# Streamlined process for releasing EUMESAT SW under open-source licenses.

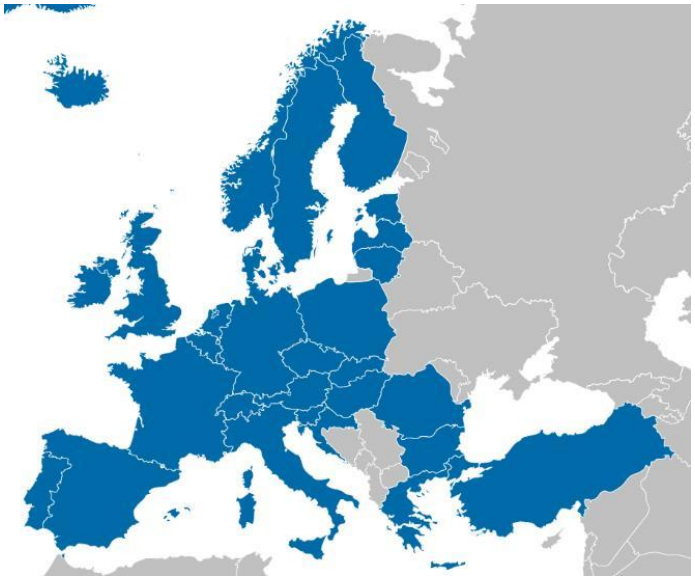
Jose Barba
*EUMETSAT*

*ESA software product assurance workshop 2023*

# EUMETSAT – Who we are

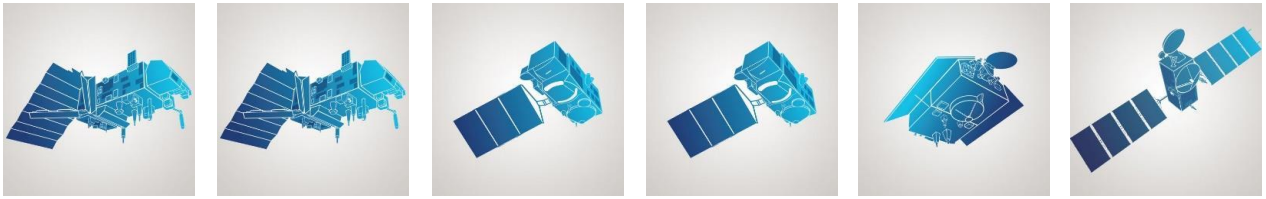


- EUMETSAT is the European operational satellite agency for monitoring weather, climate and the environment.
- Intergovernmental organization, founded in 1986.
- 30 member states.



- 4 GEO satellites (3 MSG & 1 MTG)

- 6 LEO satellites (2 Metop, 2 S3, 1 S6, 1 Jason)



# Checking EUMETSAT SW



- The TSS department provides support to the whole organisation.
- Within TSS, the SW QA team checks all EUMETSAT SW.
- Three SW aspects are evaluated:
  - Source code quality
  - Security/vulnerabilities
  - IPR/licensing aspects

sonarqube

revenera | SCA

- SW checks are performed:
  - (Before receiving the SW, reports are requested to contractors)
  - For incoming SW, the SW checks are initiated at the Incoming Inspection time, and the results are considered for the Acceptance.
  - For outgoing SW (if not previously checked), before the distribution.
  - For internal development, continuous SW checks using CI pipelines.

# SW Decision Gates– Source code quality 1/3

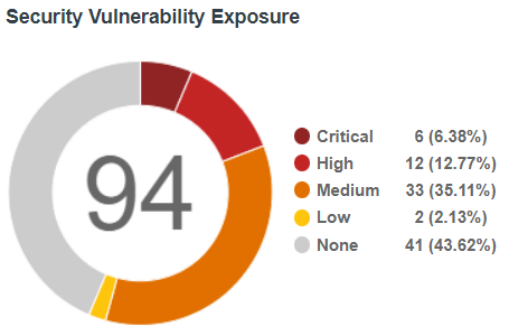


- The outputs of these checks are used in Decision Gates.
- Decision gate for source code quality: Well-known topic with mature solutions. ☺
  - EUM Quality model, based on ECSS, tailored per SW criticality class.
  - Coding standards, configured into SonarQube profiles.
  - SonarQube provides Quality Gates with clear "passed/failed" values.

