Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS 2021 | PITTSBURGH

Teach a Man How to Fish

16 June 2021

Jeroen Willemsen

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

About me

Jeroen Willemsen
@commjoenie
jwillemsen@xebia.com

"Security architect"
"Full-stack developer"

Agenda

The Situation

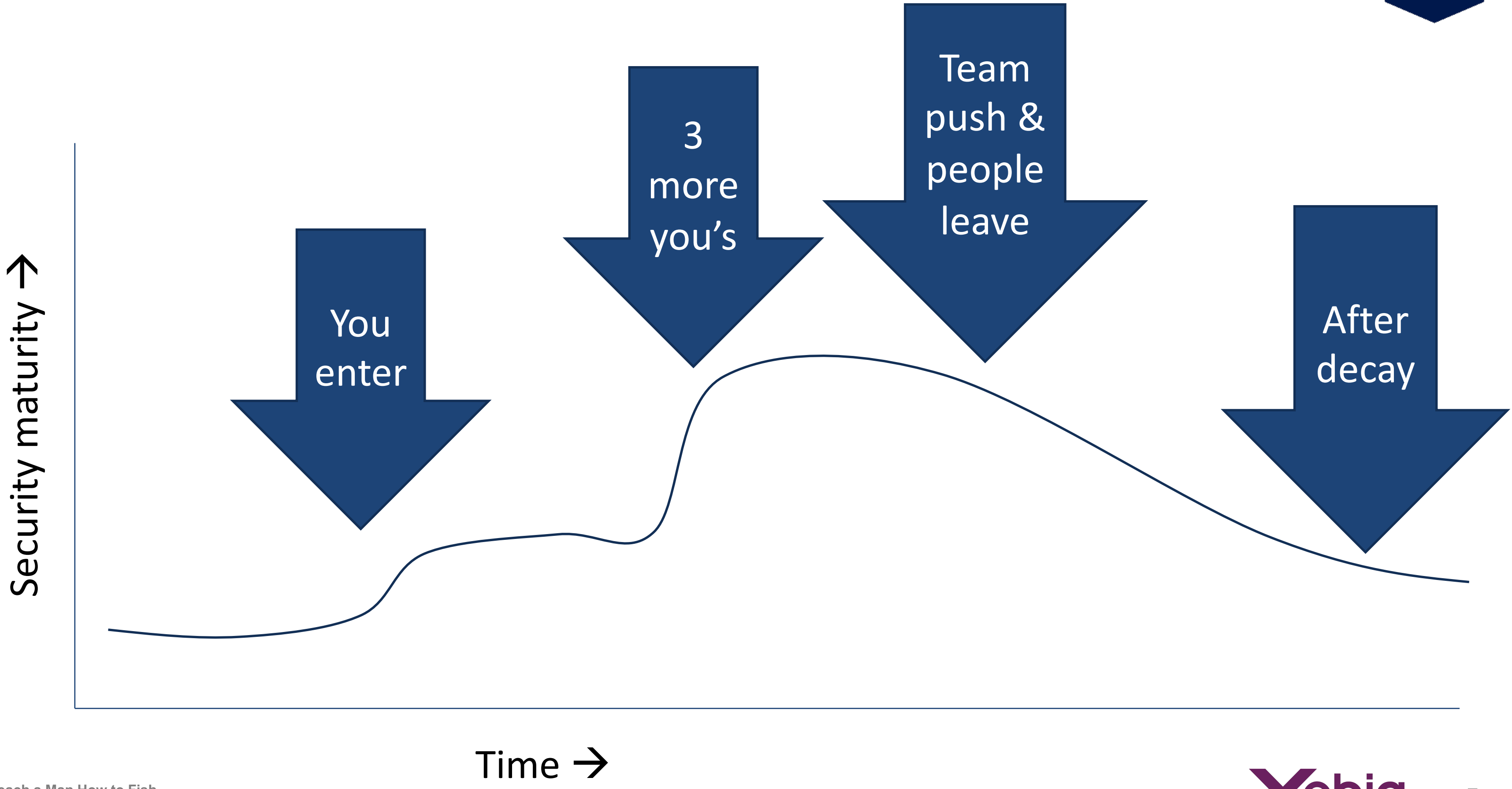
The Security Coach

Pitfalls

Recap

The Situation

You help securing



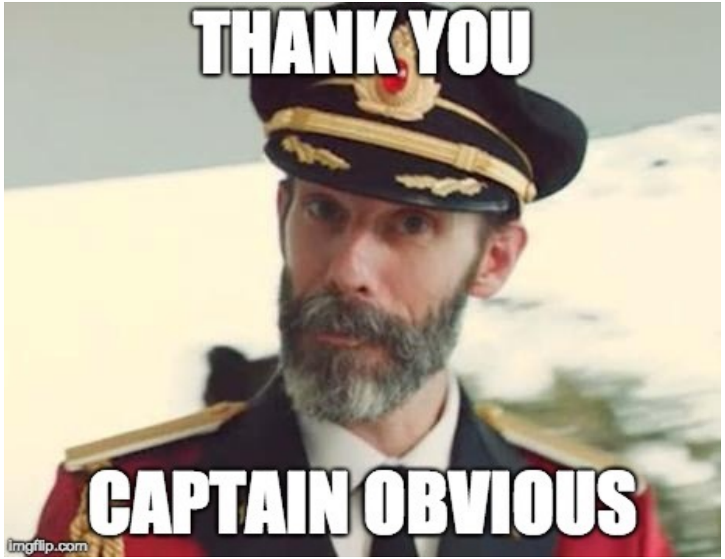
What happened?

