Ref. Ares(2026)9247119 - 30/09/2026

OSCRAT

Open-Source Cyber Resilience Act Tools

D1.4

OSCRAT – Stakeholder Engagement

Submission date: 29.09.2026

Author: PMF Research & DIH TRAKIA

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.

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Project Number	01190180
Deliverable Number & Name	D1.4 Stakeholder Engagement
Work package	WP 1 – Project Management
Due Date	31.05.2026 (according to grant agreement)
Submission Date	29.09.2026
Lead Partner	PMF Research
Contributing Partners	DIH TRAKIA All partners
Version	1.0
Status	**Final**
Type:	☒ R – Document, Report ☐ DEC – Websites, patent filings, videos, etc. ☐ DEM – Demonstrator, pilot, prototype ☐ Other
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	21/09/2026	PMF Research	First draft
0.2	25/09/2026	DIH Trakia	Review and Contribution
0.3	29/09/2026	Partners	Review and Contribution
1.0	30/09/2026	PMF Research	Finalisation

Abstract

This deliverable presents the stakeholder engagement activities carried out throughout the OSCRAT project to support the development, validation and uptake of the OSCRAT platform and its open-source tools for Cyber Resilience Act (CRA) compliance. It describes the overall stakeholder engagement approach, including the identification of target groups, the collection and analysis of stakeholder needs, and the mechanisms established to foster interaction with SMEs, digital product manufacturers, cybersecurity actors and other relevant stakeholders.

The report documents the engagement activities implemented across the project lifecycle, including surveys, training sessions, workshops, stakeholder consultations, international CRA events and participation in external European initiatives. These activities supported knowledge exchange, increased awareness of CRA requirements, gathered feedback for the refinement of project results, and contributed to the alignment of OSCRAT developments with the needs of its intended users.

The deliverable also provides an overview of stakeholder engagement outcomes and achievements, highlighting the contribution of these activities to building stakeholder capacity, supporting CRA readiness among SMEs, and promoting the adoption of the OSCRAT platform. The communication and dissemination reach of these activities is reported separately in D5.4 – Dissemination Results. Following the completion of the project implementation phase, the content presented in this deliverable may be subject to final refinements and updates during the reporting phase, in order to incorporate any consolidated information, validated results and final achievements related to stakeholder engagement activities.

Keywords

Stakeholder engagement; Cyber Resilience Act; CRA; SMEs; User needs; Workshops; Training; Stakeholder feedback; Digital Europe; OSCRAT

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

Executive Summary 6
1. Introduction 8
1.1 Purpose and Scope of D1.4 8
1.2 Stakeholder Engagement across OSCRAT and the Central Role of WP4 8
1.3 Digital Collaboration Infrastructure Supporting Engagement 9
1.4 Relationship with Other OSCRAT Deliverables 10
1.5 Methodology and evidence 11
2. Stakeholder Engagement Approach 12
2.1 Specific Objectives 12
2.2 Stakeholder groups 14
2.3 Engagement methods 14
2.4 Stakeholder Engagement KPIs 16
3. Stakeholder Needs, Survey and Requirements Alignment 17
4. Training Sessions 18
4.1 Training Session 1 – Setting the context: what the CRA changes and why it matters 20
4.2 Training Session 2 – Scope, accountability and compliance obligations 21
4.3 Training Session 3 – Standards and conformity assessment 22
4.4 Training Session 4 – Implementation roadmaps: from gap analysis to CE readiness 23
4.5 Training series: building CRA knowledge and stakeholder capacity 24
5. Workshops 24
5.1 Workshop 1 – Technical documentation and conformity readiness 26
5.2 Workshop 2 – Incident response planning and management 27
5.3 Workshop 3 – Vulnerability handling 28
5.4 Workshop 4 – Risk management 29
5.5 Workshop series: practical stakeholder interaction and knowledge exchange 30
6. OSCRAT International CRA Event 30
7. OSCRAT Final Event and Platform Launch 32
8. OSCRAT in Action Platform Demo 34
9. Engagement with European Networks and External Events 35
9.1 Synergies with European Networks and Cooperation with Other Projects 35

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.

9.2 OSCRAT Participation in External Events 37
10. Stakeholder Input into Use Cases and Best Practices 50
11. Relationship with Communication and Dissemination 50
11. Summary Stakeholder Engagement KPI Status 51
12. Conclusion 51

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.

Executive Summary

The overarching **purpose of stakeholder engagement** in OSCRAT was to **promote cybersecurity resilience by supporting European SMEs and relevant stakeholder groups in understanding and preparing for the Cyber Resilience Act (CRA),** while gathering feedback and fostering the adoption of the OSCRAT platform and its open-source tools. Engagement was implemented progressively across the project lifecycle: WP2 contributed through stakeholder-needs analysis and requirements gathering; WP4 provided the core stakeholder engagement activities; WP5 supported outreach, dissemination and participation in stakeholder-facing activities; and WP1 ensured coordination and alignment with the overall project objectives.

The **WP2 stakeholder survey** provided an early evidence base on CRA awareness, user needs and expectations. A total of 24 fully completed responses were collected, with more than 70% of respondents considering the compliance areas addressed by OSCRAT important or very important, while 67% expressed willingness to participate actively in the validation of OSCRAT tools. These findings **confirmed the relevance of the planned functionalities and informed subsequent stakeholder engagement activities**, including training sessions, workshops and platform-related activities.

The main **WP4 engagement 'programme'** consisted of **four online training sessions** delivered between September and December 2025, **followed by four thematic workshops** organised between January and April 2026. The training sessions progressively addressed the CRA regulatory context, scope, obligations, standards, conformity assessment and implementation readiness. The workshops then focused on practical compliance-related topics, including technical documentation, incident response planning, vulnerability handling and risk management. Together, these activities provided stakeholders with a structured pathway from CRA awareness raising to practical compliance knowledge and interaction with the OSCRAT approach and platform.

The stakeholder engagement programme was further strengthened through the **OSCRAT Pan-European CRA Event on 11 June 2026** and the **Final OSCRAT Event and Platform Launch on 11 September 2026**. The Final Event brought together project partners, cybersecurity experts, European stakeholders and related CRA initiatives around the completed platform, featuring a live demonstration and Q&A session. More than 160 participants registered for the event, **with 110 participants attending**.

In addition, a **dedicated platform demo event**, "OSCRAT in Action: Platform Demo and UPKIP's Cyber Resilience Assessment Journey", was organised on the final day of the project, on **30 September 2026**. The session provided stakeholders with the opportunity to explore the OSCRAT platform functionalities through a live demonstration and to hear UPKIP's testimonial on their experience with the platform and its role in supporting their Cyber Resilience Act assessment journey.

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.

Engagement also extended beyond OSCRAT-organised activities through **participation in European networks, CRA-related clusters, Digital Innovation Hub activities and external cybersecurity events.** OSCRAT contributed to cooperation frameworks including the CRA Projects Cluster, the European Cluster for Cybersecurity Certification, the Three Seas EDIH Corridor and a regional network in Plovdiv, while also maintaining cooperation with the CONFIRMATE project. These activities strengthened links with SMEs, cybersecurity experts, standardisation actors and other EU-funded initiatives, supporting broader awareness and knowledge exchange around CRA compliance.

The **formal stakeholder-engagement KPIs were overachieved,** demonstrating that the project exceeded the targets established for stakeholder participation, engagement activities and practical CRA support. **The target of at least nine workshops, training sessions and events was exceeded, with 11 relevant activities implemented**.

The minimum target of four CRA compliance use cases and best practices was also surpassed through the **12 representative scenarios developed in Deliverable D4.1.**

In addition, **four dedicated partnerships and collaborations were established,** with a fifth one finalised during the project implementation period.

The **KPI requiring more than 300 participants across workshops, training sessions and the CRA event was surpassed,** contributing to the overall overachievement of stakeholder engagement activities. A total of 307 participants were recorded across four training sessions and four workshops, while the OSCRAT International CRA Event attracted 30 participants and the Platform Launch Event reached 110 participants. Overall, these activities engaged **more than 440 participants.** Attendance figures from the Platform Demo webinar held on 30 September 2026 will be added during the final reporting phase, further contributing to the overall engagement figures.

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

1.1 Purpose and Scope of D1.4

Within **WP1 – Project Management**, Task T1.5 – Stakeholder Engagement is defined as the coordination of stakeholder engagement activities to ensure alignment with project goals and objectives. The task is led by PMF Research and involves all beneficiaries.

While T1.5 establishes the project-level coordination framework for stakeholder engagement, the main stakeholder-engagement activities of OSCRAT were implemented under **WP4 – Stakeholder Engagement**, the work package specifically dedicated to this purpose. WP4 aimed to promote cybersecurity resilience by promoting the CRA among European SMEs through the OSCRAT software and included workshops, training sessions, an international CRA event, and the identification and sharing of CRA compliance use cases and best practices.

D1.4 therefore provides a consolidated account of stakeholder engagement across the project, with **WP4 forming its principal substantive focus**. Activities implemented under other work packages are included where they directly contributed to stakeholder engagement, for example through the identification of user needs under WP2, interaction linked to platform development and testing, or stakeholder outreach and participation supported through WP5.

The deliverable focuses on **direct and meaningful stakeholder interaction**, including the identification of stakeholder needs, participation in training and workshops, knowledge exchange, interaction with cybersecurity experts and project partners, feedback, platform demonstrations, event participation and engagement with relevant European networks and initiatives.

It does not aim to reproduce the complete set of communication and dissemination activities implemented throughout the project. Broader communication reach, visibility and dissemination performance are addressed separately under WP5, in particular through D5.4 – *Dissemination Results*, and will be further consolidated in the final report.

