SecurityInnovation
THE SOFTWARE SECURITY COMPANY

Certification Project Discussion

OWASP Academies Meeting

5 & 6 January 2011
Lisbon, Portugal

Agenda

- **About Security Innovation**
  - Company
  - Ed Adams & Jason Taylor
  - eLearning/Certification Case Studies
- **OWASP Certification Project**
  - Background/Motivation
  - Critical Success Factors for Certification Programs
  - Existing Content and Technology
- **Getting to OWASP Certification Stage**
  - Discussion and Refactoring
  - Proposed model

About Security Innovation

- **Application Security and Crypto Experts**
  - 10+ years research on vulnerabilities and cryptography
  - Hundreds of assessments on world's most dominant software
- **Products, Services & Training**
  - **Software Assurance**
    - white and black box assessments
    - secure development lifecycle and crypto consulting
  - **Training & Methodologies**
    - eLearning, instructor-led, and secure coding standards
  - **Encryption**
    - fast, lightweight, patented, and future-proof
- **Helping organizations:**
  - Build internal application security competency
  - Rollout a repeatable secure SDLC process
  - Identify and reduce application risk

SecurityInnovation®

Credentials

- **Published 7 books, including two co-authored with Microsoft**
  - Upcoming: “Information Security Management: Survival Guide”, Wiley 2011
  - Improving Web Services Security, http://msdn.microsoft.com/en-us/library/ff650794.aspx
  - Application Architecture Guide, http://msdn.microsoft.com/en-us/library/ff650706.aspx
  - Security Engineering Explained, http://msdn.microsoft.com/en-us/library/ff648940.aspx
- **First publicly published software security testing methodology**
  - Adopted by McAfee, Symantec, Microsoft and SAP as part of their SDLC
- **Crypto solutions have been adopted in IEEE 1609.2 and 1363.1 standards**
  - Fastest, smallest, most secure crypto on the market
  - Seven patents for cryptography
- **Authorized security partner for EMC, Microsoft, SAP, Cisco, and IBM**
- **Winner of Gartner’s “Cool Vendor” Award**
- **Corporate Symposium Keynotes for Fidelity, McAfee, MassMutual, AT&T, Nationwide, and others**

80% of Security Innovation customers are Fortune/Global 500

SecurityInnovation®

About Ed Adams and Jason Taylor

Ed Adams
President and CEO

- **Responsible for SI, Inc. success and value**
- **SI employee since 2003**
  - Seat on Board of Directors since inception
- **Previous work experience**
  - ***Ipswitch***:
    Exec. Vice President
  - ***Lionbridge***:
    VPand BUM, VeriTest (including certification business)
  - ***Rational Software:***
    Director, Technical Marketing
  - Director and VP posts with MathSoft (now PTC), Foster-Miller, etc

Jason Taylor
Chief Technology Officer

- **Responsible for engineering, development, and tech vision**
- **Intimate knowledge of eLearning process and infrastructure**
- **Reviewer, contributor, and primary author for Microsoft patterns & practices security guidance**
- **Co-author of**
  - *"Improving Web Services Security"*
  - *"Team Development with Visual Studio Team Foundation Server"*
- **Previous work experience**
  - ***Microsoft***:
    Security Lead, Test Architect, and Dev. Manager for various releases of Internet Explorer and Windows OS

Customer Case Study:
Industry Security Standards Body

- **Major Challenges:**
  - Scale existing certification programs (3 separate certifications)
  - Introduce new certification (for new audience) and scalable awareness training (for all audiences)
  - Have zero transparency re. vendor assistance (highly political landscape)
- **Solution:**
  - *Short-term*: updated/migrated existing eLearning course to SI hosted LMS
  - *Long-term:* Created and managed entire certification business:
    - Defined eLearning courses, tracks, prerequisites; added comprehensive exams, descriptions; determined course fees, etc.
    - Used initially for annual re-certification of existing certifications
    - Deliverables include ILT presentations in addition to eLearning courses & exams
    - All courses built ready-for-localization (Japanese first in queue)
  - Mitigated dependence on and burn-out of trainers while expanding reach and revenue generation substantially

