OWASP Software Assurance Maturity Model (SAMM)

Version 2.0 Update

John DiLeo, OWASP SAMM Project Team
February 2019
About Me

• Born and raised in northeastern US
• Spent A LOT of time in school
• First career: Operations Research / Simulation
• Second career: Web Development
• Third Career: Application Security, since 2014
  – Focus on Software Assurance
  – Moved to NZ in 2017, joined Orion Health
  – Active in OWASP in US and NZ
• Joined OWASP SAMM team in June
What is SAMM?

• The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

• The resources provided by SAMM will aid in:
  – Evaluating an organization’s existing software security practices.
  – Building a balanced software security assurance program in well-defined iterations.
  – Demonstrating concrete improvements to a security assurance program.
  – Defining and measuring security-related activities throughout an organization.
Why SAMM?

"The most that can be expected from any model is that it can supply a useful approximation to reality: All models are wrong; some models are useful.”  – George E. P. Box
Core Principles of SAMM

- Changes must be iterative while working toward long-term goals
- A solution must enable risk-based choices tailored to the organization
- A solution must provide enough details for non-security-people
- OWASP Software Assurance Maturity Model (SAMM)

An organization’s behavior changes slowly over time

There is no single recipe that works for all organizations

Guidance related to security activities must be prescriptive

Overall, must be simple, well-defined, and measurable
Project History

- **OpenSAMM 1.0**: March 2009
- **March 2016**
  - **OWASP SAMM 1.1**
- **February 2017**
  - **OWASP SAMM 1.5**
- **BETA – Jan 2019**
  - **OWASP SAMM 2.0**
The Core Team

• Sebastien (Seba) Deleersnyder – Project Leader, Belgium
• Chris Cooper – Webmaster, United Kingdom
• Bart DeWin – Belgium
• John DiLeo – New Zealand
• Daniel Kefer – Germany
• Nessim Kisserli – United Kingdom
• Yan Kravchenko – United States
## The Core Framework

<table>
<thead>
<tr>
<th>Version 1.5</th>
<th>Version 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Four Business Functions</strong></td>
<td><strong>Adds a Fifth Business Function</strong></td>
</tr>
<tr>
<td>• Governance</td>
<td>• Governance</td>
</tr>
<tr>
<td>• Construction</td>
<td>• Design</td>
</tr>
<tr>
<td>• Verification</td>
<td>• Implementation</td>
</tr>
<tr>
<td>• Operations</td>
<td>• Verification</td>
</tr>
<tr>
<td></td>
<td>• Operations</td>
</tr>
</tbody>
</table>
The Security Practices

• **Governance**
  – Strategy & Metrics
  – Policy & Compliance
  – Education & Guidance

• **Design**
  – Threat Assessment
  – Security Requirements
  – Security Architecture

• **Implementation**
  – Secure Build
  – Secure Deployment
  – Defect Management

• **Verification**
  – Architecture Assessment
  – Requirements-Driven Testing
  – Security Testing

• **Operations**
  – Incident Management
  – Environment Management
  – Operational Management
The Maturity Levels

OWASP SAMM - 3 levels

• Level 1
  1 Initial
  2(a) (Partially) Managed

• Level 2
  2(b) (Fully) Managed
  3 Defined

• Level 3
  4 Quantitatively Managed
  5 Optimising

Rough alignment with CMMI levels
Activity Streams
Example – Operational Management

A: Data Protection
Level 1: Basic Data Protections in Place
Level 2: Data cataloged and data protection policy established
Level 3: Data policy breaches detected and acted upon

B: System Decommm / Legacy Management
Level 1: Identification of unused apps/services
Level 2: Decommissioning and legacy migration processes in place
Level 3: Proactive handling of legacy applications/services
Pain Points with Scoring in SAMM 1.5

**Strategy & Metrics, Level 1:** *Is there a software security assurance program in place?*

Available Responses:
- No
- Yes, it’s less than a year old
- Yes, it’s a number of years old
- Yes, it’s a pretty mature program

But, what about...
- Quality of the Programme?
- Currency of the Programme? Has it been reviewed/updated?
- How do you know the program is still relevant?
Consider Multiple Dimensions

Coverage / Standardisation

Quality

- None
- Champions
- Well spread
- Standardized

- Poor
- Useful
- Solid
- Appropriate
Combining Dimension Scores

**MATURITY SCORE = QUALITY × COVERAGE**

<table>
<thead>
<tr>
<th>Quality</th>
<th>Coverage / Standardization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>0.4</td>
</tr>
<tr>
<td>0.5</td>
<td>0.8</td>
</tr>
<tr>
<td>0.2</td>
<td>1.0</td>
</tr>
</tbody>
</table>
Level 1
Relevant employees are provided an awareness training

Level 2
Employees are provided role specific trainings

Level 3
Employee’s knowledge is regularly assessed
Open Questions

• Number of response values for quality and coverage questions
  – Four? Five?
  – Linear?

• How to compute overall maturity score from individual metric scores across levels
  – Level 2 way more expensive than Level 1
Interested in Getting Involved?

• Provide comments on the current draft
  – [https://owaspsamm.org/v2.0b/feedback/](https://owaspsamm.org/v2.0b/feedback/)

• Join our monthly project calls
  – Second Wednesday of the month, 9:30 p.m. Central European Time
  – That translates to Thursday morning, at 7:30 or 9:30 a.m.

• Join our Slack Channel
  – #project-samm on the OWASP Slack ([https://owasp.slack.com/](https://owasp.slack.com/))