YOU are not scalable

Doing the work, means that “someone needs to pick it up after you”

Doing the work, means that “you know”

Doing the work, means you “should not leave”



What happened?

You dealt with the symptoms instead of the problem

Ownership ⇔ Responsibility

Lack of: support, knowledge, budget, et-cetera

Senior management decisions you just don’t know about

Risk appetite is way different

Actual risk is way lower

The Security Coach

COACH WITH THE END IN MIND
WITHOUT YOU
imgflip.com

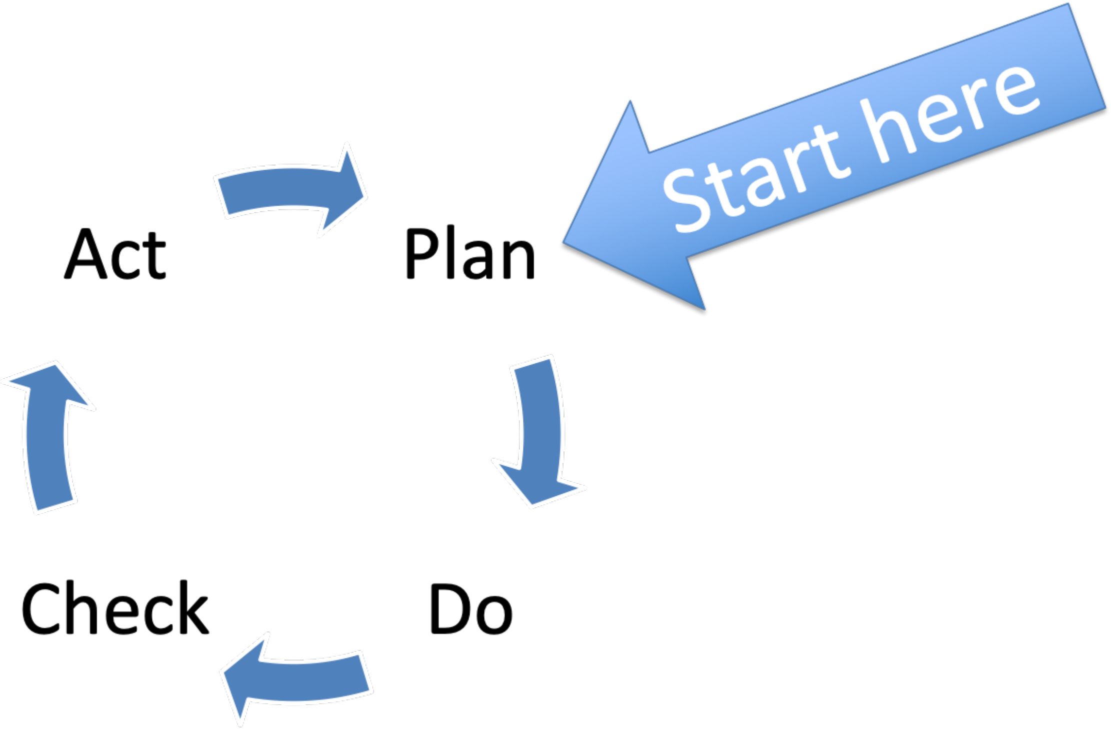
It starts with attitude!