Customer Case Study:
Florida Institute of Technology

- **Major Challenges:**
  - Promote and build upon its position as a cutting-edge Cyber Security university
  - Offer a turn-key solution for a Cyber Security certificate program
  - Break out of geographic boundaries: Central Florida, USA

- **Solution:**
  - Created curriculum of courses with tracks, prerequisites, comprehensive exams, descriptions, course fees, etc.
    - Plan is for series of Cyber Security certificate programs
    - Combination of SI- and FIT-contributed content formed the first Cyber Security certificate: Software Assurance
  - From concept to “go live” in under 3 months
  - Certificate program offered via Continuing Education (launching Q1’11)
  - Curriculum equates to ~128 hours of classroom coursework (ILT)
  - University handles student registration, payments, etc.
  - $8,000-$10,000 per student for certificate (~$700 per course)

FIT's Cyber Security SwA Curriculum

Course Number	Course Name	Prerequisite
	Introductory Courses	
101	• Fundamentals of Application Security	
102	• Introduction to the Microsoft SDL	
113	• How to Define Software Security Requirements & Design	101
	Beginner Courses	
221	• Fundamentals of Secure Architecture	101, 113
222	• Fundamentals of Security Testing	101, 113
233	• Fundamentals of Secure Development	101, 113
243	• Architecture Risk Analysis and Remediation	221
	Intermediate Courses	
301	• Classes of Security Defects	101, 102
312	• Introduction to Threat Modeling	233, 243
322	• Attack Surface Analysis	233, 243
331 **or** 332 **or** 333	• Understanding Secure Code – C/C++ **or** USC – JRE **or** USC – .NET 4.0	221
	Advanced Courses	
401	• Introduction to Cryptography	233, 243
411 **or** 412 **or** 413	• Creating Secure Code – C/C++ **or** CSC – J2EE **or** CSC – ASP.NET	331 **or** 332 **or** 333
444 **or** 445	• Exploiting Buffer Overflows **or** Web Vulnerabilities – Threats & Mitigations	411 **or** 412/413

Agenda

- **About Security Innovation**
  - Company
  - Ed Adams & Jason Taylor
  - eLearning/Certification Case Studies
- **OWASP Certification Project**
  - Background/Motivation
  - Critical Success Factors for Certification Programs
  - Existing Content and Technology
- **Getting to OWASP Certification Stage**
  - Discussion and Refactoring
  - Proposed model

OWASP Certification – Background/Motivation

- **In 2008 Jim McGovern led project to create an OWASP certification**
- **OWASP community opted "no go" in 2008 due mainly to closed source nature of a certification exam**
- **Other factors leading to "no go" included:**
  - Government(s) requiring ISO certification which counters an open notion
  - No single measure of "good OWASP Professional" (some builders, others breakers)
  - Lack of infrastructure to support training, exams, and certification
  - Desired a "higher bar" than popular industry certs (PMP, CISSP, etc.)
- **In 2010 from Dinis Cruz:**

  "Certifications are very important to OWASP and is something that if done correctly would have tremendous value to OWASP's community and help to reach a much wider audience."

Certification Programs
Critical Success Factors

- Content
  - Set of guidelines or standards against which to test and measure
- Sponsor
  - Captive/Mass audience that cares about the content or platform
  - Vendor-sponsor cert programs challenged w/ perception of bias, for-profit motivations, and lack of support from platform/sponsor (no mass appeal)
- Infrastructure
  - Ability to morph content into training or guidance
  - Hosting of automated content delivery and/or assessment vehicle(s)
  - The means through which to brand accordingly for the sponsor
  - Ability to market (ideally w/ or via sponsor) to capture interested audience
- Create Demand
  - Ultimate goal to have orgs/individuals proactively seeking the certification
  - Access to influencers in the target space with ability to bring them together
  - Ability to execute on industry PR and market awareness campaign

SI eLearning Course Roadmap – Nov 15, 2010

How to Define Security Reqts.
App Security Reqs - PCI
Application Security Reqs - Web Apps OWASP
How to Interpret and Implement Software Security Requirements

