DIGITAL-ECCC-2022-CYBER-B-03-SOC
DIGITAL JU Simple Grants
Grant Agreement No.: 101145874

Next Generation Security Operation Centres

D7.1 Initial Plan for the Exploitation and Dissemination of Results

Report Identifier:	D7.1		
Work-package:	WP7	**Task:**	T7.1
Responsible Partner:	European Dynamics Luxembourg SA (ED)	**Version Number:**	1.0
Due Date	31/03/2024	**Document Date:**	03/04/2024
Distribution Security:	PUB	**Deliverable Type:**	R
Keywords:	Dissemination, Communication, Exploitable Results, Market Positioning		
Project website: https://ng-soc.eu			

Document History

Version	Content & Changes	Issue Date
0.1	**Document created**	**21/02/2024**
0.2	**Created first version of document with placeholders for partners contributions**	**19/03/2024**
0.3	**Received and merged partners contributions. Sent document for review**	**25/03/2024**
0.4	**Document reviewed**	**26/03/2024**
0.5	**Reviews are combined**	**27/03/2024**
0.6	**Sent for Quality Assurance**	**27/03/2024**
1.0	**Quality Assurance and Submission**	**03/04/2024**

Quality Control

	Name	Organisation	Date
Editor	Alkiviadis Giannakoulias	European Dynamics	21/02/2024
Peer review 1	Marios Zacharias	Space Hellas	27/03/2024
Peer review 2	Vasileios Mavroeidis	Cyentific	02/04/2024
Authorised by (Technical Coordinator)	Vasileios Mavroeidis	Cyentific	02/04/2024
Authorised by (Quality Manager)	Alkiviadis Giannakoulias	European Dynamics	03/04/2024
Submitted by (Project Coordinator)	Anastasia Garbi	European Dynamics	03/04/2024

Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The NG-SOC Consortium members shall have no liability for damages of any kind, including, without limitation, direct, special, indirect, or consequential damages that may result from the use of these materials, subject to any liability that is mandatory due to applicable law.

Copyright notice

Table of Contents

List of Figures

List of Tables

Abbreviations

Acronym	Description
BPD	Business Plan Development
CA	Consortium Agreement
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
EC	European Commission
EU	European Union
G2M	Go-To-Market Support
GA	Grant Agreement
HRB	HORIZON Results Booster
IoC	Indicator of Compromise
IPR	Intellectual Property Rights
KER	Key Exploitable Result
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
PDES	Portfolio Dissemination and Exploitation Strategy
PG	Project Group
SW, S/W	Software
TRL	Technology Readiness Level
WP	Work Package

Executive Summary

This deliverable presents the initial Exploitation and Dissemination Plan for the NG-SOC project, and as such, its main objective is to a) identify and transform NG-SOC services and individual components into marketable products and b) produce the strategy and the plans for dissemination and communication, providing the list of dissemination and communication activities performed by the consortium during, primarily, the first project period, and what is defined for the next months of the project.

The goal of the exploitation strategy is to create profitable outcomes which could be further exploited via different routes by different stakeholder groups. Valuable inputs from the consortium partners were used to understand vital exploitation aspects and to reach conclusions. Furthermore, to implement a successful exploitation strategy, it is essential to identify and characterize key exploitable results (KERs) in NG-SOC. Their exploitation potential is expected to have either commercial, social, or scientific value. Individual exploitation plans of all consortium partners describe which results are going to be exploited, market sector and customer segments, preliminary plans for exploitation channels, expected sales and current achieved exploitation goals. A preliminary IPR strategy, which is an essential requirement for a successful exploitation has been outlined and both the background and foreground technologies have been identified.

Initially, an introduction to the dissemination and communication objectives of the project is provided. Then, the NG-SOC dissemination and communication measures are presented. Following the definition of dissemination means and mechanisms, a concrete NG-SOC implementation plan for dissemination and communication activities has been prepared to guide the efforts for the wide dissemination and ensure large scale reach of the results. Along with the planning about dissemination and communication activities, a list of KPIs is defined to periodically monitor the performance of dissemination and communication activities.

The dissemination and communication plan will be continuously updated and enhanced to consider all the results along the project maturing, with advancements reported in the subsequent deliverables.

Some of the main exploitation findings are:

The NG-SOC platform has a huge exploitation potential for increasing SOC teams' situational awareness, collaborative resilience, detection and response capacities, as well as for cybersecurity training;

Its biggest advantages include AI-enhanced technologies for effective prediction, detection, analysis, and response to threats, realistic simulations, and multi-domain functionality;

NG-SOC has a low to medium threat of new players on the market, its suppliers have a relatively high bargaining power, the threat of substitute products or services is low, its buyers have a medium bargaining power, and the overall competition can be considered low to medium;

There have been 10 identified and characterised key exploitable results (of types - software, services, and knowledge) in NG-SOC;

7 consortium partners have elaborated their individual exploitation plans;

There are 6 identified background technologies/know-how brought into the project by partners;

There are 17 identified foreground technologies/know-how produced over the duration of the project.

1 Introduction

1.1 Project Introduction

NG-SOC is a three-year (2024 - 2026) EU co-funded project implemented by a consortium of 7 partners from 5 countries. The main aim is to develop a **collaborative, interoperable SOC multi-service** that holistically combines capacities for **shared situational awareness, coordinated incident handling,** and **dedicated training sessions** and **educational programmes** in digital infrastructure security, tailored to identified training goals and objectives, ultimately enhancing national cybersecurity capabilities and cross-border collaboration, in line with current and upcoming regulatory requirements (e.g., NIS2, CRA, CSA). To achieve these objectives, NG-SOC will adopt an **open-standards-based** implementation strategy and to the extent possible utilise and enhance open-source technological solutions.

1.2 Deliverable Purpose

Although the end goal of the NG-SOC project is to enhance cybersecurity preparedness and resilience in Europe, it is very important to achieve this with a sound and sustainable approach regarding the growing cybersecurity market. It is important to underline the innovative aspects of NG-SOC, which will, at the same time, demonstrate clear advancements and benefits provided by the project when compared to the current market and existing solutions. NG-SOC, as a technologically advanced platform, will be able to provide a dynamic, modular, and adaptable solution, able to extend the capabilities of existing SOC tools used to predict, detect, analyse, and respond to threats. Being founded on scalability and sustainability in both technological and business aspects, NG-SOC should remain a competitive and up-to-date solution, being able to provide a high-quality SOC service well into the foreseeable future.

According to the European Commission glossary, "*Exploitation*" is defined as "*Means to make use of the results produced in an EU project in further activities (other than those covered by the project, e.g., in other research activities; in developing, creating, and marketing a product, process or service; in standardisation activities).*" [1]

To achieve the aforementioned longevity and sustainability, it is therefore, important that the NG-SOC project implements and maintains a tailor-made exploitation strategy that will allow to create a concrete impact on society, with the expectation that the exploitable results will be used beyond the lifetime of the project. Therefore, to implement a successful exploitation strategy, it is essential to identify and characterize the key exploitable results of NG-SOC. As a result, it will be possible to measure how much of an impact the project had. Furthermore, identifying the most innovative project outcomes and ways to exploit them will further help to increase interest as well as commercial and marketable aspects. However, it is understood that not all results produced throughout the project will be exploitable at the commercial and/or research level, but rather only ones with a high scientific, economic, or social potential.

To this end, this deliverable is a part of the horizontal-based work package WP7: Project Impact and Cybersecurity Culture Awareness. It is the initial exploitation plan, considering that D7.2 "Business plan - M18" and D7.3 "Business plan – M36" will provide more up-to-date exploitation strategies, elaborating on the market trends, the target group's needs, and the overall business model towards the potential commercialization of project results.

Thus, this deliverable reports on initial exploitation activities, which include the definition of the NG-SOC exploitation framework and its 3 core phases, followed by the identification and characterisation of key exploitable results, identification of individual exploitation plans defined by all consortium members, to lay the basis for the oncoming IPR activities as well as establish future actions in order to ensure successful impact sustainability of the NG-SOC project beyond its lifetime.

Here, the continuous development of the exploitation strategy will allow the consortium to have a better understanding of concrete outcomes and potential exploitation opportunities. Through ongoing engagement, the consortium will also take the opportunity to jointly further refine and improve the strategy towards the end of the project. During the initial definition of the exploitation strategy, we followed a structured approach with instructions, examples and expected information to understand vital exploitation aspects and to reach conclusions. Further sources used include the project grant agreement (since it outlines preliminary opportunities), project meetings, communication with WP leaders, and knowledge gained from other similar projects.

Furthermore, the deliverable presents the strategy and work plan for the dissemination and communication activities of NG-SOC and, in parallel, defines the main marketing methods and material tools (communication means) and initial dissemination plan. Planning is crucial for effective actions in communication, hence this document:

- identifies relevant target groups and optimal communication strategies;
- defines the overall dissemination and communication strategy/roadmap, and provides a detailed view on tools and means to support communication and dissemination activities;
- establishes a consistent and high-quality project graphical identity (e.g. colour palette, themes, templates, fonts) which will constitute a powerful trend about the project and develop dynamic, personalized and content-rich material (leaflets, posters, other dissemination material) in order to continuously promote and further enhance the dissemination activities.

In addition, the dissemination plan aims to track KPIs related to these activities during this project.

The Dissemination and Communication Plan will be updated and presented to the consortium at internal periodic meetings. In M18 and M36, the activities implemented will be reported for the corresponding periods.

1.3 Deliverable Structure

The structure of this document is as follows:

- **Section 2** provides an overview of the exploitation strategy and its 3 main phases. Here, the objectives are to identify and transform NG-SOC services and individual components into marketable products and as such to create profitable outcomes. These outcomes will be exploited via different routes by different stakeholder groups.
- **Section 3** provides the identification of the Key Exploitable Results. Here, the generated list represents most innovative results which will be delivered by the end of the project. Their exploitation potential is expected to have either a commercial, social or a scientific value.
- **Section 4** provides individual exploitation plans of all consortium partners. This includes results that are going to be exploited, market sector and customer segments, preliminary plans for exploitation channels, expected sales, and current achieved exploitation goals.
- **Section 5** provides an initial basis of an IPR strategy which is an essential requirement for a successful exploitation. This includes an overview of the background technologies and know-how that the consortium partners are bringing in the project, as identified in the Consortium Agreement, as well as an overview of foreground technologies and know-how generated by partners.
- **Section 6** provides an overview of the EC provided HORIZON Results Booster services provides by the EC, as NG-SOC will take advantage of this initiative and explore the possibilities to boost its impact.
- **Section 7** provides the vision of the Consortium concerning the communication of the NG-SOC's outputs; presents the high-level dissemination and communication objectives and strategy; identifies the main

target audiences along with their specific interest in the project; provides the detailed planning of the dissemination tasks to be carried out by the project partners and the optimal tools and means which will support the dissemination activities; details the dissemination tasks to be carried out by the project partners; defines the optimal tools and means which will support the dissemination activities; describes the individual partners' plans intended to disseminate the achievements of the NG-SOC project to the scientific community and to other interested stakeholders; establishes a consistent and high-quality project theme/brand which will constitute a powerful trend about the project and develop dynamic, personalized and content rich material (leaflet, poster, other dissemination material), in order to continuously promote and further enhance the dissemination activities; identifies a series of KPIs related to the dissemination and communication activities.

- **Section 8** provides the conclusion of this deliverable.

2 Initial Exploitation Strategy

One of the main objectives of the exploitation strategy is to identify and transform NG-SOC services and individual components into marketable products and, as such, to create profitable outcomes. To bring the NG-SOC solution to the market, a structured and methodological approach needs to be defined and implemented. Such a tailor-made exploitation plan will make it possible to achieve a maximum impact of the achieved project results through appropriate business models (to be detailed in D7.2 “Business plan - M18” and D7.3 “Business plan – M36”). Here, the main goal is to develop strategies for exploiting the project results and exploring their wider use, sustainability, and business feasibility.

Furthermore, it is necessary to properly coordinate and allocate the partners’ efforts, to monitor progress and plan activities during the project lifetime as well as to establish future actions to ensure successful sustainability of the NG-SOC project beyond its lifetime. A properly set-up consortium like in NG-SOC, has a high impact on the exploitation results of the project, where adequate and relevant stakeholders will help to gain a better understanding of the market. As a result, it will be easier to define and commercialize key NG-SOC products and services, as well as to include further stakeholders such as decision makers, governments, et.

2.1 Exploitation Routes

NG-SOC will produce various scientific, research, engagement, and development outcomes, which have a high potential to be exploited in different ways by different stakeholder groups, as described in Section 7. The NG-SOC consortium has identified the following initial exploitation routes: scientific, commercial, and exploitation by/through networks, associations, initiatives, policy groups.

2.1.1 Scientific Exploitation

The identified scientific exploitation objectives of the NG-SOC produced knowledge are:

- Raise awareness on the project’s outcomes and their benefits by reaching both academic and practitioner target groups.
- Build trust in the NG-SOC brand and all the solutions and services derived from this project.
- These objectives can be reached through the implementation of several scientific exploitation activities, such as **academic publications and conference participation,** where NG-SOC partners plan to be very active, participate, organise, and plan several venues.
- Other potential scientific exploitation measures are currently being explored: blog posts, action plans/research roadmaps, policy papers/recommendations, informative pieces/news and press releases, internal and external newsletters, a handbook, etc.

2.1.2 Commercial Exploitation

Commercial exploitation aims to transfer NG-SOC achievements and lessons learned, as well as to inspire interest and market demand concerning the NG-SOC final outputs. The industrial partners will use their well-established networks of European, national, and international contacts to communicate the results of NG-SOC, draw their attention, and increase its visibility. Here, the target groups are:

- **European industry**: Marketing campaigns and in-house presentations to increase public awareness and commercialise the results of NG-SOC.
- **EU citizens and customers**: Users of cyber-security products and services and cyber-security professionals are key players in the cyber-security transformation; NG-SOC will ensure that the results

of the work are available across Europe in both technical and media-focused formats, create opportunities, and that the wider public can make use of the results.

- **IT organisations and professionals**: Business decision-makers can adopt project results in the computing infrastructures or in the system architectures used at the enterprises. IT specialists and SOC members can integrate the provided software solutions into systems developed by other companies, equipment manufacturers and/or cyber-security suppliers can deliver products that may deal with highly sophisticated attacks, etc.
- **International industry and customers**: NG SOC will not constrain the potential commercialization of the results within EU boundaries but will aim to establish an international footprint and visibility through engagement, collaborations, and other networking activities such as through industry conferences and standardization with SMEs and large organisations.

Some initial findings of the early commercial exploitation routes include:

- The number and sophistication of cyber-attacks are growing at a global scale.
- Ongoing analyses show that the projections for global markets initially identified in the grant agreement are rising; thus, the business opportunities for NG-SOC remain valid.
- A rising interest in cyber security solutions for the critical infrastructure sector is predicted.
- Cybersecurity workforce demand will increase.
- There is a shortage of affordable, open-source SOC tools, especially in the micro and SME segments.

2.1.3 Networks, Associations, Initiatives, Policy Groups

NG-SOC partners are members or work together with several networks and initiatives, as well as participate in several other ongoing projects. NG-SOC partners will get in contact with potential external cooperation partners and projects, ensuring that any result and approach from NG-SOC in terms of interoperability, standards, and security, together with business validation and sustainability, can be clustered horizontally. NG-SOC outputs will be exploited through other networks and by liaising with policymakers to maximize the outreach and impact of the main project outcomes. This will have a positive effect and will influence the future game-changers in the cyber security industry; academic debates and discussions may provide new directions for the project results, which will allow for innovation and result in job creation across Europe.

NG-SOC is aligned with the European Commission’s vision to ensure security for all EU citizens, whereby consolidating all available resources and intelligence, as well as ensuring collaboration between running projects and initiatives, will produce innovative security solutions.

A **SOC Network** will be established between NG-SOC and its sister projects funded under the Digital Europe Programme (DIGITAL-ECCC-2022-CYBER-B-03) call - Capacity building of Security Operation Centres (DIGITAL-ECCC-2022-CYBER-B-03-SOC) topic. [2]

2.2 Exploitation Phases

The overall NG-SOC exploitation strategy, which is shown in Figure 1, consists of several components that play an important role in the overall NG-SOC exploitation. First is the NG-SOC consortium and its 3 types of partners, which are generally grouped in industry, academia, and research followed by the technologies and solutions comprising the building blocks of NG-SOC. These can be products, services, or knowledge, which are identified and described as Key Exploitable Results (KERs). These will be deployed in the 3 pilot sites.

Results and gained experiences make it be possible to further develop the core of the exploitation strategy. The exploitation strategy implements various activities within 3 phases: A, B and C, which are continuously performed over the duration of the project. All 3 exploitation phases are structured and planned according to the predefined meta-activities: pre-marketing activities, exploitation ramp-up and market penetration. Here, the main goal is to ensure a strong market position for NG-SOC innovative cybersecurity solutions and services while at the same time being aligned with the needs of the target exploitation groups. To this end, all exploitation actions are defined to ensure timely contributions of the project partners and efficient use of resources.

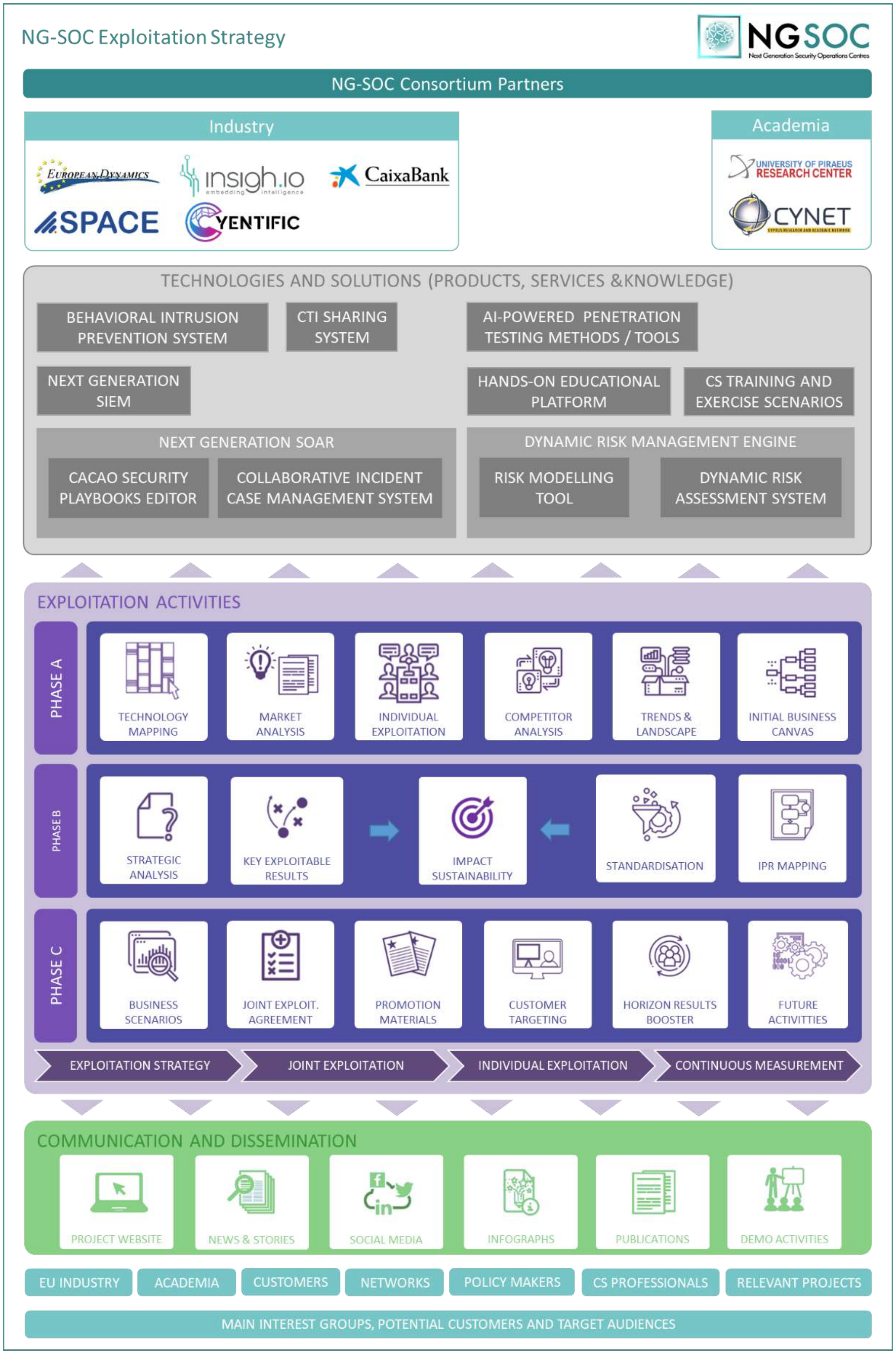


Figure 1. NG-SOC Exploitation strategy overview

T7.2 is interconnected as a part of the overall NG-SOC exploitation framework, which will be carried out in three main exploitation phases. These are structured and planned according to market analysis, business planning, exploitation actions and continuous monitoring. The 3 phases are:

Phase A | Initial pre-marketing activities: technology mapping, market analysis and trends – (that will be described in D7.2 and D7.3) will help us understand the cybersecurity market landscape, current suppliers, and available products and services, trends which could have a high impact, competitors, relevant stakeholders etc. Based on these inputs, initial business models will be proposed, which will be further elaborated as the NG-SOC platform matures.

