Agile Security Testing

Lessons learned

David Vaartjes

Securify

OWASP AppSecEU 15

Amsterdam, The Netherlands

Agenda

1. Introduction
2. The software security dream
3. How it's done
4. From Waterfall to Agile security

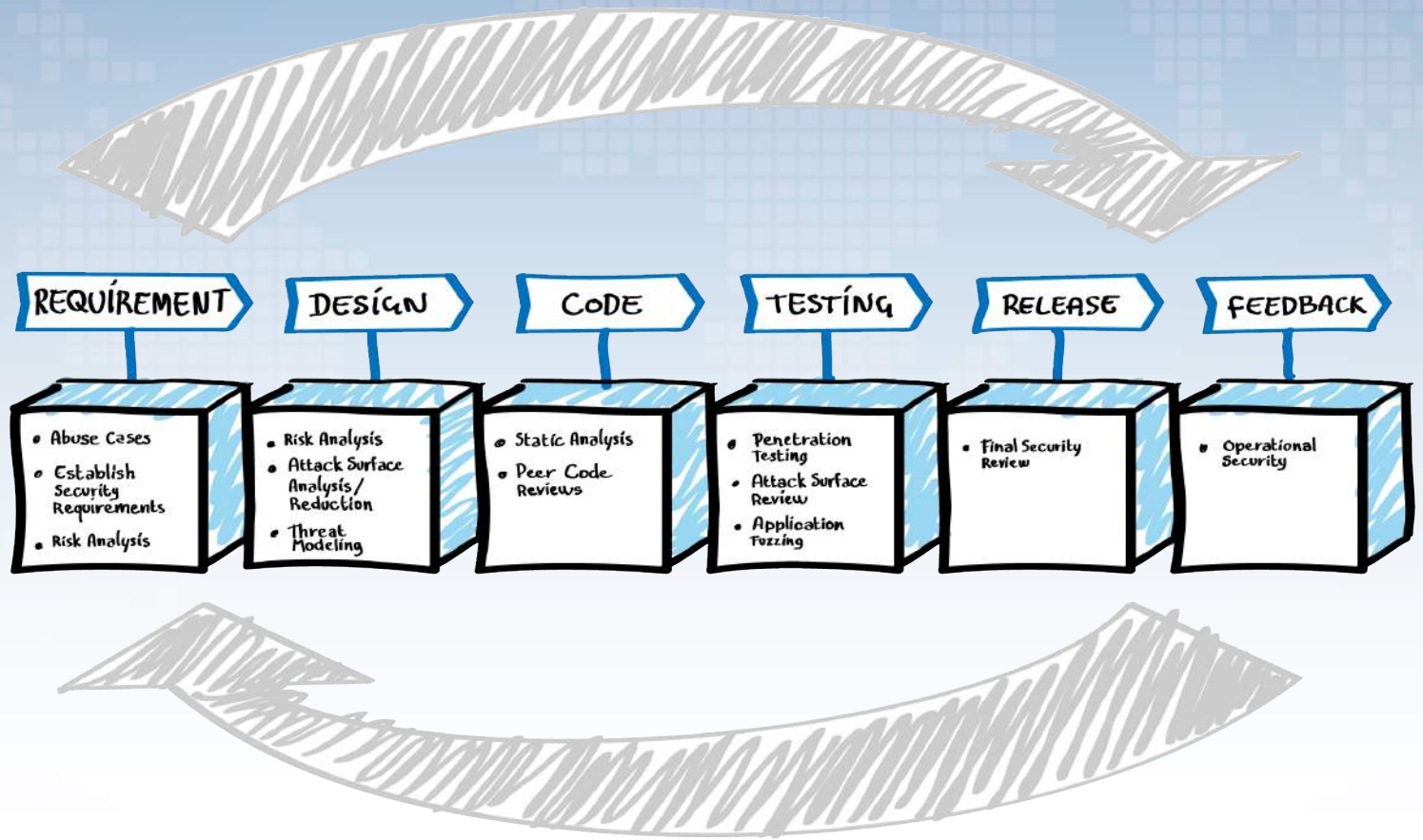
About me

- Co-founder Securify (Software Security / Build Security In)

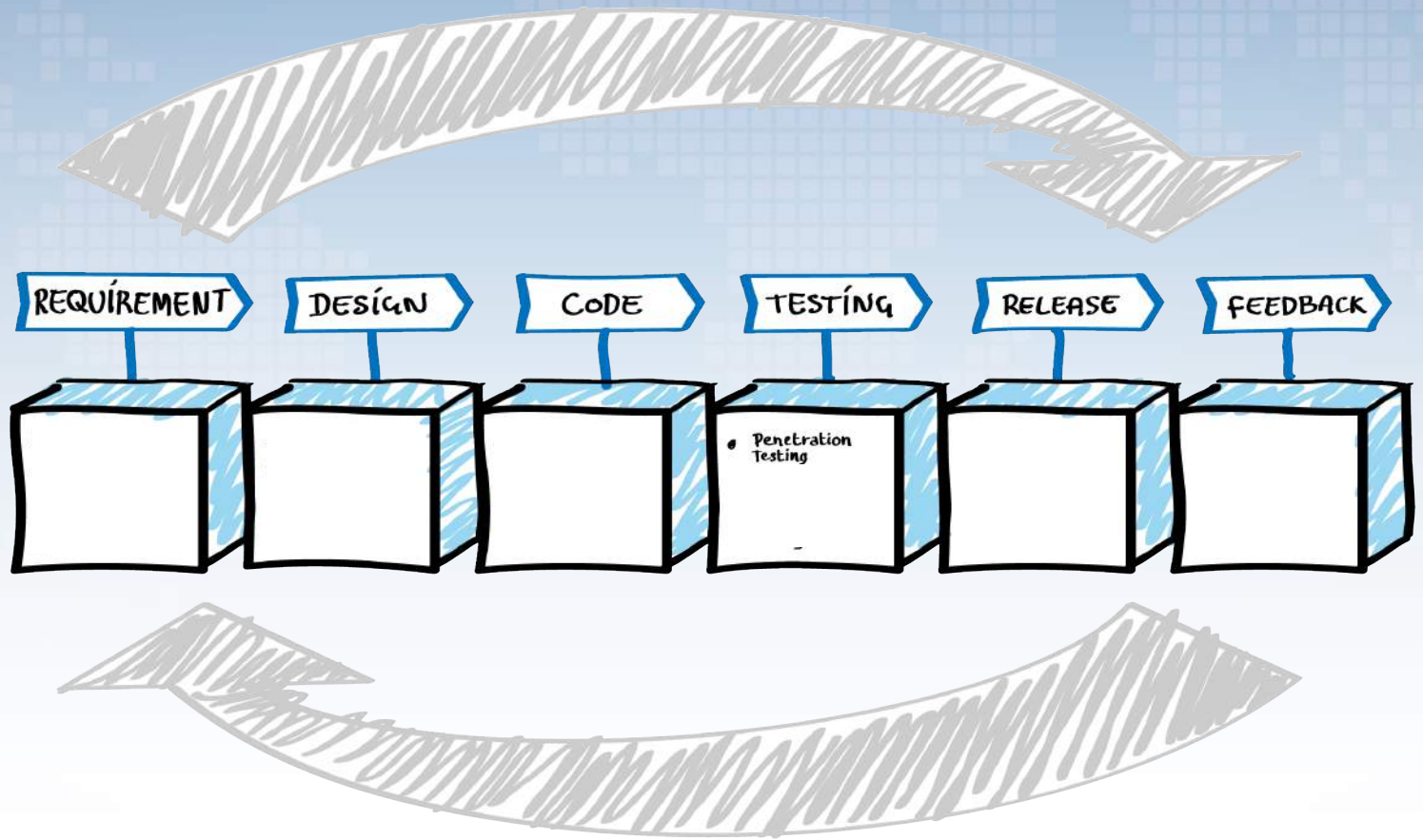
- 2 yrs software security @ Rabobank (internet banking teams)
- 8 yrs software security @ finance, insurance, gov, retail, ...

