OSCRAT

Open-Source Cyber Resilience Act Tools

D3.1

BETA RELEASE

Submission date: 27/02/2026

Author: OVES Enterprise

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

D3.1 Beta Release

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Number	101190180
Deliverable Name	D3.1 Beta Release
Work package	WP3 – Software design and development
Due Date	28/02/2026
Submission Date	27/02/2026
Lead Partner	OVES Enterprise
Author name(s)	Liliana Hornea
Version	1.0
Status	Final Version
Type:	☐ R – Document, Report ☐ DEC – Websites, patent filings, videos, etc. ☒ DEM – Demonstrator, pilot, prototype
Dissemination level:	☒ PU - Public ☐ SEN - Sensitive

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Document History			
Version	**Date**	**Modified by**	**Comments**
0.1	23/02/2026	Liliana Hornea	Draft version
0.2	23/02/2026	Nadja Dokter	Verification, Formatting and Finalisation
1.0	24/02/2026	Liliana Hornea	Final Version

Abstract

The beta release marks the stage in the product development lifecycle when the nearly finalized version is shared with a specific group of users for testing and feedback.
Following internal testing (alpha phase), external users, known as beta testers, interact with the product in real-world scenarios. The main objective is to collect feedback to identify issues, gain insights into user experience, and refine the product before its official launch.
The release will be well documented with a product release document

Keywords

Beta Release, testing, Cybersecurity,

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Table of contents

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1. Introduction

The beta release represents a key milestone in the product development lifecycle, marking the transition from internal validation to real-world user engagement. Following the completion of the alpha phase and internal testing, a nearly finalized version of the product is made available to a selected group of external users—beta testers.

This stage aims to gather valuable feedback in real-world usage scenarios in order to identify potential issues, evaluate user experience, and refine the product prior to its official launch.

The beta release can be accessed here: https://frontend-production-7c4a.up.railway.app/auth/login

2. Objectives

- **Identify issues**
  Detect problems that may arise when the product is used in real-world scenarios.
- **Gain insights into user experience**
  Understand how users interact with the product and evaluate overall usability.
- **Refine the product before its official launch**
  Improve and adjust the product based on the feedback collected from beta testers and stakeholders.

3. Beta Release

The OSCRAT Beta Release delivers a functional, end-to-end platform for managing compliance with the EU Cyber Resilience Act.

The beta includes the following core functionalities:

- **Product & Version Management** — Create products, classify them by type and risk level, and track their compliance status from initial assessment through certification.
- **CRA Compliance Assessments** — Evaluate product versions against CRA requirements using guided assessment forms, generate Declarations of Conformity, and upload Conformity Assessment Reports.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- **SBOM Generation & Vulnerability Scanning** — Connect source code repositories to automatically generate Software Bills of Materials and scan them for known vulnerabilities, with full severity classification and remediation tracking.
- **Incident & Vulnerability Management** — Log, classify, and track security incidents and vulnerabilities through structured workflows, including cross-border impact and corrective action documentation.
- **Task Management** — Create tasks manually or generate them automatically based on compliance status, assign them to team members, and track progress with comments and attachments.
- **Team Collaboration & Access Control** — Manage teams with role-based permissions, invitations and audit logging.
- **Authentication** — Sign in via email/password, magic link.

4. Next Steps

Post beta release deployment and testing, the project starts the next development cycle. Based on feedback and roadmap defined in the project work packages, the following items will be prioritized:

- **Configuration Management** — enabling users to upload and process externally performed security configuration scans, generate compliance reports, and automatically create remediation tasks based on scan results.
- **Risk Assessment** — introducing a structured workflow for identifying, evaluating, and treating risks linked to products, with exposure scoring and mandatory treatment decisions.
- **Security Awareness & Training Evidence** — automating the creation of training tasks for new users and supporting periodic re-certification through links to externally hosted training materials.
- **CRA Compliance Assessment Extension** — expanding the existing assessment questionnaire with a technical documentation checklist for verifying the completeness of required product documentation.
- **Stabilization & Quality** — addressing bugs and usability issues identified during beta testing, incorporating tester feedback, and improving platform reliability and performance ahead of the full release

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

D3.1 Beta Release

www.oscrat.eu https://www.linkedin.com/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.