Fundamentals of Secure Architecture
Intro to Threat Modeling
Architecture Risk Analysis
Creating Secure App Architecture
Attack Surface Analysis
Database Security
How to Perform an SDLC Gap Analysis
OWASP Top 10 - Threats and Mitigations
Best Practices – Security Driven Design

Fundamentals of Secure Dev'p
Creating Secure Code - ASP.Net
Introduction to Cryptography
Web Vulnerabilities Threats/Mitigations
Introduction to Integer Overflows
Introduction to Buffer Overflows
Understanding Secure Code C/C++
Creating Secure Code (CSC) – C/C++
USC – Windows 7
USC - . NET 4.0
USC - JRE
CSC – J2EE
CSC – C#

Fundamentals of Security Testing
Classes of Security Defects
Exploiting Buffer Overflows
How to Break Software Security
How to Test for the OWASP Top 10
How to Perform a Code Review
How to be Successful with Web Application Scanning

Fund of Secure SW Release
Secure Application Deployment

Fundamentals of Incident Response
Building an Incident Response Plan

Compliance

PCI Best Practices for Developers
Info Sec Risk Mgmt
Intro to PCI

Process/Other

Software Security Awareness
Six Fundamentals of Information Security
Microsoft SDL for Managers
Intro to the Microsoft SDL
Application Security Fundamentals

Existing Courses

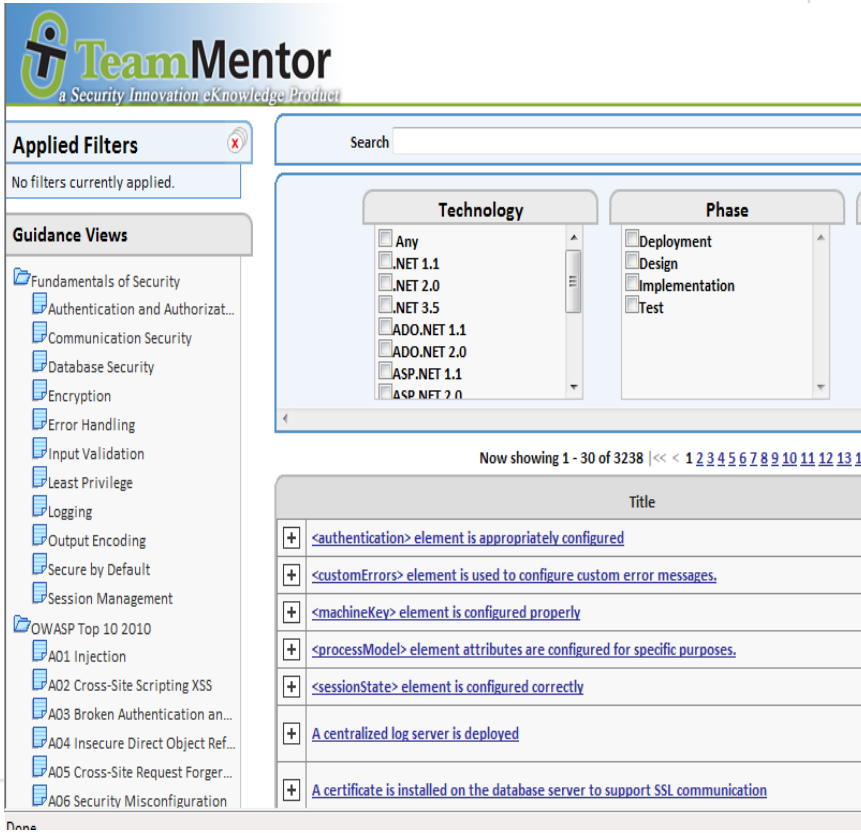
Q1'11 Courses

Q2'11 Courses

SecurityInnovation®

SI's TeamMentor – sample screenshots

- **Content Breadth and Depth**
  - Over 3,000 practical articles (grows each quarter)
  - Articles sortable/filterable by technology, role, security category, etc.
- **Pre-populated guidance views**
  - Fundamentals of Security
  - OWASP Top 10 (2010)
  - PCI DSS (each of the 12 requirements)
  - PCI 6.6 (code review)
  - etc.