Phase B | Exploitation ramp-up: identifying values, strengths, competencies, and potential issues – as the project progresses, the results and the general direction will become clearer. As such, the activities include strategic analysis, identification of key exploitable results, and mapping of interoperability, standards and IPR. The main aim is to ensure a strong market position of NG-SOC innovative cybersecurity solutions and services, while at the same time being aligned with the needs of the target exploitation groups. Here, exploitation actions aim to identify the key exploitable assets of the NG-SOC project, internal and external exploitation factors (SWOT), and macro-environmental challenges (PESTLE), as well as to understand the competition (Porter's 5 Forces). Furthermore, all partners will elaborate and update their individual exploitation plans as well as elaborate the pre-commercial agreements among partners through background/foreground technology identification.

Phase C | Market penetration: business scenarios, joint exploitation, promotion and beyond - all the activities planned for this phase are preliminary as they relate to the project's final results. Depending on the progress of the project and how it matures, the exploitation strategy will be updated accordingly. Currently, Phase C includes the following activities: definition of potential business scenarios, business model canvas (updated), customer targeting via brochures, digital marketing materials and online promotion, financial plan and pricing models, licensing and IPR, joint exploitation activities, plan for follow up projects, etc. In parallel, the NG-SOC project will fully embrace the Horizon Results Booster initiative to maximize its exploitation potential.

Some information needed for a complete exploitation strategy was still not available during this early project period. Therefore, the initial strategy will be developed at latter stages (M18, M36), where planned partner exploitation activities will be intensified when possible and all interested consortium partners will be involved in the definition of a joint business plan.

Here, exploitation actions need to identify the main exploitable assets of the NG-SOC project which will be also used to facilitate and guide targeted communication and dissemination activities. By utilising the established communication channels (project website, news, social media, infographics, publications, demos, etc.), it will be easier to reach the main interest groups, potential customers, and target audiences (EU industry, academia, industry customers, cybersecurity professionals and experts, policy makers, networks and relevant projects and initiatives). Results of all phases and individual activities will be reported within various iterations of deliverables: *Business plan - M18* and *Business plan - M36.*

3 Key Exploitable Results

During the first project phase, the consortium carried out a preliminary identification of the Key Exploitable Results (KERs), as shown in Table 1. The generated list represents the most innovative results which have been achieved or will be delivered by the end of the project. Their exploitation potential is expected to have either commercial, social, or scientific value. Here, exploitable results can include equipment, hardware, processes, products, services, knowledge & IP, and other forms of knowledge (publications, patents, etc.) [4]. In NG-SOC, the following types of results have been outlined:

- **Software/Application**: Innovative IT solutions that are integrated into the NG-SOC architecture and that enable either unique, ground-breaking, or beneficial functionalities.
- **Service**: The envisioned capacity-focused, AI-enhanced SOC service together with the dedicated training sessions and educational programmes in digital infrastructure security represent unique services focusing on increasing the level of automation in SOC/CSIRT operations while delivering multidisciplinary and realistic training and knowledge testing in multiple domains.
- **Knowledge/Use case**: provides a better understanding or otherwise not readily available information about specific use case scenarios within the banking, energy, and educational domains, which will, in turn, help to create a more realistic and useful SOC service and hands-on training.

Table 1. NG-SOC Key Exploitable Results (KERs)

No	KER	Type	Partner(s)
1.	Behavioural Intrusion Prevention System	Software / Application	SPH
2.	AI-Powered Penetration Testing Methods and Tools	Software / Application / Service	EDGR, SPH
3.	CTI Sharing System	Software / Application	EDGR, CYEN
4.	Dynamic Risk Management Engine	Software / Application	UPRC, INS, EDGR
5.	Next Generation SIEM	Software / Application	SPH
6.	Next Generation SOAR	Software / Application	EDGR, CYEN
7.	Collaborative Incident Case Management System	Software / Application	CYEN
8.	Hands-on Educational Platform	Software / Application	EDGR, ED
9.	Cybersecurity Training and Exercise Scenarios	Service	ED, UPRC
10.	Sectorial Training Programs	Knowledge / Use cases	CXB, CYNET-CSIRT

Next step is to carry out the characterisation of the identified results using a systematic approach. Here, the characterisation focuses on the assessment of the results' technological maturity (in their current phase) using the Technology Readiness Level (TRL) framework, as shown in Table 2. In any case, after the end of the project, the identified results will potentially need further development, refinement, optimisation, or investment before they can be fully exploited commercially. Furthermore, several additional parameters are used to define the results in context of innovation, uniqueness, market potential, IPR measures:

- **Description**: Brief description about the result.
- **What problems are solved**: What problems does the result solve? / Why has this result been achieved in NG-SOC?
- **Innovativeness/new approach**: What is the new element/approach/innovation of the result that distinguishes it from the state of the art?
- **Unique selling point**: In what way is the solution better (faster, cheaper, more reliable, more efficient, with less undesired effects)?
- **Competitors (solutions)**: Who are the main competitors of the result?
- **Target users / customers**: Who will potentially use the result?
- **Benefits for users / customers**: What benefit will the result bring to end users? Why should the end users invest in or adopt the result?
- **TRL level**: Estimation of the result's technology maturity.
- **Main technical challenge(s)**: What are the main technical challenges which need to be or were solved?
- **Legal / ethical requirements**: Legal, normative, or ethical requirements (Is there a need for authorisations, compliance to standards, norms, etc.?).
- **Involved partners**: Who are the principal partners involved in the delivery of the result?
- **IPR protection**: Does the result need to be protected? How? When?

Table 2. *Overview of TRL levels and their descriptions [5]*

TRL	Description
TRL 1.	basic principles observed
TRL 2.	technology concept formulated
TRL 3.	experimental proof of concept
TRL 4.	technology validated in lab
TRL 5.	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6.	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7.	system prototype demonstration in operational environment
TRL 8.	system complete and qualified
TRL 9.	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

3.1 Behavioural Intrusion Prevention System

KER 1: Behavioural Intrusion Prevention System	
Description	The BIPS aims to enhance the security posture of the organization by proactively detecting and mitigating potential threats in real-time. It implements data engineering processes on system logs, including collection, pre-processing, as well as pattern recognition and anomaly detection. The latter are realised via AI algorithms trained using supervised and unsupervised models. The outputs of this AI-based component will generate alerts to the SOC analyst, providing details on the anomaly's nature, impact, and mitigation strategies. Those alerts will be used to guide incident response processes, including system isolation, anomaly investigation, and future incident prevention. Finally, continuous learning of BIPS will be implemented by iteratively refining AI models based on new data and incident responses towards improving accuracy and effectiveness in threat detection.
What problem(s) are solved	Overall, the BIPS component plays a crucial role in mitigating cybersecurity risks, protecting sensitive data, and safeguarding the organization's assets and reputation. Particularly, the following problems are expected to be solved: **Early Insider Threat Detection**: By continuously monitoring network and system behaviour of in-house assets and actors in real-time, the BIPS can identify anomalies and potential threats before they escalate into full-blown security breaches. This approach helps prevent unauthorized access, data breaches, and other cyberattacks. **Enhanced Accuracy**: Using AI-driven algorithms and continuous learning techniques, the BIPS can accurately detect both known and novel threats. By extracting key features from data and training models, the system can distinguish between normal behaviour and suspicious activities, reducing false positives and negatives. **Timely Alerting**: The generation of comprehensive alerts upon detection of anomalies enables security analysts to respond promptly to potential security incidents. These alerts provide detailed information about the nature of the threat, its potential impact, and recommended mitigation strategies, facilitating rapid decision-making and incident response. **Incident Response Improvement**: By guiding incident response processes, including system isolation, anomaly investigation, and future incident prevention, the BIPS component helps streamline the organization's response to security incidents. This leads to quicker resolution times, reduced impact on operations, and improved overall security posture. **Adaptability to Evolving Threats**: Continuous learning mechanisms allow the IPS to adapt and evolve alongside emerging cybersecurity threats. By iteratively refining AI models based on new data and incident responses, the system can stay ahead of evolving attack techniques and maintain its effectiveness in threat detection over time.
Innovativeness / new approach	A transparent and explainable AI framework for intrusion prevention, analysing the systems' behaviour tailored to the organisations' business activity.
Unique selling point	The AI-enabled behavioural threat detection will timely capture abnormal patterns within the organisation's digital infrastructure, match them with known vulnerabilities and propose tailor-made remedies. In this regard, particularly insider threats will be prevented and/or mitigated.

Competitors (solutions)	In terms of relevant commercial solutions, there are numerous vendors offering products and services in the field of intrusion prevention systems, many of which incorporate behavioural analysis and AI-driven techniques. Some well-known commercial solutions include Cisco Firepower, Palo Alto Networks' Next-Generation Firewall with Threat Prevention, Check Point Intrusion Prevention System, and IBM QRadar. These solutions typically offer a range of features, including real-time monitoring, threat detection, alerting, and incident response capabilities, tailored to meet the security needs of organizations across various industries.
Target users / customers	**SOCs** to proactively identify vulnerabilities before they are exploited by attackers. **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts.
Benefits for users / customers	Higher efficiency for SOC teams and security analysts in terms of events and issues handling; increased visibility of threat landscape; fortification against insider threats
TRL level (1-9)	TRL 4
Main technical challenge(s)	Model training, data availability.

3.2 AI-Powered Penetration Testing Methods and Tools

KER 2: AI-powered Penetration Testing Methods and Tools	
Description	The AI-powered penetration testing methods and tools serve two purposes: a) assessing the robustness of the behavioural intrusion prevention system using comprehensive, realistic threat simulations and b) streamlining the workflow, thereby reducing human intervention, time and costs while increasing test frequency and entry point coverage, by automating critical aspects of penetration testing.
What problem(s) are solved	It automates repetitive tasks and augments human capabilities, freeing up pen testers to concentrate on higher-level strategic analysis and decision-making, allowing for faster and more scalable security assessments. It prioritizes vulnerabilities based on their potential impact, optimizing testing efficiency. Simulates and replicates advanced attack techniques, providing a more realistic assessment of an organization's security defences. Provides insights back into the intrusion prevention system for continuous learning and improvement.
Innovativeness / new approach	Use of intelligent algorithms to find and analyse the context of a vulnerability, such as its exploitability and potential impact on the system, enabling to prioritize the most critical risks and optimize the testing process, in a way that traditional methods simply can't. Shifting from a rule-based approach to a more dynamic and intelligent one, by analysing vast amounts of security data and discovering complex patterns that might indicate vulnerabilities, zero-day exploits and custom malware that traditional scanners would miss.

Unique selling point	It introduces automation, intelligent analysis, and continuous adaptation, significantly enhancing the effectiveness and efficiency of cybersecurity efforts. By leveraging machine intelligence we can uncover hidden weaknesses, adapt to new threats, and optimize the testing process for a more secure future. It's a proactive approach that anticipates and adapts to the evolving threat landscape.
Competitors (solutions)	Numerous self-hosted platforms that can potentially provide a similar solution like Deepwatch Arc, PenTest (by Rapid7), Nixeus, BreachLock (by Cymulate), AttackIQ, Cymulate. However, they are not easy to be extended. Research groups that incorporate AI in penetration testing and vulnerability identification.
Target users / customers	The module can be used by a) **Penetration Testers** to automate tedious tasks, allowing them to focus on crafting complex attacks, analysing results, and applying their critical thinking and social engineering skills; b) **Security Teams** to gain a more comprehensive vulnerability assessment, identify sophisticated threats, and prioritize risks, allowing them to make informed decisions about resource allocation and remediation efforts; c) **SOCs** to proactively identify vulnerabilities before they are exploited by attackers, giving them a head start in shoring up defences; d) **Compliance and Risk Management Teams** to ensure compliance by identifying vulnerabilities that could lead to data breaches; e) **DevOps Teams** to identify and address security vulnerabilities early in the development lifecycle, resulting in time and resources reduction compared to fixing vulnerabilities discovered later in the production stage; f) **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.
Benefits for users / customers	AI-powered penetration testing streamlines the testing process, enhances vulnerability detection, and equips teams with the knowledge to prioritize risks and make data-driven security decisions. Furthermore, it empowers users and customers with a faster, more effective way to identify and address security weaknesses. It's a proactive approach that helps organizations stay ahead of evolving threats and strengthen their overall cybersecurity posture.
TRL level (1-9)	TRL-3
Main technical challenge(s)	AI can generate both false positives (flagging non-existent vulnerabilities) and false negatives (missing real vulnerabilities), resulting in wasting time and resources investigating non-issues or leaving critical gaps in security. Fine-tuning AI models and incorporating human expertise are crucial to minimize these errors. Additionally, biased or incomplete data sets used to train the models can lead to biased results, potentially overlooking certain attack vectors or vulnerabilities specific to certain systems. Ensuring high-quality, unbiased training data is essential. Finally, ensuring seamless integration, interoperability and data sharing with existing security infrastructure (such as SIEM or IDPS) and workflows is essential for maximizing the effectiveness of AI-driven security assessments.

3.3 CTI Sharing System

KER 3: CTI Sharing System	
Description	The CTI Sharing System serves two purposes: a) collecting, storing and sharing of structured Cyber Threat Intelligence (CTI), including indicators of compromise (IoCs) and contextual information related to cybersecurity incidents, campaigns, and intrusion sets and b) managing, correlating, visualizing and analysing CTI in a structured and collaborative manner, enhancing the understanding of cyber threats.
What problem(s) are solved	The CTI Sharing System address a common problem in the cybersecurity field: limited visibility and information sharing regarding cyber threats, lack of efficient management and sharing of CTI, lack of a standardized and centralized platform for collaborative threat analysis in the dynamic and complex field of cybersecurity.
Innovativeness / new approach	This module uses and enhances: a) the MISP sharing platform [9], a platform that has several build-in functionalities that can ease the collection, storage, correlation, and sharing of cyber security indicators and threats and b) the OpenCTI threat intelligence management platform [11], a platform designed to help organizations manage their intelligence data and collaborate on threat analysis. By integrating MISP and OpenCTI in a CTI sharing system reflects innovativeness through open collaboration, adherence to standards, centralized management, scalability, automation, community involvement, advanced visualization, and a commitment to continuous development. Furthermore, the module introduces new advanced correlation techniques through automated workflows that analyse data from MISP (focusing on IoCs and IoAs) and OpenCTI (focusing on TTPs) to identify connections between threats and attacker campaigns.
Unique selling point	This solution advances MISP and OpenCTI by introducing new advanced correlation techniques and new data visualizations by combining MISP's rich graph layouts with OpenCTI's entity relationship views to provide a more comprehensive picture of the threat landscape.
Competitors (solutions)	Other CTI gathering tools, such as MISP with its default feeds [14], SpiderFoot [15] that supports the collection of information from various sources including the Dark Web, commercial thread intelligence feeds from different cybersecurity companies, and more. However, our module supports the automatic collection and the extraction of CTI from additional sources compared to our competitors. Other CTI sharing platforms, either open-source or commercial. However, they do not utilise advanced correlation techniques.
Target users / customers	The module can be used by a) **SOC teams** to share and analyse threat indicators (IOCs and IoAs) and attacker Tactics, Techniques, and Procedures (TTPs) to proactively identify and respond to threats; b) **CTI Teams** to gain a comprehensive understanding of the threat landscape (by monitoring and extracting CTI from multiple sources) and produce actionable intelligence; c) **Information Sharing Communities** (ISCs) to facilitate collaboration and information exchange within these communities; d) **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts; e) **Managed Security Service Providers** (MSSPs) to cater to the specific needs of their diverse client base; f) **Security Researchers** to identify new threats and develop better defensive strategies; g) **Law Enforcement Agencies** (LEAs) to

	share and analyse threat intelligence related to cybercrime investigations. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.
Benefits for users / customers	By combining data from MISP (IoCs, IoAs) and OpenCTI (TTPs) users can identify connections between indicators and attacker tactics, providing them with a more comprehensive picture of potential threats (broader threat visibility). Furthermore, by automating data ingestion, enrichment, and correlation we can streamline (by highlighting connections) and automate some aspects of threat analysis reducing manual effort for security analysts while enabling them to focus on more strategic tasks. OpenCTI's focus on standardized data formats ensures seamless information sharing between users and organizations. Finally, enhanced threat visibility allows users to identify potential threats before they cause harm, enabling proactive threat hunting.
TRL level (1-9)	TRL-7
Main technical challenge(s)	Since MISP and OpenCTI have different data models, robust data integration pipelines must be developed to ingest, normalize, and harmonize data from both sources, ensuring consistent analysis. Additionally, since information sharing within CTI communities can be susceptible to inaccurate or misleading data, mechanisms to assess data quality and trust must be implemented (such as reputation scoring or manual review processes) before feeding it into analysis workflows.

3.4 Dynamic Risk Management Engine

KER 4: Dynamic Risk Management Engine	
Description	The Dynamic Risk Management Engine (DRME) identifies, analyses and assigns threats and vulnerabilities to the infrastructure's assets, aiming to minimise risks with minimal intervention by risk analysts. To accomplish that, DRME will: a) Utilize mechanisms for automatic asset identification; b) Use an ontology-based knowledge representation to depict the various system services and the assets associated with these services, distinguishing them to composite and basic assets; c) Utilise ML approaches to accurately and automatically correlate identified threats with the Common Weakness Enumeration (CWE) list and other high-level vulnerabilities; d) Help analysts adopt controls based on NIST's Security and Privacy Controls for Information Systems and Organizations (SP 800-53), CIS Critical Security Controls, and technical countermeasures based on MITRE ATT&CK and MITRE D3FEND and automatically correlate them with the threats and vulnerabilities associated with the ontology's assets; e) Leverage stochastic approaches and existing relationships between CWEs and CVEs in conjunction with their scoring systems (CWSS and CVSS) towards reliable automated risk predictions regarding the identified cascading threats on assets and their interconnections.
What problem(s) are solved	DRME addresses the issue of cascading threats, over or under estimation of risks for complicated cyberphysical systems due to insufficient threat modelling, and static risk assessments. Introduces an accurate calculation of the composite risk value for complicated cyberphysical systems with correlated and cascading threats; Use of third-party sources and AI tools for zero-day attacks identification and accurate calculation of

	threat occurrence probabilities; Interconnection with other threat intelligence engines and SIEMs; DRME is adaptable to any sector.
Innovativeness / new approach	DRME proposes hierarchical modelling of multi-layered cyberphysical systems that include multiple assets and users; a new cascading threat and risk estimation engine; new AI-based techniques for risk value recalculation and automated asset identification; a new ontology for risk and threat modelling.
Unique selling point	Accurate, detailed, and dynamic risk modelling and assessment for complicated, multi-asset, multi-layered systems with significantly reduced requirement for deep technical system knowledge by the risk analysts.
Competitors (solutions)	Many risk assessment and analysis solutions exist; however, they generally lack intelligent or dynamic features, and/or they are not provided as open source. The list of solutions includes the following: Riskrecon, UpGuard, Security Scorecard, NormShield, BitSight, Microsoft Security Assessment Tool 4.0, CounterMeasures, EAR / PILAR, eBIOS Risk Manager, MEHARI Expert, Modulo Risk Manager™, Risk Management Studio, SimpleRisk, CORAS, Verinice ISMS, Practical Threat Analysis, Cyber Security Evaluation Tool (CSET), ZenGRC, CIS RAM, vsRisk, OneTrust GRC, MONARC.
Target users / customers	The module can be used by a) **SOC teams** for various technological domains monitoring cyberphysical systems; b) **CTI Teams**; c) **Information Sharing Communities**; d) **Incident Response Teams**; e) **Managed Security Service Providers**; f) **Security Researchers**. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.
Benefits for users / customers	DRME is an automated tool that can be exploited by users without deep technical knowledge of the underlying system. It provides accurate risk score calculations considering cascading risks, security controls and risks, and interconnects with third party feeds and applications to ensure dynamic reconfiguration. Moreover, DRME will be open source.
TRL level (1-9)	TRL-7
Main technical challenge(s)	The interfacing and interconnection with the SIEM and threat intelligence engines for the recalculation of threat occurrence probabilities and mainly for the identification of zero-day attacks. The integration of the automated asset identification procedures since they may be considered invasive from the perspective of a security officer. The integration with the overall NG-SOC solution.

