# LF NETWORKING

LFN Developer & Testing Forum

ONAP: Code Quality Demo

2022-01-11

- Pawel Pawlak, Kevin Sandi, Fabian Rouzaut

Why improve code quality for ONAP?

- It's important to keep in mind, ONAP could be deploy on operational environment.

- ONAP has a central position in the orchestration chain of the network.

- For a country or an operator, loss the control of ONAP has a huge impact.
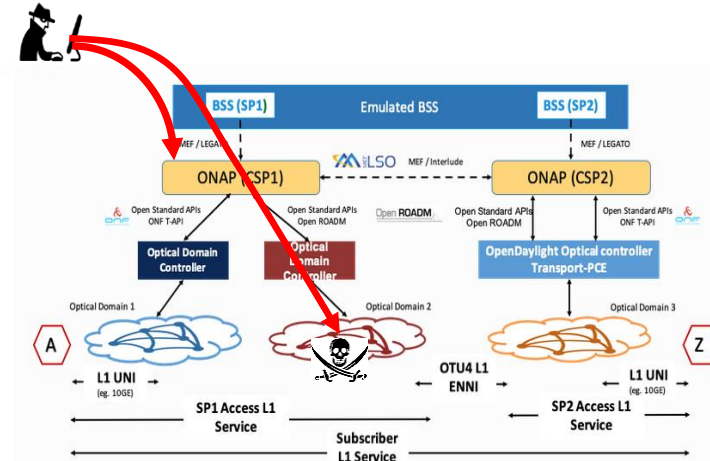
ONAP MDONS Architecture example
Through ONAP, the hacker could have the control to the network
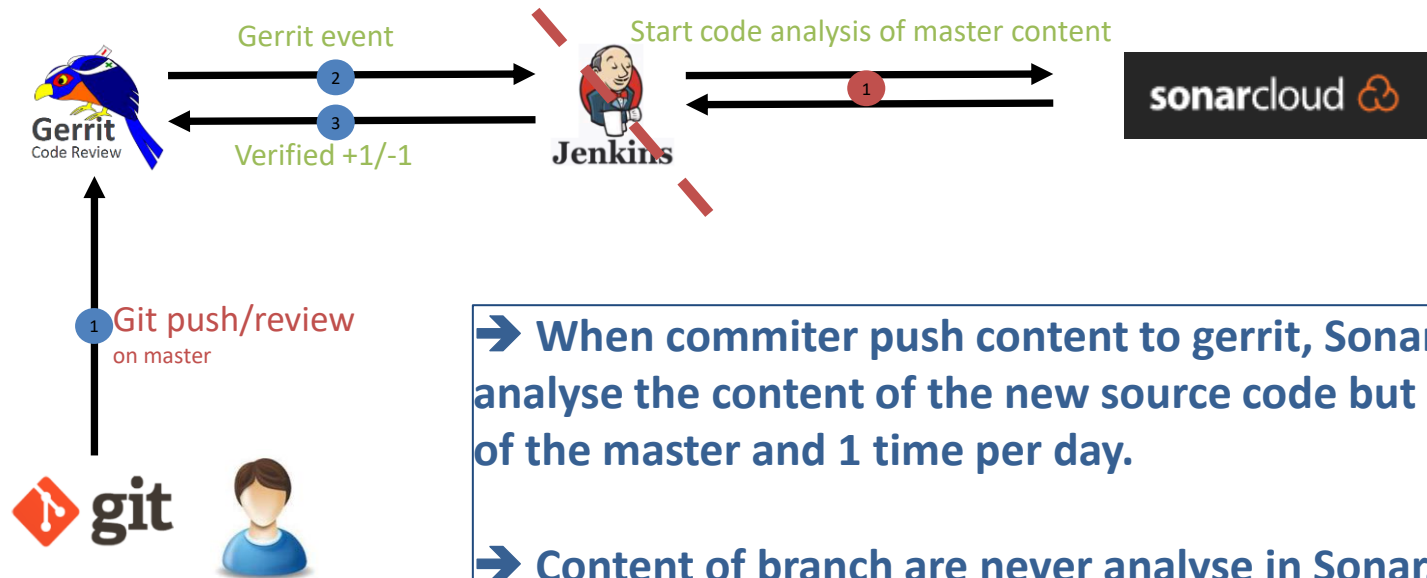
Code quality reduce threats

Why improve code quality for ONAP?

