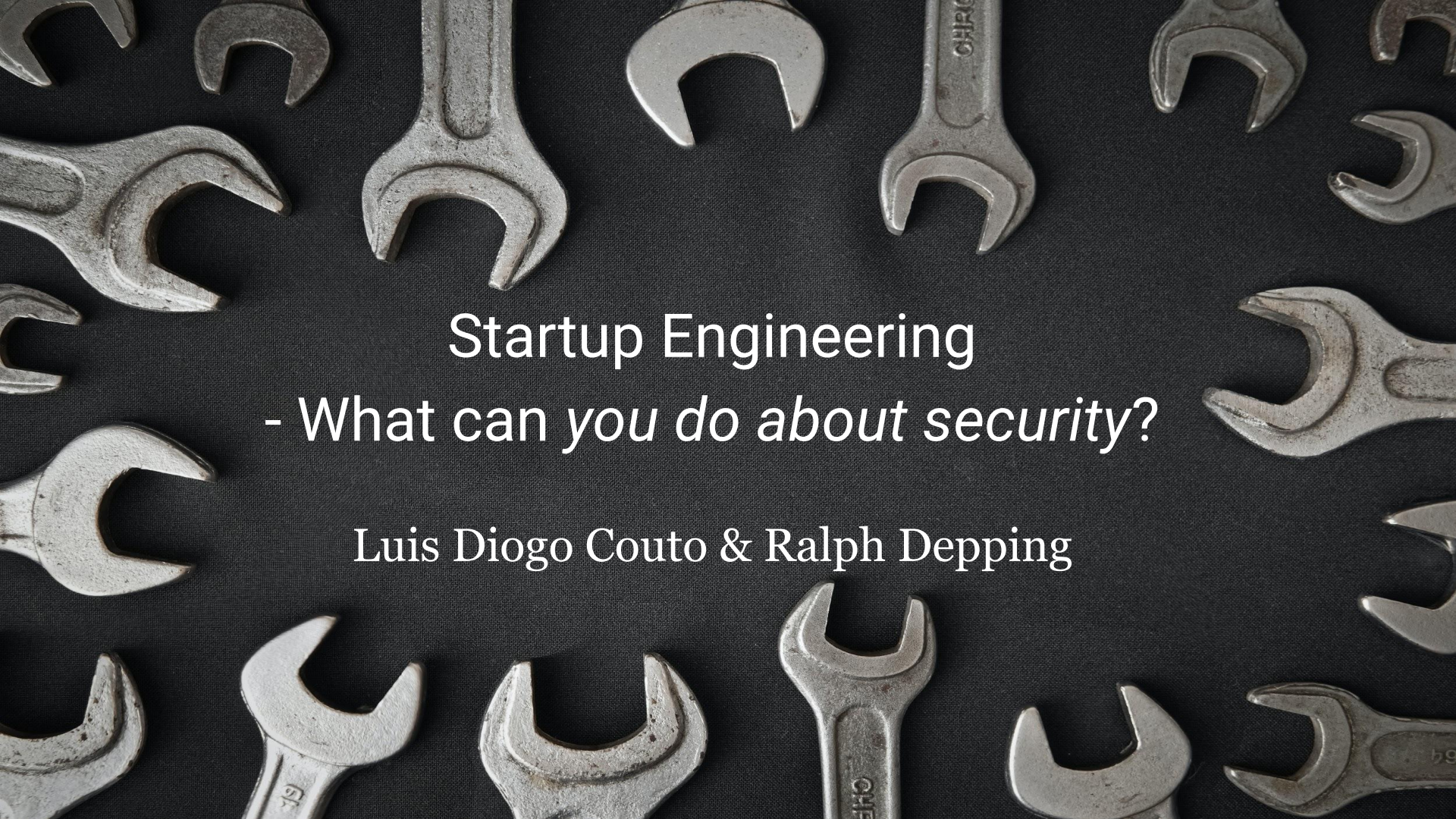


Startup Engineering
- What can *you do about security*?

