Bart De Win

- 15+ years of Information Security Experience
  - Ph.D. in Computer Science - Application Security
- Author of >60 scientific publications
- ISC² CSSLP certified
- Senior Manager @ PwC Belgium:
  - Expertise Center Leader Secure Software
  - (Web) Application tester (pentesting, arch. review, code review, ...)
  - Trainer for several courses related to secure software
  - Specialized in Secure Software Development Lifecycle (SDLC)
- OWASP OpenSAMM co-leader
- Contact me at bart.de.win@be.pwc.com
Agenda

1. Introduction
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion
This Session

Goal is to discuss how to apply SDLC in practice

Looking into different activities from a practical perspective

Based on the case of your own company

Discussing some of the challenges that you might face

Open interaction session
Before you begin

Organizational Context

Realistic Goals?

Scope?

Constraints (budget, timing, resources)

Affinity with a particular model?
What’s your Company Maturity?

- In terms of IT **strategy** and application **landscape**
- In terms of software **Development** practices
  - Analysis, Design, Implementation, Testing, Release, Maintenance
- In terms of **ITSM** practices

Company Maturity $\approx$ Feasibility SDLC Program
Complicating factors, anyone?

- Different development teams
- Different technology stacks
- Business-IT alignment issues
- Outsourced development
- ...

SDLC Workshop
SecAppDev 2014
Common SDLC strategies

- **Enterprise-wide**
  - Focus on overall methods and practices
  - Fundamental approach

- **Project-specific**
  - Focus on 1 particular project
  - Targeted approach

- **Problem-specific**
  - Focus on 1 specific problem
  - Ad-hoc approach
Typical Approach

As-Is

To-Be

Improvements
Agenda

1. Introduction
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion
As-Is

Maturity Evaluation (in your favourite model)

Depending on (your knowledge of) the organisation, you might be able to do this on your own.

If not, interviews with different stakeholders will be necessary:
   Analyst, Architect, Tech Lead, QA, Ops, Governance

Discuss outcome with the stakeholders and present findings to the project advisory board.
Scoping

For large companies, teams will perform differently

=> difficult to come up with a single result

Consider

• Reducing the scope to a single, uniform unit
• splitting the assessment into different organizational subunits

Splitting might be awkward at first, but can be helpful later on for motivational purposes
Assessment Exercise

Use OpenSAMM to evaluate the development practices in your own company

Focus on Governance and Construction Business Functions

Applicable to both Waterfall and Agile models

Sheets and questionnaires will be distributed
Assessment wrap-up

What’s your company’s score?

What’s the average scores for the group?

Any odd ratings?
Agenda

1. Introduction
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion
**To-Be**

Identify the targets for your company

Define staged roadmap and overall planning

Define application migration strategy

Gradual improvements work better than big bang

Have this validated by the project advisory board
## Staged Roadmap

<table>
<thead>
<tr>
<th>Security Practices/Phase</th>
<th>Start</th>
<th>One</th>
<th>Two</th>
<th>Three</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy &amp; metrics</strong></td>
<td>0,5</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>Policy &amp; Compliance</strong></td>
<td>0</td>
<td>0,5</td>
<td>1</td>
<td>1,5</td>
</tr>
<tr>
<td><strong>Education &amp; Guidance</strong></td>
<td>0,5</td>
<td>1</td>
<td>2</td>
<td>2,5</td>
</tr>
<tr>
<td><strong>Threat Assessment</strong></td>
<td>0</td>
<td>0,5</td>
<td>2</td>
<td>2,5</td>
</tr>
<tr>
<td><strong>Security Requirements</strong></td>
<td>0,5</td>
<td>1,5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Secure Architecture</strong></td>
<td>0,5</td>
<td>1,5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Design Review</strong></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2,5</td>
</tr>
<tr>
<td><strong>Code Review</strong></td>
<td>0</td>
<td>0,5</td>
<td>1,5</td>
<td>2,5</td>
</tr>
<tr>
<td><strong>Security Testing</strong></td>
<td>0,5</td>
<td>1</td>
<td>1,5</td>
<td>2,5</td>
</tr>
</tbody>
</table>

**Vulnerability**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td>2,5</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Environment Hardening</strong></td>
<td>2,5</td>
<td>2,5</td>
<td>2,5</td>
<td>2,5</td>
</tr>
<tr>
<td><strong>Operational Enablement</strong></td>
<td>0,5</td>
<td>0,5</td>
<td>1,5</td>
<td>3</td>
</tr>
</tbody>
</table>

**Total Effort per Phase**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7,5</td>
<td>7,5</td>
<td>7,5</td>
<td></td>
</tr>
</tbody>
</table>
**Improvement Exercise**

Define a target for your company and the phased roadmap to get there.