“Don’t feed the Hippo’s” by Martin Knobloch

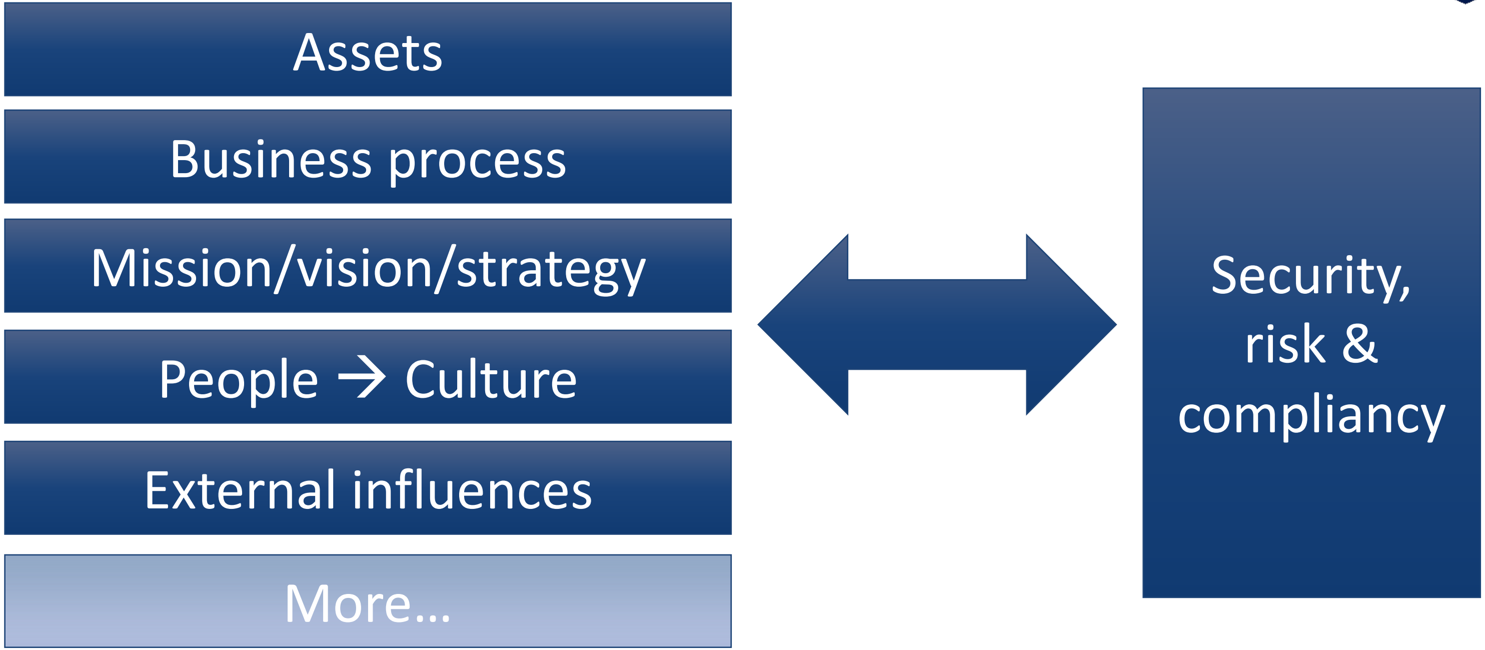
The security coach

What & Why

The security coach



Planning phase



Assets

Business process

Mission/vision/strategy

People → Culture

External influences

More…

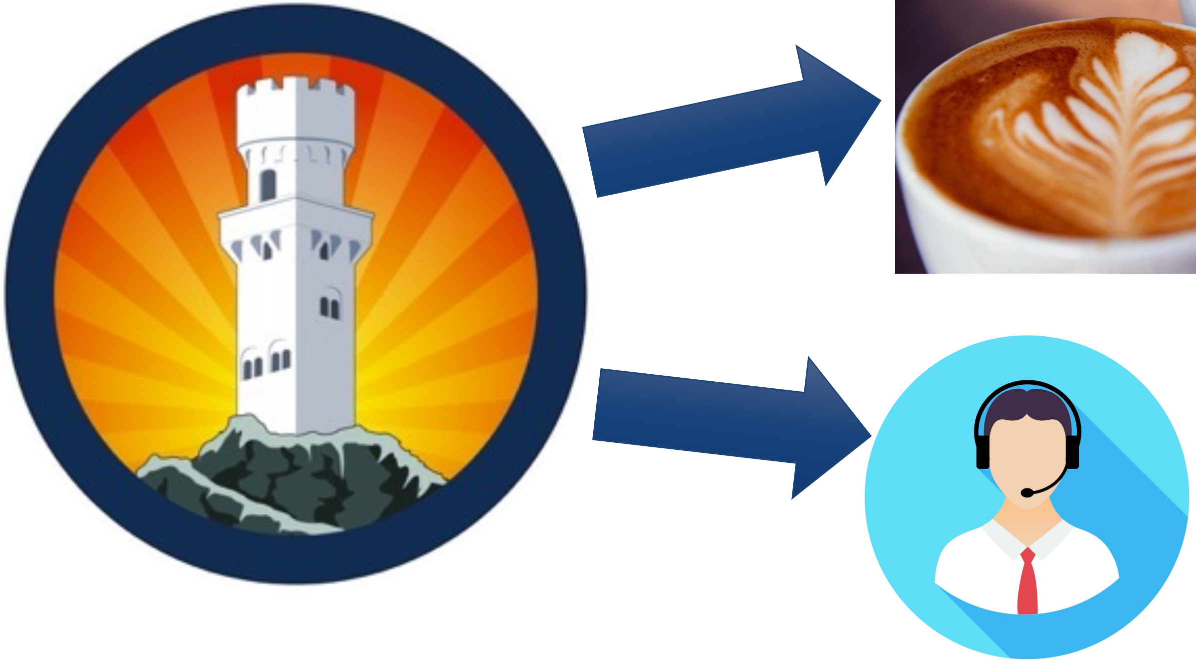
Security, risk & compliancy

Plan is not about the security process

It’s about being (as) holistic (as) possible

Be visible, understand goals, responsability & accountabiliy

Keep in touch



The security coach

"If **you** can't **measure it**, **you** can't improve **it**."

