Security Subcommittee
virtual developers event (September)

ONAP security committee
Stephen Terrill
Topics

• Introduction

• Structure and way of working

• Vulnerability Management

• Ongoing

• CII Badging Feedback
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. CLAMP Feedback today
Work in progress

• Static Code Scans
• Credential management

• https://wiki.onap.org/display/DW/ONAP+security+Recomendation+Developement
CII Badging program feedback from CLAMP
ONAP, the Secure Open Networking Platform