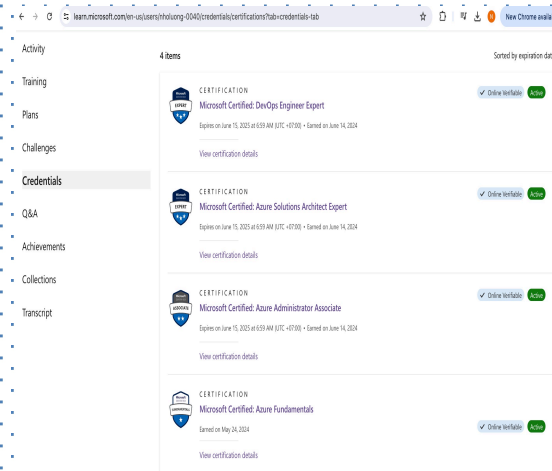
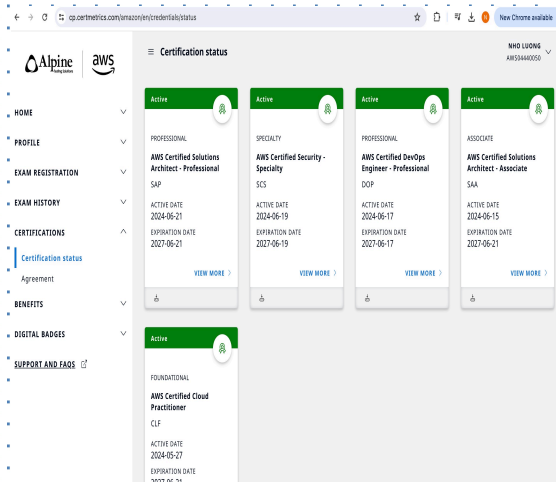
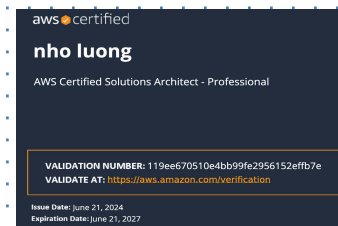


