From SAMM Project
Towards SAMM Suite

SAMM User Day
May 27th, 2021
Daniel Kefer
Daniel Kefer

- SAMM volunteer since 2015
- SecurityRAT project co-lead
- Head of IT Security @ WEB.DE, GMX, mail.com

@DKefer  in/kefer/
**Seen in Various Places**

**ASSESSMENT**
- Is there a software security assurance program in place?
- Are development staff aware of future plans for the assurance program?

**Strategy & Metrics**
- Is there a software security assurance program in place?
- Are development staff aware of future plans for the assurance program?

**Governance**

<table>
<thead>
<tr>
<th>Strategy &amp; Metrics</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a software security assurance program in place?</td>
<td></td>
</tr>
<tr>
<td>Guidance: Assurance program is documented and accessible to staff.</td>
<td>Yes</td>
</tr>
<tr>
<td>Guidance: Assurance program has been used in recent development efforts.</td>
<td></td>
</tr>
<tr>
<td>Guidance: Staff receives training against assurance program and responsibilities.</td>
<td></td>
</tr>
<tr>
<td>Are development staff aware of future plans for the assurance program?</td>
<td>Yes</td>
</tr>
<tr>
<td>Guidance: Assurance program goals are documented and accessible to staff.</td>
<td></td>
</tr>
<tr>
<td>Guidance: Assurance program goals have been presented to staff.</td>
<td></td>
</tr>
<tr>
<td>Guidance: A plan has been put in place to reach those goals in a specific period of time.</td>
<td></td>
</tr>
</tbody>
</table>
### Data Model Implementation

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function Design.yaml</td>
<td>Fix linted files.</td>
</tr>
<tr>
<td>Function Governance.yaml</td>
<td>Update Function Governance.yaml</td>
</tr>
<tr>
<td>Function Implementation.yaml</td>
<td>Textual Optimizations</td>
</tr>
<tr>
<td>Function Operations.yaml</td>
<td>Textual Optimizations</td>
</tr>
<tr>
<td>Function Verification.yaml</td>
<td>Update Function Verification.yaml</td>
</tr>
<tr>
<td>Maturity Level 1.yaml</td>
<td>Fix linted files.</td>
</tr>
<tr>
<td>Maturity Level 2.yaml</td>
<td>Fix linted files.</td>
</tr>
<tr>
<td>Maturity Level 3.yaml</td>
<td>Fix linted files.</td>
</tr>
<tr>
<td>Practice D-Security-Architecture.yaml</td>
<td>Textual Optimizations</td>
</tr>
</tbody>
</table>
# The title of this activity

**title**: Adhere to basic security principles

# Describe the benefit that is achieved by implementing this activity

**benefit**: Sets of security basic principles available to product teams

# A one sentence description of the activity

**shortDescription**: Teams are trained on the use of basic security principles during design

# A multi-paragraph description of the activity

**longDescription**: During design, technical staff on the product team use a short checklist of security principles. This checklist is intended to ensure that the basic security principles are taken into consideration during the design process. For perimeter interfaces, the team considers each principle in the context of the overall system architecture and implements the necessary security measures to ensure that the design meets the security requirements. The team also collaborates with other teams, such as development and operations, to ensure that the security principles are integrated into the entire product lifecycle.
Data Model & Derived Projects

- Model
- Website
- PDF
- Assessment spreadsheet
New GitHub Organization

https://github.com/owaspsamm
Implications on the Core Model

- Switch to semantic versioning: MAJOR.MINOR.PATCH
  - SAMMv2.0 vs SAMM v2.0.0
  - Possibly different releases of language versions

- Switch to git-flow
CI/CD Pipeline: GitHub Actions

```yaml
name: Release

on:
pull_request:
  branches:
    - main
  types:
    - closed

jobs:
  release:
    name: Publish new release
    runs-on: ubuntu-latest
    if: github.event.pull_request.merged == true # only merged pull requests must trigger this job
    steps:
      - name: Extract version from branch name (for release branches)
        if: startsWith(github.event.pull_request.head.ref, 'release/')
        run: |
          BRANCH_NAME="${{ github.event.pull_request.head.ref }}"
          VERSION=${{BRANCH_NAME#release/}}
          echo "RELEASE_VERSION=$VERSION" >> $GITHUB_ENV
```
Assessment Spreadsheet Example

[Image of GitHub interface showing a spreadsheet and code-related actions]
Work In Progress & Next Steps

- Assessment spreadsheet and PDF generator (website already done)
- Migration of issues & archiving the old repository
- Translations (integration with Crowdin)
Thank you!

https://owaspsamm.org/contact/