# SW Decision Gates – Security/Vulnerabilities 2/3



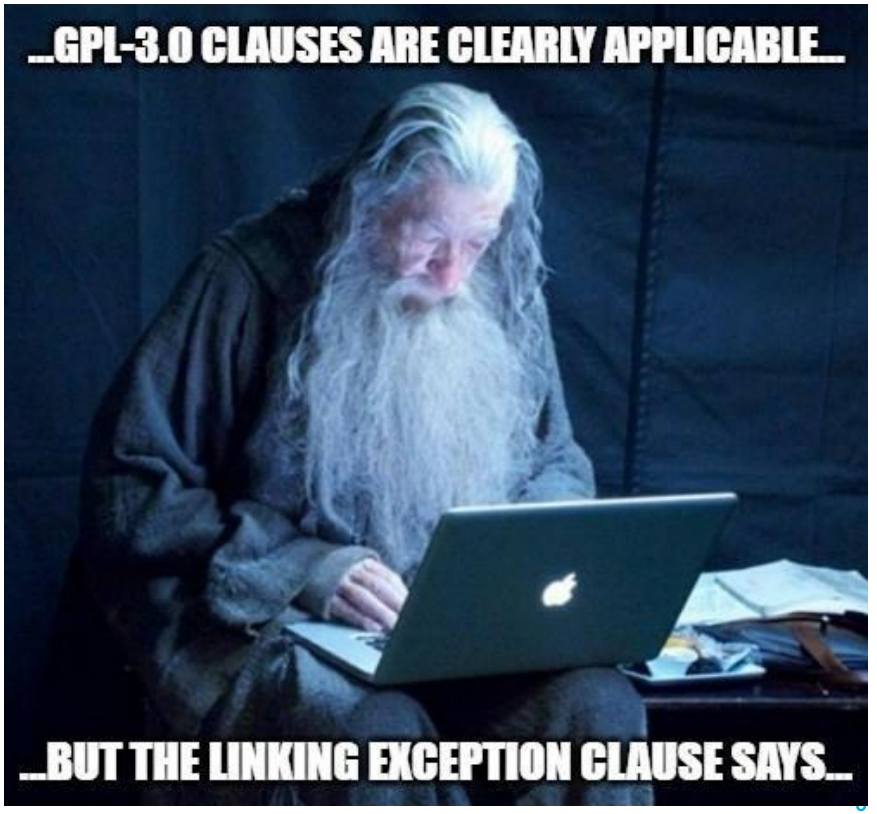
- Decision gate for security/vulnerabilities: Another well-known topic with mature solutions.☺
  - The National Vulnerability Database provides clear CVE categories (low/medium/high/critical) based on numerical scores (0 to 10).
  - A decision gate can be created by just selecting the maximum acceptable CVE category or score.




# SW Decision Gates – IPR/License 3/3



- Decision gate for IPR/licensing: Much more difficult topic, with different associated risks. ☹
  - Some standards for documenting IPR information (as SPDX) but they are not very extended.
  - Even having clear IPR info will not solve the problem, as the implications of using certain licenses are complex.
  - Some initiatives present IPR information in a more legible way (e.g. TLDRlegal.com or Joinup Licensing Assistant)
  - Expert assessment is frequently required.



# EUMETSAT approach for managing SW IPR/Licensing

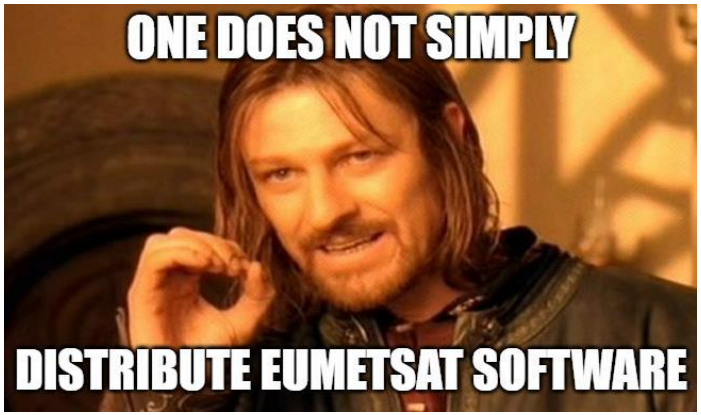


- In general, EUMETSAT expected all its SW, generated by staff or contractors, to declare EUMETSAT copyright and proprietary license.
- That means:
  - EUMETSAT has full control of the SW.
  - No use, modification or redistribution is allowed without EUMETSAT approval.
  - It is a good and legally safe option for SW running in controlled environments and (almost) never distributed.

