OSCRAT

Open-Source Cyber Resilience Act Tools

D.5.1.

OSCRAT Communication, Dissemination Strategy & Exploitation Plan

Submission date: 31 May, 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.

OSCRAT: identity and communication toolkit

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act tools
Name	OSCRAT Communication, Dissemination Strategy & Exploitation Plan
Number	D. 5.1.
Work package	WP5 – Dissemination & Exploitation
Due Date	31/05/2025
Submission Date	31/05/2025
Lead Partner	PMF Research
Author name(s)	Giuseppe Fabio Ursino
Version	1.0
Status	Draft
Type:	☒ R - Document, Report ☐ DEC – Websites, patent filings, videos, etc ☐ DEM – Demonstrator, pilot, prototype
Dissemination level:	☒ PU - Public ☐ SEN - Sensitive

Co-funded by the European Union

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	04/03/2025	PMF	First draft
0.2	28/04/2025	PMF	Final draft

Abstract

The current document presents and defines a comprehensive communication, dissemination and exploitation strategy tailored on OSCRAT goals and values.
Through this plan, the reader will be able to understand deeply:

- OSCRAT visual identity;
- Target audience and specific key messages to be delivered, based on their needs and opportunities;
- Communication tools, channels and materials, among which website, newsletters, and press releases;
- Dissemination tools and channels, including events, scientific publications and public deliverables;
- An overview of the exploitation strategy.

Keywords

- **Communication**
- **Dissemination**
- **Exploitation**
- **Sustainability**
- **Communication Plan**
- **Communication strategy**

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.
- Project: 101190180

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.

Sommario

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.

List of Figures

List of Tables

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

1.1. Introduction

The purpose of this document is to present and define a comprehensive communication, dissemination and exploitation strategy tailored on OSCRAT goals and values.

It serves as Deliverable 5.1. – OSCRAT Communication, Dissemination Strategy & Exploitation Plan, which tackles various aspects in a holistic manner. These include:

- OSCRAT Brand identity;
- Target audience and specific key messages to be delivered, based on their needs and opportunities
- Communication tools, channels and materials;
- Dissemination tools and channels;
- An overview of the exploitation strategy.

These components are defined throughout the entire Work Package 2, OSCRAT Communication, dissemination and ecosystem building, particularly in Task 2.1 - Communication tools and strategy, as well as Task 2.3 - Community events, networking, and matchmaking.

The current document and, thus, communication, dissemination and exploitation plan aim to establish a strategy, including channels, tools, and content to reach and engage a wide range of stakeholders, ensure broad dissemination of project activities and results, and target the intended audience effectively.

The communication, dissemination, and exploitation strategy, along with related activities, will strive to achieve the following:

- Effectively reach the main target groups of the project through appropriate channels and messages, raising awareness about the project and its opportunities and encouraging participation;
- Provide valuable information about project activities, events, value propositions, services and results to stakeholders;
- Identify and collaborate with similar initiatives and organisations sharing a similar mission;
- Participate in ecosystem events to increase the visibility of 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.

Therefore, this deliverable consolidates the outcomes of the Task 1.5. – Stakeholder engagement, Task 4.1 – Workshops and International CRA Event, Task 5.1. – Communication & Dissemination Strategy and Task 5.2. – Creation and adoption of OSCRAT Visual Identity.

1.2. Methodology

The OSCRAT team has meticulously developed a specialized and innovative methodology for effectively communicating and disseminating the project's activities and results to stakeholders and direct users. This strategy, crafted with the active participation and contributions from every member of the Consortium, strategically engages the target audience at three distinct levels:

- **Locally**;
- **Nationally**;
- **Internationally**.

This tiered approach ensures that the outcomes of the OSCRAT project will profoundly impact key stakeholders across various regions.

The overarching goal of this communication strategy is to pinpoint the most effective ways to connect with stakeholders and direct users, with a keen focus on the crucial importance of their engagement in the project. The strategy is meticulously designed to not only disseminate the achieved results but also to ensure that the OSCRAT tools are successfully established among the beneficiaries and utilized in the most effective manner possible.

In alignment with these objectives, the lead partner, PMF RESEARCH, in collaboration with the Consortium, pledges to adopt a proactive stance. The Consortium is committed to implementing an all-encompassing communication strategy that aims to elevate awareness and actively engage key participants throughout the project duration. This strategy will encompass a series of carefully planned communication activities, which will feature engaging and compelling messaging both in substance and form.

To further this aim, the Consortium will develop and present a comprehensive outline detailing a variety of actions and tools designed to reach an extensive audience and achieve significant impacts. These efforts will be supported through collaborative endeavors of all partners, ensuring that each phase of 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.

communication strategy not only reaches but also resonates with a broad spectrum of audiences, thereby maximizing the project's overall effectiveness and impact.

In conclusion, through these concerted and strategic efforts, the OSCRAT project is set to make a lasting impression on its intended audiences, fostering an environment of informed engagement and active participation that will propel the project towards achieving its set goals.

The primary focus of dissemination efforts for the OSCRAT project will be on sharing key findings, progress, milestones and challenges within the target groups: European SMEs, policy-makers, regulatory bodies, national and international cybersecurity authorities and other relevant stakeholders.

Digital Innovation Hubs, cybersecurity experts, and industry associations will be involved in disseminating project outcomes and promoting the OSCRAT platform to a broader audience. This will be achieved through collaborations with relevant organizations in each partner country, leveraging the strong relationships of partners like DIH Trakia in Bulgaria and Unicis.Tech in Estonia.

The project will also reach general public through awareness raising campaigns in each partner's country, utilizing PMF and Oves network across multiple countries.

The dissemination, communication, and exploitation strategy of this project is meticulously crafted to ensure that the outputs and results are communicated effectively and have a sustainable impact across Europe. Our strategy encompasses a diverse range of activities and strategic engagements to achieve the following objectives:

- **Implementing a Comprehensive Series of Actions**: this objective aims to deploy a robust series of outreach and communication measures to ensure engagement with the most relevant and broad audience possible. This strategy includes:
    - ***Digital Marketing***: utilizing SEO, social media and email campaigns to reach a wide audience of SMEs and stakeholders across Europe;
    - ***Conferences, Workshops and Training Sessions***: organizing and participating in industry and academic conferences to present project findings and progresses, engaging with stakeholders;
    - ***Public Engagement Initiatives***: hosting webinars and public discussions to facilitate broader community involvement and raising awareness;

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.

- **Increasing Awareness about OSCRAT's Core Topics**: by raising the profile of events and services related to the project's main topics, this objective seeks to draw in a more extensive base of interest and involvement. It includes leveraging media exposure, online discussions, and networking events specifically tuned to highlight OSCRAT's initiatives and breakthroughs;
- **Enhancing Stakeholder's visibility**: this involves strategies aimed at amplifying the presence and influence of project stakeholders within the community and related industries by:
    - ***Strategic Public Relations***: Developing and maintaining relationships with key industry influencers and media to promote the project's aims and successes;
    - ***Stakeholder Engagement Activities***: regularly engaging with SMEs, cybersecurity experts and regulatory bodies to ensure their roles and contributions are visible and valued;

- **Contributing to Knowledge Development**: the OSCRAT project aims to make significant contributions to the knowledge base surrounding cybersecurity practices and CRA compliance by:
    - ***Dissemination of findings in accessible format***;
    - ***Best practices and Innovative methodologies***: sharing case studies and successful strategies through workshops, online platforms meeting and industry publications.

