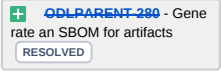


# Security tools adoption survey

The TAC is seeking a refresh of the project tool adoption. Projects should update this table by 18 Oct 2023

|        | SBOM                                                                                                                    | OpenSSF best practices badge                                                                                                                                                              | LFx Security Dashboard                                                                                                                                                                         | Static Application Security Testing (SAST) | Software Composition Analysis (SCA) | Dynamic Application Security Testing (DAST) | Container Scanning | Automated Code Coverage Testing | Code Quality | Vulnerability Reporting                                                                                              | Other                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-------------------------------------|---------------------------------------------|--------------------|---------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONAP   | In progress. Debugging SPDX Generator Jenkins integration                                                               | Adopted by all sub projects. Several sub-projects at Silver level                                                                                                                         | On-boarded. OpenSSF badging inaccuracy fixed. Stale repos removed.                                                                                                                             | SonarCloud                                 | NexusIQ                             |                                             |                    | SonarCloud                      | SonarCloud   | Implemented                                                                                                          | Activ secu sub-comr . Met regul and preerely addr threa and vulne ies.                                                                                                                                                                                 |
| FD.IO  | issue in finding suitable tool (VPP written in C code)                                                                  | Work on OpenSSF badging not started yet but on a cursory review nearly all criteria are adopted.                                                                                          | ■ On-boarded                                                                                                                                                                                   |                                            | Coverity                            |                                             | N/A                | Gcov Report Generation CI job   | Coverity     | Implemented                                                                                                          | Cove scan (and fixing issue found has t ongo since 2016<br><br>Secu Resp Proc in ple since 2016                                                                                                                                                        |
| ODL    | Integrated CycloneDX into CI<br><br> | In Progress 90%                                                                                                                                                                           | On-boarded                                                                                                                                                                                     |                                            |                                     |                                             |                    |                                 |              |                                                                                                                      |                                                                                                                                                                                                                                                        |
| Anuket |                                                                                                                         | Deemed inapplicable for spec sub-projects.<br><br>Cedric Ollivier : self declarative checks don't bring any value to the code project compared to patchset and deliverables verifications |                                                                                                                                                                                                |                                            |                                     |                                             |                    |                                 |              | See all *-grype and *-trivy views in build.opnfv.org<br><br>ex: Xtesting<br><br>xtesting-grype [Jenkins] (opnfv.org) | A few code proje are runni the v know both Pyth and Dock secu tools (ban trivy, etc.). They even runni as verifi jobs Func tox.ir funct Test suite and case verifi OPN Platts funct<br><br>Cedr Ollivi it ont mast few L proje fail ir chec the s bran |
| EMCO   | Work on SBOM not started yet                                                                                            | Work on OpenSSF badging not started yet                                                                                                                                                   | Gitlab is not yet supported by the dashboard ( <a href="https://community.lfx.dev/t/gitlab-support-or-manual-scans/1003">https://community.lfx.dev/t/gitlab-support-or-manual-scans/1003</a> ) |                                            |                                     |                                             |                    |                                 |              | GitLab issues? (nothing formalized yet)                                                                              | Secu analy (Aug 2021 vasa Adde - Sec EMC                                                                                                                                                                                                               |

|        |  |         |            |  |  |  |  |  |  |  |  |
|--------|--|---------|------------|--|--|--|--|--|--|--|--|
| XGVela |  |         | On-boarded |  |  |  |  |  |  |  |  |
| L3AF   |  |         | On-boarded |  |  |  |  |  |  |  |  |
| ODIM   |  |         | On-boarded |  |  |  |  |  |  |  |  |
| Nephio |  | started | On-boarded |  |  |  |  |  |  |  |  |