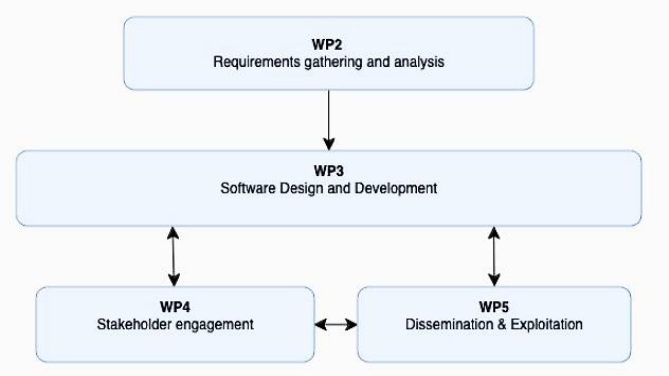
1.2 Stakeholder Engagement across OSCRAT and the Central Role of WP4

Stakeholder engagement developed progressively throughout the OSCRAT project. Different work packages contributed at different stages, but **WP4 provided the main framework for structured and direct engagement with external stakeholders**.

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.

During the earlier stages of the project, WP2 contributed to stakeholder engagement through the identification and analysis of prospective-user needs and expectations. This work provided evidence on CRA awareness, stakeholder requirements and the perceived relevance of the planned OSCRAT functionalities, helping to connect platform development with the needs of its intended users.



The main stakeholder-engagement programme was subsequently implemented under WP4 – Stakeholder Engagement, led by DIH Trakia. The Grant Agreement assigns WP4 a specific role in facilitating knowledge exchange and CRA awareness among European SMEs.

WP5 supported these activities through communication, dissemination and targeted outreach, helping to attract relevant audiences and extend OSCRAT's interaction with SMEs, cybersecurity professionals, Digital Innovation Hubs and the wider European CRA ecosystem. Some external events consequently served both dissemination and stakeholder-engagement purposes. In D1.4, these activities are considered where they involved substantive interaction, knowledge exchange or engagement with relevant stakeholders.

1.3 Digital Collaboration Infrastructure Supporting Engagement

The formal description attached to Deliverable D1.4 also refers to an online open-source Agile collaboration solution for managing meetings, activities, news and notifications. This element relates primarily to the internal collaboration infrastructure established and documented under D1.2 – *Establish Communication Channels*.

The infrastructure nevertheless supported the coordination of stakeholder engagement throughout the project. OpenProject was used as the principal project-management environment, supporting task tracking, scheduling, meeting management, activity monitoring, documentation and follow-up. Nextcloud provided the supporting document-sharing environment, enabling collaborative access, controlled storage and version management.

Together, these tools enabled partners to coordinate stakeholder-facing activities, exchange materials, document decisions and follow up actions arising from workshops, meetings, events and other engagement activities.

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.

Their role is addressed in D1.4 only insofar as they supported stakeholder-engagement coordination. The technical implementation, hosting, permissions, maintenance and detailed use of the collaboration infrastructure are documented in D1.2 and are therefore not repeated here.

1.4 Relationship with Other OSCRAT Deliverables

D1.4 is connected to several other OSCRAT deliverables, but its reporting focus is distinct. The central subject of D1.4 is **stakeholder participation, direct interaction, feedback, knowledge exchange and alignment with project objectives**, with particular emphasis on the engagement activities implemented under WP4.

Deliverable	Primary role	Boundary with D1.4	Deliverable
D1.2 - Establish Communication Channels	Establishes the open-source internal collaboration and information-sharing environment.	D1.4 refers only to how this infrastructure supported engagement coordination; it does not repeat the technical setup.	Establishes the open-source internal collaboration and information-sharing environment.
D1.4 - Stakeholder Engagement	Reports stakeholder identification, participation, interaction, feedback, knowledge exchange and alignment with project objectives.	Central focus is two-way engagement and its contribution to the project.	Reports stakeholder identification, participation, interaction, feedback, knowledge exchange and alignment with project objectives.
D1.5 - Project Updates	Covers transparent responsibilities and project progress updates through project information mechanisms.	D1.4 does not duplicate project-status communication or progress tracking.	Covers transparent responsibilities and project progress updates through project information mechanisms.
D4.1 - OSCRAT Use Cases and Best Practices Final Report	Provides 12 practical CRA assessment scenarios and best-practice guidance.	D1.4 explains how stakeholder-facing activities informed the broader learning context, without reproducing the scenarios.	Provides 12 practical CRA assessment scenarios and best-practice guidance.
D5.4 - Dissemination Results	Reports communication/dissemination outputs, channel performance, visibility,	D1.4 avoids website, social-media, newsletter,	Reports communication/dissemination outputs, channel performance, visibility,

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.

	reach and dissemination KPIs.	press and video analytics and focuses instead on direct interaction and feedback.	reach and dissemination KPIs.

Table 1 - Relationship with other OSCRAT deliverables

The distinction between D1.4 and D5.4 is particularly relevant for workshops, training sessions and events, since these activities can contribute simultaneously to engagement and dissemination. In D1.4, they are reported from the perspective of who participated, how stakeholders interacted with the consortium, what knowledge was exchanged and how the activities contributed to OSCRAT's stakeholder-engagement objectives. Their wider promotional reach and communication performance are reported separately under WP5.

1.5 Methodology and evidence

The report draws primarily on evidence generated through WP4 stakeholder-engagement activities, supplemented by relevant evidence from other work packages where this contributes to understanding the broader engagement process.

For WP4, the principal sources include records of the four training sessions, four workshops, the International CRA Event, the Final OSCRAT Event, use-case and best-practice activities, and relevant stakeholder-facing events and initiatives. These sources provide evidence of participation, interaction, knowledge exchange and, where available, stakeholder feedback.

The WP2 stakeholder survey provides complementary evidence from the earlier phase of the project, particularly in relation to CRA awareness, user needs and expectations, the perceived relevance of OSCRAT functionalities and willingness to participate in validation activities.

The report also draws on relevant meeting records, partner contributions and evidence of substantive OSCRAT participation in external conferences, Digital Innovation Hub activities, cybersecurity events, European project clusters, working groups and related networks. Such activities are included where they involved meaningful stakeholder interaction, project representation or knowledge exchange.

The analysis therefore places the WP4 stakeholder-engagement programme at the centre of D1.4, while using evidence from the wider project to show how stakeholder engagement was prepared, coordinated, supported and extended throughout OSCRAT.

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.

2. Stakeholder Engagement Approach

The overarching purpose of stakeholder engagement in OSCRAT was to support European SMEs and relevant stakeholders in understanding and preparing for the Cyber Resilience Act (CRA) through project activities and the OSCRAT platform.

Following the cross-project approach described in Chapter 1, stakeholder engagement was implemented through a structured framework centred on WP4 activities and supported by contributions from other work packages. The approach combined direct interaction activities, knowledge exchange opportunities and stakeholder-oriented resources to support stakeholders in understanding CRA requirements and exploring how OSCRAT could support their compliance journey.

Across the project, stakeholder engagement focused on:

- understanding stakeholder and prospective-user needs, constraints and expectations in relation to CRA compliance;
- creating opportunities for direct interaction between stakeholders and the consortium through surveys, training sessions, workshops, demonstrations, events and Q&A sessions;
- facilitating knowledge exchange on cybersecurity resilience and CRA compliance;
- raising awareness of CRA obligations and supporting stakeholders in understanding the compliance lifecycle;
- identifying and sharing practical use cases and best practices for CRA compliance; and
- strengthening links with SMEs, cybersecurity experts, Digital Innovation Hubs, research organisations and other actors within the European cybersecurity ecosystem.

2.1 Specific Objectives

The specific objectives of WP4 were to:

- organise webinars and workshops to raise awareness of CRA requirements among SMEs and other interested stakeholders;
- provide training activities introducing stakeholders to the OSCRAT platform, its functionalities and potential benefits;
- collect representative OSCRAT use cases and develop best-practice resources supporting future users; and
- organise an international CRA event bringing together project partners, cybersecurity experts and relevant stakeholders.

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.

These objectives were implemented through the following activities:

- **Workshops, training sessions and CRA events:**

  OSCRAT organised four training sessions and four thematic workshops addressing key aspects of CRA compliance and cybersecurity resilience. These activities provided SMEs and other stakeholders with practical guidance, opportunities to interact with experts, and insights into the functionalities and practical application of the OSCRAT platform. The stakeholder engagement programme was further complemented by the OSCRAT International CRA Event on 11 June 2026, the Final OSCRAT Platform Launch Event on 11 September 2026, and the dedicated Platform Demo event organised on 30 September 2026. The latter provided stakeholders with the opportunity to explore the OSCRAT platform functionalities through a live demonstration and to hear UPKIP's testimonial on its Cyber Resilience Act assessment journey.

- **External events and exchange with relevant peer networks:**

  Beyond the structured training, workshop and event programme, DIH Trakia and other consortium partners supported stakeholder interaction through participation in external events, networking activities and relevant peer networks, including CRA Cluster meetings and EDIH Network Working Groups. While these activities also contributed to the project's communication and dissemination objectives under WP5, they provided opportunities for SMEs, cybersecurity experts, Digital Innovation Hubs and other relevant actors to exchange knowledge, discuss practical cybersecurity and CRA compliance challenges, interact with the consortium and strengthen connections within the wider European cybersecurity ecosystem.

- **CRA compliance use cases and best practices:** OSCRAT developed representative CRA compliance use cases and consolidated practical best practices arising from the project. These resources translate project experience and stakeholder input into practical examples covering different aspects of the CRA compliance process and are intended to support future users in understanding how the OSCRAT approach can be applied in practice.

Together, these activities provided a comprehensive stakeholder engagement framework combining awareness raising, knowledge exchange, practical guidance and opportunities for interaction with the OSCRAT platform, while supporting the project's objective of strengthening SME preparedness for CRA compliance.