3.5 Next Generation SIEM

KER 5: Next Generation SIEM	
Description	This KER will implement novel functionalities that are poorly or not at all implemented in current SIEM solutions. The next generation SIEM will offer automation in data collection from different sources within the digital infrastructure. Moreover, data aggregation, correlation and categorisation capabilities are included. Finally, cyber threats' related operations will be implemented, including detection and investigation.
What problem(s) are solved	**Advanced Threat Detection:** Traditional SIEM systems may struggle to detect sophisticated and evolving cyber threats. Next-generation SIEM will leverage advanced analytics, machine learning, and behavioural analysis to identify anomalies and potential security incidents more effectively. **Increased Data Volume and Variety:** With the proliferation of digital assets and the rise of cloud computing, organizations are generating vast amounts of diverse data. Next-generation SIEM will handle large volumes of structured and unstructured data from various sources, including logs, network traffic, endpoint telemetry, OSINT data on cyber threats and vulnerabilities. **Real-Time Monitoring and Response:** Traditional SIEMs often provide retrospective analysis of security events, which may not be sufficient for detecting and responding to threats in real-time. Next-generation SIEM will offer real-time monitoring capabilities, enabling organizations to detect and respond to security incidents promptly. **Integration with Threat Intelligence:** Next-generation SIEM will integrate with external threat intelligence feeds, via CTI Sharing System, to enrich security event data. By correlating internal security events with external threat intelligence, Next Generation SIEM can identify indicators of compromise and emerging threats more effectively. **User and Entity Behaviour Analytics (UEBA):** Next-generation SIEM will incorporate UEBA capabilities to analyse the behaviour of users and entities within the organization's network. By identifying deviations from normal behaviour patterns, these systems can detect insider threats, compromised accounts, and other malicious activities. This is also associated with the Behavioural Intrusion Prevention System KER. **Automation and Orchestration:** By automating repetitive tasks and orchestrating response actions, organizations can improve the efficiency and effectiveness of their security operations. **Compliance and Reporting:** Next-generation SIEM will provide advanced reporting and compliance features to help organizations meet regulatory requirements and industry standards. This component can generate customized reports, conduct forensic analysis, and demonstrate compliance with security policies and regulations.
Innovativeness / new approach	The main innovative aspects of the NG-SOC Next Gen SIEM are its integrations with BIPS and CTI Sharing System. Those integrations offer **advanced threat hunting and investigation tools** that empower security analysts to proactively search for and investigate potential security threats. These tools leverage advanced search capabilities, visualization techniques, and threat intelligence integrations to streamline the threat hunting process. It also improves **UEBA capabilities** by leveraging advanced machine learning algorithms to analyse user and entity behaviour patterns. This will enable more accurate detection of insider threats, compromised accounts, and other anomalous

	activities. Moreover, autonomous response mechanisms help organizations respond to threats more rapidly and efficiently, reducing the impact of security breaches. Finally, **continuous improvement through self-learning** improves threat detection capabilities, analysing feedback from security incidents, user interactions, and threat intelligence feeds to refine their algorithms and adapt to evolving threats over time.
Unique selling point	The ability to provide advanced threat detection and response capabilities, leveraging advanced analytics, machine learning, behavioural analysis, real-time monitoring, integration with threat intelligence, scalability, flexibility, automation, orchestration, and compliance reporting features. These capabilities help organizations enhance their security posture and effectively defend against a wide range of cyber threats.
Competitors (solutions)	Croudstrike's Falcon Next Gen SIEM, Stellar Cyber, Gurucul SIEM,
Target users / customers	**SOCs** to proactively identify vulnerabilities before they are exploited by attackers. **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts.
Benefits for users / customers	Higher efficiency for SOC teams and security analysts in terms of events and issues handling; increased visibility of threat landscape; fortification against insider threats
TRL level (1-9)	TRL 4
Main technical challenge(s)	Interfacing and integration with BIPS; data availability so that the automation features are properly validated.

3.6 Next Generation SOAR

KER 6: Next Generation SOAR	
Description	The next generation SOAR comprises standards based interoperable and modular orchestration and automation components to assist and enhance cybersecurity operations and different operational roles. Our SOAR is based on the CACAO v2 playbooks standard. An MVP version of the solution will be open sourced whereas NG-SOC will maintain and commercialise a version with enhanced features such as the sharing component, the Generative AI based import module, and the knowledge management system which allows establishing and monitoring playbook oriented KPIs and searching, indexing, and filtering capabilities.
What problem(s) are solved	Currently SOAR solutions are utilizing proprietary formats for playbooks making them non -shareable and -interoperable across organizational boundaries and solutions. The NG-SOC SOAR allows designing and creating CACAO playbooks in a no-code manner and provides an execution engine in support of automation and orchestration. In addition, our solution will introduce a CACAO-based Generative AI component for importing playbooks traditionally documented in human natural language or graphical non-machine-readable formats, allowing defenders to seamlessly upgrade their playbooks capability while providing a clear path to automation. In addition, defenders will be able to exchange

	playbooks and create trusted and open sharing communities; a capability highly desired by the cybersecurity community but not yet materialised.
Innovativeness / new approach	Full CACAO-based (distributed) SOAR solution providing both an editor for designing and creating playbooks and an execution engine. A playbooks knowledge management system for advanced analytics, tracking KPIs, indexing, filtering, and searching based on a rich set of metadata. Sharing playbooks capability and integration with CTI. Generative-AI-based CACAO transformer to automatically transform playbooks to CACAO from unstructured sources.
Unique selling point	The cybersecurity industry will swift to standards-based interoperable SOAR since it has been researched and to a certain extent demonstrated through PoCs that they can offer certain benefits compared to existing siloed and proprietary approaches. Benefits include the ability to design and exchange playbooks across organizational boundaries and solutions and coupling them with CTI for threat informed defence. Ultimately, NG-SOC is entering this marker at a very early stage and has the know-how since consortium partners have been actively involved in developing the CACAO technical standard and demonstrated very early-stage implementations.
Competitors (solutions)	Currently, the industry is developing to a certain extent CACAO compliant solutions but none of the "competitors" provide the full set of features that described above. In fact, the CACAO Roaster[1] that we have open sourced is the first open source and known solution for creating CACAO playbooks to date.
Target users / customers	SOCs, MSSPs, and most operational cybersecurity roles, including, threat hunters, red teams, and IR, compliance, and vulnerability management teams.
Benefits for users / customers	Enhanced cybersecurity by exchanging defensive tradecraft in addition to CTI. Enhanced cybersecurity by enabling orchestration and automation. Fully interoperable product that can seamlessly integrate with any other solution of interest. Efficiency in converting IR processes and proprietary playbooks to machine readable CACAO playbooks. A knowledge management playbooks system to increase the efficiency and effectiveness on the use of playbooks.
TRL level (1-9)	TRL 4
Main technical challenge(s)	Complying fully with the CACAO specification and complexity in integrating with the Collaborative Incident Case Management System which is also based on a standards-based approach.

[1] https://github.com/opencybersecurityalliance/cacao-roaster

3.7 Collaborative Incident Case Management System

KER 7: Cybersecurity Training and Exercise Scenarios	
Description	The CICMS is a standards-based collaborative incident case management system based on the incident core extension[2] for STIX focusing on providing collaboration options for incident resolution across defenders, teams, and organizations, as well as the ability to exchange incident information and connecting it with CTI using common standardized formats.
What problem(s) are solved	✓ Addresses non-interoperability across systems and components regarding incident representation. ✓ Enables sharing incidents and relevant CTI with different teams and organisations. ✓ Provides the required capacity for teams from different organizations to collaborate in the context of incident resolution and requests for information and takedown.
Innovativeness / new approach	CICMS is the first incident case management system that can interact seamlessly with other systems and components that make use of STIX and the incident core extension. In addition, due to its interoperable nature it can exchange information with other incident case management systems or CTI platforms that make use of the extension and/or STIX. CICMS will also incorporate an API in support of automation where SOAR systems can interact with it.
Unique selling point	The CICMS will be one of the first standards-based incident case management systems entering the global market providing capacities for advanced collaboration, and integration with systems (e.g., CTI platforms) that utilize the STIX standard. In addition, its API will be tailored to the needs of SOAR systems allowing for a seamless integration within any heterogeneous defence environment.
Competitors (solutions)	Existing incident case management systems providers and open-source tools like The Hive and DFIR-IRIS.
Target users / customers	SOCs and MSSPs
Benefits for users / customers	Benefiting by enabling collective defence; in this context the ability of defenders within and across organizational boundaries to collaborate and create clusters for incident response. The exchange of incident information using a standardized format in the same way defenders exchange CTI. Seamless integration with systems that utilize STIX as their underlying CTI representation format. Integration with SOAR solutions via a tailored API.

[2] https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/incident-ef7

Readiness level	TRL 2
Main challenge(s)	Complying fully with the STIX 2.1 incident core extension and complexity in integrating with CTI platforms like OpenCTI in a distributed manner.

3.8 Hands-on Educational Platform

KER 8: Hands-on Educational Platform	
Description	A hands-on educational platform that will host multidisciplinary and realistic training sessions and educational programmes in cybersecurity across multiple domains, based on the merged principles of Massive Open Online Course (MOOC) tools and explicit use of cyber ranges as a regular hands-on learning method.
What problem(s) are solved	By integrating cyber ranges and hands-on learning methods, NG-SOC provides immersive experiences in realistic training environments, bridging the skills gap and preparing individuals for real-world cybersecurity challenges. Offering a multidisciplinary curriculum, flexible self-paced learning, and interactive assessments, the platform promotes active, experiential learning while democratizing access to high-quality, practical cybersecurity education, empowering learners from diverse backgrounds to acquire essential cybersecurity skills, meet industry demands, and contribute to global cybersecurity resilience.
Innovativeness / new approach	While both MOOCs and cyber ranges exist independently, the platform integrates them and provides a holistic approach to cybersecurity education. This allows learners to gain theoretical knowledge through MOOC modules and then immediately apply it through practical exercises in the cyber range. This cohesive approach reinforces learning and enhances skill development. By integrating collaborative learning features, flexible self-paced learning options, and offering content and exercises across multiple domains, it promotes skill development, fosters community engagement, and democratizes access to quality training resources. This innovative approach not only addresses current challenges in cybersecurity education but also anticipates the evolving needs of the industry, preparing learners to navigate complex cyber threats and contribute effectively to cybersecurity initiatives worldwide.
Unique selling point	The platform's unique selling point lies in its fusion of immersive, hands-on learning experiences with comprehensive, multidisciplinary cybersecurity education. By integrating cyber ranges and practical exercises into its curriculum, the platform offers learners the opportunity to engage in realistic simulated scenarios, enabling them to develop practical skills and problem-solving abilities crucial for success in the cybersecurity field. Additionally, its flexible self-paced learning options, collaborative features, and open-source accessibility not only addresses the skills gap in cybersecurity but also empowers individuals from diverse backgrounds to pursue careers in this rapidly evolving industry.

Competitors (solutions)	Traditional academic programs, online course providers like Coursera, edX and Udemy, cybersecurity training firms such as SANS Institute, dedicated cyber range providers. While traditional academic programs offer structured education, they may lack hands-on experiences. Online course providers offer convenience but may not provide the required depth of practical learning. Cybersecurity training firms offer comprehensive programs but at a higher cost. Dedicated cyber range providers focus on immersive experiences but may lack educational content.
Target users / customers	The platform targets a diverse audience including aspiring and current cybersecurity professionals, IT professionals seeking career transitions, academics, educators, security enthusiasts, and organizations looking to enhance their cybersecurity capabilities.
Benefits for users / customers	It empowers users to gain a deeper understanding of cybersecurity, develop practical skills, and stay ahead of the curve in this ever-changing landscape. It offers a flexible, comprehensive, practical, and accessible learning experience that can benefit anyone interested in building a strong foundation in cybersecurity, enhancing their skills, and advancing their careers in this ever-growing field.
TRL level (1-9)	TRL-7
Main technical challenge(s)	Seamless integration of MOOC and Cyber Range Platforms, as currently they do not communicate.

3.9 Cybersecurity Training and Exercise Scenarios

KER 9: Cybersecurity Training and Exercise Scenarios	
Description	To develop the training framework aligned with the vision of NG-SOC - to provide an advanced, hands-on educational platform to guide conversations around cybersecurity workforce skills development that goes beyond policies.
What problem(s) are solved	✓ Understand organisational needs for cybersecurity training based on the merged principles of online education tools and cyber ranges. ✓ Identify training and learning objectives. ✓ Develop an innovative framework for training and evaluation.
Innovativeness / new approach	Offer an innovative training framework, incorporating characteristics such as multidisciplinary, varying levels of difficulty, different training modes, real-world attacks scenarios, individual and team skills.
Unique selling point	An innovative training framework with the abovementioned characteristics, tailored to identified training goals and objectives and delivered via different training delivery methods.
Competitors (solutions)	Existing cybersecurity training platforms
Target users / customers	✓ Beginner level for non-technical users (with no relevance to information Technology) who want to be aware of cybersecurity and the basic concepts behind this.

	✓ Intermediate and advanced level for professionals in a specific domain or experts who are not domain specific.
Benefits for users / customers	✓ Offering theoretic and hands-on offensive/defensive training. ✓ Complex cross-domain/hybrid scenarios jointly built with the IoT domain. ✓ The realistic and dynamic training and exercise scenarios enable cybersecurity professionals to rapidly adapt to the evolving threat landscape.
TRL level (1-9)	TRL 4
Main challenge(s)	Compete with existing cybersecurity training programmes with professional accreditation.

3.10 Sectorial Training Programs (CYNET-CSIRT)

KER 10: Sectorial Training Programs	
Description	Adaptive and proactive training programmes for research and education. More specifically the training program will incorporate: a) a comprehensive cyber security training plan focused on studying online materials, that covers various aspects of cyber security, assuming beginner to intermediate levels of knowledge, using a scenario-based approach to educate participants on identifying and mitigating phishing threats and b) hands-on training activities designed to enhance participants' skills in ethical hacking, in recognizing and defending against social engineering attacks, with a specific focus on phishing, in handling and mitigating a cybersecurity incident involving automated malware attacks, in developing and implementing effective incident handling and response procedures, and in handling an Advanced Persistent Threat (APT) incident.
What problem(s) are solved	Test participants' ability to recognize and respond to a variety of attacks in a controlled environment, fostering a proactive approach to cybersecurity and improving their ability to i) detect, analyse, and respond to social engineering threats and sophisticated cyberattacks, ii) utilize/leverage automation tools and incident response techniques to detect, contain, eradicate, and recover from an incident, iii) create, refine, and execute incident response plans to mitigate and recover from the incident. Enhance participants' skills in ethical hacking and improve their understanding of security vulnerabilities and countermeasures.
Innovativeness / new approach	Scalable architecture of mostly virtualized components, with some physical equipment for more realistic training experience. Question based training scenario. Proposed approach is scalable for very similar business (i.e., other research and education organisations) and based on best practise
Unique selling point	The unique selling point of the adaptive and proactive training program lies in its combination of theoretical and practical training, focusing on real-world scenarios and current threats. Through scenario-based learning and hands-on activities, learning becomes practical and engaging. Participants of varying expertise levels learn to identify and mitigate phishing threats, handle automated malware attacks, and respond effectively to Advanced Persistent Threats (APTs). The program's focus on proactive defence and comprehensive incident handling equips participants with the skills needed

	to anticipate and address cybersecurity challenges effectively, making it an invaluable resource for individuals and organizations seeking to enhance their cybersecurity posture.
Competitors (solutions)	Traditional cybersecurity courses offered by universities and online platforms. However, they often lack the adaptive learning element and focus heavily on theory without enough practical exercises. Moreover, the self-paced nature of MOOCs can lead to lower engagement and lack of hands-on activities. Expensive and time-consuming certification programs (like CompTIA Security+ or Certified Ethical Hacker (CEH)) that may prioritize theoretical knowledge over practical application. Affordable security awareness training platforms able to deliver regular awareness training updates, however, focusing primarily on basic awareness, and lacking in-depth training on specific topics like ethical hacking or incident response. Vendor-specific training programs that although beneficial for in-depth knowledge of a specific platform/solution, they lack broader applicability.
Target users / customers	Overall, the program targets a diverse range of users, including individuals seeking to build a strong foundation in cybersecurity, enhance their existing skillset, or gain practical knowledge for their specific roles, professionals advancing their careers, students preparing for future roles, organizations strengthening their defences, and security teams improving their capabilities.
Benefits for users / customers	The cybersecurity training program offers a comprehensive and adaptable approach to educating users at all skill levels, providing practical skills development and theoretical knowledge across various cybersecurity domains. Participants benefit from a tailored learning path, gaining expertise in identifying and mitigating real-world threats such as phishing attacks and malware incidents. This program not only enhances individual career prospects but also strengthens organizational security postures, fostering a culture of cybersecurity awareness and readiness. With its cost-effective and accessible online format, users receive expert guidance and support while enjoying the flexibility to learn at their own pace. Overall, the program empowers users with the skills and resources needed to navigate the evolving cybersecurity landscape effectively, making it a valuable investment for both personal and professional growth.
TRL level (1-9)	TRL 4
Main challenge(s)	Complexity of the subject matter, technical requirements for hands-on activities, maintaining participant engagement and retention, addressing skill level disparities among users, addressing limited time or resources of busy professionals, evaluating progress accurately, resource constraints, staying adaptable to emerging threats and attack methods. Overcoming these challenges requires continual updates to content, ensuring accessibility to necessary resources, fostering engagement through innovative methods, and maintaining flexibility to accommodate diverse skill levels and evolving cybersecurity landscapes.

4 Individual Exploitation Plans

This section presents the initial individual exploitation plans of all consortium partners. As the project progresses, partners could potentially identify different exploitation opportunities and goals. As such, this reporting activity will also be repeated for D7.2 *Business plan - M18* and D7.3 *Business plan – M36,* where only significant changes with partner's individual exploitation will be incorporated and described. Individual exploitation plans include results that are going to be exploited by partners and which market sector and customer segments they are going to target. Moreover, preliminary plans for exploitation channels, expected sales, and current achieved exploitation goals are presented. To assist the partners with the drafting of their individual exploitation plans, the following questions were provided as a guideline:

- **Results to exploit**: Which aspects (technology, services, knowledge, experience, know-how, network, etc.) of NG-SOC do you plan to exploit, and for what purpose?
- **Market Sectors**: Are you / do you plan to collaborate with any local, national, EU, or international sectors? Which stakeholders (research, industry, academia, authorities, decision-makers, etc.) are you connected with? How many people can potentially be reached?
- **Channels/Actions**: Which channels and actions will you use to exploit NG-SOC results?
- **Expected Sales**: How is NG-SOC going to provide an added value for your organisation? (This can include financial gains, gained know-how, development portfolio, widen networks, etc.)

By following the guidelines and answering the proposed questions, the consortium partners created the basis for setting up their exploitation plans of NG-SOC outputs, as identified in this early stage of the project. Each partner defined the major exploitable items and outlined the appropriate business strategy, as shown in the following sections.

4.1 EUROPEAN DYNAMICS LUXEMBOURG SA (01 ED)

Results to exploit: European Dynamics will further exploit: a) the CTI sharing system that is built on top of MISP and OpenCTI, b) the Next generation SOAR, c) the developed training programs and exercises, and d) the research outcomes generated during the development, improvement, and optimisation of the above systems. ED will be able to provide state-of-the-art international professional training courses (either jointly with other partners or individually) on cybersecurity or other emerging aspects. ED will also consider exploiting aspects of the developed NG-SOC tools and technologies, such as reusing the acquired know-how in other commercial and research projects. In this framework, ED will explore possibilities for cooperation with new partnerships at a national, regional, and international level.

Market Sectors: NG-SOC tools may find applications in academia, industry stakeholders, law enforcement agencies, European Union agencies, or public organisations where we mainly provide services, or other leading experts in the field of cyber-security technologies. ED will explore individually but also jointly with other project partners and external experts or national authorities the possibility of establishing: a) national, regional, or sectoral SOCs, within and across EU member states that can actively communicate, cooperate, share information, and respond to cyber threats effectively and b) training courses and educational programmes for professionals that are active in the field of cybersecurity.

Channels/Actions: ED will exploit the results of NG-SOC by enlarging its products and services with genuinely needed solutions for cyber security. ED will exploit the project results in three ways: a) will enlarge its technical know-how and services within the cyber security sector with new products and services that are complementary to its own, b) will obtain new and innovative as well as competitive services that can reach public organisations where ED mainly provides services, and c) will expand its alliances with other global players of the consortium in the cyber security market.

Expected Sales: Increased revenues based on gained know-how and strategic alliances with other NG-SOC partners, which will allow us to expand our cyber-security services portfolio.

4.2 INSIGHIO IKE (02 INS)

Results to exploit: INS will pursue the exploitation of the Dynamic Risk Management Engine (DRME), which is co-developed with UPRC and integrated with ED solutions. The three partners will prepare, agree on, and follow a collaboration agreement for the joint exploitation of the developed tools, while special agreements with NG-SOC partners may be drafted in case of integration of tools and functions from other NG-SOC systems. Moreover, INS is eager to explore the utilization of the developed tools in its systems and its IoT-related use cases/products for proofing and securing their cyber physical system.

