Software Security Certification
Symantec’s Experience

Cassio Goldschmidt, Sr. Manager
December 9th, 2009
The creation of CSSLP

• Convergence among all parties
• Excellent pool of talent from various industries in all meetings
  – Independent Software Vendors
  – Online Service Providers
  – Financial Services Organizations
  – Government Organizations
• Rigorous process to create questions
  – Psychometrics
  – Peer review
  – Source requirements
• (ISC)² proven track record creating certifications
Areas where CSSLP adds value

Effective way to educate current staff

- Historically, universities have not integrate security with CS education
- Certification maintenance requirements is a good idea
- Does not replace real world practice
  - Diplomas do not replace the need for practice either
Areas where CSSLP adds value

Hiring

Old School
• One page resume

New School
• Keyword driven
• CISSP is already a keyword
Areas where CSSLP adds value

How do you tell a recruiter you need a professional familiar with all the areas listed below?

- Security Principles
- Security Requirements
- Secure Software Design
- Secure Coding
- Secure Software Testing
- Vulnerability management and response
The problem Symantec faces today
Most of our flaws are not in our code

Security Incidents in 2009

Symantec Code 54%
Open Source Third Party 46%
What should a practitioner do when an vulnerability is reported by a security researcher?

- How to assess risk?
- How to deploy the fix?
- How and when customers need to be informed?
- What kind of process and techniques can help to avoid vulnerabilities in the first place?
Symantec’s education and process
We don’t teach with certs in mind

Security Classes

ENG-2 (Dev)

ENG-4 (QA)

Symmunize (Everyone)
Symantec’s education and process
We don’t teach with certs in mind

Awareness & Continuous Education

Tech Exchanges

Cutting Edge

CTO Newsletter Articles
Thank You!

Cassio Goldschmidt
Sr. Manager, Product Security
Office of the CTO, Symantec Corporation