ROMA
MMXVI

APPSEC
EUROPE

Tell me stories about your appsec, let's skip the pentest

Qualitative and narrative interview in security audits and appsec improvement
by Timur 'x' Khrotko @ AppSecEU16

@timurxyz

- Timur 'x' Khrotko, PhD
- x@secmachine.com (secmachine.net)
- hello@defdev.eu
- timur@owasp.org
- linkedin.com/in/timurx

agenda of goo.gl/FFWxy1

- what is the interview-based research
- why to use it in appsec audits and consultancy
- the organizational culture is the context
- culture types, quality assurance and appsec maturity

the main points of goo.gl/FFWxy1

- capturing and describing S-SDLC problems is also possible based on interviewing managers and workers
  - instead of measuring the symptoms with dynamic and static methods
- the participants of the development processes themselves most of the times are aware of the problems
  - or they can tell stories from which a competent interviewer then can interpret the presence of appsec problems
- management friendly
- interview-based method becomes more adequate and efficient ín organisations with mature appsec practices
  - or with established QA culture
  - the target is improving production (building) and thus the appsec quality

interview-based research

- organizational research, not engineerish
  - talks with managers and workers, analysis of the texts
  - not a technical interview
  - oral account of the real-life world
  - postmodern (interpretation, re-interpretation, deconstruction, social constructions)
- a qualitative research method
  - eg. narrative interview
  - subjective interpretations ahead, questions predefine the answers
- audit/coaching is not a research
  - a reuse of the instrumentation created for organizational developers (OD)
- many businesses will never allow you to ask such questions
  - and it’s a managerial virtue to communicate the reality as they want to show it

bits of a how-to

- NDA, send an introduction letter, agree on the rules
- create trust
  - "It was my story several years ago …"
- questions like:
  - What would be your strategy in selling application security to your CEO? Is there any real life story regarding this?
  - What are the tasks in the secure development lifecycle that frustrate developers the most, and which frustrate the security people the most? Tell a couple of short stories!
  - Tell me stories about testing the products for security quality! How was it two years ago, how is it done now?
  - there may also be tricky questions
- prepare, 1.5 hrs, take notes, use tools
- interview analysis and report

why to use interviews

- many issues with the appsec in the production (and procurement) have root causes of organisational nature, and are methodological and process related
  - hunting root causes
  - production improvement vs quality control
- the participants most of the times are aware of the problems
  - but living in a box needs an outsider to rethink things
  - competent interpretation
- consultancy is needed for change
  - capture, observe, discuss, document it, find solutions, implement changes, coach, revisit
- interview vs vapt
  - vapt audit findings are gibberish for the decision makers
  - use in a combo with a vapt report