The software security dream

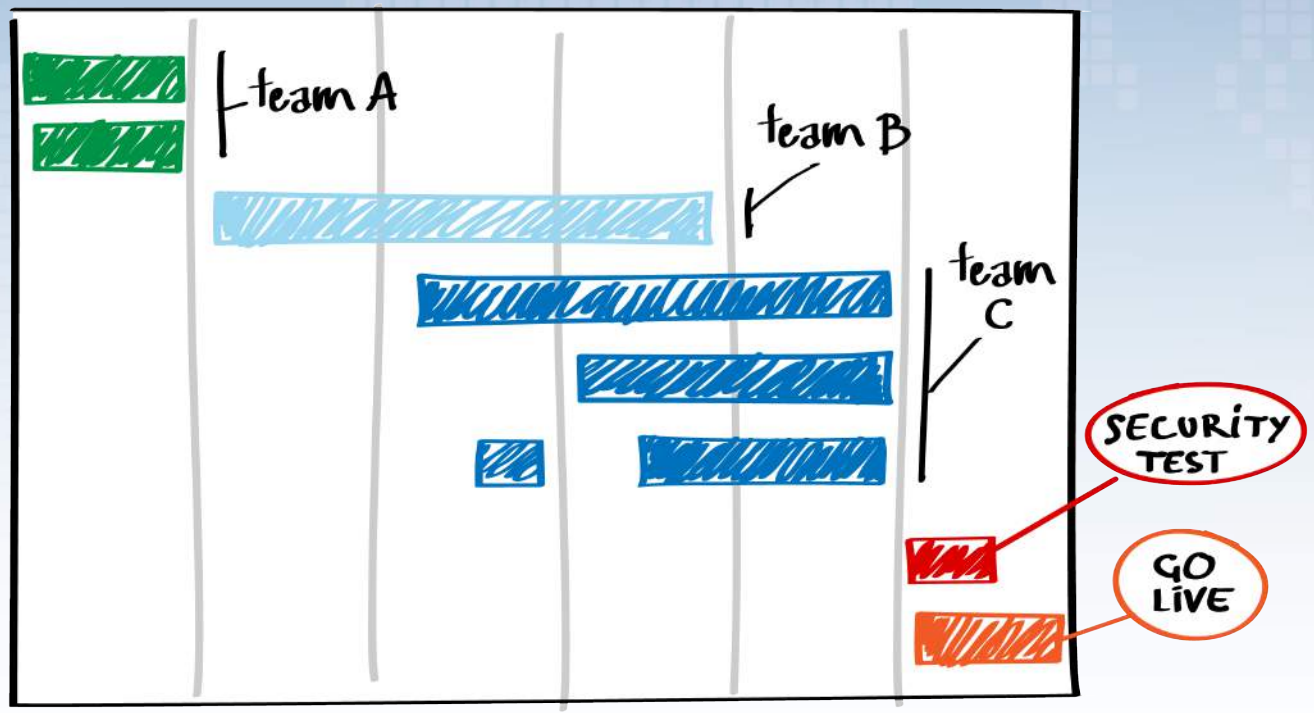
We know this


REQUIREMENT
Abuse Cases
Establish Security Requirements
Risk Analysis
DESIGN
Risk Analysis
Attack Surface Analysis / Reduction
Threat Modeling
CODE
Static Analysis
Peer Code Reviews
TESTING
Penetration Testing
Attack Surface Review
Application Fuzzing
RELEASE
Final Security Review
FEEDBACK
Operational Security

