SECCOM CII Badging

What Does it Mean to Get Gold in CII Badging? (and Silver and Passing)

SECCOM
Tony Hansen
2019/9/27
What is CII Badging About?

“The Linux Foundation (LF) Core Infrastructure Initiative (CII) Best Practices badge is a way for Free/Libre and Open Source Software (FLOSS) projects to show that they follow best practices.”

bestpractices.coreinfrastructure.org

“. . . following best practices can help improve the results of projects. For example, some practices enable multi-person review before release, which can both help find otherwise hard-to-find technical vulnerabilities and help build trust and a desire for repeated interaction among developers from different organizations.”

github.com/coreinfrastructure/best-practices-badge/blob/master/doc/criteria.md

“Compare the cost of defense to the cost of failure”
“Take the software equivalent of basic hygiene steps and combine approaches in a way that make a system harder to successfully attack”
“Failing to implement basic measures for protection, detection and recovery in systems where it matters is just a form of negligence”
“It is an easy way for an open source project to self-improve.” – Dr. David A. Wheeler

How to Develop Secure Applications: The BadgeApp Example

www.youtube.com/watch?v=5a5D4d6hcEY

Creator of the BadgeApp application

Author: Secure Programming: HOWTO dwheeler.com/secure-programs
Some Badge Earniers
Why are we doing this?

Bottom line: We are using CII Badging to get ONAP projects to verify and/or improve the security and quality of their code and the project.

Getting the silver star or gold star from the CII badge is truly secondary.
Progressively Strict

• The three levels are **Passing**, **Silver** and **Gold**

• The questions use SHOULD and MUST to differentiate between Optional (at this level) and Requirements

• Questions will progress across levels:
  - An item introduced in **Passing** as a SHOULD will become a MUST in **Silver**
  - An item introduced in **Silver** as a SHOULD will become a MUST in **Gold**

Answering a SHOULD question as YES counts at ALL LEVELS.
# The CII Sections

<table>
<thead>
<tr>
<th>Passing</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basics</td>
<td>Basics</td>
<td>Basics</td>
</tr>
<tr>
<td>Change Control</td>
<td>Change Control</td>
<td>Change Control</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting</td>
<td></td>
</tr>
<tr>
<td>Quality</td>
<td>Quality</td>
<td>Quality</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td>Analysis</td>
<td>Analysis</td>
<td>Analysis</td>
</tr>
</tbody>
</table>
How is ONAP Doing on Badging Levels?

Passing:
• 30 / 34 are 100% Passing
• Remaining 4 are >85% Passing

Silver:
• 2 are 100% Silver – Wow
• 25 are >75% Silver – Super
• 4 are 30% to 45%
• 7 are < 30%

Gold:
• 5 > 40% – Cool
• 8 are 20% to 40%
• 25 are < 20%
Multiple Categories of Concern

I’ve categorized the different questions using these categories for separate domains of questions:

- The quality of the application itself
- The quality of the project overview
- The quality of the infrastructure used to build and support the application
- The people building the application
- FLOSS encouragement

<table>
<thead>
<tr>
<th></th>
<th>Passing</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Quality</td>
<td>26</td>
<td>24</td>
<td>9</td>
</tr>
<tr>
<td>Project Quality</td>
<td>22</td>
<td>26</td>
<td>8</td>
</tr>
<tr>
<td>Infrastructure Quality</td>
<td>10</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>People</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>FLOSS Encouragement</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>66</td>
<td>55</td>
<td>23</td>
</tr>
</tbody>
</table>
# The Silver Criteria

## Project Quality
- **code of conduct**
- **coding standards**
- **coding standards enforced**
- **contribution requirements**
- **developer cert. of origin**
- **documentation achievements**
- **documentation architecture**
- **documentation current documentation quick start**
- **documentation roadmap**
- **external dependencies governance**
- **installation common installation development quick install development standard variables maintenance or update report tracker signed releases**

## Application Quality
- **test policy mandated**
- **tests documented added**
- **updateable reused comp's version tags signed vulnerability report credit vulnerability resp process**

## Crypto Quality
- **crypto tls12**
- **crypto used network crypto verification private crypto weaknesses**
- **dependency monitoring dynamic analysis unsafe hardening**
- **implement secure design input validation**
- **interfaces current internationalization regression tests added50 static analysis common vulnerabilities**
- **test statement cvrg 80 warnings strict**

## People
- **access continuity bus factor roles responsibilities**

## Infrastructure Quality
- **documentation security sites password security**
The Gold Criteria

**Application quality**
- Two person reviews
- Crypto TLS12
- Crypto Used Network
- Application Hardening
- Dynamic Analysis Tool
- Security Reviews
- 80% test branch coverage
- Test suite invocation standardized
- 90% statement test coverage

**Project Quality**
- License per file
- Copyright per file
- Continuous Integration
- Reproducible Build
- Code Review Standards
- >=2 Unassociated Contributors per project

**People**
- Bus Factor
- Small Tasks for new / casual contributors

**Infrastructure Quality**
- Distributed Repo Tools
- Hardened Site
- 2FA for contributors

**80% test branch coverage**

**90% statement test coverage**
Resources

CII Site

https://bestpractices.coreinfrastructure.org

EXTENSIVE DETAILS ON THE CII QUESTIONS

https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/other.md

Why these questions?

ONAP Resources, including answers to many “questions with ONAP-wide answers”:
https://wiki.onap.org/display/DW/CII+Badging+Program

CII ONAP Portal
http://tlhansen.us/onap/cii.html
<table>
<thead>
<tr>
<th>Name</th>
<th>Code of conduct</th>
<th>Crypto certificate verification</th>
<th>Crypto network</th>
<th>Code of conduct</th>
<th>Crypto certificate verification</th>
<th>Crypto network</th>
<th>Code of conduct</th>
<th>Crypto certificate verification</th>
<th>Crypto network</th>
<th>Code of conduct</th>
<th>Crypto certificate verification</th>
<th>Crypto network</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLHansen</td>
<td>Ref: <a href="http://tlhansen.us/onap/cii.html#silver">http://tlhansen.us/onap/cii.html#silver</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thank you

That’s all

Q & A