SENTINEL

Bridging the security, privacy, and data protection gap for smaller enterprises in Europe

D7.4 - Dissemination strategy and activities – final version

Project Information

Grant Agreement Number	101021659
Project Acronym	SENTINEL
Project Full Title	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
Starting Date	1st June 2021
Duration	36 months
Call Identifier	H2020-SU-DS-2020
Topic	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Project Website	https://www.sentinel-project.eu/
Project Coordinator	Dr. George Bravos
Organisation	Information Technology for Market Leadership (ITML)
Email	gebravos@itml.gr

Document Information

Work Package	Work Package 7
Deliverable Title	D7.4 - Dissemination strategy and activities – final version
Version	1.5
Date of Submission	27/05/2024
Main Editor(s)	Ruben Costa (UNINOVA), Cláudio Côrrea (UNINOVA)
Contributor(s)	All partners
Reviewer(s)	Siranush Akarmazyan (ITML), Konstantinos Poulios (STS)

Document Classification					
Draft		**Final**	X	**Confidential**		**Public**	X

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	14/03/2024	Draft	Confidential
1.1	11/04/2024	1st draft ready	Confidential
1.2	12/04/2024	1st review by ITML	Confidential
1.3	30/04/2024	Review by STS	Confidential
1.4	10/05/2024	2nd review by ITML	Confidential
1.5	27/05/2024	Final version ready	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
dKPIs	Dissemination Key Performance Indicators
DIH	Digital Innovation Hub
EU	European Union
HRB	Horizon Results Booster
MS	Milestone
SMEs/MEs	Small and Medium Enterprises and Micro Enterprises
UI	User Interface
UX	User Experience
WP	Work Package

Executive Summary

Deliverable D7.4 - Dissemination strategy and activities – final version is produced within Work Package 7 (Ecosystem building, Exploitation and sustainability management) of the SENTINEL Project, under Task 7.2, Dissemination and communication strategy to trigger awareness and new business opportunities.

This document presents the SENTINEL's project dissemination and communication strategy by reporting on activities carried out between the 19th month and the 36th month of the project. This follows the SENTINEL Milestone 6: Final framework's evaluation, final business plan, dissemination and exploitation reports (MS6) where the project dissemination strategy and activities executed during the second half of the project need to be reported.

The goal of the dissemination and communication concept is to identify and properly organize the activities needed to achieve the objectives of the project. Therefore, three main objectives have been defined:

- Continuous updating the project's visual identity, including conventional information material, tools (project website, social media) and audio-visual material (e.g., videos, podcasts).
- Participation and organization of outreach activities, international events (e.g., conferences and workshops) and SME-centric workshops.
- Develop solid dissemination and communication strategy and measures to be followed by the project consortium to raise awareness and reach to the relevant target audiences.

To assess the impact of the dissemination and communication activities, the dissemination KPIs (dKPIs) have also been analysed and presented. They have been monitored on a regular basis to make sure that the project' goals and impact initially defined in the scope of the project were successfully achieved.

1. Introduction

Over 25 million European Small and Medium-sized Enterprises and Micro Enterprises (SMEs/MEs), central within EU enterprise policy, face multiple challenges related to personal data protection, ranging from awareness to a clear and practical roadmap to compliance. The most prominent one is the fact that, unlike larger enterprises, SMEs/MEs lack access to enterprise-grade cybersecurity technology and capacity-building for compliance, making them increasingly often victims of costly data breaches. SENTINEL aspires to bridge this gap by boosting SMEs/MEs capabilities in this domain through tried-and-tested security and privacy technologies integrated in a unified digital architecture and. It has a potential to be European SMEs' one-stop shop for cybersecurity and GDPR-related recommendations and can catalyse adoption of market-leading safe and secure technologies among SMEs/MEs and help safeguard their and their customers' assets.

1.1 Purpose of the document

The dissemination strategy and activities – final version (D7.4), monitors and evaluates the SENTINEL's dissemination strategy and activities of the second half of the project period, including monitoring of the tools utilised to meet the activities scope, i.e. collaboration activities with other EU cluster projects, organization of events, publication of scientific results, active participation in social media channels, development of branding material (flyers, cards and roll-ups).

This deliverable, reports and analyses the results of dissemination through the indicators of success initially defined in the Grant Agreement.

Work Package 7 of SENTINEL (Ecosystem building, Exploitation and sustainability management) focuses on ensuring that the various outcomes of the project are widely disseminated to the appropriate target group, at the appropriate time and via appropriate methods. Furthermore, WP7 aims at identifying stakeholders who can contribute to the development, evaluation and uptake of the project outcomes and encouraged them to participate in the project's current and future actions.

The main objectives of WP7 are:

- Develop the project's visual identity.
- Raise awareness about the project concept, developments and findings to all key actors.
- Develop the dissemination and communication strategy of the project.
- Develop the SENTINEL business model and strategies for incentivizing/promoting project adoption.
- Create a marketing strategy that focuses on commercialization.

1.2 Structure of the document

This document is structured in the following way:

- Section 1 contains an introduction to the document.

- Chapter 2 describes an overall dissemination and communication strategy to be implemented, including monitoring and reporting procedures. It also describes the dKPIs used to measure the impact of the dissemination activities.
- Chapter 3 highlights all events that were organized by the SENTINEL consortium members, as well as all third-party events which SENTINEL has participated in the M19-M36 project period.
- Chapter 4 presents the final remarks and concludes the document.

1.3 Intended readership

This document is intended for both consortium members and external stakeholders, since it comprises the SENTINEL strategy and the dissemination and communication activities performed within the second half of the project.

2. SENTINEL Dissemination and Communication Strategy

2.1. Objectives

The dissemination and communication strategy aims to take up the results of the project for the creation and support of a dynamic innovation ecosystem, targeting to achieve maximum visibility for the technologies and services developed for both technology-related communities and broader non-technical communities and the general public.

The engagement of technology providers, policy makers and end users during and beyond the end of the SENTINEL project will enable to create a self-sustainable future experimental and trial environment that will continue attracting the usage and attention of entrepreneurs and researchers. The dissemination and communication strategy of SENTINEL is schematically depicted in Figure 1.
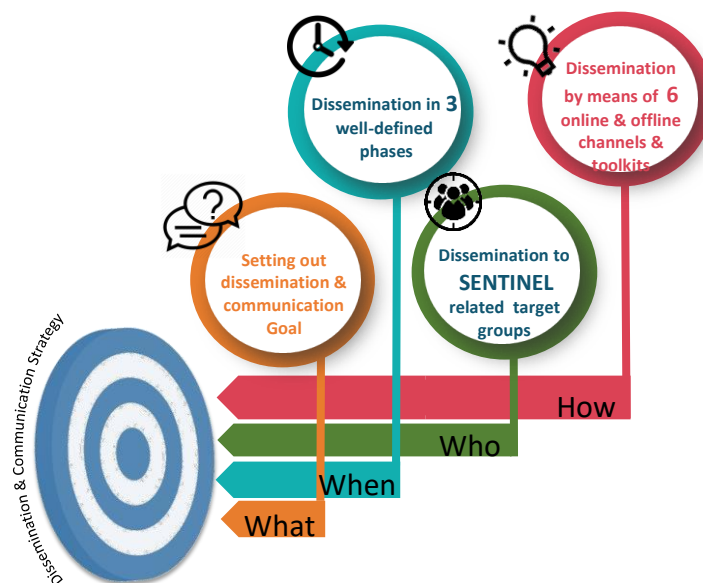
Figure 1. SENTINEL dissemination strategy

2.2. Phases and timing

The main goal of the project's is to raise awareness on an individual and organisation level about the benefits of the SENTINEL platform and influence the view of a sufficient number of stakeholders, so that they become aware of the project's new ideas, services and results, ultimately accept and adopt it. To achieve this goal the dissemination and communication strategy follows the three (3) phases shown in Figure 2 and briefly summarised below.
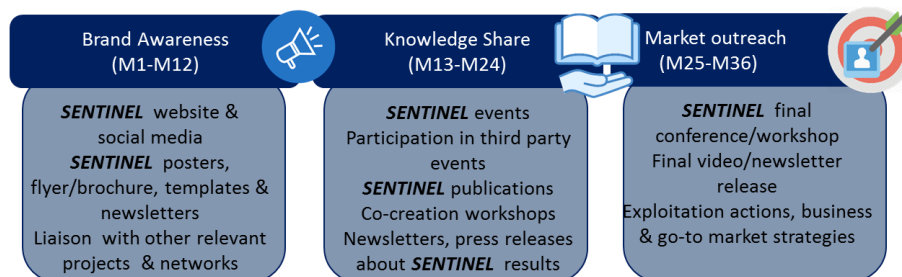
Figure 2. SENTINEL dissemination phases and methods

Phase-I: Brand awareness (M1-M12): this phase aims to promote the project, putting emphasis on awareness raising, ensuring that the project is appropriately recognized on a wide scale and securing an engagement of SMEs/MEs and any other interested stakeholder. During this period, the project's visibility was achieved by: redesigning the project logo which is the project's unique identity, designing and developing the project website, launching the social media profiles of the project, setting a clear communication and dissemination strategy and liaising with relevant projects and networks.

