Digital4Security Communication Strategy

Deliverable 5.1

29/02/2024 | DIGITALEUROPE

Table of Contents

List of Figures

List of Tables

List of abbreviations and acronyms

Term	Definition
WP5	Work Package 5
KPIs	Key performance indicators
SMEs	Small and medium-sized enterprises
D4S	Digital4Security
HEIs	Higher education Institutes
DSJP	Digital Skills and Jobs Platform
ECSF	European Cybersecurity Skills Framework
HaDEA	European Health and Digital Executive Agency

About the Digital4Security project

Digital4Security is a ground-breaking pan-European master's programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. With funding of almost €20 million from the European Union, this four-year initiative has garnered support from a Consortium comprising 35 Partners spanning 14 countries. This industry-driven programme will provide comprehensive knowledge of cybersecurity management, regulatory compliance and technical expertise to European SMEs and companies.

The communication strategy, a deliverable within the framework of Work Package 5 (WP5) for dissemination and European impact, aims at wide and effective outreach to target audiences to ensure visibility of the project and the Master's in Cybersecurity Management & Data Sovereignty among all relevant stakeholders. Its goal is also to present the overall planning for promotional strategy (RACE approach), including the communication campaigns (T5.3 and T5.7), and to outline communication activities to reach the target public. The communication strategy is built on the capacities and networks of the project Partners and in close collaboration between the Consortium team and WP5 leaders and co-leaders.

In particular, WP5 focuses on developing a dynamic pan-European Cybersecurity stakeholder ecosystem and supporting the implementation of a European Master's Programme in Cybersecurity Management. The main activities within WP5 include:

- Creation of **communications strategy, branding, and communications materials (T5.1)** in collaboration with various Partners.
- Setup and management of **digital marketing channels, tools, and website (T5.2).**
- Launch of **Digital4Security EU-wide communications campaign** to promote the Digital4Security programme, targeting potential students and industry Partners **(T5.3).**
- Collaborating with the **Digital Skills and Jobs Platform** with the goal of publishing online learning resources **(T5.4)**.
- Establishing **a Partnership development programme** to build a pan-European ecosystem of industry and education Partners and strengthen the network of contributors and host companies involved in the programme **(T5.5).**
- Conducting surveys and interviews to develop **case studies and good practice examples** to promote the programme's results **(T5.6)**.
- Implementing an **Industry and Education Campaign** to encourage the adoption of the programme format by industry and education providers **(T5.7).**
- Setting up a **monitoring tool to collect data** on communication actions and campaigns' performance to provide recommendations for improvement **(T5.8)**.

Overall, WP5 aims to establish a robust communication strategy, promote the Digital4Security programme, build Partnerships, and monitor communication performance to ensure the successful implementation and adoption of the European Master's Programme in Cybersecurity Management.

The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European Partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry Partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

Partners	Acronym
NATIONAL UNIVERSITY OF SCIENCE AND TEHNOLOGY POLITEHNICA BUCHAREST	NUSTPB
SCHUMAN ASSOCIATES SCRL	SA
ATAYA & PARTNERS	ATAYA
POLITECNICO DI MILANO	POLIMI
POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP
CONTRADER SRL	CONTRADER
DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL
INDEPENDENT PICTURES LIMITED	Indiepics
MATRIX INTERNET APPLICATIONS LIMITED	MATRIX
PROFIL KLETT D.O.O.	PROFIL KLETT
SERVICENOW IRELAND LIMITED	ServiceNow
UNIVERSITA DEGLI STUDI DI BRESCIA	UNIBS
UNIVERSITY OF DIGITAL SCIENCE GGMBH	UDS
SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET
IT@CORK ASSOCIATION LIMITED LBG	IT@CORK
ADECCO FORMAZIONE SRL	ADECCO TRAINING
UNIVERSITAT KOBLENZ	UNI KO
VYSOKE UCENI TECHNICKE V BRNE	BRNO UNIVERSITY
MUNSTER TECHNOLOGICAL UNIVERSITY	MTU
EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME
DIGITALEUROPE AISBL	DIGITALEUROPE

MYKOLO ROMERIO UNIVERSITETAS	MRU
SVEUCILISTE U RIJECI	UNIRI
NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK
UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	UNIR
NATIONAL COLLEGE OF IRELAND	NCI
TERAWE TECHNOLOGIES LIMITED	TERAWE
CY CERGY PARIS UNIVERSITE	CY CERGY PARIS
BANCO SANTANDER SA	BANCO SANTANDER
CYBER RANGES LTD	SILENSEC
RED OPEN S.R.L.	RED OPEN S.R.L.
VYTAUTO DIDZIOJO UNIVERSITETA	VMU

Associated Partners	Acronym
FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG
Pearson Benelux BV	Pearson Benelux
AGORIA ASBL	AGORIA ASBL

Document Control Information

Project	Digital4Security
Document Title	Digital4Security Communications Strategy
Work Package Number	WP5
Deliverable Number	D5.1
Lead Beneficiary	DIGITALEUROPE
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (NUSTPB)
Dissemination Level	**Sensitive** — limited under the conditions of the Grant Agreement
Authors	Irene Marinelli (DIGITALEUROPE), Fionnuala Mahon (MATRIX), Aoife O'Driscoll (MATRIX), Brian Cochrane (Schuman Associates), Lucia Grilli (Schuman Associates).
Reviewers	Chiara Longobard (DIGITALEUROPE), Eleonora Censorii (DIGITALEUROPE), Conor McCaffrey (MATRIX).
Description	Description
Status	**Final version**
Delivery Date	29.02.2024
Due date	29.02.2024
Approval Date:	29.02.2024

Revision history

Version	Date	Modified by	Comments
1	20.11.2023	Irene Marinelli (DIGITALEUROPE), Fionnuala Mahon (MATRIX), Aoife O'Driscoll (MATRIX), Brian Cochrane (Schuman Associates), Lucia Grilli (Schuman Associates)	Draft version
2	08.02.2024	Irene Marinelli (DIGITALEUROPE)	Update Revision History and template
3	23.02.204	Conor McCaffrey	Matrix review
4	29.02.204	Ciprian Mihai Dobre (UNSTPB)	Initial published version

Introduction

Digital4Security is an innovative and market-led European Master's Programme in Cybersecurity Management & Data Sovereignty that will equip European SMEs and Companies across multiple sectors with the cybersecurity management, regulatory and technical skills they need to prevent and respond to existing and emerging cybersecurity threats, helping to safeguard European industries from cyber-attack.

The overall communication strategy for Digital4Security aims at wide and effective outreach to target audiences in order to ensure visibility of the project and the Master's in Cybersecurity Management & Data Sovereignty programme among all relevant stakeholders. This is key in positioning Digital4Secuirty as the most relevant Cybersecurity Master's programme for business leaders and managers in SMEs. The communication strategy is built on the capacities and networks of the project Partners and in close collaboration between the Consortium team and WP5 leaders and co-leaders.

The overall communication strategy, a deliverable within the framework of Work Package 5 (WP5) for dissemination and European impact, aims to present the overall planning for promotional strategy (RACE approach), including the communication campaigns (T5.3 and T5.7), and to outline communication activities to reach the target audiences. The strategy includes a detailed overview of objectives, the key performance indicators (KPIs), the brand concept and strategy, channels, communication tools and activities, which enhances the overall objectives and key messages of the Digital4Security project. It also aims to provide a regularly updated communication calendar of events, communication opportunities and actions to be shared with the Partners' national websites.

The communication strategy has been developed by DIGITALEUROPE, leader of WP5, with contributions and support from the Consortium Partners including MATRIX, Schuman Associates, Indiepics, and Agoria. The communication strategy will be implemented throughout the lifetime of the project based on the active involvement of the above-mentioned project Partners.

This report is the first version of a document that will be further developed and updated by Consortium Partners in the following months for the quarterly communication reports, which will be produced and will support the further developments of future communication actions and campaigns for optimal impact.

Communication objectives and KPIs

Project objectives

The project's vision is to create an innovative and market-led European Master's Programme in Cybersecurity Management & Data Sovereignty, that will equip European SMEs and companies across multiple sectors with the cybersecurity management, regulatory and technical skills they need to prevent and respond to existing and emerging cybersecurity threats.

Main objectives of the project are:

	Goals	Actions
1.	**Addressing skills needs**	Digital4Security will create and implement an advanced, impactful, and sustainable European Cybersecurity Master's Programme. This Master's seeks to generate a consistent pool of qualified cybersecurity management experts, helping to address the growing cybersecurity skills gap that poses a threat to the stability of many European industries and public sector entities.
2.	**Attracting qualified teaching staff and students**	The programme is designed to attract a wide range of students and companies across various sectors, demographics, and cultural backgrounds, ensuring inclusivity and gender equality. The goal is to train more than 2,500 students over the four-year duration. The Consortium boasts a substantial pool of cybersecurity experts from academia and industry, serving as lecturers, mentors, and project leaders for academic courses, on-site/hybrid events, and cyber challenges. Further cybersecurity teachers and trainers can be recruited from our Consortium members and Partners.
3.	**Upgrading digital solutions, equipment and infrastructure, with a special focus on interoperability of IT systems across participating HEIs**	The DIGITAL4Security Master's programme will be administered through a centralised Digital Learning Platform, establishing a collaborative cloud-based technical infrastructure to facilitate connectivity among all Consortium Partners, including higher education institutions (HEIs), training providers, research entities and industry stakeholders, throughout the project.
4.	**Establishing structural and sustainable Partnerships**	The Consortium aims to establish a European Stakeholder Network, bringing together academia, industry, research and employment to collaboratively develop and enhance a Master's Programme for creating highly employable cybersecurity talent. We will provide capacity building and training for programme-delivering institutions, fostering partnerships and facilitating the recruitment of top-tier experts. Central to our approach is the active

		involvement of European companies and SMEs across sectors in designing and delivering the Master's, with ongoing support to identify and address cybersecurity risks and skill gaps.

Table 1: D4S project's objectives

Communication and outreach objectives

To meet the above-mentioned objectives of the project, the communication activities cover three main objectives:

1. **Develop a pan-European Cybersecurity stakeholder ecosystem involving HEIs, industry partners, training providers and cybersecurity clusters to develop, enhance and deliver** an innovative Cybersecurity Management Programme led by top experts from Europe and worldwide.

2. **Support European SMEs and companies in recruiting and upskilling their workforce in cybersecurity roles, integrating them into the Master's programme and** help them to identify cybersecurity risks, skills gaps, European Cybersecurity Skills Framework (ECSF) occupational profiles to retrain or hire candidates to fill these positions.

3. **Create a 'best practice' model for a European Master's Programme in Cybersecurity Management that can be easily and effectively adopted by mid-size European HEIs and EUIs.** This will expand the availability and accessibility of cybersecurity education across Europe.

In specific, as part of the strategy, the communication activities will focus on:

Goals	Main actions
Ensure project EU wide visibility and awareness	• **Defining strategic objectives and KPIs** for each phase of the communications activity and each year of the project. • **Identify the primary, secondary and tertiary target groups** and create a compelling value proposition and key messages. • **Set up D4S digital marketing channels and tools** for effective online promotion (social media channels, email newsletter, D4S landing pages or microsites within each Partner's own website). • **Develop a tactical promotional strategy** to reach and engage each target group with tailored messages via website, social media and email updates. • **Create a new brand identity, guidelines and promotional assets** aligned with EU visual identity guidelines. • **Design and execute a D4S launch campaign** to promote the project to internal and external stakeholders. • **Create a campaign-based strategy** to promote various activities, milestones and initiatives regularly**.** • **Execute an EU-wide online communications campaign and series of webinars and networking events** to promote the project outputs and good practice.

	• **Measure marketing results** against KPIs and report regularly to the European Health and Digital Executive Agency (HaDEA) with interim and final reports.
Enhance engagement with key stakeholders	• **Develop a stakeholder engagement strategy** to connect and develop existing networks of each Partner. • **Invite stakeholder to events, webinars, and networking sessions** with organisations and Partners, and promote project initiatives. • **Establish regular communication channels** (e.g. newsletters, forums) to keep stakeholders informed and engaged. • **Collaborate with industry associations and educational institutions** to amplify project reach and impact.
Foster collaboration and knowledge sharing	• **Facilitate collaboration between project Partners and relevant stakeholders** through workshops and working groups. • **Identify offline marketing opportunities** at EU, regional or national events to promote D4S and its initiatives. • **Liaise closely with the Digital Skills and Jobs Platform** to publish the D4S resources and content, contribute to communications campaigns and participate in webinars. • **Encourage exchange of best practices and lessons learned** among Partners and stakeholders. • **Organise joint initiatives**, such as joint research projects or training programmes, to foster collaboration. • **Promote participation in relevant conferences, seminars, and forums** to share project insights and outcomes.

Table 2: D4S communication activities

Key performance indicators (KPIs)

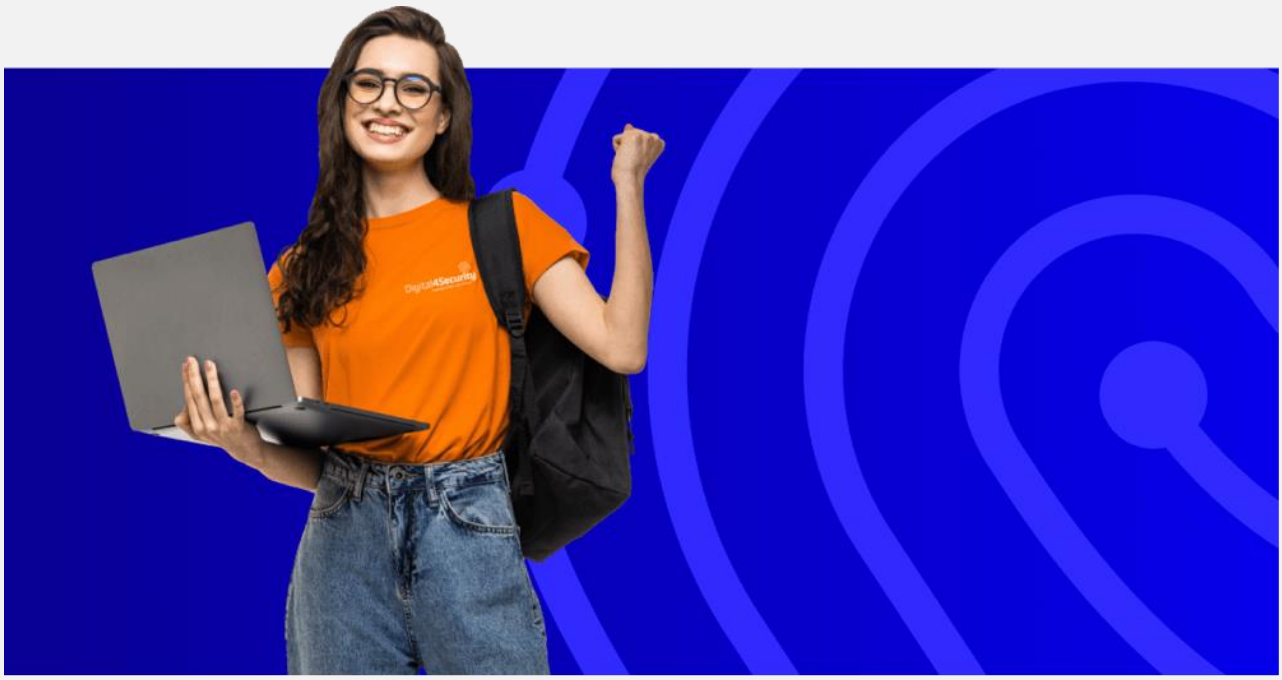
The impact of Digital4Security's communication and dissemination activities will be monitored and measured with the use of key performance indicators (KPIs), as indicated in the table below.

