KubeCon | CloudNativeCon

Europe 2020

Virtual

How to Work in Cloud Native Security

Demystifying the security role

Justin Cormack

Who am I?

Justin Cormack

Senior Engineer at Docker since 2015

Cambridge, UK

@justincormack

How I got into security by mistake

My first security work

- working as a sysadmin in a university back in the days when every machine had public IP addresses
- was an interesting target for people as we had lots of bandwidth
- not what I was expecting, which was mainly configuration management

Moved on

- moved into development
- exposed to risk management in financial services
- learnt internals of a lot of things in detail
  - Linux syscalls, networking

At Docker

- worked with Jessie Frazelle on seccomp filtering for Docker
- moved to the security team
- led the security team
- back to not-just-security

In the community

- involved with CNCF SIG Security
- maintainer of Notary
- working on Notary v2 with Amazon, Microsoft, NYU and many others
- Containerd security advisor

In the community

KubeCon CloudNativeCon Europe 2020 Virtual

- bringing security to a wider community
- working on Noise Protocol Framework
- capability based security
- lots to learn!

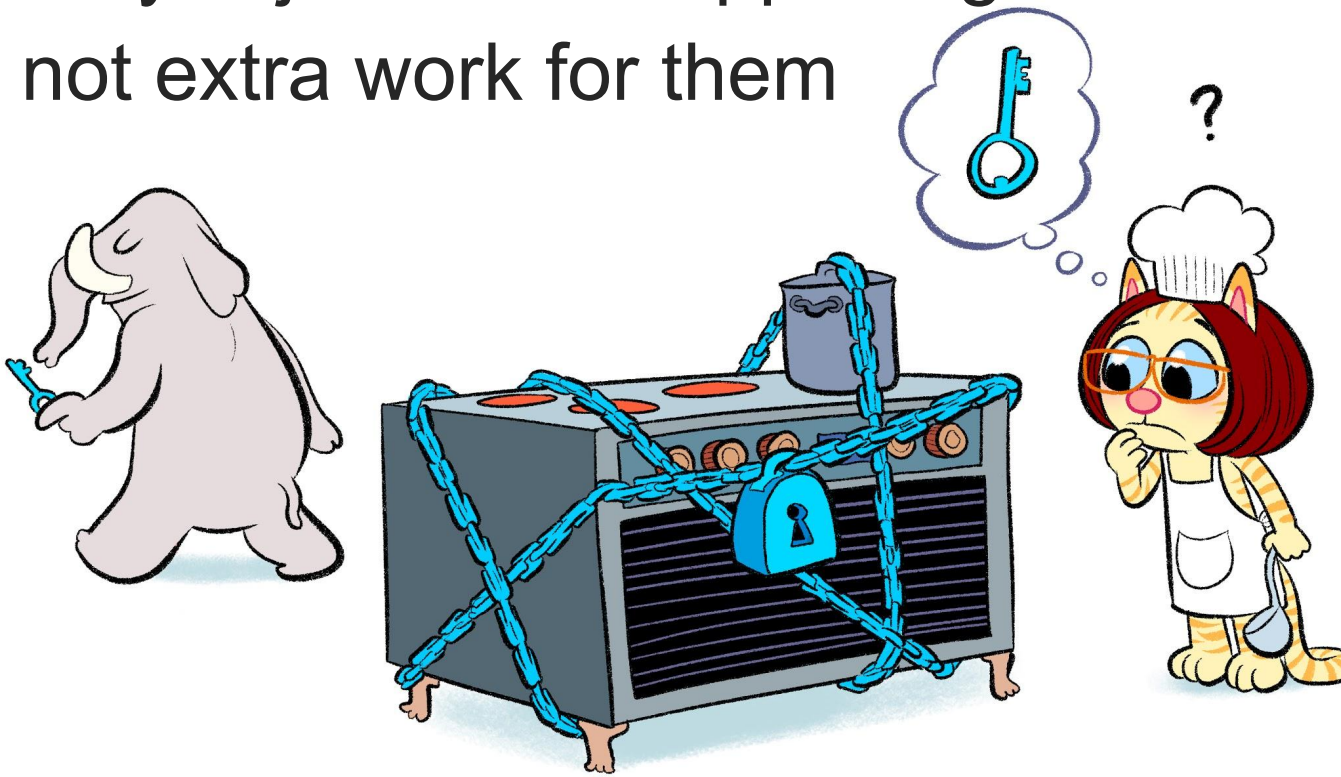
Most important things

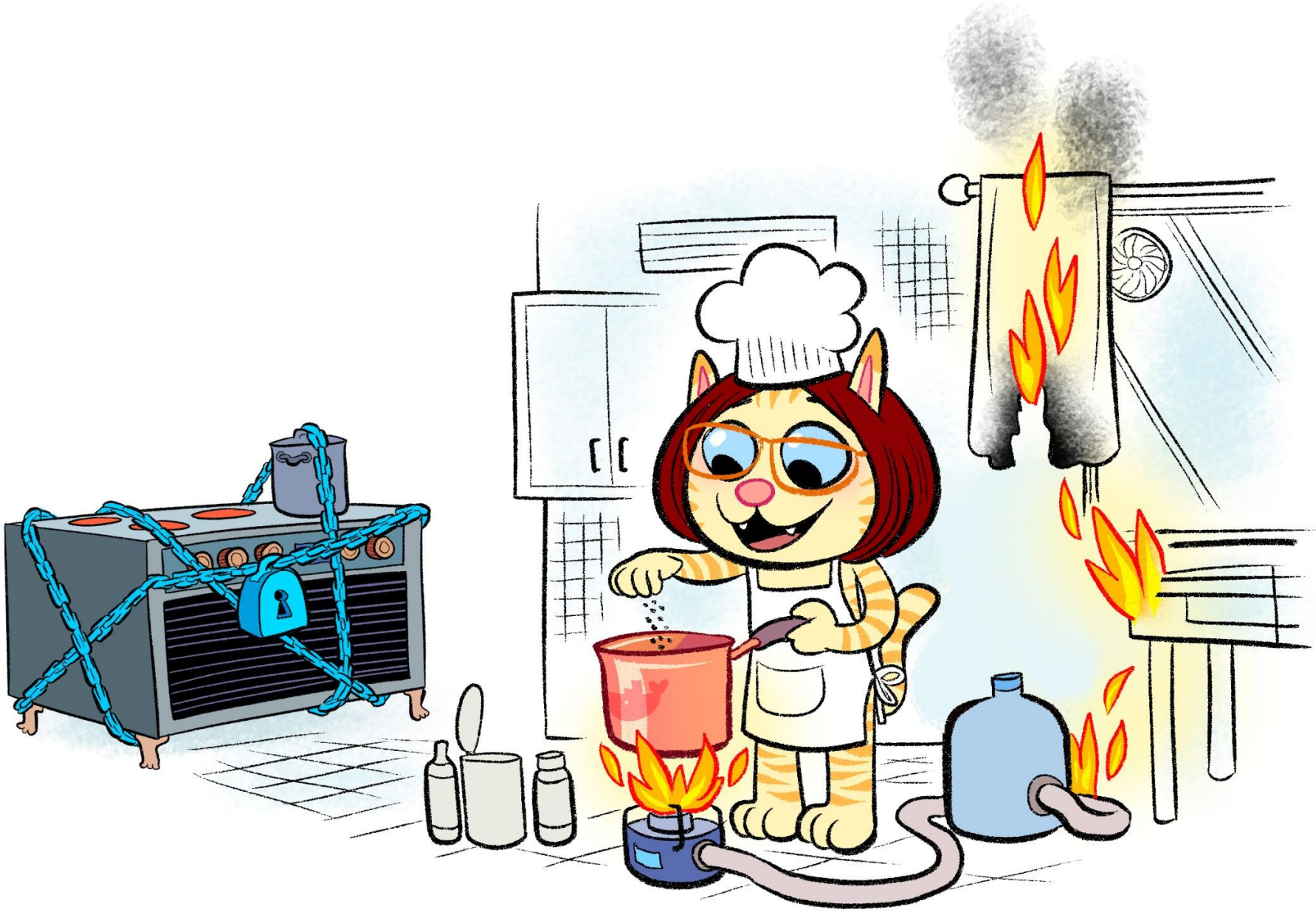
Learn things in detail

- for both offensive and defensive security, knowing an area in depth is hugely important
- separates the script kiddies from the experts
- the security issues are on the boundaries of the usual
- play, understand, break, fix

Spend time in the real world

- empathy
- security is unimportant most of the time
- the best security is just there supporting people, it is not extra work for them





Break *and* fix

- just breaking things is not sufficient
- fixing things is much harder
- you get exposed to the world of compromise
- wanting to burn everything down is a fine thing, but it's not going to happen 🔥

Meet the team

- security is not just an engineering job
- get to meet your legal team
- and your PR team
- and sell security to the business
- and compromise
- work with product team

Demand for security people

Hard to hire people

- Estimated that there will be 3.5 million unfilled security jobs in 2021
- Like every statistic about jobs this is not entirely meaningful, but there is definitely a shortage

You don't need

- formal qualifications in security
- to have hacked high profile sites
- to be a great developer

What is cloud native security?

Everything is code...

- before cloud we had security in hardware
  - firewalls
  - physical cables
  - data diode
- now everything can be reconfigured in code
- this changes everything...