Peter Drucker

Select your elements wisely

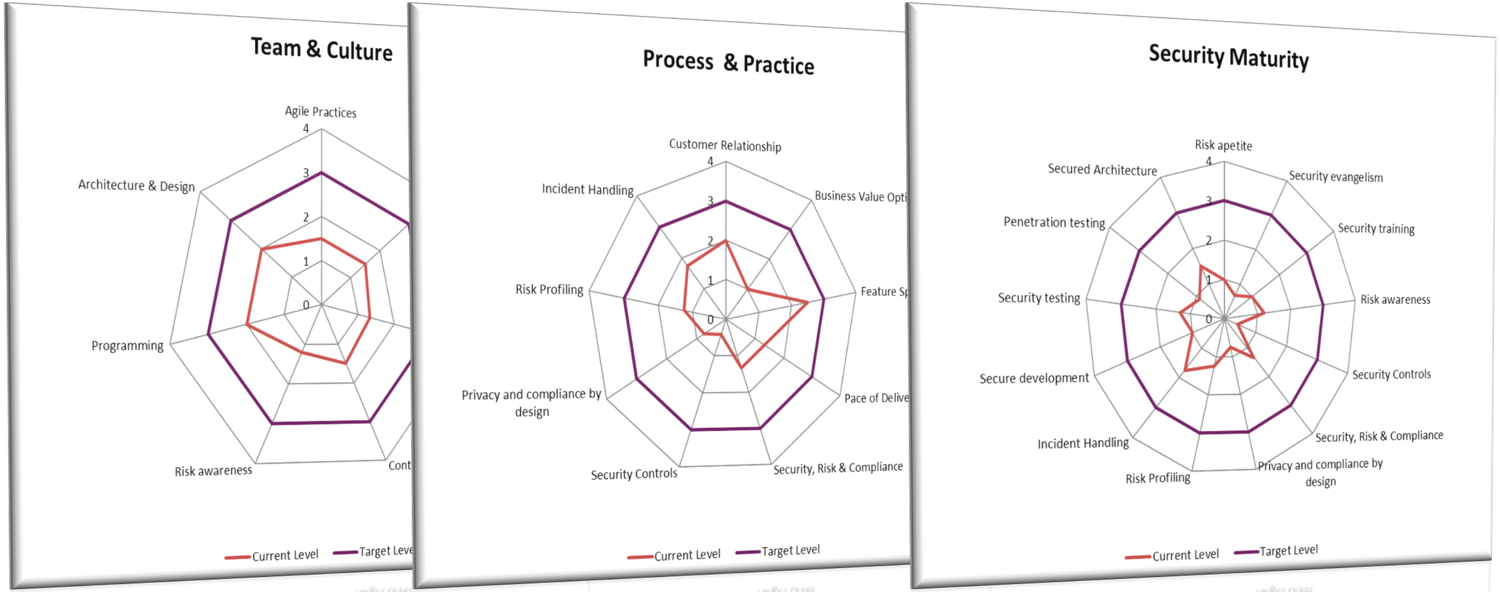
DEVOPS? ⇔ DASA DEVOPS AGILE SKILLS ASSOCIATION

Agile Practices? ⇔ Agile compass

Security Practices? ⇔ BSIMM

… insert focus here ⇔ insert metric FW here (DSOMM,etc.)

FOCUS!!!



Team & Culture

Process & Practice

Security Maturity

Get a headstart: Get & train security teams!

Source: www.hastingskickboxing.co.uk

Raise your champions

Clip slide

DevSecCon | BOSTON 11-12 SEPT 2017

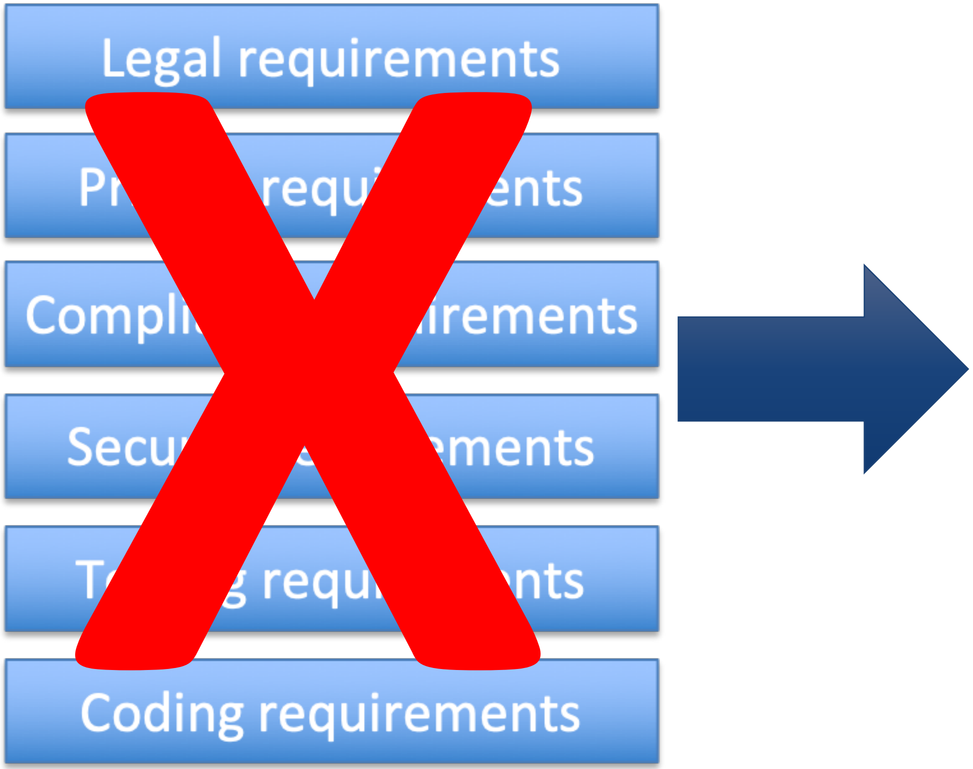
From Rogue One to Rebel Alliance

BY PETER CHESTNA, CA VERACODE

Join the conversation #DevSecCon

"From Rogue One to Rebel Alliance" by Peter Chestna

Don’t overdo it!



