Building an AppSec Program from Scratch

Chris Pfoutz, CISSP, GWAPT
Manager Application Security
Intro: Who’s Who

Chris Pfoutz

- Schooled as a developer
- 10 years Infosec
  - Consulting
  - Financial Services
  - Risk Assessments
  - AppSec
- Spent 2 years developing an application security program for a global financial technology company
- Spent the last year participating in an established 6 person team at Deloitte Touche Tohmatsu Limited.
**Intro: Audience Survey**

Show of Hands

- General IT or aspiring into security
- Security – General or other non-AppSec
- AppSec
- Development
Content

**Section 1**: Why AppSec

**Section 2**: How Most Companies Do It

**Section 3**: Steps to Build a Program

**Section 4**: Assurance Components

**Section 5**: Advice Along the Way
Section 1: Why AppSec?
Vulnerabilities

Challenges

• Relative infancy of the profession
• Traditional network/infrastructure focus
• Lack of qualified talent
• Lack of leadership understanding
Section 2: How Most Companies Do It
How Most Companies Do Things

• Tell the network security person to buy an application scanner

• Scan everything

• Send pdfs to the developers

• Have your network pen testing company pen test apps where necessary

• Intended goal: Sexy program with immediate results
Why This Doesn’t Work

• How do you know what to scan and when to scan it?
• Do you have enough manpower?
• Are your developers really going to pay attention to a pdf?
• How will you keep track of the remediation?
• Result: Frustration
Section 3: Steps to Build a Program
Step 1: Application Inventory

- Perfect for your GRC tool

- Sources
  - DR Inventory
  - Asset Inventory
  - Validate with IT and Business Owners

- Include COTS, in house developed and bespoke developed software
Step 2: Business Impact Analysis (BIA) or Risk Scorecard

• Short, multiple choice questionnaire

• Fields to Collect

  ➢ Confidentiality
    ✓ Data Elements – intellectual property, PII, employment records

  ➢ Integrity
    ✓ Financial transactions
    ✓ Branding
    ✓ Embedded systems

  ➢ Availability
    ✓ Recovery Time Objective (RTO)
    ✓ Brand
    ✓ Revenue
Step 3: Risk Ranking and Checklist

- Segregate applications into 3-5 groups

- Develop set of controls applicable to each tier of application
  - Standards
  - Risk Assessment

- Inject validation checks to ensure assurance levels are in place

- Low risk applications may get green light
**Step 4: Build Secure SDLC with Change Control Gates**

- Determine where checkpoints belong
- Have PMO add checkpoints to official SDLC
- Establish sign off gates
- Make an example
- Don’t punish them for sins of the past
Section 4:
SDLC Components
Vulnerability Assessments

• Dynamic Analysis

• Static Analysis
  ➢ Binary Analysis
  ➢ Source Code Analysis

• SaaS vs. In House
  ➢ Integration with build train
  ➢ Vendor Support
  ➢ Resources
  ➢ Cost

• What is the best tool?

• Penetration Testing
  ➢ Test, fix, retest
  ➢ Letter of attestation

• Design Reviews
Section 5: Advice Along the Way
Metrics

• Show increase of testing activity overlayed with number of flaws

• Warn team management before providing a count of flaws per team

• Break out 5-10 most important flaws at each reporting level

• Break out security flaws in issue tracking

• Drive for incremental improvement

• Remember: Many flaws are legacy
Don’t Call Their Baby Ugly
Take a Developer’s Perspective
Developer Training and Architecture/Coding Standards Breed Success
Don’t Blindly Trust your Tools…or Your Pen Testers
You Software Security Team and Consultants Need an Application Focus
Treat Security Issues as Bugs
Resources

• OWASP Software Assurance Maturity Model
• Software Security: Building Security In by Gary McGraw
• The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto

• Contact
  Chris Pfoutz
  cpfoutz@deloitte.com
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by
guarantee, and its network of member firms, each of which is a legally separate and independent
entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte
Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients
spanning multiple industries. With a globally connected network of member firms in more than 150
countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the
insights they need to address their most complex business challenges. Deloitte has in the region of
200,000 professionals, all committed to becoming the standard of excellence.

Disclaimer
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited,
its member firms, or their related entities (collectively the “Deloitte Network”) is, by means of this
publication, rendering professional advice or services. Before making any decision or taking any
action that may affect your finances or your business, you should consult a qualified professional
adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by
any person who relies on this publication.

© 2013. For more information, contact Deloitte Touche Tohmatsu Limited.