Have We Penetrated Yet ???

You, me and a pentester

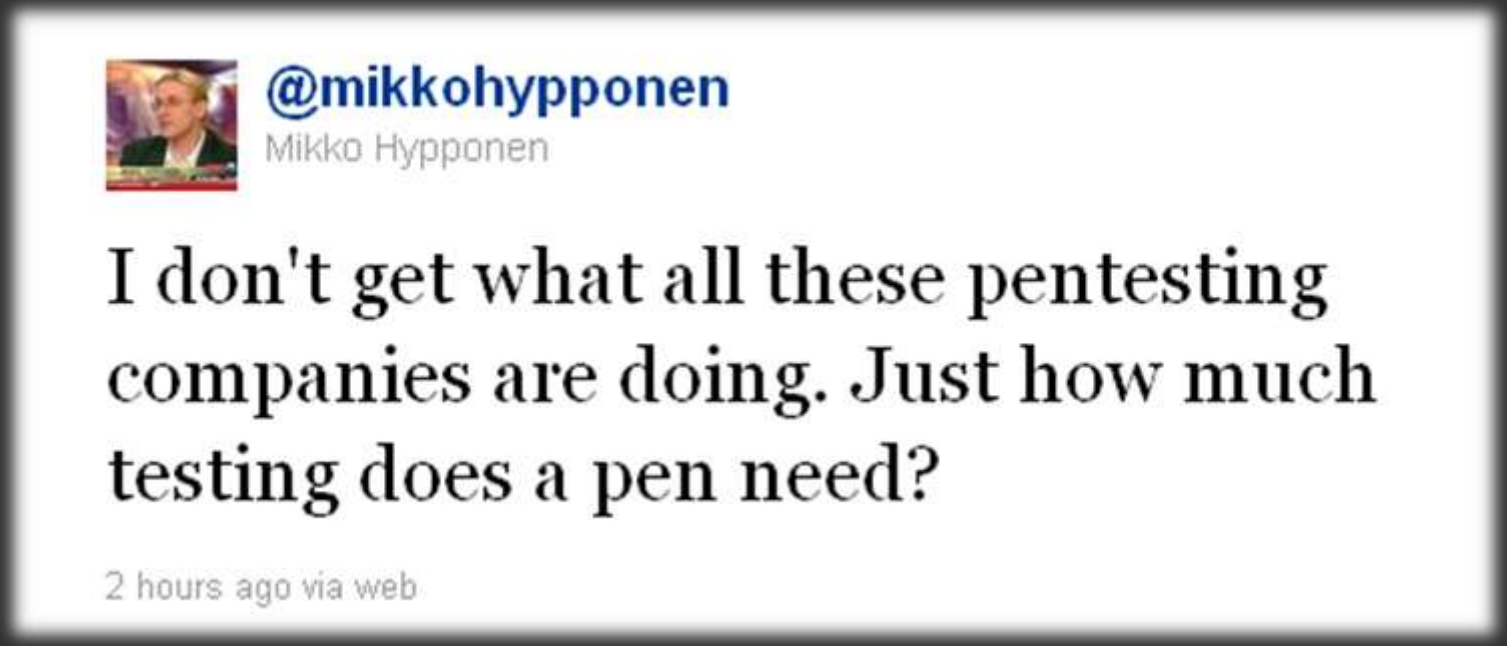
20 November 2015

EY
Building a better working world

Agenda

- Introductions
  - Why am I having this talk?
  - Type of PTs
  - How do we see it VS. How the client sees it
  - The Challenge (seeing this with the eyes of the client)
- Successful interactions (4)

Pentesting in a nutshell



Why am I having this talk?