Type	Indicator	M12	M24	M36	M48
Website	Average no. of visitors	6,000	12,000	20,000	22,000
	Average no. of actions per user*	1.0	1.5	2.0	2.5
Project newsletter	No. of issues (*every 3 months*)	2	4	4	4
	No. of subscribers	100	150	200	250
	No. of times the project was promoted in Partners newsletters	10	20	30	40
Social media	Average no. of posts per account	Min. 24	Min. 60		

			(*The frequency can be flexibly increased depending on the promotional activities and the amount of content to be published*)		
	LinkedIn – no. of impressions	15,000	20,000	25,000	35,000
	No. of followers	200	400	600	800
Media outreach	No. of joint press release	2			
	No. of media mentions	4			
Events	Average no. of participants reached via project, Partners' events and third-party events	1,000	1,500	2,000	2,500

Table 3: D4S key performance indicators

**(clicks/downloads/change of pages/internal sites searches)*



SWOT analysis

The SWOT analysis for D4S was undertaken to assess both its internal dynamics and external factors comprehensively in an objective way. This strategic evaluation enables us to leverage the programme's innovative and market-led approach (**Strengths**), address any potential areas of improvement, such as adapting to evolving industry demands (**Weaknesses**), capitalise on emerging opportunities in the cybersecurity landscape (**Opportunities**), and proactively mitigate risks to safeguard European industries from cyber threats (**Threats**). By aligning the programme with market needs, upskilling professionals, and strategically positioning D4S, the SWOT analysis serves as a vital tool for guiding our efforts in creating an impactful and sustainable European Master's Programme in Cybersecurity Management & Data Sovereignty

Key Strengths

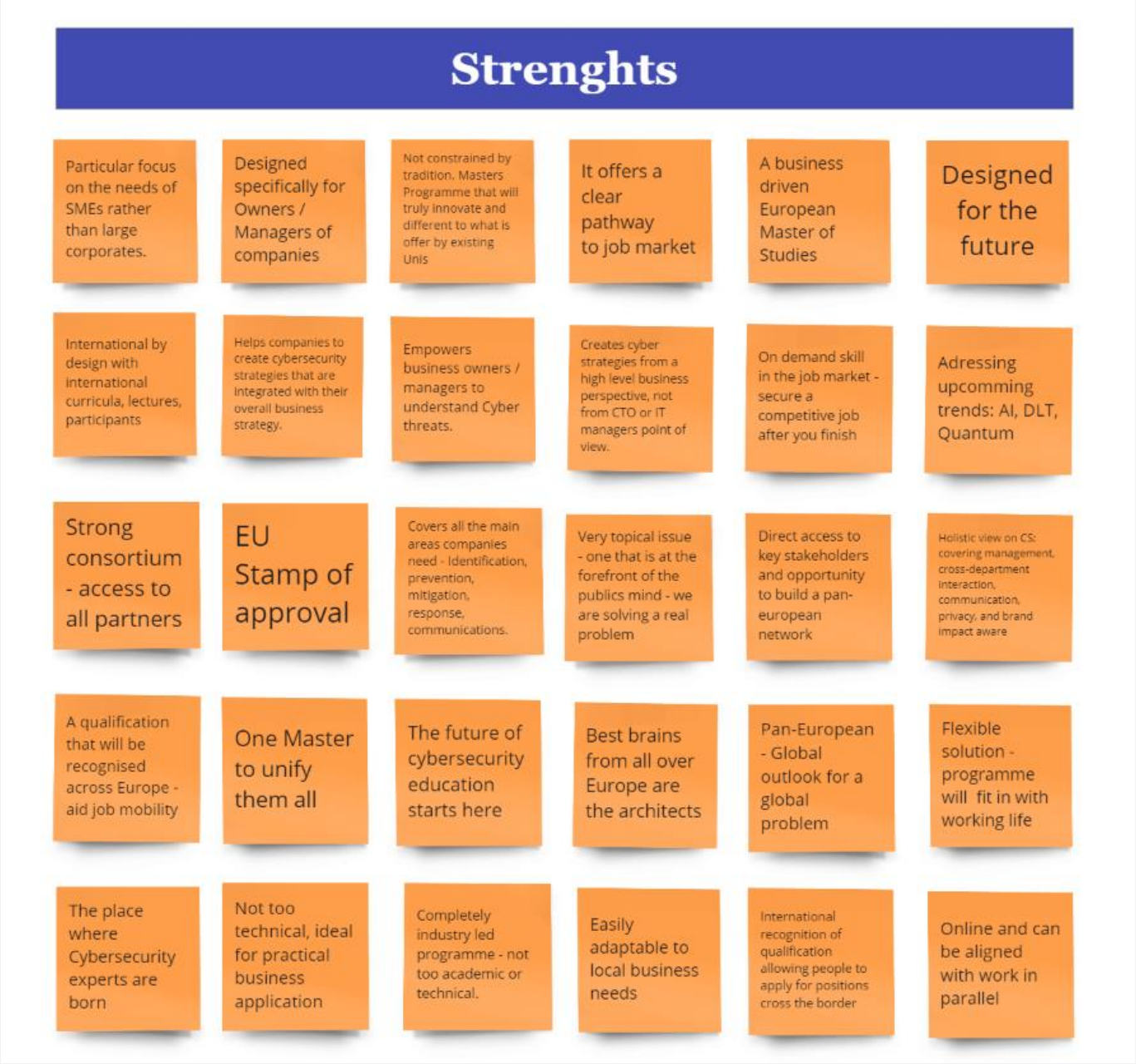


Figure 1: D4S SWOT analysis – Strengths

Weaknesses and mitigation measures

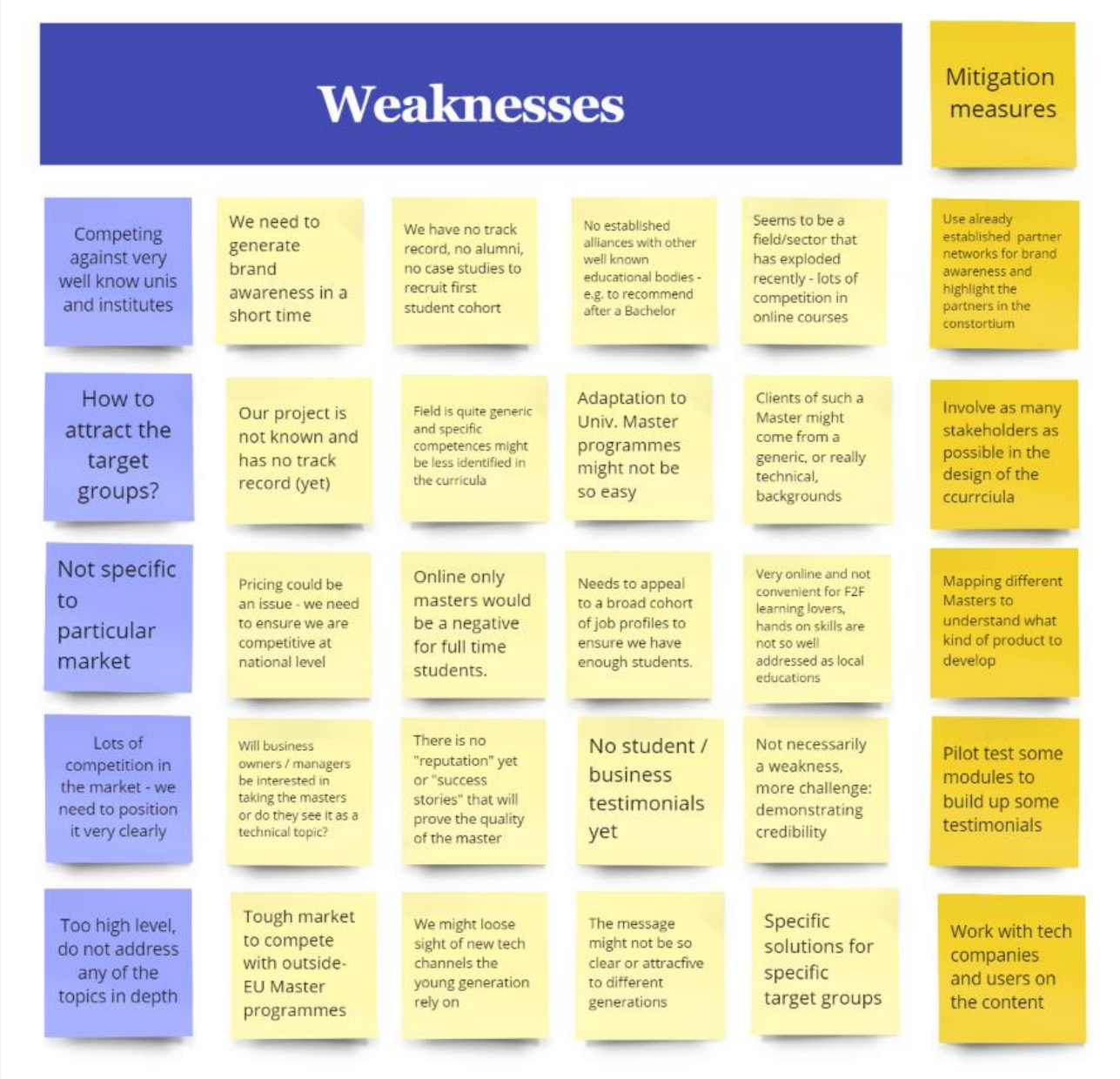


Figure 2: D4S SWOT analysis – Weaknesses

Opportunities and exploitation

Figure 3: D4S SWOT analysis – Opportunities

Threats and mitigation

Figure 4: D4S SWOT analysis – Threats and Mitigation

Target users and stakeholders

Digital4Security gathers different groups of stakeholders dealing with cybersecurity management skills from the education and industry in multiple sectors. Given the various types of stakeholders, their inherent needs and aspirations, it is relevant to identify, segment and focus on our key target audiences, as presented below.

Target audience

The main target audience of the Digital4Security programme are potential students from European companies with a specific focus on businesses involved in smart technologies and systems and/or who manage Information of very high value to cyber criminals. More details about the types of companies are provided in figure below.

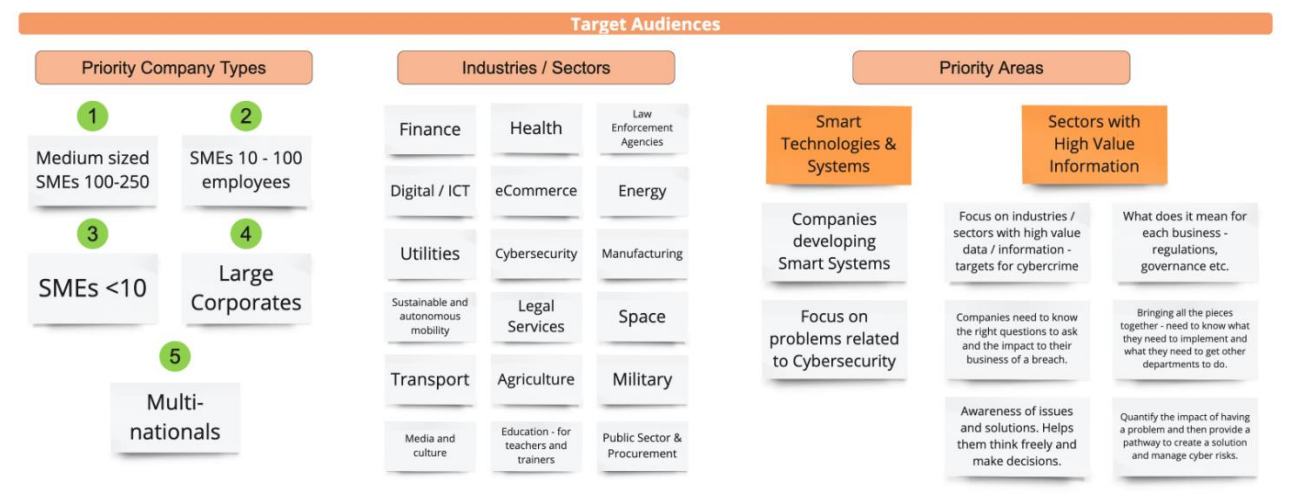


Figure 5: D4S target audience

The primary target audiences can be categorised as follows and presented in the figure below:

Potential learners	
Companies and SMEs wishing to reskill their staff to fill specific roles	SMEs who need cybersecurity management skills in their leadership team
	Larger companies who need to upskill staff or hire a cybersecurity manager
	Employees and managers in companies who wish to reskill or upskill into cybersecurity management
	ICT professionals who wish to specialise in cybersecurity management
ICT students	Students or recent graduates of degree programmes
ICT professionals	Professionals and managers wishing to specialise in cybersecurity management

	Lawyers and regulators
	Security practitioners
Non-ICT students	Students or recent graduates of degree programmes
Non-ICT professionals	Professionals and managers wishing to switch careers into cybersecurity management

Table 4: D4S primary target audience

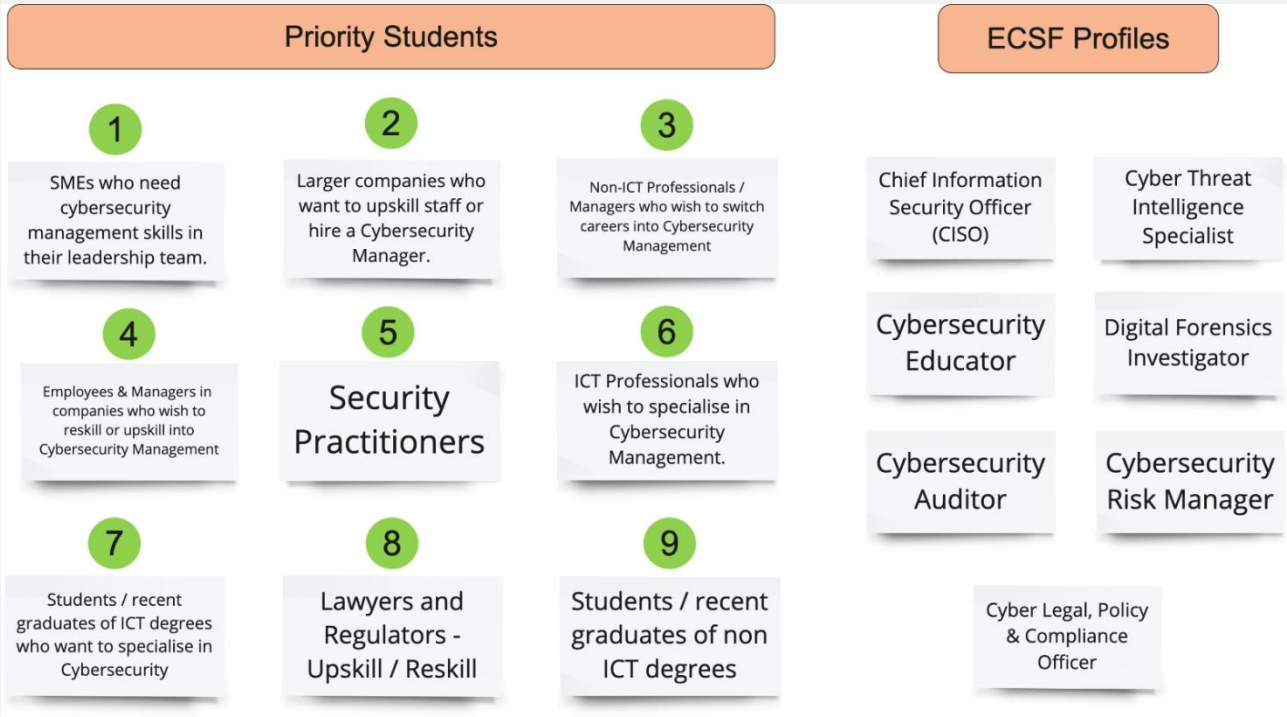


Figure 6: D4S primary target audience

In addition to the primary target audience, we also have a number of secondary target audiences for communications:

- European and international industry experts, lecturers and mentors who can contribute to the delivery of the programme.
- Higher education institutions who wish to learn from or adopt the Master's Programme themselves.
- Policy makers and key stakeholders in cybersecurity skills, education, and employment arena.