Market Sectors: As a company, INS is developing IoT, communications, and automation solutions for various verticals, namely: vehicular communications and connected/autonomous vehicles, industrial automation and robotics, precision agriculture, emergency response and disaster relief, smart cities, smart grids, and more. As a tool, DRME is vertical agnostic and is adaptable to any sector, medium, or large company. Moreover, the solution is usable and exploitable by academia (for research and innovation), authorities and law enforcement agencies, European Union agencies or public organisations, or other leading experts in the field of cyber-security technologies.

Channels/Actions: INS will exploit the project results in the following ways: a) pursue new collaborations and participation in new research and innovation actions; b) enhance its technical expertise in cyber security leading to new products and services; c) establish relations and alliances in the cybersecurity market; d) establish a permanent channel for development and exploitation with the Greek academia (UPRC); e) proceed to commercial exploitation of the solution. As far as the latter point is concerned, the INS and UPRC components of DRME will be published as open source. Commercial exploitation will be feasible using the freemium model (offering the basic version for free, while charging is applied for premium features and services), using dual licensing (users can choose between open-source and commercial licensing), providing managed hosting or cloud services for the open-source tool, taking care of installation, updates, and maintenance for clients who prefer a hassle-free solution, and offering custom development services based on the open-source tool.

Expected Sales: Increased revenues based on the exploitation of the DRME tool using the aforementioned channels and activities, including direct commercial exploitation, participation in new collaborative projects, utilization of the gained know-how and the newly acquired strategic alliance with the NG-SOC ecosystem.

4.3 University of Piraeus Research Center (03 UPRC)

Results to exploit: UPRC will pursue the exploitation of: a) the Dynamic Risk Management Engine (DRME) that is co-developed with INS and integrated with ED solutions, b) the developed training programs and exercises for the design and implementation of new university courses (under and postgraduate), and seminars (offered as professional-level online training; c) the research outcomes generated during the development, improvement, and optimisation of the risk management system. As far as DRME is concerned, the three involved partners will prepare, agree on, and follow a collaboration agreement for the joint exploitation of the developed tools.

Market Sectors: As a research and academic organization, UPRC focuses on academic channels for the provision of novel and efficient educational and training tools, as well as tools to produce new research and innovation results and algorithms. Simultaneously, UPRC and Security Systems Laboratory members are involved in relevant regulation and law enforcement authorities, where UPRC, through its reliability and prestigious profile, will provide consultancy services. Moreover, for the full exploitation of the DRME potential, UPRC will cooperate with INS utilizing its established industrial channels, while UPRC will investigate the potential of a spin-off company that will pursue industrial-commercial aspects of the solution.

Channels/Actions: UPRC will exploit the project results in the following ways: a) pursue new collaborations and participation in new research and innovation actions; b) enhance its technical expertise in cyber security leading to new products and services; c) establish relations and alliances in the cybersecurity market; d) utilize the educational and training course and material to improve the curricula for undergraduate and postgraduate courses or develop new courses and professional training solutions; e) exploit the creation of a stable channel with Greek SMEs (INS); f) proceed to commercial exploitation of the solution. As far as the latter point is concerned, UPRC and INS will propose a joint commercialization plan. Details are mentioned at the corresponding point of Sec. **Error! Reference source not found.**.

Expected Sales: Increased revenues based on the exploitation of the new training programs, the exploitation of the DRME tool using the aforementioned channels and activities, participation in new collaborative projects, utilization of the gained know-how, and the newly acquired strategic alliance with the NG-SOC ecosystem.

4.4 SPACE HELLAS (04 SPH)

Results to exploit: the KERs to be exploited by SPH are the BIPS and Next Generation SIEM. Stemming from background assets of SPH, the enhancement of those KERs will be pursued. This will happen with their deployment in sectors additional to the military domain, where the initial deployments and validations were performed (i.e., financial via the Caixa Bank pilot). New data pipelines will be explored, new business processes will be considered, and the new SIEM automation features will be leveraged to introduce a scientifically sound and technologically robust solution for a SOC team.

Market Sectors: the main target will be the Greek national SOC. SPH is a member of the EL-SOC project that implements the national SOC and is coordinated by the Greek Ministry of Digital Governance. The existing clientele of the SOC services of SPH comprised of private organisations will also be leveraged. Finally, SPH will enhance its established position in national cyber-defence by improving its current offerings with the NG-SOC outcomes. More specifically, SPH envisions deploying the NG-SOC results to military cyber ranges following national and European initiatives (i.e., CYBER RANGES[3], CapTech Cyber[4]). Finally, selected components of the two KERs will be properly tailored to be included in solutions delivered to LEAs. Such components may be AI-enabled classifiers and feature extraction capabilities that can facilitate LEA investigations that involve high data volumes (i.e., financial corruption cases, cybercrime, etc.).

Channels/Actions: SPH will leverage its existing clientele and business network around SOC services and cyber defence. It will also pursue new alliances in research and commercial contexts, stemming from the NG-SOC consortium and expanding to the EU cybersecurity and cyber defence community (e.g., EDA, DG-HOME, etc.).

Expected Sales: sales from new cybersecurity solutions incorporating the NG-SOC results; new R&D projects where NG-SOC results will be introduced as background assets.

4.5 CYENTIFIC AS (05 CYEN)

Results to exploit: the KERs to be exploited by CYEN are the CTI sharing system, the NG-SOAR, the collaborative incident case management system, and the know-how acquired while developing these tools both from a research, standardization, and implementation perspective. This will allow CYEN to increase its product (and service) portfolio by providing trustworthy state-of-the-art tools and enable the SME to be onboarded and

[3] https://eda.europa.eu/news-and-events/news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

[4] https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

collaborate with other European projects. In addition, the pertinent activities in NG-SOC will allow CYEN to become a major player in cybersecurity standardization and a trusted knowledge provider for EU policymaking.

Market Sectors: CYEN collaborates closely with academia and industry within and outside the EU. It is a trusted knowledge hub for cybersecurity information modelling, automation, and standardization activities and a big contributor to open source. Thus, it will use its extensive network, including national security authorities and CSIRTs, critical infrastructure operators, MSSPs, large and small organizations, universities and research institutes, standards-developing organizations, governments, ENISA and other EU cybersecurity-focused stakeholders, and formal cybersecurity communities such as FIRST to raise awareness about the developed tools and their provision.

Channels/Actions: as mentioned above, CYEN has direct contact with governments, national and sectorial CSIRTs, national security authorities, ENISA through the participation in different ad hoc working groups and policymaking groups, standards-developing organizations, and MSSPs and thus will aim to exploit these channels to disseminate NG-SOC results, including the developed tools and know-how. CYEN will proceed to provide demos and consult the stakeholders on how they can address specific use cases and the benefits derived from NG-SOC tools. In addition, CYEN will engage in public and academic talks, and presentations in conferences and workshops and continue supporting standardization while raising awareness about the NG-SOC tools. Finally, CYEN, to attract potential customers, will create a global community around NG-SOC where minimum viable versions of specific tools will become available and maintained as open-source.

Expected Sales: Increased revenues based on the exploitation of the tools, know-how, and the market sectors and channels identified. In addition, it is expected that CYEN will be able to participate in more EU projects as it becomes a major EU knowledge hub and tool provider in the domains of CTI, collective threat defence, automation, and AI.

4.6 CAIXABANK SA (06 CXB)

CXB plans to exploit the pilot and use cases developed in NG-SOC during and beyond the lifespan of the project. The approach for taking profit from the pilot after the project unfolds in two types of Exploitation plans: Internal exploitation plan and External Exploitation plan.

Internal exploitation plan: First, CXB employees from the Digital Security department, CSIRT and SOC plan to evaluate the usage of the tools and models extracted from finance use cases in its day-to-day operations. In a second phase, CXB plans to deploy part of the NG-SOC platform and use cases in its Security Innovation sandbox, an isolated infrastructure designed to evaluate innovative tools' integration into the Digital Security department’s day-to-day operations. The deployment of some of those tools in CXB premises, even in a laboratory environment, will allow to refine and align the tools’ requirements, to streamline and facilitate eventual integration with CXB systems in production. More concretely, the objective is to undertake an extended evaluation of NG-SOC tools and platform and the use cases in that environment, allowing a higher integration with some of CXB systems and allowing to use realistic confidential data that cannot leave CXB premises. Third, supposing the second evaluation is positive, CXB would integrate NG-SOC platform (as a whole or the specific subset of tools that allows to deploy tested finance use cases) inside the premises of the entity, replicating the resources and security processes tested in the Security Innovation sandbox and defining the governance model of the tool within the entity. That will open the platform to be used by other CXB teams, when necessary.

External exploitation plan: Due to the fact that the use cases related to finance sector explored within NG-SOC address very common problems within the Financial sector, once we can measure the benefits of the set of tools developed and models, CXB can show these benefits outside the Organization, in national and international Security Workgroups CXB is part of and whose members are mostly bank and pairs with the same necessities as CXB. To name some of these Forums and workgroups:

- EPC (European Payments Council)

- ENISA EGFI (ENISA's Experts Group in Financial Sector)
- AEB (Asociación Española de Banca)

4.7 Cyprus Research and Academic Network (07 CYNET)

Results to exploit: Cyprus Research and Academic Network will exploit a) the CTI sharing system that is built on top of MISP and OpenCTI, b) the developed training programs and exercises for the design and implementation of new training courses for its members/constituents, and seminars offered to higher management. Furthermore, CYNET will explore possibilities for cooperation with new partnerships at a national, regional and international level.

Market Sectors: CYNETs mission is the provision of an advanced network infrastructure and related innovative networking services, including efficient educational and training tools, to educational and research institutions/organizations, along with the wider promotion of innovative Internet applications with the participation of relevant national and communal research projects and the promotion of national initiatives for the benefit of the Cypriot Educational and Research community.

Channel/Actions: CYNET will exploit the project results in the following ways: a) pursuit new collaborations and participation to new research and innovation actions; b) enhance its technical expertise in cyber security leading to new products and services. c) utilize the educational and training course and material to improve the training courses for its members.

Expected Sales: Increased revenues based on the exploitation of the new training programs and future collaborations.

5 Intellectual Property Rights (IPR)

Establishment of a proper IPR strategy is an essential requirement for a successful exploitation, high impact and the protection of the identified key exploitable results produced during the NG-SOC project. Therefore, it is important that all NG-SOC consortium partners jointly develop and agree upon a strategy, which will define the collaboration framework as well as commercial or industrial exploitation aspects protected through Intellectual Property Rights. Such an agreement will be formalised within a legal document known as **IPR (Intellectual Property Rights) Agreement**. The IPR Agreement, based on the Consortium Agreement (CA) already signed by all the partners, will provide obligations and rights related to NG-SOC foreground IP (Intellectual Property) ownership and exploitation. As such, it will focus on:

- raising participants' awareness regarding IP issues
- contributing to the resolution of disagreements between participants
- assisting in the drafting of the plan for the use and dissemination of foreground
- tracking down results that should be protected and advise individual partners on the means of protection
- assisting participants in evaluating their contribution to the jointly owned foreground and establishing their respective shares
- decisions regarding third parties joining the consortium with the intention to receive ownership of the Foreground of a specific Party

NG-SOC partners will have several potential options to protect the Intellectual Property they have generated during the project [6]. These can include **trademarks** (exclusive rights over distinctive signs), **patents** (exclusive rights over an invention for a limited period, normally 20 years), **copyright** (rights over literary, scientific and artistic works, computer programs, and database structure), **trade secrets** (valuable information on technology or on any other business aspect), etc. Furthermore, the exploitable foreground of the NG-SOC project could be categorised in the following 3 main groups:

For further research (e.g., architecture module designs, algorithms, parts of software applications…)

For creating and commercializing marketable products (e.g., application, tool, component, simulation hardware…) or **services** (e.g., cybersecurity situational awareness, coordinated incident handling/response, cybersecurity training, consultancy, NG-SOC technical support, etc.)

For creating and providing a service for others:

- Joint exploitation of the NG-SOC solution developed under the project, based on the joint ownership terms and conditions.
- Individual exploitation of the individual contributions of the parties in the NG-SOC solution developed under the project.

This deliverable presents the initial identification of any new generated intellectual property. However, at this preliminary stage, the partners have not made any decisions for the most appropriate strategy to protect this IP. During the later project phase(s), in the oncoming months, an optimal route for protecting the foreground IP will be defined. The results will be presented in the second iteration of this deliverable.

Here, as previously stated, the basis has been initially setup in the NG-SOC Consortium Agreement, where among other, several relevant sections related to the management of IPR as well as ownership, transfer of results and exploitation rights are defined:

Ownership of Results (Section 8.1 of the CA): There are rules in place that handle the ownership of results, where results are owned by the party that generates them.

Joint Ownership of Results (Section 8.2 of the CA): In the case of joint ownership of results it is covered by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results, managing the legal aspects of the exploitation and protection of the IPR.

Transfer of Results (Section 8.3 of the CA): Each party may transfer ownership of its own results following the procedures of the GA Article 16.4 and its Annex 5, Section Transfer and licensing of results, sub-section "Transfer of ownership.

Access Rights to Results for Exploitation (Section 9.4 of the CA):

- Access Rights to Results if Needed for Exploitation of a Party's own Results shall be granted on Fair and Reasonable conditions.
- Access rights to Results for internal research and for teaching activities shall be granted on a royalty free basis.

5.1 Background Technologies / Know-How

Background as defined on The European Participant Portal glossary [1]:

"Any data, know-how and/or information, whatever its form or nature (tangible or intangible) including any rights such as intellectual property rights which are needed to carry out the project or exploit its results".

Table 3 shows all background technologies and know-how that the consortium partners have used for the implementation of the NG-SOC project, with particular emphasis on the associated Intellectual Property Rights, as identified in the Consortium Agreement.

Table 3. IPR Ownership of Background Technologies and Know How used

Background Technology / Know-How	IPR Ownership
QLACK WebDesktop	ED (100%)
Risk analysis and impact assessment engine (RITA)	ED (100%)
Features from PANDORA components: cyber threat intelligence; network anomaly detection; rule-based threat mitigation; SIEM environment and relevant UI components; OSINT services considering MISP, MITRE ATT&CK, Lockheed Martin Cyber Kill Chain etc	SPH (100%)
ML models for events classification and reduction of false positives	SPH (100%)
CYENTIFIC CACAO Editor	CYEN (100%)
CYENTIFIC Collective Defence Incident Case Management System (CDCM)	CYEN (100%)

5.2 Foreground Technologies / Know-How

Foreground as defined on The European Participant Portal glossary [1]:

"*Any tangible or intangible output of the action (such as data, knowledge and information, whatever their form or nature, whether or not they can be protected), which are generated in the action, as well as any attached rights, including intellectual property rights*".

Table 4 shows preliminary information regarding IPR ownership of the NG-SOC outcomes. This information should be considered as an initial identification since it will be updated and finalised towards the end of the project. IPR ownership is based on the development of relevant outcomes by specific partners, during the development of the project.

Table 4. IPR Ownership of Foreground Technologies and Know How

Partner	No.	Project Outcome
ED	1	AI-powered Penetration Testing Methods and Tools
	2	Part of the CTI Sharing System contributed by ED
	3	Part of the Dynamic Risk Management Engine contributed by ED
	4	Part of the Next generation SOAR contributed by ED
	5	Hands-On Educational Platform
	6	Cybersecurity training and exercise scenarios
	7	Cybersecurity market analysis and landscape mapping
	8	Exploitation strategy
INS	1	Part of the Dynamic Risk Management Engine contributed by INS
	2	Part of the threat landscape and domain modelling relevant to the NG-SOC project, contributed by INS
	3	Part of the strategy for skills development of cybersecurity professionals, contributed by INS
UPRC	1	Part of the Dynamic Risk Management Engine contributed by UPRC
	2	Part of the threat landscape and domain modelling relevant to the NG-SOC project, contributed by UPRC
	3	Part of the strategy for skills development of cybersecurity professionals, contributed by UPRC
SPH	1	Behavioural Intrusion Prevention System
	2	Next Generation SIEM
	3	Part of the AI-powered Penetration Testing Methods and Tools contributed by SPH
CYEN	1	Part of the CTI Sharing System contributed by CYEN
	2	Part of the Next generation SOAR contributed by CYEN
CXB	1	Banking domain modelling
	2	Risk Assessment models in banking domain
	3	Caixa Bank Risk Register
CYNET	1	CYET-CSIRT training use cases
	2	Training material that is provided by CYNET-CSIRT

6 Horizon Results Booster

To increase the impact of EU-funded projects, the EC has initiated the HORIZON Results Booster (HRB) [7]. NG-SOC will apply for the HRB services with one of HRB's key partners, Trust-IT Services. In the upcoming months, NG-SOC will take advantage of this initiative and explore the possibilities to boost its impact. As shown in Figure 2, the main objective of the Horizon Results Booster is to assist EU-funded projects with broader dissemination and exploitation possibilities without additional costs for the consortia. It is supposed to shorten and enable a better transfer of results to policymakers, the market/industry, and society. The Booster itself consists of three different areas of support, which build upon each other. The overview of services is shown in Table 5.

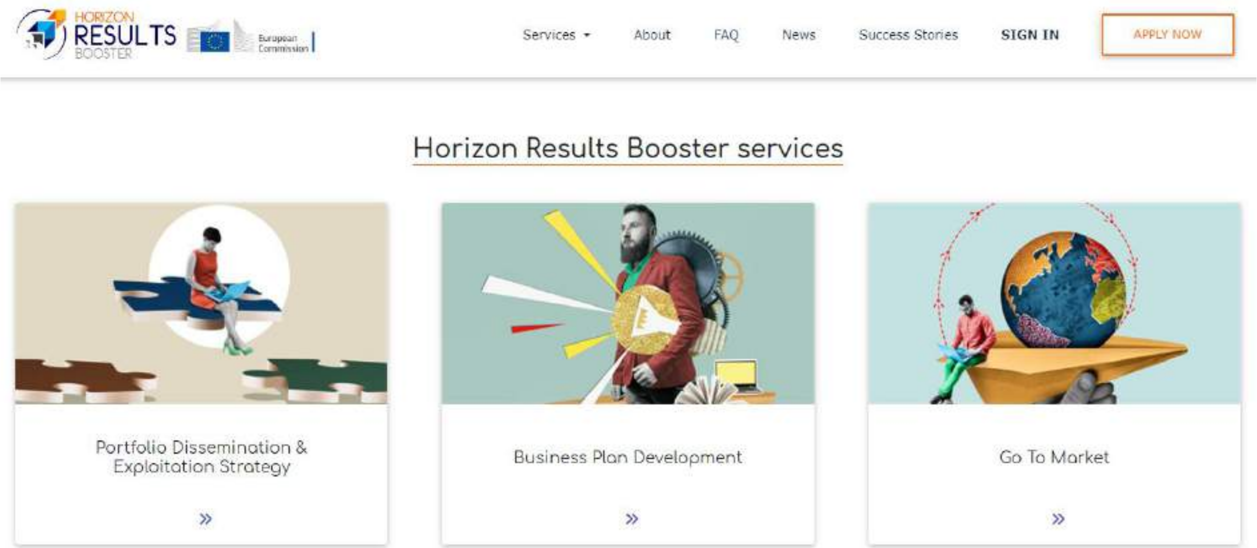


Figure 2. Horizon Results Booster EC initiative

6.1 Portfolio Dissemination & Exploitation Strategy

This service consists of three separate modules, which can be booked as single offers, in combinations of two of them, or as the whole package:

- **Module A** is about identifying and creating the portfolio of R&I project results. It supports the creation of a portfolio of results that are suitable for joint dissemination and provides guidance for identifying similar ongoing publicly funded projects on regional, national or EU level and stakeholder and target audience mapping. Useful to get to know who is doing similar/complementary activities to create critical mass.
- **Module B** supports projects in designing a joint dissemination plan and executing the actual dissemination of the portfolio results. It includes the visual identity for the beneficiary project group and a short video describing the project results.
- **Module C** supports projects in improving their already existing exploitation strategy towards effective exploitation of key exploitable results (KERs) by reviewing the project's KERs, outlining exploitation paths of results, and supporting the execution of risk analysis related to the exploitation of results.

6.2 Business Plan Development

This service aims to assist beneficiaries in bringing their results closer to the market by developing an effective business plan, including market analysis, a business strategy, an operation plan, etc. Project beneficiaries will also receive assistance to identify solutions for implementation in terms of:

- **Start-up operations** (e.g., identification of incubators, third-party support for management – legal, administrative)
- **Investors** (e.g., identification of venture capitalists in the market sector, identification of business angel networks)
- **Funding** (e.g., identification of financial instruments for start-ups or new businesses from banks, local governments, national funding, identification of crowdfunding platforms and schemes)

6.3 Go-to-Market Support

This service aims to assist beneficiaries in making their project results ready for commercialisation by supporting them in identifying and/or addressing potential obstacles to the exploitation of project results. The service provides assistance, coaching, pitching the products, IPR, innovation management and other business services.