Phase-II: Knowledge Share (M13-M24): this phase focuses on development and understanding of project's technical specifications and requirements and the planning of various workshops. During this phase, the SENTINEL partners disseminate the projects results in different third-party events by pursuing further engagement with key stakeholders. Establishing contacts and relations with new stakeholders and initiating knowledge sharing with other similar projects is an important part of the current project stage. Within this phase, based on important milestone accomplishment, an updated set of various promotional materials (posters, newsletter, etc.) support to spread a word and create new contacts.

Phase III: Market outreach (M25-36): this phase involves wide and effective dissemination of the project's tangible results, building on the project's favourable reputation and networking with the project target groups. Moreover, the project partners motivate further participation of stakeholders in the project events (workshops, conferences) and promote exchange of experiences and knowledge sharing with related initiatives and take-up of the project results. Finally, it includes the formulation of business model and go-to-market strategies.

2.3. SENTINEL target groups

The SENTINEL partners have already defined the project's relevant target audiences covering a full range of potential end users, groups and organisations of the proposed solution and categorised them in seven (7) specific groups. Each dissemination activity is tailored with a specific message to be conveyed to these groups:

- SMEs/MEs, business entities, companies, organisations (European and non-European) through the strong network of the pilot providers involved in this project: (i) Utilisation of the project's results in their everyday operations, (ii) Strengthening innovation by blending with in-house artefacts, (iii) Participation in the project's events, (v) Inspiration for new ideas and applications.
- Researchers and Academy members: Individuals engaged in research initiatives and/or working in research/academic institutes conducting core or application research cyber

ranges, data protection and cybersecurity technologies, cloud-based security services;
(i) Further advancements on the above-mentioned technologies research through extension/reuse of the project's outputs in the investigated and in other application domains,
(ii) Inspiration for future research initiatives based on the project's concept and results,
(iii) Participation in the project's events.

- Security service providers/experts, technology clusters, and other innovation communities: (i) Inclusion of project's results to collaborative research activities (roadmap, white papers, position papers), (ii) Dissemination of project's results to their members, (iii) Bilateral participation in events for knowledge exchange.
- Policy makers (at any level like Ministries and Governments, Regulatory Agencies, Standardisation Organisations e.g., ETSI, CSCG): (i) Evaluation of the project's Sociotechnological-Economic-Environmental-Political (STEEP) aspects, (ii) Definition of future research and innovation directions for national and EC initiatives, considering the project's acquired knowledge, (iii) Inputs for standardisation activities.
- H2020 projects' participants, partners and relevant stakeholders (including the projects funded under by EDA) related to security and privacy technologies and beyond: (i) Identification of common topics, (ii) Synergies and collaborations for results promotion, (iii) Enhancing innovation through results combination, (iv) Co-organisation of events, (v) Research Agenda formulation.
- General public (citizens): Individuals who benefit from the project outcomes, (i) Acquire new expertise and utilise the project results in scenarios that are addressed to the general public for gathering feedback, (ii) Increase general awareness.
- Investors: This is a crucial targeting audience from the exploitation perspective of the project. It includes angel investors and other private and/or public funds. In the case of the SENTINEL project, their exploitation interest is purely commercial and depends on the partnerships and revenue agreement. They could invest in the delivery of the innovation to the market and (commercially) capitalise on this once mature.
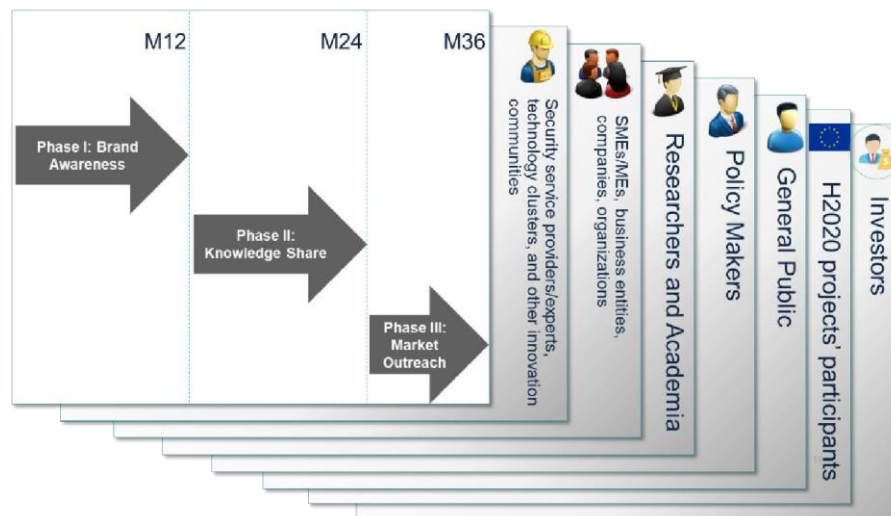

Figure 3. SENTINEL target groups

2.4. Management

Managing and reporting dissemination and communication activities is very important for the successful implementation of WP7 and it demands the close collaboration of all partners. In SENTINEL, the dissemination and communication activities are coordinated by the Dissemination and Exploitation Manager (DEM) of the project. Mr. Ruben Costa from UNINOVA, as a DEM is responsible for coordinating the dissemination and communication activities during the project lifecycle. However, all SENTINEL consortium members are responsible for actively supporting and providing contributions to such activities.

Within this respect, since the beginning of the project, monthly meetings have been executing on a regular basis, in order to discuss and plan the dissemination and communications activities to be executed within the project lifetime. Such activities can be identified as follows:

- Development and maintenance of the project's visual identity, including conventional information tools (project website, social media) and audio-visual material (e.g., videos). Considering this activity, the project website development and maintenance is under the responsibility of ITML, the social media channels (LinkedIn, Twitter and YouTube) administration are under the responsibility of UNINOVA, the publication of social media posts is under the responsibility of every partner. In order to facilitate the process of posting content in social media, the SENTINEL partners have agreed that every week each partner is responsible for providing at least one post. Considering audio-visual material, the branding material (leaflets, roll-ups and business cards) creation was undertaken by UNINOVA, with respect to videos, the first SENTINEL promotional video was developed by ITML, with the support of UNINOVA. Also, UNINOVA has setup a series of interviews with domain knowledge experts, which are also available in YouTube.
- To raise awareness about the project concept, developments and findings to all key actors (the cybersecurity and data protection industry, SMEs/MEs, academics, policy makers, general public) by participating and organising outreach activities, international events (e.g., conferences and seminars) and workshops. To raise awareness about SENTINEL, all consortium members have been fully engaged, by participating in different outreach activities and disseminating the project's scientific results through paper publications in different conferences. For more detailed information about the SENTINEL outreach activities, please refer to Chapter 3.
- To develop the dissemination and communication strategy of the project, including social presence, participation in EU events, collaboration with other related projects. Regarding this activity, all SENTINEL partners have been actively contributing. A more detailed overview of the dissemination and communication activities is described under Chapter 3 of this document.

2.5. Policy and rules

The policies for the dissemination of knowledge from the project (e.g., press releases and joint publications), along with the exploitation of foreground and background knowledge are clearly stated in Consortium and Grant Agreements. In particular, the SENTINEL Grant Agreement states that "*A beneficiary that intends to disseminate its results must give advance notice to the other beneficiaries of — unless agreed otherwise — at least 45 days, together with sufficient*

information on the results it will disseminate. Any other beneficiary may object within — unless agreed otherwise — 30 days of receiving notification, if it can show that its legitimate interests in relation to the results or background would be significantly harmed. In such cases, the dissemination may not take place unless appropriate steps are taken to safeguard these legitimate interests".

For dissemination actions, a common graphic identity is defined to allow for better visibility and recognition of the project. All dissemination material (deliverables, reports, presentation) include:

- the name and the logo of the project
- the website of the project
- acknowledge to EC public fund with the official EC logo indicating the Horizon 2020 below.

With respect to publications, each partner announced in a timely manner, to the dissemination manager and the project coordinator, the type (e.g., conference or journal article) and the context of the publication to be produced. This procedure allowed checking if they fulfil the dissemination requirements or whether they conflict with other existing papers.

Every publication produced within the scope of SENTINEL is entitled to an acknowledgement section stating the following: "*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021659*".

2.6. Monitoring and reporting

Monitoring and reporting communication and dissemination activities is very important for the successful implementation of WP7 and it demands the collaboration of all partners. For this purpose, DEM has prepared and circulated a Dissemination Activities Reporting Template where all partners reported their conducted activities regularly.

For monitoring purposes, the dissemination activities were analysed and reassessed regularly by DEM. The SENTINEL dissemination and communication activities are evaluated via Key Performance Indicators (KPIs). These KPIs are assessed both for the M19-M36 period as well as for the entire project duration and are illustrated in Table 1.