Customer personas

For each of the primary target audiences we have developed a customer persona to define their specific needs from Digital4Security and shape the activities and messages in our communications campaigns.

Mid-size company		
Personal information Latvian (40), business development manager of a mid-size company **Persona profile** Ambitious, very active, open minded, international mindset, studied at Oxford.	**What cybersecurity problems do they need to solve?** • regulatory issues, legal requirements • GDPR • worried about security, risk, disasters • brand reputation issues • wider team awareness and motivation • credibility holding international growth plans back • protect company from attack that could damage intellectual power **What solutions can D4S provide to address these problems?** • training for regulations • helping to create incident process • practical use case approach and deconstruction	**Why will they sign up for the master's / get involved? What are the benefits?** • Knowledge • Credibility • Status **How will they find out about D4S? (social, search, friends, events etc.)** • Networking events • Online marketing • Contrarian marketing voice **How and when will they want to learn? What fits their lifestyle?** • International • Hybrid • geographically diverse, visiting other countries • being part of a team • creating a new network

Table 5: D4S customer persona for Mid-size company

SME		
Personal Information Woman (50s), leader of a European SME	**What cybersecurity problems do they need to solve?** • Lack of knowledge • underestimated problem • no cybersecurity policy • limited budget, time and resources to invest in cybersecurity	**Why will they sign up for the master's / get involved? What are the benefits?** • Upskilling • timewise • incentive • future proofing • investing in future of the SME **How will they find out about D4S? (social, search, friends, events etc.)** • Social networks

	What solutions can D4S provide to address these problems? • training for regulations • Bite-sized expert knowledge and support • change in mindset • up-to-date and relevant material • Guidance	• Consortium Partners • Online dissemination by Partners • Flyers • Business associations **How and when will they want to learn? What fits their lifestyle?** • On demand • Online • Part-time • flexibility

Table 6: D4S customer persona for SME

NON-ICT student		
Personal information Student (30) **Persona Profile** Interested in cybersecurity, wants to specialise / upskill in the field.	**What cybersecurity problems do they need to solve?** • Understand external threats • protection of data • lack of awareness **What solutions can D4S provide to address these problems?** • education • Security management • Guidance, counselling, advisoring	**Why will they sign up for the master's / get involved? What are the benefits?** • Switch jobs / career chances • Competitiveness • Better source of information • Better salary prospect **How will they find out about D4S? (social, search, friends, events)** • Referral • Blog • University events • Job fairs • Podcast **How and when will they want to learn? What fits their lifestyle?** • Spare time • Using work hours with some sort of funding support • During paid leave phases

Table 7: D4S customer persona for Non-ICT Student

Security practitioner		
Personal Information Young professional, (35) **Persona profile** Collaborating remotely with banks, industry and IT public organisations in the EU and outside Europe.	**What cybersecurity problems do they need to solve?** • Prevent data and security breaches • Raising awareness • Actioning cybersecurity steps • Needs to certify the organisations **What solutions can D4S provide to address these problems?** • Education on how to Implement best practice • Sharing good practice examples • Capacity building	**Why will they sign up for the master's / get involved? What are the benefits?** • Needs a qualification for promotion / job • European perspective on problems and solutions • Keeping up with changes in world of work • Networking with others • Can work remotely (digital nomads) **How will they find out about D4S? (social, search, friends, events etc.)** • Social • Peer-to-peer **How and when will they want to learn? What fits their lifestyle?** • Part-time • Blended

Table 8: D4S customer persona for security practitioner

NON-ICT professional		
Personal Information Mid-senior manager (50) in a digital agency **Persona Profile** **3rd level qualification in law**	**What cybersecurity problems do they need to solve?** • protect personal info (e.g. patient records) • act swiftly & confidently in case of cyberattack • need of a cybersecurity plan **What solutions can D4S provide to address these problems?** • provide most up-to-date & in depth training • tools & skills	**Why will they sign up for the master's / get involved? What are the benefits?** • provide network of professionals to collaborate • flexibility of course - alongside work • pan-European course from European universities • Global perspective • climbing career ladder & make more money - futureproof career

	• official recognised certification • provide network of professionals to collaborate • insights to real scenarios from professionals	**How will they find out about D4S? (Social, Search, Friends, Events etc.)** • industry-leaders & co-workers • through other institutions • digital exhibitions & events • european/private platforms for university courses • Google search **How and when will they want to learn? What fits their lifestyle?** • live & recorded lecturer • fit alongside work schedule • immediate benefit to implement • use ongoing work, solve real-life of company • reasonably priced - company & private can pay for it (invest in their workforce)

Table 9: D4S customer persona for Non-ICT Professional

Stakeholder groups

The above key target audiences can be grouped into 3 categories, as follows:

- **Students:** individuals at the early stages of their academic journey seeking foundational knowledge and skills in cybersecurity management. Digital4Security aims to equip them with practical insights, hands-on experience, and a comprehensive understanding of cybersecurity practices. The goal is to empower students to become the next generation of cybersecurity professionals, fostering innovation and ensuring a robust talent pipeline for the industry.

- **Professionals:** This group includes individuals already employed in the workforce with varying levels of experience in cybersecurity or other fields (non-ICT). Professionals may range from mid-level managers to high-ranking executives. The project seeks to enhance and complete their existing skills, update them on the latest industry trends, and provide advanced training in cybersecurity management. Professionals can effectively address evolving cyber threats, implement best practices, and contribute to the overall cybersecurity resilience of their organisations.

- **Companies, especially SMEs**. SMEs often face unique challenges in implementing robust cybersecurity measures due to resource constraints and limited expertise. The project aims to offer tailored solutions, guidance, and training to help companies, particularly SMEs, strengthen their cybersecurity posture. It emphasises practical, cost-effective approaches that align with the specific needs and constraints of smaller businesses. By providing tools and knowledge, the project aims to empower companies to protect their assets, customer data, and overall business continuity in the face of cyber threats. Additionally, the project encourages collaboration and information sharing among companies to collectively enhance the cybersecurity resilience of the entire business ecosystem.

Brand strategy

Digital4Security will be supported by a strong brand to ensure our main target groups fully understand the project objectives, its aims, and benefits, and encourage the uptake and further dissemination of the project results.

The Digital4Security brand is reflected in the visual identity and all communications materials. To build a strong and relevant brand identity, all Digital4Security Partners contributed to a collaborative workshop during the Kick-Off Meeting in October 2023. Through interactive exercises, we collectively defined the key strengths, brand values, value propositions, aspirations, and brand positioning for Digital4Security.

Brand positioning

In the highly competitive field of cybersecurity education and training, the Digital4Security Master's programme distinguishes itself by being a dynamic pan-European Consortium, uniting various stakeholders ranging from educational institutions to industry leaders and cybersecurity clusters. This collaborative approach positions Digital4Security as an innovative force in cybersecurity management and data sovereignty education. With a focus on equipping European SMEs and companies across diverse sectors with the essential skills to combat cybersecurity threats,
The Digital4Security Master's Programme emerges as a proactive and transformative solution to safeguarding European industries from potential cyber-attacks. Through a comprehensive communication strategy that leverages the collective strengths and networks of its Partners,

Digital4Security strives to establish itself as the foremost choice for business leaders and managers in SMEs seeking top-tier cybersecurity education and guidance.

Brand name and identity

The Brand Name and Identity section of the Communications Strategy for the Digital4Security project serves as a comprehensive guideline document intended for both internal and external stakeholders engaging with the Digital4Security brand. Within this section, users will find essential information on the core elements of the Digital4Security identity. The primary goal of this guide is to ensure the uniform and consistent application of the brand, thereby enhancing its overall quality and impact.

Digital4Security Brand Guidelines V2.pdf - This guide addresses various aspects of the Digital4Security brand identity, including logos, colour schemes, typography, and their respective usage guidelines. By following these guidelines, stakeholders can maintain the brand's visual integrity and contribute to its ongoing recognition and success.
The Digital4Security Brand Guidelines offers guidance on the appropriate usage of Digital4Security logos across different visual environments, emphasising the importance of using the provided files without any distortion. Additionally, a carefully curated suite of colours is presented in Hex, RGB, and CMYK formats to cater to both digital and print applications.

Digital4Security brand name

“Digital4Security” is the name of the project. The general rule is to use the name in full, whenever possible.
Find below how to use the acronym “D4S” (always in uppercase letters):

- Use the “D4S” acronym, in lengthy written publications. It is to be noted that the acronym should always be introduced in the following manner at the beginning: “Digital4Security (D4S)”.
- Use the “D4S” acronym, when referring to a specific output of the project or product, such as the D4S Strategy, the D4S modules, D4S newsletter — and so on.
- Use the “D4S” acronym, whenever space doesn’t allow you to write the full name of the project.

In an ever-evolving digital landscape, maintaining a strong and consistent brand presence is critical. This section equips users with the knowledge and tools needed to achieve this objective. Together, stakeholders can elevate the Digital4Security brand and solidify its position as a trusted and recognised name in the digital security industry.

Digital4Security visual identity

Figure 7: D4S logo

Figure 8: D4S logo variations (the reverse options)