Table 5. Horizon Results Booster – Overview of services

Service 1 – Portfolio Dissemination and Exploitation Strategy (PDES)		
Module A: Identifying and creating the portfolio of R&I project results	Identification of who is doing similar/complementary activities to create critical mass and to form a project group (PG). Creation of portfolio results. Mapping of relevant stakeholders/target audience for each portfolio.	Single projects & project groups.
Module B: Helping projects from the portfolio to design and execute a portfolio dissemination plan (design and execution)	Supporting the project group in designing a joint dissemination plan. Creation of visual identity for joint activities. Capacity building to improve communication and dissemination skills. Support on copywriting, social media activities, etc.	Project groups.
Module C: Assisting projects to improve their existing exploitation strategy	Supporting projects in improving their already existing exploitation strategy, towards effective exploitation of key exploitable results (KERs), by a) Reviewing the KERs of the project, b) Reviewing the exploitation plan and identifying exploitation path, c) Identifying stakeholders in the value chain and d) Supporting the exploitation risk analysis	Single projects.
Service 2 – Business Plan Development (BPD)		
Assist beneficiaries to bring their results closer to the market by developing an effective business plan.		Single projects.
Service 3 – Go-To-Market Support (G2M)		
Assist beneficiaries in making their project results ready for commercialisation, by providing support to pitching, IPR guidance, innovation management, business services, exploitation options, access to non-EU funding.		Single projects & project groups with high Technology Readiness Levels (>6) and mature projects.

7 Dissemination & Communication

The first and most important step in setting the communication and dissemination plan for the NG-SOC project is to clearly define the objectives to be achieved and then have the associated activities appropriately designed to meet those objectives. According to the Grant Agreement (GA), the Consortium is committed to promoting the action and its results by providing targeted information to multiple audiences (including the media and the public) in a strategic, coherent, and effective manner.

The Dissemination and Communication Plan defines the different strategic phases of the project. For each of the phases, a series of tasks have been defined to be developed. At this moment, M3, the NG-SOC project is in the "Awareness" phase:

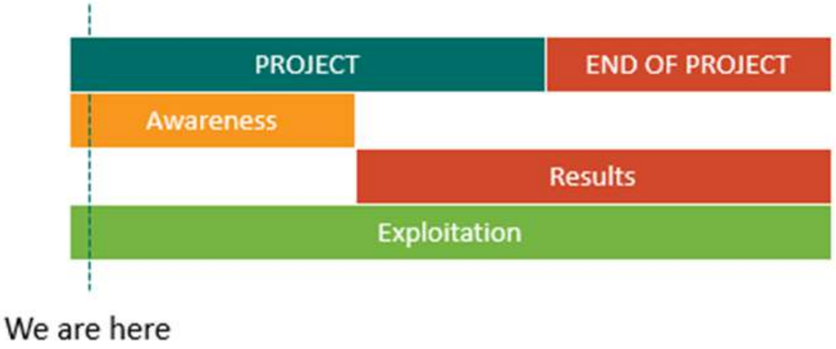
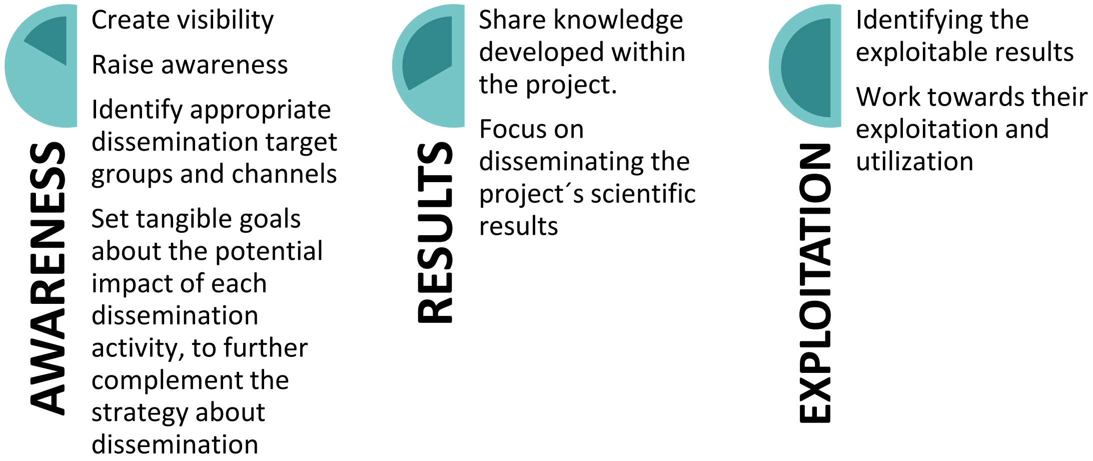


Figure 3. Phases of the NG-SOC Strategy



Create visibility

Raise awareness

Identify appropriate dissemination target groups and channels

Set tangible goals about the potential impact of each dissemination activity, to further complement the strategy about dissemination

Share knowledge developed within the project.

Focus on disseminating the project´s scientific results

Identifying the exploitable results

Work towards their exploitation and utilization

Figure 4. Description of each strategy phase of the Plan

7.1 Dissemination Objectives and Strategy

The dissemination activities deal with the diffusion of scientific and technological knowledge generated within the context of the NG-SOC project, aiming to ensure both a mid– and long-term impact by informing the target audience about NG-SOC. The dissemination strategy to be applied in the project is aligned with the high-level objectives:

Obj. I: To ensure maximum visibility of the project in the target audiences via appropriate key messages.
Obj. II: To diffuse the scientific and technological knowledge generated in the project within and beyond the project's consortium in a timely manner.
Obj. III: To establish liaisons with other projects and initiatives for knowledge and innovation transfer.
Obj. IV: To engage the target audiences to get feedback and validate the project's results.

7.2 Communication Objectives and Strategy

The communication activities include actions that contribute to the diffusion of the project's results beyond the consortium and the direct stakeholders, maximizing its contribution to innovation and attracting a wide range of stakeholders who are invited to benefit from the project's advancements.

The communication strategy is driven by the following communication objectives:

Obj. I: To create awareness of the project among the full range of target audiences defined for communication activities.
Obj. II: To provide a clear view of the project's concept, goals, and results by formulating adapted key messages, and preparing communication material.
Obj. III: To create an active community of potential users and collect feedback that will be considered by the project's activities.
In order to ensure that the different communication objectives are effectively addressed, and the expectations of the target audience groups are met, particular attention will be paid to adapting the communication means, the measures, and the content to the needs and knowledge levels of the targeted groups as well as to the status/progress and needs of the project.

7.3 Target Audience

Having defined the goals and objectives for dissemination and communications, we specified the potential targeted audiences of NG-SOC and their specific interest in the project.

The definition of the target audiences and the understanding of their special characteristics and needs is critical for directing the resources to the most relevant and interested actors, thus maximizing the project's potential impact.

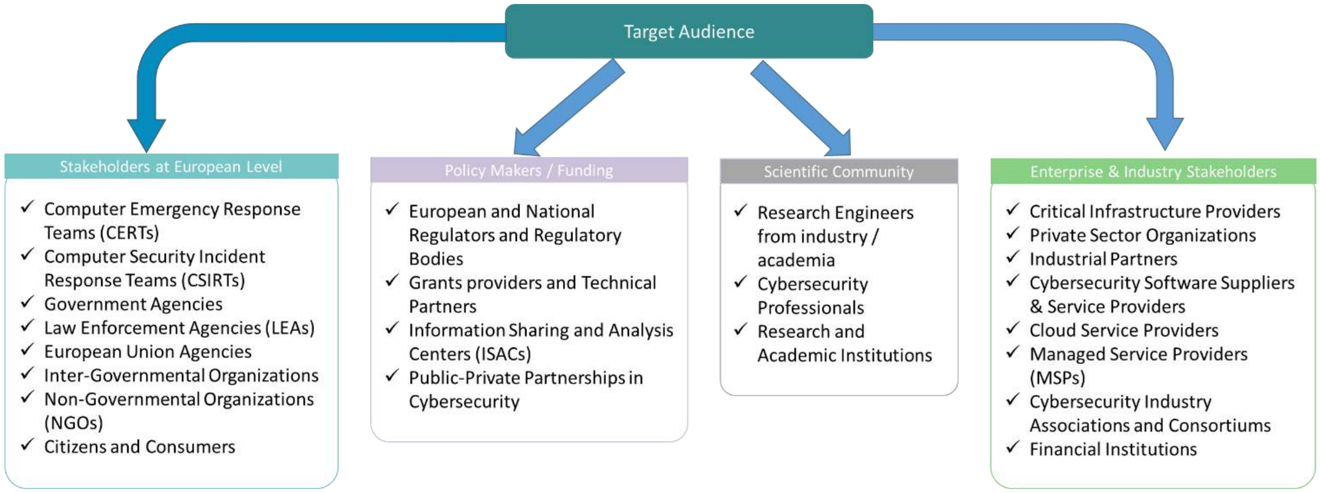

Target Audience
Stakeholders at European Level
✓ Computer Emergency Response Teams (CERTs)
✓ Computer Security Incident Response Teams (CSIRTs)
✓ Government Agencies
✓ Law Enforcement Agencies (LEAs)
✓ European Union Agencies
✓ Inter-Governmental Organizations
✓ Non-Governmental Organizations (NGOs)
✓ Citizens and Consumers
Policy Makers / Funding
✓ European and National Regulators and Regulatory Bodies
✓ Grants providers and Technical Partners
✓ Information Sharing and Analysis Centers (ISACs)
✓ Public-Private Partnerships in Cybersecurity
Scientific Community
✓ Research Engineers from industry / academia
✓ Cybersecurity Professionals
✓ Research and Academic Institutions
Enterprise & Industry Stakeholders
✓ Critical Infrastructure Providers
✓ Private Sector Organizations
✓ Industrial Partners
✓ Cybersecurity Software Suppliers & Service Providers
✓ Cloud Service Providers
✓ Managed Service Providers (MSPs)
✓ Cybersecurity Industry Associations and Consortiums
✓ Financial Institutions

Figure 5. NG-SOC Target Groups

As also shown in Figure 5, the targeted audience of the project's results can be classified into the following broad categories.

Scientific community. The scientific community includes research engineers from industry and academia, (PhD) students, and professionals; to reach this audience the Consortium will use means such as release of demo work packages via mass media channels, scientific publications in European and international venues and in press releases for popular and sectorial magazines and newspapers, as well as presentations and participations in academic events and/or conferences for cyber-security.

Enterprise & industry stakeholders. The dissemination activities targeting commercial and industrial experts aim to raise awareness and inspire interest and market demand concerning the NG-SOC output. Towards this end, companies and organisations (including manufacturers of cyber-security products and services, as well as associations, regulators, and policy makers in the cyber-security industry, the standardisation community, and the banking/finance, energy and research, and academic market communities) will become aware of the toolkit developed in the project and the final outcomes, and have by this multimodal benefits towards facing security and privacy challenges; business decision makers can adopt project results in their computing infrastructures or in the system architectures used at the enterprises, cybersecurity and IT specialists can integrate the provided SOC solutions into systems developed by companies, equipment manufacturers, and/or cyber-security suppliers can deliver products that may deal with highly sophisticated attacks, etc. The Consortium intends to organise a number of outreach activities in order to interact with the eventual beneficiaries of the NG-SOC AI-enhanced technology.

EU citizens and customers. The topics of leveraging state-of-the-art Artificial Intelligence (including Machine Learning techniques) and computing power to improve the detection of threat actors and dynamically learning about the changing threat landscape and the future structure of the cyber-security market are attracting more attention across Europe. Already billions of devices (both personal and industrial) are interconnected across the globe in a phenomenon known as the Internet of Things (IoT). Therefore, NG-SOC's results shall be available to the wider public/end customer via attractive and user-friendly techniques such as press releases in popular papers, infographics, white board animations, technical videos, technical papers available on its website, and regular updates via social media (i.e., Twitter, LinkedIn, etc.). NG-SOC Consortium will ensure that the results of the project will become available across Europe in both technical and media focused formats, to allow the public to be aware of and use the project's outcomes.

Policy makers. The envisioned capacity-focused, AI-enhanced SOC service together with the dedicated training sessions in digital infrastructure security is expected to change the current state-of-the-art in SOC/CSIRT operations while delivering multidisciplinary and realistic training and knowledge testing in multiple domains and by providing a series of unique features and services that will be incorporated in the produced platform (like CACAO Editor, Collaborative Incident Case Management System, Risk Management, AI-powered Penetration Testing Methods and Tools, etc.). The NG-SOC outcomes will enable policy makers to focus on novel methods and tools for increasing SOC teams' situational awareness and collaborative resilience against highly sophisticated attacks as well as for cybersecurity training. Furthermore, the given solution is also expected to impact the whole banking, energy and research and academic sector value chain. Towards this end, the Consortium will promote the results of this project in the EU supply chain on threat intelligence in conjunction with the European Union Agency for Cybersecurity (ENISA) and National Regulatory bodies by organising regular formal meetings with all the involved agencies in the European Commission, including also competent authorities and CSIRTs under the NIS Directive and interested national regulators who may use NG-SOC results to feed into future market designs and regulatory frameworks.

7.4 Proposed Measures for Dissemination

Dissemination activities are of the utmost importance during the project's duration, to create visibility and raise awareness among a variety of stakeholders to utilize the project's results and find ways to further continue and advance the related research. NG-SOC dissemination activities target a wide range of stakeholders, starting from the specific scientific fields tackled by the project to the end-user community and finally to players who will ultimately contribute to delivering NG-SOC to the market.

Table 6. Dissemination Activities

OBJECTIVES	ACTIONS
Awareness: Create visibility and raise awareness	• Project Logo and visual identity • Develop the Project Website and upload the first public deliverables, news about plenary meetings of the consortium and participation in conferences and workshops. • Create the Social Media channels and start building the NG-SOC Community • Share several press articles with EE mass media and prepare Scientific Publications • Participation in conferences, seminars, and workshops • Project brochure for recruiting users for pilots • Liaison with other projects and stakeholder engagement
Results: Share knowledge developed within the project	• Refine website with more concrete results and public deliverables • Social media and online promotion, such as news about early results • Press release with first results • Distribute marketing material • Attend events • Create promotional videos showcasing the progress of the project and first results • Share several press articles with EE mass media and Science Publications
Exploitation: Work towards exploitable results and utilization	• Upload into the website project results and public deliverables • Social media and online promotion • Share several press articles with EE mass media and Science Publications • Create promotional videos showcasing results • Establish open-source communities for specific NG-SOC tools

7.5 Key Messages

7.5.1 Main Message

The overall vision of NG-SOC is to design, deploy and validate a **collaborative, interoperable, capacity-focused SOC service** that holistically combines capacities for **shared situational awareness, coordinated incident handling/response, dedicated training sessions,** and **educational programmes** in digital infrastructure security, tailored to identified training goals and objectives, ultimately enhancing national cybersecurity capabilities and cross-border collaboration, in line with current and upcoming regulatory requirements. To achieve these objectives, NG-SOC will adopt an **open-standards-based** implementation strategy and will utilise and enhance open-source technological solutions. It is worth noting that open standards are a crucial element in boosting **cybersecurity automation** and building an **open ecosystem** where cybersecurity products, tools, and services can interoperate natively without the need for customized integrations that are expensive and complex to build and maintain. NG-SOC answers to the **cybersecurity challenges** faced by EU organisations and provides different technologies, tools, and techniques concurrently and in unison, as well as an ecosystem to gather initial evidence, develop, test, and experiment with novel frameworks and tools. NG-SOC aims to contribute to the priorities of the **EU's Cybersecurity Strategy** for the Digital Decade by increasing information sharing and collaboration on cyber through the NG-SOC cybersecurity-aware ecosystem. NG-SOC aims to contribute to the EU Cyber Shield initiative of the **EU Cyber Solidarity Act**[5] to establish and promote active collaboration between SOCs within member states and across member states.

7.5.2 Tailored Key Messages

In the table below, different key messages per target audience are being presented. The target audiences are:

Decision/Policymakers

Stakeholders at European Level

Scientific Community

Enterprise & Industry Stakeholders

Citizens and Consumers (i.e., General Public)

Table 7. Key messages per target group

Target Group	Message
1, 2, 3, 4, 5	NG-SOC toolkit addresses the whole cycle of the cybersecurity challenges from the identification of the involved assets and vulnerabilities up to the collaborative incident investigation and impact assessment of a possible attack
1, 2	The NG-SOC toolkit is capable of sharing information coming from different sources and therefore will achieve the maximization of the CSIRT network added value
1, 2, 3, 4	NG-SOC toolkit enables the estimation of the attack impact, driving potential investments for appropriate countermeasures
1, 2, 3, 4	NG-SOC promotes best practices in cybersecurity management solutions to the banking, energy and educational communities and through training of security experts seeks to communicate their value and thus, increase their acceptance

[5] https://www.eu-cyber-solidarity-act.com/

1, 2, 3, 4, 5	NG-SOC enhances the cybersecurity level of the banking, energy and ICT systems contributing to their uninterrupted operation
1, 2, 3, 4, 5	NG-SOC AI-enhanced technologies maximises its capability to effectively predict, detect, analyse, and respond to threats
1, 2, 3, 4, 5	NG-SOC highly sophisticated network and system behavioural monitoring, based on state-of-the-art Artificial intelligence (AI) algorithms, solves the multidimensional and complex security problem related to the identification of anomalies caused by novel multi-faceted attacks (both internal and external)
1, 2, 3, 4, 5	NG-SOC Next generation SOAR incorporates a low-code approach to security orchestration and incident management automation and a dedicated orchestration engine and case management system, driving the automation of coordinated, collaborative incident response workflows, resulting in minimum business disruption.
1, 2, 3, 4, 5	NG-SOC AI-powered penetration testing methods and tools significantly reduce time and costs while increasing test frequency and entry point coverage
1, 2	NG-SOC supports and/or strengthens and interconnects SOCs at regional, national and EU level
1, 2, 3, 4, 5	NG-SOC addresses the lack of security awareness, and limited organisational and operational capabilities in digital infrastructure security with new teaching and knowledge transfer methods that rely on cyber-ranges and realistic cybersecurity training and exercise scenarios
1, 2, 3, 4	NG-SOC supports the increased availability, quality, usability and interoperability of threat intelligence data among SOCs and relevant entities
1, 2, 3, 4	NG-SOC supports information sharing among public authorities (including competent authorities and CSIRTs), as well as with other SOCs, facilitated through appropriate sharing agreements, while complying with all obligations related to privacy and personal data protection
1, 2, 3, 4, 5	NG-SOC answers to the cybersecurity challenges faced by EU organisations and provides different technologies, tools and techniques concurrently and in unison and an ecosystem to gather initial evidence, develop, test and experiment with novel frameworks and tools
1, 2	NG-SOC aims to contribute to the priorities of the EU's Cybersecurity Strategy for the Digital Decade, by increasing the information sharing and collaboration on cyber through the NG-SOC cybersecurity aware ecosystem
1, 2	NG-SOC aims to contribute to the EU Cyber Shield incentive to establish and promote active collaboration between SOCs within member states and across member states
1, 2	NG-SOC will strengthen EU cybersecurity capacities and European Union sovereignty in digital technologies.
1, 2	NG-SOC will increase the resilience of the digital infrastructures and systems
1, 2	NG-SOC will increase the software, hardware, and supply chain security
1, 2	NG-SOC will reinforce awareness and a common cyber security management and culture
1, 2	NG-SOC will deliver smart and quantifiable security assurance in the framework of addressing the specific need for certification across the EU

7.5.3 Key Words

Security Operation Centres, Security information and event management (SIEM), Information sharing, Threat intelligence, Situational awareness, Collaboration, Collective knowledge, Artificial intelligence, Machine Learning, Cybersecurity resilience, Disruptive technologies, Supply chains, Interoperable secured communications (Security systems architecture), Risks and vulnerabilities assessment, Cybersecurity, Information Security Technologies, Attack modelling and security assurance tools, Privacy, Personal data protection, Threats investigation and impact assessment, Standards, Cybersecurity training.

7.6 Communication Activities

Communication is a very important activity in the NG-SOC project. Besides the project-oriented communication between partners, there is a need for output and impact-targeted focus, involving the Commission, the project partners and various external stakeholders.

Table 8. Communication Activities

Communication Channel and media	Activities	Language	Responsible partner(s)
Social media	Social media campaigns	EN	WP7 Leader (ED)
Website	News, deliverables, articles and events	EN	WP7 Leader (ED)
Press Articles and Publications	Press releases, opinion articles	Country's language	WP7 Leader (ED)
Logo, visual identity	Use in every of the above communication activities	EN	WP7 Leader (ED)
Conference participation and contribution	Project presentation, news/updates sharing	Country's language	Individual partners

7.7 Dissemination Plan

This section outlines the activities and tools to present the project to the target audiences.

