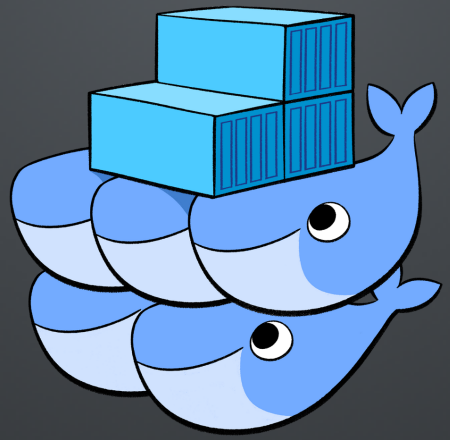
2018
LINUXCONFAU
JANUARY 22-26 SYDNEY

BECOMING THE ADMIRAL

Mastering Docker orchestration



Alistair Chapman

@agc93

WHO AM I?

Alistair Chapman

 agc93

 agc93

Information Security Engineer @ Red Hat

Microsoft MVP

Walking, talking case of impostor syndrome

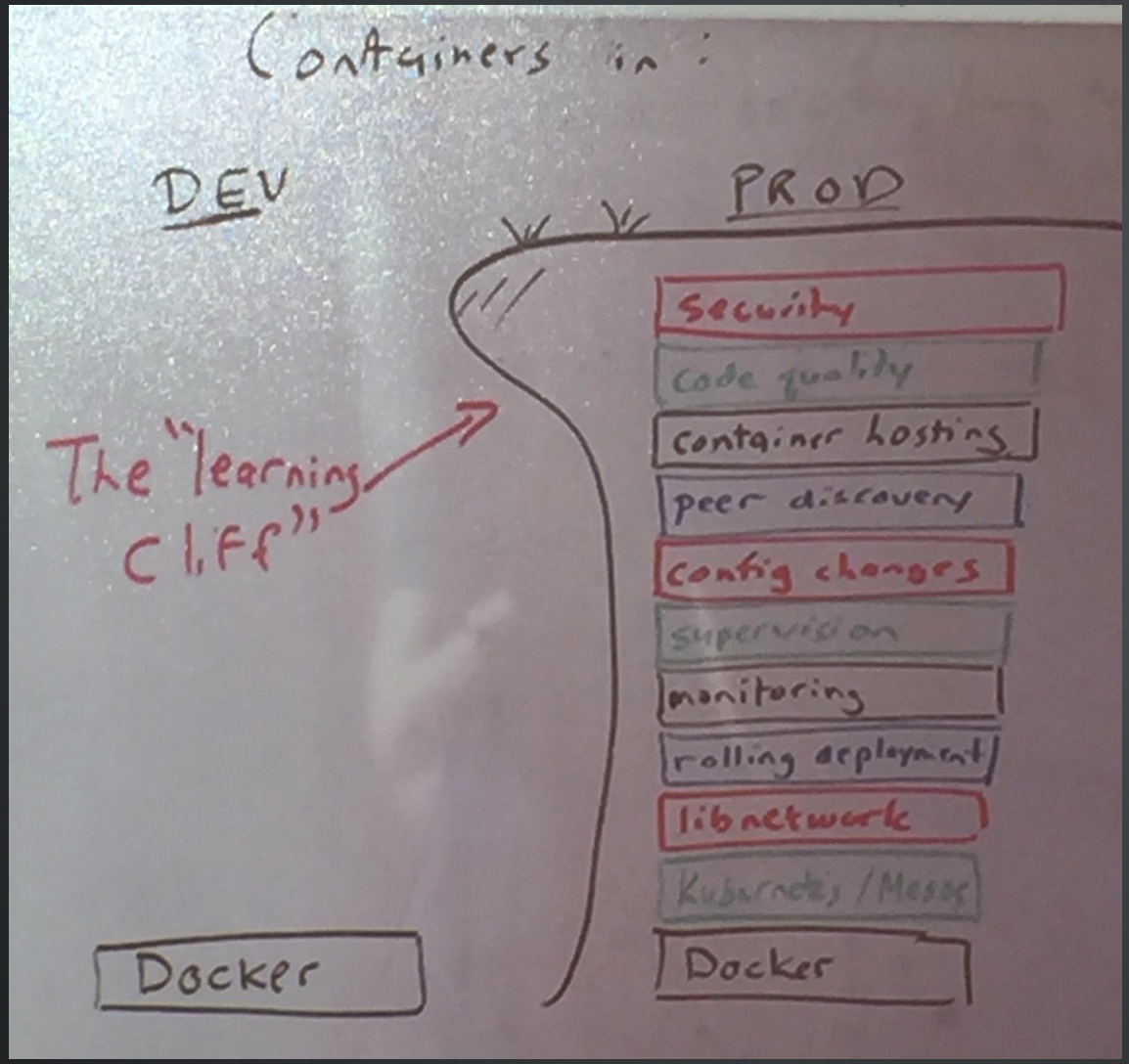
THE PLAN

(OR HOWEVER MUCH I CAN FIT IN 15 MINUTES)

- Monitoring container workloads
- Adapting your processes
- Securing your containers
- Building a solution

MONITORING CONTAINERS

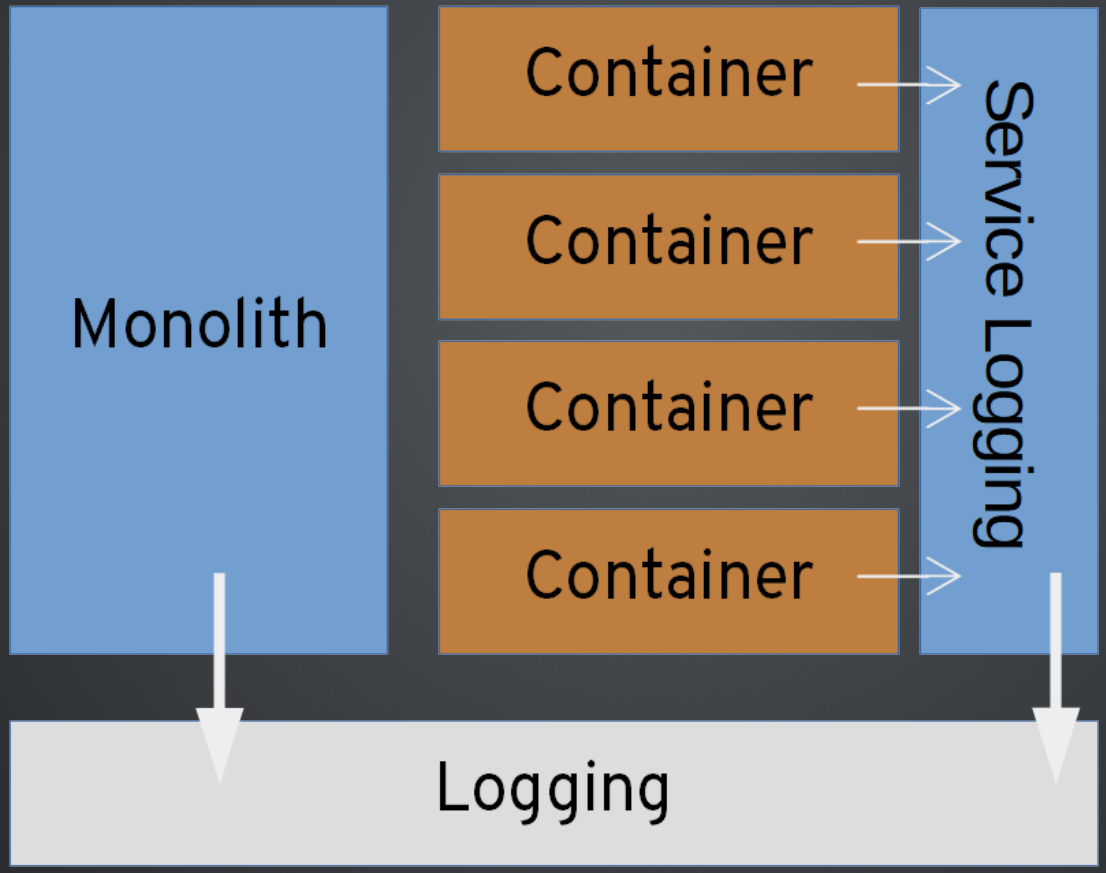
SCALE YOUR MONITORING WITH YOUR WORKLOADS



