OSCRAT
Open-Source Cyber Resilience Act Tools

D5.2.

OSCRAT – Updating of the communication and Exploitation Plan

Submission date: 04/11/2025

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
Name	Updating of the communication and dissemination strategy
Number	101190180
Work package	WP5 – Dissemination & Exploitation
Due Date	30/11/2025
Submission Date	30/11/2025
Lead Partner	PMF Research
Author name(s)	Francesco Antonio Alescio
Version	Final
Status	Draft
Type:	R – Document, report
Dissemination level:	PU - Public

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	30/10/2025	Francesco Antonio Alescio	Started working on draft n.1
1.0	04/11/2025	Francesco Antonio Alescio	Finished working on draft n.1
2.0	25/11/2025	Francesco Antonio Alescio	Document approved by consortium

Abstract

This deliverable, **D5.2. – Updating of the Communication and Dissemination Strategy**, provides an updates overview of the communication and dissemination framework for the OSCRAT project. Building on the foundations established in **D5.1.**, this document refines and strengthens the project's outreach and visibility actions, ensuring alignment with OSCRAT's progress, stakeholder feedback and the evolving European cybersecurity landscape. The updated strategy focuses on three key objectives: enhancing the visibility of OSCRAT and its open-source tools, strengthening engagement with European SMEs and other target groups, and ensuring the long-term sustainability of project results through coordinated and accessible dissemination channels. The document details improvements in communication tools and approaches, including the official website, the LinkedIn page, and the forthcoming YouTube channel, which will host a series of videos such as project introductions, training session recordings, workshops, and the beta release demo of the OSCRAT tool. Through a coherent and coordinated communication framework led by PMF Research, this deliverable ensures that OSCRAT's dissemination activities effectively support the project's exploitation objectives and contribute to raising awareness of the Cyber Resilience Act (CRA) among European SMEs. The strategy described herein positions OSCRAT as a lasting reference point for cyber resilience and regulatory compliance in Europe, ensuring that its open-source outputs remain accessible, visible, and impactful beyond the project's duration.

Keywords

OSCRAT; Communication Strategy; Dissemination; Cyber Resilience Act; CRA; Horizon Europe; Open-Source Tools; SMEs; Cybersecurity; Awareness; Exploitation; Sustainability; Stakeholder Engagement; YouTube; LinkedIn; 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.

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

Table of contents

Co-funded by the European Union

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

1. Executive summary

This document outlines the update to the communication and dissemination strategy for the OSCRAT project, with the aim to optimize dissemination activities, improving stakeholder interactions and ensuring broader visibility for the tools developed under the project.

As the project progresses, it has become crucial to refine the communication tactics in response to stakeholder feedback and evolving needs of our target.

This update focuses on the optimization of existing communication channels, the introduction of new dissemination tools and expanding the outreach efforts to ensure that the OSCRAT tools become visible to the public, particularly to European SMEs and cybersecurity experts.

The updated strategy aims to increase the visibility of OSCRAT, promote the adoption of the project's tools, and ensure that the tools are accessible and usable by SMEs for compliance with the Cyber Resilience Act (CRA). It also outlines how the dissemination efforts will be aligned with the project's sustainability goals, ensuring that the dissemination activities will continue to support OSCRAT's objectives beyond the project's duration.

The starting point will be the evaluation of the achievement level of the KPIs already introduced in **D5.1. - Communication, Dissemination Strategy & Exploitation plan**, already prepared in M6.

The key updates in the strategy can be summarised in:

- **Refinement of communication objectives**: focusing on clarity, engagement and outreach to key target audiences.
- **Optimized use of dissemination channels**: enhancing the website, social media platforms, newsletters and press releases to engage stakeholders and promote the tool.
- **Expanded dissemination activities**: refinement of training sessions and workshops to reach a broader audience and ensure deeper engagement.
- **Introduction to the Exploitation Plan**: ensuring the dissemination strategy can be use as a fundamental starting point to ensure the long-term goals of the project, particularly in terms of tool adoption and sustainability.

The main objective of this deliverable is to ensure that the communication, dissemination and exploitation efforts are updated, adapted and available in a definite version.

By improving the coordination and effectiveness of dissemination activities, this updated strategy has the goal to ensure that OSCRAT remains on track to achieve its mission of supporting SMEs in achieving cyber resilience and help them in CRA Compliance processes.

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. Introduction

The OSCRAT project, funded under the European Union's Digital Europe Programme, aims to develop open-source tools to help European SMEs comply with the **Cyber Resilience ACT (CRA)**. These tools, designed to streamline compliance processes and enhance the overall cyber resilience in the EU market, play a critical role in enabling SMEs to navigate the evolving cybersecurity landscape.

To achieve this, the need for a robust and effective communication strategy were outlined in the D5.1. – Communication, Dissemination and Exploitation plan, prepared by PMF Research and uploaded during M6.

As the project progresses, the need becomes increasingly important, also considering the approach of the official date for the tool Beta release, scheduled for February 2026.

Deliverable 5.2. – Updating of the communication and Exploitation Plan is dedicated to updating the communication and dissemination approach, based on the results from previous awareness raising activities, feedback from stakeholders and lessons learned.

This deliverable reflects the evolving nature of the project, ensuring that dissemination and communication efforts are tailored to the current project phase and long-term sustainability goals.

2.1. Purpose of the Deliverable

The purpose of this deliverable is to provide an updated strategy for disseminating the OSCRAT tools and results.

