Enhancing SW build process and licensing compliance analysis with new tools

We are introducing new tools integrated into software build processes for smoother, more secure continuous integration.

Advantages of adding ORT to the SW build process

Highly customizable:
Define excludes, choose different scanners and advisors, and evaluate the results according to the company's compliance.

Impact on Security and Legal Compliance:
Teams can proactively address issues and mitigate the risk of legal challenges related to licensing violations.

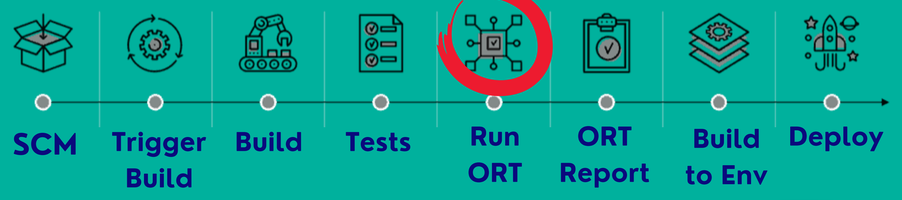
Automated policy enforcement:
ORT allows curating the detected viabilities and errors automatically.

Have you checked the compliance of your SW lately?

- **Challenge:** Track and manage all of the dependencies
- **Risk:** Security vulnerabilities, licensing issues, and copyright infringement
- **Goal:** An integrated solution into the CI build pipeline

01. Objective

Integrate a toolset to scan SW for vulnerabilities, licensing issues, and copyright infringement into software build pipelines.



02. ORT Pipeline

ORT (OSS review toolkit) is a FOSS policy automation and orchestration toolkit to manage your SW dependencies. Each tool below can be seamlessly integrated into any SW build process. The ORT pipeline consists of five main jobs that are executed before deployment.

Complete Dependency Graph Identifies deprecated dependencies	Scan all dependencies Detected licences Mismatches	Retrieves security advisories Detected vulnerabilities for malicious injections	Policy violations according to the custom license classification Provides curation if stated	Human-readable report in desired format

03. Scanner

Ort supports a variety of different scanners, including snippet scanners:

- FossID (optimized for ORT but commercial)
- ScanCode (optimized for ORT and open source)
- Askalono
- Ic
- Licensee
- SCANOSS

Performance studies show which scanner is performing the best in which environment.

04. Project Milestones

- ☑ **Build ORT docker image**
- ☑ **Run all tools locally**
- ☑ **Integrate ORT Pipeline in Jenkins**
- ☑ **Test pipeline on ESA repo GUSTO**
- ☑ **Test pipeline on ESA repo XRISM-TAC**

05. Future Outlook

Expansion to Other CI/CD Pipelines:
After Jenkins, more Deployment (CI/CD) pipelines, such as Drone, will follow.

Fully automated integration in PLATO Deployment (CI/CD) pipelines:
Seamlessly integrating the ORT tools into a new mission development pipeline.

Exploring Cautionary Aspects with ML:
We can explore machine learning's potential to enhance efficiency by automating tasks like vulnerability resolution and license exclusions.

Author: Rebecca Barth