

Why can't we be friends?
**Integrating security into
an existing agile SDLC**

Laura Bell

FOUNDER & LEAD CONSULTANT
SAFESTACK

@lady_nerd

laura@safestack.io

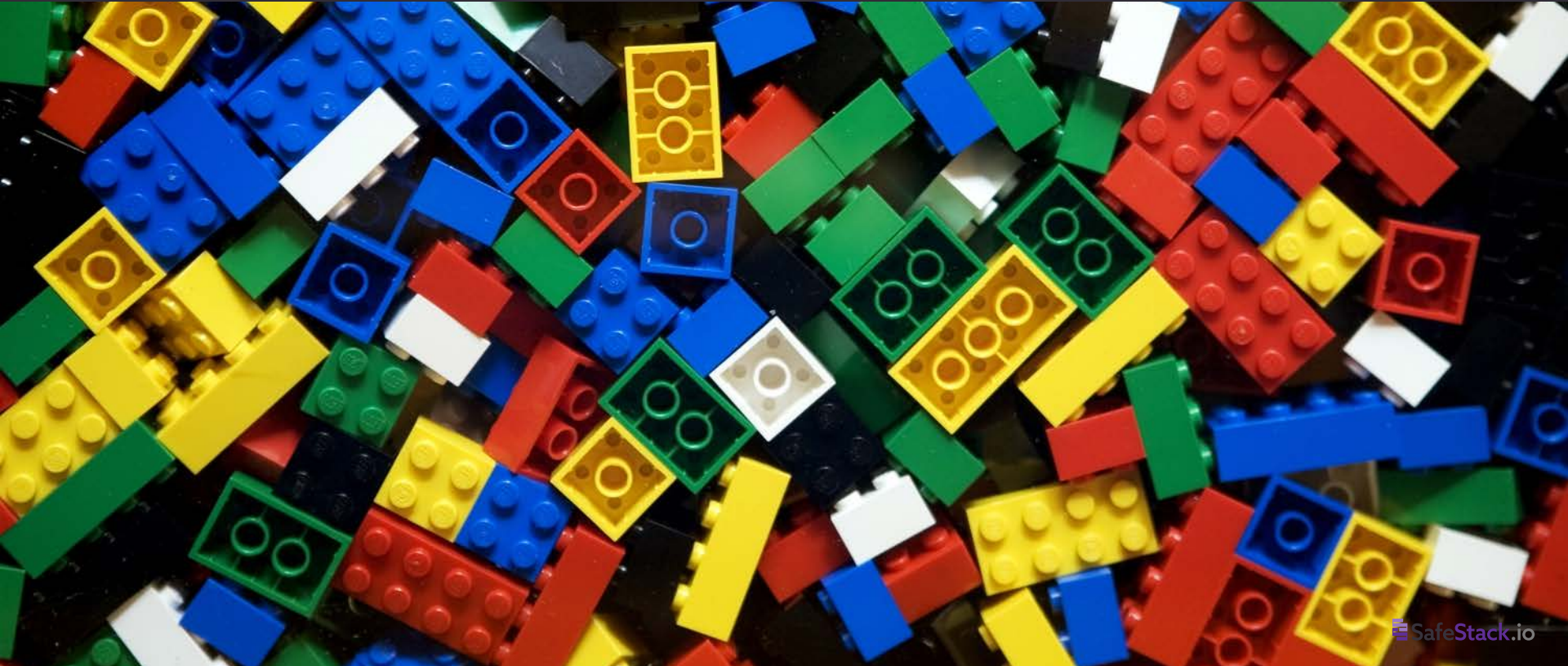
**security people are
semantically challenged
when we talk about
hacking**

Sorry about that....

once upon a **time*** ...

* Sometime in the last week for some of you

we are engineers



meanwhile in the security industry...



**and the whole world
went to hell**

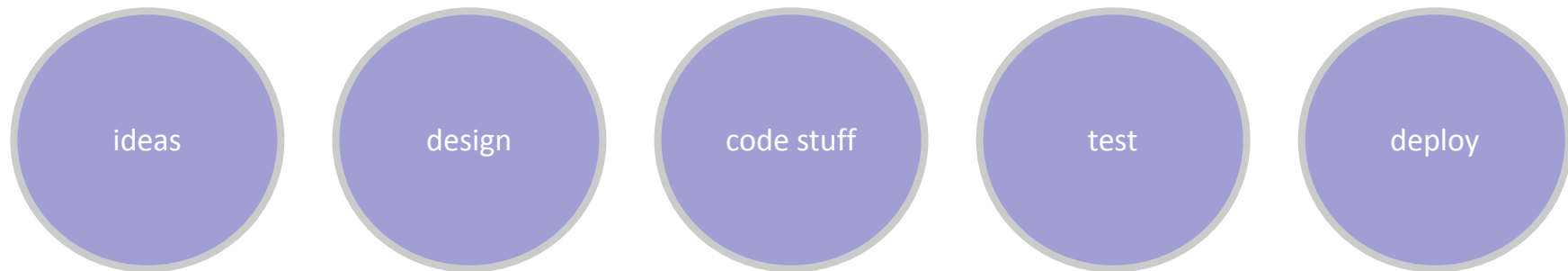


so what do we need to do?

