The Secure SDLC Panel

Real answers from real experience

Moderated by:

Sebastien Deleersnyder

Foundation Board

seba@owasp.org

Panelists

- Migchiel de Jong (Fortify)
- Bart De Win (Ascure)
- Florence Mottay (Cigital)

Agenda

- Introducing the panelists
- Panelist positions
- Moderated question & answer
- Summary & conclusions

Introducing the Panelists

Migchiel de Jong

- Background:
  - Technical Computer Science
  - HW/SW development
  - Rational Software
  - IBM
- Experience:
  - 15 years in HW/SW development
  - 4+ years at Fortify

Bart De Win

- Background:
  - MS in Computer Science
  - Extensive research background in software security
  - Currently working for Ascure, responsible for application security offering
- Experience:
  - In-depth study of different SDLC’s
  - Contributed to SAMM
  - Wide experience in application assessments

Florence Mottay

cigital

- Managing Principal Cigital EMEA.
- Background in Computer Science
- Involved in software security for 10 years
- Areas of expertise include Threat Modeling for the Enterprise and Customized Enterprise Security Solutions.

Panelist Positions

gchiel
on…

SDLC Experience

- Working for Fortify since the start in Europe more than 4 years ago
- Helped many companies with institutionalizing code review
- Member of the OAR@NHL driving the introduction of app sec in the curriculum

gchiel
on…

DOs and DON’Ts

- DO
  - Measure
  - Transfer knowledge
- DON’T
  - *Define but not execute*
  - *Just produce artifacts*

Bart on…

Key decision factors

- Common understanding of SDLC
  - “It will solve all my security problems, right?”
  - “I’m actually looking for training”
- Rationale / Type of problems to be solved
- Security appetite of the company
- Mandate level in the organization
  - Which departments does it cover ?

Bart on…

DOs and DON’Ts

- DO
  - Work towards a balanced, risk-driven SDLC target
  - Use a phased roll-out
  - Install adequate measurements to keep track of progress
- DON’T
  - Literally implement SDLC XYZ in your organization
  - Expect to find the silver bullet in short term

ence
on…

SDLC Experience

- Cigital incorporated in 1992
- Cigital’s Touchpoints published in 2006
- Contributed to 8 large scale software security initiatives
- Knowledge of other set of best practices used to integrate security in the SDLC:
    - Microsoft SDL
    - OWASP’s CLASP

ence
on…

BSIMM

- Software security measuring stick based on real data
- 9 US companies including Adobe, The Depository Trust and Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo
- 9 EU companies including Nokia, Standard Life, SWIFT, Telecom Italia, and Thomson Reuters
- 30 firms in the study, bsimm 2 is coming up soon

ence
on…

Do’s and Don’ts

- BSSIM describes 110 activities
- BSIMM is descriptive, not prescriptive
- BSIMM is a yardstick

Moderated Question & Answer

Ground Rules

- Warm up with some prepared questions
- Panelists should limit responses to 2-3 mins
- Audience participation!!!
  - Comments/questions/flames welcomed!
- I’ll try to keep things orderly

???

- What are the most significant organizational factors in determining if a secure SDLC integration will be successful?
    - Top management mandate
    - Metrics and dashboards
    - Consistent development process
    - Corporate culture
    - Regulatory drivers

???

- Rank the following in terms of priority for an organization that wants to do more security assessments in the SDLC:
  - Code review (manual or static analysis)
  - Security testing (dynamic analysis or ethical hack)
  - Design review (inspection of security mechanisms)
  - Threat modeling (assessment of what could go wrong)

???

- What's the best method for getting an organization's development, security/risk, and operations groups aligned to roll out a secure SDLC program?

???

- Carrot vs. Stick. Which should you pick when trying to change the process throughout an organization? In what situations might you decide to use the other?

???

- If someone approached you saying they had a little bit of budget for their software security program, but didn't know what to do next, how would that conversation go? Specifically, where would you steer them?

  - Hire consultants
  - Get tools/technology
  - License training content
  - Internal head-count
  - <Insert here>

???

- We talk about the importance of measurement and metrics a lot, but does anyone actually use them? If so, what are the most popular ones?

???

- Do you think it is possible to demonstrate return on investment (ROI) for secure SDLC programs? If not, why? If so, how?

Summary & Conclusions