Legal requirements

Pr requi ents

Compli irements

Secu ements

T g requi nts

Coding requirements

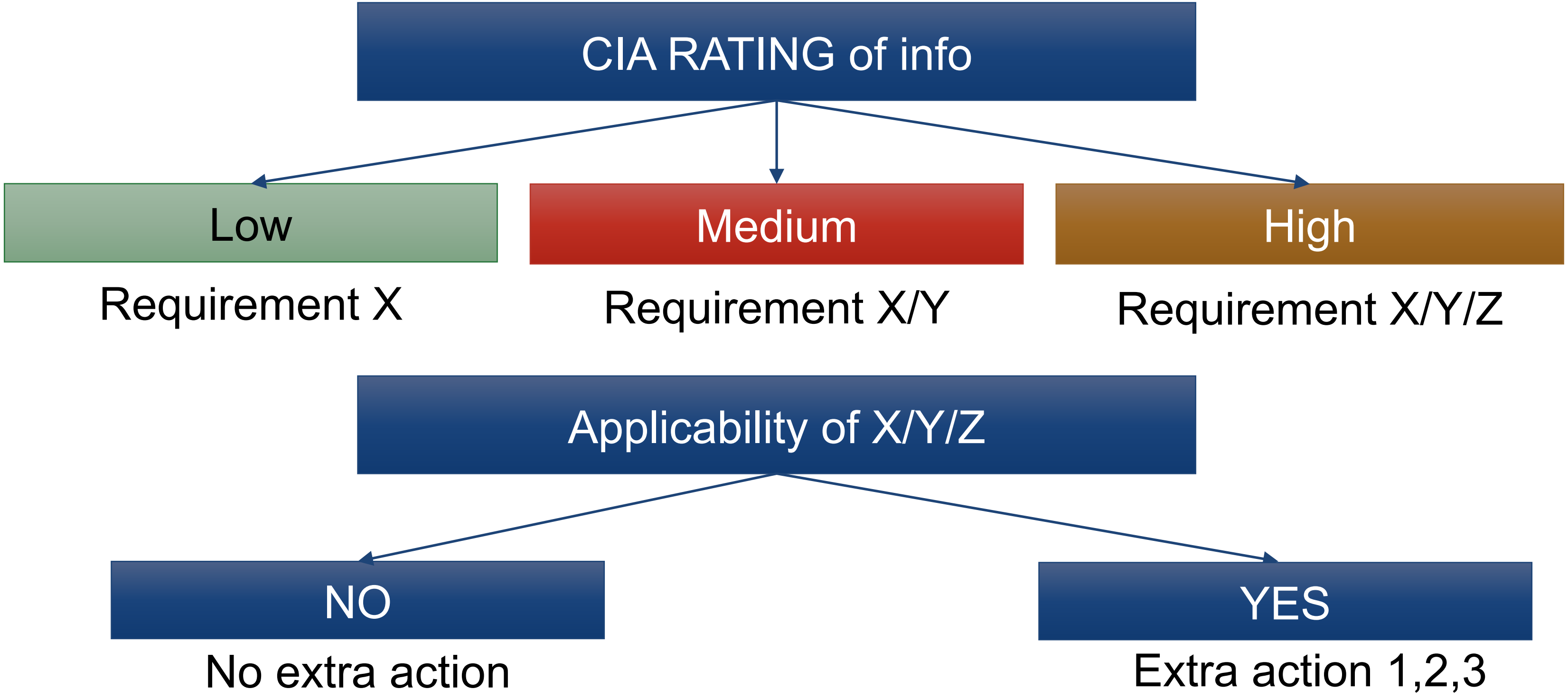
Have the smallest set of requirements based on