Table 1. Key Performance Indicators (KPIs) for measuring dissemination and communication activities

SENTINEL Channels	KPI	Method of measurements	Fre-quency	Thres.	M19-M36 period	M1-M36 period
SENTINEL website	**dKPI#1:** Number of visitors	Google analytics	Monthly	≥100	167	141
	dKPI#2: Number of page views	Google analytics	Annu-ally	>5000	38,295	46,566 total 15,500 annually
	dKPI#3: Number of downloads	Google analytics	Monthly	>500	15,000 833 monthly	16,500 (including Zenodo downloads) 458 monthly

Social Media Twitter	**dKPI#4:** Number of followers	Twitter analytics	Monthly	>20	17 (Platform changed to X and this metric was affected)	17
	dKPI#5: Number of push announcements	Twitter analytics	Monthly	≥20	29	20
	dKPI#6: Number of unique visitors	Twitter analytics	Monthly	≥30	(Platform changed to X and this metric was affected)	>30 (based only Y1 and Y2 results)
Social Media LinkedIn	**dKPI#7:** New followers	LinkedIn analytics	Monthly	≥20	15	27
	dKPI#8: Number of push announcements	LinkedIn analytics	Monthly	≥20	>31	20
	dKPI#9: New of unique visitors	LinkedIn analytics	Monthly	≥20	29	44
Brand-building materials	**dKPI#10:** Number of distributed hard copies of the SENTINEL brochure	Direct reporting	End of project	≥1000 distributed	550	>1000
	dKPI#11: Number of electronic SENTINEL brochures	Google analytics	End of project	≥1000 downloads	521	>1300 (including Zenodo downloads/views)
	dKPI#12: Regular newsletters	Admin tool	End of project	≥9 newsletters	9 5 project-related 4 cluster-related	14 10 project-related 4 cluster-related
	dKPI#13: Number of SENTINEL videos and number of views	YouTube	End of project	3 videos with >1000 views each	12	23 videos (>3200 views total)

Journal & magazine publications	**dKPI#14:** Number of international referred journal publications by SENTINEL partners	Direct reporting	End of project	>6	5 (2 accepted 1 submitted, 2 published), 2 more journal papers are under preparation)		
	dKPI#15: Number of special issues in international referred journals	Direct reporting	End of project	>2	2		
	dKPI#16: Number of publications in international (printed or online) magazines	Direct reporting	End of project	>6	5	8 (conference proceedings)	
Presentations in International Conferences	**dKPI#17:** Number of conference presentations by SENTINEL partners	Direct reporting	End of project	≥12	6	12	
Third-party events (INFO DAYs, workshops, fairs/exhibitions targeting national & EU policy makers, potential stakeholders)	**dKPI#18:** Number of events	Direct reporting	End of project	≥ 15 events with >60 attendees	12	22	
	dKPI#19: Number of audience contacts	Surveys	End of project	≥50% of the participants	The KPI was on average accomplished with approximately 50% of the participants registered as audience contacts.		
	dKPI#20: Number of participants interested in SENTINEL project	Surveys	End of project	≥40% of the participants	The KPI was on average accomplished with approximately 45% of participants demonstrating their interest in SENTINEL.		
SENTINEL Events (INFO DAYs, webinars, workshops/demonstration events)	**dKPI#21**: Number of events organized by SENTINEL partners.	Direct reporting	End of project	≥ 8 events with ≥60 attendees and 3 events with ≥100 attendees	4	11	
	dKPI#22: Number of audience contacts	Surveys, interviews	End of project	>=50% of the	Maintained strong engagement, achieving 50% of audience contacts.		

				partici-pants		
	dKPI#23: Number of participants interested in SENTINEL project	Surveys, interviews	End of project	>=50% of the partici-pants	The KPI was on average accomplished with approximately 50% of participants demonstrating their interest in SENTINEL.	
Liaisons and networking with the other relevant projects	**dKPI#24:** Number of SENTINEL members actively networking with other relevant projects	Direct reporting	End of project	≥ 6	6	17
Standardization/regulation relevant activities	**dKPI#25:** Number of "EAB" members monitoring and ensuring compliance with relevant regulations	Direct reporting	End of project	At least two (2) members of EAB	2	3

2.7. Horizon Results Booster (HRB) Programme

The Horizon Results Booster (HRB) programme supports effective transfer of research and innovation project results to policy makers, industry and society by offering various services as dissemination, exploitation strategy and business plan development to projects supported under the 7th Framework Programme (FP7) or Horizon 2020 funding schemes.

SENTINEL has applied for Service 1 "Portfolio Dissemination and Exploitation Strategy (PDES)", Module A "Identification and creation of the portfolio of R&I project results" of HRB programme and invited nine (9) projects (ELECTRON, SPATIAL, IDUNN, TRUST Aware, ERATOSTHENES, IRIS, SECANT and ARCADIAN-IoT) to take the first step towards forming a Project Group (PG) based on commonalities between their work in this research field.

Main objectives of this module can be described as follows:

- Identifying groups of projects applications from groups & individual projects.
- Identify complementary results from across the PG Cluster and group these results into Key Exploitable Results.
- Analyse all relevant stakeholders.
- Prioritise and identify their key stakeholders.
- Provide PG with contacts under these stakeholders.
- Identify relevant channels and potential recommendation for joint dissemination actions (for Module B or on their own.
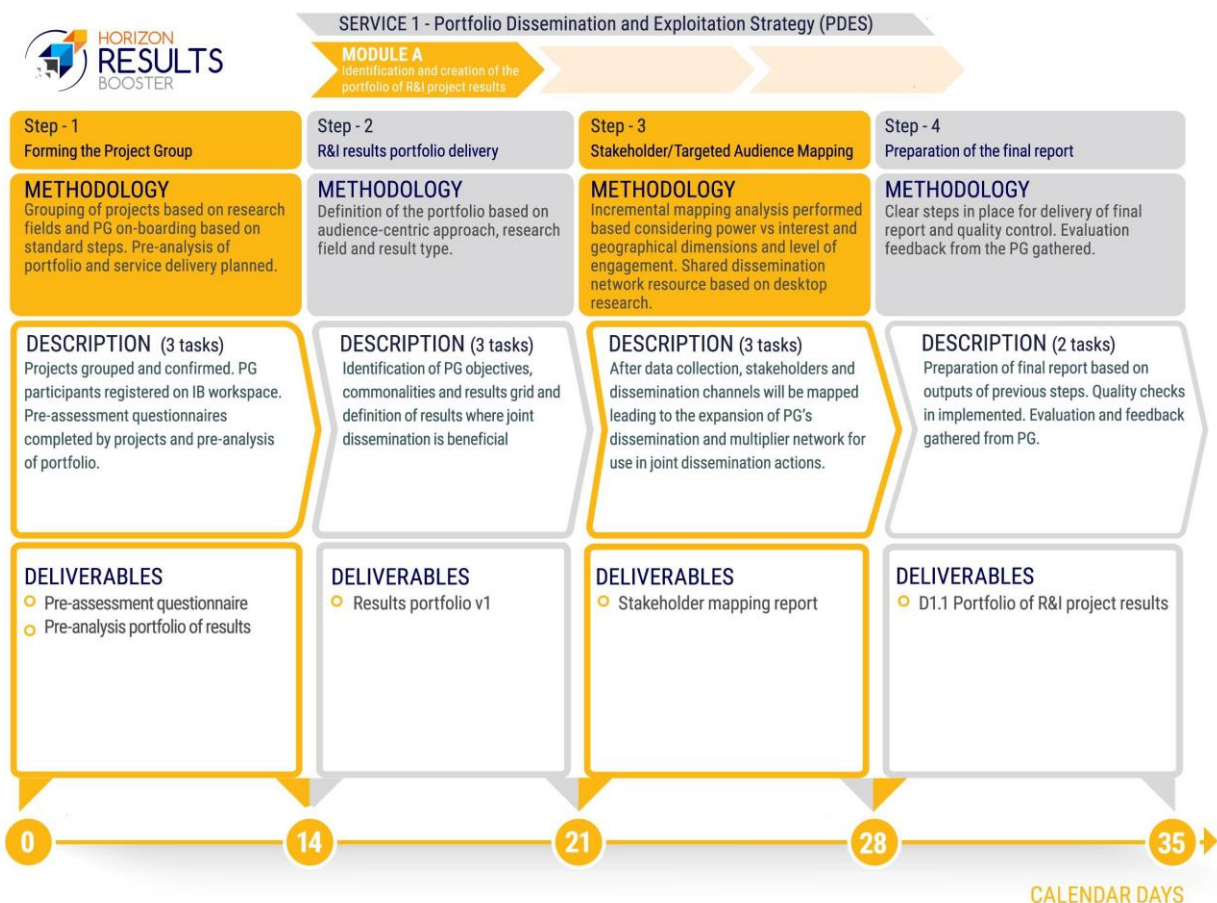- Main Output: D1.1 Portfolio of Research and Innovation Results.