Luis Diogo Couto & Ralph Depping

Secure Startup Engineering

🗻 Our Landscape

- Low bureaucracy
- Expected to do things
- Good zone of control

🗣️ Secure Software Dev

- Day to day pillar we control and affect
- Not covering ops, compliance, data protection, auth, soc2 etc.

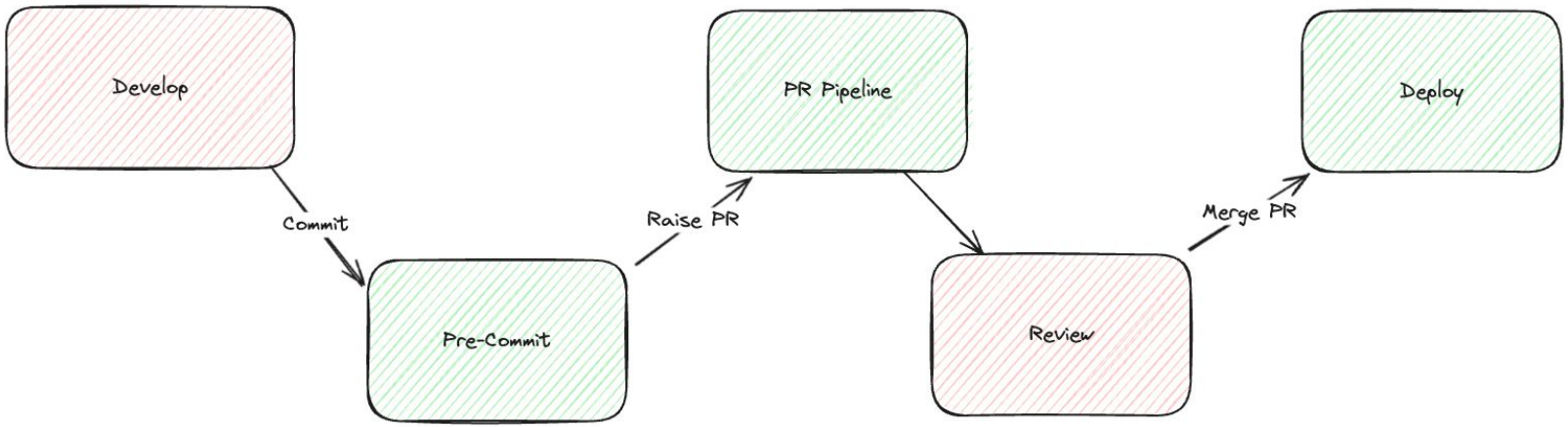
YMMV

Setup for Success

Key Guiding Principles

1. Make things as simple as possible
2. Ship all the time
3. Build tidy things we can all understand
4. Shift left with a great local development experience

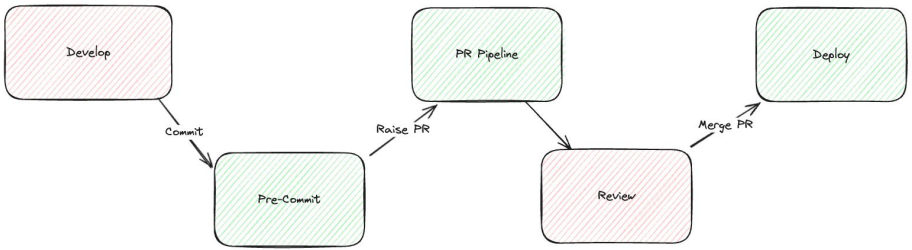
Our Flow



Practices

- Unit and component tests
- Static code analysis in pre-commit and pipeline
- Dedicated AWS stack for each PR
- Judicious component testing

Enter Docker



Ideas so far…

- 1 or 2 tools - in the right place
  - High signal to noise ratio
  - Don’t slow down going to prod