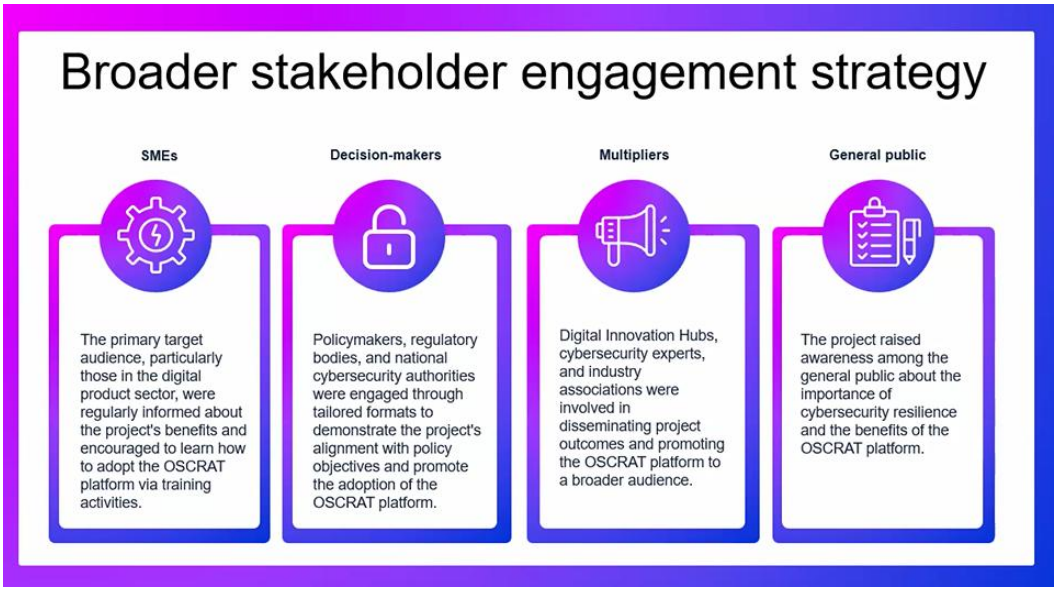
Co-funded by the European Union

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.

2.2 Stakeholder groups

The stakeholder-engagement activities addressed the main target groups identified in the OSCRAT communication and dissemination strategy:

- SMEs in the digital product sector,
- Decision and policy makers,
- Digital Innovation Hubs, Cybersecurity experts, and Industry associations.
- General Public



Particular attention was given to **SMEs developing or providing digital products**, as they represent the primary intended users of the OSCRAT platform and may face significant challenges in understanding and implementing CRA requirements. D5.2 subsequently reinforced this focus, identifying the need for more targeted engagement with SMEs, including companies beyond the countries directly represented in the consortium.

The other stakeholder groups played complementary roles. **Decision and policy makers** were relevant to the wider regulatory and policy context of CRA implementation; **Digital Innovation Hubs** acted as intermediaries capable of transferring knowledge and supporting SMEs; **cybersecurity experts** contributed technical and regulatory expertise; and **industry associations** provided access to broader business communities and sector-specific networks.

2.3 Engagement methods

OSCRAT used a range of complementary engagement mechanisms throughout the project lifecycle. This combination of approaches enabled the consortium to progress from the initial identification of stakeholder needs to more practical

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.

knowledge exchange, to direct interaction with the developed platform and its supporting resources.

A key risk identified in relation to stakeholder engagement was the possibility of limited SME participation in workshops and training sessions, which could reduce the effectiveness of knowledge dissemination and stakeholder-engagement activities.

To mitigate this risk, the consortium applied a targeted audience-outreach approach, focusing engagement and promotional efforts on relevant SME communities and other stakeholder groups through partner networks, Digital Innovation Hubs, sectoral events, European initiatives and direct outreach. This approach was used to broaden participation and ensure that stakeholder-engagement activities reached organisations with a concrete interest in CRA compliance and cybersecurity resilience.

Method	Purpose in the engagement process	Main project context
Stakeholder surveys / questionnaires	Collect structured evidence on CRA awareness, current practices, tool needs and validation interest.	WP2 - User Needs and Stakeholder Alignment
Consultations and partner review meetings	Interpret stakeholder evidence, validate decisions and refine requirements.	WP2 and cross-WP coordination
Training sessions	Build CRA understanding while presenting expected OSCRAT workflows and gathering early reactions.	WP4
Thematic workshops	Facilitate practical interaction and knowledge exchange on concrete CRA implementation topics.	WP4
International CRA Event (11 June 2026)	Bring together SMEs, cybersecurity experts, partners and ecosystem actors around CRA compliance and OSCRAT.	WP4
Final OSCRAT Event (11 September 2026)	Engage external stakeholders around the final platform through presentation, live demonstration and Q&A.	WP4 - Final project phase
Participation in external events	Create direct contact with relevant stakeholder communities where OSCRAT was actively represented.	Partner-level engagement; evidence to be consolidated
Participation in networks/working groups	Exchange with relevant peer networks, such as the CRA Cluster meetings, EDIH Network Working groups,etc.	WP4
Digital collaboration environment	Coordinate partner responsibilities, meetings, evidence, documentation and follow-up connected to engagement.	WP1 / D1.2

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.

2.4 Stakeholder Engagement KPIs

The stakeholder-engagement activities were monitored against a set of quantitative KPIs defined for the project. These indicators were intended to assess whether OSCRAT generated sufficient opportunities for interaction with European SMEs and other relevant stakeholders, translated project experience into practical CRA guidance, and fostered cooperation with external organisations.

The main stakeholder-engagement KPIs were as follows:

- **KPI: At least 9 workshops, training sessions and events facilitating interaction and CRA compliance among European SMEs.**

  This target was exceeded through the **implementation of 11 relevant stakeholder engagement activities**, including 4 training sessions, 4 workshops, the OSCRAT International CRA Event on 11 June 2026, the Final OSCRAT Event and Platform Launch on 11 September 2026, and the Platform Demo webinar held on 30 September 2026.

- **KPI: More than 300 participants across workshops, training sessions and the CRA event.**

  This target was surpassed, contributing to the overall overachievement of stakeholder engagement activities. A total of 307 participants were recorded across four training sessions and four workshops, while the OSCRAT International CRA Event attracted 30 participants and the Final OSCRAT Event and Platform Launch reached 110 participants. Overall, these activities engaged **more than 440 participants**. Attendance figures from the Platform Demo webinar held on 30 September 2026 will be added during the final reporting phase, further contributing to the overall engagement figures

- **KPI: At least 4 CRA compliance use cases and best practices.**

  This target was exceeded. D4.1 – OSCRAT Use Cases and Best Practices Final Report presents 12 representative CRA assessment scenarios, covering different aspects of the compliance process and providing practical guidance for future users.

- **KPI: 5 industry partnerships and collaborations fostered by the project, enhancing its reach and impact.**

  At the time of reporting, four dedicated collaborations had been established, with one additional collaboration in the process of being finalised. The established collaborations include: 1. CRA Projects Cluster; 2. European Cluster for Cybersecurity Certification; 3. Three Seas EDIH Corridor; 4. Regional network organisation in Plovdiv, Bulgaria – Chamber of Commerce. In addition, the EDIH Network has been actively used to promote and disseminate the OSCRAT platform, with DIH Trakia contributing through its involvement in Cyber4AllSTAR/Cyber4All 2.0,

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.

while the project also maintained sustained cooperation with the CONFIRMATE project.

Taken together, these indicators demonstrate that the stakeholder-engagement programme not only achieved the planned targets but also extended beyond the minimum objectives defined for stakeholder participation, knowledge exchange and ecosystem-building.

3. Stakeholder Needs, Survey and Requirements Alignment

Stakeholder engagement under *WP2 - Requirements gathering and analysis* played an important role in ensuring that the OSCRAT platform was aligned with the practical needs, expectations and level of preparedness of its intended users. The consultation activities involved in particular SMEs and software-oriented companies, open-source stewards, prospective OSCRAT users, cybersecurity professionals and other technical stakeholders relevant to CRA implementation.

Through the stakeholder survey, the consortium collected information on organisations' familiarity with the Cyber Resilience Act (CRA), their perceived needs in the main compliance areas addressed by OSCRAT, and their expectations regarding supporting tools. The survey was fully completed by 24 organisations. Approximately 79% of the complete respondents were software-related.

The survey results confirmed the relevance of the core functionalities planned for the platform. More than 70% of respondents considered the issues addressed by OSCRAT and the related CRA compliance tools important or very important.

The perceived relevance of the individual tools was as follows:

Tool	Respondents' Assessment
Checklist Automation / CRA self-assessment checklist	78%
Software Bill of Materials preparation and analysis	78%
Vulnerability management	95%
Incident management	95%
Documentation / central repository	82%

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.

Vulnerability and incident management received the highest level of interest, with 95% of respondents recognising the relevance of supporting tools in these areas. Checklist automation, SBOM support and centralised documentation were also considered important by a clear majority of respondents. These results provided useful confirmation that the principal functional areas selected for OSCRAT corresponded to concrete stakeholder needs.

An additional result of particular relevance to stakeholder engagement was that 67% of respondents expressed willingness to actively participate in the validation of the tools developed within the OSCRAT platform. This indicated that a significant proportion of the stakeholders consulted were not only interested in CRA compliance support but were also open to further involvement in the project and its validation activities.

At the same time, depending on the specific issue, between approximately 5% and 33% of respondents considered some of the proposed areas less relevant or expressed limited interest in related compliance tools. This variation highlighted differences in CRA awareness and preparedness across the target groups and reinforced the need for the workshops and training activities that were planned and undertaken in WP4. Stakeholder engagement was therefore relevant not only for gathering requirements, but also for improving understanding of the CRA and of the practical implications of compliance for SMEs.

These findings contributed to stakeholder alignment by confirming the relevance of the main OSCRAT functional areas and providing qualitative insight into how the tools should respond to prospective users' needs. The survey process therefore created a continuous feedback mechanism between stakeholder needs and the refinement of project requirements.

Overall, stakeholder engagement under WP2 provided structured evidence that helped align OSCRAT with the practical needs of SMEs, software providers, open-source actors and other prospective users, while also informing subsequent platform development and stakeholder-facing activities.

