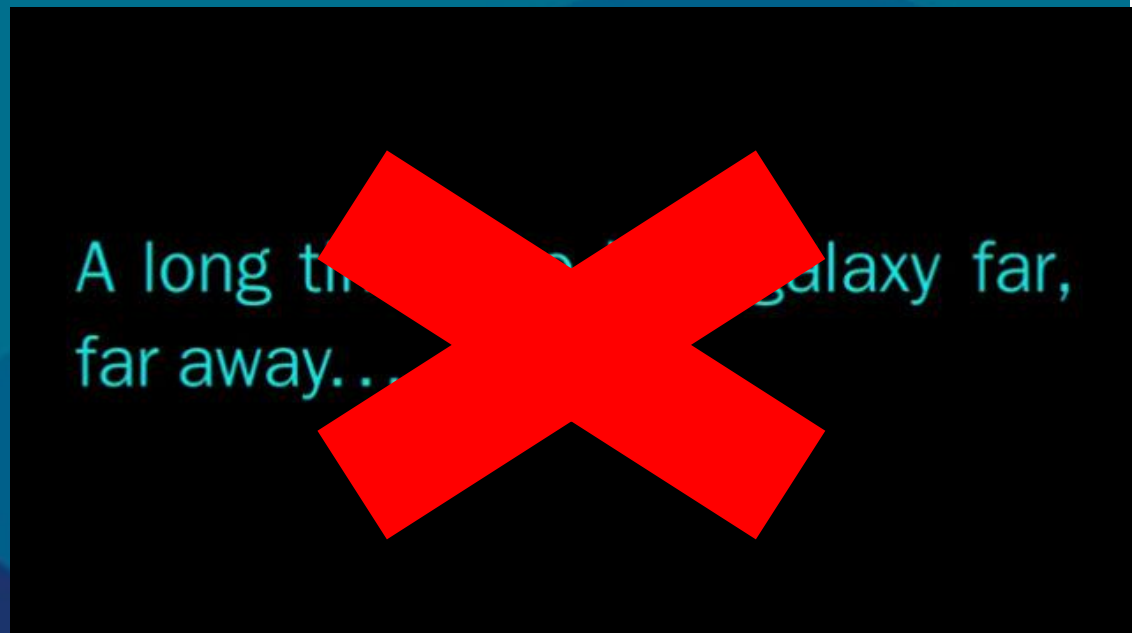
Security in ONAP: myth or reality?

Pawel Pawlak

12th March, 2019



What is ONAP (Open Network Automation Platform) ?

ECOMP

+

OPEN-O

- 2+ years of Deployment Maturity at AT&T
- Comprehensive: Design + orchestration + control + policy + analytics
- A clean plate approach for VNF / SDN enabling self-serve capabilities for instantiation and closed loop automation

- Successful release 2 (Mercury) delivered 2017/04/27
- Open TOSCA model, Architected for ease of VNF insertion (SDK)
- Most Advanced Open Source Process & Toolchain
- Redevelop Brownfields

CSP representing 70% of worldwide mobile customers have joined ONAP community

THE LINUX FOUNDATION

Platinum members (28)

Silver members (67)

Associate members (11)

Gold members (4)

aptira, INOCYBE TECHNOLOGIES, lumina networks, Microsoft

ONAP release

2017		2018				2019	
Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Amsterdam		**Beijing**		**Casablanca**		**Dublin**	

Can open source be secure?

- Code is available for everyone and can be easily inspected in Open Source Software vs. Closed Source Software
- Sharing culture
- Transparency approach
- Critical mass is there, variety of people is an added value
- Tools available on the market
- Best practices

- Developers motivation… is crucial
- Focus on features development
- Security at the very beginning is not top priority
- Documentation is not the strongest point
- In complex solution like ONAP there is a lot of security related topics to coordinate…(i.e. internal and external communication, RBAC, un/known vulnerabilities management, components release management, recommended protocols and their versions, passwords encryption methods, general security guidelines…

SECCOM general activities

- Vulnerability management = how to handle the reception of an identified vulnerability through to solution and communication of the vulnerability. The process is initiated by the reception of an email to security@lists.onap.org. The vulnerability management procedures can be found here: ONAP Vulnerability Management.
- The vulnerability management procedures are executed on by the vulnerability management sub-committee.