Confidentiality

Integrity

Availability

Don’t overdo it



CIA RATING of info

Low

Requirement X

Medium

Requirement X/Y

High

Requirement X/Y/Z

Applicability of X/Y/Z

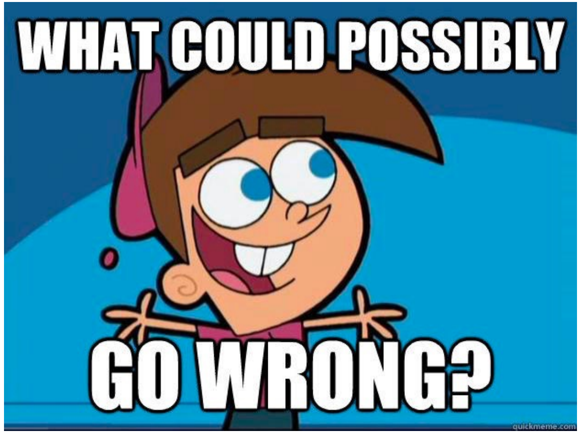
NO

No extra action

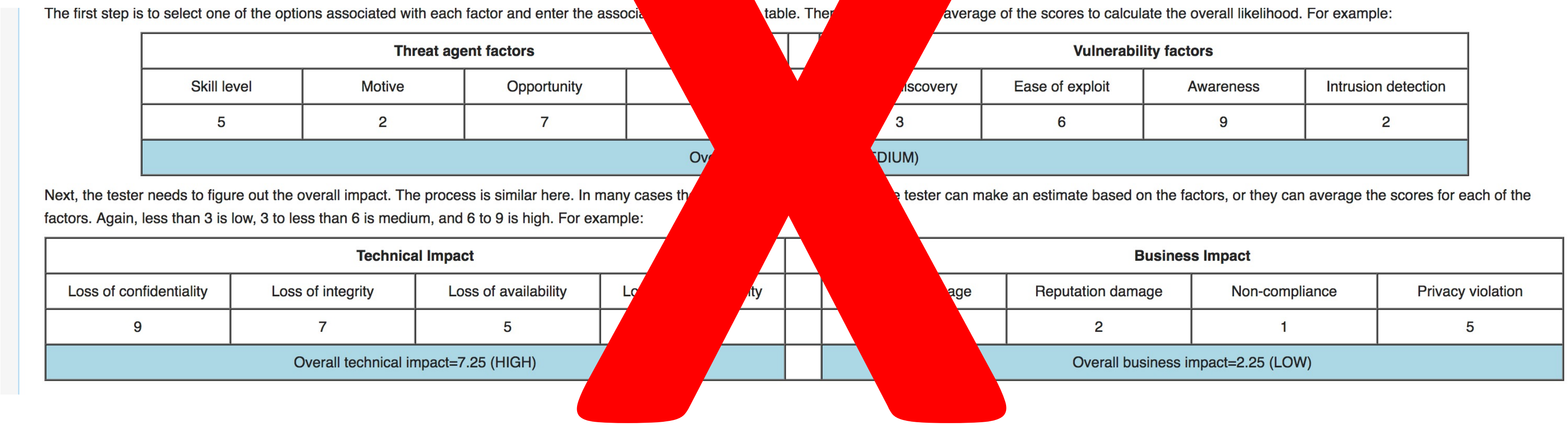
YES

Extra action 1,2,3

Threatmodelling



Threatmodelling



The first step is to select one of the options associated with each factor and enter the associa table. Ther average of the scores to calculate the overall likelihood. For example:

Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity			iscovery	Ease of exploit	Awareness	Intrusion detection
5	2	7			3	6	9	2
Ov				DIUM)				

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases th e tester can make an estimate based on the factors, or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Lo ity		age	Reputation damage	Non-compliance	Privacy violation
9	7	5				2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

Simplify: group characteristics in presets

Give supportive tooling

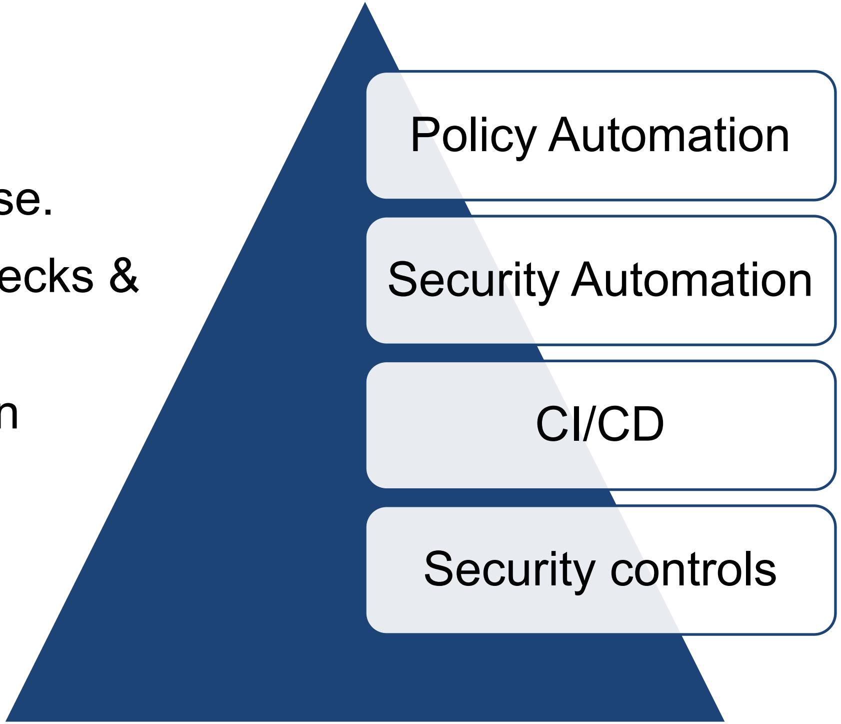
Train teams

Next step: automate!

Integrate in the tools developers use.

Security automation: hardening checks & automated vulnerability checking.

Additionally: security controls are in place: SEM, IAM, etc.


Policy Automation

Security Automation

CI/CD

Security controls

See how & when you can let go

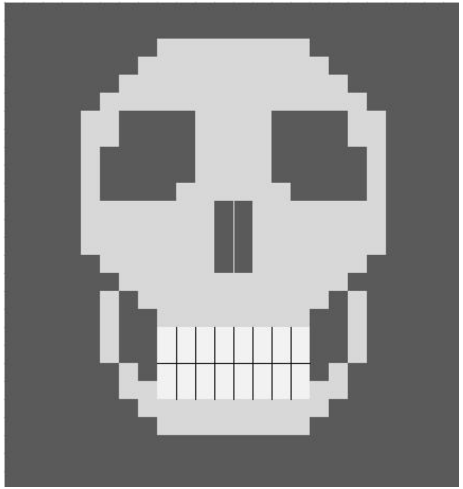
Source: http://barbschmidt.com/

Never forget!