When we say pentesting

- Hybrid Testing
  - Social Engineering
  - Red teaming
  - Process Controls
- Focused Testing
  - Infrastructure
  - Application
  - Embedded
- Compliance Testing
  - Internal Audit
  - Regulatory
  - Compliances (PCI…)

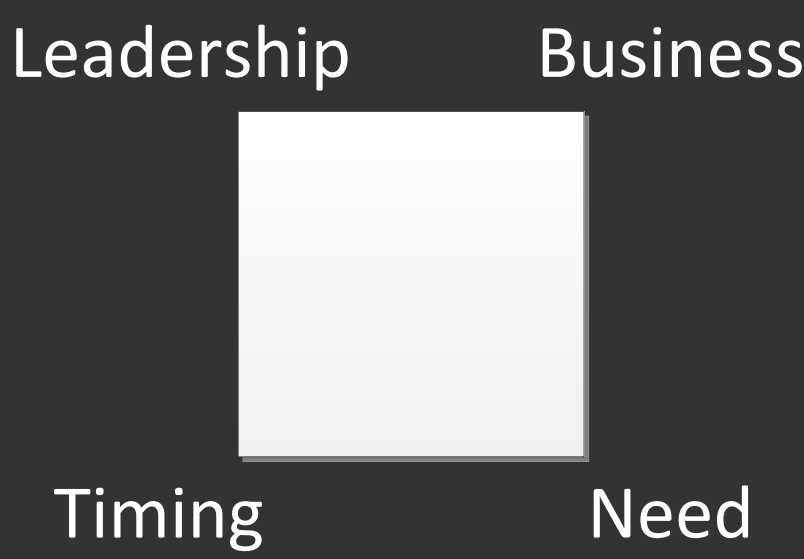
App VS. Infra

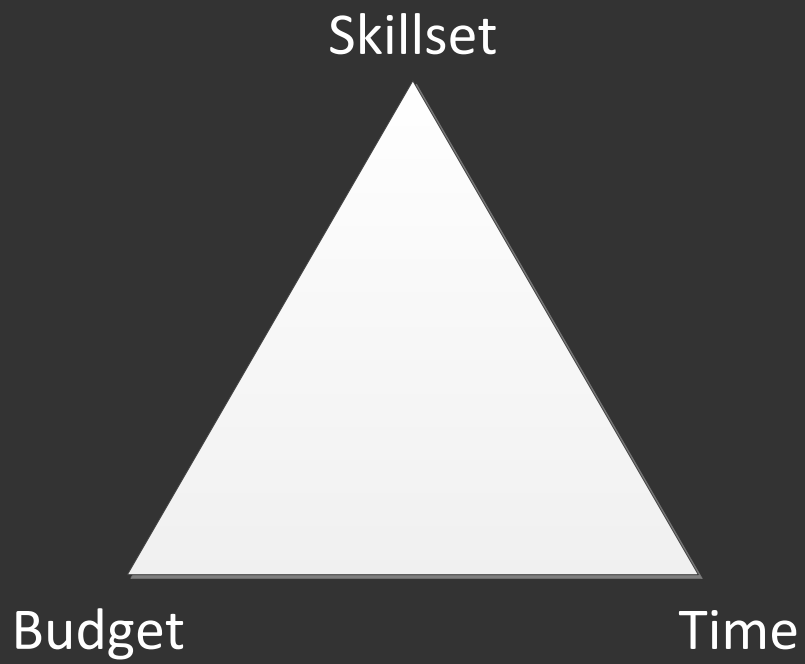
- Where does the problem lie?
  - Fixing infra, is somewhat easier…
  - We most likely have the right resources
  - We can mask it, kind off okay, if we don't want to fix it right away
- But on app sec
  - We need the right people to get it
  - The right people to fix it
  - The right process to prevent it from happening again

How do we see it VS. How the client sees it

- When do we normally get called?
  - One offs
  - Post breach
  - The board asked us what are we doing around CYBER
  - They are trying something new (cloud, big data, cloud, big data)
- When do we want to get called?
  - They made a strategic decision
  - The client is fully aware of the business process
  - The client is fully aware of the risks the organization is facing
  - The client knows what they want to test out

The Challenge





Interactions

interaction #1

- Black boxing you
  - “I want to see how real attackers can get in”
  - “Don’t spend too much time on the scanning bit, I want you to start with the attack”
  - “I can see you attacking me…”

interaction #1

- Black boxing you
  - Red Team is a black box, all else…is not really…
  - “Real world attackers” VS. Pen-testers
  - Let’s talk grey boxing this

interaction #2

- What environment do we test?
  - “I want to see how a real scenario will play out”
  - “carful, it’s a prod environment”
  - “..in the actual environment, they have implemented this a bit differently…”

interaction #2

DEEPSEC

- What environment do we test?
  - There is no real one liner here
  - This is all up to honestly, does your testing environment really represent the production one?
  - Do you have a staging environment ?