Figure 9: D4S logo variations, the symbol on its own

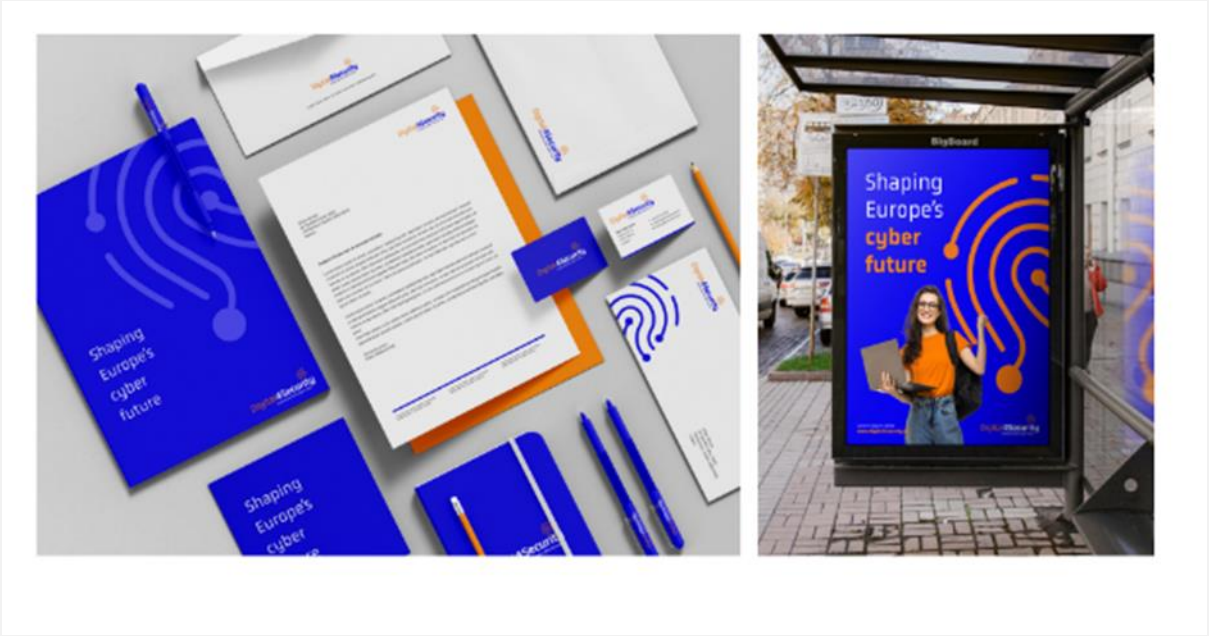


Figure 10: Using the symbol as a graphic element

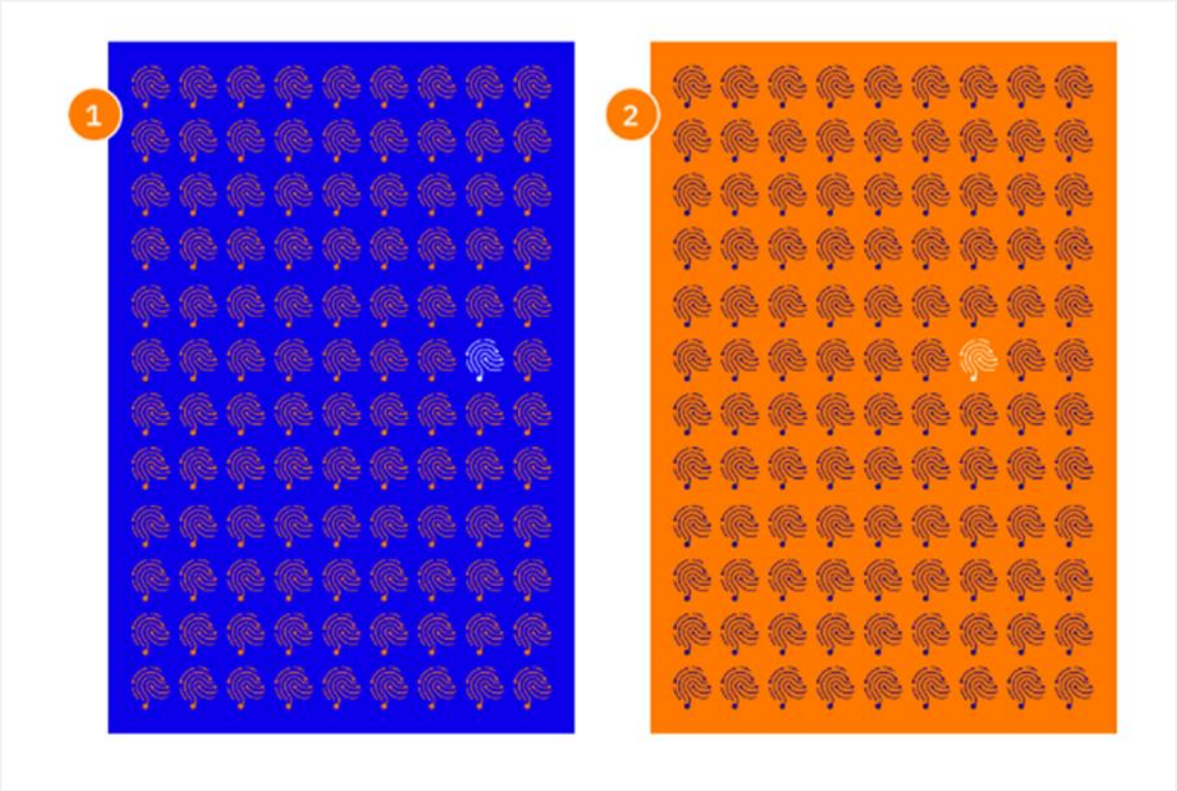


Figure 11: D4S logo variations: The repeat pattern

Digital4Security colour palette

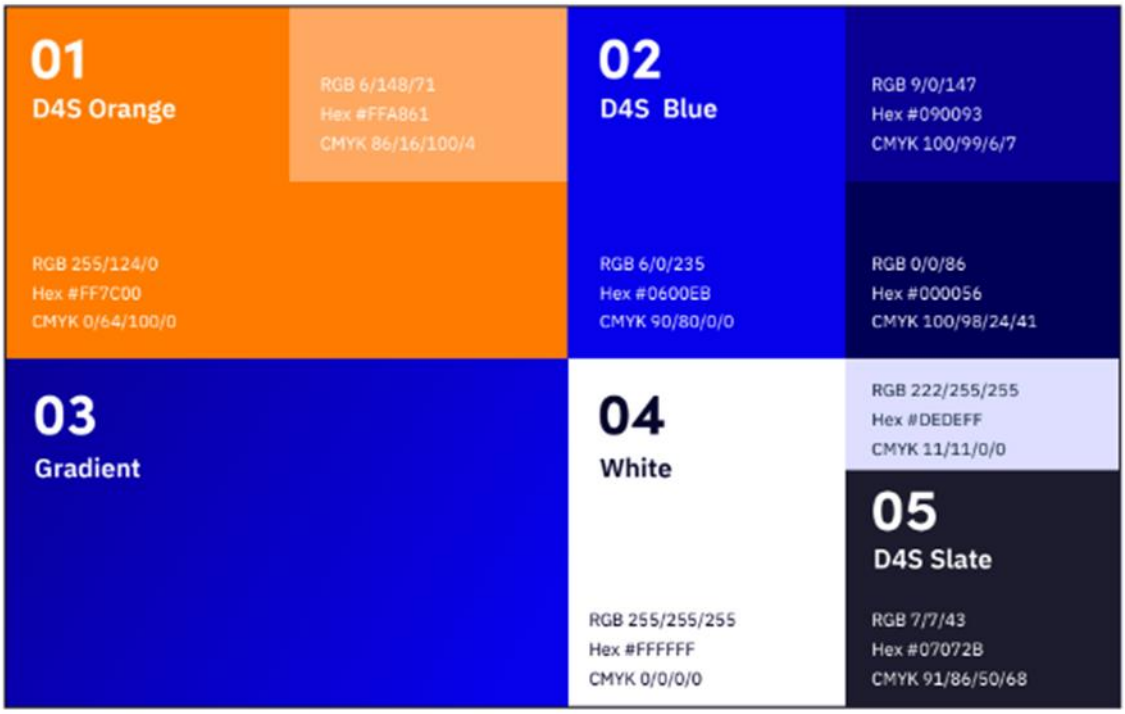


Figure 12: D4S primary colours

EU funding statement

All communication activities for Digital4Security (including media relations, conferences, seminars, information material, such as brochures, leaflets, posters, presentations, etc, in electronic form, via traditional or social media, etc), will acknowledge EU support and display the European flag (emblem) and funding statement (translated into local languages, where appropriate). The emblem will remain distinct and separate and will not be modified by adding other visual marks, brands or text. When displayed in association with other logos (e.g., of beneficiaries or sponsors), the emblem will be displayed at least as prominently and visibly as the other logos.

Figure 13: EU flag emblem and funding statement

Package of communication material

Several visual assets will be produced by the WP5 leaders to serve the communication and outreach activities throughout the project lifetime. The visual assets will be produced in English. Partners can themselves choose to localise these assets.

Figure 14: Sample visual asset for Instagram

Figure 15: Sample visual asset for LinkedIn

Figure 16: Sample visual asset for X/Twitter

The table below presents the initial assets that will be provided to the Partnership:

Asset	Use for/on
Email marketing template	Email marketing, direct emailing
Online banners	Digital4Security EU-wide and mini-campaigns, social media posts, email marketing
Flyer/brochure	Online/on-site events, project website
Infographics and branded graphics	Websites, social media posts, email marketing
Roll-up banner	Physical events
Official PPT presentation	Online/on-site events, direct emailing
Partnership logos image	Online/on-site events, social media posts
Visual identity manual & communication toolkit	Localisation and creation of own content

Table 10: Visual assets

Communication and promotional strategy

RACE strategy

The promotional strategy presents the tactics that will be deployed over the lifetime of the project to Reach, Act towards, Convert, and Engage (RACE) each of the target groups; thus, creating widespread awareness and interest in the project.
Furthermore, the tactics presented below inform the definition of the various promotional campaigns that will be implemented to disseminate the project results and activities and serve the short and long-term communication and outreach objectives.

Stage	Tactic	Key measure
Reach **Build brand awareness, increase online visibility, grow the audience**	• Officially launch the website and social media channels • User-friendly design and easy navigation on the website	• Audience volume • Audience quality

on multiple channels.	• Organise stakeholder meetings and events • Direct emailing and messages via the Partners' network • Create and deploy awareness-raising campaigns and content • Organic social media campaigns • Search engine optimisation (SEO) for the website • Promote external thematic content and events • Attend/participate in external events to present Digital4Security • Prepare launch news pack for the project Partners • Promotion via the Digital Skills & Jobs Platform	
Act Prompt interactions, subscribers and leads, increase the positive sentiment vis-à-vis the project and outputs.	• Promotion of the project newsletter • Create evergreen and thematic content for the project communication channels • Direct emailing and messages via the Partners' network • Develop engaging and interactive visual content • Launch the Digital4Security community on LinkedIn. • Attend/participate in external events to present Digital4Security • Prepare launch news pack for the project Partners • Promote project outputs and results on the website • Organic social media campaigns on need for digital skills • Create and deploy campaigns and content on specific project outputs for different stakeholders	• Time on site • Subscribers, likes and shares • Community sign-ups • Downloads of outputs • Event registrations
Convert Drive registrations for the Master's Programme and	• Develop targeted campaigns to recruit students for each intake of the Master's Programme.	• Conversion • Registrations • LinkedIn followers

short courses, persuade key stakeholders to use the project results, increase brand trust.		• Create and deploy campaigns on the benefits of the project outputs for each stakeholder • Promote positive experiences from each student cohort. • Collect and publish case studies, success stories, impact research results • Organic social media campaigns • Organise stakeholder meetings • Encourage website visitors to register their interest for future training courses. • Encourage companies, SMEs, HEIs etc to become a partner of D4S. • Direct emailing towards key policymakers • Use strong calls-to-action on the website • Organise engaging events / webinars / conferences for key stakeholders • Attract members to join a Community Group on DSJP. • Feed the community with thematic content.	• Event registrations
Engage Encourage the multiplying effect, reward users, activate the community		• Organise specialist webinars and events to promote the results in collaboration with DSJP or other Partners. • Highlight students' experience via social media video campaigns • Provide potential multipliers with a news/comms pack. • Collect and publish adopters' stories, use cases, success stories. • Active moderation on the LinkedIn Community and social media. • Active development of the Community Group on DSJP and promotion of success stories / good practices.	• Repeat interactions • Brand satisfaction and loyalty • Advocacy

	• Launch and animate online discussions on topics of interest on DSJP. • Recycle engaging content and feed it to potential new students / Partners. • Direct emailing and messages via multipliers and Partners' network. • Student support programme for new students. • Encourage the use of the D4S online learning platform tools and features and provide user support.

Table 11: RACE strategy

RACE by target audience

The RACE approach will be tailored for each of the primary target audiences to ensure we create targeted campaigns using the right channels and communicating very specific messaging as defined in the customer personas above. The RACE strategy for each target audience is outlined in the figures below:

Figure 17: RACE by target audience - mid-size company

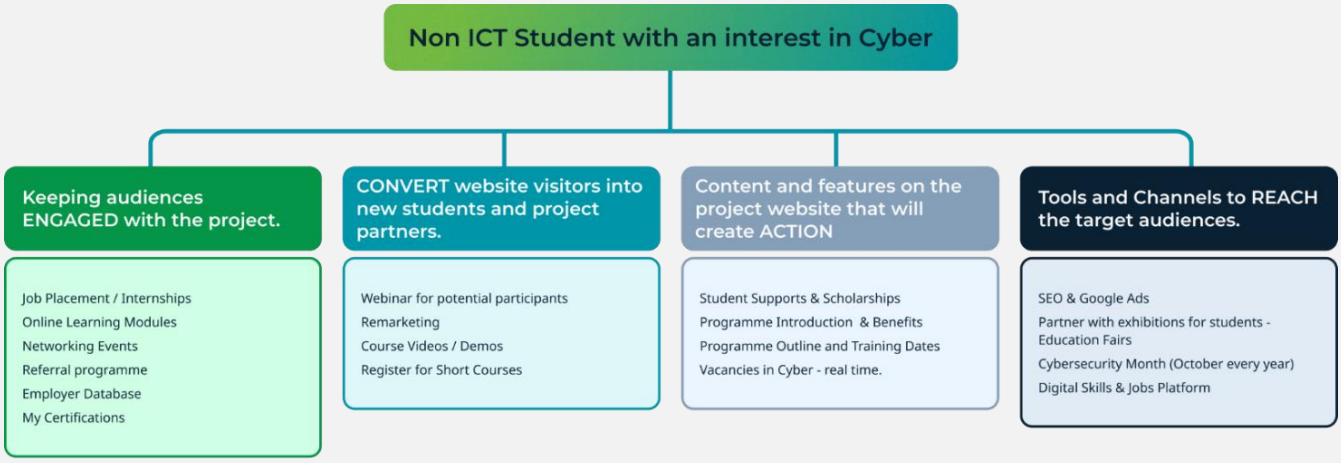


Figure 18: RACE by target audience – non-ICT students

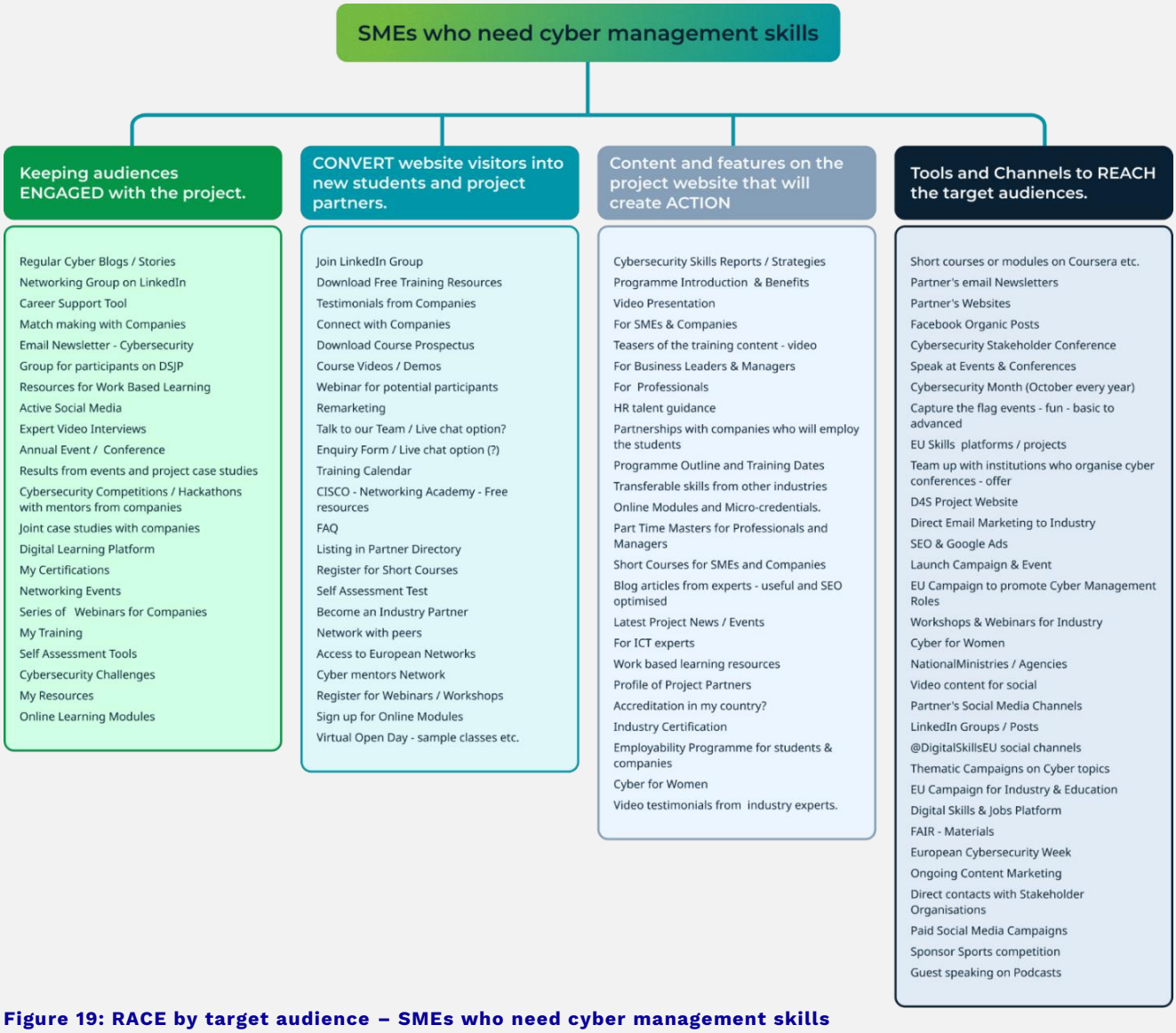


Figure 19: RACE by target audience – SMEs who need cyber management skills

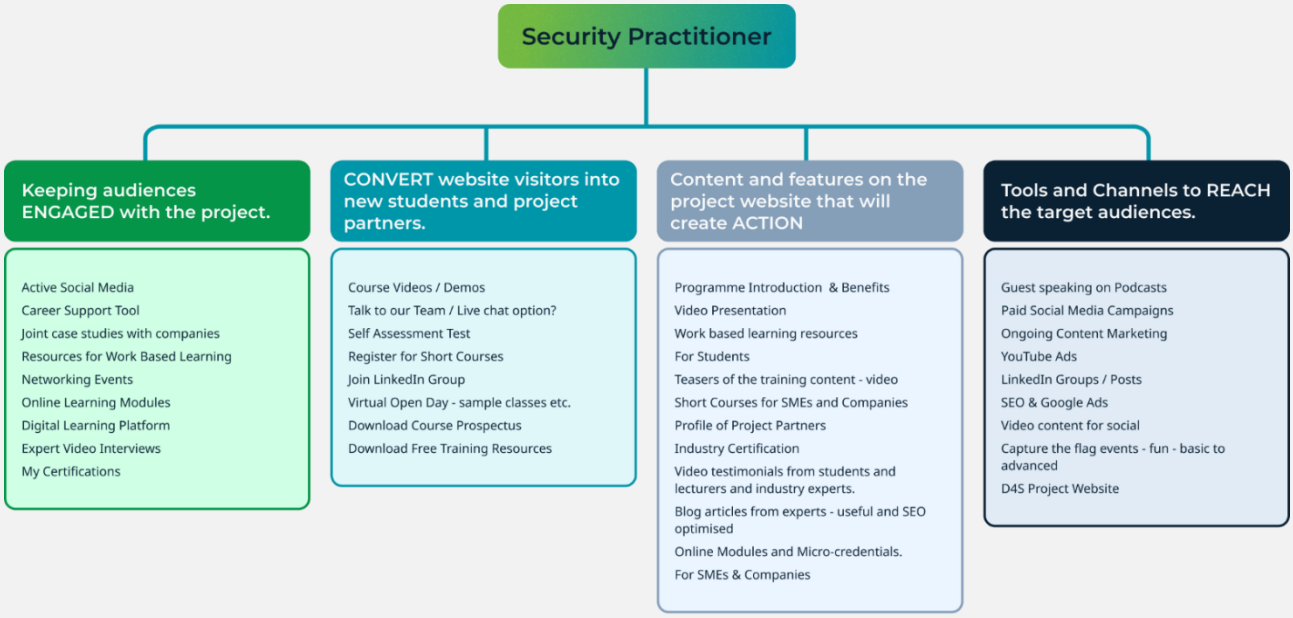


Figure 20: RACE by target audience – Security practitioner

Communication campaigns (T5.3 and T5.7)

Throughout the project duration, Digital4Security will implement several promotional campaigns to reach the communication objectives. These are implemented in two phases:

Digital4Security Launch Campaign (T5.3) (April 2024 M7 – September 2027 M48)

The DIGITAL4Security Launch Campaign involves the development and execution of a comprehensive communications campaign on a European Union scale to promote the launch of the D4S programme. The primary objective of this campaign is to provide a detailed presentation of the programme using creative content and to ensure a robust enrolment of students, with a specific emphasis on gender equality.