Figure 4. Module A- Overview and timelines

The following sub-sections highlight most relevant results as part of the Project Group's portfolio of research and innovation results.

2.7.1. Insights from stakeholder analysis

The stakeholder analysis that was carried out within Service 1, Module A of the HRB, helped the SENTINEL consortium to identify the most relevant segments to target within our communication and dissemination activities and how to address them in terms of formats. In order to attract new end users, the following suggestions were made:

- Create targeted dissemination materials, such as a video/demo and make use of social media, also through a paid-for social media campaign, for example on LinkedIn.
- Use different communication channels, including social media, website, blogs and newsletters to reach a wider audience.
- Present project results at pertinent conferences, seminars, and business events.
- In order to make project outcomes more tangible and understandable by SMEs, realise practical guidelines and/or instructions for SMEs to implement the project's results in their business practices.

- Collaborate with different stakeholders to raise awareness about cybersecurity, personal data protection and GDPR compliance.

2.7.2. Channels to approach audience

By analysing SENTINEL collective target stakeholders, it was recommended the following channels to approach our audience:

- Horizon Results Platform: It is recommended that the project upload its key exploitable results on the EC Horizon Results Platform to showcase outcomes, network, form partnerships, and attract investors and policymakers, enhancing project exploitation and visibility.
- CORDIS Results Packs: The project should utilize the CORDIS platform to package and present results in an accessible format for professionals in cybersecurity, personal data protection, and GDPR compliance, and then promote these results widely
- Demos and Videos: Tailored demos and videos should address specific challenges faced by startups, SMEs, large enterprises, and other stakeholders, with variations tailored for different platforms like social media and websites.
- Website Pages: Developing a dedicated website or specific pages within existing sites to display project results, aimed directly at different stakeholder groups such as SMEs, policymakers, researchers, and academia, ensures targeted communication.
- Social Media Strategy: Utilizing Twitter, identify and use popular hashtags and influencers to enhance visibility and engagement. Consider a joint project account for cohesive communication.
- Press Releases: Analyse media styles and topics to craft effective press releases that resonate with the press and offer exclusive interviews to deepen media engagement.
- Infographics: Create infographics that highlight key statistics and facts relevant to each stakeholder, optimized for online sharing, especially on social media.
- Policy Briefs: Develop policy briefs or position papers on cybersecurity to influence policy and provide stakeholders with authoritative insights into the project's impact and goals.

2.7.3. Conclusions and recommendations

Following the recommendations provided to the Project Group, we started by established a branding for the cluster projects group called the SecureCyber cluster. Also, we've initiated the publication of joint newsletters in a monthly basis and increased our collaborative efforts in hosting events, such as workshops, and webinars. With SecureCyber, our aim is to establish a unified entry point that consolidates and keeps track of the most significant achievements of the cluster projects. To facilitate access to this information, we've created a LinkedIn page: https://www.linkedin.com/company/101340030.

From the SENTINEL perspective, we have intensified our engagement with potential end-users by organizing two more SME-centric workshops, to reach wider audiences and create more impact. To make project outcomes more tangible and understandable for SMEs, we have focused on making the SENTINEL platform more attractive and easier to use by actively collecting and addressing feedback from end-users. Additionally, to increase the visibility of project results, we have partnered with other cluster projects to organize workshops, including the SENTINEL final event, and have increased our participation in industrial events such as INFOSHARE 2024.

3. Dissemination and Communication Activities M19 - M36

This section presents in detail the dissemination and communication activities carried out in the M19-M36 project period. During this period, WP7 intensified its efforts on implementing a number of dissemination and communication activities that resulted in the best and most effective promotion of the project.

3.1 Dissemination activities

The following subsections outline the dissemination activities that have been executed in the M19–M36 period. The subsections gather a set of activities that with the combination of communication activities helped to share the project's scope, objectives and results to the SENTINEL target audiences.

3.1.1. Scientific publications

Scientific publications are a broad-based dissemination tool and the SENTINEL academic partners joint efforts to strengthen the impact of dissemination activities by preparing and publishing scientific articles. The following table contains the publications authored by the SENTINEL partners that are directly related to the project.

Table 2. Publications in conference proceedings in the M19-M36 period

Authors & Paper title	Conference Name	DOI/URL
Kostas Drakonakis, Sotiris Ioannidis, Jason Polakis "ReScan: A Middleware Framework for Realistic and Robust Black-box Web Application Scanning"	30th Annual Network and Distributed System Security (NDSS) Symposium 2023, 27 February – 3 March 2023, San Diego, California	https://dx.doi.org/10.14722/ndss.2023.24169
Stephane Cortina, Michel Picard, Samuel Renault, Philippe Valoggia "Digitalizing process assessment approach: An illustration with GDPR Compliance Self-Assessment for SMEs"	European Conference on Software Process Improvement, (EuroSPI) 2023, 30 August – 01 September 2023, France	https://link.springer.com/chapter/10.1007/978-3-031-42310-9_9
George Hatzivasilis, Sotiris Ioannidis, Grigoris Kalogiannis, et al. "Continuous Security Assurance of Modern Supply Chain Ecosystems with Application in Autonomous Driving: The FISHY approach for the secure autonomous driving domain"	IEEE International Conference on Cyber Security and Resilience (IEEE CSR) Workshop on Cyber Resilience and Economics (CRE) 31 July 2023 - 02 August 2023, Venice, Italy	http://dx.doi.org/10.1109/CSR57506.2023.10224971

| Eva Papadogiannaki, Sotiris Ioannidis "Pump Up the JARM: Studying the Evolution of Botnets using Active TLS Fingerprinting" | IEEE Symposium on Computers and Communications (ISCC 2023), July, Gammarth, Tunisia | http://doi.org/10.1109/ISCC58397.2023.10218210 |
| Andreas Theofanous, Eva Papadogiannaki, Alexander Shevtsov, Sotiris Ioannidis "Fingerprinting the Shadows: Unmasking Malicious Servers with Machine Learning-Powered TLS Analysis" | International World Wide Web Conference 2024 (WWW), May 2024, Singapore | https://doi.org/10.5281/zenodo.10655329 |

Table 3. Publications in international referred journals in the M19-M36 period

Authors & Paper title	Journal Name	Status
George Hatzivasilis, Eftychia Lakka, Manos Athanatos, et al. "Swarm-Intelligence for the Modern ICT Ecosystems"	International Journal of Information Security – Special Issue on Cybersecurity in Healthcare, Springer, pp. 1-24, September 2024	Accepted
Eleni-Maria Kalogeraki and Nineta Polemi "A Taxonomy for Cybersecurity Standards"	Journal of Surveillance, Security and Safety" on the Special Issue on Industrial Control Systems Security and Privacy Issues	Accepted
George Hatzivasilis, et al. "Review of Smart Home Security using IoT"	Electronics, MDPI, Special Issue on New Challenges in Information Security and Privacy and Cyber Resilience	Submitted
Fereniki Panagopoulou. "Data Protection for SMEs"	E-politeia magazine, April 2024	https://www.epoliteia.gr/e-journal/2024/04/22/e-politeia-teyxos-10-aprilios-iounios-2024/
Dimitrios Tyrovolas, Nikos A. Mitsiou, Thomas G. Boufikos, et al., "Energy-Aware Trajectory Optimization for UAV-Mounted RIS and Full-Duplex Relay"	IEEE Internet of Things Journal, April 2024	DOI: 10.1109/JIOT.2024.3390767.

Table 4. Special issues in international referred journals in the M19-M36 period

Editors	SI/Journal Name	DOI/URL

| George Hatzivasilis, Sotiris Ioannidis, Konstantinos Fysarakis, Nikolaos Papadakis | Artificial Intelligence Applications in Next Generation Communication Infrastructures Security - Electronics | https://www.mdpi.com/journal/electronics/special_issues/AI_next_generation_communication_infrastructures_security |
| George Hatzivasilis, Sotiris Ioannidis, Vasileios Mavroeidis, Vasilis Katos | New Challenges in Information Security and Privacy and Cyber Resilience - Electronics | https://www.mdpi.com/journal/electronics/special_issues/Information_Security |

3.1.2. Dissemination events organized by SENTINEL

During the 2nd project phase, the consortium continued sharing knowledge and engaging key stakeholders. In this respect, the consortium has organized four (4) additional events which are listed in the table below. Each event, targeting different stakeholder groups, has contributed to the broader reach and impact.

Table 5. Events promoted by the SENTINEL partners in the M19-M36 period

Event	Date	Location	Partner
SME-centric workshop IV	25/09/2023	Online	UNINOVA
Cyber Security and Data Protection Synergies – Joint Cluster Event	16 - 17/10/2023	Lisbon, Portugal and online	ITML/UNINOVA
SME-centric workshop V	27/02/24	Athens, Greece	ITML
SENTINEL Final Event	09/04/2024	Stockholm, Sweden	ITML, INTRA, FP, UNINOVA, LIST, IDIR

3.1.2.1.   SME-centric workshop IV

The 4th pilot demonstration occurred on September 25th, 2023. The SENTINEL partners organised the SME-centric workshop, with the main scope of demonstrating the SENTINEL platform within the third pilot of the project, among external entities who have engaged via DIHs (Digital Innovation Hubs). The workshop was held online, gathering 48 participants from 24 SMEs in total. Prior to event, a full guide of instructions has been shared to the participants in order to proceed correctly with the evaluation and trial of the platform.