Source: medium.com

Pitfalls

Add too many processes & steps



Developers want to code…

Not do your paperwork…

Embed & automate

Let the developer dig for requirements

Referencing your documents

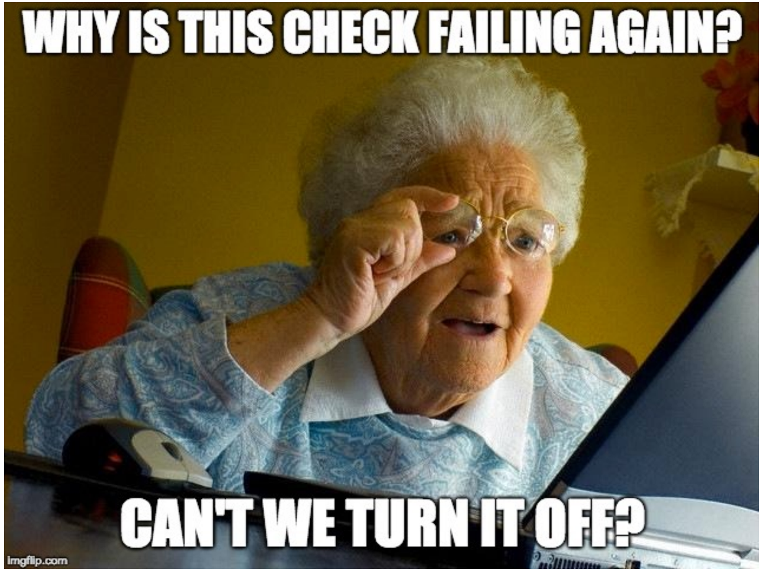
Give him long lists of items

Embed & automate

Forget to measure

"If **you** can't **measure it**, **you** can't improve **it**."
Peter Drucker

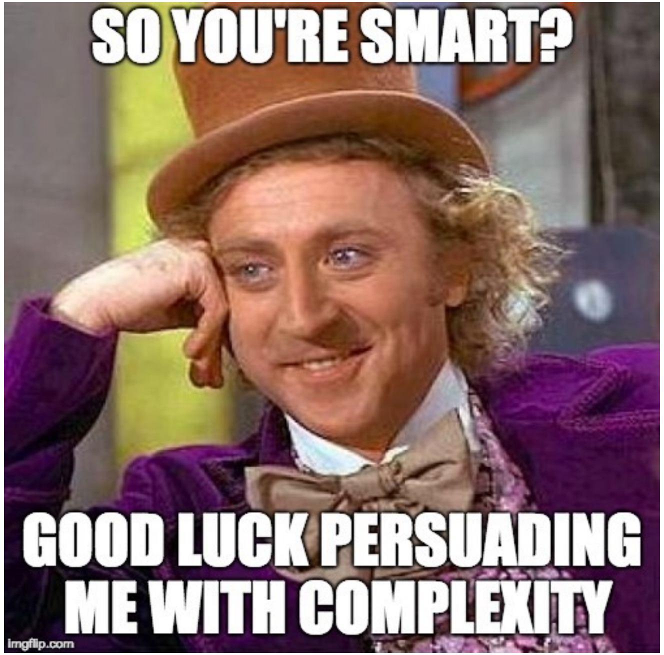
Deliver “Finalized” products



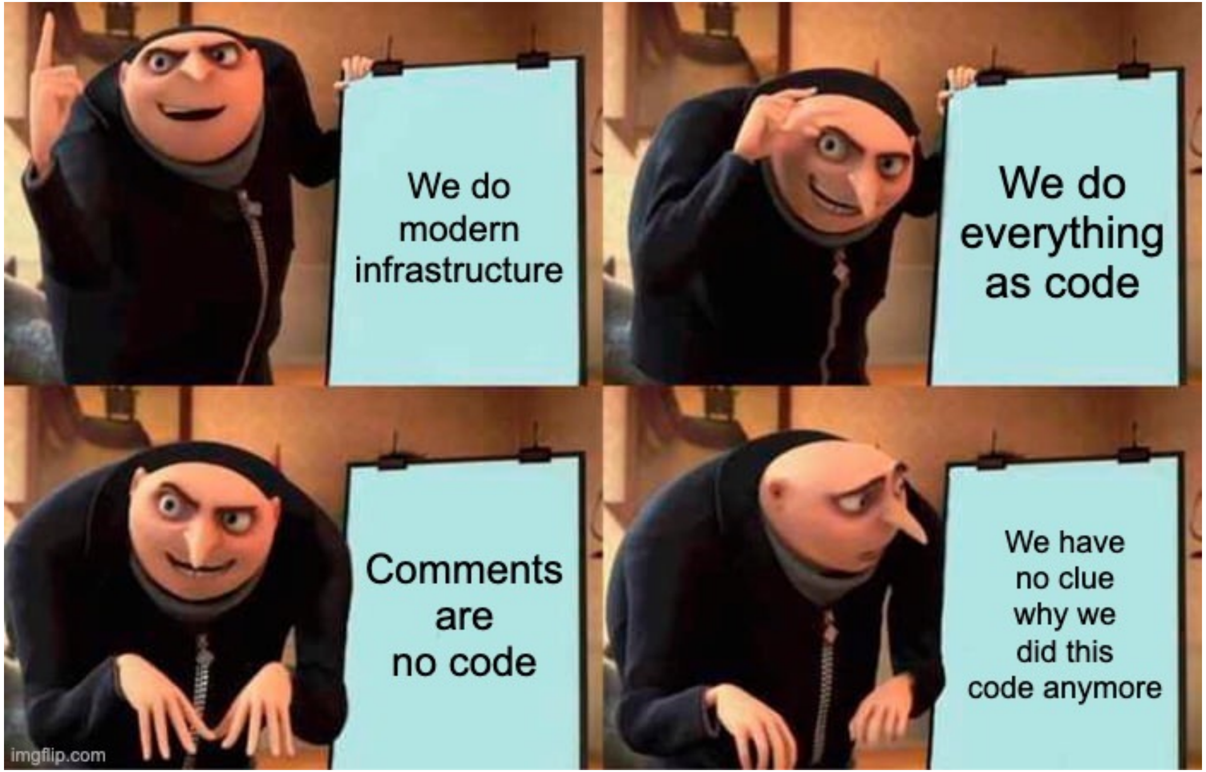
GRUMPY CAT DOES NOT LIKE YOU
BECAUSE YOU LEFT BEHIND A COMPLEX SYSTEM
imgflip.com