By refining and enhancing existing communication plan, the strategy ensures that the tools developed by the project reach the intended audience. This includes:

- Increased visibility of the OSCRAT Platform and tools.
- Wider adoption of the tools by SMEs and other stakeholders.
- Effective engagement with target audiences through tailored communication efforts.

The updated strategy also aligns with the project's broader goals of raising awareness about cybersecurity resilience, supporting SMEs in regulatory compliance, and fostering sustainable, long-term engagement with the tools developed by 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.

2.2. Background

Since its start, the OSCRAT project has been working towards the development of a suite of tools designed to help SMEs comply with the Cyber Resilience Act (CRA).

As the project nears the testing and deployment phases, it is crucial to ensure that the tools are communicated effectively, highlighting the relevance and the impact, to the stakeholder which will benefit from them, especially European SMEs, the primary target group and potential users of the tool.

To achieve this, a clear ongoing communication effort is required to ensure the tool are widely understood, adopted and effectively used.

The dissemination strategy must address the current communication gaps and ensure that all relevant stakeholders are reached and effectively engaged in the project scope and developed tools.

2.3. Scope of the Update

This deliverable will focus on providing updates to the original communication and dissemination strategy, particularly focusing on:

- Improving stakeholder engagement through more targeted communications.
- Updating the dissemination channels to better reach the intended audiences.
- Enhancing the content strategy to ensure that OSCRAT tools are presented in an accessible and engaging way.

The goal is to ensure that OSCRAT's communication efforts are aligned with the original dissemination objectives of raising awareness, promoting adoption and fostering long-term use of the tools by SMEs across Europe.

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3. Review of the previous strategy (D5.1.)

This section is dedicated to revisiting the communication and dissemination strategy outlined in **Deliverable 5.1. – Communication, Dissemination Strategy & Exploitation plan**.

The main goal is to evaluate the effectiveness of the original strategy, identify areas of success and highlight areas which require improvements.

With the review of the previous strategy, we gain insights into what has worked well and where modification is necessary to ensure a successful outreach of OSCRAT communication efforts.

3.1. Communication Objectives Review

In D5.1., the original communication objectives were designed to raise awareness about the OSCRAT Tools, promote their adoption by SMEs, and increase engagement with relevant stakeholders in the cybersecurity areas of interest. These objectives included:

- **Increasing visibility**: promoting the OSCRAT tools to a broad range of stakeholders, including SMEs, industry associations and cybersecurity experts.
- **Encouraging adoption**: motivating SMEs to integrate OSCRAT tools for their compliance procedures in aligning internal processes to cybersecurity directives and guidelines.
- **Building stakeholder trust**: establishing strong relations with key stakeholders through transparent communication and engagement efforts.

After evaluating the progress against these objectives, we can confirm that while some objectives were already achieved during the first twelve months of project implementation, there are areas where more targeted outreach is needed, particularly in engagement with SMEs.

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.

3.2. Audience and Channel Effectiveness

The original strategy identified **SMEs**, **cybersecurity professionals**, and **policy makers** as the main target audiences. However, it became clear that certain sectors and regions, such as small and medium-sized enterprises in non-partner countries, were not adequately reached. Social media channels, although effective in providing updates, could be further optimized to encourage two-way engagement.

Additionally, the website also faced some challenges in maintaining engagement beyond initial visits.

The strategy needs to be revised to encourage return visits, with a focus on improving accessibility and providing more dynamic and engaging content.

3.3. Dissemination Activities and Results

The dissemination activities outlined in **D5.1** were successful in organizing several webinars and training sessions, which attracted attention.

However, the follow-up activities post-webinars could have been stronger to maintain momentum. Further, while the social media presence was established, the engagement rates were not as high as expected.

LinkedIn is used as the official social media tool for the project, given the traceability of the achieved results and the vast pool of people in the target sector.

As the project moves forward, there will be an increased emphasis on **retargeting** stakeholders through personalized content, ensuring that they stay engaged long term.

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. Updates to Communication Objectives

The purpose of this section is to outline the refined communication objectives, based on lessons learned from past activities, feedback from target groups, and the project's current phase. These updated objectives will help ensure that the project maximizes its impact, strengthens stakeholder relationships, and sustains long-term engagement with the OSCRAT tools.

4.1. Communication and Dissemination Objectives

The communication and dissemination objectives of OSCRAT have evolved, driven by feedback from stakeholders, project developments, and the need to enhance outreach and engagement across multiple sectors. The primary aim is to effectively communicate the value of OSCRAT's tools and encourage active participation in the project's progress.

Below are the refined and expanded objectives:

Increase Awareness and Visibility of OSCRAT Tools

One of the core communication goals is to significantly improve the awareness of European SMEs regarding OSCRAT tools. While the first efforts focused on successfully establish a strong foundation for OSCRAT's recognition, it is now crucial to enhance the visibility of the developed tools, the main result of the project.

Achieving this objective requires multi-channel outreach and strategic messaging to ensure that OSCRAT is recognized not only by SMEs but also by industry bodies, cybersecurity experts and policy makers.

Key actions include:

- **Targeted Awareness Campaigns**: launching region-specific campaigns, tailored to different SME needs across Europe, emphasizing the practical advantages of OSCRAT tools for compliance with the Cyber Resilience ACT (CRA).
- **Prominent Placement in Cybersecurity Forums**: OSCRAT tools should be positioned as a go-to resource within the wider cybersecurity community. Increased participation in **industry events**, **conferences**, and **policy discussions** will help boost visibility among industry leaders and regulators.
- **Media Outreach**: Leveraging press releases, media articles, and newsletters to raise awareness about the project's goals, results, and the impact of OSCRAT tools on SMEs and cybersecurity practices.

