OpenSAMM
Project status / goals

Seba Deleersnyder

SAMM project co-leader

Project Status

- Jan-2013:
  - Seba / Bart / Kuai / Pravir to reboot SAMM project
- Main goals:
  - List of reference users
  - SAMM user group / SAMM workshops at conferences
  - Build SAMM v1.1 or 2.0

Project Status

- Feb-2013: Kick-off call
  - Meeting notes: http://goo.gl/7z1XqJ
  - Started gathering input for improvements
  - Split model / supporting material discussed on the mailing list

- Jun-2013: Roadmap call
  - Meeting notes: http://goo.gl/5k73RT
  - Roadmap: http://goo.gl/C15A3k

- Jul-2013:
  - List of refence users: https://www.owasp.org/index.php/OpenSAMM_Adopters
  - SAMM input for SDLC section ASVS

Project Status

- Aug-2013:
  - Workshops planned for AppSec Europe, USA, LATAM
  - Created HOST grant application: http://goo.gl/OOOeVg
    - Build community: newsletters, workshops, dedicated summit
    - Gather data: questionnaires, case studies
    - Improve model: v1.1 & 2.0 incl translations / training
    - SAMM online: support users / gather data

Project Roadmap

V1.1:

- Incorporate tools / guidance / OWASP projects
- Revamp SAMM wiki
- Practical usage stats, practical testimonies

V2.0:

- Revise scoring model
- Model revision necessary ? (12 practices, 3 levels, ...)
- Application to agile
- Roadmap planning: how to measure effort ?
- Presentations & teaching material
- …

To put in release buckets

- tools and how they can help in control gates
- data collection, massaging and visualisation
- link to CIA (map to assurance levels ?)
- redo some titles (e.g., operational enablement)
- define/support fixing process
- maturity assessment -> link to stakeholders
- application guidance
- supportive material: checklists and methods (links to CLASP ?)
- more on metrics ?
- 4 dimensions: process, knowledge, tools, people
  - process view is largely lacking here
- perspectives: construct, verify, manage (activity metadata)
- continuous improvement
- testing strategy
- automated vs. manual testing
- data security/anonymization
- separation of duty for developers and others
- different development environments
- prerequisites (min. reqs.) to start a software assurance project
- links/relationships between activities: if you do this, you probably need this and this (is already in there to some extent: "related levels")
- security team structure …

SAMM Resources

www.opensamm.org

- Presentations
- Tools
  - Assessment worksheets / templates
  - Roadmap templates
  - Scorecard chart generation
- Translations (Spanish / Japanese)
- SAMM mappings to ISO/EIC 27034 / BSIMM