But still do a lot of this

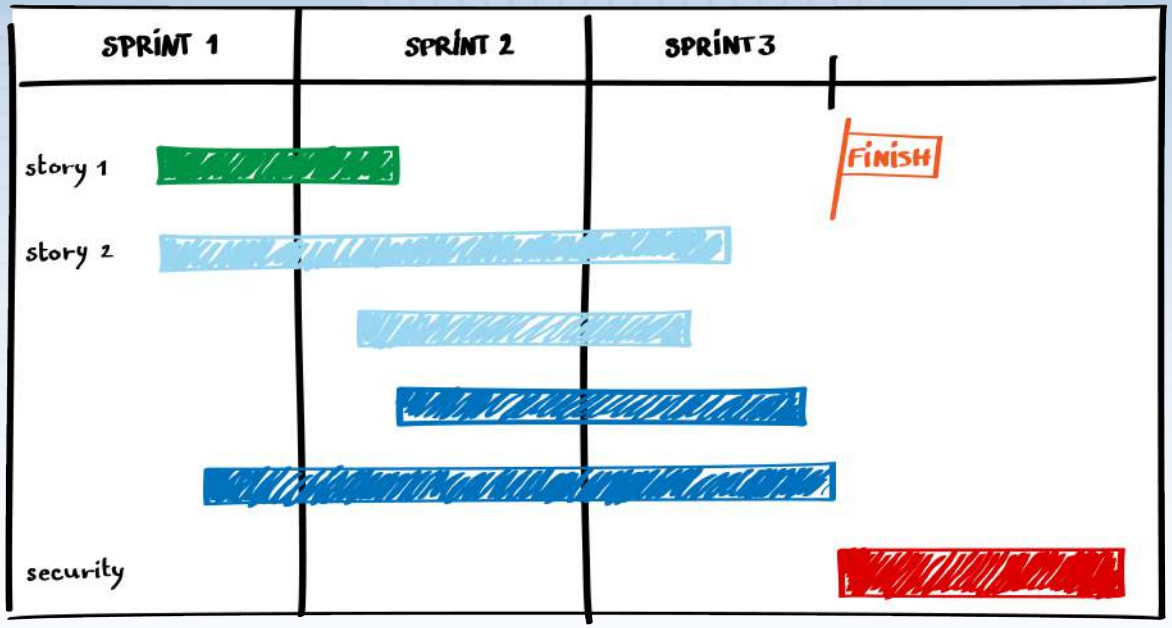


But still do a lot of this



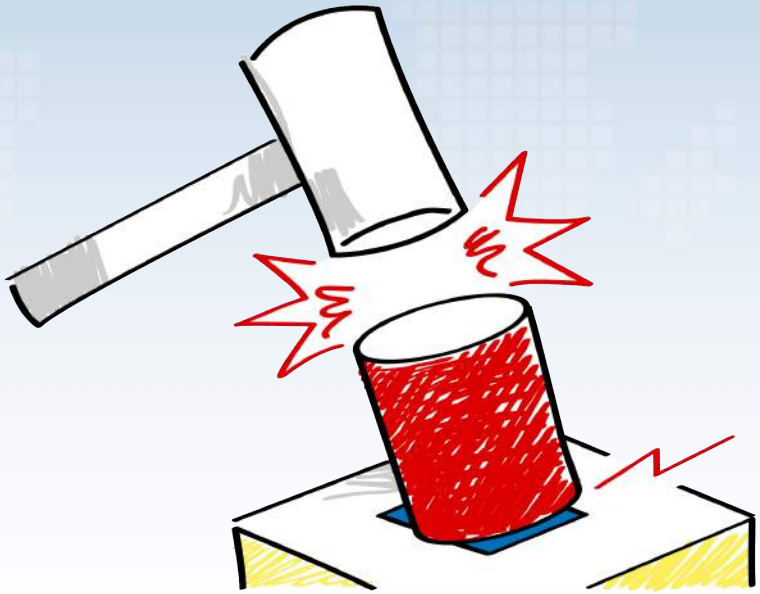
Meet the security end boss

Security sticks to waterfall



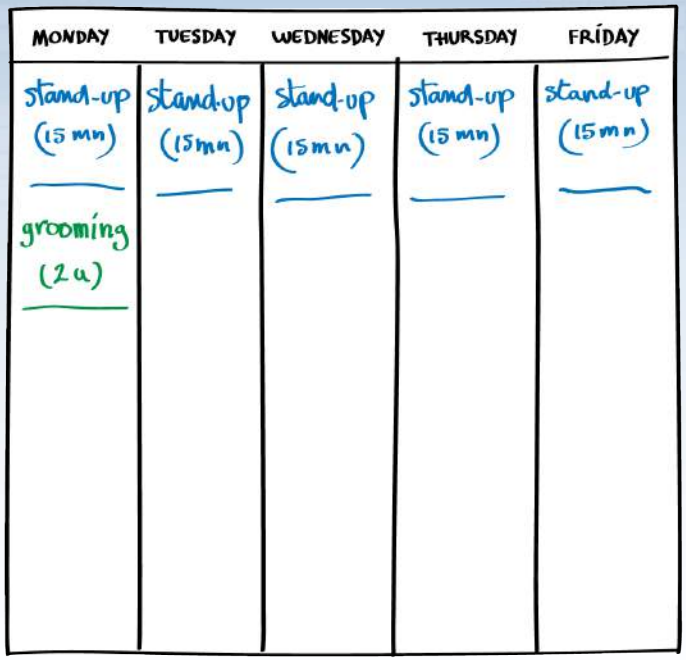
Security can’t catch up..