The external SMEs have been kindly invited to validate the Full Featured Version (FFV) of the SENTINEL platform from a twofold perspective. Firstly, to test the available functionalities of SENTINEL FFV under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trial along with other validation criteria, such as usability, performance, user satisfaction, user interface (UI), etc. And secondly, to test the way that SENTINEL FFV addresses privacy, personal data protection, and cybersecurity requirements of different processing activities utilised by SMEs in their daily business. The aim was to showcase

the platform to the SME participants and assist them to create their profiles for the organisation and follow all the instructions in order to validate all the functionalities of the SENTINEL platform.

During the event, the SMEs were invited to contribute and answer interactive questionnaire to collect data about user experience, profiling, relevance of the tool and level of awareness. The results of the questionnaire can be found in Deliverable 7.6 - Section 4.2. The Platform Demonstration video recorded during the event is available on the Sentinel Youtube Channel[1].

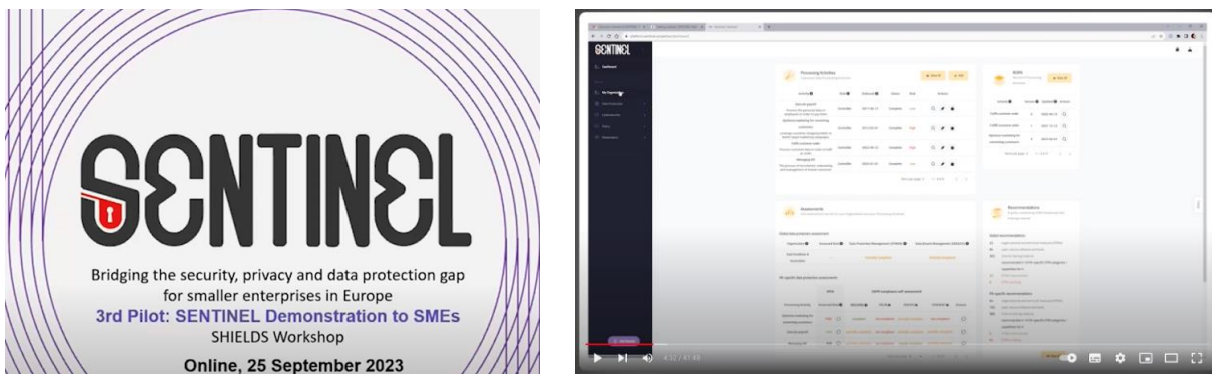*Figure 5. SME-centric workshop IV agenda*

Figure 6. SME-centric workshop IV

3.1.2.2. *Cyber Security and Data Protection Synergies – Joint Cluster Meeting*

The SENTINEL project has co-organised the "Cyber Security and Data Protection Synergies – Joint Cluster" hybrid Event. The event took place at UNINOVA premises, in Portugal, on the 16th

---

[1] https://www.youtube.com/watch?v=E9K67qc9Gx4

and 17th of October 2023 inviting also external participants to join a training session held on the 2nd day of the event.

The agenda included various presentations made by invited sister project representatives together with open discussion on relevant topics of the cyber security and data protection domain. The projects co-hosted the event were: the IDUNN Project, KRAKEN H2020, Electron Project, Secant project, CROSSCON, TRUSTaWARE, IRIS H2020 Project, SPATIAL Project, ERATOSTHENES PROJECT and the ARCADIAN-IoT. The event kicked off by the WP7 (Ecosystem building, Exploitation and sustainability management) leader of SENTINEL, the UNINOVA partner. Also, a keynote presentation took place in the beginning of the agenda from the Project Adviser of the SENTINEL project.

The main goal of this cluster event was to stimulate cooperation and synergy among diverse projects in EU cybersecurity. By uniting representatives from various initiatives, we seek to foster the exchange of knowledge, resources, and expertise. This endeavor leads to heightened effectiveness and comprehensive cybersecurity solutions tailored for the EU market.

Figure 7. Joint Cluster Meeting

The training session was open to the public and was held on the 2nd day of the event, on 17th of October 2023. The session covered a range of topics such as CyberRange for security professionals training, Integrating Blockchain with IoT for Secure and Scalable Decentralised Identity Management, etc.

Moreover, the event included a presentation of "Next Horizon Europe Calls - Topics for 2024 and pitching", presented by the SENTINEL partner, UNINOVA. The Synergies - Joint Cluster Event

was a great opportunity to create and promote more connections in the research community. There were almost 30 external attendees, and during the two-day event, all projects were involved in discussing synergies and collaborations. The highlights from this event are available on SENTINEL Youtube Channel[2]

Figure 8. Cyber Security and Data Protection Synergies – Joint Cluster Event

3.1.2.3. SME-centric workshop V

The final SME-centric workshop was held in Athens, Greece, on the 27th of February during the 2nd day of the SENTINEL plenary meeting. The event aimed to present the main achievements reached within the scope of the project, demonstrate the SENTINEL platform and elaborate on the innovation capacities of the project. It covered topics related to GDPR, personal data protection and cyber security and how these aspects can affect the SMEs' core business activities.

Figure 9. SME-centric workshop V agenda

---

[2] https://www.youtube.com/watch?v=2oOVyQmb8nw

The SENTINEL platform was presented to the audience highlighting its innovation capacities, and how an SME can utilize them to leverage its privacy and cybersecurity. The workshop welcomed 11 companies from the private sector, small and medium-sized enterprises (SMEs), startups, and Small Business Entities, without any sector restrictions.

During the event, SMEs were invited to test SENTINEL and leave their feedback and first impression through an interactive questionnaire. The results of the questionnaire can be found in Deliverable 7.6 - Section 4.3.

Figure 10. SME-centric Workshop V

3.1.2.4.   SENTINEL - ARCADIAN-IoT Symposium & Showcase (SENTINEL Final Event)

The ARCADIAN-IoT & SENTINEL Symposium and Showcase event was scheduled for the 9th of April 2024. It was a comprehensive in-person event dedicated to demonstrating the innovation capacities of both ARCADIAN-IoT and SENTINEL projects towards integrated and automated IoT Cybersecurity and Personal Data Protection, which counted with 40 physical participants. The event kicked off with a keynote presentation of the Project Adviser of both projects.

In its IoT cybersecurity stream, the event emphasised the holistic cybersecurity challenges and advancements in IoT while addressing identity, trust, security, privacy, and recovery aspects. Notable presentations included an overview of the EU IoT security landscape, key innovations from ARCADIAN-IoT and their demonstration across various IoT application domains including drones for private safety, smart grids, and medical IoT.

In the Privacy compliance stream, the symposium highlighted on how to bridge the gap in personal data protection and cybersecurity for SMEs. The stream included discussions on the EU data protection landscape, key organisational and technical measures towards GDPR compliance, as well as life demonstration on SENTINEL's one-stop-shop platform developed to increase SMEs' security in the cyberspace and protect their data and digital assets.

A panel session at the end of the event was dedicated to exploring the unaddressed challenges and opportunities for IoT cybersecurity and data privacy.

08.30 – 09.00 WELCOME AND REGISTRATION

09:00 – 12:35 MORNING SESSION: OUTCOMES AND LEARNINGS FROM ARCADIAN-IOT AND SENTINEL PROJECTS

- 09:00 – 09:15 Welcome from ARCADIAN-IoT and SENTINEL projects and RISE Sweden
- 09:15 – 09:35 European projects' afterlife (Juuso Stenfors, European Commission)

Stream A – Holistic cybersecurity addressing identity, trust, security, privacy and recovery

- 09:35 – 09:50 EU IoT security landscape overview (Shahid Rasa – RISE)
- 09:50 – 10:05 Enabling holistic cybersecurity for IoT (Sérgio Figueiredo – IPN, ARCADIAN-IoT Project coordinator)
- 10:05 – 11:05 Holistic Cybersecurity applied to specific IoT application domains: Drones for private safety (Pedro Colarejo – LOAD) | Smart grids (Alexandru Gliga – BOX2M) | Medical IoT (Ricardo Nolasco Ruiz – RGB Medical)

Coffee break | Poster exhibition

Stream B – Security and Personal Data Protection for SMEs

- 11:30 – 11:55 EU data protection landscape: EU data protection landscape; Intro to SENTINEL(George Bravos – ITML) | Key challenges and drivers (Manolis Falelakis – INTRA) | Data protection requirements and challenges (Philippe Valoggia – LIST) | The importance of organisational and technical measures (Thanos Karantjias – FP)
- 11:55 – 12:35 Enabling one-stop-shop security and personal data protection: Organisation profiling and processing activities record-keeping (Yannis Skourtis – IDIR) | Self-assessments and policy recommendations (Thanos Karantjias – FP) | Q&A

Lunch break | Poster exhibition

13:35 – 16:35 AFTERNOON SESSION: EUROPEAN CYBERSECURITY & DATA PRIVACY INDUSTRY AND RESEARCH LANDSCAPE

- 13:35 – 13:55 Keynote from Ericsson R&D (Eva Fogelström)
- 13:55 – 16:00 European Cybersecurity & Data Privacy: Research and Industry landscape: Moderator Shahid Raza (RISE) | Participants: Eva Fogelström (Ericsson), Sérgio Figueiredo (IPN, ARCADIAN-IoT Project coordinator), Giovanni Maria Riccio (E-lex), Philippe Valoggia (LIST, SENTINEL Project), Francesco Regazzoni (SECURED project).