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.

Foster the Widespread Adoption of OSCRAT Tools

Raising awareness is only one of the bigger dissemination strategies. The goal is for SMEs to adopt OSCRAT's tools as an integral part of their business operations for CRA compliance.

As the tools become more refined and accessible, it is essential to create a compelling case for their adoption by demonstrating their value and their ability to be a useful tool which helps SMEs in achieving the alignment with the CRA Directive.

This can be achieved through the following strategies:

- **Engaging Training and Demonstrations:** Organizing interactive training sessions, webinars, and live demonstrations of OSCRAT tools. These sessions will showcase real-life use cases, showing SMEs how the tools can be easily integrated into their day-to-day activities.
- **Clear Value Proposition**: Simplifying the messaging around OSCRAT's tools to emphasize their immediate and long-term benefits, including cost savings, improved compliance, and enhanced cybersecurity.
- **Success Stories and Case Studies**: Publishing detailed case studies and success stories from early adopters of the tools. These stories should highlight SMEs that have successfully integrated OSCRAT tools into their operations and the tangible benefits they've experienced.

Elevate the Importance of Cyber Resilience and Compliance

A crucial part of the OSCRAT project is to highlight the importance of cyber resilience and compliance to the latest development in the sector for European SMEs.

The increasing frequency and sophistication of cyberattacks, coupled with the evolving regulatory landscape, make it essential for SMEs to adopt proactive rather than reactive strategies, to provide operational continuity.

OSCRAT tools are designed to help businesses navigate the complexities of compliance and resilience, but SMEs need to understand why this matters.

To achieve this, the communication strategy should focus on:

- **Educational Content**: Creating easy-to-understand resources that explain cyber resilience and the CRA compliance process. This could include white papers, guides, and infographics aimed at demystifying complex cybersecurity and regulatory concepts for non-experts.
- **Collaborations with Cybersecurity Experts**: Engaging with prominent cybersecurity experts and consultants to provide expert opinions on the significance of CRA compliance and how OSCRAT can help SMEs meet these requirements.
- **Policy Advocacy**: Engaging with policy makers and regulatory bodies to ensure that OSCRAT's tools are recognized as a key resource for CRA compliance and that their utility is advocated within official cybersecurity frameworks.

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.

Elevate the Importance of Cyber Resilience and Compliance

While reaching SMEs is vital, it is equally important to build and sustain strong relationship with industry stakeholder, cybersecurity experts and regulatory authorities to ensure that OSCRAT tools are continuously refined and remain relevant.

Engagement should go beyond dissemination and aim to foster **active collaboration** among all project partners and external stakeholders. This can be achieved by:

- **Ongoing Stakeholder Feedback**: regular updates and communications will be shared with project stakeholders, including SMEs and industry experts, to inform them about new developments, features and updates related to OSCRAT tools. This can be very effective starting from February 2026, after the OSCRAT tool Beta Release.
- **Direct Stakeholder Feedback**: through workshops and training sessions, stakeholder will have the opportunity to share feedback and suggestion on potential improvements to the tool, ensuring that OSCRAT continuously adapts to user needs.

Collaboration Through Targeted Dissemination Activities

Engagement efforts will be closely tied to the dissemination activities outlined in the project, ensuring that stakeholders, including regulatory bodies and industry associations, are actively involved in key events such as:

- **Workshops and training sessions:** designed to help stakeholders, particularly SMEs, understand the tools and provide valuable feedback on usability and functionality.
- **Information Sharing:** Regular project updates will be shared via established communication channels (e.g., newsletters, press releases) to keep all stakeholders informed about progress, deliverables, and upcoming milestones.

Long-Term Collaboration in Dissemination and Adoption

While the project itself will conclude at the end of its lifespan, the **long-term sustainability** of OSCRAT tools is essential. Ensuring that the tools continue to meet the needs of SMEs after the project ends requires ongoing visibility and collaboration with key stakeholders, such as:

- **SMEs**: Supporting SMEs in their ongoing use of OSCRAT tools to ensure compliance with the CRA.
- **Industry Associations**: Building relationships with industry associations to ensure that OSCRAT tools continue to be promoted and used by SMEs in their respective sectors.

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.

- **Regulatory Authorities**: Keeping regulatory bodies informed and engaged, ensuring that OSCRAT's tools are aligned with the evolving regulatory landscape and remain relevant for SMEs post-project.

By engaging stakeholders in this way, the dissemination strategy will not only achieve immediate project goals but will also build the foundation for the continued use and relevance of OSCRAT tools beyond the duration of the project itself, helping in the Exploitation efforts.

4.2. Additional New Objectives

New objectives have been introduced in response to the evolving nature of the project and feedback from stakeholders, with a pressing need to expand the outreach efforts to regions where SMEs have limited awareness or resources for CRA compliance.

Strengthen Outreach and Inclusiveness Across Europe

The communication and dissemination strategy must ensure that OSCRAT's visibility and impact extend across Europe, reaching relevant actors in cybersecurity and SME ecosystem.

While initial efforts have primarily focused on the consortium's partner countries, the updated strategy aims to strengthen the project's presence in a broader European context – ensuring that information, materials and results are accessible and relevant to a diverse audience of stakeholders.

The objective is not to create new regional initiatives but to enhance the inclusiveness and reach of OSCRAT's dissemination activities through more targeted communication, better use of existing channels and improved accessibility of project materials.