7.7.1 Scientific Publications

Since NG-SOC also has a research dimension, the consortium plans the publication of the project's development and outputs in high-quality journals and conferences. The tables that follow (Table 9 and Table 10) present an indicative list of journals and conferences that are relevant to the NG-SOC research areas. Please notice that the following list is non-exhaustive, and the submission of articles will be based on whether journals or conferences specific topics (or call for papers in special issues) match those of the particular work carried out in the context of NG-SOC.

Table 9. Indicative list of scientific journals

ID	Title of Journal	Aim	Website	Acronym	Publisher
1	ACM Transactions on Information Systems	Information Systems (TOIS) is a scholarly journal that publishes previously unpublished high-quality scholarly articles in all areas of information retrieval	https://tois.acm.org/	TOIS	ACM
2	IEEE Transactions on Knowledge and Data Engineering	The scope includes the knowledge and data engineering aspects of computer science, artificial intelligence, electrical engineering, computer engineering, and other appropriate fields	https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=69	TKDE	IEEE
3	Large-Scale Data- and Knowledge-Centered Systems	The objective of the international journal on Large Scale Data and Knowledge Centered Systems is to provide an opportunity to disseminate original research contributions and a high quality communication platform for researchers and practitioners	https://www.irit.fr/tldks/		Springer
4	International Journal of Human-Computer Studies	Publishes original research over the whole spectrum of work relevant to the theory and practice of innovative interactive systems	https://www.journals.elsevier.com/international-journal-of-human-computer-studies	Elsevier	IJHCS
5	Information Processing and Management	Information Processing and Management is a leading international journal focusing on publishing peer-reviewed original research concerning theory, methods, or	https://www.journals.elsevier.com/information-processing-and-	IPM	Elsevier

		application in the field of information science	management		
6	Journal of Cybersecurity, Computers & Security (Elsevier).	One of the most respected journals in IT security, being recognized worldwide as THE primary source of reference for IT security research and applications expertise	https://www.sciencedirect.com/journal/computers-and-security	C&S	Elsevier
7	ACM Transactions on Privacy and Security	Publishes high-quality research results in the fields of information and system security and privacy. Studies addressing all aspects of these fields are welcomed, ranging from technologies to systems and applications, to the crafting of policies. Topics of interest include Security Technologies, Fundamentals, Secure Systems, Privacy Methods, Security and Privacy Applications, Privacy and Security Policies	https://dl.acm.org/citation.cfm?id=J789	ACM	TOPS
8	International Journal of Learning Technology	An international, refereed, scholarly journal providing an interdisciplinary forum for the presentation and discussion of important ideas, concepts, and exemplars that can deeply influence the role of learning technologies in learning and instruction. This unique and dynamic journal focuses on the epistemological thrust of learning vis-à-vis instruction and the technologies and tools that support the process. IJLT publishes papers related to theoretical foundations, design and implementation, and effectiveness and impact issues related to learning technologies	https://www.inderscience.com/jhome.php?jcode=ijlt	InderScience	IJLT
9	IEEE Transactions on Visualization and Computer Graphics	Publishes papers on subjects related to computer graphics, information and scientific visualization, visual analytics, virtual and augmented reality, focusing on theory, algorithms, methodologies, human-computer interaction techniques, systems, software, hardware, and applications in these areas	https://www.computer.org/csdl/journal/tg	IEEE	TVCG
10	IEEE Transactions on Dependable and Secure Computing	The purpose of TDSC is to publish papers in dependability and security, including the joint consideration of these issues and their interplay with system performance	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858	IEEE	TDSC
11	IEEE Transactions on Information Forensics and Security	The IEEE Transactions on Information Forensics and Security covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206	IEEE	TIFS
12	IEEE Security & Privacy	IEEE Security & Privacy’s primary objective is to stimulate and track advances in security, privacy, and dependability and present these advances in a form that can be useful to a broad cross-section of the professional community- ranging from academic researchers to industry practitioners	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013	IEEE SECUR PRIV	IEEE
13	Computers & Security	Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world	www.journals.elsevier.com/computers-and-security	COSE	Elsevier
14	IET Information Security	IET Information Security publishes original research papers in the following areas of information security and cryptography	https://digital-library.theiet.org/content/journals/iet-ifs	IET	IFS
15	International Journal of Information Security	The Journal offers prompt publication of high quality research on system security (intrusion detection, operating system security, database security), network security (Internet security, firewalls, mobile security, security protocols, anti-virus), foundations (privacy, access control, authentication, identification, applied cryptography, and formal security methods)	https://link.springer.com/journal/10207	Springer	IJIS
16	Network Security	Network Security is devoted to solving your network security issues in detail, now with even more news, information and solutions to your network security	www.journals.elsevier.com/network-security	Elsevier	NS

		problems			
17	Future Generation of Computer Systems	The journal aims to lead the way in advances in distributed systems, collaborative environments, high performance and high performance computing, Big Data on such infrastructures as grids, clouds and the Internet of Things (IoT)	https://www.journals.elsevier.com/future-generation-computer-systems	Elsevier	FGCS
18	IEEE Access	The scope of this journal comprises all of IEEE's fields of interest, emphasizing applications-oriented and interdisciplinary articles	https://ieeeaccess.ieee.org/	IEEE ACCESS	IEEE
19	Journal of Information Security and Applications	Provides a common linkage between a vibrant scientific and research community and industry professionals by offering a clear view on modern problems and challenges in information security, as well as identifying promising scientific and "best practice" solutions. JISA issues offer a balance between original research work and innovative industrial approaches by internationally renowned information security experts and researchers	https://www.journals.elsevier.com/journal-of-information-security-and-applications	JISA	Elsevier
20	ACM Transactions on Cyber-Physical Systems	Publishes high-quality original research papers and survey papers that have scientific and technological understanding of the interactions of information processing, networking and physical processes. This journal is published on a quarterly basis	https://dl.acm.org/journal/tcps	TCPS	ACM
21	Protection Automation and Control (PAC) World Magazine	The Protection, Automation and Control (PAC) World aims to promote better understanding and knowledge of the industry through networking with professionals. PAC itself is an industry magazine and forum for specialists to share knowledge and this event is run by the PAC World community	https://www.pacw.org/	PAC	PAC World Magazine

Table 10. Indicative list of scientific and industry conferences

ID	Title of Journal	Aim	Website	Acronym	Publisher
1	ACM International Conference on Web Search and Data Mining	WSDM publishes original, high-quality papers related to search and data mining on the Web and the Social Web, with an emphasis on practical yet principled novel models of search and data mining, algorithm design and analysis, economic implications, and in-depth experimental analysis of accuracy and performance	http://www.wsdm-conference.org/2024/	WSDM	Annual
2	ACM International Conference on Management of Data	The annual ACM SIGMOD/PODS Conference is a leading international forum for database researchers, practitioners, developers, and users to explore cutting-edge ideas and results, and to exchange techniques, tools, and experiences. The conference includes a fascinating technical program with research and industrial talks, tutorials, demos, and focused workshops. It also hosts a poster session to learn about innovative technology, an industrial exhibition to meet companies and publishers, and a careers-in-industry panel with representatives from leading companies	https://2024.sigmod.org/	SIGMOD	Annual
3	Conference on Innovative Data Systems Research	CIDR encourages papers about innovative and risky data management system architecture ideas, systems-building experience and insight, resourceful experimental studies, and provocative position statements. Papers are encouraged to present novel approaches to data systems architecture and usage, to inspire discussions on the latest innovative and visionary ideas in the field.	https://www.cidrdb.org/	CIDR	Biennial
4	ACM Conference on Research and Development in Information Retrieval	SIGIR is the premier international forum for the presentation of new research results and for the demonstration of new systems and techniques in information retrieval	http://sigir.org	SIGIR	Annual

5	IEEE International Conference on Data Mining	ICDM has established itself as the world's premier research conference in data mining. It provides an international forum for sharing original research results, as well as exchanging and disseminating innovative and practical development experiences. The conference covers all aspects of data mining, including algorithms, software, systems, and applications. ICDM draws researchers, application developers, and practitioners from a wide range of data mining related areas such as big data, deep learning, pattern recognition, statistical and machine learning, databases, data warehousing, data visualization, knowledge-based systems, high-performance computing, and large models. By promoting novel, high-quality research findings, and innovative solutions to challenging data mining problems, the conference seeks to advance the state-of-the-art in data mining	https://icdm2024.org/	ICDM	Annual
6	International Conference on Data Science, Technology and Applications	The purpose of the International Conference on Data Science, Technology and Applications (DATA) is to bring together researchers, engineers and practitioners interested on databases, big data, data mining, data management, data security and other aspects of information systems and technology involving advanced applications of data	https://data.scitevents.org/	DATA	Annual
7	European Conference on Research in Computer Security	The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas	http://conf.laas.fr/esorics/	ESORICS	Annual
8	ACM Conference on Computer and Communications Security	The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results	http://www.sigsac.org	CCS	Annual
9	IEEE Cyber Security and Resilience (CSR) conference	The conference focuses on theoretical and practical aspects of the security, privacy, trust, and resilience of networks, systems, and services as well as novel ways for dealing with their vulnerabilities and mitigating sophisticated cyber-attacks	https://www.ieee-csr.org/	CSR	Annual
10	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	The IEEE TrustCom (IEEE International Conference on Trust, Security and Privacy in Computing and Communications) is a forum for presenting leading works on trusted computing and communications, with regard to trust, security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks		TrustCom	Annual
11	International Conference on Computer Safety, Reliability, and Security (SafeComp)	SafeComp is an annual event covering the state-of-the-art, experience and new trends in the areas of safety, security and reliability of critical computer applications. SafeComp provides ample opportunity to exchange insights and experience on emerging methods, approaches, and practical solutions. It is a single-track conference allowing easy networking.	https://www.safecomp2024.unifi.it/	SafeComp	Annual
12	IEEE International Conference on Software Quality, Reliability and Security (QRS)	IEEE QRS gives engineers and scientists from both industry and academia a platform to present their ongoing work, relate their research outcomes and experiences, and discuss the best and most efficient techniques for the development of reliable, secure, and trustworthy systems.	https://qrs24.techconf.org/	QRS	Annual
13	IEEE Cybersecurity Development (SecDev)	SecDev is a venue for presenting ideas, research, and experience about how to develop secure systems. It focuses on theory, techniques, and tools to "build security	https://secdev.ieee.org/2024/home	SecDev	Annual

		in” to existing and new computing systems and does not focus on simply discovering the absence of security.			
14	IEEE Symposium on Security and Privacy (S&P)	EEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.	https://www.ieee-security.org/TC/SP2025/	S&P	Annual
15	RSA Conference	RSA Conference is the premier series of global events and year-round learning for the cybersecurity community. RSAC is where the security industry converges to discuss current and future concerns and have access to the experts, unbiased content and ideas that help enable individuals and companies advance their cybersecurity posture and build stronger and smarter teams. Both in-person and online, RSAC brings the cybersecurity industry together and empowers the collective “we” to stand against cyberthreats around the world. RSA Conference. Where the world talks security.	https://www.rsaconference.com/usa	RSAC	Annual
16	FIRST Conference	The conference, hosted by FIRST (Forum of Incident Response and Security Teams), provides a crucial platform for global collaboration in enhancing computer security. Attendees, irrespective of membership, engage in discussions and initiatives aimed at strengthening cybersecurity measures. The event fosters communication and information sharing among Computer Security Incident Response Teams (CSIRTs) worldwide, emphasizing coordination in incident response and prevention. The diverse audience includes technical staff, decision-makers, law enforcement, legal counsel, senior managers, and government executives committed to protecting critical systems. Past participants span information security practitioners, network architects, vendors, ISPs, and various professionals in the field	https://www.first.org/conference/2024/	FIRST	Annual
17	International Conference in Information Visualization (iV)	The iV conference includes a wide variety of topics in the areas of information visualisation including theory & practice, evaluation, applications, visualization and storytelling, visual analytics & data science, social media analytics, and others	https://iv.csites.fct.unl.pt/pt/	iV	Annual
18	International Conference on Information Systems Security and Privacy	The International Conference on Information Systems Security and Privacy is an event where researchers and practitioners can meet and discuss state-of-the-art research about the technological, social, and regulatory challenges that regard the security, privacy, and trust of modern information systems. The conference welcomes papers of either practical or theoretical nature, and is interested in research or applications addressing all aspects of trust, security and privacy, and encompassing issues of concern for organizations, individuals and society at large	https://icissp.scitevents.org/?y=2025	ICISSP	Annual
19	USENIX Security Symposium	USENIX Security brings together researchers, practitioners, system administrators, system programmers, and others to share and explore the latest advances in the security and privacy of computer systems and networks	https://www.usenix.org/conference/usenixsecurity24	USENIX	Annual
20	IEEE European Symposium on Security and Privacy	IEEE SP has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field	https://eurosp2024.ieee-security.org/	EuroSP	Annual
21	ACM Asia Conference on Computer and Communications Security	Presentation of novel research from academia, government, and industry on all theoretical and practical aspects of computer and network security	https://asiaccs2024.sutd.edu.sg/	AsiaCCS	Annual
22	ARES: International Conference on	ARES aims at a full and detailed discussion of the research issues of security as an integrative concept that covers	https://www.ares-conference.eu	ARES	Annual

	Availability, Reliability and Security	amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.			
23	CyberWiseCon Europe	CyberWiseCon is a premier IT security conference that brings together cybersecurity experts, industry leaders, and IT professionals from around the Europe.	https://cyberwisecon.eu/	CyberWiseCon	Annual
24	European Interdisciplinary Cybersecurity Conference	The conference is devoted to exploring and presenting original innovative applications, scientific and technological advancements in the field of cybersecurity	https://www.fvv.um.si/eicc2024/	EICC	Annual
25	IEEE Conference on Network Softwarization	Software-Defined Networking (SDN), Network Function Virtualization (NFV) and Cloud-Edge-Fog Computing are driving an unprecedented techno-economic shift in the Telecom and ICT industries. Network softwarization and programmability promise to reduce operational costs, provide better flexibility and bring new service paradigms. In particular, they are enabling the deployment of 5G infrastructures, spanning from high data rate fixed-mobile services to the Internet of Things, which is expected to accelerate the digital transformation that all the industry is witnessing. As a result, new service models and new value chains will emerge, leading to novel business models and significant socio-economic impact.	https://netsoft2024.ieee-netsoft.org/	IEEE Netsoft	Annual
26	IEEE International conference on cyber security and resilience	The conference focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks (to share results/promote work carried out in the project/train professionals)	https://www.ieee-csr.org/	CSR	Annual

7.7.2 Trade Fairs, Exhibitions, Workshops and other Events

The NG-SOC consortium will be proactive in putting forward proposals for themed workshops and symposia addressing priorities of H2020, DEP programme and bringing together key industrial sectors represented within the targeted value chains and public sector to present NG-SOC, look at integration opportunities and best practice examples, and allow communication of NG-SOC outputs to a wide audience. Additionally, stakeholders will be invited to workshops organized by NG-SOC to learn about the outcomes of the project and explore synergies and cooperation possibilities. All partners will be involved in the aforementioned activities in order for workshops to be organised. To this end, the NG-SOC Consortium plans the organisation of a number of special sessions (an indicative list of events is presented in Table 11).

Table 11. Indicative list of events organised by NG-SOC

ID	Event type	Aim	Outreach impact	Partners leading the effort
1	International Cyber Expo	Designed to help buyers' source solutions they need to improve the security and resilience of their businesses and critical infrastructures, International Cyber Expo bursts with networking and business opportunities with a highly sophisticated visitor base.	The event provides the best platform to facilitate networking and business opportunities with a highly sophisticated visitor base of top-level cyber security professionals. International Cyber Expo will deliver an audience of CISOs, top-level c-suite professionals, cyber policymakers, export leaders and Government all looking to network with leading suppliers and source the latest products vital to protect our nation and secure our networks.	ED
2	CYBERSEC Expo & Forum	The CYBERSEC Expo & Forum is a unique event – a combination of a debate on the	The CYBERSEC Forum is the key cybersecurity event in Europe and one of its kind in the world. The conference	ED

		most important strategic challenges regarding cybersecurity and an EXPO dedicated to the cyber industry in Poland, Europe and the world	will include discussion panels and workshops with the participation of high-ranking representatives of international institutions and organisations, public administration and the private sector. The formats will be devoted to the most important cybersecurity problems, such as the issue of international cooperation during the crisis, the role of cyberspace in modern warfare, the security of digital infrastructure, the use of artificial intelligence for the public good, or the development of 6G technology.	
3	2024 IEEE International Conference on Cyber-Security and Resilience (IEEE CSR)	The conference focuses on theoretical and practical aspects of the security, privacy, trust, and resilience of networks, systems, and services as well as novel ways for dealing with their vulnerabilities and mitigating sophisticated cyber-attacks	The conference is expected to address a wide audience of cyber-security stakeholders including academics, research engineers from industry and academia, (PhD) students, and security professionals	ED/CYEN
4	International Conference on Cybersecurity, Situational Awareness and Social Media (Cyber Science 2024)	The International Conference on Cybersecurity, Situational Awareness and Social Media (Cyber Science 2024) is a multidisciplinary conference. It brings academics, researchers, practitioners and participants together to share and discuss new and emerging ideas, concepts and research outcomes. The conference focuses in advancing the principles, methods and applications of cybersecurity, situational awareness and social media.	This multidisciplinary conference will be featuring notable keynote speakers from industry, academia, and government. These experts will discuss topical and emerging topics ranging from Multidisciplinary and Multidimensional Cybersecurity, Ethical and Responsible use of Artificial Intelligence (AI), Cyber Insurance, Cyber Situational Awareness, Resilience and Government Security to Blockchain Regulation & Environmental, Social and Governance (ESG).	ED
5	IEEE International Conference on CYBER Technology	IEEE-CYBER is sponsored by IEEE Robotics & Automation Society focusing on the advanced Cyber techniques in automation, control, and intelligent cyber systems.	The main conference topics are (but are not limited to): a) CPS / Industrial Intelligence, b) Modelling / Control / Optimization / Automation, c) Robotics / Unmanned Systems, d) Internet of Things/Digital Twins, e) Sensors / Measurement, f) Carbon Peaking and Neutrality/Energy Systems	ED
6	IEEE Conference on Big Data 2024	In recent years, "Big Data" has become a new ubiquitous term. Big Data is transforming science, engineering, medicine, healthcare, finance, business, and ultimately our society itself. The IEEE Big Data conference series started in 2013 has established itself as the top tier research conference in Big Data.	Within the IEEE Big Data, the workshop in cyber threat intelligence and hunting is organized for the last 7 years from University of Oslo and has become one major avenue for EU and other international entities to disseminate novel research. In cybersecurity.	CYEN

7.7.2.1 Technical factsheets

Each of the three pilots planned in NG-SOC (i.e., banking, energy, academia and research sectors) will develop factsheets with information about successful application and implementation of the project solutions. The factsheets, provided in English and in native language of the demonstration host country, will be updated regularly and will be used to demonstrate the project's progress and to promote the technological benefits of the NG-SOC platform to the interested/involved stakeholders. Technical factsheets will be available on the project's website and will also be promoted through the social media, online trade news sites, and relevant information portals.

7.7.3 Project Synergies and other Targeted Initiatives

NG-SOC will identify European projects related to cyber security, threat intelligence, situational awareness, cybersecurity resilience, cybersecurity and preparedness training (please find an indicative list in Table 12). For clustering with other projects and stakeholders, the reference point of communication will be the project website and the social media channels, which will drive the clustering activities. This will allow for finding synergies with other projects to establish cluster participation in events and publications, as well as to multiply the dissemination potential of the public website and social media by sharing news and links. These synergies are empowered by the commitment of the partners to disseminate NG-SOC in other H2020 projects.

Research on similar and relevant projects which have been funded under H2020 program leads to a preliminary list of projects NG-SOC can potentially start a collaboration with.

