rules.
downloading config...
running 30 rules...
/src/src/main/java/com/tintulip/webapplication/user/UserRestController.java
severity:error rule:policies.command_injection: User controlled strings in exec() will result in command execution.
30:            var process = Runtime.getRuntime().exec(decoded);
ran 30 rules on 14 files: 1 findings

[Container] 2021/07/19 10:42:04 Command did not exit successfully docker run --rm -v "$CODEBUILD_SRC_DIR:/src" -v
"$CODEBUILD_SRC_DIR_policies/semgrep-rules/java:/policies" tintulip.jfrog.io/docker-remote/returntocorp/semgrep -c="p/java" -
c="/policies" /src --error exit status 1
[Container] 2021/07/19 10:42:04 Phase complete: BUILD State: FAILED
[Container] 2021/07/19 10:42:04 Phase context status code: COMMAND_EXECUTION_ERROR Message: Error while executing command: docker run
--rm -v "$CODEBUILD_SRC_DIR:/src" -v "$CODEBUILD_SRC_DIR_policies/semgrep-rules/java:/policies" tintulip.jfrog.io/docker-
remote/returntocorp/semgrep -c="p/java" -c="/policies" /src --error. Reason: exit status 1
```

What we built:
Introduced semgrep and custom rules to check against source code

Why we built it:
Lightweight check against the source code to flag any issues before executing anything that is attacker controlled

```
using config from https://semgrep.dev/p/terraform. Visit https://semgrep.dev/registry to see all public rules.
downloading config...
