Ref. Ares(2026)9268284 - 30/09/2026

OSCRAT

Open-Source Cyber Resilience Act Tools

D5.4

OSCRAT – Dissemination Results

Submission date: 30.09.2026

Author: PMF Research

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	D5.4 Dissemination Results
Work package	WP 5 Dissemination and Exploitation
Due Date	31.05.2026 (in Portal)
Submission Date	30.09.2026
Lead Partner	PMF Research
Contributing Partner	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

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	22.09.2026	PMF Research	First draft
0.2	29.09.2026	All partners	Contributions
1.0	30/09/2026	PMF Research	Final version

Abstract

This deliverable reports the communication and dissemination results achieved by the OSCRAT project throughout its implementation period. It consolidates the activities foreseen in the Description of Action and further developed through D5.1 and D5.2, and assesses their implementation through relevant quantitative and qualitative indicators. The report covers the project website, social media, newsletters and press releases, audiovisual content, workshops and training sessions, OSCRAT events, dissemination of public project resources, external events, partner-level dissemination, and the overall stakeholder and geographic reach achieved. It also provides a consolidated overview of the formal communication and dissemination KPIs and related stakeholder-engagement KPIs.

As the project ends on 30 September 2026 and this deliverable is finalised at project closure, the assessment is based on the latest verified data available at the drafting cut-off. Any remaining analytics generated during the final project days will be consolidated in the Final Technical Report, where applicable. Exploitation activities are intentionally excluded, as they are addressed separately in D5.3.

Keywords

Communication; Dissemination; Cyber Resilience Act; CRA; SMEs; Stakeholder outreach; Stakeholder engagement; Digital Europe; OSCRAT; KPIs; Workshops; Training; Events.

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 7
1.1 Purpose of D5.4 7
1.2 Scope of the report 7
1.3 Reporting period and data cut-off 8
1.4 Methodology and sources of evidence 8
2. Communication and Dissemination Framework 9
2.1 Objectives 9
2.2 Target audiences 9
2.3 Evolution from D5.1 to D5.2 10
2.4 OSCRAT Visual Identity and EU Visibility 10
3. OSCRAT Website and Digital Resource Hub 11
3.1 Website development and role 11
3.2 Website content development 12
3.3 Website analytics 12
4. Social Media Communication 13
4.1 OSCRAT LinkedIn 13
4.2 Partner amplification 16
5. Newsletters 16
6. Press Releases 18
7. Video and Audiovisual Dissemination 19
8. Workshops, Training Sessions and CRA International Event as Dissemination Activities 21
8.1 Training sessions 21
8.2 Workshops 22
8.3 OSCRAT.eu International CRA Event 23
8.4 OSCRAT Final Event and platform launch 23
8.5 OSCRAT in Action Platform Demo 24
8.6 Aggregated results 25
9. Major OSCRAT Results and Resources 26
9.1 OSCRAT platform 26
9.2 D4.1 – OSCRAT Use Cases and Best Practices 27

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.

9.3 User Manual and technical/public resources 27
9.4 Public deliverables 28
10. Participation in External Events, Conferences and Networking Activities 28
11. Other Communication and Dissemination Materials 31
12. KPI Overview 33
12.1 Core communication and dissemination KPIs – WP5 33
12.2 Related stakeholder-engagement and dissemination KPIs – WP4 34
13. Evolution and Adaptation of Communication and Dissemination Approach 35
14. Conclusion 36

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

This deliverable presents the communication and dissemination results achieved by the OSCRAT project throughout its implementation period. It provides an evidence-based overview of the activities implemented under WP5, together with related stakeholder-engagement outputs that contributed to raising awareness of the Cyber Resilience Act (CRA), engaging target audiences and supporting the visibility and reuse of project results.

The dissemination approach combined multiple complementary channels, including the OSCRAT website, LinkedIn communication, newsletters, press releases, audiovisual content, stakeholder events, training sessions, workshops, external event participation and partner-level dissemination. Over the project lifecycle, communication progressively evolved from raising awareness about OSCRAT and the CRA towards promoting concrete project outputs, including the OSCRAT platform, public resources, technical documentation and practical CRA compliance guidance.

The project website acted as the central dissemination hub, providing access to project information, public deliverables, resources, events and the OSCRAT platform. Digital communication activities generated significant visibility, including 58 LinkedIn posts, 8 newsletters, 4 press releases and 10 audiovisual outputs published at the drafting cut-off. Partner dissemination further extended the project's reach through institutional communication channels and professional networks.

Stakeholder engagement activities represented an important component of the dissemination strategy. Four training sessions and four workshops supported CRA knowledge transfer and reached 307 participants in total. The project also organised the International CRA Event, the Final OSCRAT Event and the OSCRAT in Action Platform Demo, providing additional opportunities to showcase project results and support knowledge exchange with relevant target groups. The D4.1 Use Cases and Best Practices report further strengthened dissemination by providing 12 practical CRA assessment scenarios, exceeding the formal project target.

The final KPI assessment confirms that the main communication and dissemination objectives were achieved. The project exceeded the targets established for social-media activity and audiovisual dissemination, achieved the planned newsletter and press-release outputs, and created a broad ecosystem of reusable communication and knowledge resources. Overall, OSCRAT successfully combined digital outreach, stakeholder engagement and open access resources to support awareness, understanding and practical preparation for CRA-related cybersecurity requirements.

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 of D5.4

Communication and dissemination are essential components of OSCRAT, as the project aims not only to develop open-source tools supporting Cyber Resilience Act (CRA) compliance, but also to ensure that the related knowledge, resources and results are visible, accessible and effectively transferred to European SMEs and the wider cybersecurity ecosystem. WP5 was established to raise awareness of OSCRAT, identify and engage relevant target groups, tailor communication activities and messages to different audiences, and support the dissemination of project knowledge, activities, deliverables and outcomes.

The Description of Action assigns WP5 a key role in designing and implementing a dissemination campaign targeting relevant stakeholders, ensuring effective knowledge sharing, maximising the visibility of OSCRAT's core topics and results, increasing awareness of the CRA and the Digital Europe Programme, and implementing communication activities capable of reaching audiences at local, national and European level.

D5.4 presents the results achieved through this process. It documents the activities implemented, the communication and dissemination channels used, the audiences reached, and the performance of the relevant KPIs against the objectives defined in the project's Communication, Dissemination Strategy and Exploitation Plan.

1.1 Scope of the report

This report covers the communication and dissemination activities implemented under **WP5 – Dissemination & Exploitation**, together with related outreach activities originating from **WP4 – Stakeholder Engagement** that materially contributed to dissemination, awareness raising and visibility of the OSCRAT project and its results.

The report covers the dissemination of OSCRAT project outputs, including public resources and deliverables, the promotion of the OSCRAT platform, consortium-level and partner-level outreach activities, media and press activities, digital communication activities, newsletters, social media engagement and event-based dissemination.

While **D1.4 – Stakeholder Engagement** provides a detailed overview of stakeholder identification, engagement methodology, consultation activities, workshops, training sessions and interaction outcomes, this deliverable focuses specifically on the **dissemination dimension** of these activities. Therefore, where stakeholder engagement activities also generated dissemination results, D5.4 reports only the related communication outputs, dissemination channels, audiences reached and visibility achieved. Detailed stakeholder profiles, engagement approaches and feedback mechanisms are addressed in **D1.4 – Stakeholder Engagement**.

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 report does not cover the exploitation strategy, ownership arrangements, licensing model, commercialisation approach, post-project governance model or sustainability planning of the OSCRAT platform. These aspects are addressed separately in **D5.3 – Exploitation Plan**. Where communication activities supported platform visibility or uptake, this is reported only as an observable dissemination result.

1.2 Reporting period and data cut-off

Following the approved amendment, OSCRAT runs from 1 December 2024 to 30 September 2026, for a total duration of 22 months. D5.4 is due at the end of the project and is therefore being finalised while some of the final September 2026 analytics are still being generated.