Coffee-break | Poster exhibition

CONT. AFTERNOON SESSION

- 16:20 – 16:35 Closing remarks

Figure 11. SENTINEL - ARCADIAN-IoT Symposium & Show-case agenda

Figure 12. SENTINEL - ARCADIAN-IoT Symposium & Showcase

3.1.3. Participation in third-party events and conferences

Within the reference period, SENTINEL also recorded intensive third-party event participation. The members of the consortium seized the opportunity to spread, (directly or indirectly), information about SENTINEL and develop a network among interested stakeholders in several dissemination events. These activities are listed in the table below:

Table 6. Participation in third-party events and conferences in the M19-M36 period

Event	Date	Location	Partners
Joint Cyber Security Webinar	19/01/2023	Online	ITML
Safer Internet Day	10/02/2023	Greece	TUC
EU-Made Cybersecurity for Safe, Resilient and Trustworthy Applications and Services" - Workshop	27/02/2023	Online	UNINOVA
FIC Forum 2023	6-7/04/2023	Lille, France	ACS, AEGIS
Security Strategy 2023 - IDC Security Roadshow	20/04/2023	Lisbon, Portugal	UNINOVA
PUZZLE's Cybersecurity Conference	21/06/2023	Novi Sad, Servia	AEGIS
Final Event of the CitySCAPE project	28/06/2023	Athens, Greece	ITML
CyberHOT Summer School 2023	29/09/2023	Crete, Greece	TUC

ATTRACT EDIH public presentation	10/01/2024	Oporto, Portugal	UNINOVA
AIP Roadshow I&D	29/02/2024	Portugal	UNINOVA
Data Protection Day	29/02/2024	Luxembourg	LIST
Cyber Threat Intelligence: Empowering IoT Security Workshop- CTI Workshop	06/03/2024	Online	ITML
Conference presentations			
Conference	**Date**	**Location**	**Partner**
30th Annual Network and Distributed system Security Symposium 2023 (NDSS)	27/02/2023 – 03/03/2023	San Diego, USA	TUC
28th IEEE Symposium on Computers and Communications (ISCC),	09-12/07/2023	Tunis, Tunisia	TUC
IEEE International Conference on Cyber Security and Resilience (CSR) Workshop on Cyber Resilience and Economics (CRE)	31/07/2023 – 02/08/2023	Hybrid	TUC
30th European Conference on Software Process Improvement, (EuroSPI) Conference	01/09/2023	France	LIST
International World Wide Web Conference 2024 (WWW)	13-17 May 2024,	Singapore	TUC
INFOSHARE Conference	22-23/05/2024	Poland	ITML, STS, AEGIS and INTRA

3.1.4. Networking and liaisons with other relevant projects

The aim of this communication approach was to plan and implement joint activities with relevant projects, initiatives and networks. This was facilitated through various channels including the project website, but also the links and networking profiles of the SENTINEL partners that are part of several consortia and networks. Towards this effort, the relevant projects that the SENTINEL project has established contacts during the 2nd half of the project are listed below.

Table 7. Networking and liaisons with other projects in the M19-M36 period

Project	**Further information**
HEIR	https://heir2020.eu/
CROSSCON	https://crosscon.eu/
KRAKEN	https://www.krakenh2020.eu/
SPATIAL	https://spatial-h2020.eu/
TRUST AWARE	https://trustaware.eu/
ELECTRON	https://electron-project.eu/

Highly supported by these projects, the "SecureCyber Cluster" initiative was created in January 2024. A group of very talented people from all the cluster projects, aiming to organize joint collaborative activities. These activities were supported by a LinkedIn page[3] and a periodic newsletter which provide information about dissemination and communication conducted by this initiative on a regular basis. Up to now, four (4) newsletter issues have been produced and are available in LinkedIn page.

Figure 13. SecureCyber cluster logo

SENTINEL has been actively participating in SecureCyber Cluster, by contributing with relevant content for the periodic newsletters, participating in the monthly meetings and helping to disseminate news from the cluster projects.

3.2 Communication activities

The communication plan gathers a set of strategically planned communication activities aiming at promoting the results of the project to a multitude of audiences (including media and public) in an effective manner and possibly engaging in a two-way exchange to ensure that the project stakeholders are properly informed about the objectives and offerings. In this context, a range of SENTINEL communication and promotion materials have been released during this time period and are uploaded to the project's website:

- SENTINEL branding material (business card, roll-up, leaflet, poster)
- SENTINEL videos/podcasts
- SENTINEL newsletters

3.2.1 SENTINEL branding material

The SENTINEL branding material developed is presented in APPENDIX-II of D7.3. In addition to this one addition branding material was designed and presented during the InfoShare 2024 event in May 2024

---

[3] https://www.linkedin.com/company/101340030/admin/feed/posts

Figure 14. SENTINEL branding material presented in the Infoshare2024 event

3.2.2 SENTINEL videos and podcasts

Several video/podcasts have been created over the course of the M19-M36 project period and shared via the project's website and YouTube channel. These materials are listed in the table below.

Table 8. SENTINEL videos and podcasts released in the M19-M36 period

	Type of Material	**Date**	**Link**
SENTINEL Videos	Joint Cyber Security Workshop	28/02/2023	https://www.youtube.com/watch?v=GPYM07a8z9g
	Shields Workshop - Highlights	20/10/2023	https://www.youtube.com/watch?v=7D3OCjF9NK4
	Synergies – Joint Cluster Event – Highlights	24/10/2023	https://www.youtube.com/watch?v=2oOVyQmb8nw
	Sentinel Platform Presentation – 3rd SME Centric Work-shop	03/11/2023	https://www.youtube.com/watch?v=E9K67qc9Gx4
	Final SME Centric Workshop - High-lights	11/03/2024	https://www.youtube.com/watch?v=rUiIXcF-ucY

	Final Event	09/04/2024	https://www.youtube.com/watch?v=rUiIXcF-ucY
SENTINEL Podcasts	Podcast #5 – talk with Pedro Rosa	03/01/2023	https://www.youtube.com/watch?v=XVeXe4CGXJk
	Podcast #6 – talk with Ana Ferreira, Woman4Cyber	07/02/2023	https://www.youtube.com/watch?v=myxAEYojcKQ
	Podcast #7 – Paulo Antunes, Phd student	04/05/2023	https://www.youtube.com/watch?v=Otjro9y4nb4
	Podcast #8 – talk with Daryl Holkham	17/07/2023	https://www.youtube.com/watch?v=lNfcBKBAwWs
	Podcast #9 – talk with Marinos Tsantekidis and Stavros Tsipras	26/072023	https://www.youtube.com/watch?v=Kw64H9R7_OI
	Podcast #10 – Talk with Kostas Poulios	29/01/2024	https://www.youtube.com/watch?v=8dG9hIt0OVM

3.2.3 SENTINEL newsletters

The next informative material is the SENTINEL newsletter. The purpose of releasing newsletters is to create a news item that can briefly illustrate the project updates. The newsletters described the project's progress related to technical activities, project publications as well as other dissemination and communication activities. The material preparation was conducted by UNINOVA with the support and valuable inputs of all the partners. Proof-reading activities were conducted by ITML. During the 2nd half of the project the following newsletters were prepared and released.

Table 9. SENTINEL newsletters released in the M19-M36 period

Type of Material	Date	Link
Newsletter #6	March, 2023	
Newsletter #7	June, 2023	
Newsletter #8	October, 2023	https://sentinel-project.eu/dissemination-materials/
Newsletter #9	March, 2024	
Newsletter #10	May, 2024	

3.2.4 SENTINEL social media

The presence of the SENTINEL project in social media continued to be one of the key actions for dissemination and communication activities. SENTINEL's presence in social network is enabled via three main social media channels namely, LinkedIn, Twitter, YouTube and Zenodo Community.