4. Training Sessions

Training sessions constituted one of the core stakeholder-engagement activities foreseen under WP4. *Task T4.2 – Training sessions* focused on the organisation of online training activities "*to facilitate interaction and knowledge sharing among European SMEs regarding CRA compliance*". The wider objectives of WP4 also foresaw training sessions involving project partners and companies interested in OSCRAT, supporting them in understanding the benefits and functionalities of the platform during its development.

The trainings were thus a mechanism for direct engagement and capacity building. It provided SMEs and other interested stakeholders with a structured introduction to the Cyber Resilience Act (CRA), while creating opportunities to

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.

interact with experts, raise questions and progressively develop the knowledge needed to understand both CRA compliance obligations and the practical support offered by OSCRAT. They contributed directly to the broader WP4 objective of promoting cybersecurity resilience and CRA awareness among European SMEs.

Between September and December 2025, OSCRAT organised four online training sessions, each lasting for two hours. The sessions followed a progressive learning pathway: beginning with the regulatory context and overall structure of the CRA, then moving to scope and responsibilities, standards and conformity assessment, and finally practical implementation and readiness. The OSCRAT Resources section provides the recordings and supporting materials from all four sessions.

Training session	Date	Main focus	Contribution to stakeholder engagement
Training Session 1	08/09/2025	**Setting the context: what the CRA changes and why it matters**	Established a common understanding of the CRA and its relevance for organisations developing or providing products with digital elements.
Training Session 2	13/10/2025	**Scope, accountability and compliance obligations**	Helped stakeholders examine whether products fall within CRA scope and understand responsibilities across the supply chain.
Training Session 3	10/11/2025	**Standards and conformity assessment**	Connected legal compliance requirements with standards, technical evidence and conformity-assessment processes.
Training Session 4	08/12/2025	**Implementation roadmaps: from gap analysis to CE readiness**	Translated the regulatory framework into a practical pathway towards organisational and product-level CRA readiness.

Table: Overview of OSCRAT Training Sessions

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.

4.1 Training Session 1 – Setting the context: what the CRA changes and why it matters



The first training session, held on **8 September 2025**, established the common regulatory foundation for the subsequent stakeholder-engagement activities. Rather than approaching the CRA solely as another cybersecurity guideline, the session explained its role as a binding horizontal regulatory framework introducing cybersecurity requirements for products with digital elements.

The session introduced participants to the structure of the CRA and the role of its annexes, as well as the broader enforcement and conformity-assessment framework. It also positioned the CRA within the wider EU cybersecurity and resilience landscape, helping participants understand how product-level cybersecurity requirements relate to other European regulatory initiatives.

From a stakeholder-engagement perspective, this introductory session was particularly important because the earlier stakeholder survey had demonstrated significant differences in CRA awareness among prospective users. The training therefore helped establish a shared baseline of knowledge before participants were asked to engage with more specialised issues in later sessions and workshops.

The session was aimed especially at **European SMEs, software-oriented organisations and other stakeholders interested in understanding how the CRA could affect their products and compliance responsibilities**. Through the online format, stakeholders could access specialist knowledge while beginning to relate the regulatory framework to their own organisational context.

Participation in training session 1: 35 stakeholders.

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.

4.2 Training Session 2 – Scope, accountability and compliance obligations



The second training session, held on **13 October 2025**, moved from the general regulatory context to questions that are particularly relevant for companies preparing for CRA compliance: whether a product falls within the scope of the Regulation, which products are affected, and how responsibilities are allocated among the different economic actors involved.

The session examined the application of the CRA to **products with digital elements**, including software, hardware and relevant remote data-processing components necessary for a product to function. It also addressed the roles and obligations of economic operators and the consequences associated with non-compliance.

This topic was particularly relevant to stakeholder engagement because determining CRA applicability is one of the first practical challenges faced by SMEs. For organisations with limited regulatory or cybersecurity resources, uncertainty about whether a product is covered and which obligations apply can make it difficult to define an appropriate compliance pathway.

The session therefore supported participants in moving from general awareness towards an understanding of their own potential responsibilities. It also provided an important conceptual basis for the later OSCRAT workflows concerning CRA applicability and compliance assessment.

The materials published through the OSCRAT Resources section covered products, economic operators, obligations and sanctions, together with complementary material concerning the relationship between the CRA and cloud services.

Participation in training session 2: 36 stakeholders

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.

4.3 Training Session 3 – Standards and conformity assessment



The third training session, held on **10 November 2025**, addressed the relationship between regulatory compliance, technical standards and conformity assessment. The session emphasised that CRA compliance requires organisations not only to implement appropriate cybersecurity measures but also to be able to demonstrate, through structured and traceable evidence, that the relevant requirements have been addressed.

The training therefore examined the role of standards in translating regulatory obligations into more concrete organisational and technical practices. Topics included the relevance of management-system approaches such as ISO 27001, the roles of laboratories and certification bodies, and the relationship between horizontal and sector-specific standards. The session also discussed the emerging European standardisation landscape supporting implementation of the CRA.

For participating stakeholders, this represented an important progression from understanding what the CRA requires towards considering how compliance can be demonstrated. This distinction is particularly relevant for SMEs, which may have cybersecurity practices in place but lack the structured documentation, traceability or conformity-assessment knowledge required to demonstrate compliance.

The training therefore contributed to the WP4 objective of knowledge exchange by connecting legal requirements with the practical evidence and organisational processes that companies need to develop. It also provided a foundation for subsequent workshop activities addressing technical documentation and conformity readiness in greater depth.

Participation in training session 3: 35 stakeholders

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.

4.4 Training Session 4 – Implementation roadmaps: from gap analysis to CE readiness



The fourth training session, held on **8 December 2025**, concluded the 2025 training arc by bringing the previous topics together within a practical implementation pathway. Whereas the earlier sessions focused on understanding the CRA, its scope and the mechanisms through which compliance is demonstrated, the final training examined how organisations can begin preparing systematically for implementation.

The session highlighted the importance of the CRA annexes as practical elements of the compliance framework, including their relevance to technical documentation, declarations of conformity and conformity-assessment procedures. It also introduced the use of a CRA gap analysis as a practical starting point for identifying the difference between an organisation's existing practices and the requirements that will need to be addressed.

Participants were also introduced to the different conformity-assessment pathways that may apply depending on the product and its risk classification. The session explained that certain higher-risk products may require third-party assessment, while other products may follow self-assessment pathways subject to the applicable regulatory conditions and standards.

From the perspective of stakeholder engagement, this final session was particularly relevant because it moved beyond awareness towards practical readiness. It helped participants understand CRA compliance as a sequence of interconnected activities rather than as a single certification exercise. This also prepared the ground for the subsequent workshop phase, in which stakeholders engaged with specific implementation topics such as technical documentation, incident response, vulnerability handling and risk management.

Participation in training session 4: 33 stakeholders

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.

4.5 Training series: building CRA knowledge and stakeholder capacity

The four training sessions facilitated interaction and knowledge sharing on CRA compliance. The sequence progressively moved participants from general regulatory understanding to scope and responsibilities, conformity assessment and practical implementation.

The programme also responded to needs identified through the earlier WP2 stakeholder survey, which showed varying levels of CRA awareness among prospective users. The training sessions therefore provided a bridge between the stakeholder-needs analysis under WP2 and the more practical workshops subsequently implemented under WP4.

In total, 139 stakeholders participated in the training sessions.

The recordings and training materials remain available through the OSCRAT Resources section: https://oscrat.eu/resources/#training-sessions

5. Workshops

Following the training sessions implemented between September and December 2025, WP4 continued its stakeholder-engagement activities *(ref. Task 4.1 Workshops and International CRA Event)* through **a series of four thematic online workshops held between January and April 2026**. Building on the regulatory and compliance foundations established during the training programme, the workshops shifted the focus towards more specific implementation challenges and practical application.

The workshops were designed as interactive stakeholder-facing activities, particularly for SMEs and other organisations working with products with digital elements, as well as cybersecurity and technical professionals. Their purpose was to deepen knowledge exchange and provide practical guidance on key CRA compliance areas. In line with the content presented on the OSCRAT website, the workshops addressed regulatory, technical and documentation-related requirements while linking these topics to the functionalities and workflows supported by the OSCRAT platform.

Workshop	Date	Topic	Stakeholders / interaction	Main engagement outcome
Workshop 1	28/01/2026	**Technical documentation and conformity readiness**	SMEs, prospective OSCRAT users and other stakeholders working with digital products. The session also included practical presentation of the	Supported participants in relating CRA applicability and conformity requirements to concrete product information and documentation needs.

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 platform and its applicability survey.	
Workshop 2	23/02/2026	**Incident response planning and management**	SMEs and cybersecurity/technical stakeholders. Expert contributions addressed regulatory and operational aspects of incident management.	Provided practical insight into incident-response processes, automation and orchestration, threat intelligence and the relationship between structured incident handling and CRA reporting requirements.
Workshop 3	30/03/2026	**Vulnerability handling**	SMEs, cybersecurity practitioners and prospective platform users.	Explored practical vulnerability-management processes and supporting approaches, including vulnerability intelligence and VEX in the context of CRA compliance.
Workshop 4	27/04/2026	**Risk management**	SMEs, cybersecurity professionals and other stakeholders concerned with CRA implementation.	Addressed identification and assessment of cybersecurity risks, treatment options, risk registers, traceability and the relationship between risks, vulnerabilities, controls and compliance evidence.

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.

5.1 Workshop 1 – Technical documentation and conformity readiness



The first OSCRAT workshop focused on **technical documentation and conformity readiness** and combined an update on the evolving EU cybersecurity regulatory framework with a practical demonstration of the OSCRAT platform. The regulatory part covered recent CRA-related developments, product classification and conformity-assessment considerations, while also linking the CRA with the broader EU cybersecurity framework.

The practical part demonstrated how these requirements are translated into the OSCRAT platform. Participants were shown how to define their organisational role, create a product and complete the CRA applicability assessment through a structured questionnaire covering issues such as market placement, digital elements, connectivity and relevant product categories.

Overall, the workshop helped participants move from understanding which CRA requirements may apply to their products towards seeing how these assessments can be structured and documented through the OSCRAT platform.