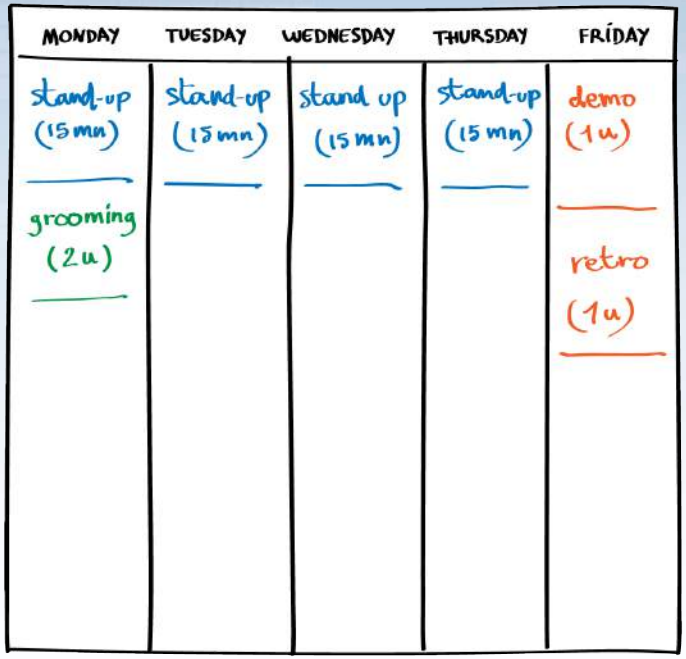
We need change



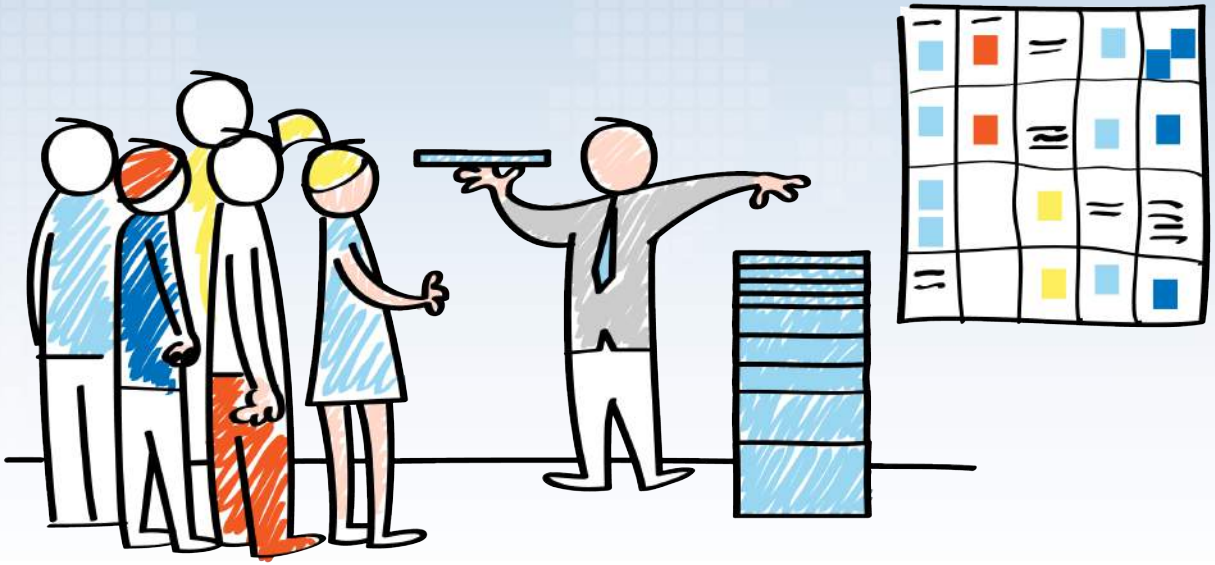
Lets fix this together - pilot

Join meetings

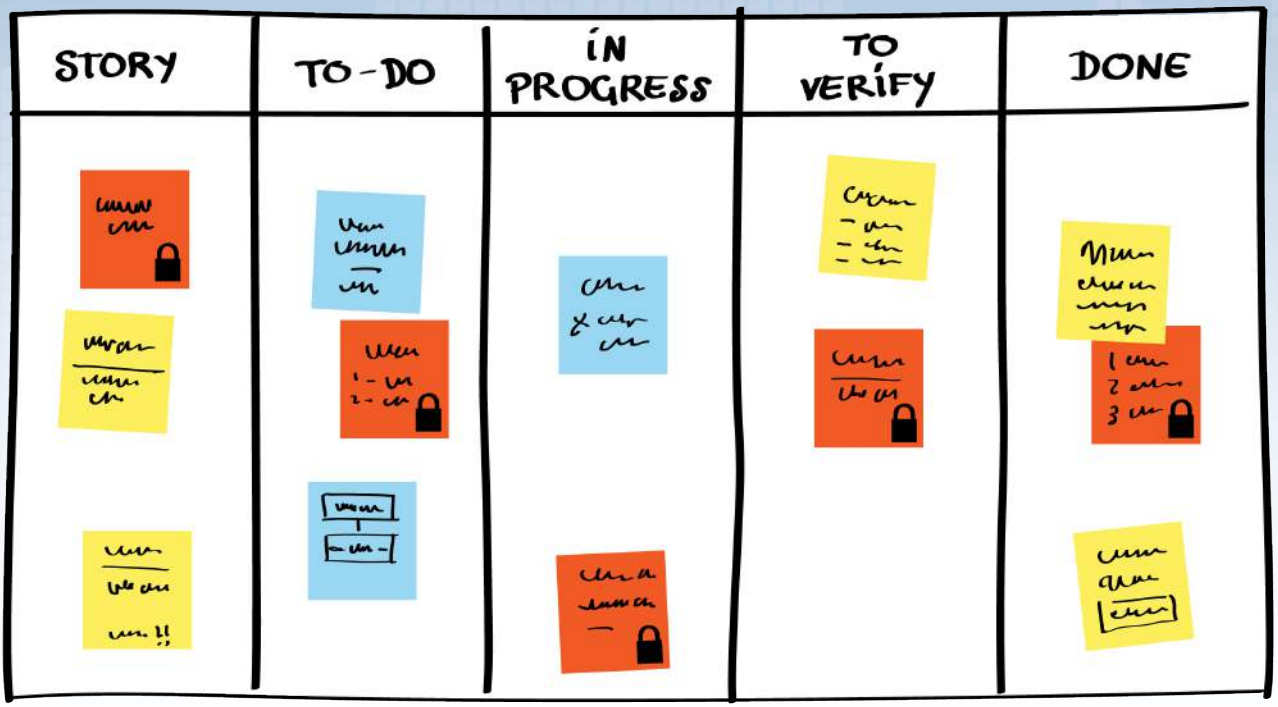




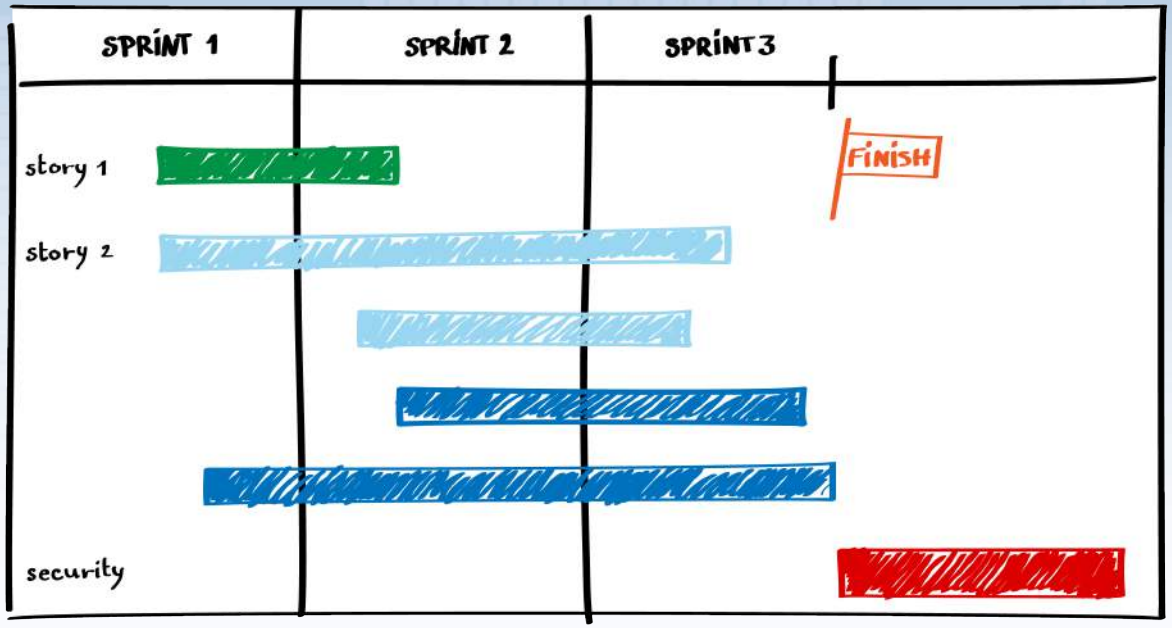
Grooming



Tag user stories / risk based