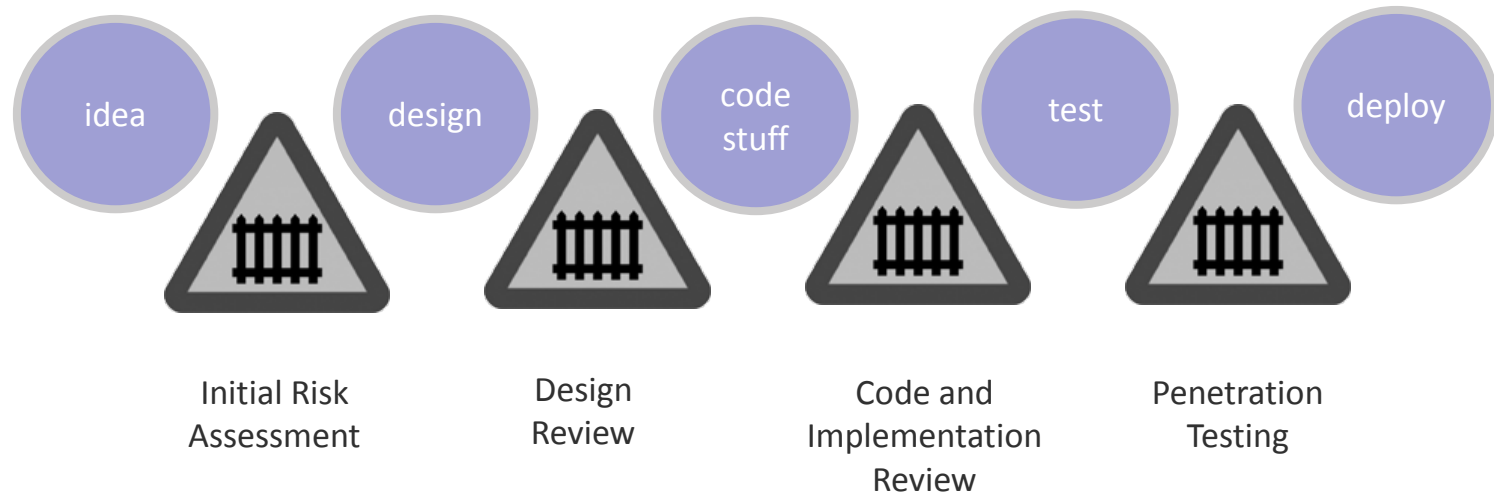
In this talk

- Common misconceptions in agile security
- Ten steps to bring security to your agile development lifecycle
- Challenges and pitfalls (and how to succeed)

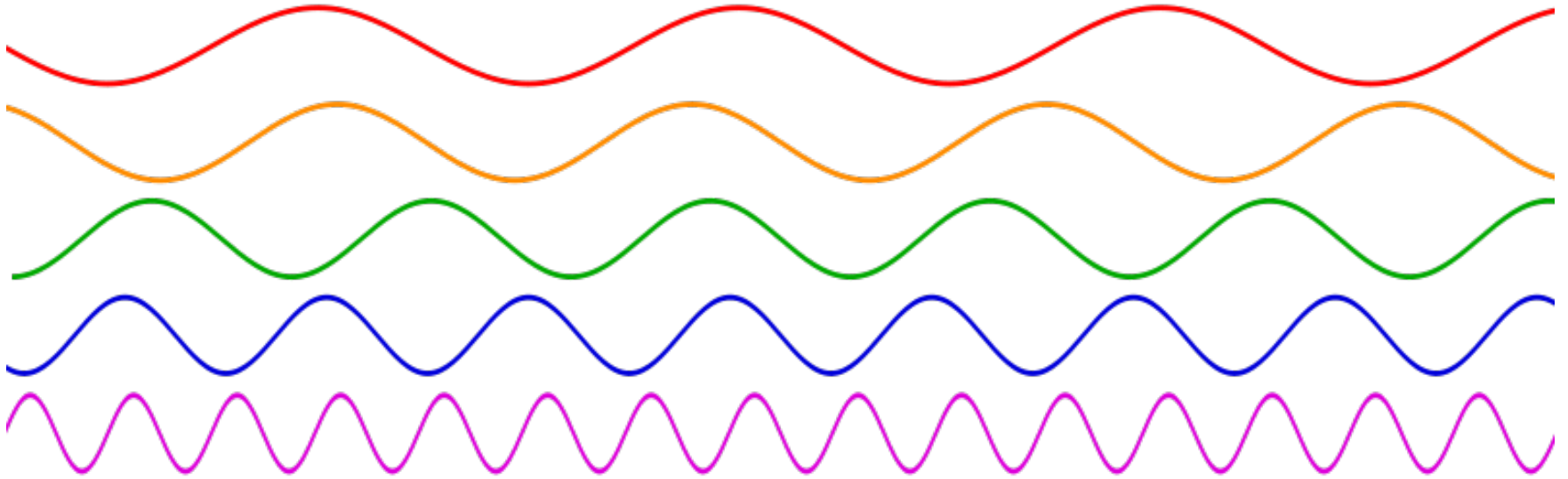
basic development lifecycles



security was about gates



same thing, just more frequently?