For this reason, D5.4 uses the most recent verified data available at the drafting cut-off. Where a value is not yet final, the document uses an explicit placeholder rather than an estimate. Remaining figures generated in the final days of September will be consolidated in the Final Technical Report, ensuring that the final project reporting contains the complete communication and dissemination dataset.

1.3 Methodology and sources of evidence

The assessment combines documentary evidence, public communication outputs and channel-specific analytics. The main documentary baseline is provided by *D5.1 – Communication, Dissemination Strategy & Exploitation Plan*, *D5.2 – Updating of the Communication and Dissemination Strategy*, *D4.1 – OSCRAT Use Cases and Best Practices Final Report*, and the available project documentation related to dissemination activities.

Quantitative evidence is drawn from **website analytics, LinkedIn analytics, newsletter and email statistics, video-platform data, event registrations and attendance records, participant lists, feedback forms, partner dissemination records and media evidence**, where available.

The public OSCRAT website was used to support the verification of implemented communication and dissemination outputs, including the **News, Events, Deliverables, OSCRAT Tool and Resources** sections. The website content, together with available communication records, provided evidence of the dissemination activities implemented throughout the project lifecycle.

These activities were complemented by continuous dissemination through digital channels, including the OSCRAT LinkedIn page and partner communication channels, ensuring the visibility of project developments, results and resources among relevant target groups.

OSCRAT Resources:
https://oscrat.eu/resources/

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 News:
https://oscrat.eu/news/

OSCRAT Events:
https://oscrat.eu/events/

OSCRAT Deliverables:
https://oscrat.eu/deliverables/

OSCRAT Tool:
https://oscrat.eu/oscrat-tool/

OSCRAT LinkedIn:
https://www.linkedin.com/company/106299311/admin/page-posts/published/

2. Communication and Dissemination Framework

2.1 Objectives

The original communication and dissemination framework was established in D5.1 and aligned with the objectives of WP5. The underlying approach was to make OSCRAT visible to the organisations most affected by the Cyber Resilience Act, communicate project progress in an accessible way, and progressively disseminate the practical outputs generated by the technical and stakeholder-engagement work packages.

The main communication and dissemination objectives pursued throughout implementation were to raise awareness of OSCRAT and of the CRA; reach and engage European SMEs; increase visibility of the OSCRAT platform; disseminate project activities, outputs and results; engage cybersecurity stakeholders and multipliers; make practical project knowledge accessible; support broad European outreach; maintain a recognisable visual identity; and coordinate communication across multiple channels and consortium partners.

2.2 Target audiences

D5.1 identified the core target groups: SMEs in the digital-product sector, decision- and policy-makers, Digital Innovation Hubs, cybersecurity experts and industry associations. These groups remained central throughout implementation because they combine direct potential users of OSCRAT with multipliers capable of extending the reach of the project's results across relevant European stakeholder communities.

As the project matured, dissemination also reached additional ecosystem actors, including organisations supporting SMEs, other European initiatives addressing CRA implementation or cybersecurity standards, research and innovation stakeholders, event participants, media contacts and the wider professional public. The messaging evolved according to the audience: SMEs were addressed with practical compliance-oriented content, while experts, DIHs

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 multipliers were engaged through technical sessions, events, resources and cross-project exchange.

2.3 Evolution from D5.1 to D5.2

D5.2 updated the original strategy in response to project progress, emerging results and the evolving needs of the target audiences. The update emphasised clearer and more targeted communication, optimisation of the website and social-media channels, broader European outreach, stronger visibility of the tools, refinement of training and workshop activities, and the introduction or strengthening of audiovisual dissemination.

This evolution was particularly important during the second half of the project. As the technical work progressed from requirements and testing towards a complete operational platform, communication increasingly moved from general project awareness to result-oriented dissemination. The website Resources section, training and workshop recordings, platform demonstrations, User Manual, product documentation, use cases and Final Event all supported this transition.

2.4 OSCRAT Visual Identity and EU Visibility

A coherent visual identity was established at the beginning of the project in order to give OSCRAT a recognisable presence and ensure consistency across consortium communication. D5.1 documents the development and adoption of the OSCRAT logo, colour palette, typography and common visual templates for public-facing materials.

The visual system was applied across the project website, deliverables, PowerPoint presentations, social-media graphics, newsletters, press releases, training and workshop materials, event communication and other promotional assets. This ensured that content produced by different partners remained identifiable as part of the same project.

EU visibility requirements were integrated into the communication framework through the use of the EU emblem, the required funding statement, the ECCC identity where applicable, and the standard disclaimer. These elements were incorporated into the OSCRAT deliverable template and reused consistently across public project materials and event outputs.

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.

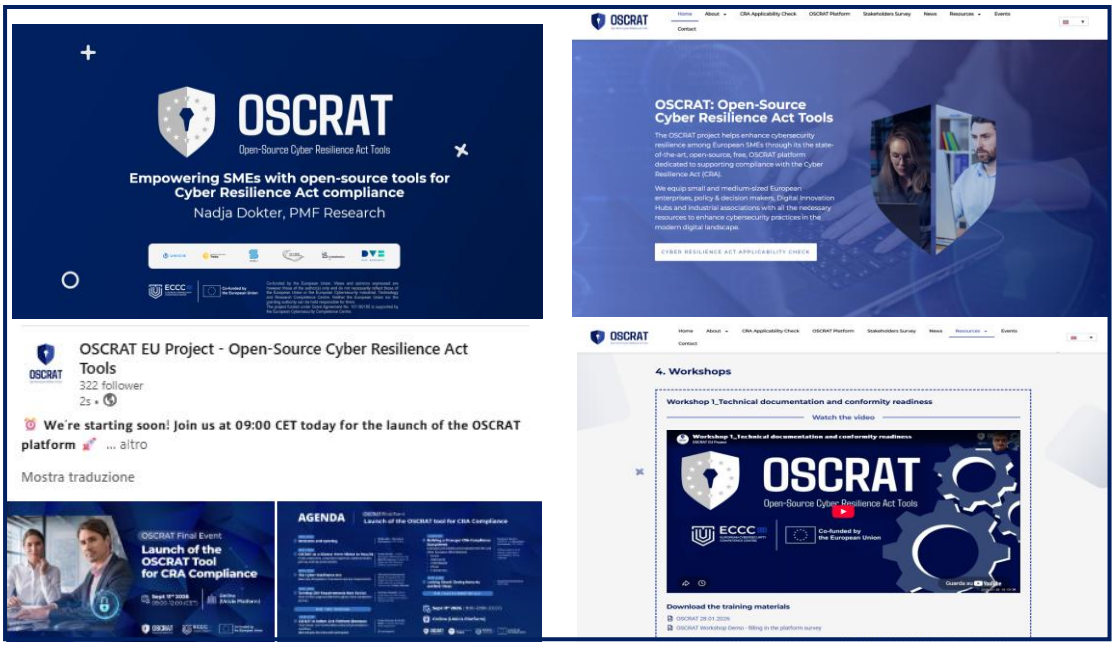
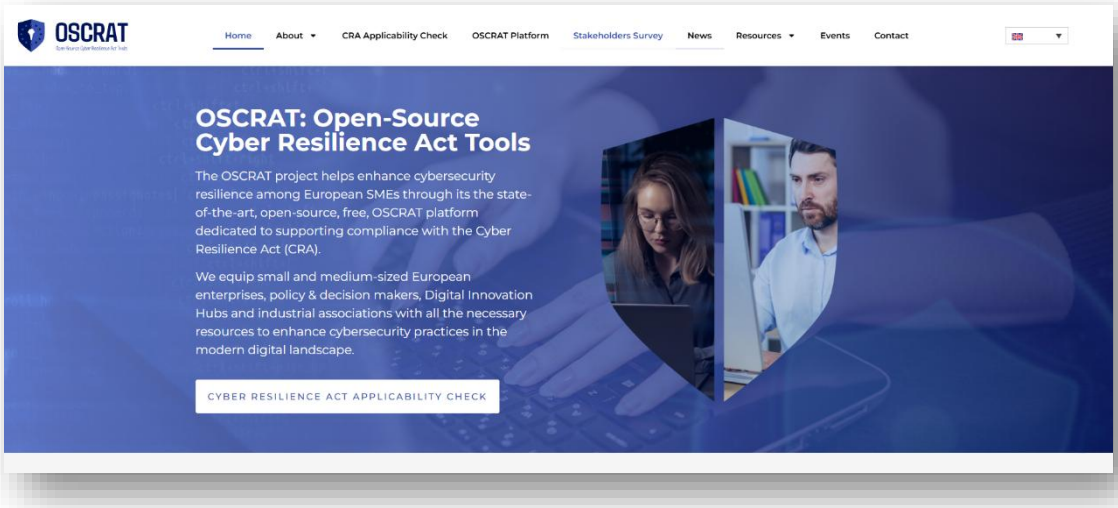


Figure 1: Examples of OSCRAT visual identity application across project materials and communication channels

The examples above illustrate the consistent application of the OSCRAT visual identity across project templates, the website, social media content and workshop materials.