Participation in workshop 1: 39 stakeholders

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.

5.2 Workshop 2 – Incident response planning and management



The second OSCRAT workshop focused on **incident response planning and management**, examining how organisations can move from reactive handling of cybersecurity incidents towards more structured, traceable and resilient processes. The session connected CRA requirements with practical activities such as identifying security gaps, reviewing system architecture, managing vulnerabilities, maintaining an SBOM, assessing risks and documenting supporting evidence.

A further focus was placed on **automation and orchestration of incident response**. Participants were introduced to challenges such as high alert volumes, disconnected tools and manual investigations, and to approaches involving SOAR, threat intelligence, vulnerability information and structured incident-response workflows. The workshop also highlighted how these processes support regulatory reporting and compliance under frameworks including the CRA.

Overall, the workshop helped participants understand incident management as an integrated process combining detection, response, documentation, vulnerability information and regulatory obligations, while illustrating the importance of structured workflows for improving both operational resilience and CRA readiness.

Participation in workshop 2: 47 stakeholders

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.

5.3 Workshop 3 – Vulnerability handling



The third OSCRAT workshop focused on **vulnerability handling**, with particular attention to how organisations can identify, assess, prioritise and manage vulnerabilities in the context of CRA compliance. The session linked vulnerability management with broader product-security processes and with the need to maintain structured evidence throughout the product lifecycle.

Particular attention was given to risk intelligence and VEX (Vulnerability Exploitability eXchange), helping participants understand how vulnerability information can be evaluated in relation to a specific product, documented appropriately and used to support remediation and compliance decisions.

Overall, the workshop helped participants understand vulnerability management as a continuous CRA-related process involving monitoring, assessment, prioritisation, remediation and documentation, while illustrating how OSCRAT can support organisations in managing these activities in a more structured and traceable way.

Participation in workshop 3: 46 stakeholders

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.

5.4 Workshop 4 – Risk management



The fourth and final workshop focused on risk management, **risk management under the CRA**, explaining why cybersecurity risk assessment is a mandatory and continuous process throughout the product lifecycle. The session covered product-specific risk assessment, including intended use, operational context, likelihood and impact, as well as the need to document and update risk decisions over time.

Particular attention was given to the link between risks, vulnerabilities, SBOMs, treatment decisions and compliance evidence. Participants were introduced to the main risk-treatment options — accept, reduce, avoid and transfer — and to the importance of maintaining a clear and traceable chain from identified risk to implemented control and supporting evidence.

The workshop also demonstrated how OSCRAT supports this process through product-level risk records, structured risk assessment, treatment workflows and links between risks, tasks and evidence. Overall, the session showed how risk management can be integrated into an auditable CRA compliance workflow rather than treated as a one-off exercise.

Participation in workshop 4: 36 stakeholders

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.

5.5 Workshop series: practical stakeholder interaction and knowledge exchange

Taken together, the four workshops deepened the stakeholder-engagement process initiated through the training sessions by moving from general CRA awareness towards more practical implementation challenges. The sessions focused on technical documentation and conformity readiness, incident response, vulnerability handling and risk management, providing participants with opportunities to relate CRA requirements to concrete organisational and technical processes.

The workshops also supported direct knowledge exchange between the consortium and stakeholders, particularly SMEs, software-oriented organisations and cybersecurity professionals. By addressing practical compliance questions and demonstrating how OSCRAT can support structured workflows, the series helped connect regulatory requirements with the operational needs of prospective users.

Total number of participants in the workshops: 168

The recordings and training materials remain available through the OSCRAT Resources section: https://oscrat.eu/resources/#workshops

6. OSCRAT International CRA Event



The *OSCRAT pan-EU Event*: *Best Practices for CRA Compliance via Open-Source Tools* was organised on 11 June 2026 by the European Digital Innovation Hub Trakia in hybrid format at the Technical University of Sofia and online, alongside Spinoff Europa 2026. Building on the preceding eight OSCRAT

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.

training sessions and workshops, the event brought together SMEs, cybersecurity experts, project partners and other stakeholders to consolidate key lessons on CRA implementation and practical compliance.

The programme focused on helping organisations understand how to prepare smart and connected products, software and digital solutions for the requirements of Regulation (EU) 2024/2847. It also demonstrated how the OSCRAT platform can support SMEs through guided assessments, SBOM-related functionality, vulnerability handling, incident management and compliance documentation. The main session was led by Yasen Tanev, Lead Cybersecurity Auditor and Ecosystem Manager at Trakia Digital Innovation Hub.

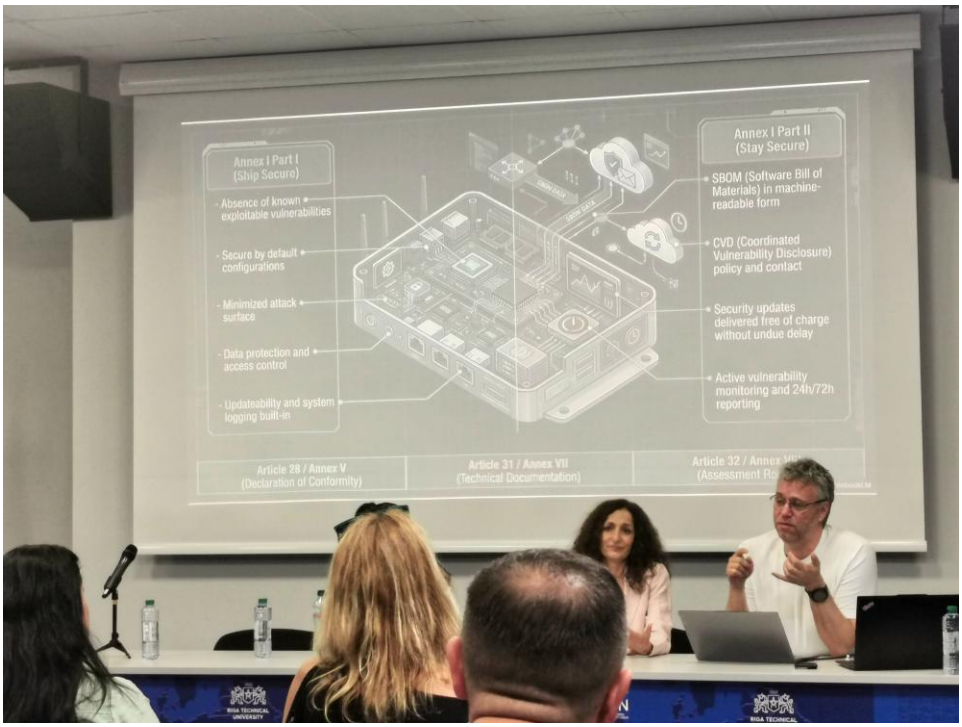
Beyond the technical content, the event created an opportunity for participants to exchange views with OSCRAT consortium partners, discuss practical compliance challenges and connect the lessons from previous project activities with real SME needs.

Total number of participants: 30



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.



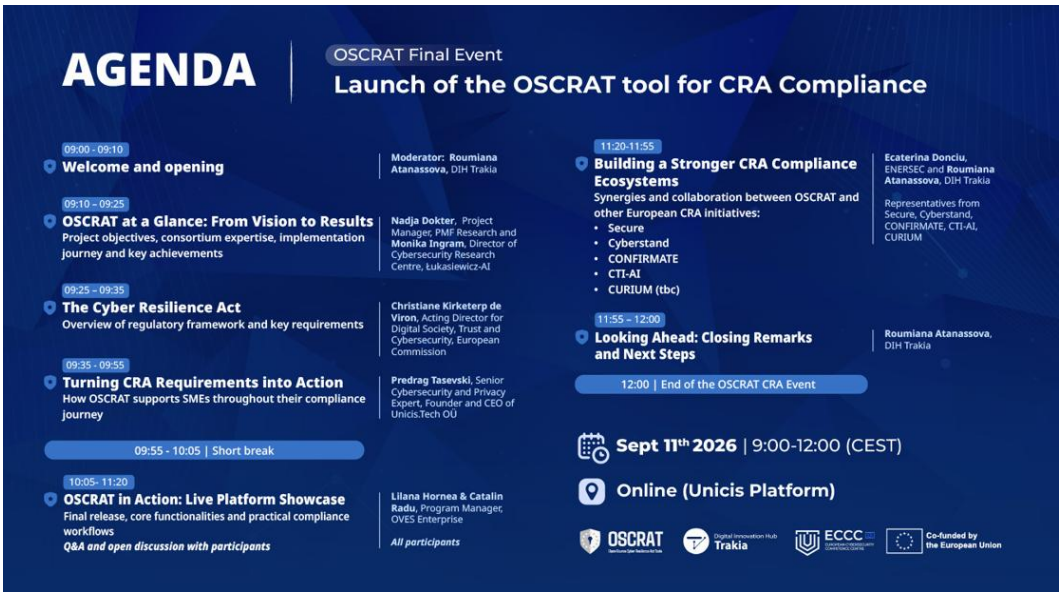
7. OSCRAT Final Event and Platform Launch



The international **OSCRAT Final Event** was held online on **11 September 2026**, marking the **official launch of the final OSCRAT platform**. The event was deliberately organised on the date on which the first CRA reporting obligations entered into application, providing a timely opportunity to present the project's final results and discuss their relevance for European SMEs and manufacturers of products with digital elements.

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.



The event brought together cybersecurity experts, European stakeholders, digital innovation actors and organisations preparing for CRA implementation. In total **over 110 stakeholders participated in the platform launch.** The **programme opened** with *Nadja Dokter, Project Manager at PMF Research,* and *Monika Ingram, Director of the Cybersecurity Research Centre at Łukasiewicz-AI,* who presented the **OSCRAT journey, project objectives and main achievements.** *Roumiana Atanassova, Digital Innovation Hub Trakia*, moderated the event.

The **regulatory perspective** was provided by *Christiane Kirketerp de Viron, Acting Director for Digital Society, Trust and Cybersecurity at the European Commission*, while *Predrag Tasevski, Senior Cybersecurity and Privacy Expert and Founder and CEO of Unicis.Tech OÜ,* presented how CRA requirements can be translated into practical compliance actions with the support of OSCRAT.