- The ONAP security sub-committee identifies and creates proposals related to security in ONAP. As one example, it has created the proposal for the Vulnerability management procedures which are now in effect. The ongoing efforts of the ONAP security sub-committee are now to explore more proactive security activities.
- The email address for the onap sub-committee is: onap-seccom@lists.onap.org
- SecCom meetings: Wednesdays 3 PM (Warsaw/Paris time)

Recent hot ONAP security topics

Security sub-committee Jira Kanban board:

https://jira.onap.org/secure/RapidBoard.jspa?rapidView=103

ONAP security requirements

CII Badging

https://wiki.onap.org/display/DW/CII+Badging+Program

Secure communication to xNF aka 5G use case security

https://wiki.onap.org/display/DW/Secure+Communication+to+Network+Functions

Recommended protocols

https://wiki.onap.org/display/DW/Recommended+Protocols

Cryptographic Signing of Release Artifacts

https://wiki.onap.org/display/DW/Cryptographic+Signing+of+Release+Artifacts

Dublin security by design

https://wiki.onap.org/display/DW/Proposed+Updates+to+Release+Templates+%28Dublin%29+-+Security+Questions

Casablanca maintenance projects vulnerabilities review

VNF requirements

https://jira.onap.org/browse/SECCOM-22

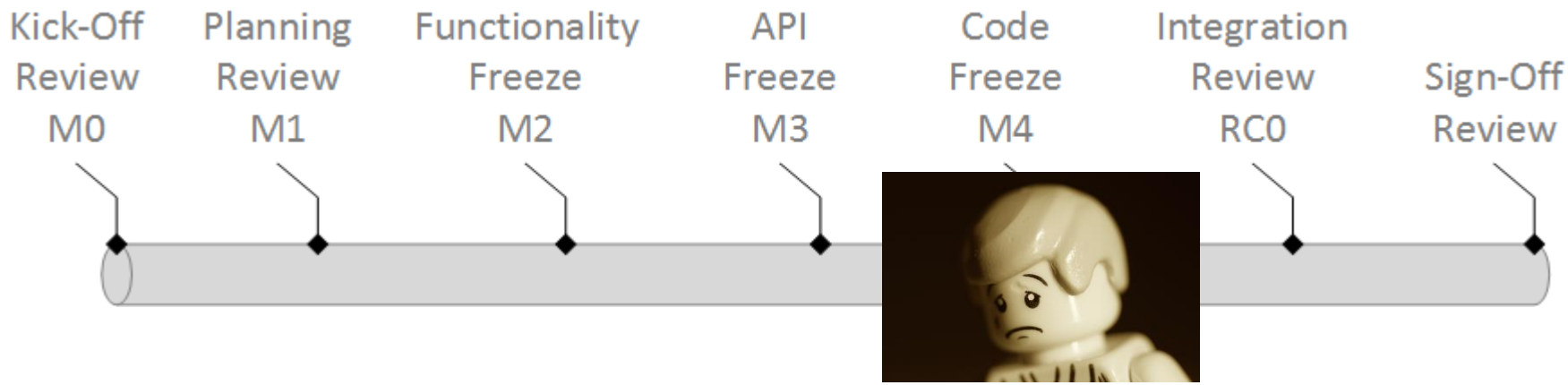
https://onap.readthedocs.io/en/latest/submodules/vnfrqts/requirements.git/docs/Chapter4/Security.html

Casablanca penetration tests

Example: security by design

ONAP Release Lifecycle Overview

More details: https://wiki.onap.org/display/DW/Release+Lifecycle#ReleaseLifecycle-ReleaseAPIFreeze



Why don't we ask right questions at the right time?

https://wiki.onap.org/display/DW/Proposed+Updates+to+Release+Templates+%28Dublin%29+-+Security+Questions

Security in ONAP: myth or reality?

Rome was not built in one day…

- Mature security open source project example:

openstack®

- In ONAP we build security awareness among the community…
- Security is everyone's responsibility
- Focus on processes, tools, techniques
- DevSecOps target

THANK YOU!