3. OSCRAT Website and Digital Resource Hub

3.1 Website development and role



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 **OSCRAT website** has served as the project's main public information hub. Its role expanded over time from presenting the project and consortium to providing direct access to practical outputs, news, event information and the final platform. D5.1 planned the website as a user-friendly, responsive and regularly updated channel capable of reaching both core stakeholder groups and the wider public.

The website now provides access to project information, consortium and work-package descriptions, public deliverables, News, Events, the CRA Applicability Check, the OSCRAT platform, stakeholder-survey information and the dedicated Resources section. This structure allows the website to function simultaneously as a communication channel, a repository of project outputs and a practical entry point to the OSCRAT tool ecosystem.

3.2 Website content development

Throughout the project implementation, the website was progressively populated with news items, event announcements, newsletters, press releases, project outputs, training materials, workshop resources and links to the OSCRAT platform. The later-stage addition and enrichment of the Resources section was especially important because it transformed live activities into learning material accessible beyond the original participants.

At the drafting cut-off, the Resources section contains four training sessions and four workshops, with video access and downloadable materials. The News section contains six newsletters and four press releases. D4.1 has been completed and published in the Resources section, providing an additional added value for SMEs and other stakeholders. OSCRAT's public deliverables are also accessible through the website Deliverables section.

3.3 Website analytics

The formal WP5 KPI requires at least 7,000 website visits over the project period. In addition to this formal target, website performance is assessed through a broader set of metrics capable of showing audience size, user engagement, geographic reach and the relative visibility of specific resources.

The final analytics table below combines the formal KPI with supplementary web indicators, including users, page views, engagement indicators, geographic distribution and the most visited website sections.

Website Indicator	Results (by 25 September – reporting cut-off)	Comment
Website visits – formal KPI (page views)	17,688	KPI Target ≥ 7,000

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.

Users	5,442	Audience size
Bounce rate	52.31%	User engagement
Average engagement time per session	00:03:01	User engagement
Click to Url & File Download	5,442	User interactions
Most visited pages	Home – OSCRAT (5,620 views); Events – OSCRAT (1,275 views); Stakeholders Survey – OSCRAT (931 views); News – OSCRAT (915 views); OSCRAT Tool – OSCRAT (893 views)	Content performance

Table 1: OSCRAT website analytics

With 17,688 page views recorded at the reporting cut-off, the website substantially exceeded the formal KPI of at least 7,000 website visits.

OSCRAT reached a geographically diverse audience. Users accessed the website from both European and non-European countries, with the highest number of users recorded in the United States (1,484), followed by Italy (596), China (405), Germany (384), Bulgaria (325) and Poland (322). Additional users were recorded from other European and international countries, including Romania (248), the Netherlands (207), Singapore (200) and Finland (120), confirming the broad geographical reach of the project communication activities. The presence of users from countries represented within the consortium, including Italy, Bulgaria, Poland and Romania, highlights the role of partner networks in supporting project visibility and outreach. At the same time, the international distribution of users indicates that OSCRAT communication activities reached audiences beyond the immediate project ecosystem.

Regarding **website engagement**, the OSCRAT website recorded 5,442 users and 17,688 page views during the reporting period. The average engagement time per session was 3 minutes and 1 second, indicating sustained interaction with the available content. The most visited pages were the Home page (5,620 views), Events section (1,275 views), Stakeholders Survey page (931 views), News section (915 views) and OSCRAT Tool page (893 views), showing interest in both general project information and key project results, including project activities, engagement opportunities and access to the OSCRAT platform.

4. Social Media Communication

4.1 OSCRAT LinkedIn

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.

LinkedIn was the principal OSCRAT social-media channel and was used continuously throughout the project to announce key milestones, promote workshops and training sessions, share CRA-related information, disseminate newsletters and press releases, promote events, and direct audiences towards the project website and the OSCRAT platform. The channel was particularly suited to the project's professional target groups, including SMEs, cybersecurity experts, Digital Innovation Hubs (DIHs), industry stakeholders and policy-related audiences.

The formal project **KPI** required **at least 20 social-media posts**. In addition to monitoring the number of posts published, the project assessed a broader set of LinkedIn performance indicators, including impressions, reach, interactions, clicks, reactions, comments, reposts, CTR, engagement rate, page visits generated by posts and followers gained from posts. These indicators provide a more complete picture of the visibility, reach and interaction generated by OSCRAT's social-media activity.

LinkedIn Indicator	Result
Posts published – formal KPI	**58**
Cumulative impressions	20,889
Cumulative reach	9,419
Total interactions	1,902
Total clicks	819
Total reactions	958
Total reposts / shares	118
Overall CTR	3.92%
Overall engagement rate	9.11%
Page visits generated from posts	131

Table 2: OSCRAT LinkedIn performance indicators and cumulative results

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.

LinkedIn activity **substantially exceeded the formal project KPI of at least 20 social-media posts. A total of 58 posts were published** through the OSCRAT LinkedIn page, meaning that the target was exceeded by 38 posts.

The available post-level analytics also show sustained visibility and interaction. The posts generated 20,889 cumulative impressions and a cumulative reach of 9,419, together with 1,902 interactions. These interactions comprised 819 clicks, 958 reactions, seven comments and 118 reposts/shares. Based on the aggregated figures, the overall CTR was 3.92% and the overall engagement rate was 9.11%. LinkedIn activity also generated 131 visits to the OSCRAT page and 42 new followers directly attributable to individual posts.

The cumulative data reported above represent the sum of the post-level analytics that could be retrieved. Metrics were available for the vast majority of LinkedIn posts, while data could not be collected for a limited number of posts, mainly among the older publications. The overall CTR and engagement rate were calculated using the aggregated available data.