- ***Ensuring accessibility if results to main actors***: it is crucial that the results of the OSCRAT project are easily accessible to a diverse range of actors within the European territory. This goal will be achieved through the following means:
    - ***Open-Source tool Development***: the main result of the project will be an open-source, freely available tool that assists European SMEs in adhering to CRA compliance procedure. This tool will be developed with user-friendliness in mind, ensuring that it can be easily adopter and implemented by business of all sizes;
    - ***Training and support***: to maximize the tool adoption and effective use, OSCRAT members will provide comprehensive training sessions, user guides and ongoing support. This will include tutorial, live Q&A sessions and dedicated support in utilizing the tool effectively;

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.

- ***Partnerships with Industry Bodies***: collaboration with industry associations and regulatory bodies will help promote the tool and encourage its integrations into standard business practices across Europe.

This strategic emphasis guarantees that the technological outputs of the OSCRAT project are not only sophisticated and functional but also freely available, aiding a broad spectrum of European SMEs in achieving compliance with the CRA efficiently and economically. This approach is poised to substantially enhance the overall cybersecurity stance and resilience of the European digital marketplace.

This dissemination strategy is intricately linked to a robust **Exploitation Plan**, crafted to optimize the long-term impact and practical application of the OSCRAT tool. The key steps in creating this plan include:

- ***Evaluating the project outputs***: a comprehensive assessment of the OSCRAT project's deliverables will be carried out to determine if modification, enhancements or exclusions are needed, ensuring they resonate with market demands and meet stakeholder's expectations;

- ***Managing and Coordinating partner Contributions***: it is crucial to oversee and coordinate the activities of all project partners, in order to ensure they align with the OSCRAT project's objectives and adhere to high standards of quality;

- ***Performing Value Proposition Analyses***: Each key deliverable of the OSCRAT Project will be subject to an in-depth value proposition analysis. This step will confirm that the advantages and benefits of the project's outcomes are effectively communicated and comprehended by potential users and stakeholders. This analysis will highlight the ways in which these results facilitate CRA compliance and bolster cybersecurity measures within European 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.

2. Brand identity

2.1 Introduction

The OSCRAT Brand Identity, including brand voice and visual identity, has been meticulously crafted to embody the project's core mission and values, aiming to be engaging, people-centred, and professional.

The brand voice of OSCRAT is strategically tailored to create a strong connection with its primary audience—European SMEs. It is designed to be engaging and supportive, while maintaining a professional demeanour. This distinct brand identity and voice ensure that OSCRAT's manner of communication clearly conveys its purpose and the benefits it provides, allowing stakeholders to fully grasp the importance of the project in fostering cybersecurity awareness and CRA compliance.

The visual identity includes all the graphic elements that distinguish OSCRAT's communications.

2.2 Logo

Central to this identity is the OSCRAT logo, which has been developed in multiple versions to ensure it is suitable for various applications, ensuring that the brand's core values are consistently communicated across all platforms.

The OSCRAT brand originates from a conceptual idea focused on protecting European small and medium-sized enterprises from online threats. The pictogram depicts a shield, a symbol of security, adorned with the stars of the European Union.

Figure 1: OSCRAT Logo Composition

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 order to recall OSCRAT main topics and mission, two primary brand colours combinations have been selected for the **logo**:

- ***Blue/White***: commonly associated with security, reliability and stability, this is an ideal choice for this project. Blue colour is universally associated with calm and serenity. These associations can strengthen the perception of a secure and protected environment, essential for a cybersecurity project. Blue is also predominantly present in the European flag, using it in a European funded project can reinforce the visual identity and the associated with EU initiatives and symbols, promoting a sense of unity;
- **Black/White**: this colour combination offers advantages in logo design, especially in professional and technological contexts, such as cybersecurity. The simplicity and clarity of this colour combination allows the logo's message and symbol to stand out clearly, ensuring that the logo is immediately recognizable. The versatility of this colour combination also ensures effectiveness across all surfaces, whether printed on paper or used in promotional material. Although black & white don't offer very much of emotional stimuli, the neutrality can be an advantage in sector such as cybersecurity because a neutral palette conveys stability and seriousness, key points in OSCRAT activities. Indeed, Black and white are considered neutral and universally acceptable across different cultures. This makes them particularly suitable for international or global organizations, such as those operating in the cybersecurity field at a European or worldwide level.

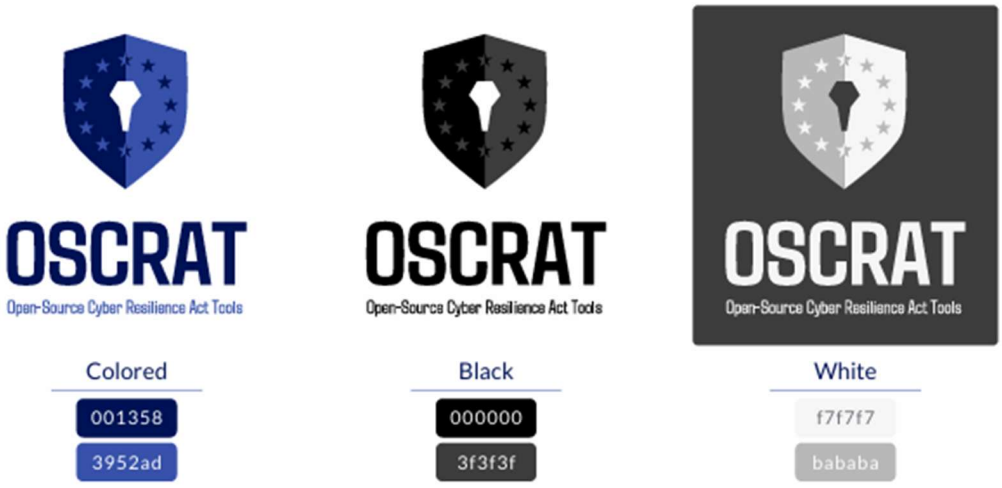

Figure 2: OSCRAT Logo Colour codes

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:OSCRAT Horizontal Logo – Colour Variants

Figure 4: OSCRAT Vertical Logo – Colour Variants

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 regards the Typography, the choice of "**Agadisma**" font for our project was driven by several considerations:

- ***Modern and Innovative design***: the font stands out as innovative but also classic font, making it particularly suitable for projects, presenting a forward-thinking image;
- ***Enhanced Legibility***: one of the main reasons for choosing this font is its exceptional legibility, featuring distinct character shapes and spacing, enhancing its adaptability and readability across various media and devices;
- ***Professionalism***: Agadisma exudes a professional quality that lends credibility and authority to OSCRAT's communication. In the context of cybersecurity, where professionalism and precision are extremely valued, this font reinforces the serious nature of the project's work and the consortium commitment to excellence.

Figure 5: OSCRAT Logo Font – Agadisma

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.