- You're not monitoring a few servers anymore!
- Get your host ↔ app balance right
- Identify your "bridging"/interface points
- Herd those cats!

MONITORING CONTAINERS

UNDERSTAND YOUR APPROACH

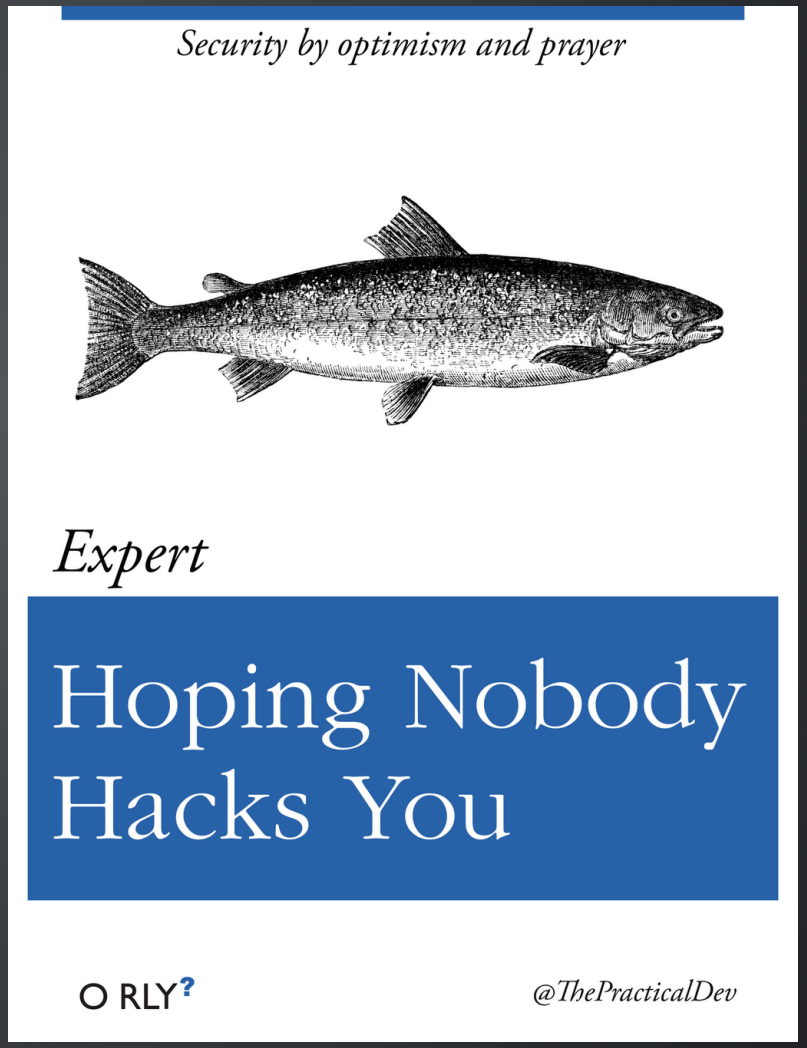


IMPROVE YOUR RESPONSE TOOLKIT

- The same tools and processes **don't** apply to containers!
- Know how to make the most of Docker
- Be wary of reliance on documentation
- Prepare for each layer of the stack