Table 12. Related European projects

Project Acronym	Project name	Website	Short Description	Coordinator
PANDORA	Cyber Defence Platform for Real-time Threat Hunting, Incident Response and Information Sharing	Link	The PANDORA project aims at contributing to EU cyber defence capacity building, by designing and implementing an open technical solution for real-time threat hunting and incident response, focusing on endpoint protection, as well as information sharing.	Space Hellas
AINCEPTION	AI Framework for Improving Cyber Defence Operations	Link	AInception main aim is to develop novel AI-based tools and techniques for detection and response: from detecting adversarial behaviour from logs and network traffic; to understanding, contextualizing and explaining the detected threat; to generating risk and impact aware response action; all the way to automating the execution and evaluation of the response action on the underlying infrastructure. AI will play a central role for all these steps in the AInception tool pipeline. These tools will be combined into a proof-of-concept end to-end detection and response prototype, evaluated in operational scenarios with end users.	Space Hellas
ACTING	Advanced European platform and network of Cybersecurity training and exercises centres	Link	The project “Advanced European platform and network of Cybersecurity training and exercises centres” (ACTING) will develop a network of advanced interconnected (federated) domain oriented cyber ranges for training and exercises. It aims to incorporate sophisticated methods and techniques for simulation of users, analysis of the performance of the cyber operators, and scoring cyber security situational awareness	Bulgarian Defence Institute - Professor Tsvetan Lazarov
PRIVATEER	Privacy-first Security Enablers for 6G Networks	Link	Ensuring security, whether of your home or your data network, requires disclosing certain information to third parties. The more complicated the system to be protected, the more opportunities or needs arise for sharing critical pieces of information. Working under the philosophy that intrusive security is no longer acceptable in the 6G environment, the EU-funded PRIVATEER project will pave the way for 6G ‘privacy-first security’. It will study, design and develop innovative security enablers for 6G networks following a privacy-by-design approach. The enablers will complement and be compatible with standard 5G/6G security controls to achieve a holistic, privacy-friendly security solution for future networks	Space Hellas
SEPTON	Network security for medical devices	Link	Networked medical devices, including life-supporting or sustaining devices such as pacemakers, patient monitors and infusion pumps have played a transformational role in healthcare. At the same time, they are vulnerable to hacking and unauthorised access, potentially compromising patient safety. As such, there is an unmet need to address such security risks and safeguard patient health information and safety. The EU-funded SEPTON project aims to develop a cybersecurity toolkit capable of protecting networked medical devices. The approach will incorporate blockchain and machine learning techniques to allow for vulnerability assessment and improved data-exchange security. Results will be applicable in	Space Hellas

			hospitals and other healthcare centres	
DEGREES	Development and Evolution of the Greek Governmental Sector	Link	The project aims at the development of a new service, a cyber-physical platform that enhances the security over satellite public safety networks. DEGREES will introduce new services to support crisis management through a communication framework with reinforced security and increased reliability. The main goal of DEGREES is the study, design and assessment of a security system based on multiple technologies in order to protect space control ground stations and satellite links against cyber-attacks, and to activate intelligent reconfiguration mechanisms in case of failure or compromise concerning the ground stations networks and the satellite links	Space Hellas
PALANTIR	Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises	Link	The rapid advances in digital technology necessitate finding ways to ensure digital security and help small and medium-sized enterprises (SMEs) recover from cyberattacks. The EU-funded PALANTIR project aims to implement a framework combining privacy assurance, data protection, incident detection and recovery aspects. The project will also focus on cyber-resilience and ensure the SMEs' compliance with the relevant data privacy and protection regulations. The outcomes of the project will provide those enterprises with security tools that will boost their resilience at a reasonable cost.	DIADIKASIA Business Consulting S.A.
AI4CYBER	Artificial Intelligence for next generation CYBERsecurity	Link	Artificial intelligence (AI) has a big role to play in cybersecurity – good and bad. It can be a powerful mechanism to detect threats and protect systems against attacks. It can also be used by attackers as a weapon. In this context, the EU-funded AI4CYBER will provide an Ecosystem Framework of next-generation trustworthy cybersecurity services that leverage AI and Big Data technologies to support system developers and operators in effectively managing AI-powered cyberattacks. Specifically, it will develop a new breed of AI-driven software robustness and security testing services with smarter flaw identification and code-fixing automation. The project will focus on the energy and banking sectors, as well as hospital services.	FUNDACIÓN TECNALIA RESEARCH & INNOVATION
CitySCAPE	City-level Cyber-Secure Multimodal Transport Ecosystem	Link	EU-funded CitySCAPE project will improve cybersecurity within multimodal transport. The project will produce a modular software toolkit, whose purpose is fourfold. First, it will detect suspicious traffic and data flows. Second, it will evaluate the technical and financial impact of a cyber-attack. Third, it will enhance the predictability of zero-day attacks. Last but not least, it will train relevant authorities and improve the circulation of information among them.	I-SENSE RESEARCH GROUP of ICCS/NTUA
JCOP	Joint Cybersecurity Operations Platform	Link	JCOP is a prototypical implementation of Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, and a model that can be applied to all EU Member States. The project develops a Joint Cybersecurity Operations Platform (JCOP) tailored to the needs of EU Member State authorities entrusted with cybersecurity. The platform, as per the EU Recommendation 2017/1584, will enable (i) sharing threat situational awareness, (ii) performing coordinated incident response and (iii) preparedness through relevant and tailored training.	Technical University of Crete
PHOENi²X	A European Cyber Resilience Framework with Artificial Intelligence-assisted orchestration & automation for business continuity, incident response & information exchange	Link	PHOENi²X aims to design, develop, and deliver a Cyber Resilience Framework providing Artificial Intelligence (AI) - assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.	University of Patras
CYBERUNITY	Community for Integrating and Opening Cyber Range Infrastructures that Build an Interoperable Cross-Domain and Cross-Sector Cyber Range Federation	Link	CYBERUNITY main goal is to build an interoperable community of Cyber Ranges in Europe, initially by bringing together the cyber ranges owned and operated by the partners in the consortium, whilst “opening” the cyber range interoperability specifications for building and expanding a thriving community of cybersecurity experts, researchers and professionals. CYBERUNITY aims to contribute to the aim of making Europe a world leader, by developing open interoperability specifications and providing the first interoperable cyber range infrastructure. CYBERUNITY will deploy a secure	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU

			framework that enables cross-organisation and cross-border trustworthy and privacy-compliant integrated cyber range services, whose capabilities will be demonstrated by means of several cross-border scenarios involving systems in critical sectors.	
CY-TRUST	Cypriot Sectorial Security Operations Centres	Link	CY-TRUST aims to increase the capacity the Republic of Cyprus to defend its infrastructures & citizens from cyber threats, through the introduction of Sectorial Security Operations Centres (Sectorial SOCs), covering 4 sectors (including Energy, Maritime, Governmental & SMEs), that will be interconnected with the National Competent Authority entrusted with cyber security, the Digital Security Authority (DSA) of Cyprus. This effort will follow and adopt a recently proposed Cyber Security Operations Centres (CSOCs) Blueprint for cross-border, cross-organisational, and cross-functional cooperation, collaboration, and coordination, combining capacity for shared situational awareness, coordinated incident handling, and joint preparedness.	ARCHI PSIFIAKIS ASFALEIAS - DIGITAL SECURITY AUTHORITY
SYNAPSE	An Integrated Cyber Security Risk & Resilience Management Platform, With Holistic Situational Awareness, Incident Response & Preparedness Capabilities	Link	SYNAPSE aims to design, develop & deliver an Integrated Cyber Security Risk & Resilience Management Platform, with holistic Situational Awareness, Incident Response & Preparedness capabilities.	CONSIGLIO NAZIONALE DELLE RICERCHE
C-SOC	Cretan Security Operations Center	Link	C-SOC proposes the development of such a Security Operation Center in the island of Crete. Supported by FORTH, one of the leading Research Centres in the area of Cybersecurity, C-SOC (i) will use advanced AI approaches to detect even weak signals of attacks and (ii) will capitalize on the more than 60,000 IP addresses available to FORTH in order to build an effective “network telescope”. Using a multi-phase expansion plan, C-SOC will first offer its services to FORTH, and then expand to SMEs at the Science and Technology Park (second phase), and then to SMEs in Crete (third phase).	IDRYMA TECHNOLOGIAS KAI EREVNAS

7.7.4 Standardisation Activities

An important part of NG-SOC is to make a wider contribution to the cybersecurity landscape, beyond the platform, and deliver roadmap that aims to establish a wider set of certifications and standards. Such standardization activities will involve engaging with organisations and events relevant to establishing standards for cyber-resilience across Europe. This may involve contacting and working with organisations such as ENISA, FIRST, ITU, CEN-CENELEC, and OASIS. NG-SOC will specifically monitor, contribute to, and incorporate cyber security standards relevant to critical infrastructure domains and sectors and seek input and feedback on the roadmap throughout its development. It is worth noting that NG-SOC already contributes to different standardization activities such as STIX & TAXII, OpenC2, CACAO, and the TAC ontology.

7.7.5 Individual Partner Plans

This section presents in individual partner’s dissemination and communications plans; each plan is in-line with the related partner’s expertise, capability, and commitment to the project. ED, being the leader of WP7, overseas all communication and dissemination activities and ensures that the individual plans will be treated in respect.

7.7.5.1 EUROPEAN DYNAMICS (ED)

During the first three months of the project, ED developed the first communication results including the NG-SOC project logo, general designs, templates and the overall project identity which were agreed among all partners. Furthermore, social media accounts (Twitter and LinkedIn) were launched.

To maximize the impact of the NG-SOC project, ED will develop a clear definition of target values, target audiences, key messages, channels and communication tools. ED is very active in the provision of IT and commercial solutions in the private and public sector offering –among others– services for the professional community of Governments services and Security, thus participating in related events, conferences, fairs, and workshops. ED will disseminate the project results through its channels/ networks with its extensive expertise in disseminating project results. NG-SOC, through these channels, will be presented to both commercial as well as research stakeholders thus creating a more "adapted awareness" regarding the functionalities and technologies the solution offers. ED plans to participate in conferences, exhibitions, events and workshops relevant to NG-SOC and to author articles and journal publications presenting the outcomes of the project and the innovations related to the development of the modules that ED is responsible for, and the project as a whole. Furthermore, ED will draw on its networks consisting of current and former proposal and project partners to create a) awareness for the NG-SOC project and b) networks between related projects by connecting the social media channels and promoting the exchange and setting up of links between websites of sister projects. In addition to highlighting the project on the company's website, ED will present the NG-SOC project in internal meetings of other projects in order to explore potential synergies. ED will also highlight NG-SOC project during national and European events where the company is represented – such as the ICT Proposers Days, the Security Research Event in Brussels or national events. Dissemination to related Business Interest Groups, namely ICT applications suppliers and Industrial Community (Technological domain), will be produced, demonstrating that NG-SOC can easily be the basis for many other applications for other target groups and even other application domains.

7.7.5.2 INSIGHIO (INS)

INS is an IoT company with end-to-end hardware & software solutions; therefore, the cybersecurity domain is a new opportunity for dissemination and communications of the company's solution portfolio – focusing on its risk and trust assessment methodologies and tools. Through NG-SOC, INS is introduced to the consortium, which is comprised of both commercial and research stakeholders. INS will pursue close collaboration with the partners by integrating their open and acclaimed solutions. INS will investigate its participation in open projects (e.g., oasis-open.org) with new extensions and integration of existing tools. INS will attempt to exploit all communication channels provided by NG-SOC to reach larger audiences. INS will pursue the publication of the scientific results through articles, journals, and publications in conference proceedings with the cooperation and guidance of UPRC. Generally, INS employs a dissemination strategy that involves engaging in pertinent conferences, exhibitions, events, and workshops promoting NG-SOC results. INS will promote NG-SOC through the company's website and use the LinkedIn platform to inform its connections of new developments with the purpose of triggering new collaborations.

7.7.5.3 University of Piraeus Research Center (UPRC)

UPRC participates in several events, conferences, and workshops. Through those, UPRC will disseminate the project results and organise NG-SOC-specific sessions to promote the project results. Furthermore, members of the UPRC team will author scientific papers that will be submitted to conferences and journals, presenting the outcomes of the project and the innovations related to the development of the modules that UPRC is responsible for, as well as the project as a whole. Furthermore, UPRC will raise awareness for the NG-SOC project through its network, which consists of current and former proposals and project partners.

7.7.5.4 SPACE HELLAS (SPH)

NG-SOC will be introduced to both commercial and research stakeholders through these channels, fostering a deeper understanding of the solution's functionalities and technologies. SPH's dissemination strategy includes participation in relevant conferences, exhibitions, events, and workshops related to NG-SOC. Additionally, SPH will contribute to articles and journal publications showcasing the project's outcomes and innovations in module development, both independently and as part of the overall project. Moreover, SPH will utilize its network of current and past proposal and project partners to raise awareness of the NG-SOC project and facilitate connections between related initiatives through social media promotion and corporate website linkage. The project will be featured on the company's website and highlighted in internal meetings of other projects to explore potential collaborations. Dissemination efforts will extend to relevant Business Interest Groups, including ICT application suppliers, cybersecurity solutions' vendors belonging to the collaborators' network of SPH and clients of the company's SOC-managed services provision. In this regard, the versatility of NG-SOC will be demonstrated for various applications and target groups across different domains.

7.7.5.5 CYENTIFIC AS (CYEN)

CYEN will disseminate and communicate NG-SOC results in various contexts, including journals and scientific and industry conferences and workshops, special interest groups such as the FIRST Automation SIG and the ENISA ad hoc working groups on cyber threat landscapes and security operations centres, standards developing organizations like OASIS and ITU and in particular in the context of the standards we are actively supporting and utilizing, international interoperability plugfests such as the well-known cybersecurity automation village organised annually in the US., other EU projects related to NG-SOC such as CY-TRUST, social media as we have a tremendous following, and ad-hoc presentations and discussions to the extensive network we have established, including EU governmental entities, national and sectorial security authorities, MSSPs, small organizations and SMEs, large organizations and critical infrastructure operators, and policymakers.

7.7.5.6 CAIXABANK SA (CXB)

CXB participates in several events, conferences, and workshops, especially related to the finance sector. As mentioned before, CXB is a member of several groups (ESBG -European Savings and Retail Bank Group-, ENISA's Financial experts Working Group, FI-ISAC, EPC -Payment Security Support Group and Card Fraud Prevention-, etc.). Through these different forums, CXB will disseminate the overall project, promoting NG-SOC as a holistic approach, project tools, results, and potential benefits. It will also participate in and organize internal and external training sessions and workshops to raise awareness for the NG-SOC project and showcase the potential benefits of the project in the short-, mid-, and long-term for SOCs.

7.7.5.7 Cyprus Research and Academic Network (CYNET)

CYNET participates in several events, conferences, and workshops. Through those, CYNET will disseminate the overall project and will organize training sessions/events promoting NG-SOC as a holistic approach and project. Finally, CYNET will raise awareness for the NG-SOC project through its network consisting of current and former partners and network community.

7.8 Communication Plan

A series of communication actions are planned to enhance the project visibility and to raise awareness of the NG-SOC activities and results for the EU society at large.

The aim to raise public awareness and ensure maximum visibility of the project's key facts, objectives, activities, and findings is well connected with the success of the project and the creation of the grounding conditions for the future take-up of the project's SOC services and the dedicated training sessions and educational programmes in the market. Communication channels will be used to announce and promote NG-SOC activities and events to maximize the expected attendance and the potential for stakeholders' engagement, effectively supporting and promoting the project's results. The communication element involves all consortium partners and their respective staff. There is awareness that communication is a continuous process, not a one-time effort, when the project ends since one of the main targets is to ensure the project's sustainability in the long term.

ED will set up the most appropriate mechanisms and tools for maximum visibility and impact, ensuring that all partners contribute to communication activities and assess the communication results. The following list summarizes the selected communication actions, along with the respective timings:

- **Logo and graphic identity:** Development of the project logo and visual identity (M1), Preparation of templates for deliverables, reports, presentations, etc. (M2)
- **Printed material:** Production and distribution of project communication materials: project flyers (M6, M24) and poster (M7, M24), pilot factsheets for each use-case to proclaim the pilot outcomes (could be created both in English and in the local languages) (M36)
- **Videos:** Creation of two info-graphics videos (M12 & M24)
- **Newsletters:** Production of 6-month e-Newsletters (M6 – M36)
- **Website:** Creation & Management of the website (M1 – M36)
- **Social media:** Update and management of the social networks, project LinkedIn group, and Twitter accounts (M4 – M36)
- **Assessment and reorientation of communication activities:** Assessment of the project communication and dissemination activities (M12, M24), re-organization of the communication and dissemination strategy (M12, M24)

7.8.1 Communication Tools

7.8.1.1 Visual Identity and Project Logo

The NG-SOC project will build a strong project identity through effective branding and delivering clear messages to a variety of target audiences. To this end, a project logo, project templates, and a dedicated brand book (brand guidelines) were created to establish a consistent appearance that will be used throughout the whole project duration in all applicable communication and dissemination channels (website, poster, templates, and presentations). This is the most effective way to ensure that a consistent identity of NG-SOC is widely communicated.

A dedicated logo has been agreed upon by the project partners and will serve as a trademark, promoting instant public recognition and triggering reactions from the viewers even from the early stage of communication and dissemination activities. NG-SOC's logo was chosen to be simple, easily recognizable, and self-explanatory so that people could immediately understand the main idea of the project. The logo mainly uses:

- Green; symbolizing growth, safety, and protection.
- Black; signifying **sophistication, power, and authority**. It can also represent **seriousness and secrecy**, which are relevant to the cybersecurity domain.
- White; representing **purity, cleanliness, and transparency** and is used to balance out darker colours like black or green and add a sense of **openness**.

Iconography, depicts the **SOC** as a brain, with the **lines and dots representing the various components and connections within the SOC**. These components can include security tools, data feeds, and personnel. The connections between these components represent the flow of information, processes, and communications within the SOC. Therefore, the image metaphorically conveys the idea of a SOC as a complex and interconnected system that works together to effectively detect, analyse, and respond to security threats.

NGSOC
Next Generation Security Operations Centres
NGSOC
Next Generation Security Operations Centres

Figure 6. NG-SOC Logo

Furthermore, the primary colours used in the logo variations and the dissemination and communication material, as well as the fonts used, are listed in Table 13.

Table 13. NG-SOC main colour scheme, body and headline font (Google Free Font)

🟩	rgb(49, 137, 140) HEX #31898C CMYK 36/1/0/45	**Typography** Calibri **Designer:** Luc(as) De Groot ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 1234567890~!@#$%^&*(){[}]’”? The quick brown fox jumps over the lazy dog. *The quick brown fox jumps over the lazy dog.* **The quick brown fox jumps over the lazy dog.**
🟩	rgb(118, 198, 200) HEX #76C6C8 CMYK 32/1/0/22	
🟩	rgb(136, 208, 132) HEX #88D084 CMYK 28/0/30/18	

7.8.1.2 Project Website

The project's website is one of the most important communication channels, and it will serve as a key element of engagement with the identified key audiences. The website will present the project's general description, objectives and impact, partners, events, and news.

At M3, the website http://ng-soc.eu was made publicly available and will be continuously updated with all the NG-SOC latest news, events, and publications.

The structure (sitemap) of the website is designed to provide visitors with immediate access to all public information about the project. For the visitors’ convenience, almost all subpages of the website are accessible from the main page with respective quick links. Moreover, links to the social media accounts (LinkedIn and Twitter), amplifying the branding of the project, are available on the Home Page of the website.

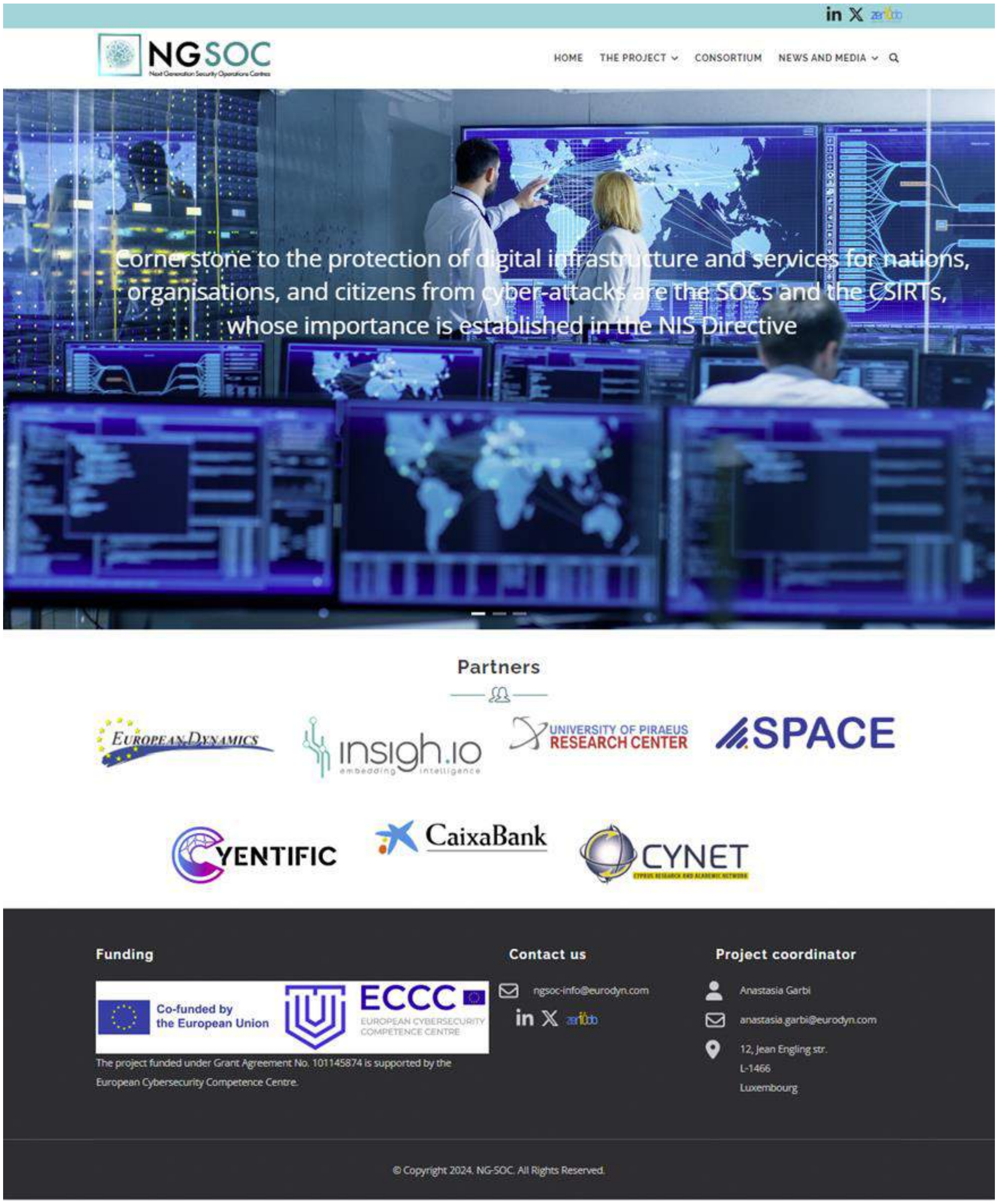
ACTION PLAN

At M1 ED drafted specifications for website development and started implementing the strategy. At M2, the project website is implemented, and since M3 it is publicly available.