Encourage Active Participation from SMEs

SMEs should be encouraged to engage actively with the tools and the project's ongoing development, rather than being merely passive recipients of information. Key strategies to achieve this include:

- **Engagement through Feedback**: inviting SMEs to test OSCRAT tools, provide feedback and suggest new features and implementations.
- **User-Centered content**: Developing content that reflects real SME challenges and offers clear, actionable advice for using OSCRAT tools to solve those challenges.
- **Active Participation in Training Sessions and Workshops**: Encouraging SMEs to participate in interactive workshops and roundtables, where they can ask questions, share experiences, and gain deeper insights into OSCRAT tools.

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.

Ensure Balanced European Representation

Dissemination activities will highlight OSCRAT's European dimension, ensuring that communication materials, success stories, and project updates reflect the diversity of the consortium and its multi-country impact. The dissemination team will:

- Use case studies and testimonials from different partner countries to demonstrate how OSCRAT tools can be applied across various national contexts and industrial sectors.
- Promote cross-country visibility by featuring examples of activities and results from all consortium members in newsletters, social media posts, and the project website.

Collaboration Through Targeted Dissemination Activities

Engagement efforts will be closely tied to the dissemination activities outlined in the project, ensuring that stakeholders, including regulatory bodies and industry associations, are actively involved in key events such as:

- **Workshops and training sessions** designed to help stakeholders, particularly SMEs, understand the tools and provide valuable feedback on usability and functionality.
- **Information Sharing**: Regular project updates will be shared via established communication channels (e.g., newsletters, social media) to keep all stakeholders informed about progress, deliverables, and upcoming milestones.

In summary, the additional communication objectives introduced in this updated strategy aim to reinforce OSCRAT's visibility, inclusiveness, and long-term impact within the European cybersecurity and SME ecosystem. The focus is on ensuring that dissemination activities are not only wide-reaching but also balanced and accessible across all partner and non-partner regions.

By strengthening outreach efforts, simplifying communication materials, and leveraging the consortium's existing networks, OSCRAT will ensure that its tools and results are effectively shared with a diverse audience of SMEs, policymakers, and industry stakeholders.

The goal of these updated objectives is to foster awareness, encourage adoption of the OSCRAT tools and sustain engagement beyond project duration.

The Beta Release, expected in February 2026, will be a turning point for the dissemination activities. After the release, OSCRAT consortium can tailor the dissemination efforts to promoting the tool, showing practical examples on how to use it and how it can benefit SMEs in their compliance process.

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. Target Audience Analysis & Communication Channels

With the updated objectives, it is also important to revisit the target audience to ensure that all relevant stakeholders are effectively reached.

This section updates the previous audience segmentation and channels to be used, ensuring the correct stakeholders are targeted with tailored messages through appropriate channels.

5.1. Target Audience

The target audience remains largely the same, though with an emphasis on reaching broader SMEs across Europe and engaging more directly with non-traditional stakeholders.

As previously mentioned, the main goal of the next dissemination efforts will be tailored to the objective of the promotion of OSCRAT tool, highlighting the positive impact it can have in managing compliance processes for European SMEs.

- **SMEs in the digital product sector**: the primary end-users of OSCRAT tools. They include small and medium-sized businesses involved in creating, distributing or maintaining digital products that must comply with the Cyber Resilience Act.
- **Decision-makers and policymakers**: This group includes government bodies, industry regulators, and other policymakers who influence or oversee cybersecurity legislation and standards.
- **Cybersecurity experts and consultants**: They play an advisory role to SMEs, helping them implement and adapt cybersecurity measures. Engaging this group is crucial for broader tool adoption and influence.
- **Industry associations**: These organizations can help promote OSCRAT tools to their members, provide validation, and help integrate the tools into standard practices.

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. Optimization of Dissemination Tools & Channels

OSCRAT Website

The OSCRAT website serves as the project's main public interface, ensuring transparency and providing stakeholders with key information about the project's objectives, progress and consortium composition.

Rather than functioning as a repository of resources, the website is a gateway to information, acting as a reference point for visitors seeking information on the project activities and status.

The website, with it's contact section, is also used to gather information about potential stakeholders and update the project's mailing list, used to disseminate project materials and communications (i.e. press releases & newsletters).

The new approach involves the introduction of more dynamic content, tailored to user needs, such as case studies and success stories, to keep users engaged and return frequently.

Specifically, **videos from the project's training sessions and workshops** will be made publicly available through the **official OSCRAT YouTube channel** and subsequently **embedded within the website**.

This integration will:

- Extend the reach of the project's training content, offering SMEs and stakeholders who could not attend live sessions the opportunity to access the same material at any time.
- Enhance engagement and visibility, as embedded YouTube videos allow for seamless interaction and improved analytics while maintaining OSCRAT's branding consistency.
- Ensure sustainability of project outcomes, by preserving a long-term digital record of the project's knowledge-sharing and capacity-building efforts.

All multimedia content shared through the website will undergo validation and quality control under the coordination of **PMF Research**, ensuring coherence with the project's communication plan and compliance with EU visibility standards.

OSCRAT Social Media: LinkedIn

LinkedIn is the project's primary social media channel for dissemination and stakeholder engagement.

Its professional nature, strong focus on innovation, policy and research make it the most suitable platform to reach SMEs, policymakers, cybersecurity experts and industry associations.