The maintenance of LinkedIn, Twitter and YouTube channels was carried out by DEM. Regular posts and updates relating to the project's developments and news, as well as reporting interesting news about project related topic have been published in these channels during the reporting period. The dissemination team strategically focused on the quality rather than the quantity of posts, aligning with the review recommendation for a more impactful social media presence. As a result, these accounts have shown significant growth by M36 compared to M18. This approach has also helped for interaction with both industrial and academic communities, and the general public, to provide information about the progress of the project and allowing for a means of a directly communicated feedback and information sharing mechanism. In addition, the YouTube channel has observed a substantial growth in content and viewership by the end of the third year. The enhanced content strategy, focusing on high-quality video production, has effectively showcased the project's outcomes to a commercial-oriented audience.

Finally, the project's Zenodo Community has been a keystone for providing open access to all publications and results of the project.

SENTINEL Zenodo Community[4]	
Number of Items Uploaded	39 items
Number of Downloads & Views	~1,500

The website and social media channels' main statistics for the M19-M36 period are illustrated in Appendices in more detail.

---

[4] https://zenodo.org/communities/sentinel-h2020/records?q=&l=list&p=1&s=10&sort=newest

4. Conclusion

As the SENTINEL project reaches the last phase, we are proud to state that the project has achieved its success in bridging the security, privacy, and data protection gaps for small and medium-sized enterprises across Europe. The dissemination and communication activities implemented, had contributed to raising awareness, engaging stakeholders, and promoting the adoption of the SENTINEL's offerings.

Throughout this period, SENTINEL has executed an effective dissemination strategy that included the publication of relevant scientific papers, active participation in key industry events, and liaisons with relevant projects and key stakeholders. These efforts were complemented by communication activities that effectively used digital platforms, social media, and direct engagements through workshops, ensuring widespread visibility and impact.

The project's ability to foster collaborations, both within the consortium and with external entities, has been fundamental. Organizing events like the Joint Cluster event aiming to foster strategic liaisons with other projects, SME-centric workshops prove to be a unique playground to effectively pitch SENTINEL offerings, leading to strength the data protection and cybersecurity ecosystem and create valuable synergies with key stakeholders in a joint endeavour to address emerging challenges in cybersecurity and data protection.

Moreover, the development of multiple communication tools such as newsletters, podcasts, and videos has enabled SENTINEL to maintain an ongoing dialogue with its diverse audience, ensuring that the project's innovations and benefits were clearly understood and readily accessible. These tools have not only facilitated the dissemination of results but have also laid the groundwork for sustained impact beyond the project's duration.

In conclusion, we truly believe that SENTINEL project has not only met its dissemination objectives but has also set a strong foundation for the continued evolution and uptake of its results. As the project transitions from dissemination to sustained exploitation, the strategies implemented will continue to influence and shape the cybersecurity and data protection landscape, supporting SMEs in their journey towards enhanced digital security and GDPR compliance.

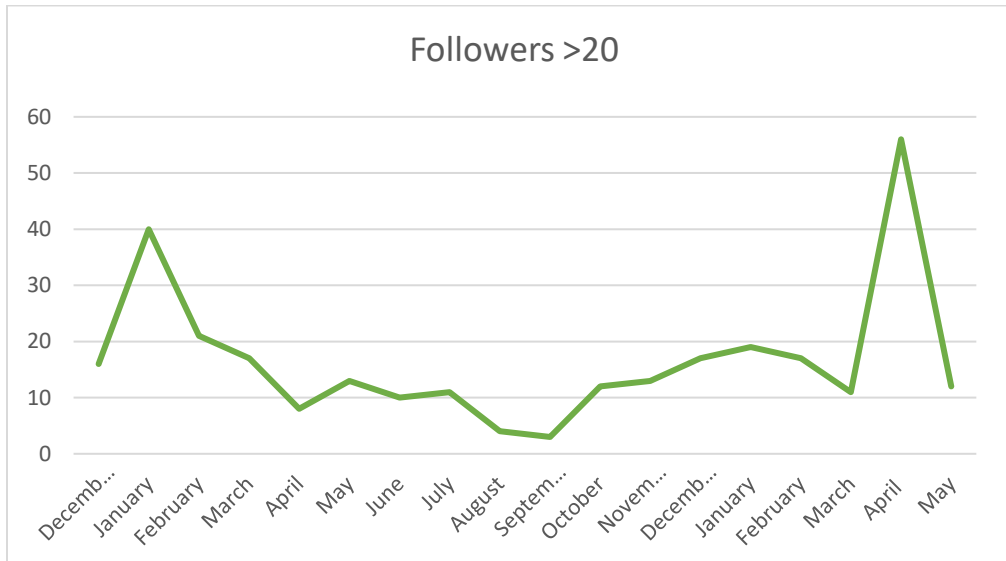# Appendices

Appendix – I: SENTINEL website and social media
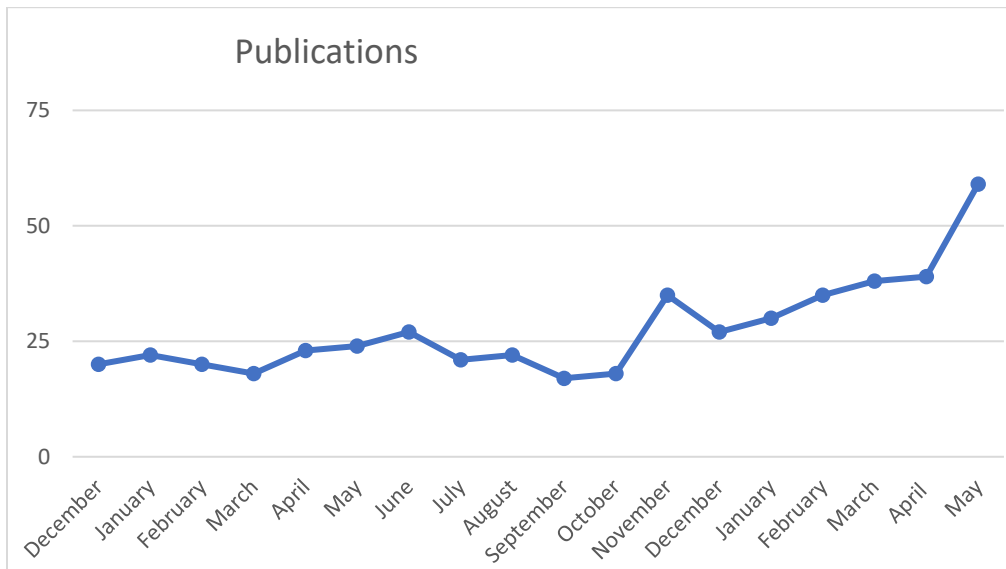
a) SENTINEL website (M19-M36)