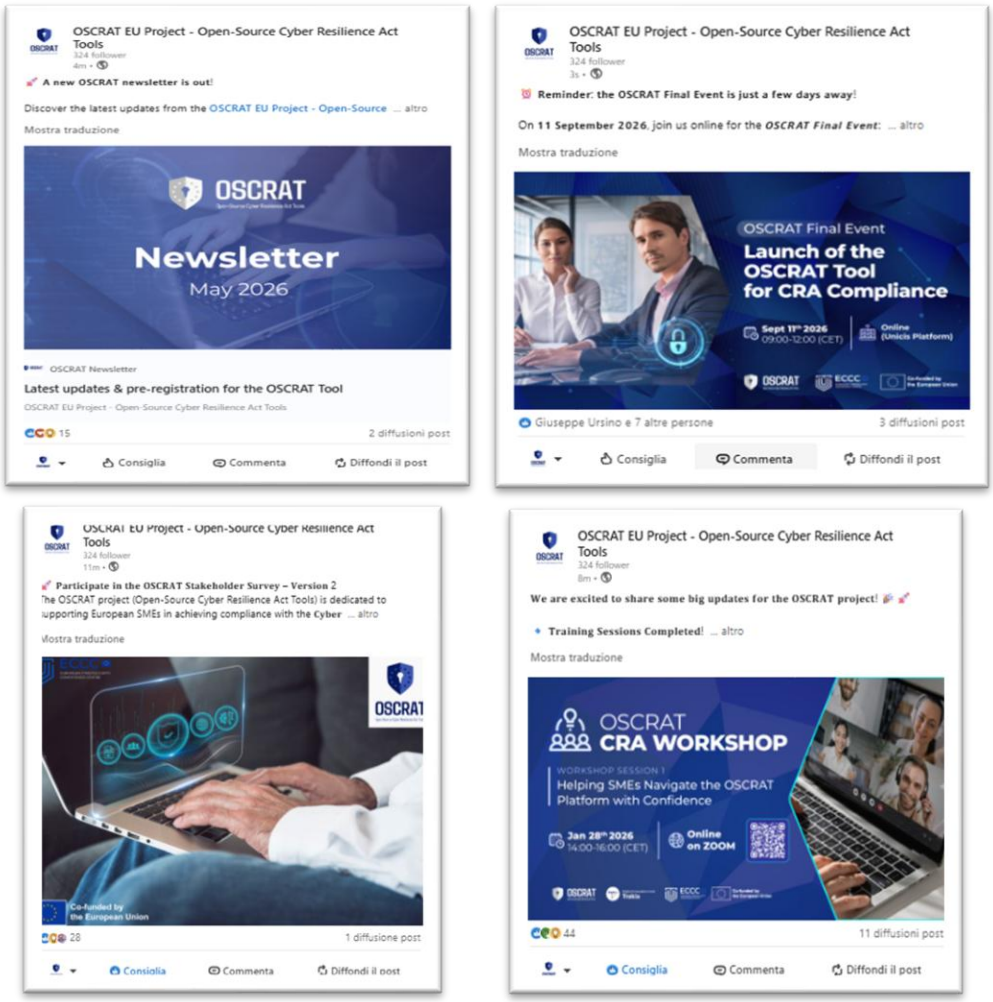


Figure 2: Examples of OSCRAT LinkedIn communication activities

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.

4.2 Partner amplification

Communication and dissemination through the OSCRAT central project channels was complemented by partner amplification through their organisational social-media accounts, websites and professional networks, further extending project visibility. Based on the dissemination activities recorded, partners published a total of **110 OSCRAT-related LinkedIn posts**, **9 posts on X** and **16 posts on Facebook**, complemented by **12 website-related dissemination activities.**

Across the available analytics, partner **LinkedIn activities** generated **15,963 cumulative impressions**, while **X activities** generated **284 cumulative impressions** and **Facebook activities** generated **9,498 cumulative impressions**. **Website-related activities** for which analytics were available accounted for an additional **458 recorded impressions**. Overall, this corresponds to **26,203 cumulative impressions** recorded across partner dissemination channels. These figures reflect the analytics that could be retrieved and should be interpreted as cumulative exposure rather than as unique individuals reached.

Partner amplification involved all consortium organisations. **PMF Research** primarily used LinkedIn; **Unicis.Tech OÜ** combined LinkedIn, X and website communication; **Łukasiewicz AI** disseminated OSCRAT content through LinkedIn, X, Facebook and its website; **EDIH Trakia** used Facebook, LinkedIn, X and its website; **ENERSEC** focused primarily on LinkedIn; and **Oves Enterprise** contributed through LinkedIn posts published by company representatives. Together, these activities extended OSCRAT communication beyond the central project channels and helped disseminate project activities and results, including events, workshops, training opportunities, stakeholder surveys, newsletters, CRA-related information, project developments and resources across the partners' respective networks.

The cumulative figures presented above are based on the available analytics for the recorded partner activities. As impression data could not be retrieved for all publications, particularly on LinkedIn, these totals should be considered a conservative estimate of the visibility generated through partner channels.

5. Newsletters

As foreseen in D5.1 – Communication, Dissemination Strategy & Exploitation Plan, newsletters were used as a recurring communication format to provide stakeholders with updates on OSCRAT activities, developments and results. Email distribution was managed through **Brevo**, while a subscription form available on the project website enabled interested stakeholders to register for project updates. **LinkedIn** was also used as a complementary dissemination channel for selected newsletters. Overall, **eight newsletters were produced and disseminated** during the project, covering project progress, stakeholder

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 activities, workshops and training sessions, platform development and launch, and resources supporting CRA compliance. Table 3 summarises their main topics, dissemination dates and available outreach figures.

All eight newsletters are publicly available through the OSCRAT News page.

Newsletter	Main topic/title and link to website	Month of dissemination	Audience reached / distribution
1	Introduction to OSCRAT project, objectives and workflow	April 2025	**Brevo**: 708 recipients
2	Berlin TPM: project progress and stakeholder engagement	May 2025	**Brevo:** 689 recipients
3	OSCRAT workshops, training events and stakeholder engagement	July 2025	**Brevo:** 683 recipients
4	OSCRAT Training sessions and ENISA Conference participation	September 2025	**Brevo:** to be updated
5	Training sessions, WP2 closure, upcoming workshops, Beta Release and EU Tour activities	January 2026	**Brevo:** 638 recipients **LinkedIn:** 153 users reached
6	Resources, OSCRAT tool pre-registration and EU Tour activities	May 2026	**Brevo:** 620 recipients
7	OSCRAT Platform launch announcement and Final Event	July 2026	**Brevo:** 575 recipients **LinkedIn:** 314 users reached
8	OSCRAT Official platform launch and CRA compliance resources	September 2026	**Brevo:** 555 recipients **LinkedIn:** 52 users reached

Table 3: OSCRAT newsletters – topics, dissemination dates and outreach

Based on the **Brevo analytics available at the time of reporting**, the newsletters reached a cumulative total of **4,468 deliveries**, with individual campaigns reaching between 555 and 708 recipients.

For three newsletters, **LinkedIn** was used as an additional dissemination channel to further extend visibility and engagement beyond the mailing list. As Brevo and LinkedIn measure outreach through different metrics and distribution mechanisms, their figures are reported separately and are not aggregated into a single reach figure.

As the project remains active until 30 September 2026, any remaining analytics not yet consolidated at the drafting cut-off will be updated, where applicable, and reported in the Final Technical Report.

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.

6. Press Releases

Press releases were used as communication outputs to **highlight key OSCRAT developments, milestones and achievements** throughout the project lifecycle. Their purpose was to translate technical progress and project results into accessible content for stakeholders, partner networks and wider audiences, supporting the visibility of the project and its outcomes.

Four press releases were prepared by PMF Research and published on the OSCRAT News page. They were also promoted through the central OSCRAT LinkedIn channel and shared with consortium partners to support further dissemination through their respective communication networks. The outreach figures reported in Table 4 refer specifically to the visibility generated through the central OSCRAT LinkedIn promotion of each press release.

The press releases covered the main stages of OSCRAT implementation, including the introduction of the project and its objectives, progress in platform development, updates on project activities, and the official launch of the OSCRAT platform. Additional evidence of partner-level dissemination activities will be consolidated during the final reporting phase to provide a more complete overview of the outreach and uptake generated.

Press Release No. 4, published on 11 September 2026, communicated the official launch of the final OSCRAT platform. It highlighted the main platform capabilities and presented the Final Event as an opportunity to showcase the completed solution and engage stakeholders around the project results.

The four press releases and their main milestones are summarised in Table 4 below.

Press Release	Date	Main milestone / subject	Title of Press Release and link	LinkedIn outreach
1	March 2025	Introduction to the OSCRAT project, its objectives, consortium and planned open-source CRA compliance tool	OSCRAT: a European Project to strengthen the cybersecurity of SMEs and verify compliance with the Cyber Resilience Act	377
2	November 2025	Completion of WP2 and transition to the design and development phase of the OSCRAT platform	OSCRAT: WP2 completed. Development of the cybersecurity and CRA compliance tool begins	566
3	February 2026	WP2 completion, training sessions, upcoming workshops, Beta Release and cybersecurity events	OSCRAT: beta launch in 2026 and first workshops coming soon	524
4	September 2026	Official launch of the final OSCRAT platform at the Final Event	OSCRAT launches state-of-the-art, free, open-source platform for European SMEs	355

Table 4: OSCRAT press releases and dissemination

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.