2.3 Documents templates

For the templates of the documents (docx, ppt and deliverables), **Montserrat** font has been selected as a typeface, with **9,5 sizes**. Such font, is very adaptable, thanks to its aesthetic simplicity and can be used in various context including websites, publishing, branding, editorial, print, posters and so on.

In order to guarantee a coherent internal and external communication, templates and materials have been produced since M1 and progressively updated and improved according to project partners' needs, among which:

- ***Deliverables Word Template***: created for the purpose of writing reports, strategies and deliverables;
- ***General Word Templates***: created for the purpose of being used in agendas, notes, meeting minutes, etc.;
- ***PowerPoint Template***: created for the purpose of visual aid in terms of presenting project's main objectives, values, strategies, both internally and externally;
- ***Newsletter template***;
- ***Press Release template***: to be uploaded in OSCRAT website within the News section and also disseminated in partner's social media accounts and websites.

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 6: OSCRAT - Deliverables Word Template

The header of the Deliverables Word template contains the project, ECCC and Co-Funded logos, following the European Cybersecurity Competence Centre guidelines. This ensures the visibility of funding for EU Projects funded through DEP – Objective 3 Cybersecurity.

The same applies regarding the footer, which contains the official disclaimer and project number, ensuring the correct adherence with the Specific Rules of DEP Model Grant Agreement, art 17.2 and relevant reference in Grant Agreement.

Figure 7: OSCRAT – Word Template

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.

Regarding PowerPoint, the template was created by PMF Research and made available to consortium member, in order to have a uniformed template to use for every presentation related to the project.

Figure 8: OSCRAT – PowerPoint Template

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. Communication & Dissemination Strategy

The OSCRAT Communication Strategy & Dissemination Strategy will strategically outline how to effectively deliver and convey information, key messages and ideas to achieve specific objectives and stakeholders.

A robust communication strategy will equip the OSCRAT consortium with essential guidelines for effectively communicating about the project. It will ensure that all communication efforts are consistent, coordinated, and in alignment with OSCRAT's overarching goals and values. To achieve this, the following objectives will be addressed in this chapter:

- ***Define and Analyse the OSCRAT Target Audience***: Understanding who our key stakeholders are, including their needs and how best to engage with them;
- ***Craft Key Messages***: Developing clear and impactful messages tailored to our identified audience, ensuring that the communication precisely conveys the project's objectives and benefits;
- ***Identify Key Performance Indicators (KPIs) and Communication Goals***: Establishing measurable indicators and goals to evaluate the effectiveness of the communication activities and ensure they contribute to the project's success;
- ***Explore OSCRAT Communication Channels and Tools***: Reviewing and selecting the most effective channels and tools to reach our audience, ranging from digital platforms to traditional media;
- ***Outline the Communication Strategy***: Detailing the approach to be implemented to meet the established communication goals, including tactics, timelines, and responsibilities.

This structured approach will provide a clear roadmap for OSCRAT's communication activities, ensuring they are strategic and results-oriented.

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.

3.1 Define and Analyse the OSCRAT Target Audience

The identification, definition and understanding of the target audience for OSCRAT activities is crucial for developing an effective and successful communication strategy. This strategy is foundational in ensuring the achievement of OSCRAT's goals. For each target group, we will provide a precise definition of whom the communications and activities will address. We will outline their specific, context-based needs and the opportunities that arise from OSCRAT. This approach ensures that all communications are relevant, targeted and impactful, directly addressing the unique aspects and requirements of each audience segment.

The target groups identified based on OSCRAT goals, topics and activities are:

- SMEs, particularly those in digital product sector;
- Decision & Policy makers;
- Digital Innovation Hubs;
- Cybersecurity experts;
- Industry associations.

3.1.1. SMEs in digital product sector

Target Group	**SMEs in digital product sector**
Definition	Businesses engaged in the creation, development, and distribution of digital products such as software, apps, digital platforms, and other technology-driven solutions. These enterprises typically have a smaller employee base and lower revenue compared to larger companies. SMEs in this sector are characterized by their innovative approaches to solving problems through digital means, agility in adapting to market changes, and often, a focus on niche or specialized markets. They play a crucial role in the tech ecosystem, driving innovation and competition.
Needs	• Sensitive data (customer information, financial records, proprietary business data, etc.) protection; • Threat Detection and Response; • Compliance to CRA requirements and procedures; • Employee Training; • Cloud Access Control; • Affordable and Scalable solutions; • Vendors/Subcontractor Security measures.

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.

Opportunity	OSCRAT is designed to enhance the cybersecurity awareness of SMEs in the digital product sector. It aims to inform them about the critical importance of cybersecurity compliance and the tools available to maintain it. The tool will increase their knowledge on how to implement robust security measures effectively and choose the right strategies based on their specific business needs. By using OSCRAT, SMEs can shift their approach from reactive security measures to a proactive, preventative cybersecurity strategy. This shift not only helps in managing potential threats more efficiently but also contributes to a fundamental behavioural change in how cybersecurity is integrated into their everyday business practices.
Key Message	OSCRAT can positively transform SMEs' approach to cybersecurity management. As a comprehensive resource, OSCRAT empowers businesses by providing them with a showcase of compliance tools and educational resources designed to bridge the knowledge gap in cybersecurity. With OSCRAT, SMEs are equipped to enhance their security measures and ensure their digital environments are not only compliant but also resilient against threats.

Table 1: OSCRAT – SMEs in digital product sector

3.1.2. Decision & Policy makers

Target Group	**Decision & Policy makers**
Definition	Individuals who hold the authority and responsibility to make strategic decisions regarding the protection of an organization's information system and digital assets (such as Chief Information Security Officers, Chief Technology Officers, IT directors and other senior IT staff.
Needs	• Threat Intelligence; • Risk Management Tools; • Compliance Assurance; • Security Awareness and Training; • Incident Response and Recovery Plans; • Budget usage; • Vendor & Third-Party Risk Management; • Data Protection and Privacy; • Executive Support.

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.

Opportunity	The engagement in OSCRAT project enhances access to advanced threat intelligent and advanced risk management tools, in compliance with regulatory standards, by offering a free-access and open-source tool. Additionally, it provides resources for developing robust incident response and recovery plans, although offering useful strategies for facing third-parties vendor risks.
Key Message	OSCRAT can enhance cybersecurity resilience and compliance, leveraging cutting-edge threat intelligence, advanced risk management tools and collaborative industry insights to safeguard digital assets and the overall defences against evolving cybersecurity threats.

Table 2: OSCRAT – Decision & Policy Makers

3.1.3. Digital Innovation Hubs

Target Group	**Digital Innovation Hubs**
Definition	Collaborative entities with the focus on accelerating the adoption on cutting-edge technologies and practices among businesses, particularly small and medium enterprises (SMEs). They provide access to technical expertise, technology testing facilities and advanced cybersecurity resources, serving as a bridge between research institutions, industry experts and companies, facilitating the knowledge transfer, enhancing the overall cyber resilience.
Needs	• Access to Latest Technologies; • Strong Industry Partnerships; • Training and educational Programs; • Networking and Collaboration Opportunities
Opportunity	By giving access to advanced cybersecurity tools and technologies, OSCRAT can enhance the DIHs supporting business activities. Also, the open-source nature of the tool, provides opportunities of collaboration and networking, fostering a enhancement of cybersecurity best practices. DIHs can also benefit from involvement in R&D activities within the OSCRAT project, driving innovation in cybersecurity solutions that are practical for business applications. Ultimately, the participation in OSCRAT activities can help increase visibility and credibility, by the association with a significant project, making them more attractive to businesses looking for guidance in cybersecurity compliance processes.
Key Message	OSCRAT activities and tool can empower DIHs cybersecurity offerings, elevating the capabilities in protecting businesses against the latest cybersecurity threats. By participating in the activities and adopting the tool into their services, DIHs can enhance the ability to provide

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.

	cutting-edge solutions, fostering innovation and ensuring a reliable compliance to the CRA for SMEs and startups.