The OSCRAT communication approach on LinkedIn focuses on:

- Raising awareness about the project's progress, milestones, and key achievements.
- Promoting participation in events such as training sessions and workshops.
- Highlighting consortium expertise through posts featuring partners' roles and contributions
- Fostering discussion around cybersecurity and CRA-related topics, thus positioning OSCRAT as a credible actor in the European cybersecurity ecosystem.

Content production and publication are coordinated by PMF Research, to ensure consistency with the visual identity and communication guidelines.

Consortium partners are strongly encouraged to share and amplify OSCRAT posts through their social media channels, to reinforce visibility and outreach at a European level.

At the time of writing the document, the page has 170 followers and a total of 17 posts.

Starting from November 2025, LinkedIn official page will also be used to disseminate newsletters and press releases, enhancing the reach and potential requests for collaboration.

Press and Media Communication

Press releases and media communication remain essential components of OSCRAT's dissemination efforts, helping extend visibility beyond digital channels and reach new stakeholder groups.

Planned actions include:

- Preparing press releases for important project achievements.
- Disseminating information through partners' institutional channels and specialized European outlets in the fields of cybersecurity, digital innovation, and SME development.
- Ensuring all communication materials comply with EU visibility and acknowledgment requirements, including correct references to the

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.

funding programme and the European Cybersecurity Competence Centre.

To engage active participation from the OSCRAT Consortium, press releases and newsletters content is agreed upon the consortium, with the aim to provide relevant information, especially regarding the status of the development, achieved results and participation in relevant events.

Content	Date	Channel
Press release n.1	31/03/2025	Brevo, LinkedIn (post)
Newsletter n.1	28/04/2025	Brevo, Website
Newsletter n.2	28/05/2025	Brevo, Website
Newsletter n.3	11/07/2025	Brevo, Website
Newsletter n.4	12/09/2025	Brevo, Website

Table 1: OSCRAT – Press Releases and Newsletters

During the next 6 months of project implementation, n.8 additional newsletters will be created and disseminated, using Brevo, LinkedIn official page and Brevo mailing lists.

Work Package	Nov-25	Dec-25	Jan-26	Feb-26	Mar-26	Apr-26	May-26
Work Package 1 - Project Management							
T. 1.1. - Product discovery and low level scope definition							
T. 1.2. - Develop a project plan							
T. 1.3. - Establish communication channels							
T. 1.4. - Monitor progress							
T. 1.5. - Stakeholder engagement							
T. 1.6. - Project updates							PR4
Work Package 2 - Requirements gathering and analysis							
T. 2.1. - Define scope							
T. 2.2. - Identify requirements							
T. 2.3. - User needs							
T. 2.4. - Analyze data							
T. 2.5. - Stakeholder Alignment and Project Requirements Refinement	NL5						
Work Package 3 - Software Design and Development							
T. 3.1. - Design							
T. 3.2. - Product Design (Architecture)							
T. 3.3. - Development							
T. 3.4. - Integrations					PR3		
T. 3.5. - Testing	PR2						
T. 3.6. - Documentation					NL7		NL8
Work Package 4 - Stakeholder engagement							
T. 4.1. - Workshops and International CRA Event							
T. 4.2. - Training sessions							
T. 4.3. - Use-cases and best practices			NL6				
Work Package 5 - Dissemination & Exploitation							
T. 5.1. - Communication & Dissemination Strategy							
T. 5.2. - Creation and adoption of OSCRAT visual identity							
T. 5.3. - Dissemination activities							
T. 5.4. - Development of the Exploitation Plan							

Figure 1: OSCRAT – Upcoming Press Releases and Newsletters

The image above highlights those responsible for creating the content of upcoming newsletters and press releases.

The structure was decided upon to link the content of the informational material to the key activities of the project (e.g., the closure or opening of new development phases).

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.

Videos and Webinar Content

As foreseen in the project's Description of the Action, the OSCRAT dissemination strategy includes the production and publication of **two official videos** on the project's YouTube channel, which will be created and launched in **December 2025**.

1. **Video 1 – Introduction to the OSCRAT Project**
    a. Publication period: second week of December 2025
    b. Objective: To provide a concise and visually engaging overview of the OSCRAT project, its objectives, implementation phases, and key results achieved to date.
    c. Content:
        i. Brief presentation of the consortium and project coordination.
        ii. Explanation of OSCRAT's purpose within the European cybersecurity ecosystem.
        iii. Overview of the project's main work packages and milestones.
        iv. Expected impact on SMEs, industry, and policy-making communities.

The video will serve as a general introduction for new stakeholders and as a communication tool for presentations, events, and online dissemination.

2. **Video 2 – OSCRAT Tool Demonstration (Demo Video)**
    a. Publication period: to be defined in coordination with WP3 partners
    b. Objective: To present a short and practical demonstration of the OSCRAT tool, its features, and its usability for SMEs
    c. Content:
        i. Step-by-step overview of the tool's interface and functionalities.
        ii. Explanation of how the tool supports CRA compliance for SMEs.
        iii. Brief showcase of potential user scenarios and benefits.

This video will highlight the technological achievements of the project and contribute to the promotion of OSCRAT's open-source tools during dissemination and training activities.

This activity is intended to support the overall objective of enhancing visibility accessibility and engagement among the project's key target audience – particularly SMEs, cybersecurity experts and policymakers – by using visual and dynamic formats to communicate the project's progress and results.

The use of audiovisual content contributes to a more inclusive and lasting dissemination impact, as it allows complex information about OSCRAT tools and activities to be presented in an engaging, clear, and easily accessible format. All videos will be produced under the coordination of **PMF Research**, in close

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.

collaboration with the partners responsible for the technical development (WP3).