To achieve these goals, a multifaceted approach will be employed. This includes:

1. **Communication material development**, with detailed information about the D4S programme, its benefits and unique selling points. The visually appealing and informative content will be used across various platforms and will incorporate infographics, videos, and engaging text.

2. **A step-by-step approach for HEIs and training providers**, with clear instructions and guidelines for them to follow, to maximise the impact of their D4S landing pages.

3. **Supplementary materials to support the campaign**, such as brochures, posters, and digital banners, to be shared both online and offline. These materials will be tailored to resonate with the target audience and emphasise gender equality.

4. **A minimum of four on-site or virtual info days and webinars** to provide in-depth insights into the D4S programme organised in collaboration with HEIs.

5. **SMEs and industry players outreach**, with tailored communication activities that encourage their involvement in the D4S programme.

6. **Tracking mechanisms to continuously monitor and evaluate the effectiveness of the campaign**, including website analytics, social media engagement metrics, enrolment statistics, and feedback from participating institutions, students, and industry partners.

7. **Cyclical campaign planning** for repeating the launch campaign for each new cycle of the D4S programme, ensuring continuous promotion and sustained growth. We will incorporate lessons learned from previous campaigns to refine strategies and improve outcomes.

The above action plan provides a detailed roadmap for executing task 5.3 "D4S Launch Campaign & Student Recruitment", covering various aspects of communication, engagement, and outreach to maximize its impact.

Industry and Education Campaign (T5.7) (October 2025 M25 – September 2027 M48)

The Industry and Education Campaign is a comprehensive EU-wide communications initiative designed to promote the results and outputs of the Digital4Security programme, with a primary focus on fostering the extensive adoption of the online Master's format. To achieve this objective, a strategic advocacy plan, developed in collaboration with partner contributors, will establish connections between the D4S programme and the latest policy developments in digital skills education, including the Cyber Skills Academy and other related initiatives.
The campaign will be also based on the collaboration with HaDEA/DG CNECT and industry and education partners to ensure alignment with existing initiatives and leveraging synergies for maximum impact.

The operational elements of the campaign are the following:

- **A minimum of eight events or webinars** in collaboration with Partners to showcase key outputs and results of the D4S programme. The content will include case studies collected in T5.6 that highlight success stories and practical applications of the programme. For these events, countries with lower level of advanced digital skills/cybersecurity skills (DESI 2022) will be prioritised.
- **Preparation of engaging and informative content** for events and webinars: presentations, demos, and interactive sessions.
- **Empower industry and education stakeholders** by providing them with tools, resources, and knowledge to effectively utilise the results of the D4S programme.
- **Case studies and results dissemination** through various channels, including the campaign website, social media, and partner networks.

Digital Skills and Jobs Platform – collaboration and online learning resources

The Digital Skills and Jobs Platform (DSJP) is an initiative by the European Commission aimed at addressing the digital skills gap and fostering digital literacy across Europe. It serves as a central hub for various resources, tools, and initiatives related to digital skills development and job opportunities in the digital sector. The platform provides access to a wide variety of high-quality information, online courses, training programmes, funding opportunities and events, allowing individuals and organisations to enhance their digital skills and stay informed about the latest trends and opportunities in the digital field. It also offers a community space for networking and collaboration both on European and national level. Additionally, the platform facilitates collaboration among stakeholders, including policymakers, educators, industry experts, and learners, to promote the advancement of digital skills and employment across the European Union.

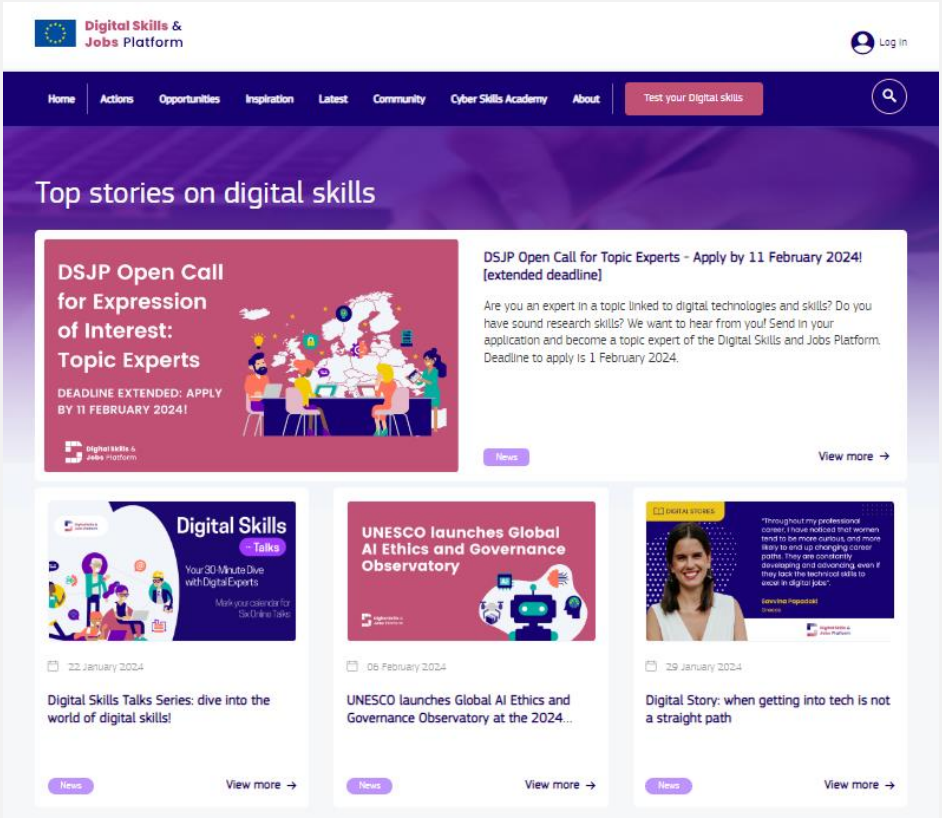


Figure 21: DSJP homepage

The Digital4Security Consortium will liaise closely with the DSJP team to develop content and publish the Digital4Security results, including online learning resources on the platform, contribute to communications campaigns, participate in webinars, and support community building. More collaboration avenues at the EU and national level will be investigated, such as, but not limited to, the Digital Skills and Jobs National Coalitions and European Digital Innovation Hubs.

To start our collaboration with the DSJP, we will:

- Join the drop-in session of the DSJP on DEP-funded master's and short-term courses to gather main information on the Platform and coordinate with the team.
- Send a first timeline of the D4S project and the main information related to the Master's programme.

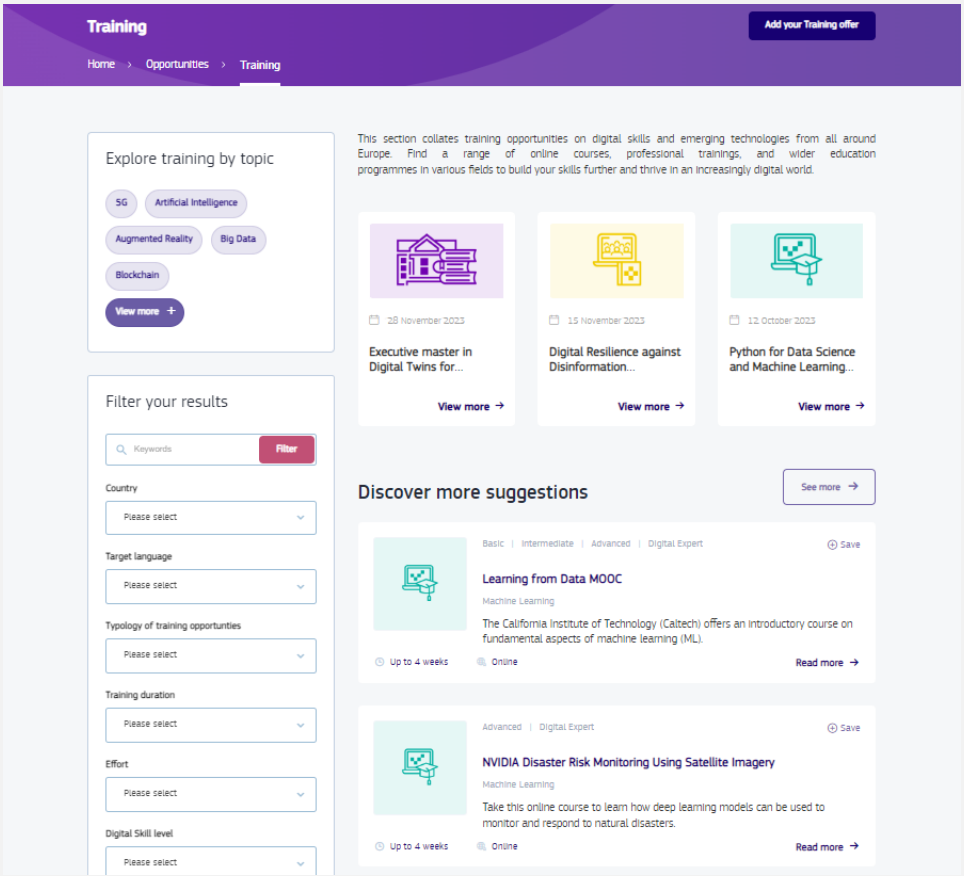


Figure 22: DSJP – Training opportunities section

Our collaboration with the DSJP will include the following:

Editorial content

- **Training offers, events, news, digital skills resources**: We will contribute by submitting content related to the D4 under these sections, one item in the calendar per week.
- **Landing page**: set up a landing page for the project where we can include the main information about the initiative and some visual cards that link to related resources (training, events, news, etc.) that also need to be published on the platform.
- We could include some of our resources on cybersecurity in the **Learning Paths** of the Platform.
- **Opinion posts**: experts of the Consortium can write an opinion piece on cybersecurity which can promote the Master's programme.

Community and communication

- **DSJP community and engagement**: we can interact with community members and start a public conversation (discussion thread) to highlight any activities or special events.
- **Participate in joint campaigns** with the DSJP which includes sending comms kit to the Platform.
- **Communications and networking:** We can coordinate with the DSJP team to share info and updates on D4S project, courses, events and activities, directly on the @DigitalSkillsEU channels (Facebook and X). We can also share some highlights of the projects and activities on the Digital Skills and Jobs Digest, which is out twice a month.

- **National Coalitions monthly meeting**: we will consider the possibility to participate in the National Coalitions monthly meetings, organised once a month, where we can present the project and the Master's to the Digital Skills & Jobs National Coalitions.

Content marketing

We will develop a content marketing strategy to continuously feed the target groups with relevant outputs and content of interest, including a calendar of website, social media and email updates.

Key topics and activities

We will use the RACE approach to launch D4S, recruit new students and Partners, and keep both students and companies engaged with the project over the long term. Figure 23 below outlines the various activities, channels and content that will be utilised within each RACE stage:

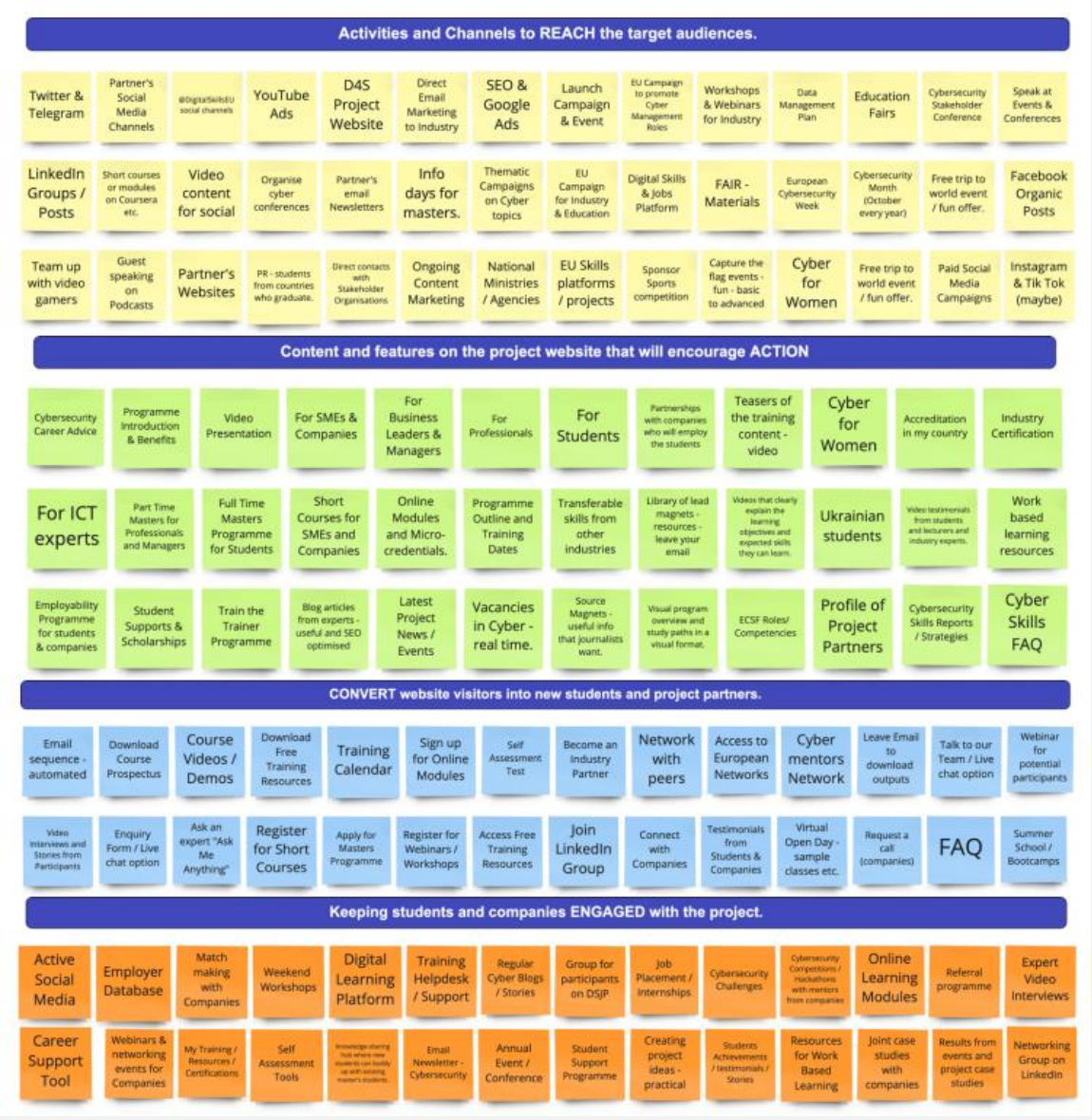


Figure 23: D4S RACE strategy activities

Content calendar (M1 – M6)

The table below presents the content types and their estimated publication frequency on the D4S's core communication channels:

Content type	Publication frequency
LinkedIn posts	Min. 60 per year
Newsletter	Min. 4 per year
Direct mailing	Min. 6 per year
News and events	Min. 2 per month

Table 12: D4S content type and publication frequency

The WP5 Team uses our regular biweekly meetings to align key messages as well as discuss and planning content development. During such meetings, we prepare the monthly communication calendar to include proposed content and publication frequency, which will be shared with the WP leaders of the Consortium.