- Fixing problems after merge has a cost.(which can be 20-50% more expensive).

- Post-merger problem solving could be impossible without a business view

- We have done the exercise on a few components, but the gain in safety was small.

Fixed issues after merge:
- Security hotspot : 10
- Blocker : 17
- Critical bug : 63
- Major bug : 119

Open Network Automation Platform (ONAP) / sdc / master

Overview   Issues   Security Hotspots   Measures   Code   Activity

Quality Gate   Passed

Reliability Measures

99 D
Bugs

started 2 years ago

Security Measures

12 B   46 E
Vulnerabilities   Security Hotspots

Maintainability Measures

174d A   10k
Debt   Code Smells

security by design need to be implemented

Current status

Gerrit event

Start code analysis of master content

Verified +1/-1

Git push/review
on master

➜ When commiter push content to gerrit, Sonar does not analyse the content of the new source code but the content of the master and 1 time per day.

➜ Content of branch are never analyse in Sonar.
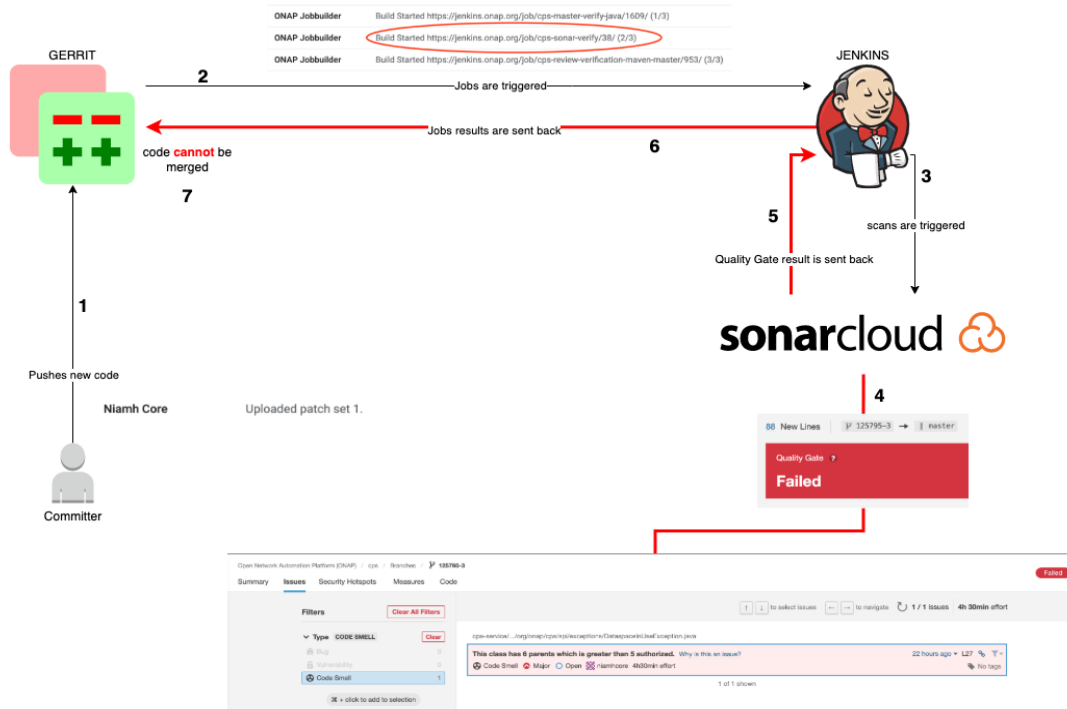
Proposal