Applied Filters

No filters currently applied.

Guidance Views

- Fundamentals of Security
  - Authentication and Authorizat...
  - Communication Security
  - Database Security
  - Encryption
  - Error Handling
  - Input Validation
  - Least Privilege
  - Logging
  - Output Encoding
  - Secure by Default
  - Session Management
- OWASP Top 10 2010
  - A01 Injection
  - A02 Cross-Site Scripting XSS
  - A03 Broken Authentication an...
  - A04 Insecure Direct Object Ref...
  - A05 Cross-Site Request Forger...
  - A06 Security Misconfiguration

Search

Technology	Phase	Type	Category
Any	Deployment	Attack	Anti-Virus
.NET 1.1	Design	Checklist Item	Application State
.NET 2.0	Implementation	Code Example	Assembly Level Checks
.NET 3.5	Test	Guideline	Auditing and Logging
ADO.NET 1.1		How To	Authentication
ADO.NET 2.0		Inspection Question	Authorization
ASP.NET 1.1		Principle	Bindings
ASP.NET 2.0		Question and Answer	Code Access Security

Now showing 1 - 30 of 3238 |<< < 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 ... > >>|

Title	Technology	Phase	Type	
<authentication> element is appropriately configured	ASP.NET 1.1	Implementation	Checklist Item	Conf
<customErrors> element is used to configure custom error messages.	ASP.NET 1.1	Implementation	Checklist Item	Conf
<machineKey> element is configured properly	ASP.NET 1.1	Implementation	Checklist Item	Conf
<processModel> element attributes are configured for specific purposes.	ASP.NET 1.1	Implementation	Checklist Item	Conf
<sessionState> element is configured correctly	ASP.NET 1.1	Implementation	Checklist Item	Conf
A centralized log server is deployed	PCI DSS	Deployment	Checklist Item	Audi Logg
A certificate is installed on the database server to support SSL communication	SQL Server 2000	Deployment	Checklist Item	Depl Cons

Existing Content Available

- **SI eLearning courses**
  - See list to the right (SI library)
  - Demo ?
- **SI' s TeamMentor**
  - OWASP Top 10 Guidance Views
  - Other role-based guidance
  - note: SI's intent re. TM/OWASP
  - Demo ?
- **OWASP Projects**
  - Top 10: Threats & Mitigations
  - Lifecycle/Maturity
  - Protect
  - Detect
  - Audit
- **Other?**

	Relevant to:		
	Compliance	Web / OWASP	Microsoft
Awareness			
Software Security Awareness	✓		
Six Fundamentals of Information Security	✓		
Microsoft SDL for Managers			✓
Introduction to the Microsoft SDL			✓
Information Security Risk Management	✓		
Fundamentals of Application Security	✓	✓	
Define & Design			
How to Define Security Requirements			✓
Fundamentals of Secure Architecture			
Architecture Risk Analysis			
Creating Secure Application Architecture			
Introduction to Threat Modeling			✓
Attach Sufrace Analysis			✓
Database Security			
OWASP Top 10 - Threats & Mitigations	✓	✓	
How to Interpret Software Security Requirements			✓
Application Security Requirements - PCI	✓		
Application Security Requirements - Web Apps	✓		
Implement / Code			
Fundamentals of Secure Development	✓	✓	
Introduction to Cryptography	✓		
Web Vulnerabilities: Threats & Mitigations	✓	✓	
Introduction to Integer Overflows			
Introduction to Buffer Overflows			
Understanding Secure Code - Windows 7	✓		✓
Understanding Secure Code - .Net 4.0	✓	✓	✓
Best Practices for Developers - PCI	✓		
Creating Secure Code - ASP.NET	✓	✓	✓
Creating Secure Code - Java Web Apps	✓	✓	
Creating Secure Code - C/C++	✓		
Creating Secure Code - J2EE	✓		
Creating Secure Code - C#	✓		✓
Understanding Secure Code - C++	✓		
Understanding Secure Code - JRE	✓		
Test / Verify			
Fundamentals of Secure Testing	✓		✓
Classes of Security Defects		✓	
Exploiting Buffer Overflows			
How to Break Software Security	✓		
How to Test for the OWASP Top 10	✓	✓	
Be Successful with Static Analysis	✓		✓
Deploy / Release			
Fundamentals of Secure Software Release	✓		
Secure Software Deployment	✓		
Fundamentals of Incident Response	✓		
Building an Incident Response Plan	✓		