Partner Website Articles and News Content

Partner amplification also went beyond social-media redistribution. Unicis.Tech and Łukasiewicz AI developed dedicated articles and news content on their institutional websites, providing more extensive editorial coverage of OSCRAT, its relevance for SMEs and CRA compliance, and the development and launch of the platform. These publications helped translate the main press-release messages into more detailed content tailored to the partners' own audiences and provided an additional dissemination layer beyond social media.

The main partner website articles identified in connection with the press-release milestones include:

- **Unicis.Tech** – *Introducing OSCRAT: Strengthening Cyber Resilience for European SMEs*
- **Unicis.Tech** – *Cyber Resilience Act Compliance: A Practical Guide for SMEs — and How OSCRAT Can Help*
- **Łukasiewicz AI** – *OSCRAT – Supporting European SMEs in Enhancing Cyber Resilience*

7. Video and Audiovisual Dissemination

Audiovisual dissemination gained importance during the second half of the project as a means of extending the accessibility and lifetime of training, workshop and platform-related content beyond live participation. In line with the updated communication approach outlined in D5.2, video recordings were increasingly used to transform stakeholder-facing activities into reusable dissemination resources for SMEs and other interested stakeholders.

The formal WP5 **KPI** required **at least two videos** to be published on the project website and YouTube. This target was exceeded: at the drafting cut-off, **10 audiovisual outputs** had been published on the OSCRAT YouTube channel. With the exception of the general project presentation, the remaining nine videos were also made available through the OSCRAT website. These included the recordings of the four training sessions, the four thematic workshops and the Final Launch Event.

The training and workshop recordings are integrated into the **OSCRAT Resources section** alongside the related supporting materials, strengthening their value as reusable learning resources and ensuring continued access to the content beyond the live sessions.

A further audiovisual output, "OSCRAT in Action: Platform Demo and UPKIP's Cyber Resilience Assessment Journey," will be published as soon as it is finalised. Once published, this will bring the total number of audiovisual outputs to 11.

The audiovisual outputs published at the drafting cut-off and their available YouTube viewing data are summarised in Table 5 below.

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.

Audiovisual Output	Title/Topic (add link)	Channel	Publication date	YouTube views
Project Presentation	OSCRAT EU Project Presentation	YouTube	07/01/2026	**107**
Training session 1	Setting the context - what CRA changes, and why it matters	YouTube / Website	04/02/2026	**64**
Training session 2	Scope, accountability, and the compliance obligations that will "stick"	YouTube / Website	04/02/2026	**21**
Training session 3	Standards and conformity assessment - how "compliance" becomes credible	YouTube / Website	04/02/2026	**27**
Training session 4	Implementation roadmaps - from gap analysis to CE readiness	YouTube / Website	04/02/2026	**39**
Workshop 1	Technical documentation and conformity readiness	YouTube / Website	09/03/2026	**47**
Workshop 2	Incident response planning and management	YouTube / Website	09/03/2026	**29**
Workshop 3	Vulnerability handling	YouTube / Website	17/04/2026	**27**
Workshop 4	Risk management	YouTube / Website	04/05/2026	**28**
Final Launch Event	Launch of the OSCRAT Tool for Compliance	YouTube / Website	24/09/2026	**11**
Platform Demo	**OSCRAT in Action: Platform Demo and UPKIP's Cyber Resilience Assessment Journey**	YouTube / Website	Available soon	**n.a**

Table 5: OSCRAT audiovisual dissemination outputs, channels and views

At the drafting cut-off, the **10 published audiovisual outputs** had generated a cumulative total of **400 YouTube views**. The general **OSCRAT EU Project Presentation** recorded the highest number of views (**107**), followed by **Training Session 1** (**64 views**) and **Workshop 1** (**47 views**). The audiovisual programme therefore substantially exceeded the formal target of two videos and created a broader repository of reusable **project, training, workshop and event content** that remains publicly accessible beyond the individual 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.

8. Workshops, Training Sessions and CRA International Event as Dissemination Activities

The workshops and training sessions were implemented under **WP4 as stakeholder-engagement activities** and are comprehensively documented in **Deliverable D1.4 – Stakeholder Engagement**. However, they also contributed significantly to dissemination, awareness raising and CRA knowledge sharing and are therefore referenced here in D5.4. This deliverable focuses specifically on their role in increasing OSCRAT visibility, disseminating project knowledge and engaging relevant stakeholder groups, while avoiding duplication of the detailed activity descriptions provided in D1.4.

8.1 Training sessions

Four online training sessions were implemented between September and December 2025. The training sequence was structured as a progression from understanding the CRA context to identifying scope and obligations, exploring standards and conformity assessment, and finally translating the regulatory framework into an implementation roadmap. The online format supported participation from stakeholders across different countries and allowed the consortium to record and later publish the sessions as reusable resources.

The four training sessions, their main topics and participation figures are summarised in Table 6 below.

Session	Date	Main theme	Participants
Training 1	08/09/2025	Setting the context: what the CRA changes, and why it matters	**35**
Training 2	13/10/2025	Scope, accountability and compliance obligations	**36**
Training 3	10/11/2025	Standards and conformity assessment	**35**
Training 4	08/12/2025	Implementation roadmaps: from gap analysis to CE readiness	**33**

Table 6: OSCRAT training sessions – topics, dates and stakeholder participation

Overall, the **four training sessions** reached **139 participants**, providing a structured CRA knowledge pathway from regulatory awareness to practical implementation considerations. Together with the workshops presented in Section 8.2, the training sessions contributed to the formal project KPI requiring

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.

at least 300 participants across workshops and training sessions (see Section 8.6).

The **training content was** subsequently integrated into the **OSCRAT Resources section** together with **downloadable materials**. This ensured that the educational value of the sessions extended beyond live attendance, providing a permanent knowledge resource for SMEs and other stakeholders interested in CRA compliance.

8.2 Workshops

Four thematic workshops were implemented during 2026, focusing on practical CRA compliance topics directly connected to the functionality of the OSCRAT platform and the challenges faced by SMEs in preparing for compliance. The workshops progressed from technical documentation and conformity readiness to incident response planning, vulnerability handling and risk management, providing stakeholders with practical guidance on key aspects of the CRA compliance process.

The four workshops and their main topics and participation figures are summarised in Table 7 below.

Session	Date	Main theme	Participants
Workshop 1	28/01/2026	Technical documentation and conformity readiness	**39**
Workshop 2	23/02/2026	Incident response planning and management	**47**
Workshop 3	30/03/2026	Vulnerability handling	**46**
Workshop 4	27/04/2026	Risk management	**36**

Table 7: OSCRAT workshops – topics, dates and participation

Overall, the **four workshops** reached **168 participants**, providing practical guidance on key CRA compliance topics and supporting stakeholders in translating regulatory requirements into concrete implementation actions.

As with the training sessions, **the workshop recordings and supporting materials are available online** through the **OSCRAT Resources section**. This supports continued dissemination beyond the live activities and provides SMEs and other stakeholders with topic-specific CRA guidance that can be revisited when needed.

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.

8.3 OSCRAT.eu International CRA Event

The Description of Action foresaw an International CRA Event under T4.1, designed to bring together cybersecurity experts, project partners and relevant stakeholders to promote practical knowledge on CRA compliance among European organisations. This activity was implemented through the **OSCRAT.eu pan-European event on 11 June 2026**, organised in a hybrid format at the **Technical University of Sofia**, with online participation alongside Spinoff Europa 2026.

The event aimed to support SMEs in understanding the implications of Regulation (EU) 2024/2847 and showcased how the open-source OSCRAT platform can support practical compliance and digital resilience. Its hybrid format combined in-person participation with online access, extending the reach of the activity beyond the local audience and enabling engagement with stakeholders across Europe.

International CRA Event indicator	Result
Date	11/06/2026
Format	Hybrid – Sofia + online
Participants	30

Table 8: OSCRAT International CRA Event – participation and outreach indicators

Together with the four training sessions and four workshops, the International CRA Event brought the number of stakeholder-facing activities to nine, achieving the formal KPI of at least nine workshops, training sessions and events.