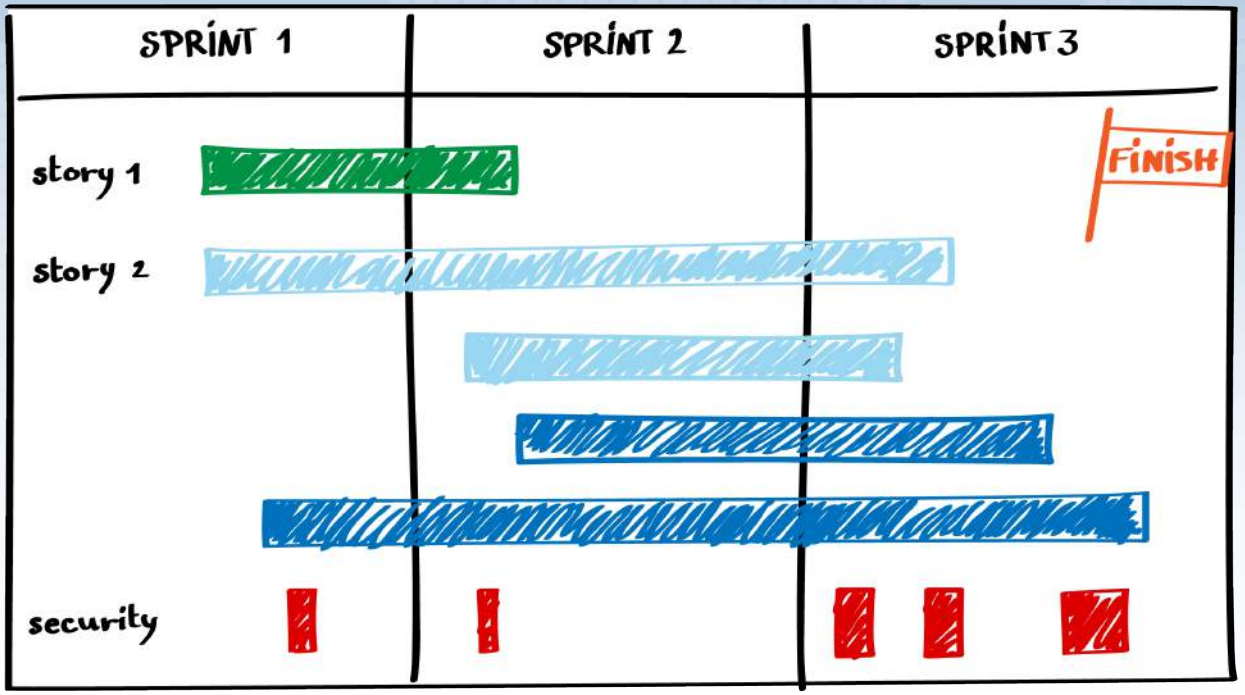


More efficient test/review



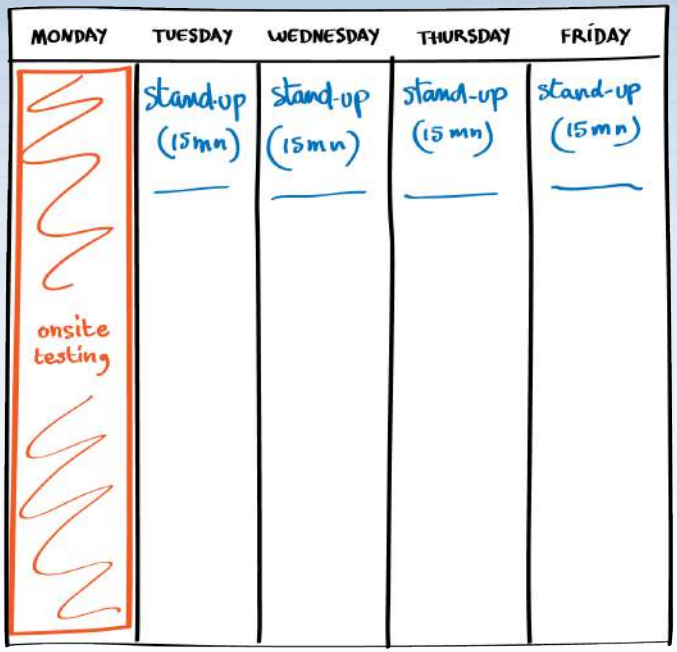
Next: early code reviews

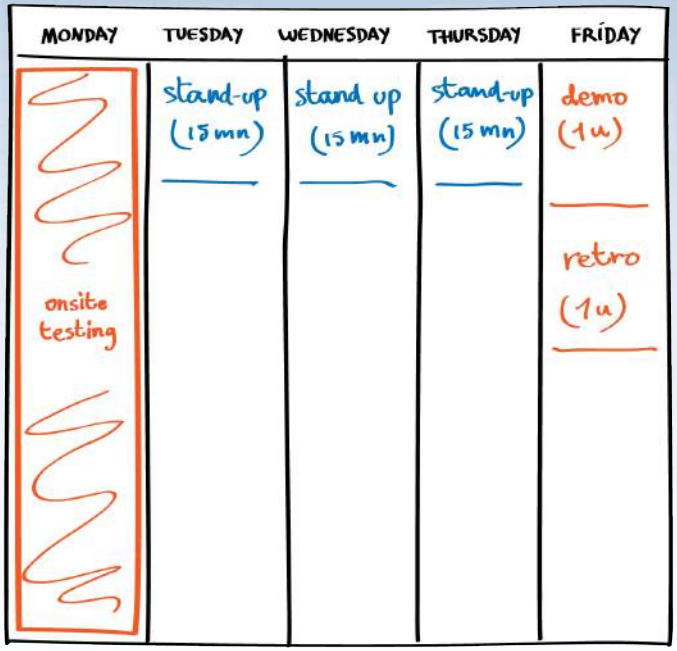
Slicing up this end boss



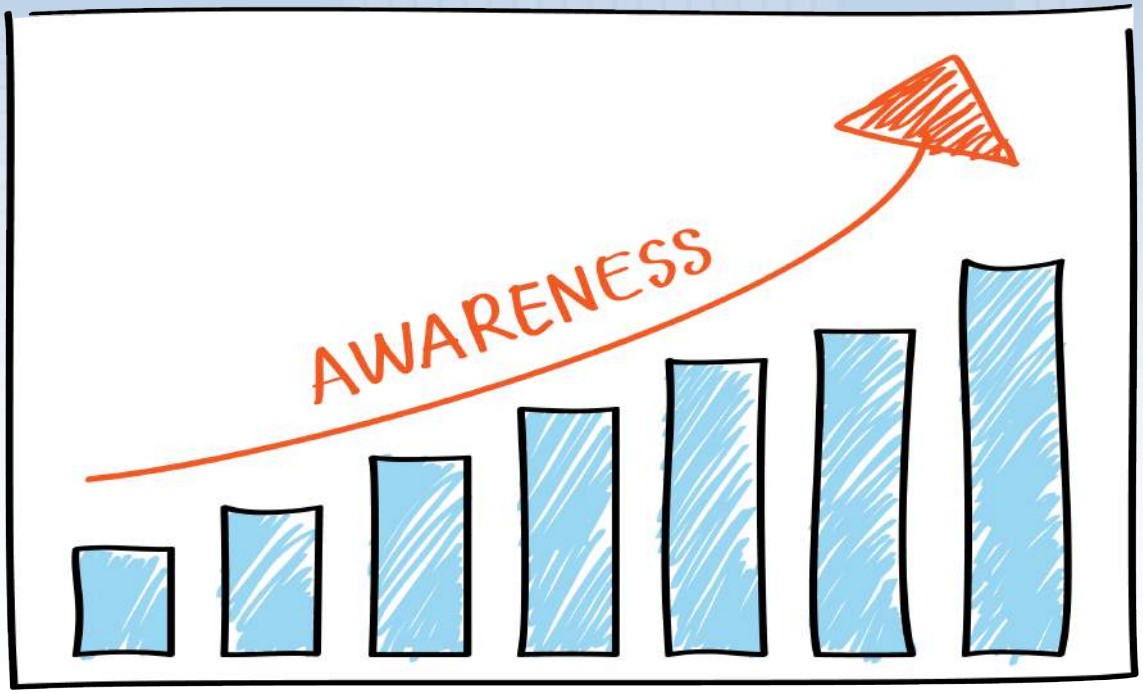
Retro