Table 3: OSCRAT – Digital Innovation Hubs

3.1.4. Cybersecurity Experts

Target Group	**Cybersecurity Experts**
Definition	Professionals specialized in protecting computer systems, networks and data from various types of cyber threats. These experts possess a deep understanding of IT, network security and are skilled in the vulnerability identification, risks mitigation and the implementation of safeguarding solutions against potential security threats. Their role is crucial in developing security strategies, responding to incidents and educating other employees in adopting better security practices to protect the organization's digital assets.
Needs	• Up-to-Date Threat Intelligence; • Advanced Security Tools and Technologies; • Compliance with guidelines and standards; • Incident Response Plans and Forensics Tools; • Legal and Regulatory expertise; • Automated Compliance Solutions.
Opportunity	OSCRAT adoption can offer cybersecurity experts a significant opportunity to enhance their expertise, integrating and advanced free-to-use tool, improving their organization ability to detect, analyse and respond to cyber threats, elevating security measures to the new CRA standards. Being involved in OSCRAT project enables cybersecurity experts to shape the tool's development, ensuring it meets specific needs and helps set industry standards. Overall, the OSCRAT tool and project not only enhance cybersecurity operations but also align them with broader business and regulatory goals, fostering a proactive and knowledgeable cybersecurity community.
Key Message	Adopting the OSCRAT tool and engaging in project's activities can enhance cybersecurity expertise, security capabilities, streamline compliance in businesses and position them as industry leaders.

Table 4: OSCRAT – Cybersecurity Experts

Co-funded by the European Union

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

3.1.5. Industry associations

Target Group	Industry associations
Definition	Organized groups composed by professionals, companies and other stakeholders within specific industry sectors. These groups promote collaborations, expertise sharing and advocate for common interests. These associations strive to elevate the professional standards, growth, and practices of their members within the cybersecurity sector through educational initiatives, networking events, research activities, and the creation of industry benchmarks. Additionally, they act as a unified voice to shape public policy and regulations, tackling common issues and bolstering the overall robustness and resilience of the industry.
Needs	• Effective advocacy; • Up-to-Date Information and Research; • Standardization and Best Practices; • Collaboration and Partnerships; • Cybersecurity resilience; • Public Awareness; • Inclusion of different practices.
Opportunity	The OSCRAT project and tools provide valuable possibilities to enhance industry association effectiveness and reach. The project also supports the development and standardization of best practices across the cybersecurity landscape, promoting uniform security measures and compliance processes. Furthermore, OSCRAT aids in public awareness campaigns by providing clear insights into cybersecurity challenges and solutions, helping demystify complex issues for the wider public. It also embraces a broad spectrum of cybersecurity practices, ensuring inclusivity and adaptability to different needs within the sector.
Key Message	OSCRAT empowers cybersecurity initiatives with a cutting-edge tool designed to enhance industry associations advocacy, standardization and cyber-resilience.

Table 5: OSCRAT – Industry associations

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. Communication channels and tools

After the definition of the target groups and related key-message to deliver, it is essential to screen the different means of digital communication that will be implemented, in order to effectively reach the aforementioned groups.

In the following section, the communication channels and tools, as well as related KPIs, to be adopted within the OSCRAT communication & dissemination strategy are outlined in detail.

4.1. Key Performance Indicators

	KPI
Number of website's visits	7000
Number of posts on social media	At least 20
Videos posted in the website and YouTube	2
Newsletters & Press release	12

Table 6: OSCRAT – Communication KPIs

4.2. Website

The OSCRAT website is available at www.oscrat.eu. The initial version of the website was developed in M4 of the project and will be regularly updated by PMF Research Communication Manager. Throughout the duration of the OSCRAT project, the website will be meticulously designed to be user-friendly, featuring easy navigation and a responsive layout that works seamlessly across all mobile devices. It aligns with the official brand identity and is visually oriented, intuitive, and interactive. The site adopts a friendly tone of voice, aiming first to engage all identified groups and stakeholders

Co-funded by the European Union

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

involved in the project and secondly to reach the broader public not specifically targeted within the project's scope.

The website contains general information on the project, mainly the key points, project outputs, consortium description and deliverables that will be produced and published throughout the project's duration.

The sections in the website are:

- ***Home***: landing page containing info about the project;
- ***Consortium***: this website section will display OSCRAT project partners' logos, description of project partners' profile, and role and contribution within OSCRAT;
- ***Work Packages:*** this section provides useful info about the activities and outcomes of each WP;
- ***Deliverables:*** this section contains the list of the project results, divided by Work Package;
- ***News:*** this website section contains all the news concerning the field of interest of the project written both by project partners and third parties (inserted in the website with a short introduction by project partners), the dissemination material developed during the whole life of the project (newsletters, press releases, etc), as well as information about relevant events, namely those organized by OSCRAT consortium, the ones in which a OSCRAT representative participates as presenter, and those events significant for the topic. In this section, a form was created, to gather emails from stakeholders interested in receiving newsletters by email;
- ***Contact:*** this website section offers the possibility to join the project, to get information about one or more activities foreseen by the OSCRAT project and eventually to get part of it (e.g., community events, workshops, training sessions, etc). In addition, this section displays the main OSCRAT contacts and a form to send a message to the OSCRAT consortium directly from the website.

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.

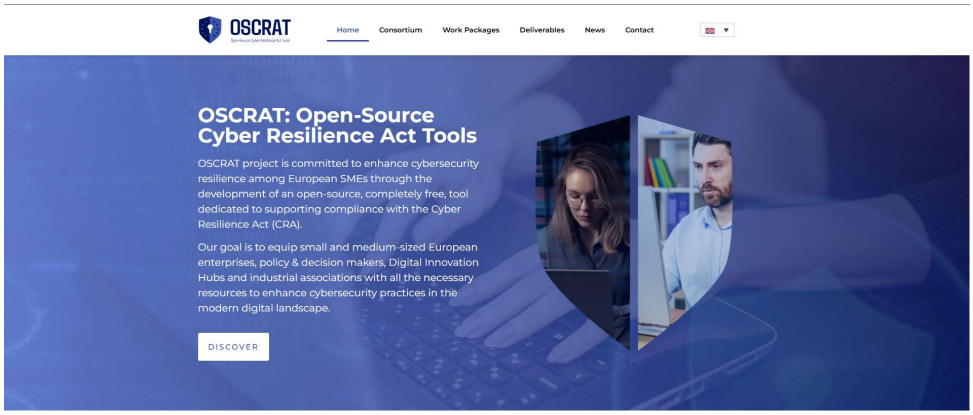

Figure 9: OSCRAT website – Home

4.3. Social Media: LinkedIn (OSCRAT EU Project - Open-Source Cyber Resilience Act Tools)

OSCRAT engagement on social media is designed to expand the overall reach, connect with key audiences and promoting interactive exchanges, all while highlighting the mission, objectives and key themes of the OSCRAT project.