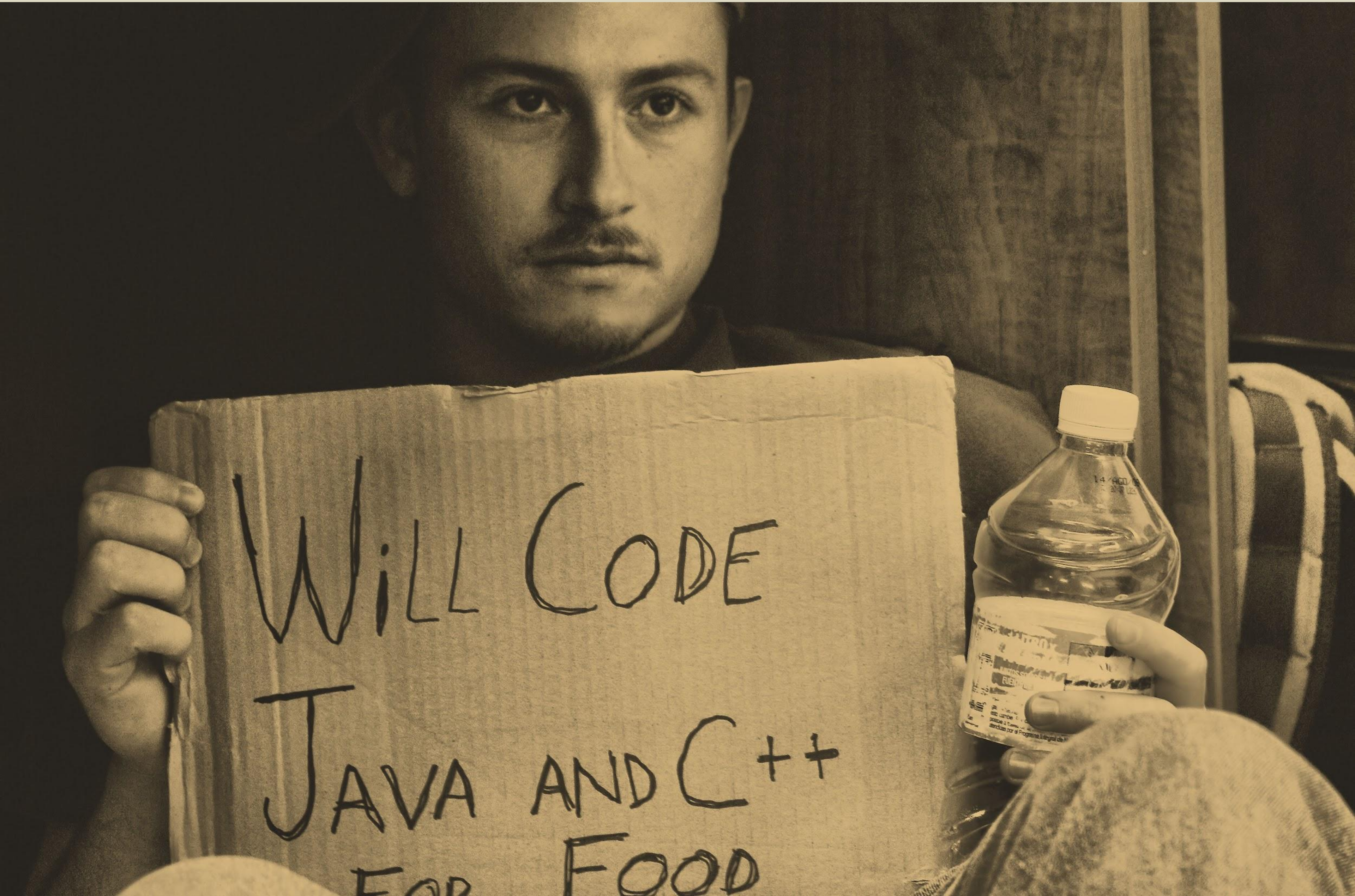
why to use interviews, contd.

- the meaning is understandable for the management
  - of the objectives, of the talks and of the reports
  - Utlish
  - the added value is understandable, so call the budgets
- upselling a consultation is an opportunity
  - consult the sec folks and devs
  - make group sessions
  - coach
- organisations with mature appsec needs it
  - a start for the S-SDLC reengineering project
  - revision of the decision making and responsibilities

appsec maturity
/ type of culture of the QA (appsec)

Mature				
Advanced				
Basic				
	Requirements driven	Champion sustained	Engineered regulations	Collectively engaged

Corp culture: ‘Requirements driven’ (‘’the untrustable devs’’)



Corp culture: ‘Quality sustained by the champions’

Corp culture: ‘Engineered regulations’ (compliance driven)

Corp culture: ‘Collective engagement’ (in quality and methodologies)

appsec maturity
/ type of the culture of the appsec QA

Mature			banks	x
Advanced	security aware production	software houses	compliance subjects	startups w QA mindset
Basic	the mass market			
	Requirements driven	*Champion sustained*	*Engineered regulations*	*Collectively engaged*

end of goo.gl/FFWxy1

- timur@owasp.org
- x@secmachine.com
- hello@defdev.eu
- @timurxyz