EY

interaction #3

DEEPSEC

- I want you to test this application \ infra for…
  - “I cant give you an attack scenario, you find it…”
  - “please be very specific on how you got that finding…”
  - “How would you recommend we fix this in our environment?”

EY

interaction #3

- I want you to test this application \ infra for…
  - Operational risk people…
- So you don’t always know, but there are other people that are working on penetration testing, but they are NOT technical people, at all…

interaction #4

- I want you to find all of my vulnerabilities…
  - The client doesn’t care about threat actors
  - The client isn’t into automation
  - The client isn't working this as a process (one offs again…)

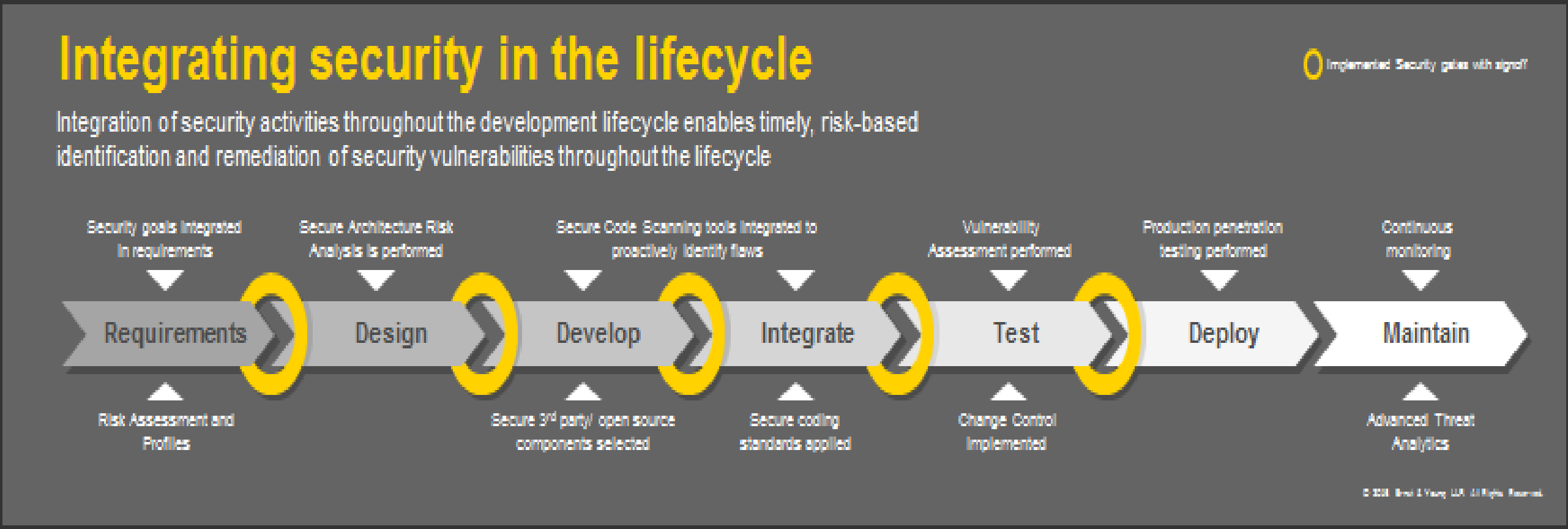
interaction #4

- Guide the client on the best ways to use you
  - Separate logical flaws, from just plain old software defects
  - Real pen testers, aren't afraid of the dynamic and static code scanning tools…so shouldn’t you
- Know what types of threat are out to get you
  - Preform threat assessments

interaction #4 (Continued…)

DEEPSEC

- Let’s talk SDLC without falling asleep…



EY


ANY
QUESTIONS
?