Cloud Native Security

Author: Nho Luong

Skill: DevOps Engineer Lead

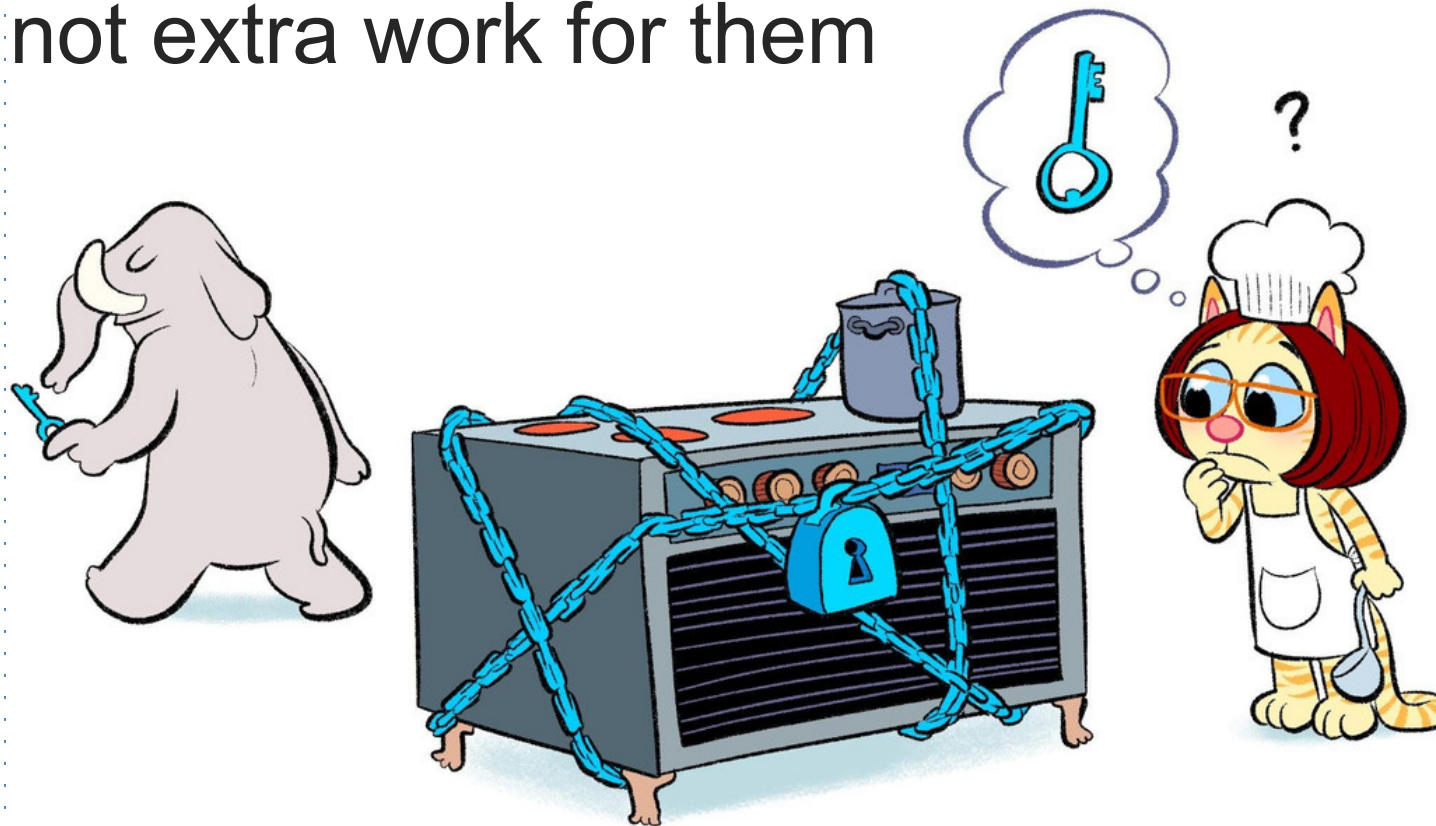


Learn things in detail


- 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

Everything is code...

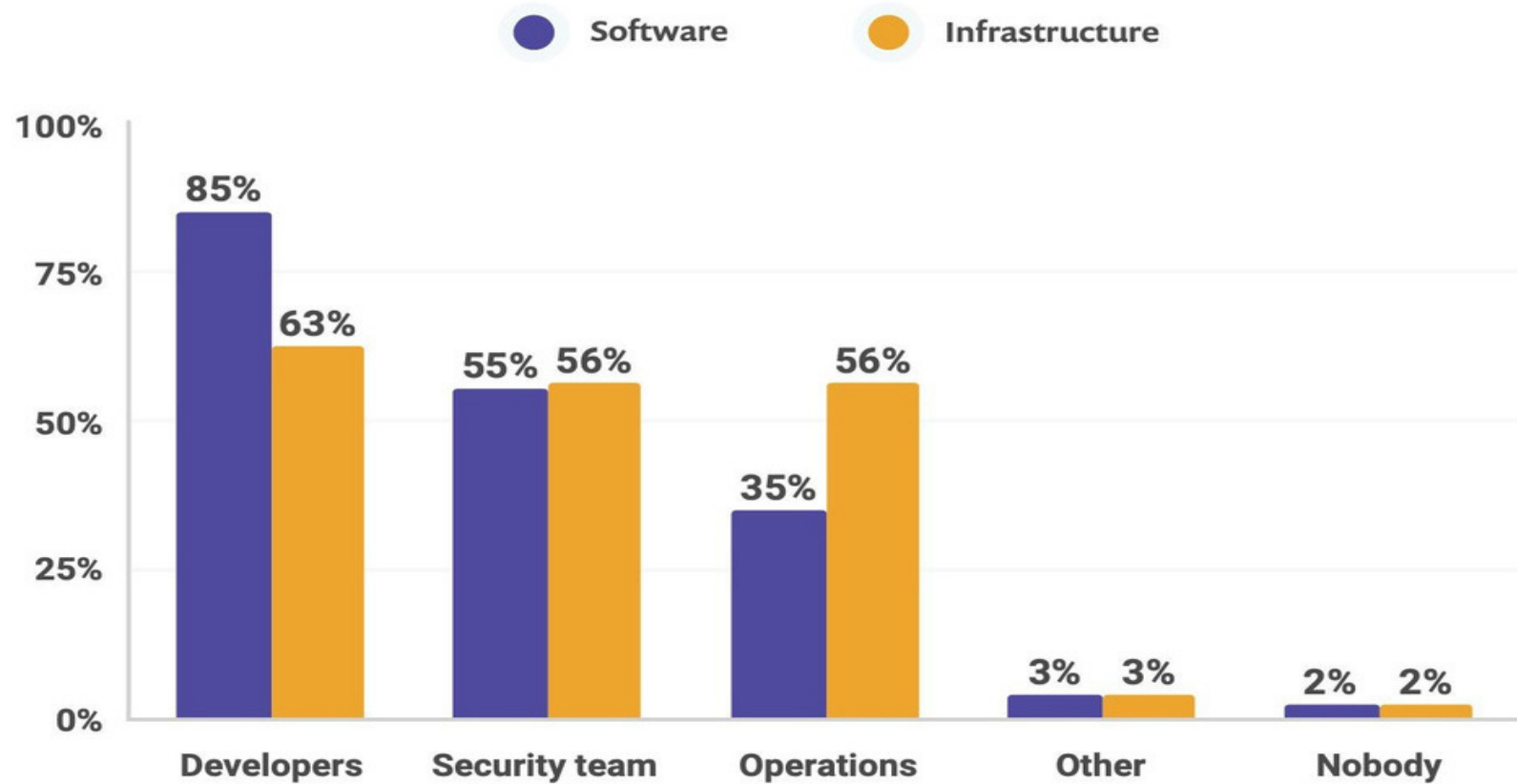
- before cloud we had security in hardware
 - firewalls
 - physical cables
 - data diode
- now everything can be reconfigured in code
- this changes everything...

