Security@ONAP virtual developers event (July)

ONAP security committee
Stephen Terrill

24 July, 2017

Topics

- Introduction
- Vulnerability Management
- CII Badging
- Static Code scanning
- Feedback Reception

Introduction

- ONAP security page: https://wiki.onap.org/display/DW/ONAP+Security+coordination

- Security sub-committee
  - Identifying proposed activities to help the ONAP community create secure system
  - ONAP is creating a mission critical system
  - Onap-seccom@lists.onap.org

- Vulnerability Management
  - The process for managing identified and reported vulnerabilities.

Vulnerability Management

- Vulnerability management is the process to handle identified vulnerabilities
  - Approved Vulnerability Management procedures: https://wiki.onap.org/display/DW/ONAP+Vulnerability+Management
    - How to submit a vulnerability, acknowledge a vulnerability, and manage the process to conclusion including communication.
    - Email: security@lists.onap.org
  - Vulnerability management team (volunteers) are in place:
    - Arul Nambi (ambocs), Amy Zwarico (AT&T), Oliver Spatsh (AT&T). Raun He (orange) Support from Stephen Terrill (Ericsson, security coordinator), David Jorm, Linux foundation (Phil, Andy, Kenny).
    - Will follow a
      - Case lead on a “step-up” approach on per case by case basis.
      - Support team to step in to ensure nothing falls through.
      - Security coordinator also to ensure that all is working ok.
- Note: The vulnerability management sub-committee cannot solve the vulnerabilities, but work with the teams to do so under embargo. *Your support will be critical*.

CII (core infrastructure initiative) badging program

- CII (core infrastructure initiative) has been created by the linux foundation in response to previous security issues in open-source projects (Heartbleed in openSSL).

- The CII has created a badging program to recognize projects that follow a set of identifies best practices that could be adopted.
  - There are three levels passing, silver and gold.

- The security sub-committee has looked at these and feels that given ONAP is managing core critical infrastructure, *the ONAP projects should follow the gold level*.
  - This is a challenge!

- A stepwise introduction is proposed.

CII Badging program, 3 levels

Gold

- More stringent criteria
  - Security Review, project continuity, continues test integration, 70%+ test coverage, secure design, ….

Silver

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

Passing

- Basic practices
- Largely also covered by Release Best Practices

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

Example criteria

- Passing:
  - The project website MUST succinctly describe what the software does (what problem does it solve?).
  - The project MUST use at least one automated test suite that is publicly released as FLOSS (this test suite may be maintained as a separate FLOSS project).
- Silver
  - The project MUST document what the user can and cannot expect in terms of security from the software produced by the project. The project MUST identify the security requirements that the software is intended to meet and an assurance case that justifies why these requirements are met. The assurance case MUST include: a description of the threat model, clear identification of trust boundaries, and evidence that common security weaknesses have been countered
- Gold:
  - The project MUST have at least 50% of all proposed modifications reviewed before release by a person other than the author, to determine if it is a worthwhile modification and free of known issues which would argue against its inclusion.

CII Badging Scope and Sample Requirement Areas

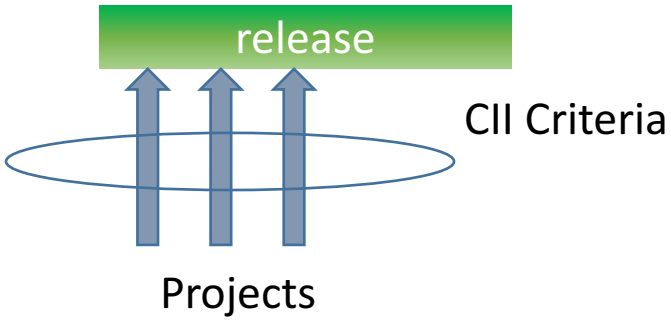
- **General Project Areas**
  - Project description, OSS licensing, documentation, website, support TLS, change control, unique version numbering, release notes
- **Reporting**
  - Bug-reporting process, vulnerability report process
- **Quality**
  - Maintain golden source for rebuilding, use common tools, automate test suite, perform new-functionality testing, address compiler warning flags
- **Security**
  - Developers security knowledgeable, use good cryptographic practices, protection against man-in-the-middle (MITM) attacks, fix publicly known vulnerabilities, don't leak valid private credential
- **Analysis**
  - Perform static code analysis, perform dynamic code analysis, fix vulnerabilities

CII badging program in ONAP

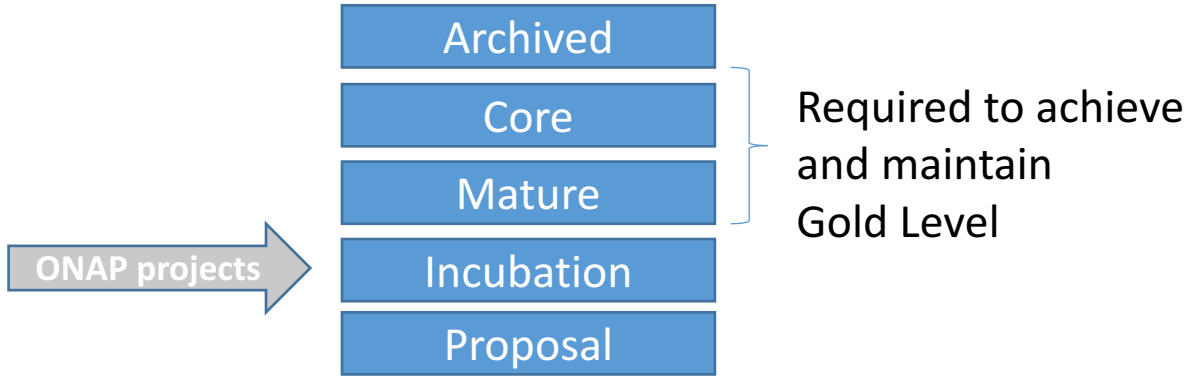
- Current proposal:
  - Stepwise introduction:
    - Start with 1 project
    - Any volunteer?
  - Code producing project is gold for a release, exceptions taken to TSC.
    - ONAP is mission critical software.

- It was pointed out that we could tie this to the project maturity instead.

Release Based Approach



Project Maturity Based Approach



Community View ????

Static Code Scans

- Currently the sub-committee is looking to create a proposal to achieve static code scans of submitted codes.
  - Purpose of code scans is to identify security vulnerabilities.
  - A concrete proposal is not ready at this stage, so we are just sharing early thoughts for feedback.

- Tools:
  - Nexus Lifecycle Management tool; Other?

- How
  - Scan on push?
  - Scan on time?

- Process considerations
  - Need to manage the tool conclusions.
    - Eliminate false positives
    - Handle identified issues
    - Who?

Note: This is considered as an additional measure, not to remove the responsibility from the projects to produce secure code

Community View ????

Other Feedback

- Security subcommittee has:
  - Created the vulnerability management procedures
  - Proposed actions for CII badging programe
  - Investigating static scanning

- We would like feedback from the community about other pressing issues that are on your mind.

Community View ????

ONAP, the Secure Open Networking Platform