Additionally, social media serve as a vital tool for distributing information via real-time updates and prompts communications, expanding the OSCRAT network and fostering valuable collaborations and partnerships. Social media also provides the OSCRAT consortium with access to essential data and analytics, which are instrumental in assessing the effectiveness of the dissemination activities and results.

For OSCRAT's activities, LinkedIn has been selected as the primary social media platform.

This professional network is globally recognized and utilized by both individuals, experts and organizations (target groups) to establish connections, engage in collaborative efforts and disseminate professional content.

LinkedIn's significant base of professionals and experts makes it an ideal platform for raising awareness about the central themes and objectives of the OSCRAT project, and for drawing the attention of potential collaborators, investors, and other interested entities.

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.

Current Status	
Followers	**59**
Visitors	**45**
Unique visitors	**20**
Posts Impressions	**565**
Posts Reactions	**147**

Table 7: OSCRAT – LinkedIn account current status (updated to 31 May 2025)

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 10: OSCRAT LinkedIn account (screenshot)

PMF Research is responsible for the publication of posts on the official LinkedIn project's page and the preparation of posts templates to be used in dissemination 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 11: OSCRAT LinkedIn post template

4.4. Social Media: X (OSCRAT EU - Open-Source Cyber Resilience Act Tools)

OSCRAT presence on X is strategically developer to broaden our reach, engage key audiences and facilitate dynamic interactions.

X platform is perfect for sharing information swiftly through real-time updates and immediate communication, which plays a crucial role in expanding the OSCRAT network.

This platform enables the OSCRAT project to quickly engage with broad and diverse audience, making it a good tool to raise awareness about OSCRAT's core topics and objectives, also attracting potential stakeholders interested in the project's 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 12: OSCRAT X account (screenshot)

4.5. Content strategy

A OSCRAT content strategy providing guidelines on how to effectively communicate has been developed and tailored taking into consideration the target groups, including the key messages to be delivered, and the above mentioned online channels to use for dissemination purposes.

The content is created according to its purposes. Among the foreseen purposes of social media posts, is it possible to find:

- **Awareness raising** – about the OSCRAT related relevant topics;
- **Information** – about OSCRAT progress, including public deliverables and milestones;

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.

- **Activity promotion** – to invite and involve the target audience in the OSCRAT project activities;
- **Engagement** – to stimulate audience to be more responsive on LinkedIn.

Usually, a post will consist of a picture, a video or website page preview along with a caption. At the end of each caption, it is possible to find OSCRAT partners with a direct link to their LinkedIn company page, and a series of hashtags, both mandatory and chosen based on relevance and popularity.

In order to plan, manage and monitor the project communication strategy and content to be shared, a OSCRAT editorial plan, bi-weekly based has been created and kept updated by the OSCRAT communication leader (PMF Research).

In general, at least **2 posts per month are guaranteed**, thanks also to project partner's support.

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.

4.6. Campaign strategy

With the purpose of attract and engage the specific target groups identified by the consortium, necessary to reach the objectives set by OSCRAT with a significant impact, a tailored effective campaign strategy has been designed and described below.

The targeted campaign strategy will mostly adhere to the following structure:

- Mapping the relevant stakeholders;
- Defining the Campaigns Objectives and key messages/value propositions;
- Employing effective communication channels;
- Organising shared content calendars;
- Measuring and optimising the campaign strategy.

Mapping the relevant stakeholders

In the context of the OSCRAT project, five main target stakeholders have been identified: SMEs, particularly those in digital product sector, decision & policy makers, Digital Innovation Hubs, Cybersecurity experts, Industry associations. The target groups definitions, needs and opportunities OSCRAT project are bound to bring them are outlined under 3.1 sub-paragraphs.

Defining the Campaigns Objectives and Value Propositions

The primary goal of the communication campaign is to foster a genuine, proactive and informed community of stakeholders who will derive benefits from project's activities and outputs. The campaign seeks to gradually cultivate interest and trust, while enhancing engagement and proactive participation. In order to achieve this, the campaign strategy must be visually engaging, offering a clear summary of the project, its activities and the potential advantages for those involved.

Beyond the onboarding phase, it is crucial for the project to maintain stakeholders' interest through timely, targeted communications and relevant activities and events that provide tangible benefits to the stakeholders.

As previously mentioned in this deliverable, the OSCRAT purpose is to reach a diverse range of target groups and stakeholders. Effective engagement is achievable only through carefully tailored messages for each group. This method is particularly crucial

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.

for individual communications, while a broader approach can be adopted for collective communications.

Key messages for general communication purposes – targeting an even wider audience – should be comprehensive, informing about OSCRAT and designed to increase awareness of the project's relevant topics and achievements.

The outcome will be a strategic blend of individual and collective communications, designed to effectively reach and impact all specific target groups in a dynamic campaign strategy.

Employing effective communication channels

The communication campaign will leverage a variety of tools to connect with and engage stakeholders effectively. Several of those tools have been implemented or conceptualized by the project and its partners. Specifically, the toolkit includes:

- Newsletters;
- Press releases;
- Leaflet;
- Social Media;
- Mailing lists;
- Website;
- General project presentations;
- Memorandum of Understanding (MoU) to formalise collaborations with industry stakeholders.

Other activities that could be relevant for the OSCRAT consortium partners is the organisation or participation in:

- Events, conferences and congresses;
- Workshops and training sessions;
- Local or international community building activities.

Another aspect of the communication campaign consists of the involvement of multiple organisations that could significantly enhance the reach of OSCRAT key messages. Each partner will be called upon sharing, disseminating and promoting both the content produced and the general communication activities through their networks of organisations and key stakeholder to reach the targeted groups.

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.

Organising shared content calendars

The communication campaign, which covers both individual and group channels, necessitates a unified and concerts effort form all project partners. The essential tools for reaching and engaging stakeholders need to be pre-planned and collaboratively monitored.