In particular, our internal coordination for task T5.2, Setup and management of Digital Marketing Channels, Tools and Websites, will be as follows:

1. Matrix will set up and manage D4S digital marketing channels/tools such as project website, social media accounts, newsletter.
2. Matrix will support Partners to set up a D4S landing page on their websites (local language) with the project domain name/sub-domain.
3. Matrix will coordinate with DE to produce monthly editorial calendars and visual assets.
4. Indiepics will coordinate with Matrix and DE on the production of video or animated GIFs for digital marketing campaigns.
5. Further development iterations of the project website by Matrix will link to the Digital Learning Platform (D3.1) and a central online course registration system.

The Communication Strategy will be further developed into a shared online Editorial Calendar allowing all parties to see the monthly communications activities, content and campaigns for D4S. This Editorial Calendar will be reviewed and updated during regular project meetings to coordinate activities.

Communication channels and tools

Communication channels and tools

The primary communication channels and activities will include:

- Email and meetings for direct outreach with Partners.
- Newsletters and notification emails to the subscribers and mailing list contacts.
- News and events published on the D4S website.
- D4S and the Consortium Partners' social media channels (LinkedIn, Twitter, Facebook and Instagram).

All social media activities will hinge on close collaboration of the project's communication team with the Active Partners' communication teams in order to:

- Implement campaigns through the D4S and Partners' social media channels.
- Engage spontaneously with users and potential participants to recruit for the master's.
- Obtain engagement figures for reporting purposes.

Communication and promotional activities for D4S will be executed using both online and offline channels and tools. Online communication focuses on highlighting the project's core content and promotion around the website to communicate the main information and latest news on the Master's. Offline communication focuses on promoting the Master's at events organised by the European Commission and other EU bodies, Partners, and stakeholders in the field of cybersecurity.

Tool/Channel	Characteristics	Results	Impact
D4S website and Partners' websites	• Official • Informative	• Increase of page views. • Increase number of visitors.	• Increase awareness about the Master's and its programme • Increase enrolment
D4S and Partners social media	• Informal • Interactive • Engaging	• Increase number of contacts	• Increase visibility of core sections

		•	of the website
Email marketing	• Official • Informative	• Increase number of people reaching out for information	• Expanding reach of the Master's
Events (online and offline)	• Official • Informative • Promotional • Appealing	• Increase number of registrations to the Master's	• Expanding reach of the Master's
Promotional material for events (graphics, visuals)	• Official • Informative • Promotional • Visual • Appealing	• Increase number of registrations to the Master's	• Increase visibility of the Master's programme at face-to-face events • Increase engagement with promotional acitivites on social media

Table 13: D4S communication channels and tools

Website

The Digital4Security website is available at www.Digital4Security.eu. The website has two main purposes:

- Informative: it informs stakeholders about the project — through a narrative-based user experience — make all public project results available.
- Collaborative: it will host/link to the Digital4Security LMS.

The website uses a WordPress CMS to allow content updates and collaboration across the Consortium Partners.
The website will be developed in two phases:

1. **Light version:** static website with basic pages, a contact form and blog posts. (launch).
2. **Full version:** integration of the resource section (due date: dependant on completion of course content).

The website's blog, a.k.a. News & Events section, is the central location for the latest updates on the project and related topics — positioning Digital4Security as the leader and expert in its field. It will include:

- Informative articles on the project's milestones, outputs progress/release, and activities.

- News on related European projects and initiatives.
- Announcement of all Digital4Security events.
- Evergreen content and hot topics content on cybersecurity related topics.

Social media

Digital4Security will communicate on partner channels initially, until the Master's programme is at recruitment stage.
Digital4Security will launch a LinkedIn, Facebook or Instagram account, if required when recruiting for the first cohort of students commences. Prior to the launch of the official channels, social media presence on Facebook and Instagram will be ensured via the Partners' social media channels (see annex 1) and active multipliers — respectively to reach out to education and training professionals and potential learners, more specifically students.

Social media engagement strategy
Resources will be allocated to specific actions to create an active community of followers on the Digital4Security social media accounts:

- Regular flow of publications and interactions with the Digital4Security ecosystem
- Promotion of Digital4Security accounts via the project email newsletter
- Promotion of Digital4Security accounts via Partners' social media channels and email newsletters
- Promotion towards targeted audiences with the use of sponsored content
- Use of relevant hashtags

Studies show that social media communications including hashtags are more likely to draw engagement. Thus, Digital4Security channels will leverage existing popular hashtags:

#Cybersecurity #Master'sDegree #InfoSec #CyberAware #DigitalSecurity
#TechEducation #CyberDefense #DataProtection #OnlineSafety
#ITSecurity #PrivacyProtection #SecureYourFuture #CyberThreats
#NetworkSecurity #CyberSkills #TechCareer #SecureData #InformationSecurity
#CyberRisk #CyberAwareness

In parallel, Partners will use a common hashtag #Digital4Security to improve brand awareness and facilitate the tracking and impact assessment of Digital4Security communications.

WP5 leaders manage the Digital4Security social media accounts to ensure a regular flow of information and editorial consistency. Partners are encouraged to submit interesting and related content directly to Irene Marinelli (irene.marinelli@digitaleurope.org) or Aoife O'Driscoll, (aoife@matrixinternet.ie) such as:
· Partners' own content related to the topics of the project
· Third-party content that Partners find suitable and interesting for Digital4Security target audiences (e.g., evergreen content, hot topics content).

Partner	LinkedIn	Twitter	Facebook	Instagram
University POLITEHNICA of Bucharest (UPB)		https://twitter.com/upb1818	https://www.facebook.com/UPB1818	https://www.instagram.com/upb1818/
National College of Ireland (NCI)	https://ie.linkedin.com/school/n	https://twitter.com/NCIRL	https://www.facebook.com/NCIRL	https://www.instagram.com/ncirl

	ational-college-of-ireland/			
University of Digital Science GGMBH (UDS)	https://www.linkedin.com/company/uds-university/			https://www.instagram.com/uds_university/?hl=de
University of Rijeka (UNIRI)	https://www.linkedin.com/school/15093575/	https://twitter.com/UniRijeka	https://www.facebook.com/uniri.hr	https://www.instagram.com/university_of_rijeka
The Università degli Studi di Brescia (UNIBS)	https://www.linkedin.com/school/universita-degli-studi-di-brescia/	https://twitter.com/unibs_official	https://www.facebook.com/unibs.official	https://www.instagram.com/unibs.official/
Politecnico di Milano (Polimi)	https://it.linkedin.com/edu/politecnico-di-milano-13843	https://twitter.com/polimi	https://www.facebook.com/polimi	https://www.instagram.com/polimi
University of Koblenz		https://twitter.com/unikoblenzde	https://www.facebook.com/universitaet.koblenz	https://www.instagram.com/uni_koblenz/
CY CERGY PARIS UNIVERSITE	https://www.linkedin.com/school/cycergyparisuniversit%C3%A9/	https://twitter.com/UniversiteCergy	https://www.facebook.com/CYCergyParisUniversite/	https://www.instagram.com/cy_univ/
Mykolo Romerio Universitetas (MRU)	https://www.linkedin.com/school/mykolas-romeris-university/	https://twitter.com/mru_university	https://www.facebook.com/MykoloRomerioUniversitetas/	https://www.instagram.com/mru.universitetas/
Universidad Internacional de La Rioja SA (UNIR)	https://www.linkedin.com/school/unir-universidad-internet/	https://twitter.com/UNIRUniversidad	https://www.facebook.com/UNIRUniversidad	https://www.instagram.com/uniruniversidad/
Brno University of Technology (BRNO-BUT)	https://www.linkedin.com/school/vysok%C3%A9-u%C4%8Den%C3%AD-technick%C3%A9-v-brn%C4%9B	https://twitter.com/VUTvBrne	https://www.facebook.com/BrnoUniversityOfTechnology	http://instagram.com/vutvbrne
Munster Technological University/ Cyber Ireland (CI)	https://www.linkedin.com/school/munster-technological-university/ https://www.linkedin.com/com	https://www.twitter.com/MTU_ie https://twitter.com/CyberIreland	https://www.facebook.com/myMTU	https://www.instagram.com/MTU_ie

	pany/cyber-ireland/			
SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	https://www.linkedin.com/company/skillnetireland/	https://twitter.com/skillnetireland	https://www.facebook.com/SkillnetIreland/	
Adecco Formazione S.r.l.	https://www.linkedin.com/company/adecco/	https://x.com/AdeccoItalia?s=20	https://www.facebook.com/adeccoitalia/?fref=ts	https://www.instagram.com/adeccoitaly/
DTSL	https://www.linkedin.com/company/digital-technology-skills-limited/	https://twitter.com/DigiTechSkills		
ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA (TAG)	https://www.linkedin.com/company/theadeccogroup/	https://twitter.com/AdeccoGroupITA?lang=it	https://www.facebook.com/theadeccogroup/?fref=ts	https://www.instagram.com/theadeccogroupitaly/
Ataya & Partners	https://www.linkedin.com/company/ataya-and-partners/?viewAsMember=true			
IT@Cork Association Limited	https://www.linkedin.com/company/techindustryalliance/			
Matrix Internet	https://www.linkedin.com/company/matrix-internet-ireland	https://twitter.com/matrix_internet	https://www.facebook.com/matrixinternetireland	https://www.instagram.com/matrix_internet/
G & N SILENSEC LTD	https://www.linkedin.com/company/silensec-group/	https://twitter.com/silensec	https://www.facebook.com/SilensecGroup/	https://www.instagram.com/silensec_group/
Schuman Associates	https://www.linkedin.com/company/schuman-associates	https://twitter.com/schuman_eu?lang=es		
Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev	https://www.linkedin.com/company/fraunhofer-institut-f%C3%BCr-software-und-systemtechnik/	https://twitter.com/fraunhoferist		
Naukowa I Akademicka Siec Komputerowa -	https://www.linkedin.com/company/nask	https://twitter.com/NASK_pl	https://www.facebook.com/NASK-	

Panstwowy Instytut Badawczy (NASK)			164270215939388 3/	
Lietuvos Kibernetiniu Nusikaltimu Kompetenciju Ir Tyrimu Centras (L3CE)	N/A	N/A	N/A	N/A
Polish Cyber Security Cluster	https://www.linkedin.com/company/clustercybermadeinpoland/			
Contrader s.r.l.	https://www.linkedin.com/company/contrader-group		https://www.facebook.com/contradergroup	https://www.instagram.com/contraderjob/
ServiceNow Ireland Limited	https://www.linkedin.com/company/servicenow	https://twitter.com/servicenow	https://www.facebook.com/servicenow	https://www.instagram.com/servicenow/
DIGITALEUROPE AISBL	http://www.linkedin.com/company/digital-europe	https://twitter.com/digitaleurope	https://www.facebook.com/ICTDIGITALEUROPE	https://www.instagram.com/digitaleurope_org/
Agoria Asbl	https://www.linkedin.com/company/agoria	https://www.twitter.com/agorianl	https://www.facebook.com/agoria.be	https://www.instagram.com/agoria.be
European Digital SME Alliance (DIGITAL SME)	https://www.linkedin.com/company/european-digital-sme-alliance/	https://twitter.com/EUdigitalsme	https://www.facebook.com/DIGITALSMEAlliance/	
Terawe Technologies Limited	https://www.linkedin.com/company/terawe/	https://twitter.com/TeraweTech	https://www.facebook.com/teraweetech	https://www.instagram.com/teraweecorp/
BANCO SANTANDER SA	https://www.linkedin.com/company/banco-santander	https://twitter.com/bancosantander	https://www.facebook.com/santanderglobal	https://www.instagram.com/santander.global/
RED OPEN S.R.L.	https://it.linkedin.com/company/redopen	https://twitter.com/red_open_srl		https://www.instagram.com/red.open/
Pearson Benelux BV (Certiport),	https://www.linkedin.com/company/pearson-benelux		https://www.facebook.com/pearsonenglish/	
Indiepics	https://www.linkedin.com/company/231236/?trk=tyah	https://twitter.com/indiepicsIE	https://www.facebook.com/IndiePicsIE/?ref=br_rs	https://www.instagram.com/indiepics.ie/?hl=en
ProfilKlett	https://www.linkedin.com/company/profil-klett-hrvatska		https://www.facebook.com/ProfilKlettSkolskiPortal	

Table 14: D4S Consortium Partners' social media

Email marketing

The official Digital4Security newsletter will be set up on Brevo. It will be issued every second month — starting from year 2 — and in an ad-hoc manner, when needed. It will be used to communicate about the project progress and results and key related topics.

The WP5 leader manages the Digital4Security newsletter editorial line to ensure consistency. Partners are encouraged to submit interesting and related content directly to WP5 leader to be promoted on the newsletter. Partners' own content related to the topics of the project.
Third-party content that Partners find suitable and interesting for our target audiences (e.g., evergreen content, hot topics content).

All Partners can already subscribe to Digital4Security newsletter. To promote the newsletter, Partners are encouraged to share it with their network.

Website visitors can subscribe to the newsletter via an embedded form on the homepage.
For some specific communication and outreach purposes such as surveys, event invitations, or establishing the first contact for further communication and support, Consortium Partners will reach out to stakeholders and potential multipliers via direct mailing. This includes:

- Sending emails to individuals and organisations by Consortium representatives
- Using Partners' mailing lists/contacts to target specific target audiences.

All mailing lists will be managed respecting GDPR norms.

Press and media

Press releases will be published throughout the project. These aim to enhance the visibility of the Digital4Security project and share the most relevant outcomes of the project with the press. The following press release has already been produced:

- Press release on the launch of the Digital4Security (October 2023)

Each project partner will distribute the press releases to their respective networks and media contacts. Project Partners will also be encouraged to host the press releases on their website and share them via their newsletters and social media channels.

Events and networking

As part of the promotional strategy of D4S, DIGITALEUROPE will develop and implement an EU-wide communications campaign to promote the results and outputs of the DIGITAL4Security programme. DE, together with Matrix and Partner contributors, will prepare an advocacy plan to link D4S with the latest policy developments and to digital skills education, Cyber Skills Academy, and other relevant initiatives. A series of of events and webinars will be organised to present the key outputs and results, case studies collected and empower industry and education stakeholders to use the D4S results.