A central part of the event was the **OSCRAT in Action: Live Platform Showcase**, presented by *Lilana Hornea and Catalin Radu from OVES Enterprise*, who demonstrated the final platform and its practical compliance workflows. The platform demonstration was later continued by Catalin Radu and included interaction and Q&A with participants.

The programme also included a dedicated presentation on **OSCRAT stakeholder engagement** by *Hristian Daskalov, Digital Innovation Hub Trakia,* followed by a session on cooperation with other European CRA initiatives. Contributions were provided by *Luigi Colucci, Cyberstand.eu and Project Manager at Trust-IT Services*, and *Łukasz Wawrowski, Łukasiewicz-AI, representing CTI-AI,* before the concluding Q&A.

The Final Event therefore represented both the culmination of the project's development activities and an important stakeholder-engagement milestone, enabling participants to interact directly with project partners, technical experts

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.

and related European initiatives while seeing the completed OSCRAT platform applied to practical CRA compliance workflows.

The recording is available on OSCRAT's Youtube channel.

The event attracted significant stakeholder interest, with **over 160 registered participants** and more than **110 attendees joining the session.**

8. OSCRAT in Action Platform Demo



The event was organised following the strong interest expressed by participants during the Platform Launch Event, where stakeholders requested further guidance and a more detailed demonstration of the OSCRAT platform functionalities. The session provided a practical walkthrough of the platform through the example of the digital product UPKIP, showcasing how OSCRAT can support organisations throughout their Cyber Resilience Act (CRA) assessment journey.

During the event, UPKIP shared its experience with the platform and presented its assessment journey, providing stakeholders with a practical example of the application of OSCRAT in a real-world context. It was also highlighted that UPKIP is not only assessed and registered within the OSCRAT platform, but that the OSCRAT platform will be integrated into the UPKIP platform, demonstrating the potential for further adoption and integration of OSCRAT-based functionalities by digital product providers.

Total number of participants: to be added during the final reporting phase.

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.

9. Engagement with European Networks and External Events

Stakeholder engagement extended beyond activities organised directly by OSCRAT. Consortium partners participated in European cybersecurity networks, CRA-related initiatives, sectoral events and external conferences, creating additional opportunities to engage SMEs, cybersecurity professionals, Digital Innovation Hubs and other relevant stakeholders. These activities supported knowledge exchange on CRA implementation, increased interaction with prospective users of OSCRAT and facilitated cooperation with other European initiatives developing complementary tools, guidance and standards.

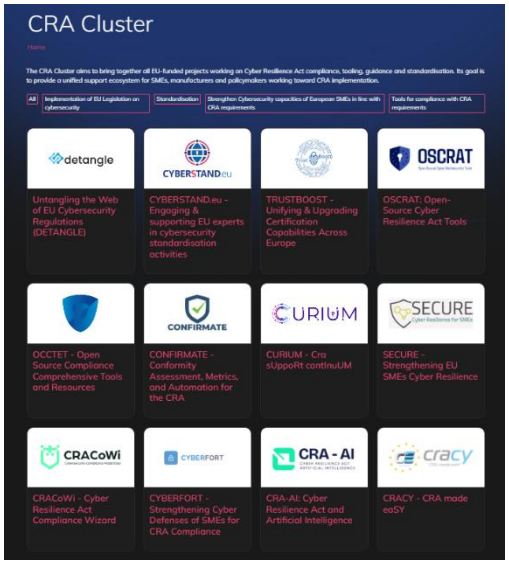
9.1 Synergies with European Networks and Cooperation with Other Projects

Cooperation with European and regional networks represented an important component of OSCRAT's stakeholder-engagement approach. These networks provided structured opportunities to exchange knowledge and tools, connect with complementary initiatives and extend engagement beyond activities organised directly by the consortium.

This activity was also linked to a specific project KPI: **"5 industry partnerships and collaborations fostered by the project, enhancing its reach and impact."** At the time of reporting, **four dedicated collaborations had been formalised, while one additional collaboration was in the process of being finalised**, bringing the project close to full achievement of this target.

1. CRA Projects Cluster – CYBERSTAND.eu

OSCRAT is a member of the CRA Projects Cluster, coordinated through CYBERSTAND.eu, which brings together EU-funded initiatives working on CRA compliance, tooling, guidance and standardisation. The cluster supports coordination and knowledge exchange between projects and contributes to a more coherent support ecosystem for SMEs, manufacturers, policymakers and other stakeholders preparing for CRA implementation. OSCRAT participated in CRA Cluster meetings and related networking and joint activities.



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.

2. European Cluster for Cybersecurity Certification



OSCRAT also joined the European Cluster for Cybersecurity Certification, together with sister projects DOSS, EMERALD, COBALD and TELEMETRY. Participation in the cluster provided opportunities to exchange knowledge on cybersecurity certification, standardisation and related European developments and to connect OSCRAT with projects addressing complementary aspects of cyber resilience.



3. Three Seas EDIH Corridor

OSCRAT is member of Three Seas EDIH Corridor, a cooperation framework connecting Digital Innovation Hubs across Europe and the Mediterranean. Participating hubs share tools, expertise and services with one another, enabling solutions developed within individual initiatives to reach wider stakeholder communities.





OSCRAT contributed the OSCRAT platform and related CRA-support resources to this cooperation framework, and the relevant collaboration charter was signed.

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.

4. **Regional Network: Plovdiv Chamber of Commerce**

   OSCRAT participated in the regional Plovdiv network, providing an additional channel for exchanging knowledge, tools and information with organisations active within the regional European ecosystem.

5. **EDIH Network and Cyber4AllSTAR/Cyber4All 2.0**

   The EDIH Network has been actively used as a channel to promote and disseminate the OSCRAT platform among relevant stakeholders. Through DIH Trakia's involvement as a partner in **Cyber4AllSTAR/Cyber4All 2.0**, OSCRAT results have been shared within the wider Digital Innovation Hub ecosystem, supporting further outreach and knowledge exchange. In addition, the project maintained sustained cooperation with the **CONFIRMATE project**.

Cooperation with the CONFIRMATE Project

Cooperation with **CONFIRMATE** was particularly sustained and illustrates the project's approach to building synergies with complementary EU-funded initiatives. During 2025, OSCRAT and CONFIRMATE implemented **three joint activities**, followed by further interaction during the CRA conference in Bucharest.

This cooperation enabled the two projects to exchange experience on CRA implementation, jointly engage relevant stakeholder communities and explore complementarities between their respective approaches and resources. It also contributed to the broader objective of avoiding isolated project activities and instead connecting OSCRAT with other European initiatives working towards practical CRA implementation.

9.2 OSCRAT Participation in External Events

Alongside participation in formal networks and cooperation frameworks, OSCRAT partners represented the project at external conferences, sectoral events, workshops and networking activities. These engagements provided opportunities to present the project and the emerging and then final OSCRAT platform, interact with prospective users and exchange practical knowledge on CRA implementation with SMEs, cybersecurity professionals, Digital Innovation Hubs, industry representatives and other European initiatives.

Stakeholder Engagement through the European Digital Innovation Hub (EDIH) Days:

A particularly relevant engagement channel was the **European Digital Innovation Hub (EDIH) Days format** implemented by EDIH Trakia. These

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.

recurring events were used to introduce OSCRAT and CRA-related topics to SME communities from different economic sectors.

Throughout the project, **more than 12 EDIH Days sessions** included dedicated content related to OSCRAT and the Cyber Resilience Act. Sessions typically lasted between **30 and 90 minutes** and involved approximately **50–100 participants**, depending on the event. Audiences were predominantly Bulgarian SMEs and ecosystem actors, although several sessions were delivered in English or bilingually and included speakers and participants from other countries.



The format enabled OSCRAT to engage different SME audiences on a recurring basis rather than relying on a single stakeholder community. Depending on the specific event, sessions introduced CRA requirements, cybersecurity-resilience topics, the OSCRAT approach and available project tools and resources, while also allowing participants to interact with experts and project representatives.

The main EDIH Days and other external events involving substantive OSCRAT stakeholder engagement are presented below in chronological order.

30–31 January 2025 – European Digital Innovation Days: Insurance Sector, Sofia Tech Park

The first sector-oriented EDIH Days brought together insurance-sector stakeholders, cybersecurity specialists and businesses interested in digital transformation and cyber resilience. Within EDIH Trakia's broader outreach activities, OSCRAT was promoted as one of the European initiatives supporting



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.

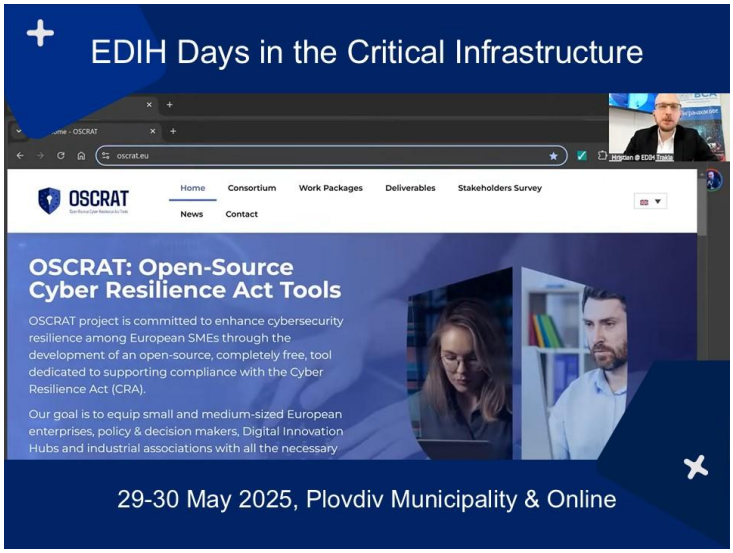
organisations in preparing for emerging cybersecurity and regulatory requirements. The event also provided access to a broader community of SMEs and professionals interested in practical cybersecurity solutions.