- Low maintenance - right base image
- Lint your own stuff - hadolint pre-commit
- Non-gating vulnerability scans

Secure Infrastructure

⏩ Controlling our own infrastructure is very good for flow

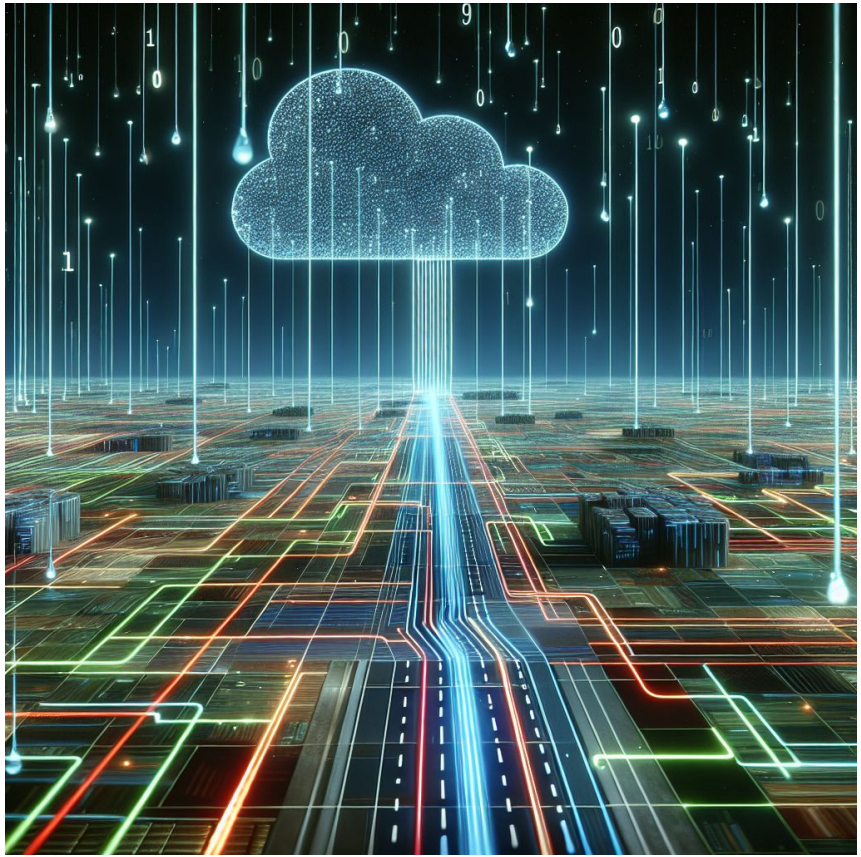