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

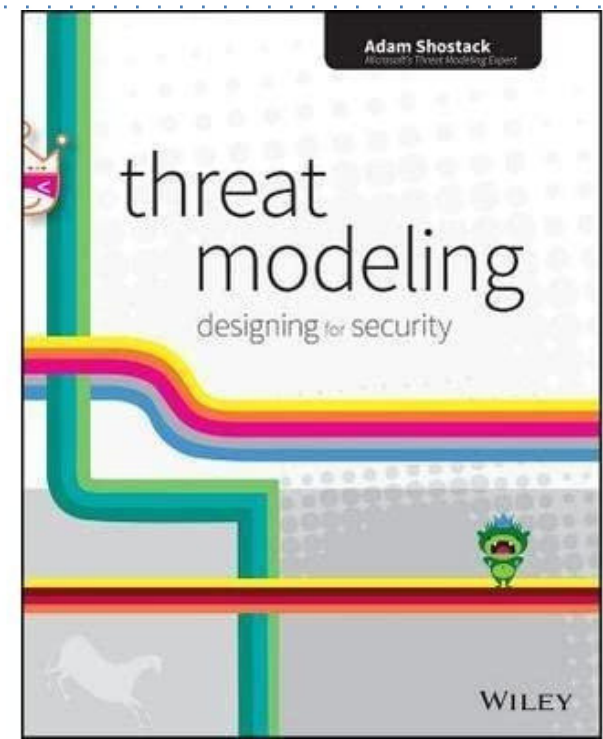
Who should be responsible for security?



Multiple responses allowed.

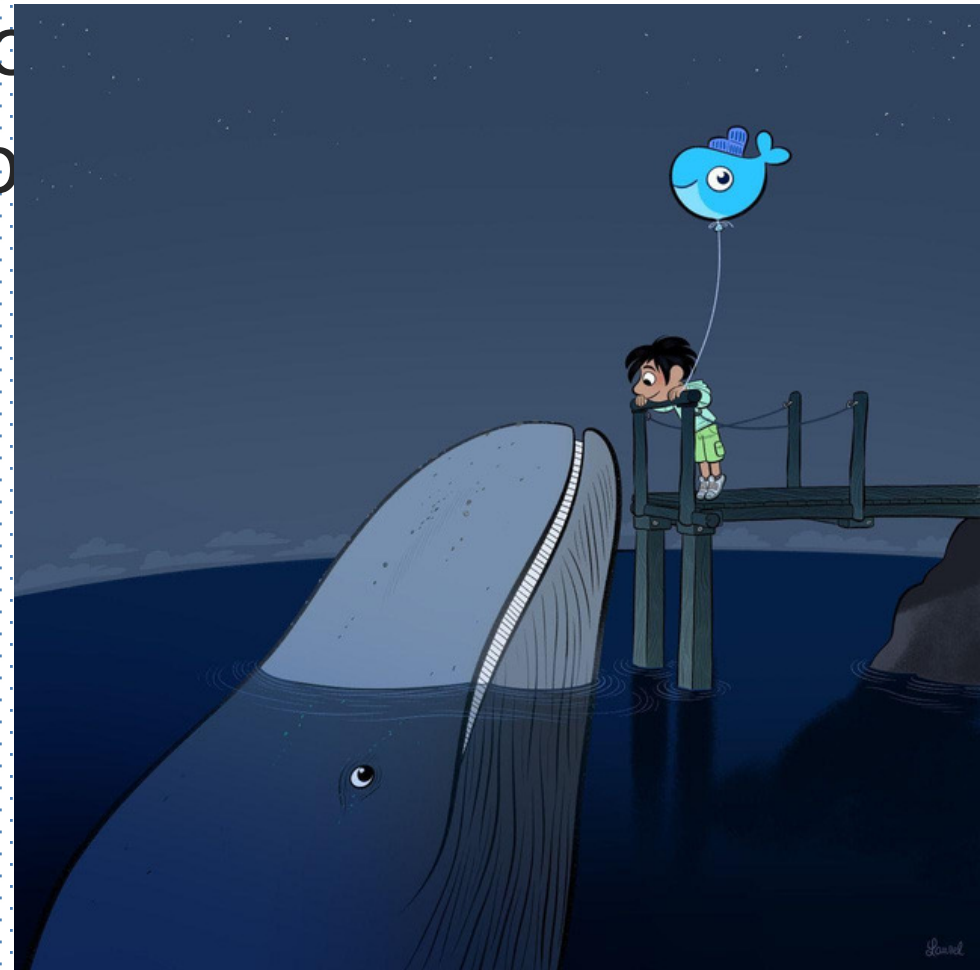
Security in your code

- 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 in security roles

- you cannot tell anyone about what you do a lot of the time
- not enough people, so you have to do everything
- live away from the happy





Thank You

Author: Nho Luong
Skill: DevOps Engineer Lead