Focus on the most urgent/heavy-impact practices first.

Try balancing the complexity and effort of the different step-ups.
Implementation

Implementation of dedicated activities according to the plan

Iterative, Continuous Process

Leverage good existing practices
## Selected Examples

<table>
<thead>
<tr>
<th>Application</th>
<th>Internal</th>
<th>B2B / B2C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Kerberos/SPNEGO + (StrongAuth OR SSL/X509 mut.)</td>
<td>SAML/HTTP-POST (red.) + StrongAuth</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Kerberos/SPNEGO</td>
<td>SAML/HTTP-POST (red.)</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>None (*)</td>
<td>None (*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>Internal</th>
<th>B2B / B2C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Kerberos/SPNEGO (S)  Kerberos/SPNEGO (R)  + SSL/X509 mut.</td>
<td>SAML/SOAP (S)  SAML/HTTP-POST (unsol.) (R)  + StrongAuth</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Kerberos/SPNEGO (S)  Kerberos/SPNEGO (R)</td>
<td>SAML/SOAP (S)  SAML/HTTP-POST (unsol.) (R)</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>None (<em>) (S)  None (</em>) (R)</td>
<td>None (<em>) (S)  None (</em>) (R)</td>
</tr>
</tbody>
</table>
Session management

**Problems:** Session hijacking, session fixation, session riding

**Solutions**

- Protect session id: *not leaked to client (always enable cookies)*
- Cookie protection: *secure, HTTPOnly, domain, path* flags (*manual, ESAPI*) – session cookies by Java framework, new cookies by developer
- Lifetime: *short timeout* (based on balancing risk and business functional requirements)
- Regenerate session id on authentication/authorization/protocol change: *manual, framework (reuse-session-id) -> ok in Java framework*

**Best practices**

- Session id needs strong algorithm
- Don’t use persistent cookies
- Avoid concurrent sessions
- Proper working logout mechanism available on all non public pages
Agenda

1. Introduction
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion
The importance of a Business Case

If you want your company to improve, management buy-in is crucial ⇒ You will need a business case to convince them

Typical arguments:
• Improved security quality
• Better cost efficiency
• Compliance
• Risk management
• Customer satisfaction
• Reputation management
**Entry Points**

- Pick the weak spots that can demonstrate short-term ROI

- Typical examples
  - Awareness training
  - Coding Guidelines
  - External Pentesting

- Success will help you in continuing your effort
**Application categorization**

Use this to rationalize security effort (according to the application risk)

Granularity!

Inter-Connectivity!
Communication & Support

Critical success factor!

Spreading the message – broad audience

Setup a secure applications portal!

Regular status updates towards management
Monitoring & Metrics

The only valid measurement of code quality: WTFs/minute

(c) 2008 Focus Shift
Responsibilities

Core Security team

Security Satellite
  Analysts
  Architects
  Developers
  Operations
  Management

Formalized RACI will be a challenge
The Power of Default Security

Construct development frameworks that are secure by default

Minimizes work for developers

Will lower number of vulns.
SDLC Cornerstones (recap)

- People
  - Roles & Responsibilities
- Process
  - Activities
  - Deliverables
  - Control Gates
- Knowledge
  - Standards & Guidelines
  - Compliance
  - Transfer methods
- Tools & Components
  - Development support
  - Assessment tools
  - Management tools
Agenda

1. Introduction
2. Assessment
3. Improvements
4. Tips & Challenges
5. Discussion
Discussion Topics

Practical experiences

3rd party development (near-shoring, off-shoring)

COTS / Packaged software

Mobile

...
Conclusions

SDLC is the overall framework for most of this week’s sessions

Models need to be adapted to your situation

Find balance for all cornerstones

Risk Management is key for rationalizing effort

Beware the big bang