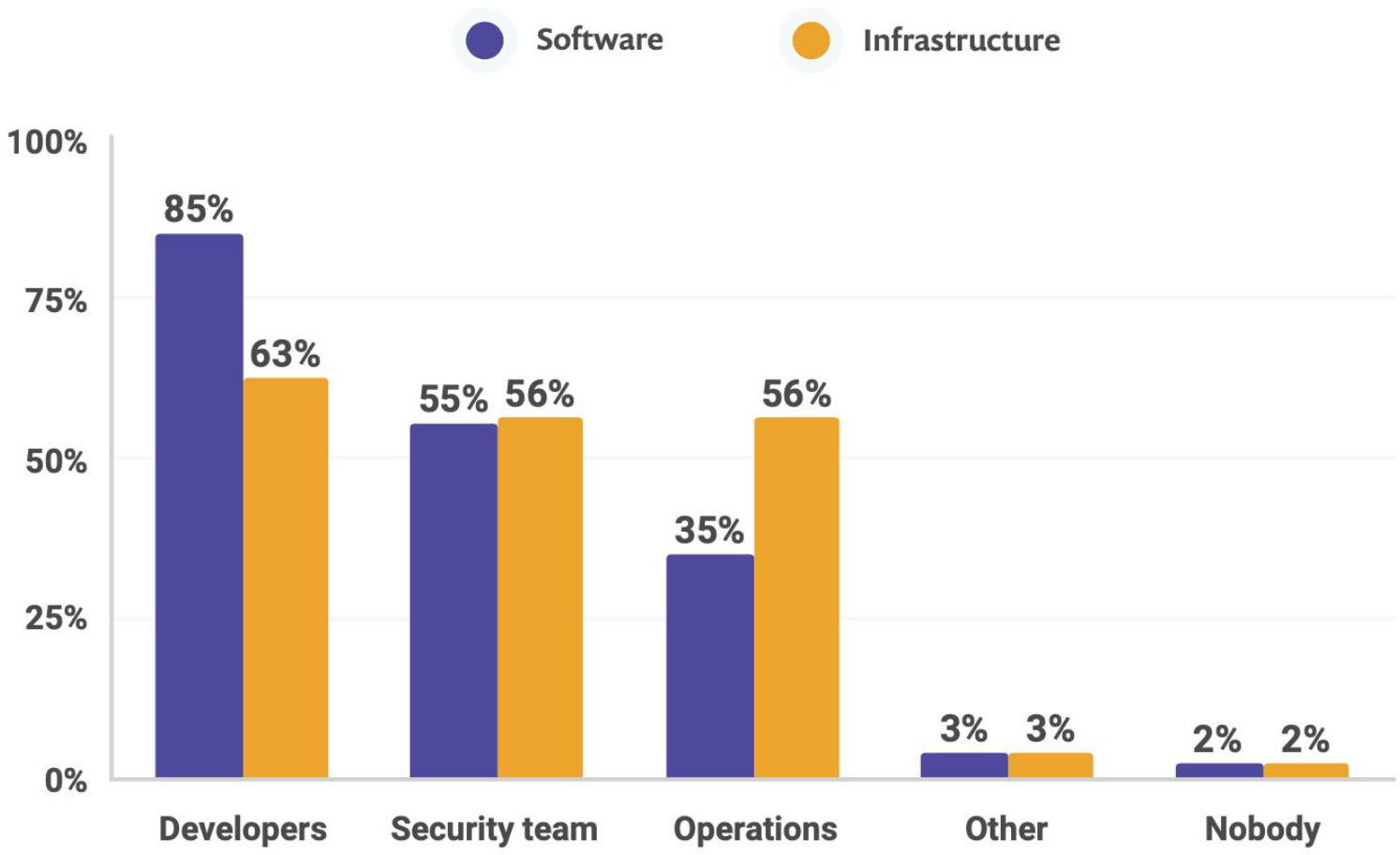
Implications

- cannot separate security from development or operations DevSecOps
- everything changes much faster
- new places to attack, eg supply chain
- dev and ops must get involved

DevSecOps

Who should be responsible for security?

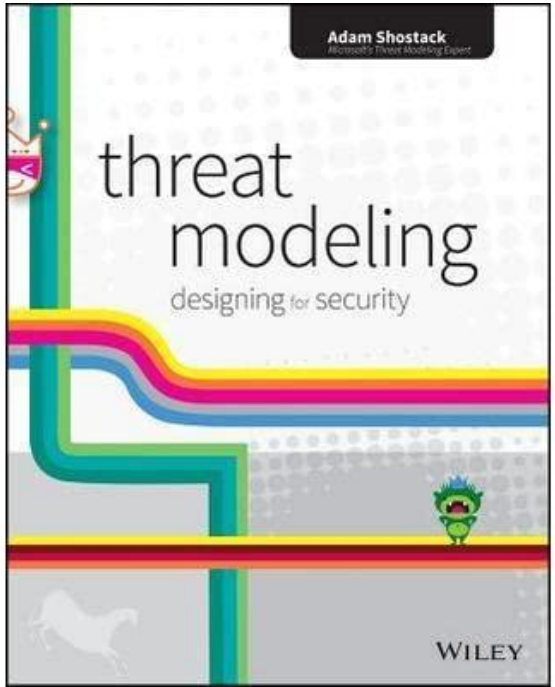
snyk



Multiple responses allowed.

Security in your code

- understand the threat model
- security is quality
  - handle errors and the unexpected
  - understand the issues in domain
  - write security tests
- think like an attacker
- spend time attacking
- learn from external audits



Burnout

Burnout in security roles

- you cannot tell anyone about what you do a lot of the time
- not enough people, so often overworked
- live away from the happy path

@justincormack


KubeCon
CloudNativeCon
Europe 2020
Virtual

Title

Text

KubeCon | CloudNativeCon

Europe 2020

Virtual

Getting into security by mistake

KubeCon | CloudNativeCon

Europe 2020

Virtual

Getting into security by mistake

KubeCon | CloudNativeCon

Europe 2020

Virtual

Getting into security by mistake