20–21 March 2025 – European Digital Innovation Days in Industrial Cybersecurity, Sofia Tech Park



The industrial edition of the EDIH Days targeted companies operating in Industry 4.0 environments, including IoT, robotics, automation and other digitally connected industrial systems. OSCRAT was presented in the context of EU-funded tools and support available to businesses seeking to strengthen cybersecurity and regulatory readiness. The event combined expert presentations, interactive discussions and networking, creating opportunities to engage industrial companies facing practical cybersecurity and CRA-related challenges.

29–30 May 2025 – European Digital Innovation Days in Critical Infrastructure, Plovdiv



Organised by the Municipality of Plovdiv and EDIH Trakia, the two-day event addressed cybersecurity risks affecting industrial enterprises and critical infrastructure. **Hristian Daskalov** presented OSCRAT and its planned support for companies seeking to prepare for the Cyber Resilience Act, including the open-source compliance tools, training sessions and workshops being developed through the project. The event enabled direct

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.

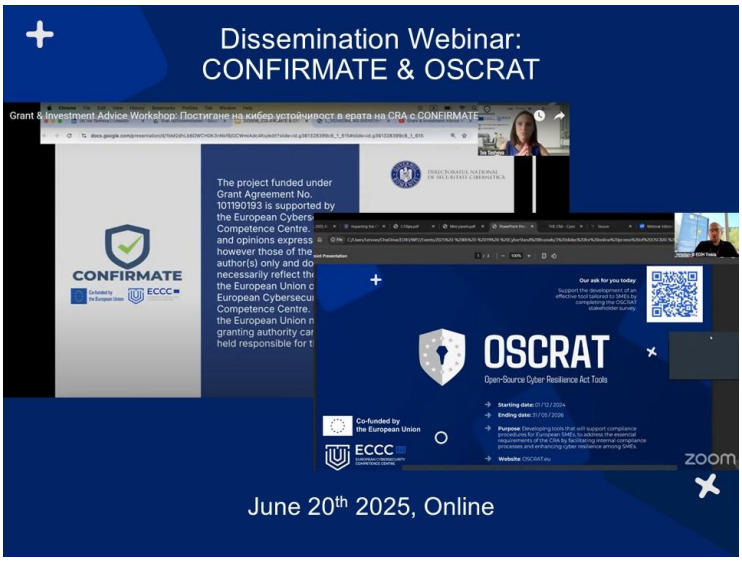
exchange with industrial and critical-infrastructure stakeholders on cyber risks, regulatory requirements and available European support.

19–20 June 2025 – European Digital Innovation Days / Spinoff Europa 2025, GATE Institute, Sofia



OSCRAT was represented during the European Digital Innovation Days organised alongside **Spinoff Europa 2025**, which brought together more than 200 participants from research, industry, start-ups, investment and innovation ecosystems. During a session on EU and venture-capital funding opportunities, *Roumiana Atanassova* presented the support available through OSCRAT alongside other European cybersecurity initiatives. The event created opportunities to engage entrepreneurs, innovators and SMEs and to position OSCRAT within the wider European innovation ecosystem.

20 June 2025 – First joint OSCRAT–CONFIRMATE dissemination event



The Spinoff Europa programme also provided the setting for the **first of three joint engagement activities between OSCRAT and CONFIRMATE**. The dedicated session connected cybersecurity, innovation and funding perspectives and promoted cooperation between the two Digital Europe projects. Discussions focused on the need for coordinated innovation and practical tools capable of helping

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.

European companies respond to CRA requirements. This marked the beginning of a sustained collaboration between the two projects during 2025.

25 September 2025 – Second joint OSCRAT–CONFIRMATE event, International Technical Fair, Plovdiv



A second joint OSCRAT–CONFIRMATE activity was organised in connection with the **International Technical Fair in Plovdiv**, one of Bulgaria's major industrial and technology events. The setting provided access to manufacturers, technology companies and other industrial stakeholders and supported further exchange on CRA compliance and practical cybersecurity solutions. The activity strengthened cooperation between the two projects while extending their outreach to an industry-oriented audience. The International Technical Fair itself ran from **24 to 27 September 2025**.

8 October 2025 – CRA – Making the EU Market Resilient, Bucharest



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 participated in the first edition of ***"CRA – Making the EU Market Resilient"***, held in Bucharest and organised with the involvement of **ENISA, the European Cybersecurity Competence Centre (ECCC) and the Romanian National Cyber Security Directorate**. *Giuseppe Ursino, CEO & Founder of PMF Research,* represented OSCRAT during the panel "***Empowering Business and Innovation in the CRA Era***", alongside representatives of other European initiatives including CONFIRMATE, CRACY, SECURE and CYBERFORT.



The discussion focused on how EU policy and funding can be better connected with the practical needs of SMEs, highlighting the importance of supporting concrete solutions, improving the visibility of available resources and facilitating SME access to EU initiatives. Participants also discussed how EU funding can help companies adopt emerging technologies such as AI while remaining compliant, and how the CRA can be approached not only as a regulatory obligation but also as a driver for innovation and stronger cyber resilience.



The event provided a valuable opportunity for OSCRAT to exchange perspectives with EU institutions, cybersecurity experts and other Digital Europe projects working on CRA implementation. In addition to the panel discussion, OSCRAT representatives engaged directly with participants at the project booth, creating further opportunities to present the project, discuss SME compliance needs and explore synergies with related European cybersecurity initiatives.

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.

13 November 2025 – European Digital Innovation Day for Open Innovations, UniBIT, Sofia



OSCRAT participated in the European Digital Innovation Day for Open Innovations hosted at **UniBIT** and aimed particularly at start-ups, innovators and organisations involved in digital entrepreneurship. According to the project stakeholder-engagement records, the event also formed the **third joint engagement activity with CONFIRMATE**, consolidating the collaboration developed during the earlier June and September activities. The event provided another channel for connecting CRA-related support with start-up and innovation communities.

20 January 2026 – CRA Standards Unlocked – EU Tour, Zagreb



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 participated in the ***CRA Standards Unlocked – EU Tour in Zagreb***, organised within the CYBERSTAND.eu cluster, where *Ecaterina Donciu from Enersec Technology* represented the project during a session dedicated to CRA compliance tools and funding opportunities for SMEs. The event brought together representatives of EU initiatives, cybersecurity experts and other ecosystem actors to discuss CRA requirements, harmonised standards, certification, conformity assessment and practical implementation. OSCRAT presented its open-source approach to CRA compliance and its focus on the operational needs of European SMEs, while the discussions and feedback gathered during the event provided useful input for the continued refinement of the OSCRAT tools.

21 May 2026 – CRA Standards Unlocked – EU Tour, Malta



OSCRAT was represented at the ***Malta stop of the CRA Standards Unlocked – EU Tour***, hosted by DiHubMT in cooperation with CYBERSTAND.eu. During the session on CRA compliance tools and funding opportunities, *Predrag Tasevski from UNICIS.Tech* represented OSCRAT alongside several complementary EU projects. The event focused on translating CRA requirements and emerging standards into practical guidance for SMEs, while providing a forum for

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.

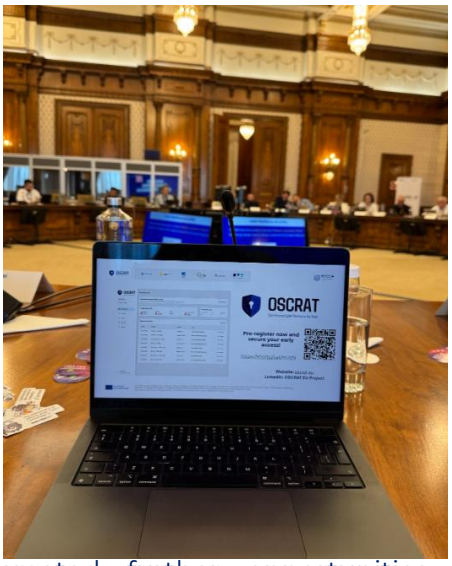
exchange between compliance-tool projects, standardisation actors and businesses.

24 June 2026 – CRA Standards Unlocked – EU Tour, Bucharest



OSCRAT was again represented at the ***CRA Standards Unlocked – EU Tour in Bucharest***, hosted at the Romanian Senate. The project presented its approach to making CRA compliance more accessible to European SMEs and showcased platform capabilities related to compliance assessment, SBOMs, vulnerability and risk management, incident handling and documentation. The event created further opportunities to engage European institutions, SMEs, cybersecurity experts, industry representatives and standardisation stakeholders.





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.

26 May 2025 – Cybersecurity Day hosted by Embassy of Belgium – Flanders Investment & Trade Representative Office in Warsaw, Poland



On 26 May 2025, the OSCRAT project was presented by Dariusz Rogowski and Michał Chrobak from Łukasiewicz-AI at an event organized by the Embassy of Belgium – Flanders Investment & Trade Representative Office in connection with a delegation of Belgian companies visiting Poland. The delegation consisted primarily of startups operating in the cybersecurity sector.

On the same day, a Pitch Event and Networking Session was held, during which the OSCRAT project was presented and companies were invited to complete a survey regarding the needs of SMEs in relation to the Cyber Resilience Act (CRA).

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.

2 September 2025 - 7th Cybersecurity Forum as part of the 34th Economic Forum in Karpacz, Poland



On 2 September 2025, the Polish Ministry of Digital Affairs and NASK – National Research Institute (NASK-PIB) organized the 7th Cybersecurity Forum as part of the 34th Economic Forum in Karpacz, addressing current issues, challenges, and solutions related to cybersecurity.