Making it complex

ONE DOES NOT SIMPLY DO
SDLC
imgflip.com



Too little architecture


We do modern infrastructure
We do everything as code
Comments are no code
We have no clue why we did this code anymore
imgflip.com

Chief excuse officer

If you blame someone else, you cannot fix the problem

If you blame circumstances, you will not have control

NOTE: this is not easy…

… Do as I say… not as I do ☹

Wanting to hold on

Holding on makes you irreplaceable

Holding on will make you defend your progress

Holding on will make it harder to get to new ideas & concepts

Holding on can complicate things

Recap

Recap

Start analyzing with the end in mind

Have proper metrics & measure

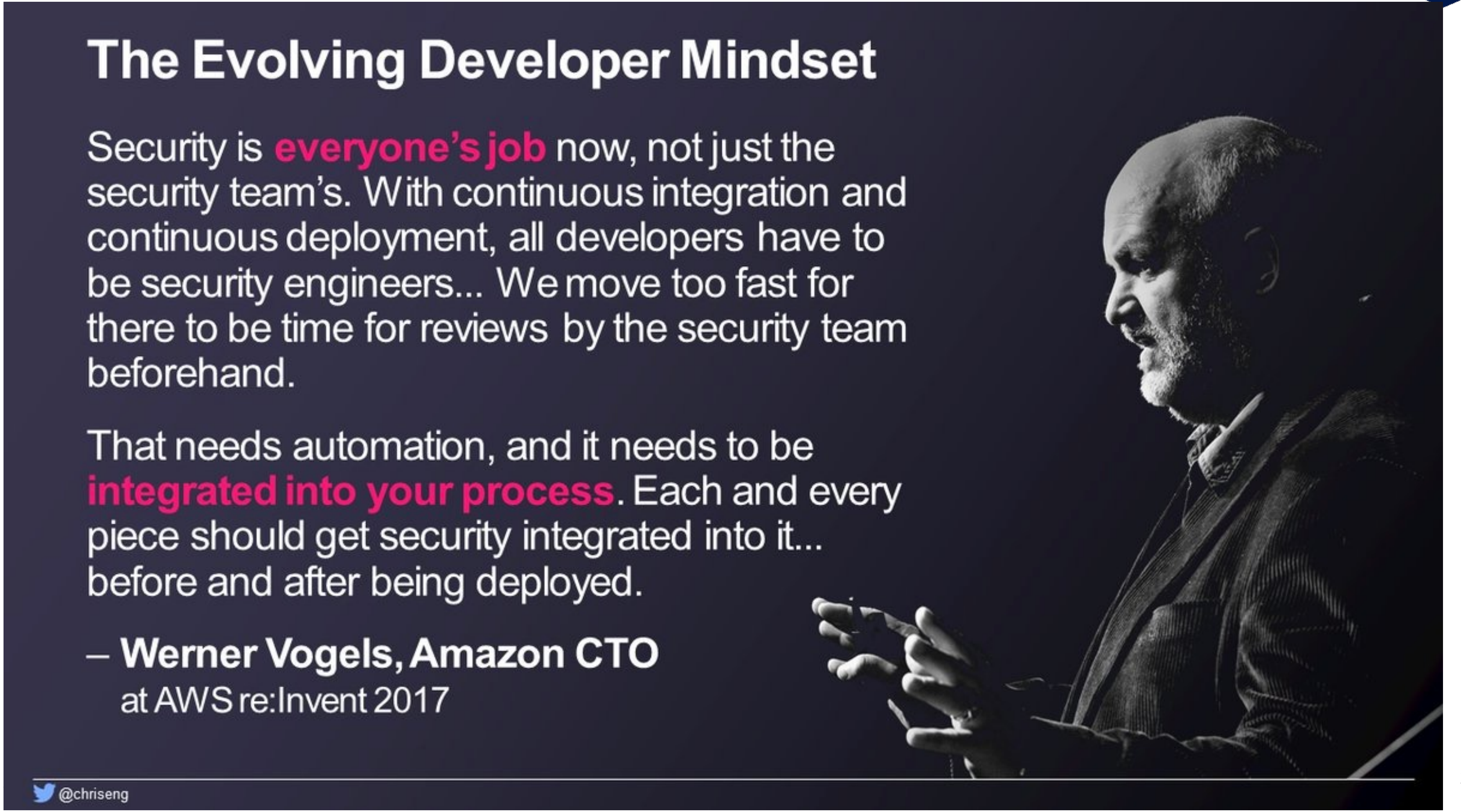
Train your security team, developers & champions

Don’t overdo & overcomplicate

Automate as much as you can

Raise teams with you leaving in mind

Questions?



The Evolving Developer Mindset

Security is **everyone's job** now, not just the security team's. With continuous integration and continuous deployment, all developers have to be security engineers... We move too fast for there to be time for reviews by the security team beforehand.

That needs automation, and it needs to be **integrated into your process**. Each and every piece should get security integrated into it... before and after being deployed.

– **Werner Vogels, Amazon CTO**
at AWS re:Invent 2017

@chriseng

Carnegie Mellon University Software Engineering Institute

DEVSECOPS DAYS

PITTSBURGH

Questions?

@commjoenie

jwillemsen@xebia.com

https://s.truqu.com/B3MJmJ