Training Session Integration

In addition to the two main videos, the recording of **Training Session n.4**, which will take place on the 8th of December 2025, will also be published on the official YouTube channel and made available through embedding in the OSCRAT's official website.

The **embedding of the training video on the OSCRAT website** will allow stakeholders — particularly SMEs and participants who cannot attend the live session — to access the material asynchronously. This ensures broader participation, reinforces the project's visibility, and supports the overall capacity-building goals of OSCRAT.

Coordination and Quality Assurance

All audiovisual materials will be produced in English, following a **script and storyboard approved by PMF Research** and validated by the consortium prior to publication. PMF Research will ensure that:

- The content accurately reflects OSCRAT's objectives and results.
- Visual and textual elements are consistent with the OSCRAT brand identity and EU visibility guidelines.
- The videos maintain professional quality standards suitable for institutional communication.

Consortium partners will contribute to the content definition and review process to ensure technical accuracy (WP3 Leaders for the demo video) and comprehensive representation of the project's multidisciplinary scope.

Expected Impact

The use of video content represents a key enhancement to OSCRAT's dissemination strategy, ensuring wider accessibility and long-term visibility of the project's results.

By combining the YouTube channel with the embedding of videos on the official website, OSCRAT will be able to:

- Strengthen its outreach and engagement with non-specialist audiences.
- Support SMEs and stakeholders in understanding the project's objectives and practical outcomes.
- Guarantee that the project's communication materials remain publicly available and reusable after the end of 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.

5.3. Consistency and Coordination

All dissemination activities will continue to be managed in a centralized and coordinated manner to ensure massage consistency across the various channels.

As leader of Work Package 5, PMF Research is responsible for:

- Overseeing content planning, approval and publication.
- Guaranteeing that all outputs reflect the OSCRAT visual identity and tone.
- Supporting partners in adapting communication through its local and professional networks, reinforcing OSCRAT's reach wile adhering to a single and unified communication strategy.

The activities are already planned until the project's end date, with constant communication between dissemination responsible for each of the project beneficiary.

The choice of appointing a person responsible for communication activities permits a faster communication and approval of the published content, ensuring a reliable process for content production, checks and approval.

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. Updates to Dissemination Activities and Sustainability

This section outlines the updated dissemination priorities for the second phase of the project and measures to guarantee long-term visibility and sustainability of the OSCRAT tools and results.

6.1. Enhanced Dissemination Efforts

Following the successful establishment of OSCRAT visual identity, website and social media channels, dissemination activities will now focus on showcasing tangible results and promoting active engagement among target audiences.

The second phase of dissemination will therefore emphasize content quality, targeted messaging and coordinated communication across partners to ensure consistent European visibility.

Key priorities are:

- **Showcase OSCRAT achievements**: dissemination activities will increasingly showcase the concrete progress made under WP2, WP4 and WP4. Posts, newsletters and articles will summarize technical outcomes in a non-technical language, to make the content accessible to SMEs and other stakeholders.
- **Promoting events and training activities**: workshops and training sessions will continue to serve as important dissemination vehicle, engaging SMEs and cybersecurity practitioners directly. Each event will be followed by communication actions on LinkedIn and the project website to summarize key insights and share information on participation opportunities.
- **Leveraging audiovisual content**: the launch of the official OSCRAT YouTube channel in December 2025 will significantly enhance the project's dissemination reach. Videos – including a presentation of the project – will serve as a powerful tool to communicate information in an engaging and understandable format, extending the visibility of results to audiences that might not regularly access written materials.
- **Expanding visibility through partner networks**: each consortium member will continue to disseminate project information through its institutional channels, events and professional contacts, ensuring that OSCRAT's messages reach a broad ad diverse European audience. PMF Research will continue in its efforts to coordinate and validate all dissemination materials to maintain message coherence and alignment with visual identity guidelines.
- **Maintaining alignment with the EU visibility rules**: All materials, events, and public communications will continue to comply with the European Commission's communication and dissemination guidelines, ensuring

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 appropriate acknowledgment of EU funding and adherence to branding and disclaimer requirements.

These updated priorities will ensure OSCRAT transitions from general awareness raising to the promotion of concrete results, strengthening stakeholder engagement by using hands-on on the results and increasing the project's visibility in European cybersecurity ecosystem.

6.2. Building long-term Sustainability

Beyond dissemination, sustainability is a key objective for ensuring that OSCRAT's results and impacts persist after the project's completion. Sustainability, in this context, refers to continued availability, visibility and usefulness of the tools and knowledge generated by the project.

To guarantee this, OSCRAT's sustainability approach focuses on the following elements:

- **Durability of communication assets**: the OSCRAT website and social media channels will remain active after the end of the project, ensuring that information about the project's results remain accessible to the audience. The official OSCRAT YouTube channel and website will continue to host the training and dissemination videos, preserving a permanent record of the project's communication and knowledge transfer.
- **Ongoing use of the OSCRAT Tools**: dissemination efforts will focus on actively promote the use and adoption of the OSCRAT tools among SMEs, digital innovation hubs and industry bodies. By encouraging their integration into business and compliance workflows during the project's lifetime, OSCRAT will foster a self-sustaining user base that continues to apply and improve the tools beyond the project's duration.
- **Open-Source Approach as a driver of sustainability**: a major contributing factor to the long-term sustainability of OSCRAT is the open-source nature of its tools. By making the software freely accessible, modifiable and reusable, OSCRAT ensures that it remains a living and adaptable solution even after the project concludes. This approach not only reduces barriers for SMEs — enabling them to adopt and tailor the tools to their specific needs — but also allows external developers, cybersecurity experts, and organizations to contribute to further improvements. The open-source model thus guarantees continuous evolution, encourages community-driven innovation, and prevents technological obsolescence, extending the project's impact well beyond its formal timeline.
- **Institutional visibility and network synergies**: consortium partners will maintain and integrate OSCRAT's outcomes within their institutional and professional networks, ensuring that methodologies, frameworks and communication assets remain visible and relevant. Partners'

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.

ongoing participation in European cybersecurity and digital innovation initiatives will help keep the project's legacy active and recognized at both national and EU levels.