Better planning

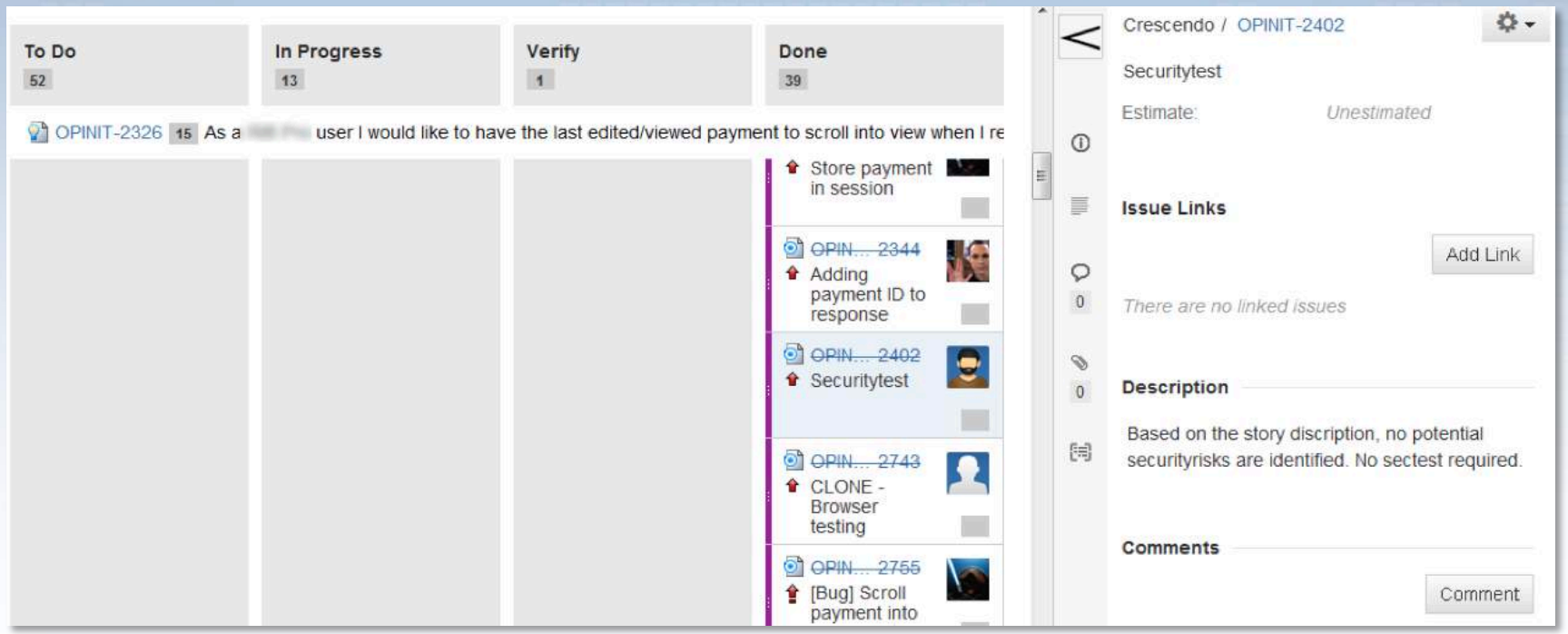




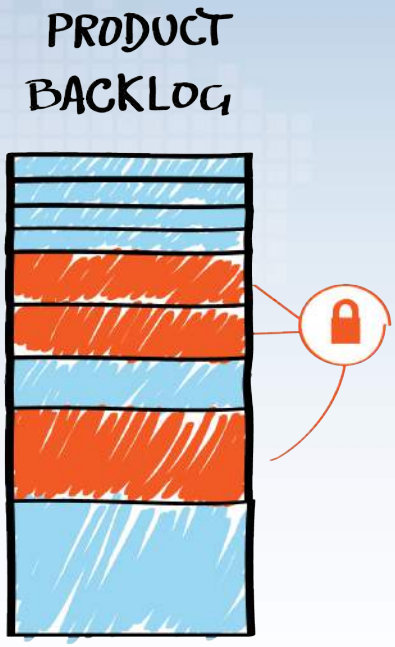
This works

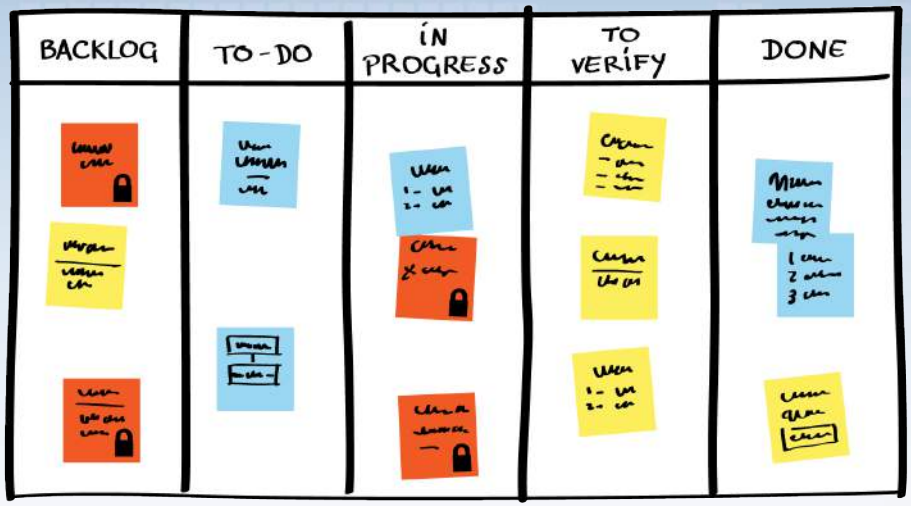


Next: be visible on the board



Next: add findings / create stories

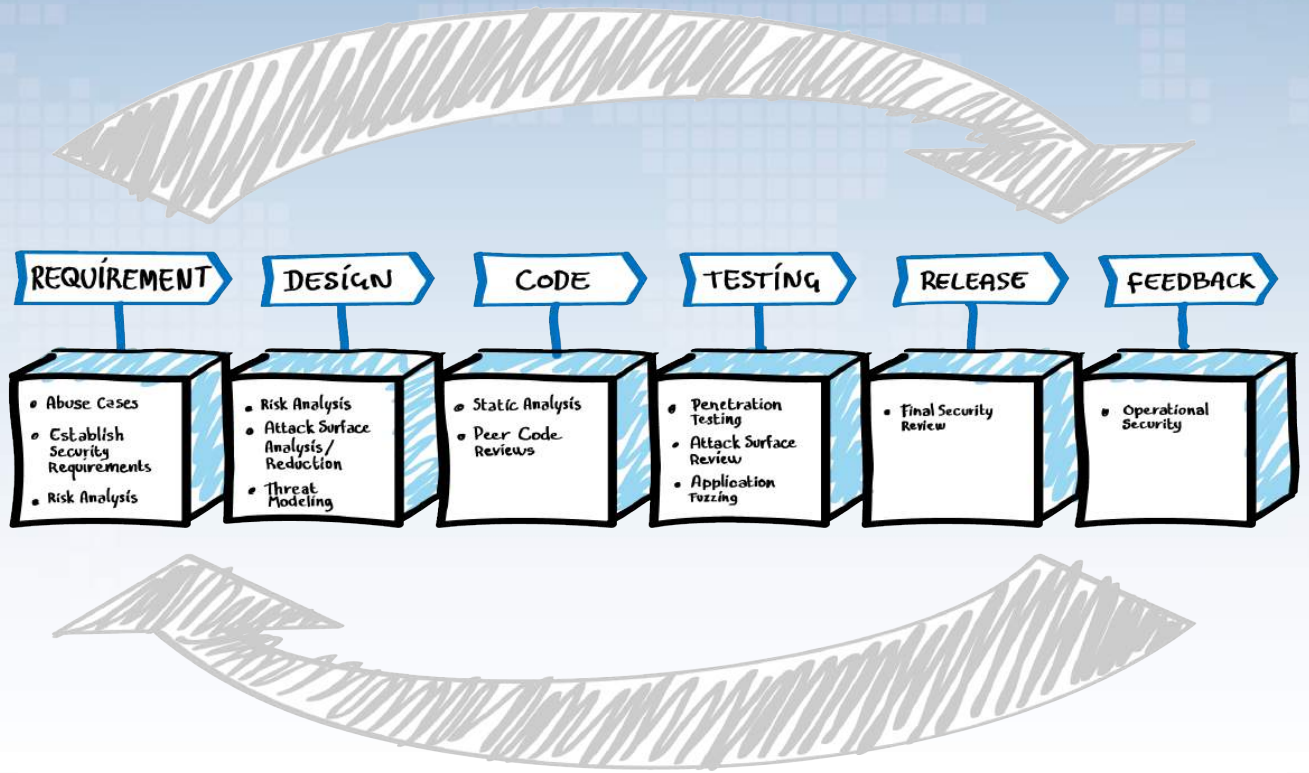