running 8 rules...
/src/environments/preproduction/main.tf
severity:error rule:policies.allow-specific-provider: data external.shell_command is not allowed
399:data "external" "shell_command" {
ran 8 rules on 22 files: 1 findings

[Container] 2021/07/15 11:53:32 Command did not exit successfully docker run --rm -v "$CODEBUILD_SRC_DIR:/src" -v
"$CODEBUILD_SRC_DIR_policies/semgrep-rules:/policies" returntocorp/semgrep -c="p/terraform" -c="/policies" /src --error exit status 1
[Container] 2021/07/15 11:53:32 Phase complete: PRE_BUILD State: FAILED
[Container] 2021/07/15 11:53:32 Phase context status code: COMMAND_EXECUTION_ERROR Message: Error while executing command: docker run
--rm -v "$CODEBUILD_SRC_DIR:/src" -v "$CODEBUILD_SRC_DIR_policies/semgrep-rules:/policies" returntocorp/semgrep -c="p/terraform" -
c="/policies" /src --error. Reason: exit status 1
```

What we learned from it:

- Tfsec custom checks have less flexibility than semgrep but more focused on Terraform
- Semgrep does not support Terraform but rather you match against patterns

Resource available at this Link

Read-only access for web team

What we built:

Web team (Mozart) can now access app logs

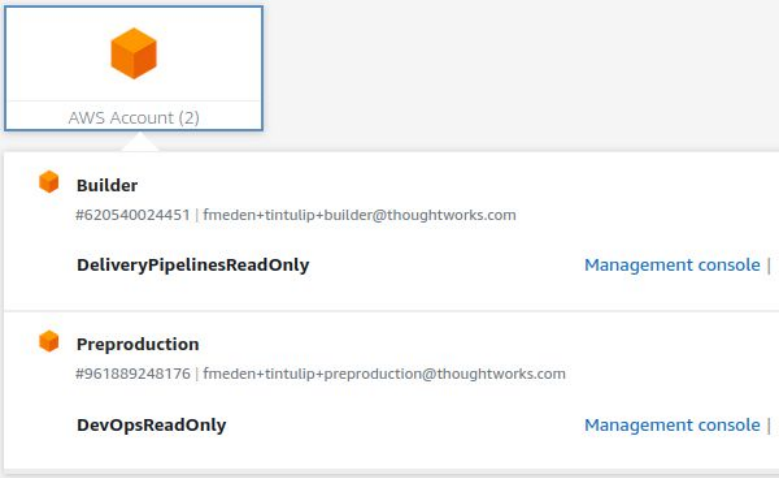
Why we built it:

Teams being able to operate their services

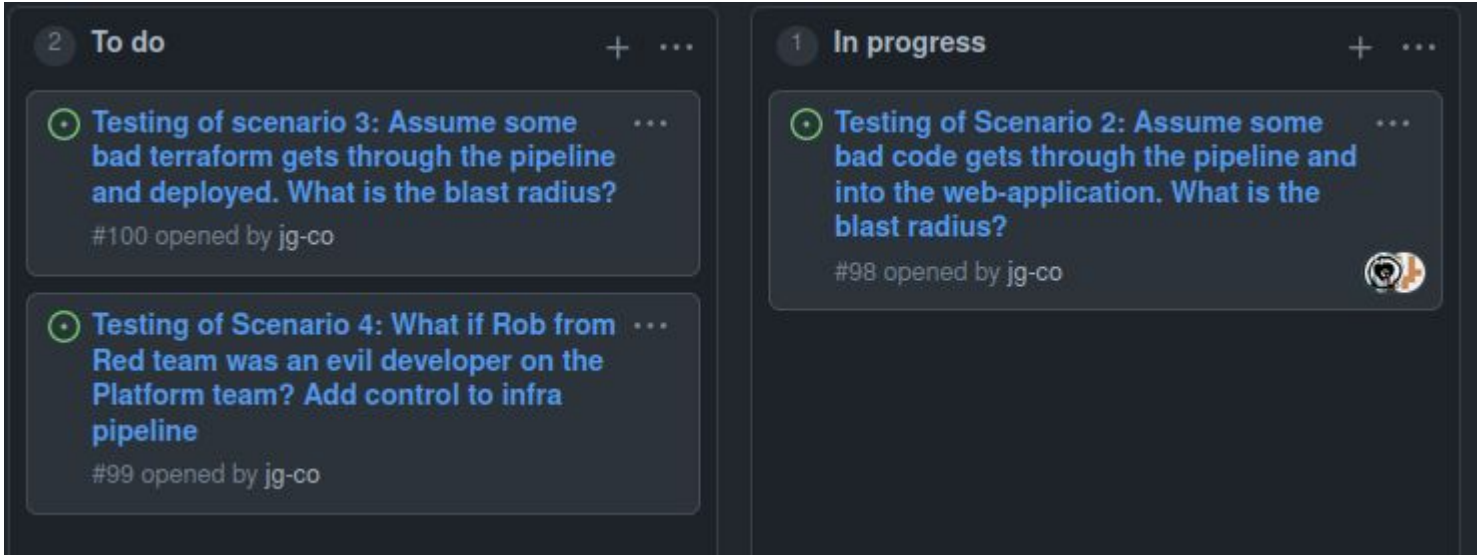
+ SSO customisations are now in TF

What we learned from it:

- AWS SSO can only have managed policy attachments + 1 inline policy



Red team update



Red team update

Scenario 2:

- Inserted web shell into application -> blocked during deployment by semgrep
- Used Reflection to obfuscate method calls -> bypasses semgrep
- Base64 input and output encoding to bypass WAF
- Able to read from environment variables, execute system commands within container, access AWS metadata service
- Temp AWS credentials didn’t get access to anything else

AWS Configuration Review

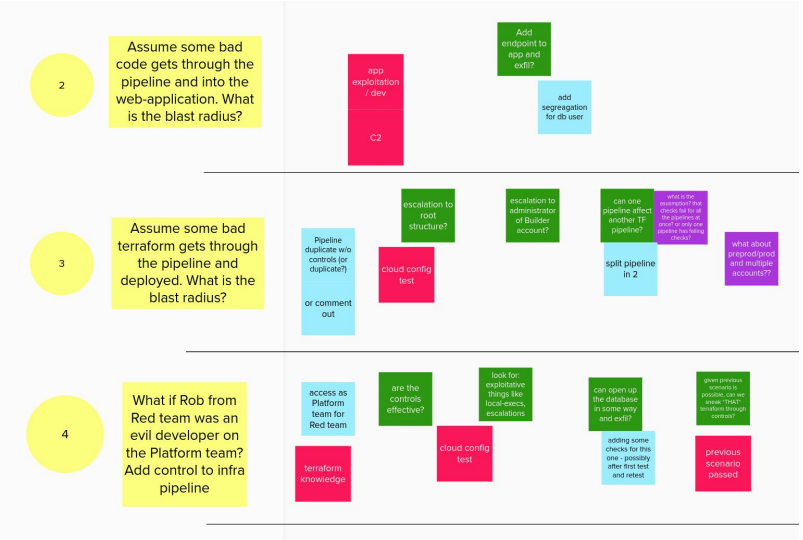
- Builder + Preproduction accounts
- Identified and in the process of documenting the issues on Github
- Issues include: Missing logging + monitoring controls / IAM (password policies etc) / Security Groups
- Primary Concern: Can an unprivileged user escalate privileges within an account

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?
- COMPLETED
  Assume some bad terraform gets through the pipeline and deployed. What is the blast radius?
- NEXT WEEK
  Assume a Platform developer has malicious intent. Can they bypass automated checks and add malicious Terraform?

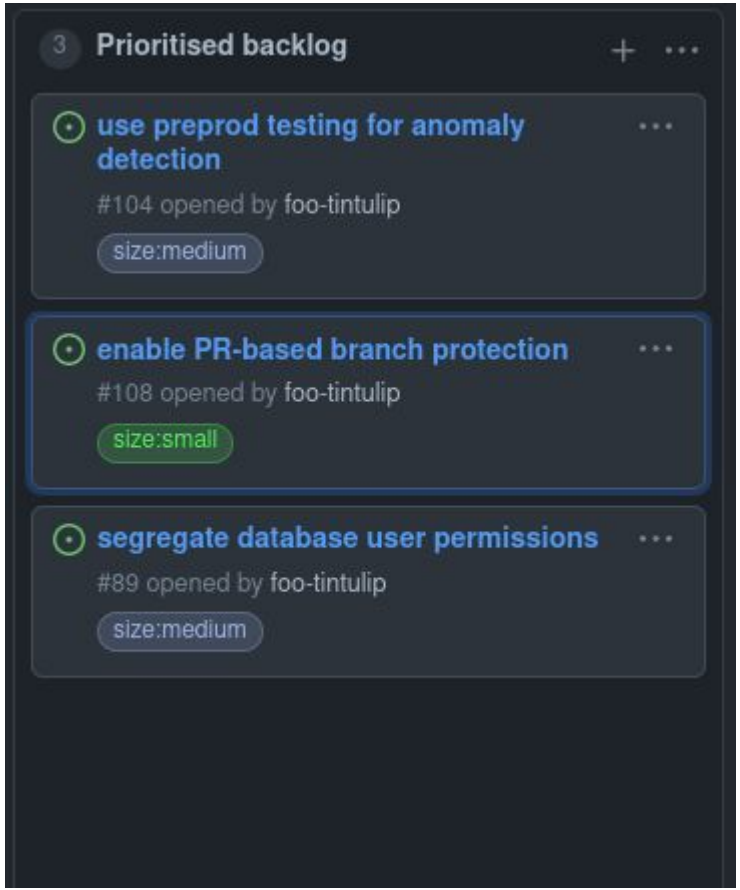


Breakdown board at [Link]

Next priorities for Blue team

In order:

- Complete Artifactory PoC
- Introduce a control for supply chain attacks
- Clean up code and documentation deliverables



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!