** Italicized: To be released early 2011*

SecurityInnovation®

Agenda

- **About Security Innovation**
  - Company
  - Ed Adams & Jason Taylor
  - eLearning/Certification Case Studies
- **OWASP Certification Project**
  - Background/Motivation
  - Critical Success Factors for Certification Programs
  - Existing Content and Technology
- **Getting to OWASP Certification Stage**
  - Discussion and Refactoring
  - Proposed model

Discussion and Refactoring

- **Open requirements for**
  - Exam question pool(s)
  - Source content for training
- **OWASP Projects**
  - Most popular/referenced/viewed
  - Most comprehensive re. content breadth and depth
- **Certification to offer for individuals**
  - Type(s) to offer
  - Sequencing/Priority
- **What SI brings to the party**
  - Experience running turn-key certification programs (for self and others)
  - Experience building and managing eLearning portals and businesses
  - Access to industry leaders with independent voice in AppSec space
  - Ability and willingness to invest in PR and market awareness
  - Augmentation and value-add to OWASP content and web projects, e.g., TM

Proposed Model

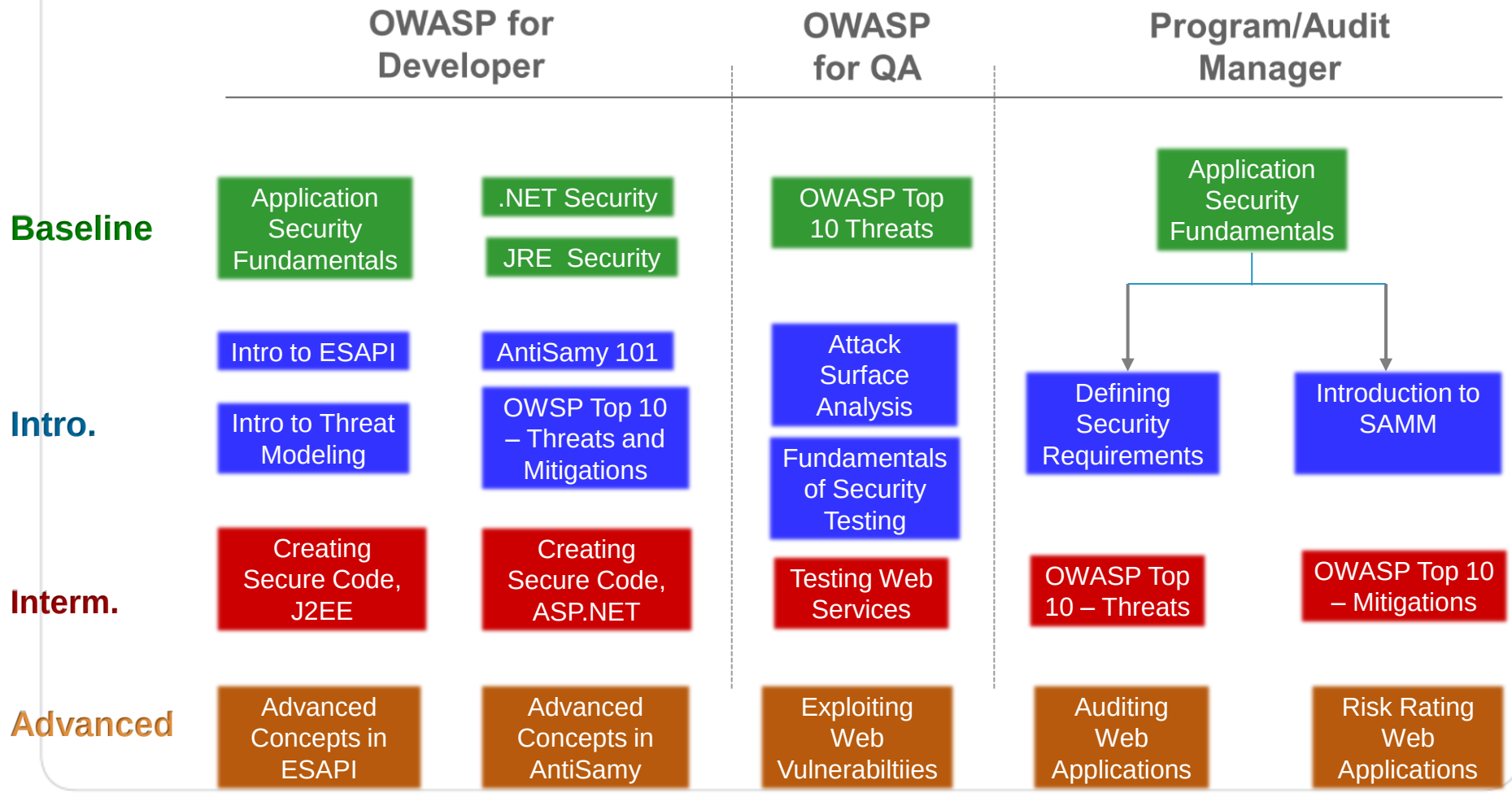
- **Start small, but communicate "big picture"**
  - 1 or 2 certifications upon launch
  - Show intentions for other certifications
- **By Role**
  - Lifecycle/System-wide (based on SAMM, CLASP, Risk Rating, etc.)
    - Project/Program Management
    - Auditing
  - Function-specific (Detect/Protect or by Functional Role)
    - Architect
    - Developer
    - Tester/QA