- What we need, when we need it

🔒Have to do it securely

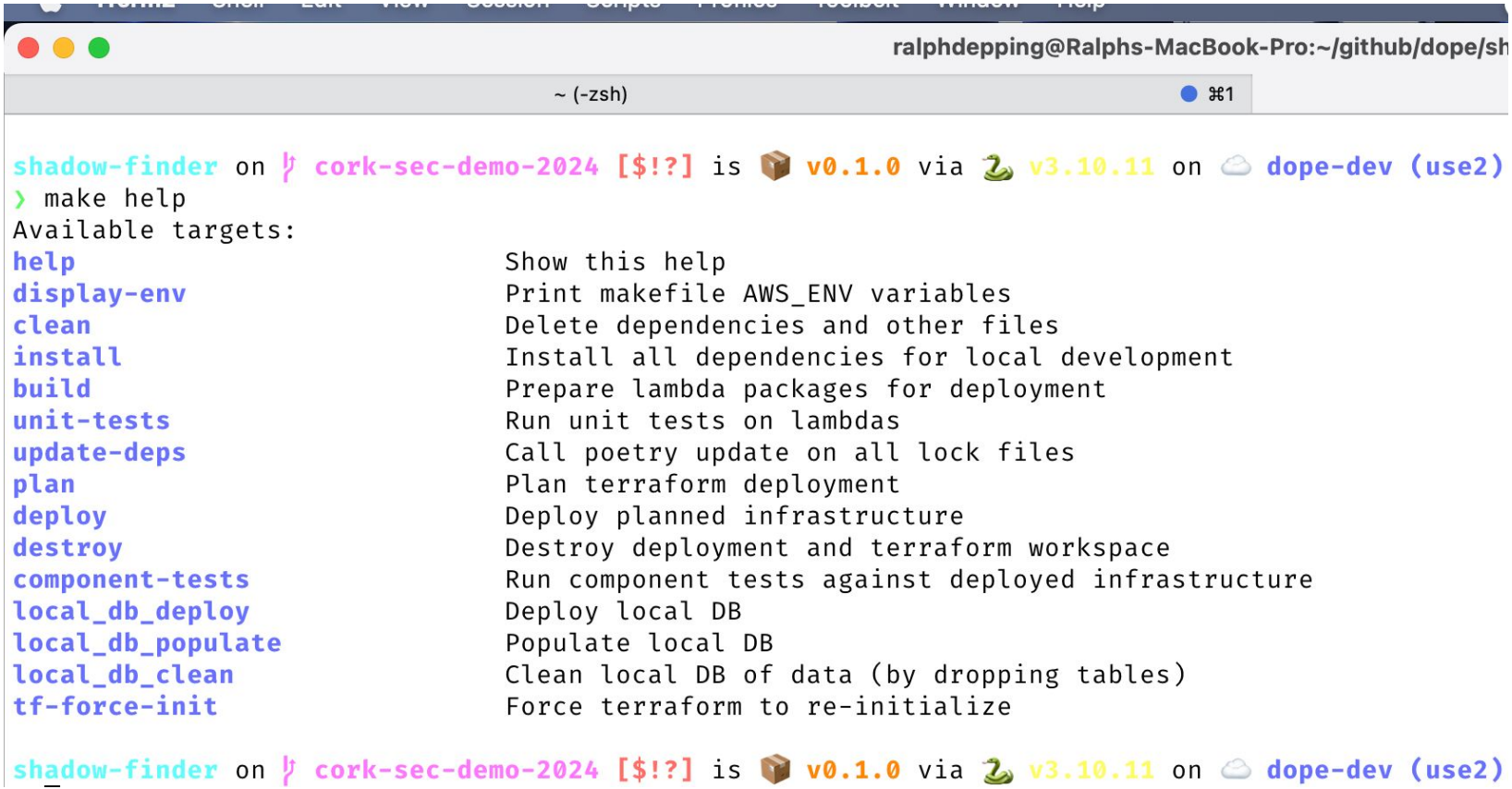
- Requires deep cloud knowledge

📝 Infrastructure as Code

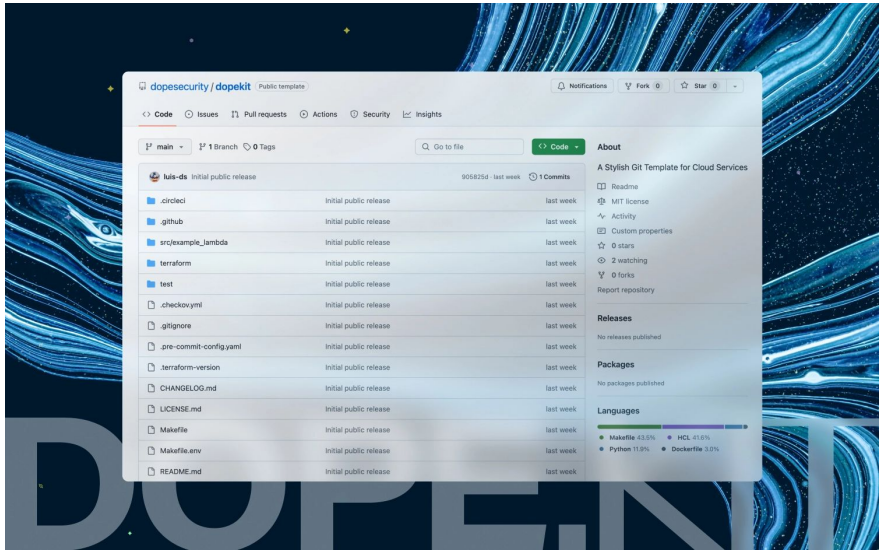
- Fits beautifully with PRs
- Static Analysis



