# Secure Application Development: What works and what doesn't ?

**Alumni Workshop**

Alexander Helleboogh
Nelis Boucké

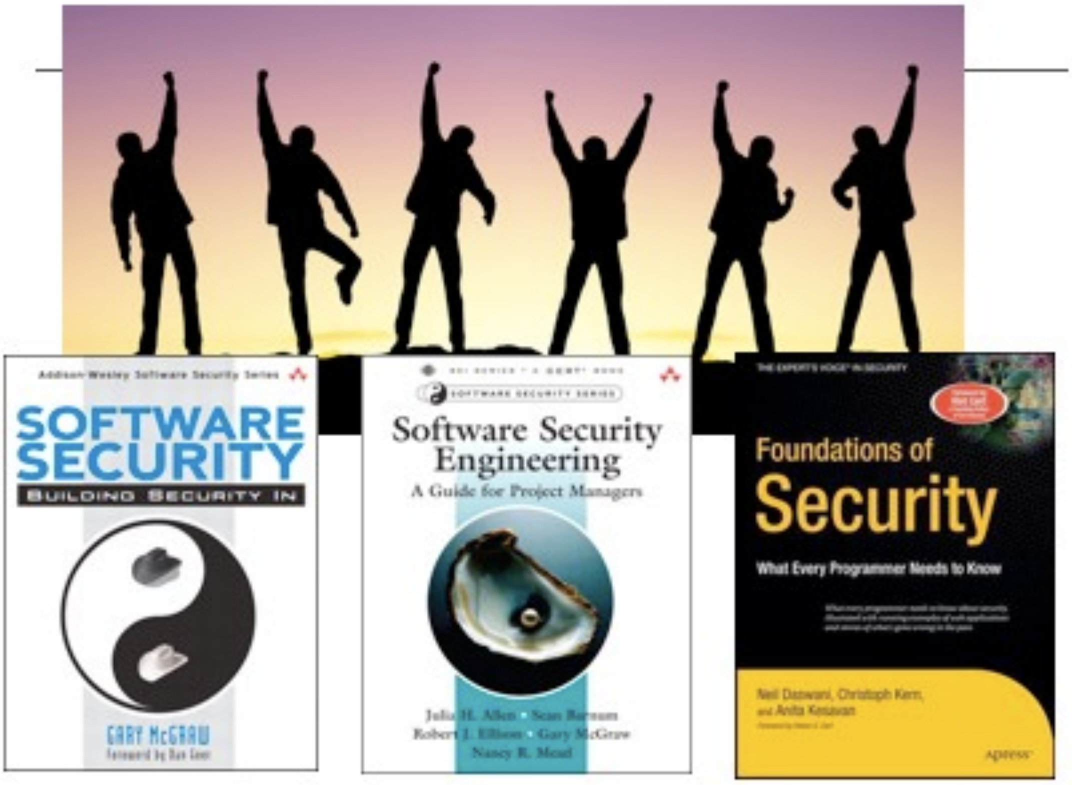
## Session agenda

- **Intro**
- Your biggest SecAppDev failure
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- Your biggest SecAppDev success
  - What works? (15')
  - Why? (15')
  - Dot voting (5')
- Wrap up
  - Preparation of plenary pitch (10')
  - Conclusion (5')

Learn from *your* mistakes

Preferably, learn from others'

## Success has many fathers


Addison-Wesley Software Security Series
SOFTWARE SECURITY
BUILDING SECURITY IN
GARY McGRAW
Software Security Engineering
A Guide for Project Managers
Julia H. Allen • Sean Barnum
Robert J. Ellison • Gary McGraw
Nancy R. Mead
Foundations of Security
What Every Programmer Needs to Know
Neil Daswani, Christoph Kern, and Anita Kesavan
Apress

# Failure is an orphan

**Alternative?**

# Goal of this session = Learn!

- Learn from each other's experience

1. Start with sharing your SecAppDev failure
2. Highlight your SecAppDev success

**Alumni Anonymous**

# Examples

- Think broad:
  - Organization structure/Frameworks/ Development methods
- Examples approaches
  - Misuse cases for capturing requirements
  - Penetration testing as only/holy grail
  - SDL (Security Development Lifecycle)
  - Using code analysis tools
  - Code reviews
  - BSIMM