- **Training materials and videos as permanent resources**: The recordings of training sessions and workshops, embedded on the website via the official YouTube channel, will serve as long-term dissemination tools. These materials will remain available to SMEs, practitioners, and stakeholders, ensuring that OSCRAT continues to support awareness and capacity-building activities after the end of the project.
- **Continuous engagement through LinkedIn**: the OSCRAT LinkedIn page will continue to serve as a reference point for updates and to contact OSCRAT's consortium. Posts and discussions may continue after the project's formal conclusion, maintaining visibility and supporting the ongoing exchange of knowledge and best practices within the OSCRAT community.

Through this multidimensional approach - with the combination of the durability of different communication assets, the open-source model and the active involvement of consortium partners – OSCRAT ensures that its results will remain accessible, reusable and relevant in the long term. This will secure project's contribution to enhancing cyber resilience and compliance among European SME well beyond its funded duration.

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. Integration with the Exploitation Plan

Dissemination and exploitation are closely interconnected within the OSCRAT framework.

While dissemination efforts focus on raising awareness and ensuring visibility of the OSCRAT achievements, exploitation activities aim to maximite the use, adoption and long-term impact of the project's results.

This section outlines how the updated **Dissemination Strategy (D5.2.)** directly supports and complements the **Exploitation Plan (D5.3.)**, ensuring that the communication efforts implemented under WP5 contribute to sustained use and real-world application of OSCRAT outcomes.

7.1. Alignment between Dissemination and Exploitation

The dissemination action outlined in this deliverable play a strategic role in preparing the ground for the exploitation of project's results.

Every communication activity contributes to positioning OSCRAT as a reliable, open-source solution that supports European SMEs in achieving Cyber Resilience Act (CRA) compliance.

The alignment between dissemination and exploitation is achieved through the following mechanism:

- **Visibility leading to adoption**: dissemination raises awareness among the target audiences about the existence, accessibility and benefits of OSCRAT's tools. By increasing visibility, dissemination opens the route for exploitation by creating informed and interested users who are willing to adopt the results.
- **Targeted Communication to Key Stakeholders**: the project's communication channels (especially LinkedIn and partner networks) are used to reach potential adopters and multipliers, such as SME clusters, cybersecurity associations and policy actors. These groups play an essential role in facilitating the uptake and replication of OSCRAT tools within their ecosystems.
- **Promotion of Usability and Value Proposition**: Dissemination messages emphasize the practical advantages of OSCRAT tools — simplicity, accessibility, and compliance support. These elements are crucial to the exploitation phase, as they translate technical results into tangible benefits for users, thus encouraging their integration into SMEs' daily operations.
- **Reinforcement through Training and Demonstration**: Training sessions and workshops serve as bridges between dissemination and exploitation. By demonstrating how the tools can be applied in real scenarios, these activities help potential users understand the practical value of OSCRAT and build confidence in adopting the solution.

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.

7.2. The role of the Open-Source model in Exploitation

The open-source nature of OSCRAT's tools is central to both dissemination and exploitation strategy.

By ensuring the software remains freely available, adaptable and expandable, OSCRAT removes the typical barrier that often limit the adoption of cybersecurity compliance tools in some ecosystems, like SMEs.

The open-source model provides several key advantages for exploitation:

- **Ease of Access:** SMEs and organization can freely access, test and implement the OSCRAT tool without financial or licensing constrains, making it easier to integrate the tool into their compliance and cybersecurity practices.
- **Community-Driven Improvement:** developers, cybersecurity experts, and researchers can continue to refine and expand the tool, adding new functionalities that respond to emerging regulatory and technological needs.
- **Sustainability Beyond the Project Duration:** as the source code remains available, the project's outcomes can evolve and remain relevant well after the project's end, ensuring ongoing exploitation and impact.

7.3. Synergy between consortium partners

The collaboration between consortium partners is a fundamental enabler of successful exploitation.

Each partner contributes to specific expertise and network access that reinforces both dissemination and exploitation goals.

Key synergies include:

- **PMF Research,** as Work Package 5 leader, ensures strategic communication coordination and promotes results through institutional and industry networks.
- **Lukasiewicz AI & Oves Enterprise,** leading Work Package 2 & Work Package 3 respectively, provide technical foundations for the exploitation of the OSCRAT tools, ensuring their quality, reliability and usability.
- **DIH Trakia & Unicis.Tech** strengthen the link between dissemination and market uptake through their networks of SMEs, innovation hubs and digital ecosystems.
- **Enersec** contributes to promoting cybersecurity-related use cases and ensuring that exploitation aligns with real-world industrial needs.

This coordination ensures that dissemination activities feed directly into exploitation pathways, transforming awareness and visibility into tangible adoption and practical use of OSCRAT's 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.