8.4 OSCRAT Final Event and platform launch

The dedicated **OSCRAT Final Event** was implemented online on **11 September 2026 from 09:00 to 12:00 CEST**. The event marked the official launch of the final OSCRAT platform and summarised the project's journey, principal achievements, CRA context and practical platform workflows in a single public dissemination moment.

The programme presented the practical implications of the CRA for SMEs, included a live launch and demonstration of the final platform, and created opportunities for interaction through Q&A and dialogue with other European CRA-related initiatives. Press Release No. 4 was issued on the same date and positioned the platform launch in the context of the start of the CRA reporting

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.

obligations, providing a strong communication hook for the final project dissemination activities.

The event was particularly important from a dissemination perspective because the consortium used the Final Event to demonstrate how OSCRAT translates regulatory requirements into practical workflows covering applicability and compliance assessment, SBOMs, vulnerability management, incident handling, risk management, tasks and documentation.

The main event characteristics, participation indicators and available outreach results are summarised in Table 9 below.

Final Event indicator	Result
Date	11/09/2026
Format	Online – UNICIS platform
Registrations	160+
Participants	110
Q&A / interaction	Yes – Q&A session included
Post-event recording views to date	11 YouTube views

Table 9: OSCRAT Final Event and Platform Launch – participation and outreach indicators

Available evidence confirms the implementation of the OSCRAT Final Event and Platform Launch on 11 September 2026 in an online format, with more than **160 registrations and 110 participants recorded**.

8.5 OSCRAT in Action Platform Demo

Following the official launch of the final OSCRAT platform, a dedicated practical demonstration session was organised on **30 September 2026** to showcase how the platform can support organisations in their Cyber Resilience Act (CRA) compliance journey.

The online session, entitled **"OSCRAT in Action: Platform Demo and UPKIP's Cyber Resilience Assessment Journey"**, provided participants with a practical introduction to the OSCRAT Platform through the assessment testimonial journey of UPKIP. The session illustrated how OSCRAT can support organisations

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.

in assessing products, managing cybersecurity information and preparing compliance documentation.

During the event, participants explored how UPKIP used OSCRAT to carry out its CRA assessment and gained insights into the practical application of the platform's compliance functionalities.

The OSCRAT in Action demo represented an important dissemination and knowledge-transfer activity following the platform launch. The event materials and related resources will be made available soon through the OSCRAT website Resources section, contributing to the long-term accessibility and reuse of project results.

8.6 Aggregated results

The four training sessions and four workshops represented **eight structured stakeholder-facing activities** with a strong dissemination and awareness-raising component. Together with the **International CRA Event implemented on 11 June 2026**, the project reached the target of at least nine workshops, training sessions and events. **The Final OSCRAT Event and Platform Launch held on 11 September 2026 and the subsequent OSCRAT in Action Platform Demo on 30 September 2026** represented additional dissemination milestones beyond this minimum count.

The main quantitative results of the training sessions, workshops and CRA-related events are summarised below. The overview highlights the number of activities implemented, their contribution to the project's dissemination objectives and the consolidated participation figures available at the drafting cut-off.

indicator	Result
Training sessions	4
Workshops	4
International CRA Event	1
Final OSCRAT Event	1
OSCRAT in Action Platform Demo	1 additional dissemination activity
Minimum confirmed activity count (target: 9)	11 activities: 4 training sessions, 4 workshops, 1 International CRA Event, 1 Final Event and 1 Platform Demo
Total participants in training sessions	139

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.

Total participants in workshops	168
International CRA Event participants	30
Final OSCRAT Event participants	110
Platform Demo participants	Not yet available
Total Combined participants	**447 participants** (training sessions, workshops, International CRA Event and Final Event; Platform Demo attendance not available)

Table 10: Aggregate results of OSCRAT stakeholder-facing activities and dissemination events

The **stakeholder engagement activities** implemented by OSCRAT achieved the minimum target of at least nine workshops, training sessions and events, which was further exceeded when including the Final Event and the Platform Demo. These activities created multiple opportunities for participants to increase their understanding of CRA requirements and explore the practical application of the OSCRAT platform.

Across the main stakeholder engagement activities, OSCRAT reached **447 participants**, including 307 participants in the four training sessions and four workshops, 30 participants in the International CRA Event and 110 participants in the Final OSCRAT Event. The formal KPI concerning participation in workshops and training sessions and CRA event was therefore achieved, with the additional events further extending the project's outreach. Attendance figures for the Platform Demo were not available at the drafting cut-off. Any additional verified participation or outreach data will be consolidated and reported in the Final Technical Report, where applicable.

9. Major OSCRAT Results and Resources

9.1 OSCRAT platform

As the technical development progressed, dissemination increasingly focused on the **OSCRAT platform**. Activities in the lead-up to the final release included website information, training and workshop demonstrations, calls to action, the Final Event, Press Release No. 4, social-media activity and direct links to the CRA Applicability Check and platform access.

The final platform brings together a set of capabilities relevant to CRA-oriented product-security management and compliance support, including applicability

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 compliance assessment, Software Bill of Materials management, vulnerability and incident management, risk assessment, configuration management, compliance tasks, technical documentation, Declaration of Conformity workflows and audit logging.

D5.4 reports the communication and dissemination activities supporting the visibility and uptake of the OSCRAT platform. Ownership, licensing aspects and post-project technical continuity are outside its scope and are addressed separately in D5.3 – Exploitation Plan.

9.2 D4.1 – OSCRAT Use Cases and Best Practices

D4.1 has been completed and provides **12 representative CRA assessment scenarios**. The report translates different product situations into practical examples covering intake and classification, SBOM and security-scan analysis, compliance assessment, remediation activities and conformity-related decisions. Its practical orientation makes it a valuable dissemination resource for SMEs and organisations seeking concrete examples of how CRA-related assessment processes can be structured and applied.

The formal project KPI required at least **four CRA compliance use cases and best practices**. With **12 scenarios included in the final report**, this target has been substantially exceeded. The report is publicly available through the **OSCRAT website (Deliverables section and the Resources section)**, where it supports the dissemination of practical CRA guidance among SMEs and other stakeholders.

9.3 User Manual and technical/public resources

The final communication ecosystem also provides access to the **OSCRAT User Manual** and **Full Product Documentation**, supporting different user needs around the adoption, use and understanding of the solution.

The **OSCRAT platform** represents the main access point to the project result. The **User Manual** provides step-by-step guidance to support users in navigating the platform and understanding its main functionalities, while the **Full Product Documentation** provides more detailed technical information on the platform structure, components and implementation aspects. Together, these resources complement the platform itself by supporting both end users and technical stakeholders interested in adopting and reusing the project results.

The **Full Product Documentation** corresponds to **D3.8 – Full Product Documentation**, which is also available through the OSCRAT website Deliverables section.

Their public availability strengthens the accessibility and reuse of OSCRAT results, enabling SMEs, technical stakeholders and other interested organisations to consult guidance and technical information beyond live demonstrations, training sessions and workshops.

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.

9.4 Public deliverables

The OSCRAT website **Deliverables section** provides an overview of the project outputs across all work packages and provides public access to the deliverables that are classified as publicly available. This contributes to transparency and ensures that the knowledge generated by OSCRAT can be accessed and reused by stakeholders beyond the consortium.

The Deliverables section lists the project outputs produced across the different work packages, including both publicly available and restricted deliverables according to their applicable dissemination level. Deliverables classified as public (PU) are made available through the website, while deliverables classified as sensitive (SEN) remain subject to restricted access and are not published as public resources.

At the time of drafting this deliverable, the OSCRAT website provides access to **16 publicly available deliverables** covering different areas of the project, including project management, requirements analysis, platform development and testing, stakeholder engagement, use cases and best practices, and communication and dissemination activities.

The main public deliverables relevant for external stakeholders include:

D2.1 – Comprehensive Project Requirements Document

D3.8 – Full Product Documentation

D4.1 – OSCRAT Use Cases and Best Practices Final Report

D5.1 – Communication & Dissemination Strategy

D5.4 – Dissemination Results

Any remaining updates concerning the publication status of project outputs, including possible uploads completed during the final project phase, will be reflected in the Final Technical Report, where applicable.