Work Package	Unicis	Oves Enterprise	Enersec	Trakia	EMAG	PMF	Mar-25	Apr-25	May-25	Jun-25	Jul-25	Aug-25	Sep-25	Oct-25	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	X	X	X	X	X	X															
T. 1.2. - Develop a project plan	X	X	X	X	X	X															
T. 1.3. - Establish communication channels	X	X	X	X	X	X															
T. 1.4. - Monitor progress	X	X	X	X	X	X															
T. 1.5. - Stakeholder engagement	X	X	X	X	X	X															
T. 1.6. - Project updates	X	X	X	X	X	X															
Work Package 2 - Requirements gathering and analysis																					
T. 2.1. - Define scope	X		X		X																
T. 2.2. - Identify requirements	X		X		X																
T. 2.3. - User needs	X		X		X			EMAG													
T. 2.4. - Analyze data	X		X		X				ENERSEC												
T. 2.5. - Stakeholder Alignment and Project Requirements Refinement	X	X	X	X	X	X				EMAG		EMAG	ENERSEC	UNICIS	EMAG						
Work Package 3 - Software Design and Development																					
T. 3.1. - Design	X	X																			
T. 3.2. - Product Design (Architecture)	X	X						UNICIS			UNICIS		UNICIS				UNICIS	OVES	UNICIS		
T. 3.3. - Development		X							OVES			OVES		OVES							
T. 3.4. - Integrations	X	X	X												ENERSEC				ENERSEC		
T. 3.5. - Testing	X	X	X	X	X	X										OVES	TRAKIA	EMAG			
T. 3.6. - Documentation	X	X	X	X	X	X														ENERSEC	OVES
Work Package 4 - Stakeholder engagement																					
T. 4.1. - Workshops and International CRA Event	X	X	X	X	X	X				TRAKIA											
T. 4.2. - Training sessions	X	X	X	X	X	X					TRAKIA					TRAKIA				TRAKIA	
T. 4.3. - Use-cases and best practices	X	X	X	X	X	X															TRAKIA
Work Package 5 - Dissemination & Exploitation																					
T. 5.1. - Communication & Dissemination Strategy						X															
T. 5.2. - Creation and adoption of OSCRAT visual identity	X	X	X	X	X	X															
T. 5.3. - Dissemination activities	X	X	X	X	X	X	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF	PMF
T. 5.4. - Development of the Exploitation Plan	X	X	X	X	X	X															

Figure 15: OSCRAT Social media plan for beneficiaries

This approach ensures that messages are delivered efficiently and on schedule, thereby avoiding potential pitfalls such as “void period” or excessive messaging, which can lead to problems in stakeholders’ engagement in the long run.

Furthermore, the monitoring of the dissemination KPIs will ensure the alignment with the project’s expected results regarding dissemination efforts, providing critical insights for ongoing improvement and optimization of the campaign.

Measuring and optimising the campaign strategy

The effectiveness of the communication channels will be evaluated based on metrics such as audience reach, impression and levels of engagement. For example, social media platforms provide straightforward metrics that allow for tracking various engagement indicators related to the impact of OSCRAT.

This method can be applied to the other tools such as newsletters, mailing lists and website.

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.

Collecting these measurements will contribute to an analysis of how effectively the messages are reaching different stakeholder groups and the degree of engagement of each group.

4.6.1. Newsletters

Regular newsletters are planned for OSCRAT to provide updates on project activities, enhance awareness of the project's main topics and engage target groups. Over the course of the project, at least 8 newsletters will be produced using Brevo and distributed through email lists. Interested individuals can subscribe to the email list via the website form or using the link provided in social media posts.

Work Package	Unicis	Oves Enterprise	Enersec	Trakia	EMAG	PMF	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25	Jun-25	Jul-25	Aug-25	Sep-25	Oct-25	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	X	X	X	X	X	X																		
T. 1.2. - Develop a project plan	X	X	X	X	X	X																		
T. 1.3. - Establish communication channels	X	X	X	X	X	X																		
T. 1.4. - Monitor progress	X	X	X	X	X	X																		
T. 1.5. - Stakeholder engagement	X	X	X	X	X	X																		
T. 1.6. - Project updates	X	X	X	X	X	X				NL1 PR1														PR4
Work Package 2 - Requirements gathering and analysis																								
T. 2.1. - Define scope	X		X		X																			
T. 2.2. - Identify requirements	X		X		X																			
T. 2.3. - User needs	X		X		X																			
T. 2.4. - Analyze data	X		X		X							NL2												
T. 2.5. - Stakeholder Alignment and Project Requirements Refinement	X	X	X	X	X	X												NL5						
Work Package 3 - Software Design and Development																								
T. 3.1. - Design	X	X																						
T. 3.2. - Product Design (Architecture)	X	X																						
T. 3.3. - Development		X														NL4								
T. 3.4. - Integrations	X	X	X																			PR3		
T. 3.5. - Testing	X	X	X	X	X	X												PR2						
T. 3.6. - Documentation	X	X	X	X	X	X																NL7		NL8
Work Package 4 - Stakeholder engagement																								
T. 4.1. - Workshops and International CRA Event	X	X	X	X	X	X																		
T. 4.2. - Training sessions	X	X	X	X	X	X								NL3										
T. 4.3. - Use-cases and best practices	X	X	X	X	X	X														NL6				
Work Package 5 - Dissemination & Exploitation																								
T. 5.1. - Communication & Dissemination Strategy						X																		
T. 5.2. - Creation and adoption of OSCRAT visual identity	X	X	X	X	X	X																		
T. 5.3. - Dissemination activities	X	X	X	X	X	X																		
T. 5.4. - Development of the Exploitation Plan	X	X	X	X	X	X																		

Figure 13: OSCRAT Newsletter & Press release calendar

The content of each newsletter will be aligned with the progress of OSCRAT project, reflecting public deliverables, start/end of relevant activities and significant milestones.

Custom banners for the newsletter, including both header and footer, have been designed in Month 4 (M4) and will be used in the newsletter prepared by the partnership throughout the project's 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.

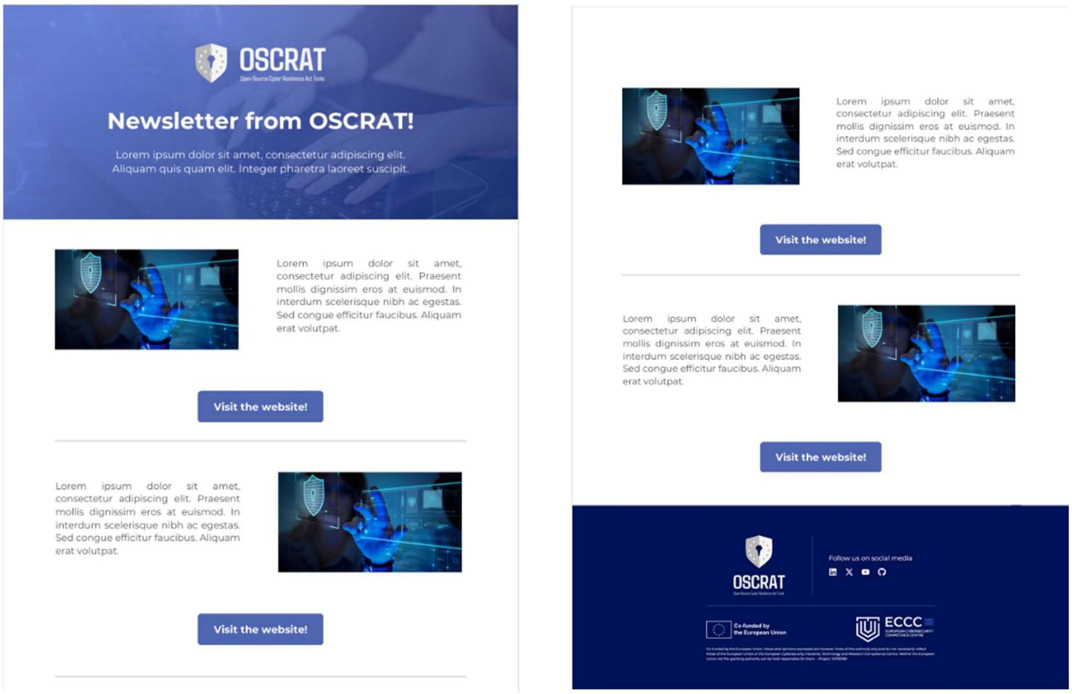

Figure 14: OSCRAT Newsletter Template

The template was created by PMF Research using Canva so it can be adapted to various content types, making it a useful tool to disseminate project's news and relevant information.

