The Anatomy of Real-World Security Programs

http://www.opensamm.org

Pravir Chandra
OpenSAMM Project Lead
chandra@owasp.org
What are we talking about?

- Lessons from real programs
- A mild intro to the OpenSAMM model
- The project and it's future
Lessons From Walking the Path
We do ___ for security.
We’re all snowflakes.
It’ll help, I promise...
It's not technical, you geek.
Control your future.
Real ROI is possible.
Specifically, get specific.
Multiply thyself.
Measure on a moving scale.
Samm v. Bsimmm v. SDL
The OpenSAMM model
Drivers for a Maturity Model

- An organization’s behavior changes slowly over time
- Changes must be iterative while working toward long-term goals
- There is no single recipe that works for all organizations
- A solution must enable risk-based choices tailor to the organization
- Guidance related to security activities must be prescriptive
- A solution must provide enough details for non-security people
- Overall, must be simple, well-defined, and measurable
SAMM Business Functions

- Start with the core activities tied to any organization performing software development
- Named generically, but should resonate with any developer or manager

Governance
Construction
Verification
Deployment
SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘sil’o’ for improvement
Under each Security Practice

• Three successive Objectives under each Practice define how it can be improved over time
• This establishes a notion of a Level at which an organization fulfills a given Practice
• The three Levels for a Practice generally correspond to:
  • 0: Implicit starting point with the Practice unfulfilled
  • 1: Initial understanding and ad hoc provision of the Practice
  • 2: Increase efficiency and/or effectiveness of the Practice
  • 3: Comprehensive mastery of the Practice at scale
Check out this one...

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>EG 1</th>
<th>EG 2</th>
<th>EG 3</th>
</tr>
</thead>
</table>

**Objective**

<table>
<thead>
<tr>
<th>EG 1</th>
<th>EG 2</th>
<th>EG 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offer development staff access to resources around the topics of secure programming and deployment</td>
<td>Educate all personnel in the software life-cycle with role-specific guidance on secure development</td>
<td>Mandate comprehensive security training and certify personnel for baseline knowledge</td>
</tr>
</tbody>
</table>

**Activities**

<table>
<thead>
<tr>
<th>EG 1</th>
<th>EG 2</th>
<th>EG 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Conduct technical security awareness training</td>
<td>A. Conduct role-specific application security training</td>
<td>A. Create formal application security support portal</td>
</tr>
<tr>
<td>B. Build and maintain technical guidelines</td>
<td>B. Utilize security coaches to enhance project teams</td>
<td>B. Establish role-based examination/certification</td>
</tr>
</tbody>
</table>

...more on page 42
Per Level, SAMM defines...

- Objective
- Activities
- Results
- Success Metrics
- Costs
- Personnel
Conducting assessments

- SAMM includes assessment worksheets for each Security Practice

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>✦ Have most developers been given high-level security awareness training?</td>
<td></td>
</tr>
<tr>
<td>✦ Does each project team have access to secure development best practices and guidance?</td>
<td></td>
</tr>
<tr>
<td>✦ Are most roles in the development process given role-specific training and guidance?</td>
<td></td>
</tr>
<tr>
<td>✦ Are most stakeholders able to pull in security coaches for use on projects?</td>
<td></td>
</tr>
<tr>
<td>✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?</td>
<td></td>
</tr>
<tr>
<td>✦ Are most people tested to ensure a baseline skill-set for secure development practices?</td>
<td></td>
</tr>
</tbody>
</table>

EG 1

EG 2

EG 3
Assessment process

- Supports both lightweight and detailed assessments
- Organizations may fall in between levels (+)
Creating Scorecards

• Gap analysis
  • Capturing scores from detailed assessments versus expected performance levels
• Demonstrating improvement
  • Capturing scores from before and after an iteration of assurance program build-out
• Ongoing measurement
  • Capturing scores over consistent time frames for an assurance program that is already in place
Roadmap templates

- To make the “building blocks” usable, SAMM defines Roadmaps templates for typical kinds of organizations
  - Independent Software Vendors
  - Online Service Providers
  - Financial Services Organizations
  - Government Organizations
- Organization types chosen because
  - They represent common use-cases
  - Each organization has variations in typical software-induced risk
  - Optimal creation of an assurance program is different for each
Building Assurance Programs

1. Start
2. Conduct initial assessment
3. If existing roadmap template, select appropriate roadmap; otherwise, create empty roadmap.
4. If adding another phase, select practices to improve; otherwise, mark selected improvements on roadmap.
5. Adjust roadmap to organization.
6. Done.
The OpenSAMM project
Quick stats

- About 40+ orgs using OpenSAMM for their programs
- 7500 unique hits in the last 12 months
- Dozens of contributed tools/resources
Expert contributions

- Built based on collected experiences with 100’s of organizations
- Including security experts, developers, architects, development managers, IT managers

**Author & Project Lead**
Pravir Chandra

**Contributors/Reviewers**

<table>
<thead>
<tr>
<th>Fabio Arciniegas</th>
<th>Brian Chess</th>
<th>Matteo Meucci</th>
<th>John Steven</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matt Bartoldus</td>
<td>Dinis Cruz</td>
<td>Jeff Payne</td>
<td>Chad Thunberg</td>
</tr>
<tr>
<td>Sebastien Deleersnyder</td>
<td>Justin Derry</td>
<td>Gunnar Peterson</td>
<td>Colin Watson</td>
</tr>
<tr>
<td>Jonathan Carter</td>
<td>Bart De Win</td>
<td>Jeff Piper</td>
<td>Jeff Williams</td>
</tr>
<tr>
<td>Darren Challey</td>
<td>James McGovern</td>
<td>Andy Steingruebl</td>
<td></td>
</tr>
</tbody>
</table>
Industry support
The OpenSAMM Project

- [http://www.opensamm.org](http://www.opensamm.org)
- Beta released August 2008, 1.0 released March 2009
- Dedicated to defining, improving, and testing the SAMM framework
- Always vendor-neutral, but lots of industry participation
  - Open and community driven
- Targeting new releases every ~18 months
- Change management process
Future plans

- Mappings to existing standards and regulations (many underway currently)
- PCI, COBIT, ISO-17799/27002, ISM3, etc.
- Additional roadmaps where need is identified
- Additional case studies
- Feedback for refinement of the model
- Translations into other languages
Get involved

• Use SAMM and tell us about it
• Blog, email, etc.
• Latest news at http://www.opensamm.org
• Sign up for the mailing list
Thanks for your time! Questions?

http://www.opensamm.org

Pravir Chandra
OpenSAMM Project Lead
chandra@owasp.org