# EUM approach for the exceptional SW distribution



- The process for distributing any EUMETSAT SW is to produce a assessment report ensuring that there are no risks for EUMETSAT.
- The identified potential risks are:
  - Disclosure of SW may affect EUM activities.
  - SW contains vulnerabilities or disclosure of sensible information.
  - The selected license is not fit for the purpose.
  - IPR information is not clearly indicated, or there are IPR issues.
  - SW quality is not acceptable for the purpose.
- These assessments must be reviewed by the requester, the SW check responsible, a security responsible, a legal representative… and approved by the Director of the Department where the SW belongs to.
- Unfortunately, with this process, if the SW evolves it would require a new assessment for each version.
- In summary, the process requires a significant effort, with lots of people involved, potential bottlenecks, several iterations needed…



# EUMETSAT new approach for IPR



- But times are changing and the need for distributing SW is becoming more and more frequent.
- There is a pushing trend towards other licensing options:
  - EUMETSAT distributes public tools, used for data access, with frequent upgrades.
  - Training materials, specifically created for open distribution, and encouraged to be redistributed and modified by our users.
  - Projects funded by Copernicus Programme, using Copyleft licenses (GPL-3.0), owned by the European Commission.
  - Evolutions of ESA SW, with ESA Community license.
  - Some collaboration projects with other organisations, using open-source licenses and not owned by EUMETSAT.
- A new process (faster, simpler) is required for approving SW distribution.

# Streamlined approach for distributing open-source SW - 1



- Based on the existing process, and the lessons learnt, a new solution/process has been proposed:
  - An initial check is performed by the SW checks team.
  - SW is distributed only through EUMETSAT's GIT repositories.
  - GitLab pipelines are configured to launch the SW checks (both SonarQube and Revenera SCA) automatically.
  - SW QA regularly monitors the status of these public repositories, but…
  - …moving the responsibility down to the SW responsible (and not involving directors!).
  - Training and support is provided to the SW teams on how to read the outputs, how to fix the issues, and when to escalate to the SW checks team.
  - A decision gate, with **clear criteria for each potential risk**, has been agreed with all the roles involved in the previous assessments (next slide…)

# Streamlined approach for distributing open-source SW - 2

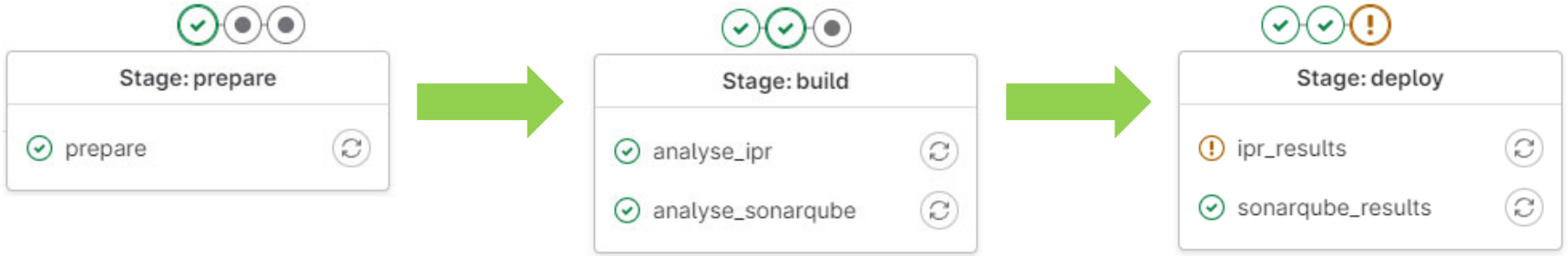


- Pass/fail criteria for each aspect.
  - SW value for EUM → Only applies to training material & open tools.
  - Vulnerabilities → No critical (9-10) or high (7-8.9) CVE scores detected.
  - Sensible information → No "vulnerabilities" or "security hotspots" in Sonar.
  - SW quality → SonarQube shows a green quality gate.
  - License fit for the purpose → Only a pre-approved set of licenses can be used (MIT, Apache-2.0, GPL-3.0)
  - IPR status → No IPR issues detected:
    - Files with the wrong copyright,
    - Files with incompatible licenses,
    - Files with unknown copyright or license,
    - No README or LICENSE file,
    - Code snippets (with confidence > threshold).

# Pipeline examples



- A simple pipeline with three stages is configured/added for these public repositories.
  - Prepare stage: for establishing the environment for launching the SonarQube and Revenera checks.
  - Launch analysis stage: launching both analysis.
  - Analysis result stage: getting the results and applying the pass/fail criteria.



# Pipeline IPR results



- Logs show more information, plus a link to the Revenera tool:

**Package general information**

**Vulnerabilities on the detected libraries/dependencies**

**IPR issues**

Incompatible/unknown licenses

**List of rejected libraries**

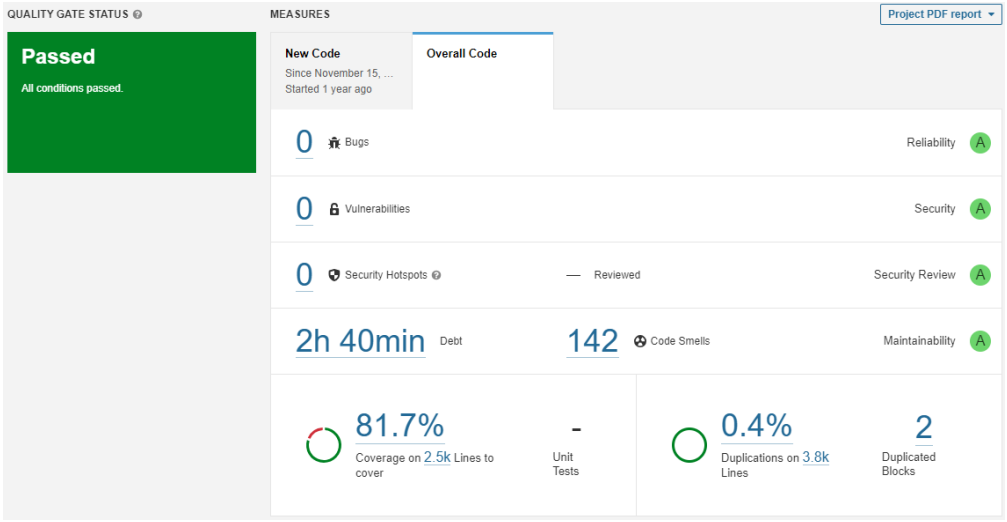
**Other IPR issues**

```
156 ------------------------------ANALYSIS RESULTS------------------------------
157 Policy profile used: Apache SW License Policy Profile (Reject CVSS 6-10)
158     Scan Summary
159      -Files:  19
160      -Size:  16.68 MB
161      -LOC:  501
162     Security Vulnerability Exposure
163      -Critical:  0
164      -High:  3
165      -Medium:  2
166      -Low:  0
167      -None:  5
168      -Total:  10
169     License Exposure
170      -P1 - Strong Copyleft:  4
171      -P2 - Weak Copyleft:  0
172      -P3 - Permissive: 16
173      -Unknown: 0
174      -Total:  20
175     Inventory Review status
176      -Approved:  16
177      -Rejected:  4
178           - clamav-scanner 0.99.4 (GPL-2.0-only)
179           - policycoreutils 2.5 (GPL-2.0-only)
180           - python-sssdconfig 1.16.2 (GPL-3.0-only)
181           - syslog-ng 3.5.6 (GPL-2.0-or-later)
182      -Not reviewed:  0
183      -Total:  20
184     Published Inventory Items
185      -Reviewed Evidence Files:  9 of 15 --> 60.0 %
186 For further information please go to:
187 http://flexnet.opscloud.eumetsat.int:8888/codeinsight/FNCI#myprojectdetails/?id=2261&tab=projectInventory
188 -------------------------------------------------------------------------------
```

# Pipeline SW quality results



- For the SW quality checks, the logs show a link to SonarQube:

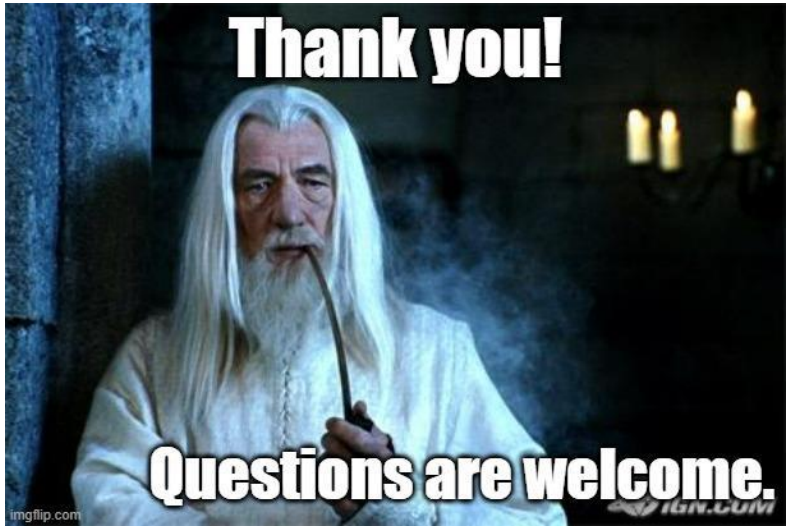



- A SonarQube project portfolio is used to monitor the process:

# Conclusions



- The new process has been successfully implemented on the public repositories (already approved via risk assessments) in order to monitor that they remain risk-free.
- It has reduced considerably the time for approving the distribution of SW:
  - No need to wait for feedback from the different roles.
  - The development teams (internal or external) have clear goals.
  - Issues are addressed directly by the dev. team with (almost) immediate feedback.
  - The SW checks team can contribute, in a temporary branch and with a merge request, directly to the Git repository (file headers, README and LICENSE.txt files, SBoM…)
  - Some issues can only be solved by the SW checks team (e.g.: false positives, components requiring manual analysis…) but iterations are much faster now.
- It reduced the time for distributing new versions of already approved SW. Once a SW package is "risk-free", it requires little effort to keep it like that.


Thank you!
Questions are welcome.
imgflip.com