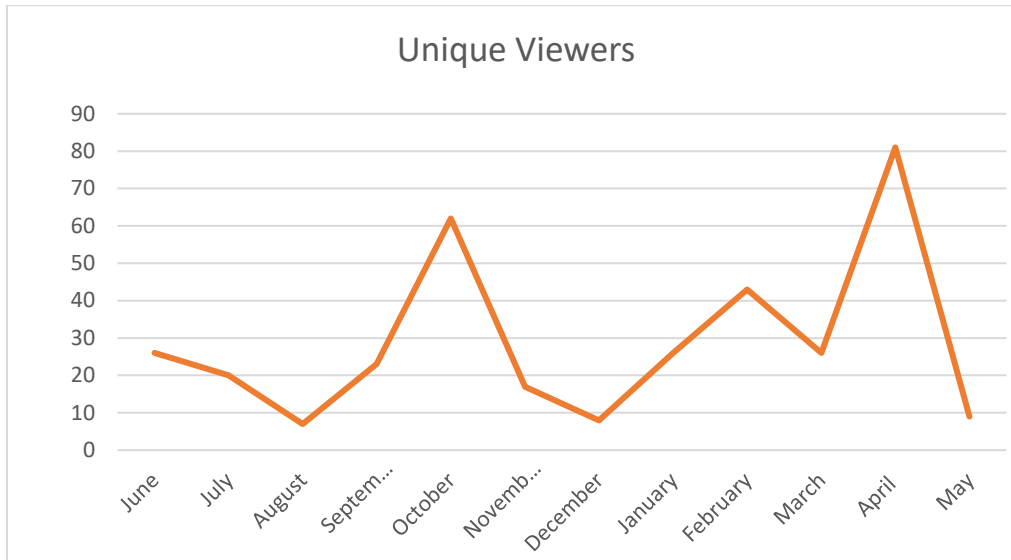**Pageviews and Downloads**
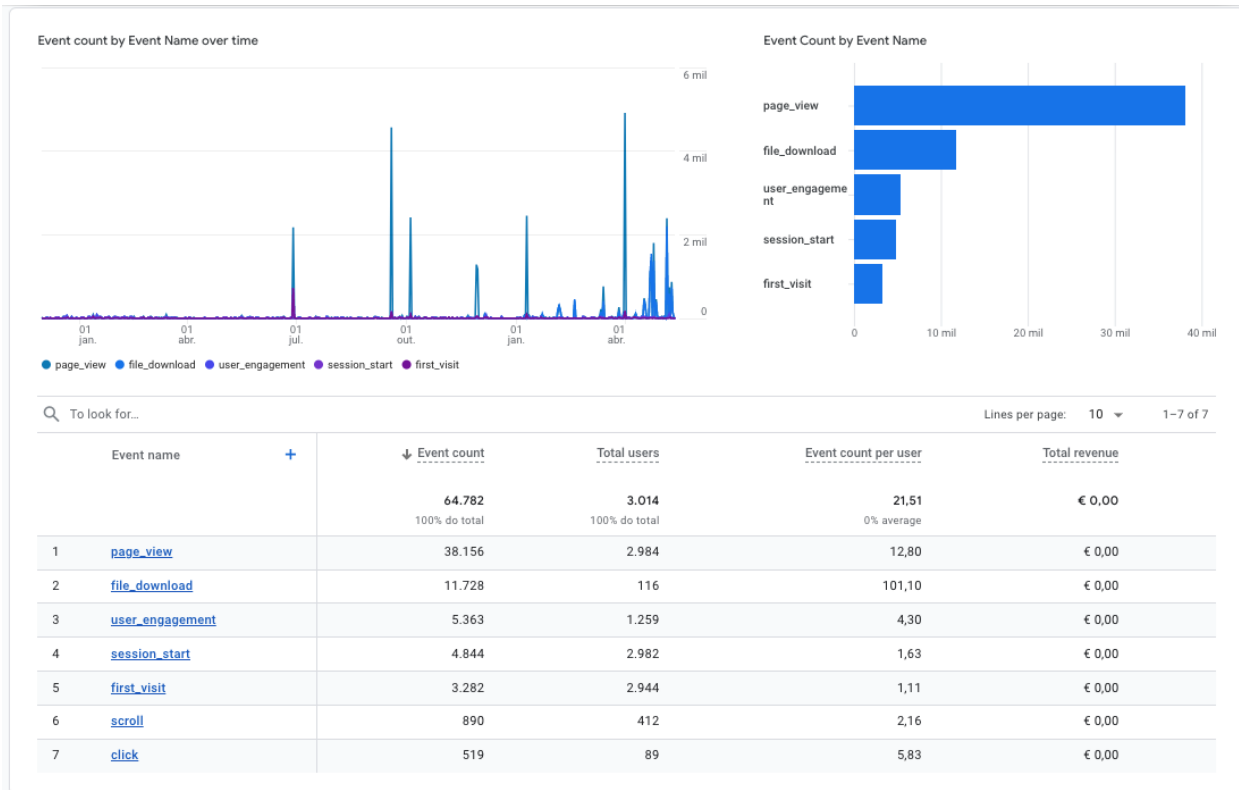
b) SENTINEL LinkedIn page (M19-M36)

Number of followers
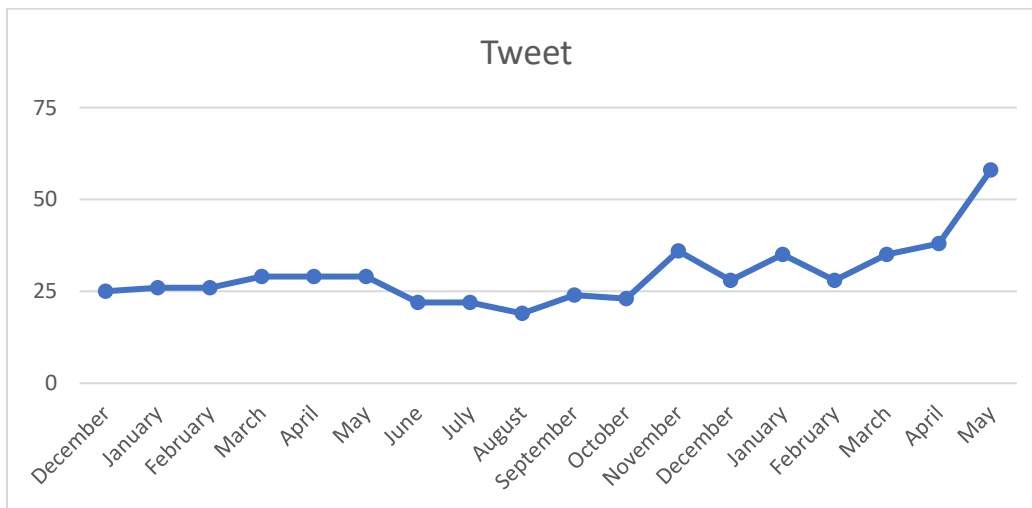

Followers >20

Number of posts

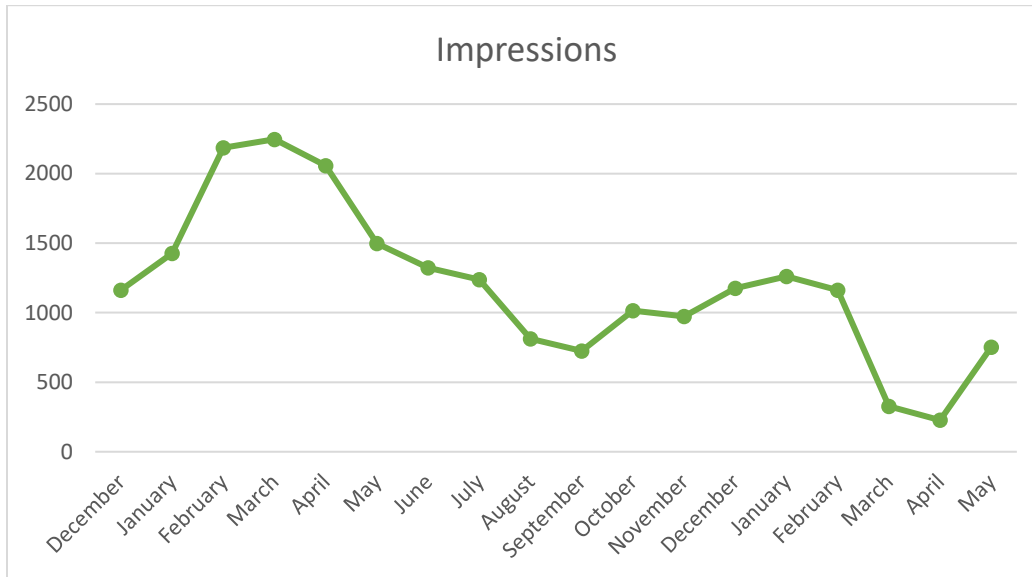Publications

Number of Unique Viewers

c) SENTINEL Twitter page (M19-M36)

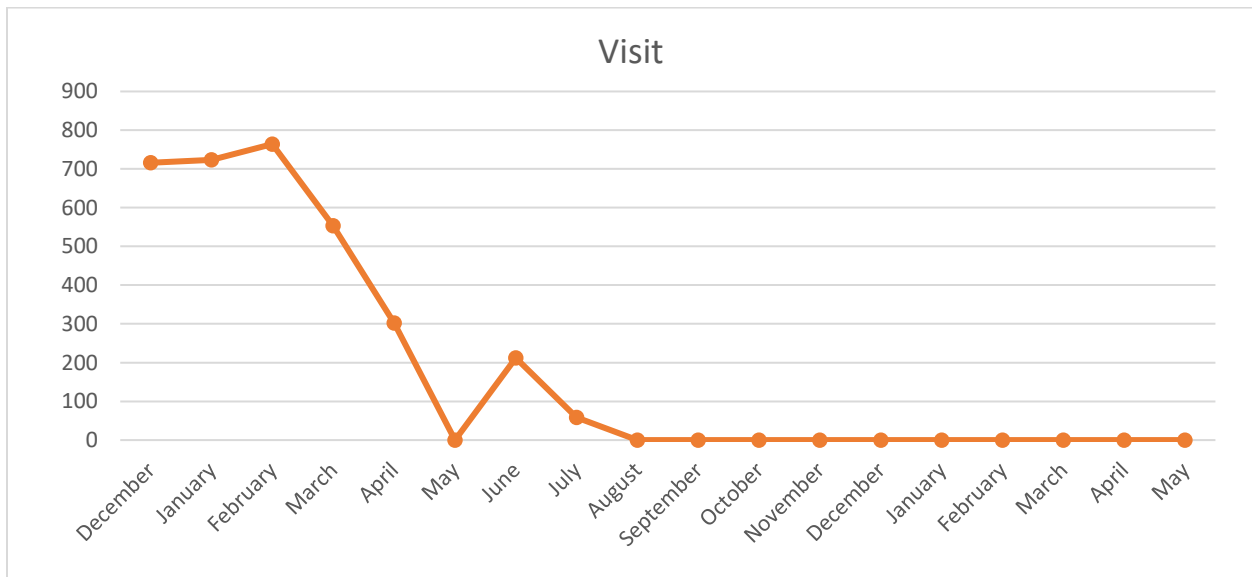**Number of tweets**

Number of impressions

Number of visits[5]

---

[5] *After the change of Twitter to X (July 2023), this number became unavailable.*