We will also consider external events on cybersecurity where D4S could find new audiences, or suggest speakers to present the project and/or discuss the topic of cybersecurity in Europe. More events will be considered in the future and added to the list.

Event	Date	City
The International Conference on the EU Cyber and Resilience Acts	11 – 13 March 2024	Brussels, Belgium
PDP 2024	20-22 March 2024	Dublin, Ireland
ECSO Award Finals 2024	21 – 22 March 2024	Bochum, Germany
Forum InCyber Europe	26 – 28 Match 2024	Lille, France
2nd ENISA Cybersecurity Policy Conference	17 April 2024	Brussels, Belgium
2024 Cyber Threat Intelligence Conference	15 – 17 April 2024	Berlin, Germany
Nordic IT Security Forum	23 May 2024	Stockholm, Sweden
SPHERE24	28 – 29 May 2024	Helsinki, Finland
Cybersec Europe	29 – 30 May 2024	Brussels, Belgium

Table 15: List of external events for Digital4Security exposure

Promotional assets

DIGITALEUROPE and Indiepics will produce various promotional assets to be used for above-mentioned communication and outreach activities on different channels. Partners will play an important part in the promotional roll-out, as actions and materials will be channelled through their websites. Therefore, these assets will regularly be made available as suites of ready-to-use promotional materials, to promote the website, the project and Master's across target countries.

The primary promotional assets include:

Asset	To be used for
Responsive HTML email template	Email marketing
Animated online banners	D4S and Consortium Partners and third party websites Social media Email marketing
Promotional flyers / brochures in all languages	D4S and Consortium Partners and third party websites Social media Email marketing
Infographics Animated Gifs Branded graphics Videos Other artworks	D4S and Consortium Partners and third party websites Social media Email marketing
Print flyers / brochures Roll-up banners	Relevant events
Promotional messages Social media share copies	Email marketing Social media
Press Releases	D4S and Consortium Partners and third party websites Email marketing Press and media
Brand guidelines Logo artwork files	To be used by Partners who wish to create their own materials or promote the platform.

Table 16: D4S primary promotional assets

All promotional assets will be stored in the D4S Team's channel, accessible to project Partners.

Monitoring and reporting

DIGITALEUROPE, as WP5 Leader, will ensure an efficient and effective implementation of the communication, dissemination and stakeholder engagement plan throughout the project.

Internal Communications Tools

D4S Partners will use the Digital4Security Microsoft Teams environment as the main internal communication tool: **WP5 Dissemination and European Impact.**
Another tool that will be used by all Partners is the **Digital4Security - Comms milestone tracker** created on MS Form to collect and report all communication activities performed every 3 months by Partners to promote Digital4Security activities. The first form was sent out to Partners on Thursday, February 15, to gather information on all communications activities conducted by their organisations over the last 4 months (October 1, 2023 to January 31, 2024).

Reporting and evaluation

The project Consortium will undertake constant and effective monitoring and analysis of communications and dissemination results. Every 3 months, all Partners will fill in a communication and performance reports, managed by WP5 leader, determining the advancements on the KPIs and recommendations to improve or maintain high performance.
These quarterly reports will be produced and will support the further developments of future communication actions and campaigns for optimal impact.

The data collected will be used for:

1. Providing the necessary information to the Project coordination to fill in the project internal reports (interim, final reports).
2. Assessing the impact of the communication and outreach activities implemented to reach the KPIs.

The first reporting cycle will start in July 2024 (M10) and will cover the previous 10 months of activities. From then onwards, the Partners will report on the set quarterly basis as follows:

Cycle	Date of reporting	Period covered
1.	July 2024 (M10)	October 2023 – June 2024
2.	October 2024 (M13)	July – October 2024
3.	January (M16)	November 2024 – January 2025
4.	April (M19)	February – April 2025
5.	July (M21)	May – July 2025
6.	October (M24)	August – October 2025
7.	January (M27)	November 2025 – January 2026
8.	April (M30)	February – April 2026
9.	July (M33)	May – July 2026
10.	October (M36)	August – October 2026
11.	January (M39)	November 2026 – January 2027
12.	April (M42)	February – April 2027
13.	July (M45)	May – July 2027
14.	October (M48)	August – October 2027

Table 17: D4S Reporting cycles

Annexes

Annex I: Digital4Security Brand Manual

The **Digital4Security brand manual** provides detailed guidelines on how to use D4S logo and its variations, colour palette, typeface and how to apply the EU flag emblem, funding statement and disclaimer.

Rate	1	2	3	4	5
Quality Parameter	very low/strongly disagree	low/dis agree	moderate/ neither nor	high/ agree	very high/strongly agree
1. The work performed corresponds to the requirements and methodological standards of the project.	☐	☐	☐	☐	☐
Please insert any comments here					
2. The drafting and structuring of each deliverable include the contribution of all relevant experts.	☐	☐	☐	☐	☐
Please insert any comments here					
3. Deliverables use clear and easily understandable language in the text and the design is professional and in line with the project brand identity, guidelines, and document template.	☐	☐	☐	☐	☐
Please insert any comments here					
4. The output is in line with the standards adopted by the European Commission.	☐	☐	☐	☐	☐
Please insert any comments here					
Name of the WP Leader	DIGITALEUROPE				
Submission Date	29/02/2024				

Funded by
the European Union

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED DIGITAL SKILLS

DIGITAL EUROPE PROGRAMME

Co-funded by the European Union

Digital4Security
Brand guidelines

ADVANCED DIGITAL SKILLS
DIGITAL EUROPE PROGRAMME

Co-funded by the European Union

Digital4Security
Shaping Europe's cyber future

Contents

Introduction

This brief guideline document has been created to provide users of the **Digital4Security** identity with a guide to its basic elements. The guide has been prepared to assist both in-house and external users. It has been developed to ensure consistency in the application of the identity and enhance the quality of the brand.

In relation to the logos, this manual identifies solutions in all visual environments. Only the supplied files can be used – as depicted in this guide without distortion of any kind. A suite of colours has also been selected for use with the brand. As Digital4Security is a digital brand we have elected to specify colours in Hex, RGB and CMYK. When working with the provided logo files be sure to work in RGB colour mode. In relation to print the vast majority of printing is now digital and the CMYK codes are suitable for this.

An essential part of the brand identity is that of typography and we have specified two fonts that complement the brand. These are universally available.

This brand was created and developed by the Brand Team at Matrix Internet.

The Digital4Security logo is composed of three distinct graphic elements:

The Fingerprint (the Symbol)
The Logotype
and
The Tagline

Each of these are essential elements in the visual presentation of the brand.

The Master Logo uses three principal corporate colours:

D4S Orange
D4S Blue
D4S Dark Blue

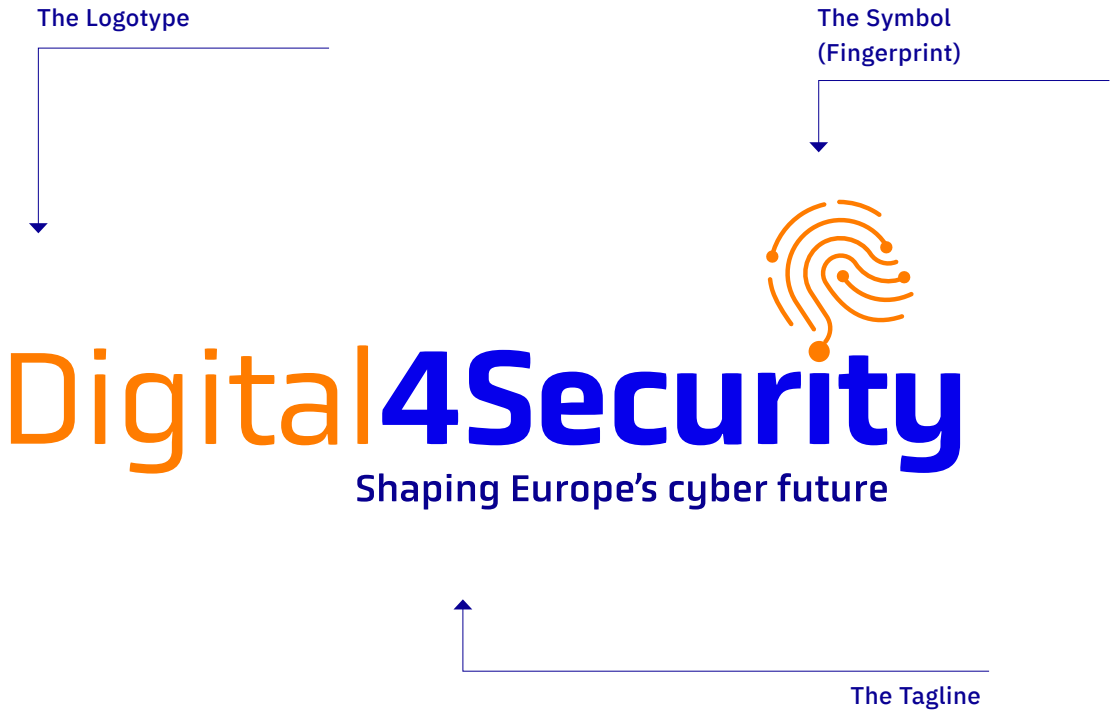
The fingerprint symbol is also available in solo files without the title and logotype.

The Master Logo is available in the following formats:

Vector: **.ai**
Vector: **.svg**
Windows: **.jpg**
Windows: **.png**

1.1 MASTER BRAND ELEMENTS

1.1.1 The Master Logo



The Digital4Security logo has been designed to be flexible in its use of colour and its ability to work on a wide variety of backgrounds and colours.

The logos illustrated here are:

1 **D4S (Master) Reverse**

2 **D4S (Master) Reverse Blue**

3 **D4S (Master) Reverse BW**

The Reverse Logos are available in the following formats:

Vector: **.ai**
Vector: **.svg**
Rasterised: **.png**

1.1 MASTER BRAND ELEMENTS

1.1.2 Logo variations: The reverse options

1

2

3

The Digital4Security symbol is a useful element to add interest in presentations and documents. Deployed on its own it can create impact and help develop the importance of the symbol as core element on its own.

It has been designed to be flexible in its ability to work on a wide variety of backgrounds and colours.

The logos illustrated here are:

1 **D4S (Master) Symbol**

2 **D4S (Master) Symbol Blue**

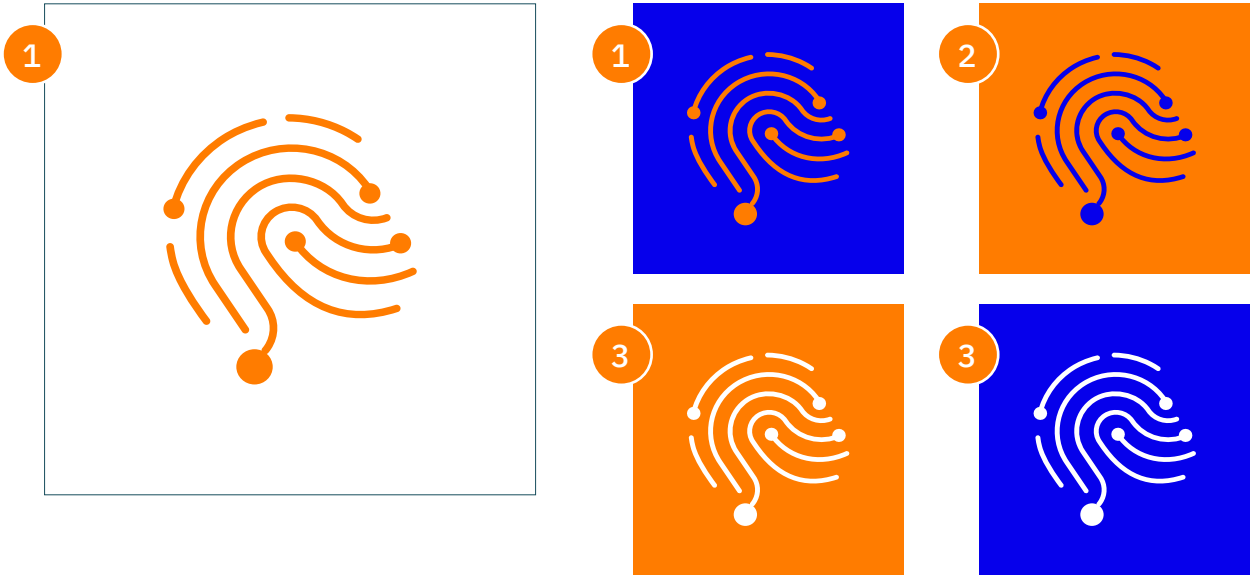
3 **D4S (Master) Symbol Reverse**

The Reverse Logos are available in the following formats:

Vector: **.ai**
Vector: **.svg**
Rasterised: **.jpg**
Rasterised: **.png**

1.1 MASTER BRAND ELEMENTS

1.1.3 Logo variations: The Symbol on its own



The brand symbol provides graphic, motion graphic and web designers with endless opportunities in relation to creating visually striking materials. These include the ability to add the symbol as tonal additions to comms materials and interesting backgrounds for adverts and social media posts. There is no strict guide in terms of its use other than to ensure it never dominates to the point that the 'logo' is visually overwhelmed. We have included some examples here, however, we are confident that in the hands of good designers this element will become one of the memorable features of the brand.

1.1 MASTER BRAND ELEMENTS

1.1.4 Using the symbol as a graphic element

A repeat pattern has been generated to provide users with an interesting additional element to the brand toolkit. It can be applied as end papers on publications or as chapter break pages. This element needs to be used with caution and preferably by a professional Graphic Designer.

The files illustrated here are:

1 **D4S Pattern 1**

2 **D4S Pattern 2**

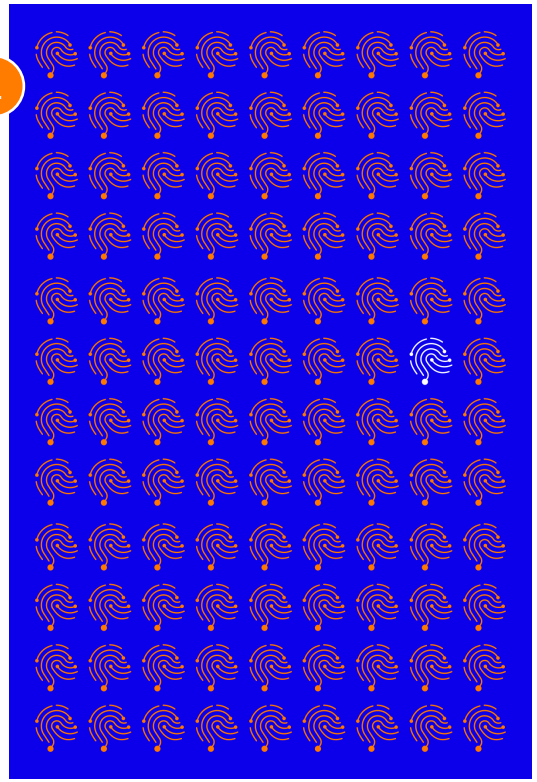
This file is available in the following formats:

Vector: **.ai**
Vector: **.svg**
Rasterised: **.png**

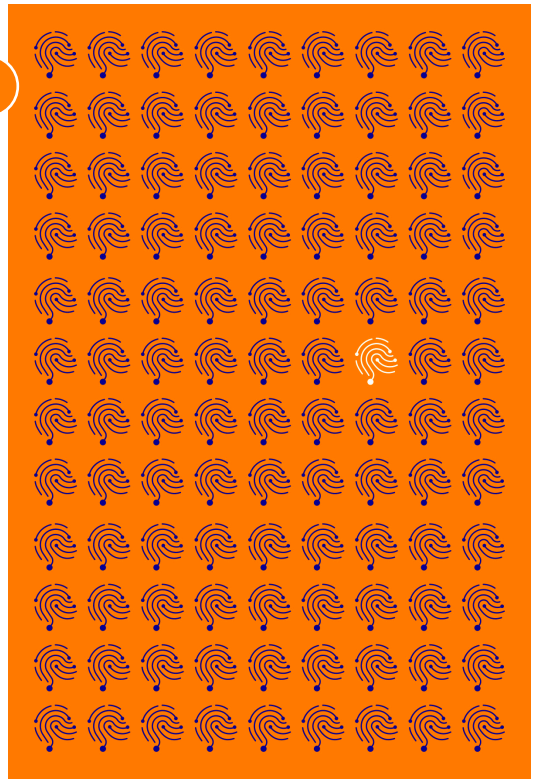
1.1 MASTER BRAND ELEMENTS

1.1.5 Logo variations: The repeat pattern

1



2



Each of the logos has been mastered and saved in a variety of formats, suitable for Print (vector) and Online (Windows).