common misconceptions



avoidance != management

we're too little to fail
(at security)

it's impossible so why try

agility increases risk

we've always done this...
nobody's hacked us yet

**Ten steps to a
better,
stronger
and
more secure you**

1

Languages

Libraries

Operating Systems

Applications

Third Party Services

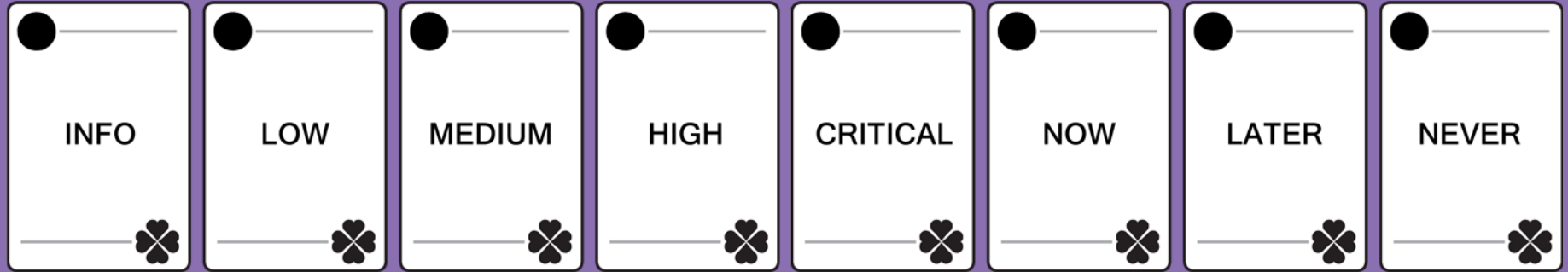
know your stack

2



add, adapt and abandon

3



communication

4



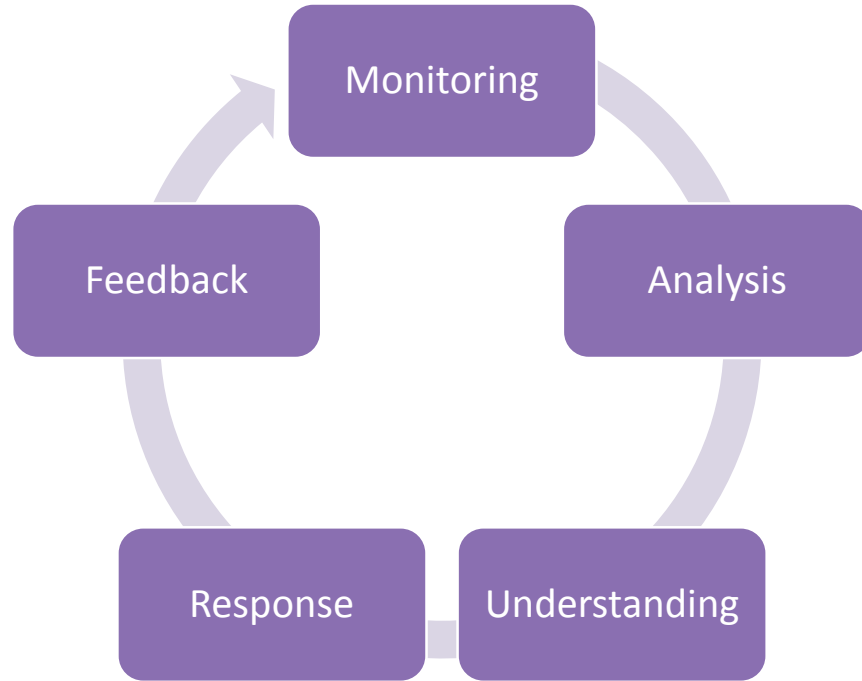
manage your debt

5

“engage security early and often and be sure to have it included in your definition of done”

Engage early (ideally for ideas)

6



prepare for the worst

7



build an army

8

“the best technical people I know work really hard to make themselves redundant.”

automate your workflows

9

**security fails
when it
is a
special event**

10

“if you are going to spend the money,
research your options, scope well and be
demanding”

outsource smartly

common challenges

compliance is a priority
but it won't save you

maintain momentum

“more secure today than yesterday”

hire good people

“learn what good means for your organisation”

use your words

“find the middle ground between yes and no”

Summary

- Common misconceptions in agile security
- Ten steps to bring security to your agile development lifecycle
- Challenges and pitfalls (and how to succeed)

Questions?

Laura Bell

FOUNDER & LEAD CONSULTANT
SAFESTACK

@lady_nerd

laura@safestack.io