7.4. Supporting long-term Exploitation through communication

Communication activities will continue to play a role even after the formal end of the project.

The persistence of the website, LinkedIn page, and YouTube channel will ensure that OSCRAT's results remain discoverable and usable by future stakeholders.

Specifically:

- The **OSCRAT website** will continue to provide institutional visibility and direct users to the open-source repositories.
- The **LinkedIn page** will remain active as a reference point for sharing updates, testimonials and community feedback.
- The **YouTube channel** will host explanatory and demonstrative content, supporting future users in understanding and adopting the tool.

Through these sustained communication assets, OSCRAT will continue to facilitate the exploitation and long-term adoption of its results, supporting the goal of the European Cyber Resilience Act and contributing to enhance the cybersecurity maturity of European SMEs.

7.5. Expected Impact

The strong integration between dissemination and exploitation within OSCRAT ensures a high degree of **continuity, accessibility, and real-world relevance**.

As dissemination drives awareness and interest, exploitation transforms visibility into adoption — ensuring that the project's outcomes have measurable, lasting benefits.

The expected impacts include:

- Increased **adoption and reuse** of OSCRAT tools by SMEs and cybersecurity practitioners across Europe.
- Strengthened **alignment between project results and EU cybersecurity policy objectives**.
- Creation of a **sustainable and collaborative ecosystem** around OSCRAT's open-source tools.
- Enhanced **European leadership** in cybersecurity innovation and compliance support for SMEs.

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. Conclusion

The updated Communication and Dissemination Strategy presented in this deliverable reflects OSCRAT's transition from the initial awareness phase to a more mature stage focused on result-driven communication, stakeholder engagement and long-term visibility.

Through the coordinated efforts of all consortium partners, OSCRAT has established a solid foundation of communication tools – including a clear visual identity, a professional website, an active LinkedIn presence and the upcoming YouTube channel – that will ensure effective outreach and sustainable dissemination throughout the project and beyond.

This deliverable defines how dissemination activities will evolve to accompany the project's technical progress and growing visibility within the European cybersecurity ecosystem.

The key priorities include:

- Promoting the achievements and concrete outputs of the project, especially the OSCRAT open-source tools developed under WP3.
- Enhancing stakeholder engagement through accessible communication formats such as videos, workshops, and online campaigns.
- Ensuring coordinated and consistent communication across partners and channels under the leadership of PMF Research.
- Strengthening sustainability and exploitation links, ensuring that dissemination continues to support the adoption and long-term use of the project's results.

The integration of audiovisual materials, particularly the two official videos to be published on YouTube and embedded on the project's website, represents an important step toward improving accessibility and engagement.

These resources will provide both educational value and long-term visibility for the project, reinforcing OSCRAT's mission to support SMEs in achieving **Cyber Resilience Act (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.

9. Next Steps

Following the submission of this deliverable, the next steps for WP5 and the consortium will focus on implementing and monitoring the dissemination and communication activities outlined in this updated strategy. Key actions include:

- **Launching the Official OSCRAT YouTube Channel**: scheduled for December 2025. This channel will serve as the main platform for hosting and disseminating all project videos, allowing for the embedding of content on the OSCRAT website and ensuring a broader accessibility of materials for SMEs and stakeholders. The launch will coincide with the publication of the first official project video.
- **Finalizing and publishing the official videos**: the first official video will present the OSCRAT project, its objectives, structure and achieved milestones. This video, planned for release during the second week of December 2025, will introduce the project to a wider audience and act as a cornerstone of the project's communication efforts. It will highlight the cybersecurity landscape and its role in supporting SMEs compliance processes with the Cyber Resilience Act (CRA).
- **Upload of the recordings from training sessions and workshops**: the embedding of these recordings on the OSCRAT website will make the content accessible to all target groups who could not attend the live event, supporting OSCRAT's capacity-building and awareness-raising activities.
- **Publication of additional multimedia content**: Following the first release phase, further video materials will be prepared and uploaded in coordination with WP3 and WP4 partners. These will include:
    - **Training Session n.4 Video** – recording of the final OSCRAT training session, summarizing lessons learned and participant feedback.
    - **Workshop n.1 Video** – highlights and key insights from the first OSCRAT workshop, focusing on practical implementation of CRA compliance and project outcome.
    - **Beta Release Demo Video** – a demonstration of the OSCRAT tool's beta version, presenting its main features and functionalities to SMEs and stakeholders.
    These videos will collectively reinforce the visibility and usability of OSCRAT results, ensuring that project outcomes are presented in an engaging and easily accessible format.
- **Ongoing Dissemination and Partner Coordination**: The consortium will continue promoting OSCRAT's achievements and activities through LinkedIn and partner institutional channels. Dissemination content will highlight key project milestones, training events, and the release of new materials, ensuring coherent and

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.

continuous visibility across Europe.
PMF Research will maintain overall coordination of the dissemination activities, guaranteeing consistency of communication materials and compliance with EU visibility requirements.

- **Monitoring, Evaluation, and Synergy with Exploitation (WP5 & WP3)**: PMF Research will oversee the monitoring of dissemination performance and ensure that each activity contributes to the project's exploitation objectives. The coordination between WP5 (Dissemination & Communication) and WP3 (Tool Development and Testing) will be particularly important to ensure that communication outputs — such as the beta release demo — effectively support the uptake and real-world use of the OSCRAT tool.

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 – Updating of the communication and dissemination strategy

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.