SECURE YOUR CLOUD

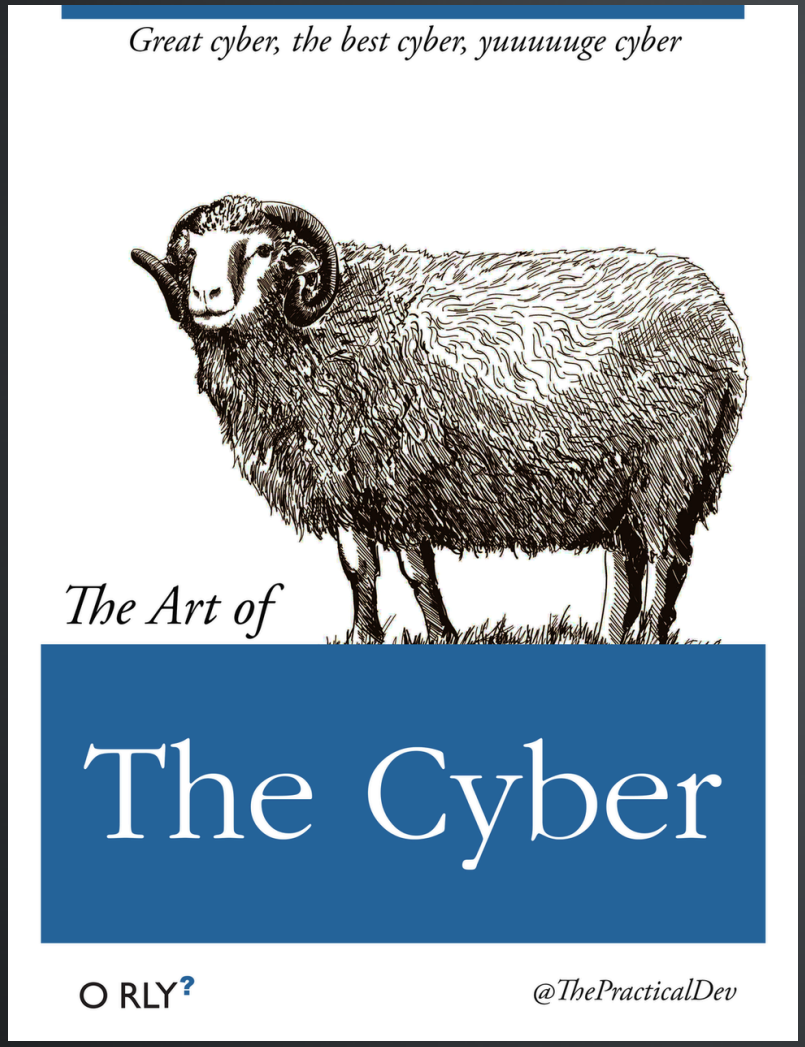
- This should be a **basic** requirement
- Assume everyone's out to get you
- Don't implicitly trust third-party apps



SECURE YOUR CLOUD

A shell is run in a container	`container.id != host and proc.name = bash`
Unexpected outbound Elasticsearch connection	`user.name = elasticsearch and outbound and not fd.sport=9300`
Write to directory holding system binaries	`fd.directory in (/bin, /sbin, /usr/bin, /usr/sbin) and write`
Non-authorized container namespace change	`syscall.type = setns and not proc.name in (docker, sysdig)`
Non-device files written in /dev (some rootkits do this)	`(evt.type = creat or evt.arg.flags contains O_CREAT) and proc.name != blkid and fd.directory = /dev and fd.name != /dev/null`
Process other than skype/webex tries to access camera	`evt.type = open and fd.name = /dev/video0 and not proc.name in (skype, webex)`

SECURE YOUR CLOUD



- Behavioural monitoring
- Standard network-based detection
- Proper user controls and RBAC
- API activity (including baselining)
- Platform access controls

BUILDING YOUR SOLUTION

PRO-TIP: IT'S NOT DOCKER

- The answer isn't Docker
  - or Kubernetes, or OpenShift
- Containers are not a turn-key solution
- Build a stack around both sides of your infrastructure

ALISTAIR CHAPMAN

@agc93

(essentially everywhere)

https://slides.agchapman.com

https://blog.agchapman.com/