Have (simple) security sign-off

Share knowledge

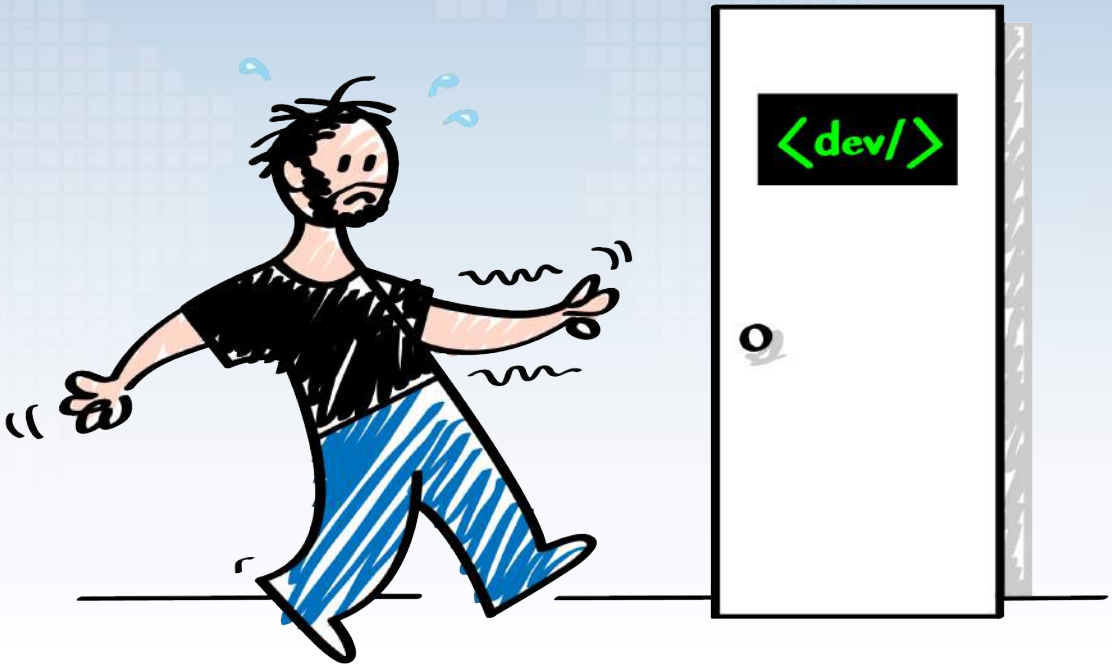
Hey, this all starts to look like..



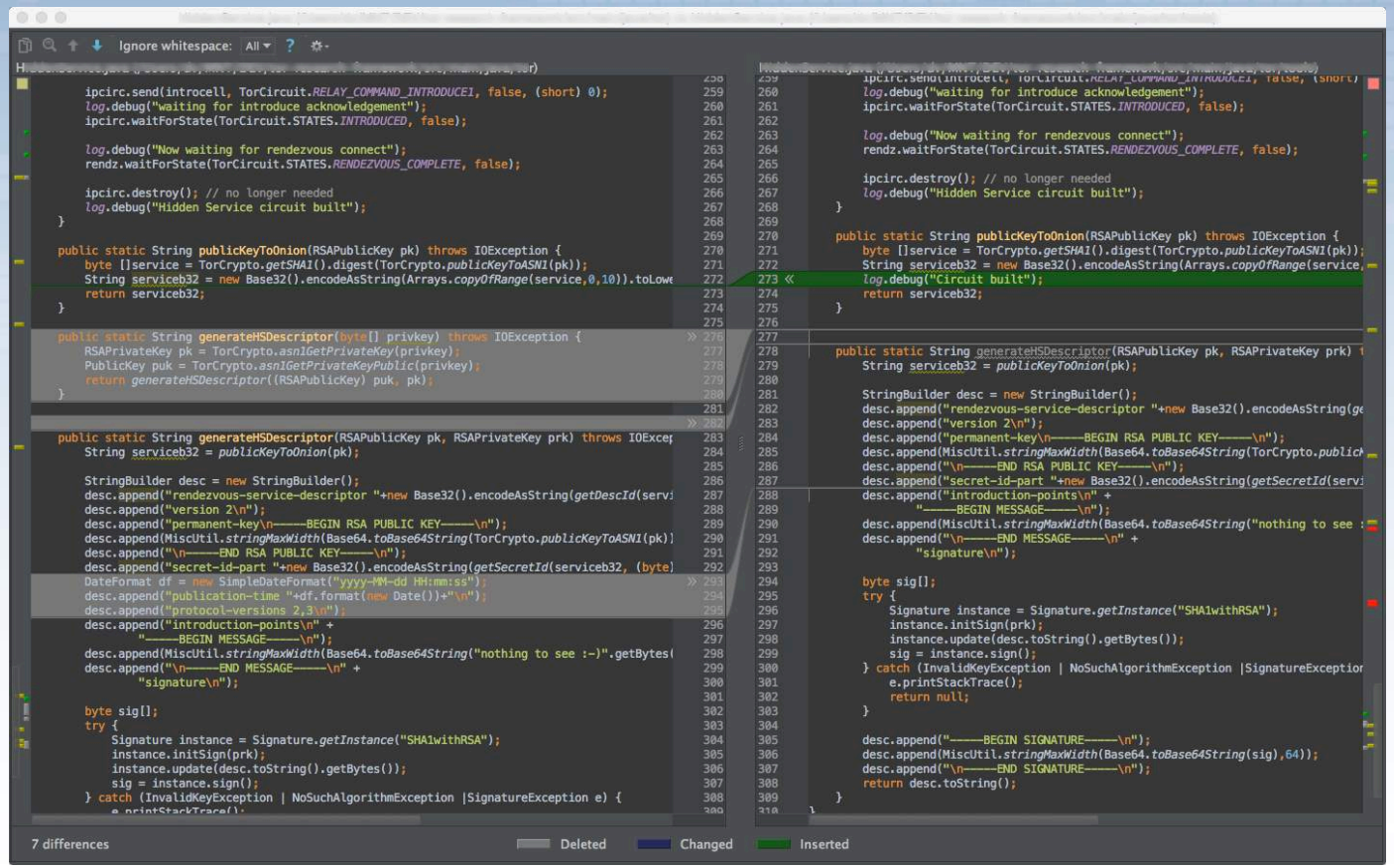
Agile, a blessing for software security?

Takeaways

Security, leave your comfort zone!