As D4S is a digital first brand the files are provided in RGB colour. For print usage see CMYK conversions on page 13.

Windows files are primarily for use in Word applications and Online.

Vector files are production files used in the design and print areas. They are suitable for all graphic work including signage and packaging.

Reverse files are supplied only in .ai, .svg and .png formats

ONLY these files can be used and cannot in any fashion be distorted or altered. No element can be removed or added.

1.2 MASTER BRAND ELEMENTS (MASTER LOGOS)

1.2.1 The master files listing

FILE:	D4S (Master) Colour.ai	VECTOR	All design applications
FILE:	D4S (Master) Colour.svg	VECTOR	Windows and Online
FILE:	D4S (Master) Colour.jpg	RASTERISED	Windows and Online
FILE:	D4S (Master) Colour.png	RASTERISED	Windows and Online
FILE:	D4S (Master) BW.ai	VECTOR	All design applications
FILE:	D4S (Master) BW.svg	VECTOR	Windows and Online
FILE:	D4S (Master) BW.jpg	RASTERISED	Windows and Online
FILE:	D4S (Master) BW.png	RASTERISED	Windows and Online

Each of the logos has been mastered and saved in a variety of formats, suitable for Print (vector) and Online (Windows).

Windows files are primarily for use in Word applications and Online.

Vector files are production files used for Design and Print applications. They are suitable for all graphic work including signage and packaging.

Reverse files are supplied only in .ai, .svg and .png formats

ONLY these files can be used and cannot in any fashion be distorted or altered. No element can be removed or added.

1.2 MASTER BRAND ELEMENTS (REVERSED LOGOS)

1.2.2 The master files listing

FILE:	S4R (Master) Reverse.ai	VECTOR	All design applications
FILE:	D4S (Master) Reverse.svg	VECTOR	Windows and Online
FILE:	D4S (Master) Reverse.png	RASTERISED	Windows and Online
FILE:	S4R (Master) Reverse Blue.ai	VECTOR	All design applications
FILE:	S4R (Master) Reverse Blue.svg	VECTOR	Windows and Online
FILE:	S4R (Master) Reverse Blue.png	RASTERISED	Windows and Online
FILE:	S4R (Master) Reverse BW.ai	VECTOR	All design applications
FILE:	S4R (Master) Reverse BW.svg	VECTOR	Windows and Online
FILE:	S4R (Master) Reverse BW.png	RASTERISED	Windows and Online

The Master Symbol files have also been created in a suite of suitable formats.

Reverse files are supplied only in .ai .svg and .png formats

ONLY these files can be used and cannot in any fashion be distorted or altered. No element can be removed or added.

1.2 MASTER BRAND ELEMENTS (MASTER SYMBOL)

1.2.3 The master files listing

FILE:	D4S (Master) Symbol.ai	VECTOR	All design applications
FILE:	D4S (Master) Symbol.svg	VECTOR	Windows and Online
FILE:	D4S (Master) Symbol.jpg	RASTERISED	Windows and Online
FILE:	D4S (Master) Symbol.png	RASTERISED	Windows and Online
FILE:	S4R (Master) Symbol Blue.ai	VECTOR	All design applications
FILE:	S4R (Master) Symbol Blue.svg	VECTOR	Windows and Online
FILE:	S4R (Master) Symbol Blue.jpg	RASTERISED	Windows and Online
FILE:	S4R (Master) Symbol Blue.png	RASTERISED	Windows and Online
FILE:	S4R (Master) Symbol Reverse.ai	VECTOR	All design applications
FILE:	S4R (Master) Symbol Reverse.svg	VECTOR	Windows and Online
FILE:	S4R (Master) Symbol Reverse.jpg	RASTERISED	Windows and Online
FILE:	S4R (Master) Symbol Reverse.png	RASTERISED	Windows and Online

The special treatment file are the D4S Patterns listed on the right.

ONLY these files can be used and cannot in any fashion be distorted or altered. No element can be removed or added.

1.2 MASTER BRAND ELEMENTS (SPECIAL ELEMENTS)

1.2.5 The special files listing

FILE:	D4S Pattern 1.ai	VECTOR	All design applications
FILE:	D4S Pattern 1.svg	VECTOR	Windows and Online
FILE:	D4S Pattern 1.png	RASTERISED	Windows and Online
FILE:	D4S Pattern 2.ai	VECTOR	All design applications
FILE:	D4S Pattern 2.svg	VECTOR	Windows and Online
FILE:	D4S Pattern 2.png	RASTERISED	Windows and Online

As Digital4Security is predominantly digital brand we have elected to specify colours in Hex, RGB and CMYK. When working with the provided logo files be sure to work in RGB colour mode. In relation to print the vast majority of printing is now digital and the CMYK codes are suitable for this.

The primary colours for the brand are:

D4S Orange
D4S Blue

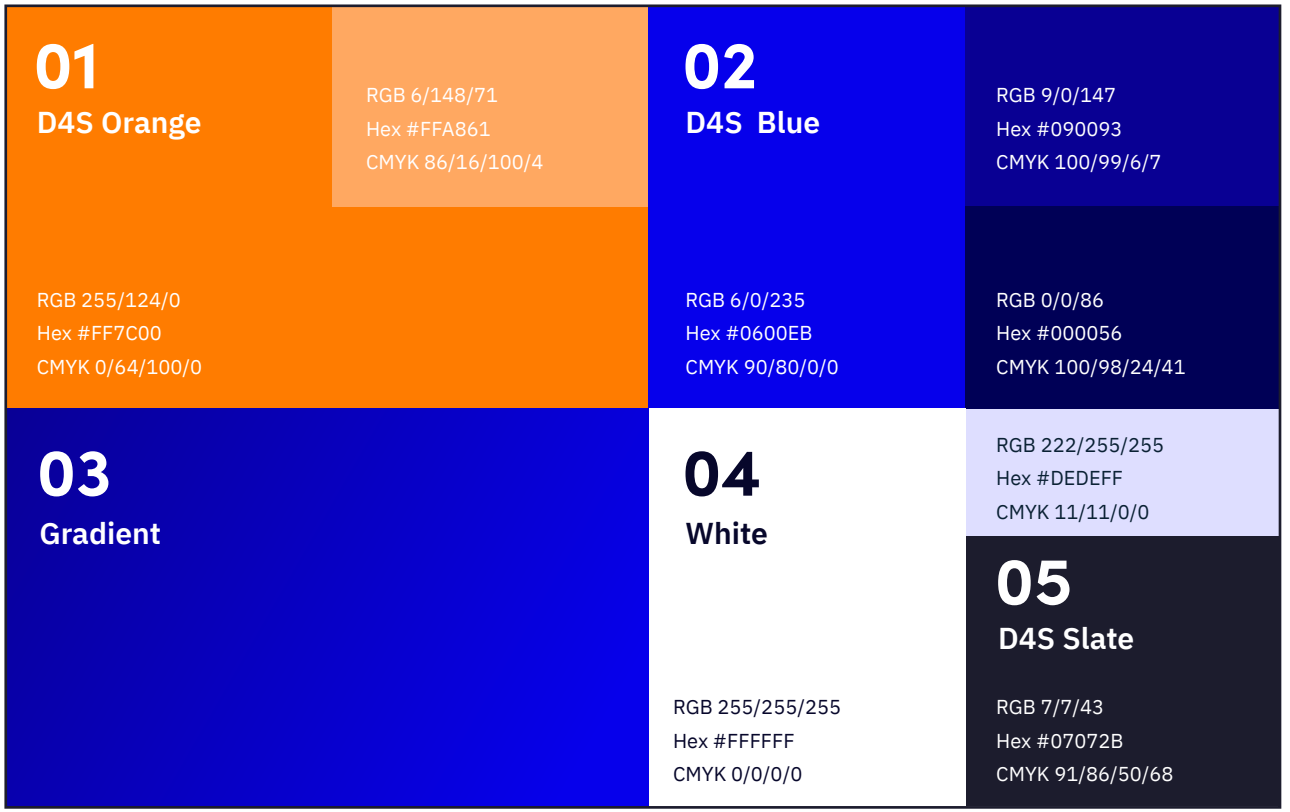
An Adobe Illustrator file is enclosed to allow you to create your own colour library of the specified colours.

NOTE:
Please note that the colours illustrated here may vary depending on the implementation environment. Digital printing will vary as will screen values which are dictated by each user's equipment.

DO NOT use digital print-outs of this guide from desktop printers for colour matching as digital printing does not deliver stable colour.

2.1 **COLOUR:** The Primary Colours

2.1.1 The Primary Colours



In terms of typography we have selected a specific display font for the Brand Identity. This is Cairo.

This font is not really suitable for body content or large paragraphs of text. However, short statements could be considered in lighter weights.

Suggested weights are:

Cairo Light

Cairo SemiBold

Cairo Bold

For Online applications such as email, PowerPoint presentations, documents and any other Online communications it is prudent to employ a universally used font. The Cairo Family has been sourced from the Google Font Library which is universally available: https://fonts.google.com/specimen/Cairo?preview.

3.1 TYPOGRAPHY: Display Font

3.1.1 Display Font

AaBbCc123 **Cairo Bold**

In a world that is bewildering in terms of competitive clamour,

Cairo SemiBold

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789@£$%&?

Cairo Light

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789@£$%&?

We have selected a contrasting content font that works well with Cairo - **Work Sans.** This font is sourced from the Google Fonts Library and comes in a wide variety of weights. It can be used primarily for content but in the hands of a good designer will also work in display.

Work Sans Light

Work Sans Light Italic

Work Sans Regular

Work Sans Regular Italic

Work Sans Medium

Work Sans Medium Italic

Work Sans SemiBold

Work Sans SemiBold Italic

Work Sans Bold

Work Sans Bold Italic

Work Sans ExtraBold

Work Sans ExtraBold italic

Work Sans Black

Work Sans Black Italic

3.1 **TYPOGRAPHY:** Content Font

3.1.2 **Content font**

AaBbCc123 Work Sans Regular

In a world that is bewildering in terms
of competitive clamour,

Work Sans Light

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789@£$%&?

Work Sans Bold

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789@£$%&?

Cairo and Work Sans work well together as illustrated on the right. The use of font weights and sizes should always be based on a good balance with the goal of good readability.

We would discourage the use of some of the lighter fonts in the Work Sans Family to ensure accessibility on digital material.

3.1 **TYPOGRAPHY:** The fonts in action

3.1.3 The fonts in action

Introduction

In a world that is bewildering in terms of competitive clamour, brands represent clarity.

Atus exces magniet iusa cus expeles tiaecae explam vero et evendit assitecae et, que estiatur, nonsend uciatiur, et officimUgitaspe repudaepedis velleni squamusciet, cum volupta tistiis imoluptur? Quia volorit, con re cum eum quia.

1.0 The research project

Atus exces magniet iusa cus expeles tiaecae explam vero et evendit assitecae et, que estiatur, nonsend uciatiur, et officimUgitaspe repudaepedis **velleni squamusciet**, cum volupta tistiis imoluptur? Quiavolorit, con re cum eum quia **conserrorume** volupicius.

2.0 The findings

Atus exces magniet iusa cus expeles tiaecae explam vero et evendit assitecae et, que estiatur, nonsend uciatiur, officim Ugitaspe repudaepedis velleni squamusciet, cum volupta tistiis imoluptur? Quiavolorit, con re cum eum quia conserrorume volupicius.

Every organisation has a distinctive Tone of Voice (TOV). During the brand workshop this was discussed and the general consensus is detailed on the right. This is important to consider when preparing content for any Digital4Security communication.

Likewise the key values will also help shape the content both in terms of the written and visual material.

4.1 **TONE OF VOICE** (AND VALUES)

4.1.1 Tone of Voice

Knowledgeable & Engaging (1st)

Friendly (2nd)

4.1.2 Values

Trustworthy
Innovative
Accessible
Sustainable

It is crucial that the Digital4Security identity is deployed in a consistent manner at all times - particularly when the identity is being placed with other brands. For this reason we have set up a minimum ‘Breathing Space’ guide as illustrated on the right.

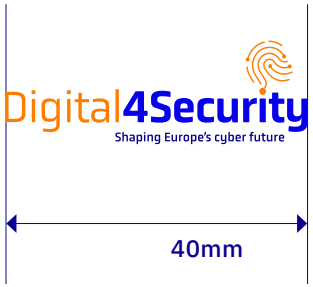
It is also important to deploy the logo at sizes where it will retain its readability and structural integrity. We have set a minimum size of 50mm as the guide for this.

5.1 THE BRAND IN APPLICATION

5.1.1 Breathing Space

The letter 4 of the word mark is used as a device to indicate ‘minimum space’

5.1.1 Minimum logo size



40mm (displayed at 100%)

A lot of care has been taken to create this identity and consequentially its application should be consistent. Common sense should be used when working with the logo.

The logo should never be distorted and the elements should never be separated or altered. The logo itself must never be placed on busy photographic backgrounds, or colours that detract from it, and should always be visible across all media.

5.2 THE BRAND IN APPLICATION (DON'T DO'S)

5.1.2 Don't Do's

DON'T change the colours for any reason

DON'T change or remove any of the logo's elements

Never distort the logo

DON'T move any elements around

DON'T even think of changing the typeface

Use the appropriate logo for the background

Digital4Security

Shaping Europe's cyber future

Thank you

Developed & designed by Matrix Internet

matrix INTERNET

mylia_ | THE ADECCO GROUP | AGORIA | AP ATAYA&PARTNERS | Santander | BRNO UNIVERSITY OF TECHNOLOGY | contrader | CY UNIVERSITÉ | DIGITALEUROPE | Digital Technology Skills Ltd | European DIGITAL SME Alliance | Fraunhofer ISST

CYBER RANGES | indiepics | Tech Industry Alliance Skillnet | matrix INTERNET | CYBER IRELAND | MRU Mykolas Romeris University | National College of Ireland | NASK | CERTIPORT | #Cyber Made InPoland | POLITECNICO MILANO 1863

PROFIL Klett | ReD OPEN | SCHUMAN ASSOCIATES | servicenow | Skillnet IRELAND | terawe | unir LA UNIVERSIDAD EN INTERNET | UNIVERSITY OF BRESCIA | German University of Digital Science | university of koblenz | Faculty of Informatics and Digital Technologies | VYTAUTAS MAGNUS UNIVERSITY