To be "security by design" ready , ONAP code changes must be automatically analyzed through SonarCloud scans before the merge stage.
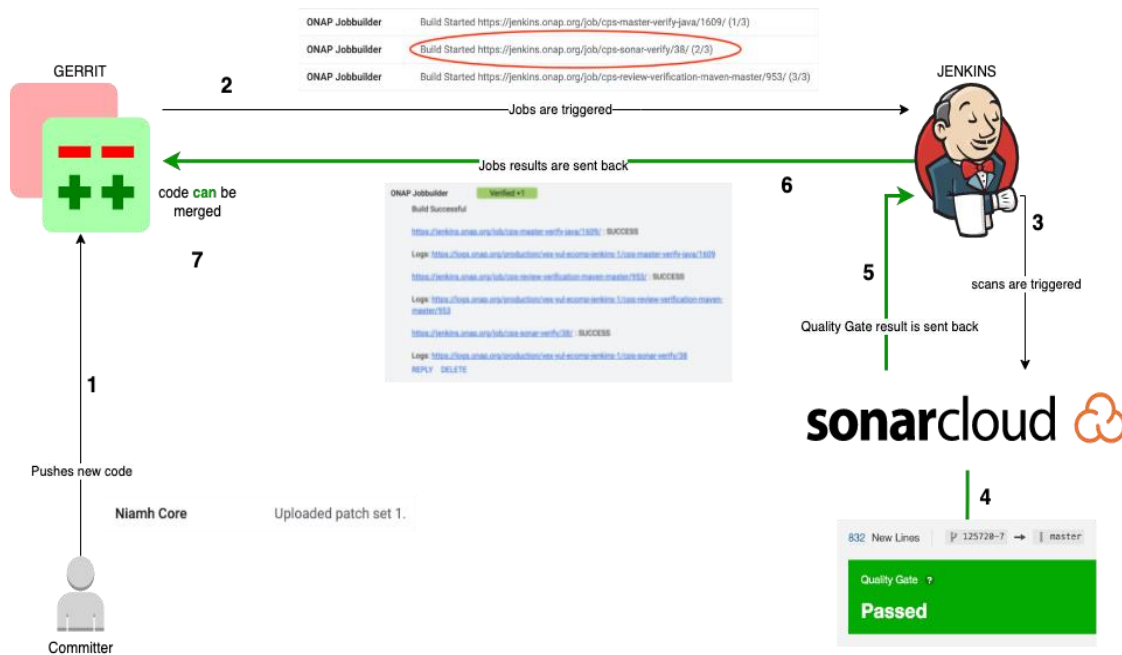
Proposal

<u>Worse case</u>

Scenario #2

Sonarcloud – quality gates proposal

https://wiki.onap.org/display/DW/Code+Quality+Gates

Bronze (mature project not at all)

Metric	Operator	Value
...ge	greater than	55%
...tspots	equal	A
...ting	equal	A

Silver (in progress to mature project)

Metric	Operator	Value
Test coverage	greater than	60%
...Lines	less than	6%
...lity Rating	greater than or equal to	B
...ating	greater than or equal to	B
...tspots	equal	A
...ting	equal	A

Gold (code mature)

Metric	Operator	Value
Test coverage	greater than	80%
Duplicated Lines	less than	3%
Maintainability Rating	equal	A
Reliability Rating	equal	A
Security Hotspots	equal	A
Security Rating	equal	A

Next steps

- New job "gerrit-maven-sonar-verify" → Done and good

- Setting and adapt a quality gate for a POC → Done

- POC : Implement on one of CPS project → Done but too good
  - Need a second project for a POC (SO project candidate)

- Define quality gate for Mature, no mature project → Need to talk about it
- Generalize to all projects → To be done