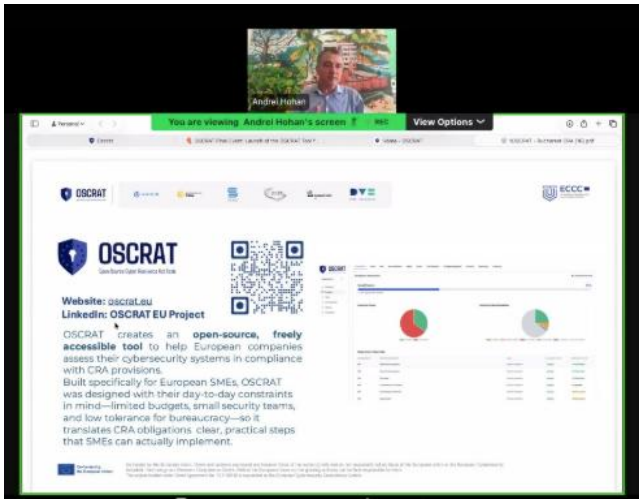
On behalf of NASK and Mr. Paweł Kostkiewicz, Director, Łukasiewicz – AI was invited to participate in an expert panel discussion on the Cyber Resilience Act (CRA). Dariusz Rogowski from Łukasiewicz-AI highlighted OSCRAT project in his presentation on *'Open-Source Cyber Resilience Act Tools to enhance cybersecurity resilience among European SMEs'*.

29 July 2026 – CRA for Manufacturing SMEs: From Compliance Requirements to Practical Solutions



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 participated in this online webinar organised for manufacturing SMEs by EIT Manufacturing and the MANTRA project in collaboration with Cyberstand.eu. *Andrei Hohan of Enersec Technology* represented OSCRAT during the ***session on CRA compliance tools***, presenting the platform and demonstrating how its functionalities can support SMEs in addressing CRA requirements. The event also brought OSCRAT together with representatives of Cyberstand.eu, CRA-AI and SECURE and included a direct Q&A with the audience.

21 September 2026 – Forum BEZPIECZEŃSTWA 360°, Warsaw

OSCRAT was represented at ***Forum BEZPIECZEŃSTWA 360°, Warsaw***, an event dedicated to public-sector security, cyber resilience and continuity of essential services. *Monika Ingram, Director of the Cybersecurity Research Centre at Łukasiewicz-AI,* delivered the presentation *"From Supplier Risk to City-Wide Cyber Crisis: Building Resilience in Local Government and Public Services."* This presentation demonstrated how to identify critical dependencies on suppliers and analyze the impact of cyber threats on the operational continuity of local government and infrastructure. It also covered the use of crisis simulations and decision-making exercises to prepare the administration for disruptions and mitigate their impact on residents. The event provided OSCRAT with an opportunity to contribute to discussions on supply-chain risk, cyber resilience and practical preparedness with public-sector and cybersecurity stakeholders.

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.

22–24 September 2026 – Gartner Security & Risk Management Summit, London



OSCRAT was also represented at the ***Gartner Security & Risk Management Summit 2026 in London***, which brought together CISOs, cybersecurity leaders, Gartner analysts and technology and solution providers from across Europe and beyond. *Monika Ingram from Łukasiewicz-AI* **represented OSCRAT in matchmaking and networking activities**, presenting the project and the OSCRAT platform as a practical tool to support CRA compliance to senior cybersecurity decision-makers, including CISOs and other security and risk-management professionals. The event offered access to a high-level cybersecurity community, including more than 200 European CISOs through the matchmaking activities, and created opportunities to discuss OSCRAT with potential users, industry stakeholders and organisations responsible for security and risk management. This engagement supported the project's wider objective of connecting OSCRAT with organisations facing practical cybersecurity, compliance and risk-management challenges.

These external engagements complemented the project's own training, workshop and event programme by strengthening OSCRAT's links with the wider European ecosystem working on CRA implementation and standardisation. They provided opportunities not only to present project progress and discuss relevant CRA-related issues, but also to exchange

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.

knowledge and experience with SMEs, industry representatives, standardisation experts and other EU-funded initiatives addressing similar compliance challenges, thereby contributing to a stronger and more interconnected CRA ecosystem across Europe.

As part of OSCRAT's sustainability strategy beyond the end of the project, consortium partners will continue to actively promote the OSCRAT platform and its publicly available resources, including the use cases, training materials and workshop resources. Partners will also continue to engage with relevant events, networks, working groups and CRA Cluster meetings, helping to maintain the visibility and enhance the practical use of OSCRAT within the wider European CRA ecosystem.

10. Stakeholder Input into Use Cases and Best Practices

As part of WP4 stakeholder-engagement activities, Deliverable **D4.1 – OSCRAT Use Cases and Best Practices Final Report consolidates 12 representative CRA assessment scenarios and practical lessons for manufacturers and SMEs**. The scenarios cover different types of products and illustrate how product evidence can be translated into classification, SBOM and security-scan analysis, compliance assessment, remediation actions and conformity-related decisions.

The scenarios were developed within the project and, where applicable, informed by WP4 stakeholder-engagement activities, including feedback from training sessions, workshops, stakeholder consultations and testing activities. Since the final OSCRAT platform was still being completed when the assessment cases were prepared, they were conceived as representative practical examples drawing on project experience and stakeholder input. In this way, the report translates the knowledge generated through OSCRAT into a reusable resource that can support future users in understanding and preparing for CRA compliance.

The report is publicly available in the **Resources section** of the OSCRAT website.

11. Relationship with Communication and Dissemination

Stakeholder engagement and dissemination are complementary but distinct functions within OSCRAT. Dissemination makes information, outputs and results available to relevant audiences and measures their visibility and reach. Stakeholder engagement requires a more direct relationship: participation, interaction, questions, feedback, consultation, knowledge exchange or another form of two-way involvement.

This distinction explains why some activities appear in both D1.4 and D5.4 but are reported differently. A workshop, for example, is a dissemination output

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.

when considering its promotion, online availability, video views and broader reach; in D1.4 it is relevant because SMEs and experts interacted with the consortium, discussed practical CRA issues and provided questions or feedback. D5.4 should therefore be consulted for website, social-media, newsletter, press-release, video and other communication analytics, which are intentionally not duplicated here.

11. Summary Stakeholder Engagement KPI Status

Key Performance Indicator	Target	Status
Workshops, training sessions and events facilitating interaction and CRA compliance among European SMEs	9	4 training sessions 4 workshops 1 CRA event 1 OSCRAT Final Launch Conference 1 Platform Demo **Total of 11 activities**
CRA compliance use cases and best practices	4	**12 representative scenarios in D4.1**
Participants among workshops and training sessions and international CRA event	>300	307 participants in trainings and workshops 30 at the international CRA event 110 at the Launch event **More than 440 participants involved**
Number of industry partnerships and collaborations fostered by the project (enhancing the project's reach and impact)	5	**4 dedicated collaborations fostered and 1 in the process of being finalised**

12. Conclusion

Stakeholder engagement was an integral component of OSCRAT throughout the project lifecycle. While Task T1.5 under WP1 provided the coordination framework, WP4 – Stakeholder Engagement formed the core of the project's direct engagement activities, with a particular focus on promoting cybersecurity resilience and helping European SMEs understand and prepare for CRA compliance. Complementary activities under WP2 and WP5 supported this process through stakeholder-needs analysis, targeted outreach and broader connections with relevant European communities.

The engagement process evolved progressively. Early stakeholder consultation under WP2 provided evidence on CRA awareness, user needs and the perceived relevance of the OSCRAT functionalities. These findings informed a structured

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.

WP4 programme consisting of four training sessions and four thematic workshops, which moved stakeholders from a general understanding of the CRA towards increasingly practical topics such as conformity readiness, incident management, vulnerability handling and risk management. The OSCRAT International CRA Event, the Final OSCRAT Event and Platform Launch, and the Platform Demo further extended this process by connecting SMEs and other stakeholders with cybersecurity experts, project partners and the completed OSCRAT platform.

Stakeholder engagement was not limited to activities organised directly by the project. Participation in European networks, CRA clusters, Digital Innovation Hub activities and external events enabled OSCRAT to interact with a wider community of SMEs, cybersecurity professionals, policymakers, standardisation actors and complementary EU-funded initiatives. Cooperation with other projects and networks strengthened knowledge exchange, created opportunities for joint activities and connected OSCRAT with the wider European ecosystem supporting practical CRA implementation.

The project also translated stakeholder-facing activities and project learning into reusable resources. D4.1 consolidates 12 representative CRA assessment scenarios and practical best practices, providing future users with examples of how different aspects of CRA compliance can be approached using structured evidence, assessment and remediation processes. These scenarios complement the training materials, workshop resources and OSCRAT platform itself, extending the value of stakeholder engagement beyond the individual activities held during the project.

From a quantitative perspective, the stakeholder-engagement programme exceeded the planned targets. The project implemented 11 relevant stakeholder-engagement activities against a target of nine and delivered 12 CRA compliance use cases and best-practice scenarios against a minimum target of four. Four dedicated collaborations were established, with a fifth collaboration finalised during the project implementation period. The KPI requiring more than 300 participants across workshops, training sessions and the CRA event was surpassed, contributing to the overall overachievement of stakeholder engagement activities. A total of 307 participants were recorded across four training sessions and four workshops, while the OSCRAT International CRA Event attracted 30 participants and the Platform Launch Event reached 110 participants. Overall, these activities engaged more than 440 participants. Attendance figures from the Platform Demo webinar held on 30 September 2026 will be added during the final reporting phase, further contributing to the overall engagement figures.

The distinction between stakeholder engagement and communication and dissemination has been maintained throughout this report. While WP5 reports the wider reach and visibility of OSCRAT through communication channels and dissemination activities, D1.4 focuses on participation, interaction, feedback, knowledge exchange and cooperation. This distinction makes it possible to

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.

assess not only how widely OSCRAT was communicated, but also how stakeholders interacted with the project and how those interactions supported its objectives.

Beyond the formal end of the project, the consortium will continue actively promoting the OSCRAT platform and its publicly available resources, including the use cases, training materials and workshop resources. Continued participation in relevant events, networks, working groups and CRA Cluster meetings will support the visibility and practical use of the project results and maintain OSCRAT's connection with the evolving European CRA ecosystem.

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

OSCRAT – D1.4
Stakeholder Engagement

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.