10. Participation in External Events, Conferences and Networking Activities

D5.1 foresaw participation in relevant conferences, events and networking opportunities as part of the dissemination mix. Such activities allowed OSCRAT to reach stakeholders beyond the project's own digital channels and supported interaction with cybersecurity initiatives, SME-support structures and European regulatory and standardisation communities.

For the purposes of D5.4, only external events where OSCRAT was actively represented by consortium partners, through presentations, speaking contributions, networking activities or other forms of direct stakeholder

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.

interaction, are considered as dissemination outputs. Events merely promoted through the OSCRAT website are not included in the overview below.

Throughout the project, OSCRAT partners actively participated and were engaged in **external events, conferences, webinars and networking activities** across several European countries, including Bulgaria, Poland, Romania, Croatia, Malta and the United Kingdom, as well as online formats. These activities enabled the consortium to present OSCRAT, discuss CRA compliance challenges with relevant communities and connect with SMEs, cybersecurity professionals, Digital Innovation Hubs, policymakers and related European initiatives.

The external engagement activities included recurring **European Digital Innovation Hub (EDIH) Days**, dedicated to OSCRAT and CRA-related topics, typically involving 50–100 participants per session. Detailed information on these activities and other external engagements is provided in **D1.4 – Stakeholder Engagement**.

Other relevant engagements included European cybersecurity events such as **CRA – Making the EU Market Resilient in Bucharest**, **CRA Standards Unlocked events**, and the **Gartner Security & Risk Management Summit 2026**, where OSCRAT was presented to senior cybersecurity stakeholders, including a matchmaking community involving more than 200 European CISOs.

The main external events and networking activities where OSCRAT was actively represented are summarised in Table 11 below. The overview includes events where consortium partners contributed through presentations, speaking roles, networking activities or other forms of direct stakeholder interaction.

These activities also supported the development of structured collaborations with other initiatives and ecosystem actors, including joint dissemination events with the CONFIRMATE project. In this respect, the project contributed to the KPI on industry partnerships and collaborations fostered by the project (target: 5), with four collaborations formalised and a fifth being finalised at the drafting cut-off, as detailed in D1.4 – Stakeholder Engagement.

Date	Event	Partner	OSCRAT role
30–31 January 2025	European Digital Innovation Days: Insurance Sector, Sofia Tech Park	EDIH Trakia	Project promotion and stakeholder outreach
20–21 March 2025	European Digital Innovation Days in Industrial Cybersecurity, Sofia Tech Park	EDIH Trakia	Project promotion and stakeholder outreach
26 May 2025	Cybersecurity Day hosted by Embassy of Belgium – Flanders Investment & Trade Representative Office, Warsaw	Łukasiewicz-AI	Project presentation

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.

29–30 May 2025	European Digital Innovation Days in Critical Infrastructure, Plovdiv	EDIH Trakia	Speaker / presentation
19–20 June 2025	European Digital Innovation Days / Spinoff Europa 2025, GATE Institute, Sofia	EDIH Trakia	Speaker / presentation
20 June 2025	First joint OSCRAT–CONFIRMATE dissemination event	EDIH Trakia	Joint presentation / networking
2 September 2025	7th Cybersecurity Forum as part of the 34th Economic Forum in Karpacz, Poland	Łukasiewicz-AI	Speaker / expert panel presentation
25 September 2025	Second joint OSCRAT–CONFIRMATE event, International Technical Fair, Plovdiv	EDIH Trakia	Joint presentation / networking
8 October 2025	CRA – Making the EU Market Resilient, Bucharest	OSCRAT Consortium (represented by PMF Research)	Panel speaker / booth networking
13 November 2025	European Digital Innovation Day for Open Innovations, UniBIT, Sofia	EDIH Trakia	Project presentation / networking
20 January 2026	CRA Standards Unlocked – EU Tour, Zagreb	ENERSEC	Speaker / presentation
21 May 2026	CRA Standards Unlocked – EU Tour, Malta	UNICIS.Tech	Speaker / presentation
24 June 2026	CRA Standards Unlocked – EU Tour, Bucharest	ENERSEC	Speaker / presentation
29 July 2026	CRA for Manufacturing SMEs: From Compliance Requirements to Practical Solutions	ENERSEC	Speaker / presentation
21 September 2026	Forum BEZPIECZEŃSTWA 360°, Warsaw	Łukasiewicz-AI	Speaker / presentation
22–24 September 2026	Gartner Security & Risk Management Summit 2026, London	Łukasiewicz-AI	Networking / matchmaking

Table 11: OSCRAT participation in external events and networking activities

Selected examples of OSCRAT participation in external events are provided in Figure 3 below, illustrating the project's presence and contribution to external stakeholder 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.

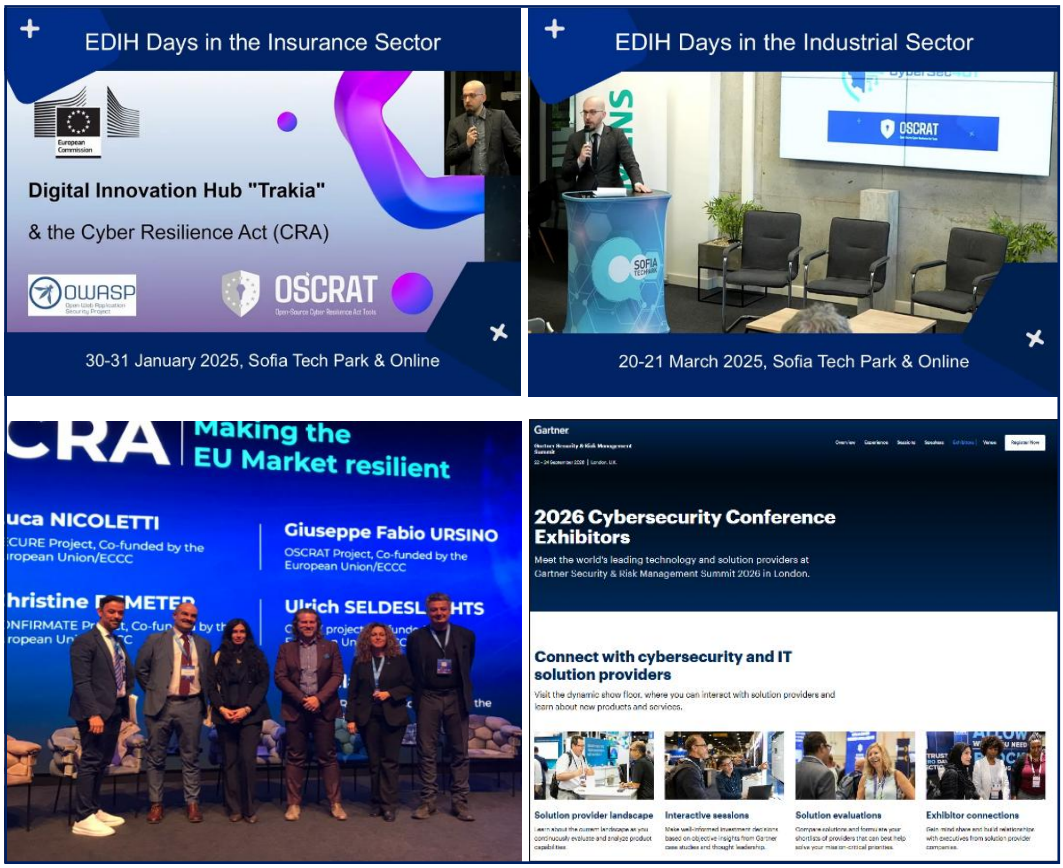


Figure 3: Examples of OSCRAT representation at external events and networking activities

11. Other Communication and Dissemination Materials

Beyond the main dissemination channels described in the previous sections, OSCRAT produced and used a range of supporting communication materials to ensure consistency, reuse and visibility of project results. These included the project visual identity, presentation templates, social-media assets, the project brochure, newsletter and press-release formats, training and workshop materials, the User Manual, Full Product Documentation and practical CRA resources such as the D4.1 Use Cases and Best Practices report. These materials supported communication activities across the project lifecycle and were reused through the website, events, partner channels and stakeholder engagement activities.