Demo

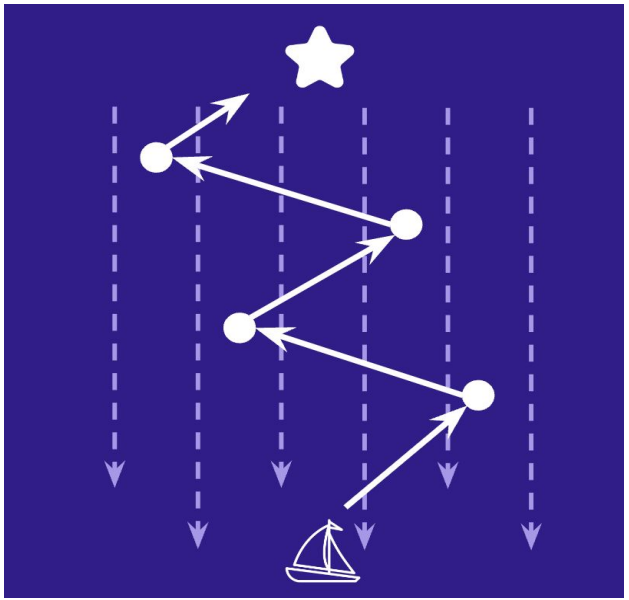

ralphdepping@Ralphs-MacBook-Pro:~/github/dope/sh
~ (-zsh)
⌘1
shadow-finder on cork-sec-demo-2024 [$!?] is v0.1.0 via v3.10.11 on dope-dev (use2)
❯ make help
Available targets:
help Show this help
display-env Print makefile AWS_ENV variables
clean Delete dependencies and other files
install Install all dependencies for local development
build Prepare lambda packages for deployment
unit-tests Run unit tests on lambdas
update-deps Call poetry update on all lock files
plan Plan terraform deployment
deploy Deploy planned infrastructure
destroy Destroy deployment and terraform workspace
component-tests Run component tests against deployed infrastructure
local_db_deploy Deploy local DB
local_db_populate Populate local DB
local_db_clean Clean local DB of data (by dropping tables)
tf-force-init Force terraform to re-initialize
shadow-finder on cork-sec-demo-2024 [$!?] is v0.1.0 via v3.10.11 on dope-dev (use2)

dope.kit - stylish git template for cloud services



- https://github.com/dopesecurity/dopekit
- https://dope.security/post/dopekit-a-stylish-git-template-for-cloud-services

Learnings



Looking back…

- “**local stacks with make**” replaces “each dev has their own AWS region”
- **pre-commit** hooks
  - checkov - all or nothing
  - takes time to address warnings
- **docker hardening** “invest as you go”

Bring people along

<u>Not always easy…</u>

- People do get scared 😬
  …how do you **reassure** them?
- Just do it
  …**it'll work** and build trust
- Soft influence rarely shifts things
  …you have to **"have the juice"**

Over to you 👇

🎯 Zone of control

- What things could you change today - *pretty much* - without asking?
- Improve those things

▶️ Where to Start

- Look at pre-commit
- Starting a new service

  …don’t just dive in…tidy and improve as you go

  … how can I make things better?

💪 *You don’t need permission to be a good engineer*

Questions?