4.6.2. Press releases

Regular press releases are also planned in OSCRAT communication strategy to provide the relevant achievements and updates regarding project's activities, enhancing awareness on the project's main topics and engage target groups. A total of 4 press releases will be produced by PMF Research, distributed to all the consortium partners in order to use various channels to disseminate them.

Figure 15: OSCRAT Press Release Template

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. Exploitation Plan

OSCRAT's exploitation activities will be developer under Work Package 5: Dissemination & Exploitation (WP5). WP5 already started in M1 of the project while the activity **5.4.: Exploitation Plan** is will officially start on M16 (March 2026). This part of the plan will be updated and modified, considering the project's needs in M18, during the development of the deliverable **D.5.3. Exploitation Plan**.

In these early stages of the project, the primary objective is to ensure that the OSCRAT's deliverables, particularly the open-source tool, are effectively positioned to maximize their impact on the European Cybersecurity landscape, with a specific emphasis on SMEs and other target groups.

When it comes to the sustainability and exploitation efforts for OSCRAT, specific activities and tasks will be shared with the entire consortium, in order to support the exploitation of the project results by project partners, target groups and external stakeholders., ensuring the uptake and long-term use of the results.

The final aim is to assist community members, promote offerings to peer initiatives and organizations across the EU and collaborate with other ecosystem representatives in the field of cybersecurity and CRA compliance.

By sharing lessons learned and fostering collaboration, the goal is to stimulate the adoption of project outputs, particularly the OSCRAT open-source tool, and generate broader impacts in collaboration with peers and stakeholders.

Most of these efforts will be carried out within WP5 - Dissemination & Exploitation - which spans the duration of the project, supported by the work developed by the entire Consortium, due to the ongoing need to maintain an open communication line between OSCRAT, partner networks, potential users, and future replicators.

While the official Exploitation Plan (D5.3) will be delivered later in the project, activities within WP5, together with its deliverables – especially D5.1 OSCRAT Communication, Dissemination Strategy & Exploitation Plan – will form the backbone of the project's sustainability and uptake efforts. These activities will ensure that OSCRAT tools and methodologies are effectively disseminated, adopted, and integrated into business practices, particularly by SMEs, policymakers, and industry associations, thereby contributing to the enhancement of cybersecurity resilience across the EU.

Co-funded by the European Union

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

5.1. Objectives of the Exploitation Plan

The Exploitation Plan aims to ensure that OSCRAT delivers tangible and sustainable benefits to its stakeholders, while aligning with the broader goal of the EU Cyber Resilience Act (CRA). The activities are very linked to Work Package 4 – Stakeholders Engagement (WP4) and Work Package 5 – Dissemination & Exploitation activities.

During the initial stages of the project, the objectives can be summarized as:

- **Positioning OSCRAT as a valuable resource**: the open-source tool will be established as a good solution for SMEs aiming to comply with CRA requirements;
- **Engaging Stakeholders**: the goal is to build awareness and trust among potential users, including SMEs, policy-makers and industry associations;
- **Gathering Feedback**: collect input from early adopters to refine the tool and align its features with user needs;
- **Laying the groundwork for long-term adoption of project's results**: identify opportunities for partnerships and collaborations beyond the project's lifecycle.

5.2. Exploitation Activities

The first step in exploitation is to identify and engage with key stakeholders who will benefit from or contribute to OSCRAT's outcomes. These include:

- **Primary Stakeholders**: SMES, particularly in the digital product sector, who are directly impacted by the adoption of the CRA and need to comply with the requirements;
- **Secondary Stakeholders**: policy and decision makers, Digital Innovation Hubs (DIH), cybersecurity experts and industry associations;

The activities will be related to WP4, with the organization of targeted workshops and training session to introduce OSCRAT and gather useful feedbacks, and to WP5, with the promotion of OSCRAT relevant activities and achievements during the entire project 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.

5.3. Early demonstration of the OSCRAT Tool

To ensure relevance and usability of the tool, it is crucial to test and refine it early in the project.

The activities are related to:

- Developing of a prototype of the OSCRAT tool by November 2025 (M12);
- Identify and onboard pilot users, focusing on SMEs across diverse industries and geographical locations (M13-M15);
- Conduct initial testing sessions and collect feedback on usability, functionality and relevance (M15-M16);
- Create a preliminary report summarizing insights from the pilot phases to inform further development, which will lead to a better understanding of user needs, integrations to the tool and also a fine-tuned strategy for the Exploitation of results after the project duration.

5.4. Dissemination and Communication for Exploitation

Effective communication is mandatory to exploitation, ensuring that stakeholders are a full understanding of OSCRAT's value proposition, motivating the adoption by SMEs.

The activities related to this objective are:

- Publish articles and useful news to different audiences, such as SMEs and policymakers, on the benefits of OSCRAT project;
- Leverage social media campaigns to promote early successes and engage with stakeholders;
- Distribute Newsletters and Press Releases highlighting key milestone 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.

5.5. Building Strategic Partnership

Collaboration with industry leaders and relevant organizations will be essential to maximize OSCRAT's reach and impact.

The activities related to this objective are:

- Expression of Interest with at least 3 industry associations or Digital Innovation Hubs;
- Engagement with EU policymakers and regulatory bodies to promote OSCRAT as a model for CRA compliance;
- Explore synergies with other EU-funded projects to share knowledge on the topic.

5.6. Sustainability Planning

To ensure the long-term impact of OSCRAT, especially the CRA compliance tool, sustainability planning is crucial to plan the management of results after the project duration.

The activities related to this objective are:

- Explore the possibility of creating partnerships with industry bodies, potential business models for maintaining and updating the OSCRAT tool and/or the possibility to integrate a subscription-base service (two years after the official project's end date);
- Identify potential funding opportunities, including future EU grants, to support a further development and integrations for the OSCRAT's results;
- Develop a sustainability plan, outlining key actions and responsibilities, to be finalized in D.5.3. – Exploitation Plan.

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.