The main supporting communication and dissemination materials developed and used throughout the project are summarised in Table 13 below.

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.

Planned item / action	Status	Evidence / data required
Project visual identity	Implemented	Applied across website, deliverables, presentations and communication materials
PowerPoint template	Implemented	Project presentations and events
Social media visual materials	Implemented	LinkedIn posts and event promotion materials
Project brochure	Implemented	Digital and printed brochure
Newsletter template	Implemented	8 newsletters disseminated through Brevo
Press-release format	Implemented	4 public press releases
Training materials	Implemented	OSCRAT Resources section
Workshop materials	Implemented	OSCRAT Resources section
User Manual	Implemented	Publicly available resource
Full Product Documentation	Implemented	Publicly available resource
D4.1 Use Cases and Best Practices	Implemented	Public resource

Table 13: Overview of additional communication and dissemination materials

These materials contributed to the accessibility, reuse and long-term visibility of OSCRAT results by allowing stakeholders to access project knowledge beyond individual events and live dissemination activities. Any additional updates concerning the availability of communication materials will be reflected in the Final Technical Report, where applicable.

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.

12. KPI Overview

The OSCRAT project includes a **set of formal KPIs** to monitor the achievement of its objectives. For the purposes of D5.4, the core assessment focuses on the communication and dissemination indicators related to WP5. Selected WP4 indicators are also reported separately, as workshops, training sessions, the International CRA Event and the use cases generated relevant dissemination and awareness-raising outputs. This distinction ensures that work package responsibilities remain clear while capturing the contribution of WP4 activities to the overall dissemination effort without duplicating reported activities.

12.1 Core communication and dissemination KPIs – WP5

KPI	Target	Actual at drafting cut-off	Status
Website visits	≥ 7,000	**17,688 page views**	**Achieved**
Social-media posts	≥ 20	**58 LinkedIn posts**	**Achieved**
Videos on website / YouTube	≥ 2	**10 audiovisual outputs published on YouTube (9 also available through website)**	**Achieved**
Newsletters + press releases	≥ 12	**12 outputs: 8 newsletters + 4 press releases**	**Achieved**

Table 14: Overview of core communication and dissemination KPIs – WP5

The KPI assessment confirms that the main WP5 communication and dissemination targets were achieved at the drafting cut-off. The project exceeded the targets for social-media activity and audiovisual dissemination, while also achieving the planned output targets for newsletters and press releases.

D5.1 operationalised the combined newsletter and press-release KPI through a plan of at least eight newsletters and four press releases. This target was achieved, with eight newsletters and four press releases produced and disseminated during the project.

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 KPI assessment above reflects the verified data available at the drafting cut-off. Any additional figures generated during the final project days, including updates related to newly published audiovisual content or remaining communication analytics, will be consolidated and reported in the Final Technical Report, where applicable.

12.2 Related stakeholder-engagement and dissemination KPIs – WP4

KPI	Target	Actual at drafting cut-off	Status
Workshops, training sessions and events	≥ 9	**4 training sessions, 4 workshops, International CRA Event, Final Event and the OSCRAT in Action Platform Demo, bringing the total number of stakeholder-facing activities to 11.**	**Achieved**
CRA compliance use cases and best practices	≥ 4	**12 developed in D4.1**	**Achieved**
Participants in workshops, training sessions and CRA event	≥ 300	**447 participants**	**Achieved**
Industry partnerships and collaborations fostered by the project	≥ 5	**4 formalised collaborations; 1 being finalised**	**Almost achieved**

Table 15: WP4 stakeholder-engagement and dissemination KPI assessment

The stakeholder-engagement and dissemination-related KPIs were achieved at the drafting cut-off.

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. Evolution and Adaptation of Communication and Dissemination Approach

The communication and dissemination approach evolved throughout the project lifecycle in response to project maturity, stakeholder needs and the progressive availability of project results. Rather than being applied as a fixed plan, the strategy was refined during implementation to ensure that communication activities remained aligned with the development of the OSCRAT platform and the needs of relevant target audiences.

During the early phase, activities focused on establishing the OSCRAT identity, introducing the project objectives, raising awareness of the Cyber Resilience Act (CRA) and building an initial community around the initiative. This created a shared understanding of the project before the technical outputs became mature enough for detailed promotion.

As implementation progressed, the focus shifted towards structured knowledge sharing and more targeted engagement activities. The four training sessions progressively introduced CRA concepts, while the four workshops addressed specific practical and operational aspects. The publication of recordings and supporting materials represented an important evolution of the dissemination approach, transforming live activities into reusable knowledge resources accessible beyond the original participants.

A further evolution concerned the increasing use of digital and professional communication channels. While D5.1 included different social-media channels, implementation placed stronger emphasis on LinkedIn as the main platform for reaching professional audiences, including SMEs, cybersecurity stakeholders, Digital Innovation Hubs and innovation communities. At the same time, audiovisual dissemination, the Resources section and public documentation became increasingly important tools for extending the accessibility and lifetime of OSCRAT's project results.

In the final phase, communication became increasingly result-oriented, directing audiences towards concrete outputs including platform demonstrations, public deliverables, the User Manual, Full Product Documentation, the 12 use cases, the International CRA Event and the public launch of the completed OSCRAT platform. This transition from general awareness raising towards practical support resources allowed OSCRAT to connect CRA knowledge with concrete tools and guidance supporting compliance preparation.

The project extension also provided additional time for completing technical activities, stakeholder engagement actions and final dissemination efforts. While the extension did not modify the project scope or budget, it supported stronger outreach activities, including the promotion of the final platform version and related resources.

Overall, the communication and dissemination approach evolved from an initial awareness-building phase into a more mature ecosystem combining digital communication, knowledge transfer, partner networks and reusable resources.

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.

This progression strengthened the visibility, accessibility and long-term value of OSCRAT results.

The qualitative observations presented in this section are based on the implementation of communication and engagement activities, participation data, partner dissemination contributions and the use of project resources. No additional formal testimonials or structured qualitative feedback were available at the drafting cut-off.

14. Conclusion

OSCRAT implemented broad, multi-channel communication and dissemination activities combining digital communication, knowledge-sharing activities, event-based dissemination and open access to project resources. The communication approach evolved progressively throughout the project lifecycle, moving from establishing project visibility and raising awareness of the Cyber Resilience Act towards the dissemination of concrete outputs and the final public launch of the OSCRAT platform.

The website acted as the central public hub and was complemented by social-media communication, newsletters, press releases, training sessions, workshops, audiovisual resources, public deliverables and partner dissemination activities. The four training sessions and four workshops created a structured learning pathway around CRA compliance, while the International CRA Event, the Final Event and the OSCRAT in Action Platform Demo provided additional opportunities to showcase project results and support knowledge exchange with relevant target groups. The transformation of live activities into permanent online resources further strengthened accessibility and enabled the reuse of project knowledge beyond the original audiences.

The completion of D4.1 with 12 representative CRA assessment scenarios substantially exceeded the formal minimum target for use cases and provided an additional practical dissemination resource for SMEs and other interested organisations. The final communication phase increasingly focused on concrete project results, including the completed OSCRAT platform, public documentation, practical use cases and demonstrations supporting CRA compliance preparation.

The KPI results confirm that the main communication and dissemination objectives were achieved. The project exceeded the targets established for social-media activity and audiovisual dissemination, while achieving the planned outputs for newsletters, press releases, training activities, workshops and related stakeholder-engagement indicators. Any additional analytics generated during the final project days, including remaining audiovisual or platform-related metrics, will be consolidated in the Final Technical Report where applicable.

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.

Overall, D5.4 provides an evidence-based overview of the communication and dissemination activities implemented by OSCRAT, demonstrating how the project combined digital channels, partner networks and reusable resources to translate project results into visible and accessible support for CRA-related cybersecurity preparedness.

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 – D3.4 Dissemination Results

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.