# What fails in SecAppDev? 15 min

- Per person: Security practice behind (worst) failure – 3 min

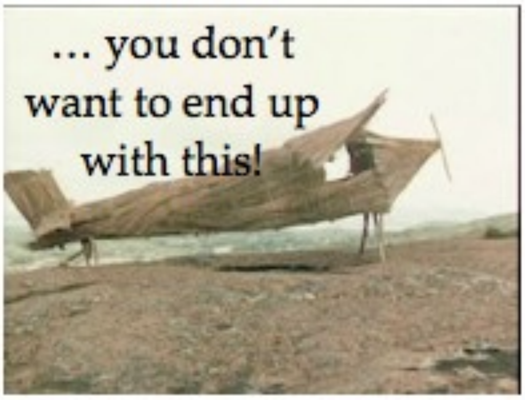
- Around the table – 12 min
  - Ask questions and discuss to make sure you understand every post-it

**ASSIGNMENT**

# Why do some things work in SecAppDev and some things don't?

# Cargo Cult

- Achieving the successful results of advanced cultures by mimicking their behaviour.
- Purely imitating because others do or told you so, is a sure path to failure.
  - Security Board
  - (Expensive) tools
  - Programming models
  - …



… you don't want to end up with this!

# Context Matters

- What works in some context, might not work in your context!
  - Across organizations but also within an organization
- Difference can be subtle
  - People and teams
  - Risks
  - Experience
  - Environment
  - Problem at hand

# No Silver Bullet

Frederik P. Brooks junior *"No Silver Bullet: Essence and Accidents of Software Engineering"*

- We are all often hoping for some magical solutions to our problem.
  - A tool, a method or a new understanding that make all our troubles go away
- Sadly, there isn't always such a silver bullet!
  - And there is a very good reason why not …
- Not all complexity can be 'fixed'
  - Some complexity is part of the essence of a system and can not be 'abstracted' away!

# Where did failure come from?

- write reason for failure on pink post-it
- cluster - 15 min

**ASSIGNMENT**

# dot voting

🔵 eryone has 3 blue dots and 3 green dots

: I have experienced this pain myself

🟢 : I have not done this, but am convinced this is a bad idea

**ASSIGNMENT**

# Session agenda

- Intro
- Your biggest SecAppDev failure
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- Your biggest SecAppDev success
  - **<u>What works? (15')</u>**
  - Why? (15')
  - Dot voting (5')
- Wrap up
  - Preparation of plenary pitch (10')
  - Conclusion (5')

# Session agenda

- Warm up
- SecAppDev failures
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- SecAppDev successes
  - What works? (15')
  - **<u>Why? (15')</u>**
  - Dot voting (5')
- Wrap up
  - Preparation of plenary pitch (10')
  - Conclusion (5')

# Session agenda

- Warm up
- SecAppDev failures
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- SecAppDev successes
  - What works? (15')
  - Why? (15')
  - **Dot voting (5')**
- Wrap up
  - Preparation of plenary pitch (10')
  - Conclusion (5')

# Session agenda

- Warm up
- SecAppDev failures
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- SecAppDev successes
  - What works? (15')
  - Why? (15')
  - Dot voting (5')
- Wrap up
  - **Preparation of plenary pitch (10')**
  - Conclusion (5')

# Session agenda

- Warm up
- SecAppDev failures
  - What fails? (15')
  - Why? (15')
  - Dot voting (5')
- SecAppDev successes
  - What works? (15')
  - Why? (15')
  - Dot voting (5')
- Wrap up
  - Preparation of plenary pitch (10')
  - **Conclusion (5')**

# It is better to understand **why** you did the **wrong thing** than it is to do the **right thing** **without understanding.**

*Since the first grants you a **learning experience** whereas the second is just heading for **another failure.***