5.7. Preliminary Exploitation Roadmap

Month	Activity	Output
M3	Launch of the OSCRAT website and communication tools	Website and marketing materials available
M4 – M8	Needs analysis and value proposition development	Survey results and value proposition
M12	Prototype Development & Beta Testing	Easly feedback report
M14 - M18	Strategic partnerships and sustainability planning	Preliminary sustainability plan

Table 8: OSCRAT - Preliminary Exploitation Roadmap

6. Impact & Conclusions

The communication, dissemination, and exploitation plan for the OSCRAT project aims to effectively reach and engage a diverse range of stakeholders, raise awareness about the project and its benefits, and ensure widespread dissemination of project activities and results, especially the open-source tool for the CRA compliance. The plan takes a comprehensive and strategic approach by addressing the following key aspects:

- **OSCRAT Brand Identity**: Establishing a strong and recognizable visual and brand identity to effectively convey the project's mission, values, and objectives.
- **Target Audience and Key Messages**: Identifying specific target groups, such as SMEs, policymakers, cybersecurity experts, and industry associations, and tailoring messages to address their specific needs and opportunities.
- **Communication Tools, Channels, and Materials**: Leveraging a range of tools, including the project website, social media platforms, newsletters, and press releases, to ensure effective outreach and engagement.
- **Dissemination Tools and Channels**: Utilizing events, scientific publications, public deliverables, and collaborations with ecosystem partners to maximize the reach and impact of project results.
- **An Overview of the Exploitation Strategy**: Providing a preview of how OSCRAT results, particularly the open-source tool, will be positioned for adoption, sustainability, and long-term use by stakeholders.

Co-funded by the European Union

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

6.1. OSCRAT Brand Identity

The **OSCRAT Brand Identity** has been carefully crafted to embody the project's mission to enhance cybersecurity resilience and promote compliance with the EU Cyber Resilience Act (CRA). This includes the creation of a distinct visual identity, such as the OSCRAT logo, brand colours and typography, al of which convey professionalism, trust and innovation. The choice of introducing a shield in the logo (together with EU stars) symbolizes both security and the project alignment with European values and standards. The choice of the blue as primary colour is aligned with these principles, conveying the perception of stability, reliability and trustworthiness, which are key elements in the field of cybersecurity.

Beyond the visual elements, OSCRAT's tone of voice is equally important. It has been designed to be supportive, engaging and approachable for SMEs that may lack internal technical expertise. In communication with institutional entities, the tone of voice will be adapted to convey a message of trustworthiness and credibility.

The OSCRAT brand identity creates a unified and recognizable framework that ties together all communication materials, from templates to presentations. This cohesive approach enhances OSCRAT's visibility across multiple platforms and establishes a strong association with dependable and cutting-edge solutions for CRA compliance. By projecting professionalism and clarity, the brand identity becomes a cornerstone for fostering stakeholder confidence, encouraging engagement, and amplifying the project's reach. It ensures that OSCRAT's mission is not only communicated effectively but also leaves a lasting impression on its audience.

6.2. OSCRAT Target Audience and Key Messages

The understanding of OSCRAT's target audiences and crafting of tailored key messages are essential elements of the project's communication and dissemination strategy.

The OSCRAT project focuses on five main stakeholder groups: SMEs in the digital product sector, policymakers, digital innovation hubs (DIHs), cybersecurity experts, and industry associations. Each group presents unique needs and opportunities in relation to cybersecurity and CRA compliance, necessitating customized messaging to effectively address their priorities and challenges.

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.

A good communication strategy needs to address the needs of each target group, creating a series of communication activities with the goal of giving a strong solution to the various identified needs.

SMEs' needs are related to a reduction of complexity in streamlining CRA compliance processes, enhancing their cybersecurity posture in the European economic environment. Providing an accessible, user-friendly and open-source tools is the key message that has to be communicated in dissemination activities for this target group.

Policymakers are primarily concerned with regulatory alignment and the promotion of best practices. Key messages for this group highlight OSCRAT's contributions as a model for CRA compliance, its ability to support policy implementation, and its role in advancing Europe's broader cybersecurity objectives.

Regarding **DIHs and industry associations**, OSCRAT provides opportunities to foster collaboration, knowledge sharing and strengthening their networks' cybersecurity capabilities. The messaging focuses on how integrating OSCRAT's tools can empower their communities, streamline CRA compliance processes, and support the advancement of a more resilient and secure digital ecosystem.

Cybersecurity experts, as technical stakeholders, are drawn to OSCRAT's advanced features and the opportunity to shape its development. Messages for this group emphasize the value of contributing to an innovative tool designed to improve both operational security and compliance standards.

By customizing its communication to resonate with each audience, OSCRAT ensures its efforts are impactful, fostering engagement, adoption, and long-term impact across Europe.

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.

6.3. Communication Tools, Channels and Materials

OSCRAT employs a comprehensive mix of tools, channels, and materials to effectively engage its stakeholders and achieve its communication objectives.

The **project website** acts as a central information hub, offering straightforward access to project updates, deliverables, news, and resources. Designed with a responsive and user-friendly interface, the website is accessible across all devices and caters to both technical and non-technical users, ensuring inclusivity and ease of use.

Social media platforms, especially LinkedIn and X (formerly Twitter), play a vital role in OSCRAT's outreach strategy. These channels provide real-time updates, foster interaction with stakeholders, and enhance the project's visibility within professional and industry networks. Posts are carefully crafted to showcase milestones, upcoming events, and achievements, ensuring consistent communication and engagement with the audience.

Newsletters and Press Releases will also be essential to distribute information about the project activities, results and milestones. These materials will be shared via partner networks, ensuring a broader reach, including those who may not actively follow the project on social media. The creation of the mailing list will be supported by the introduction of the registration form in the website and also the share of the link in social media posts.

To maintain consistency and professionalism, OSCRAT uses standardized templates for presentations, reports, and press releases, all of which align with the project's brand identity. Additionally, the use of custom-designed banners, infographics, and videos makes the messaging more engaging and visually appealing, helping to convey complex ideas effectively.

This multi-channel strategy ensures that OSCRAT reaches its diverse audience with impactful and accessible communication, fostering engagement and supporting the project's goals.

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.

6.4. Overview of the Exploitation Strategy

The exploitation strategy for OSCRAT focuses on ensuring the long-term adoption and sustainability of the project's results, particularly the open-source tool for CRA compliance. During the first 16 months, the primary goal is to establish a strong foundation for the tool's exploitation by engaging stakeholders, refining the tool based on feedback, and identifying pathways for its long-term use.

Early exploitation efforts focus on piloting the tool with SMEs and other key stakeholders to showcase its value and collect feedback for further refinement. Workshops and training sessions are designed to help users become familiar with the tool's features and benefits, while collaborations with industry associations and digital innovation hubs open pathways for wider adoption and integration.

A core aspect of the exploitation strategy is establishing a clear and tailored value proposition for each stakeholder group:

- For **SMEs**, the tool's simplicity, affordability, and practicality are highlighted as major benefits;
- For **policymakers**, the tool's alignment with CRA requirements and its ability to support regulatory compliance emphasize its significance and relevance;
- For **DIHs and industry associations**, OSCRAT provides opportunities to enhance their service offerings by integrating a powerful, easy-to-use cybersecurity tool into their networks, enabling them to better support their members and foster collaboration;
- For **cybersecurity experts**, the tool's advanced capabilities and open-source nature are key highlights, providing them with opportunities to actively contribute to its enhancement while staying at the forefront of innovation in CRA compliance.

To ensure sustainability, OSCRAT will explore potential partnerships with regulatory bodies or industry associations that can support the tool's maintenance and further development.

For this purpose, collaboration with other EU-funded projects and cybersecurity initiatives can certainly enhance the tool's visibility and integration into existing ecosystems.

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

Communication, Dissemination Strategy & Exploitation plan

oscrat-eu-project

OscratEUProject

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.