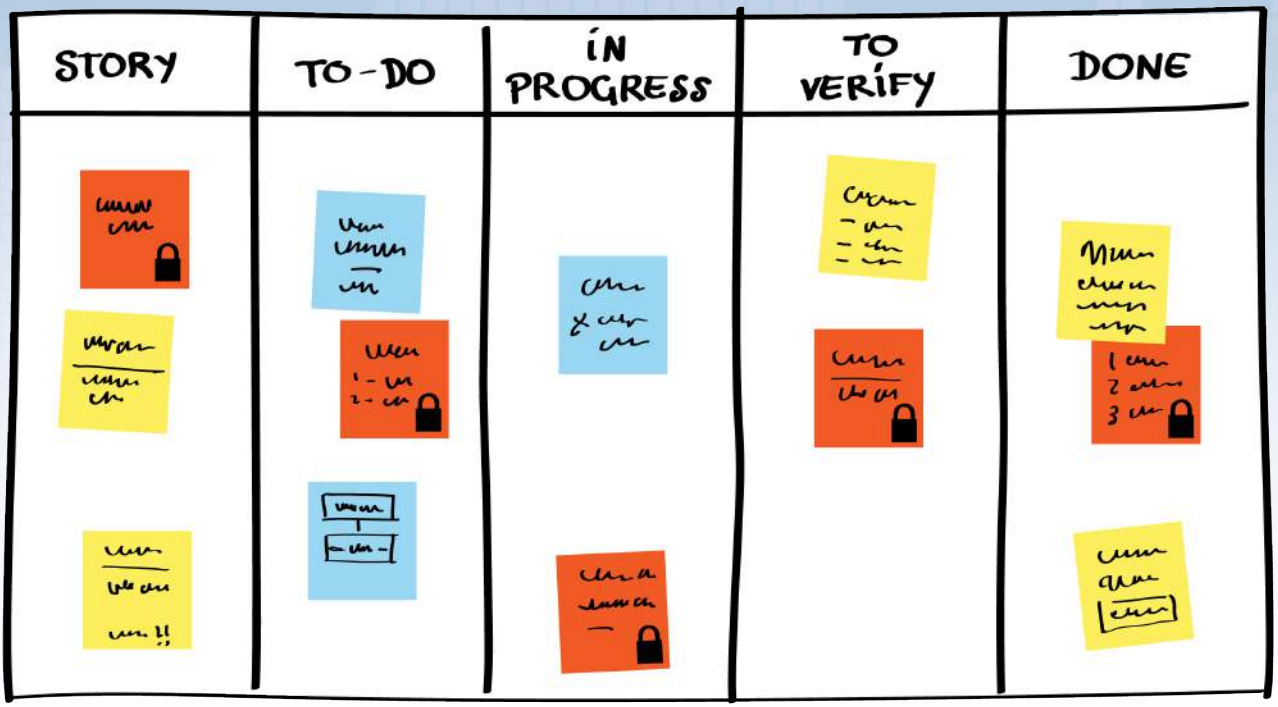


Code reviews over (pen)testing!

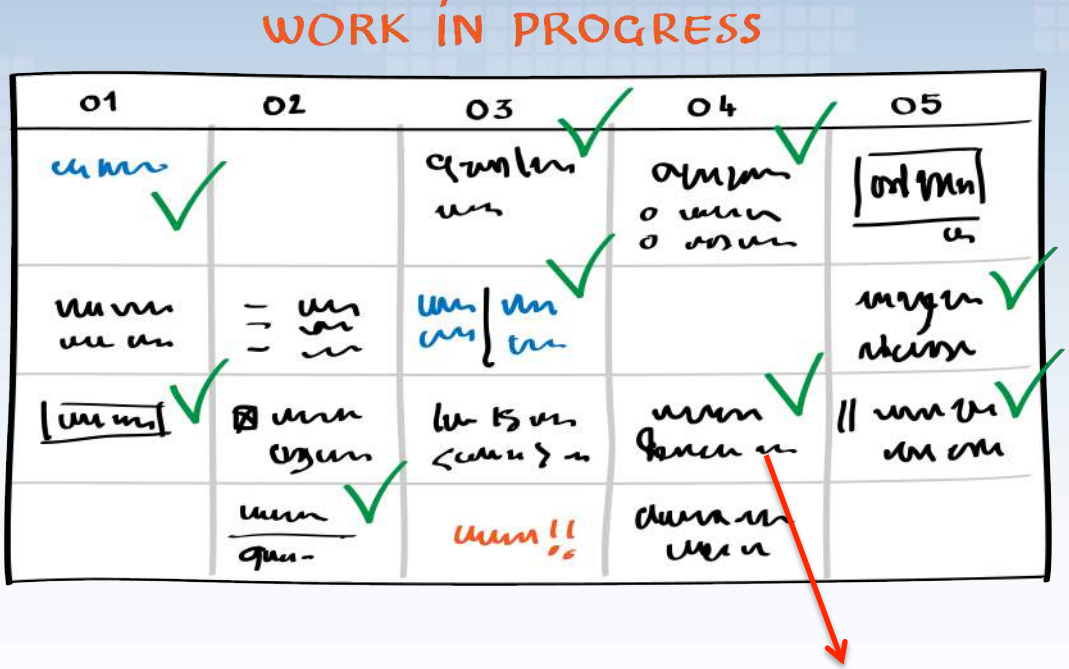


OWASP AppSecEU 15
Amsterdam, The Netherlands

Only test when needed!

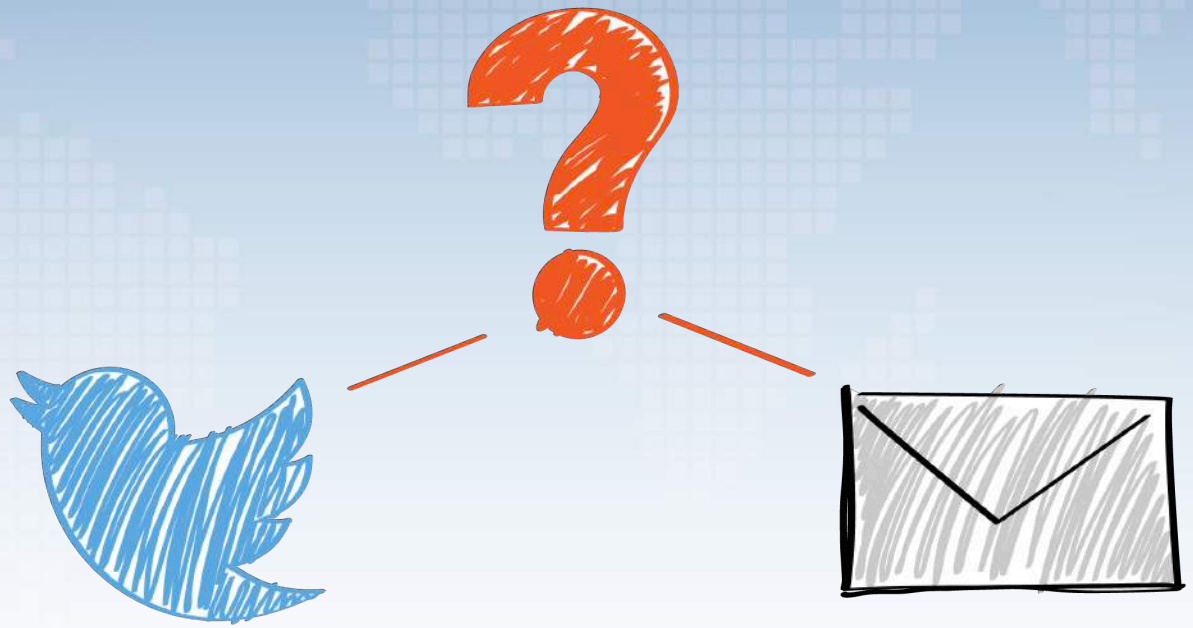


Stay Agile, keep improving!



Automation ;-)

Thanks!



@securifybv

david.vaartjes@securify.nl

Securify

OWASP AppSecEU 15
Amsterdam, The Netherlands