  Note: for function-specific, how granular, e.g., by platform? Language (for devs)? Implementation Guide (ESAPI, AntiSamy, etc.)?

Proposed Model (cont.)

- **SI branded and hosted**
  - Cloud-based eLearning portal for training
  - Access to TeamMentor/OWASP for reference and practice (contribute as OWASP project?)
  - SI bears all cost and risk in creating courses, portal, and launching program
- **Business Model and Promotion**
  - Fee-based system
    - By course, exam, or certification?
  - SI supports OWASP via content contribution and marketing sponsorships
    - OWASP conferences
    - Continued membership
    - Other?
  - Industry and university involvement
    - Corporate leaders endorse/prefer OWASP certifications
    - Large group discounts (corporate/government)
    - Open access to active university students?

Sample Role-Based Training Tracks (*simple/non-comprehensive option*)



SecurityInnovation®

OWASP Involvement

- **Official "endorsement" challenging, but could facilitate with…**
  - Public reviews of certifications delivered at OWASP Conferences (created by an OWASP Leaders who go through the process)
  - 'OWASP Quote' where OWASP Board + Leaders can make an 'on the record' comment on an OWASP-based certification. (ref: http://www.owasp.org/index.php/Quotes)
  - List Certification(s) on a 'Commercial Services' registry (ref: http://www.owasp.org/index.php/OWASP_Related_Commercial_Services)
- **Other methods through which we can create "stickiness"**
  - Free access/certification to University students?
  - Corporate/Group discounts promoted at OWASP events and website?
  - Endorsement from corporate CSOs re. hiring preference for those with OWASP certification (Salesforce, Google, Oracle, SAP, etc.)

Open Questions/Challenges

- **Complete Openness**
- **Training and exam proctoring / authentication**
- **Other?**

Contact info:

Ed Adams
eadams@securityinnovation.com
+1.978.694.1008 x123
eadams2330 (Skype)

Jason Taylor
jtaylor@securityinnovation.com
+1.978.694.1008 x125
tlaloc75 (Skype)