Search Engine optimization (SEO) parameters and web statistics were performed and planned to be regularly analysed to drive more visits to the NG-SOC website.

M2-M36: the website is enriched with content by all partners, in line with the project progress and the achievement of results and is regularly updated. It also shows recent tweets connected or addressed to the NG-SOC Twitter.

From M36 onwards: the website is maintained beyond the end of the project lifetime by ED.


HOME
THE PROJECT
CONSORTIUM
NEWS AND MEDIA
Partners
EUROPEAN DYNAMICS
insigh.io
UNIVERSITY OF PIRAEUS RESEARCH CENTER
SPACE
CYENTIFIC
CaixaBank
CYNET
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cornerstone to the protection of digital infrastructure and services for nations, organisations, and citizens from cyber-attacks are the SOCs and the CSIRTs, whose importance is established in the NIS Directive

Funding

The project funded under Grant Agreement No. 101145874 is supported by the European Cybersecurity Competence Centre.

Contact us

ngsoc-info@eurodyn.com

Project coordinator

Anastasia Garbi

anastasia.garbi@eurodyn.com

12, Jean Engling str.
L-1466
Luxembourg

© Copyright 2024. NG-SOC. All Rights Reserved.

Figure 7. NG-SOG Website Homepage

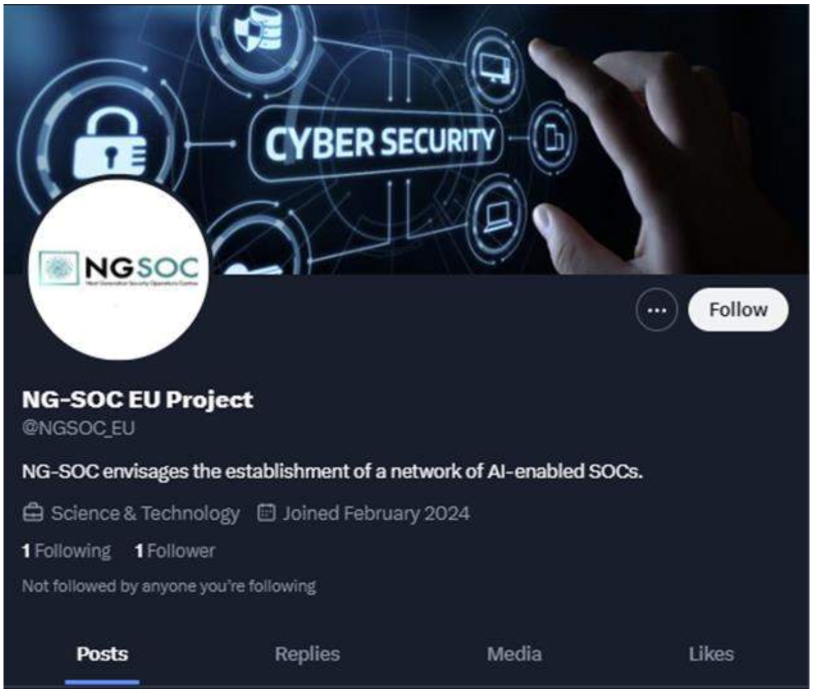
7.8.1.3 Social media

Social media has become ubiquitous and instrumental for communication, networking, and content sharing purposes. Successful social media activities will help NG-SOC to increase its visibility and maximise its potential outreach specially to get the maximum reach. Therefore, NG-SOC will actively engage in social media as a channel for communication of the project idea and outcomes as well as for interaction with target audiences.

From M2, the NG-SOC is present in 2 social networks, LinkedIn and Twitter.

7.8.1.3.1 Twitter

Twitter is one of the two social networking platforms that are used in this project and is ideal for spreading news and engaging with users in real-time. @NGSOC_EU interacts with relevant accounts and promotes the project's vision and progress.



NG-SOC EU Project
@NGSOC_EU

NG-SOC envisages the establishment of a network of AI-enabled SOCs.

Science & Technology Joined February 2024

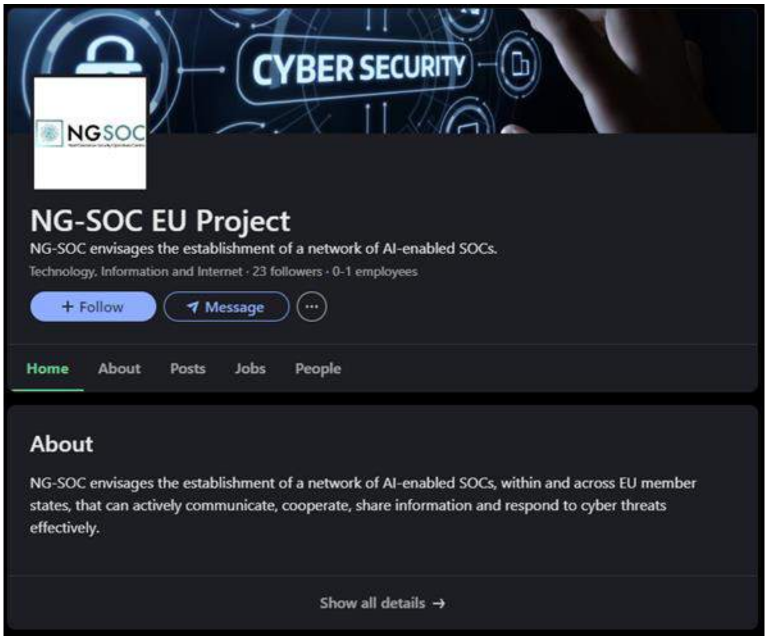
1 Following 1 Follower

Not followed by anyone you're following

Figure 8. NG-SOC Twitter Account

7.8.1.3.2 LinkedIn

LinkedIn is the most popular professional network on the internet. Registered members can establish connections with professionals who are in their interest and interact in group discussions. A LinkedIn account has also been set up under @NG-SOC EU Project and is continuously updated with the latest news, events, and deliverables. The @NG-SOC EU Project account will enable to build a strong network with some of the project's key audiences, such as research institutes, industry, policymakers, ESCOs, banks, and individuals involved in the technology, information, and Internet.



NG-SOC EU Project

NG-SOC envisages the establishment of a network of AI-enabled SOCs.

Technology, Information and Internet · 23 followers · 0-1 employees

About

NG-SOC envisages the establishment of a network of AI-enabled SOCs, within and across EU member states, that can actively communicate, cooperate, share information and respond to cyber threats effectively.

Figure 9. NC-SOC LinkedIn Account

7.8.1.3.3 Hashtags

All NG-SOC posts include specific hashtags to connect social media content to the right topic, event, theme or conversation. They also make it easier to make posts more discoverable around those specific topics, since they aggregate all social media content with that same hashtag. The usage of specific hashtags will help to increase the post's visibility and the followers' engagement with the posts.

The hashtags used are #eu, #cybersecurity #dep, #ng-soc, #technology, #information, #cybersecurityawareculture, #AI, #EUCyber.

<u>**ACTION PLAN**</u>

M2-M36: All four social media accounts are continuously updated with posts about project news, events, major updates and the project’s overall progress.

7.8.1.4 Newsletters

Newsletters are another communication channel which aims at providing the project stakeholders and the general audience with information related to the project activities. Disseminating the project results using Newsletters will further raise the awareness of the audiences and at the same time will increase the communication impact. Newsletter will be made available both in printed and electronic form.

<u>**ACTION PLAN**</u>

A project newsletter template will be produced at M6 to promote the key concepts and messages of NG-SOC, including clear and appealing infographics.

7.8.1.5 Press releases and articles

Digital press releases and articles are established as an effective mechanism to promote the NG-SOC outcomes and create awareness and familiarity with the project topic, objectives and results at national (in pilot countries) and at European level.

<u>**ACTION PLAN**</u>

NG-SOC consortium plans to contact media mainly through press releases to raise awareness about the project and its goals. These will be released at every major milestone, development, and result of the project.

Regional media could also be reached through members involved in demo processes.

Approaching each milestone as part of a bigger story is a must to raise the media's attention, create a presence on these channels, and reach the target groups.

Approximately 15 articles and press releases will be published in several media throughout the project's course.

Articles: ED plans to address several mass media specialized on the NG-SOC theme, and all demo leaders will find national channels in pilot countries for sharing NG-SOC content and translating the press releases into their local languages.

Press releases: Press releases published will be based on the following topics:

- Press release #1: At M4, indicating the project's start.
- Press release #2: At M14, announcing the pilots' start.
- Press release #3: At M36, sharing the project's end, along with its results.

7.8.1.6 Media Kit

A set of promotional materials for the project will be developed and distributed through various mass media channels for publicity use. This media kit will be designed by ED and will include project flyers/leaflets/ brochures, and a poster that will allow the project consortium to reach a large audience over a short period of time. These releases will be distributed, e.g., promotional project flyers for the large non-specialist community as well as for the community of relevant stakeholders. Print-outs will be distributed to partners' institutions (to be further distributed through their networks and channels) and at public events. Leaflets will describe the project and its main features, timeline, contact information, and expected outcomes to the general public in an easily understandable way. The flyers are intended for distribution during banking, energy, and academia sector events, where NG-SOC core partners are involved as organisers or co-organisers, as well as online, and to communicate the project concept in a comprehensible manner.

ACTION PLAN

A project flyer/leaflet/brochure will be produced at M6 to promote the key concepts and messages of NG-SOC, including clear and appealing infographics to be distributed on the web (social media, communities, partners' networks, external blogs, etc.). Revised versions will be prepared at M24.

The project flyers/leaflets/ brochures will be uploaded in electronic format onto the project website in order to be easily downloaded and publicly shared.

Partners will send electronic copies to relevant contacts to enhance the project visibility and promote the NG-SOC contributions.

7.8.1.7 Other Channels

Promo videos, webcasts, podcasts, and presentations will be developed to present the NG-SOC project to the public in an easily understandable way. A YouTube channel will be created, where the Consortium will plan short series of white board videos/animations to explain the role and the goals of the NG-SOC project in a focused and digestible way for all targeted stakeholder groups. Furthermore, presentations will be offered at local level (aiming at all target groups) during the project lifetime and towards the end of the project to present the project results to policy makers and potential investors. Research-active partners will create awareness of NG-SOC at research level, presenting the project findings to the engineers and scientists of the future through lectures and seminars for undergraduate and postgraduate students and academics. Special focus will be made in identifying and promoting opportunities for innovation and entrepreneurship that encourage uptake by groups that are under-represented in the cyber-security sector across Europe.

ACTION PLAN

ED will prepare an initial script for the video, from use cases perspective.

ED will design a video at M12 and then at M18 to highlight the project's objectives, outcomes, case studies, etc. to wider audience. Partners will validate the content of the videos.

ALL partners will disseminate the videos among the NG-SOC network of contacts. ED will create a NG-SOC YouTube channel, where all the videos will be uploaded to. ED will also share the videos on the project website to make them accessible to the public.

Partners will promote these videos through their respective contact lists and networks.

7.8.1.8 Project Publications

The NG-SOC partners will work towards the preparation of publications that will illustrate project results, in open access peer-reviewed journals and magazines. They will be prepared each time the project has key findings to disseminate. In addition, project partners will possibly contribute to e-Journals, blogs and newsletters targeting a larger public with shorter articles and news, as well as to policy-oriented publications to enhance project outreach to policymakers. Those publications will be based on the results of the activities, including but not limited to development guides, study reports, recommendations, lessons learnt and event outcomes. Like specific deliverables, publications may only contain non-confidential and non-classified information.

Within the NG-SOC project an active publication and dissemination strategy is envisaged, including all results related to the derivation of resilience indicators from big and open data. Open access will be provided to publications covering NG-SOC and featuring in news sources, peer-reviewed journals, etc. Open access provision will be achieved through publication in open access publications, publication via the 'gold' route, whereby authors pay a fee to the journal to publish the material as open access immediately or publication via the green route. The decision will be based on the publisher selected, the article and the partners who have contributed to the publication. The consortium has allocated budget to cover the cost of gold open access publishing. In terms of the green route, the consortium members have agreed that the material will be deposited immediately upon publication and that the article will be open for access after the shortest embargo period allowed by the respective publication. The contributing partners will agree embargo periods with the publisher upon acceptance of the article. The Zenodo repository will be used as a default for publications using the green route, unless a more specific repository is assessed by the consortium as being more suitable for the material and/or is more consistent with the partner's institutional norms and requirements. NG-SOC deliverables will also be deposited in Zenodo at the close of the project to maximize their reach and ensure their preservation.

A preliminary list of key targeted journals for publications currently identified is provided in Table 9.

7.9 Expected Impact

Table 14. Targets of the dissemination and communication activities

WP – Activities	Performance Indicator	Framework for Metrics	Target Values
WP7 – Project Impact and cybersecurity culture awareness	7-1 Dissemination, communication and awareness raising activities	• Visibility of the public NG-SOC website	Website ready by M03 Approximately 2000 visitors per year, 900 downloads per year
		• Number of articles, and press releases and journal publications	>10
		• Number of news items presented on the website and other social media	≥ 15 per year
		• Number of presentations (in external events i.e. symposiums, meetings, conferences)	>8
		• Number of # hashtag used on Twitter	1200
		• Number of followers on LinkedIn	600
		• Online presence in social media channels such as LinkedIn, Twitter, spreading news about the project	>1000 stakeholders >200 monthly impressions
		• Multimedia video podcasts presenting the project, its innovation, and its key outcomes	>3 videos produced >2.000 views in YouTube
		• Number of Thematic Workshops Organisation	>3
		• Number of Cluster of European projects and other initiatives	>5
		• E-newsletters	>6 newsletters >1000 contacts reached >30% opening rate
		• Brochures, leaflets, flyers in events, roll-up banners, posters, also available online for printing through the project's website	>2.000 printed copies distributed >4 roll-up banners/posters
		• Promotion of periodic non-technical reports (publications) to fora and blogs to create awareness on NG-SOC potential and features	>5 publications to blogs >5 blogs/for a to post

7.10 Implementation of the Dissemination and Communication Plan

7.10.1 Roadmap and preliminary action plan

A communication roadmap will be determined for the whole duration of the project. At M4, ED will create a communication plan template, which will be distributed to all NG-SOC partners, in order to fill in all their planned dissemination activities until M12. This action will be repeated at M10, M16, M22, M28 and M34 of the project (every six months), to have a complete and successful communication of the project and reach the targeted KPIs.

7.10.2 Dissemination Procedures

The participation of consortium partners in any event with an opportunity for dissemination and promotion of (conferences, workshops, etc.), as well as the performance of every dissemination activity related to NG-SOC (presentations, paper submissions, material distribution etc.), has to be communicated beforehand to the Dissemination Manager in order to ensure high-quality publications, presentations and other communication material, avoid overlaps and possible disclosure of restricted or confidential information and lastly, monitor and record the project's communication and dissemination activities and their impact in an effective way.

7.10.3 Acknowledgement of EU Funding

There are three types of acknowledgments that must be added depending on the type of materials produced. Beneficiaries must use for: (a) communication activities of the beneficiaries related to the action; (b) dissemination activities; and (c) any infrastructure, equipment, vehicles, supplies or major result funded:

- The European Union’s flag and funding statement “Co-funded by the European Union” to download at this link and follow the operational guidelines for EU funding recipients at this link.
- The European Cybersecurity Competence Centre’s special logo to download at this link and acknowledge the ECCC as granting authority.

Please consider the indicative examples below:

Co-funded by
the European Union
ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

“The project funded under Grant Agreement No. 101145874 is supported by the European Cybersecurity Competence Centre”

- Beneficiaries must also use for (a) communication activities of the beneficiaries related to the action; and (b) dissemination activities, the following disclaimer (translated into local languages where appropriate)[6]:
  - “Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European

[6] DEP Model Grant Agreement Art 17.3 and relevant reference in Grant Agreement. (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/agr-contr/mga_dep_en.pdf)

Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.”

- For infrastructure, equipment and major results, please add the European Union’s flag and the following sentence:
    - “This [infrastructure] [equipment] [insert type of result] is part of the NG-SOC project. This project is co-funded by the European Union under grant agreement No 101145874 and supported by the European Cybersecurity Competence Centre. Content reflects only the authors' view and neither the European Union nor the European Cybersecurity Competence Centre European Commission is responsible for any use that may be made of the information it contains."

8 Conclusion

This deliverable presented the initial Exploitation and Dissemination Plan for the NG-SOC project where the main objective is to a) identify and transform NG-SOC services and individual components into marketable products and b) produce the strategy and the plans for dissemination and communication. Regarding point a) the deliverable included an overview of possible exploitation routes and 3 exploitation phases which are structured and planned according to the predefined meta-activities: pre-marketing activities, exploitation ramp-up and market penetration. Regarding point b) this deliverable provided the list of dissemination and communication activities performed by the consortium during, primarily, the first project period, and what is defined for the next months of the project.

As an outline, NG-SOC platform has a huge exploitation potential both for increasing SOC teams' situational awareness and collaborative resilience as well as for cybersecurity training. Its biggest advantages include AI-enhanced technologies for effective prediction, detection, analysis, and response to threats, as well as realistic simulations and multi domain functionality in cybersecurity training.

Furthermore, there have been 10 identified key exploitable results, whose exploitation potential is expected to have either a commercial, social or a scientific value. These include software/applications that are represented as components in the NG-SOC architecture, followed by services represented as NG-SOC pen-testing, read-teaming, cybersecurity training and exercises, and lastly know how represented as sector specific (banking, energy, research and academia) use cases. Characterisation has been performed for each KER and focused among others, on innovativeness, target users and benefits for them, technical challenges, legal and IPR considerations, technological maturity, etc.

Additionally, 7 individual exploitation plans of all consortium partners described the results that are going to be exploited, market sector and customer segments, and preliminary plans for exploitation channels. IPR strategy has been initiated and both the foreground and background technologies have been identified. For the next step, NG-SOC will explore the possibilities to boost its impact via Horizon Results Booster.

All abovementioned aspects will be constantly monitored and through ongoing engagement, the consortium will also take the opportunity to jointly and continuously refine and improve the strategy until the end of the project. Therefore, as the project advances, any changes that may affect the exploitation strategy will be updated in the second iteration D12.12 “Exploitation plan (II)”, which is due in M36.

Finally, regarding dissemination and communication activities this deliverable provides the vision of the Consortium concerning the communication of the NG-SOC's outputs and will serve as the principal communications guide to how the project will disseminate findings and research to the target audience to raise awareness. NG-SOC partners are confident that the activities presented in this document will generate awareness of the issues addressed and the solutions offered by NG-SOC, thus paving the way (i) to achieve higher visibility and recognition from both industry and academia and (ii) to the successful exploitation and market uptake of the projects' results.

References

[1] "Glossary of the Funding and Tenders Portal - European Union" https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/glossary (accessed Jun. 21, 2021).

[2] DIGITAL-ECCC-2022-CYBER-B-03-SOC, "Projects funded under this topic", https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2022-cyber-b-03-soc (accessed on Feb. 22, 2024).

[3] NCP Flanders, "Evaluation completed - call DIGITAL-ECCC-2022-CYBER-B-03", https://ncpflanders.be/news/evaluation-completed-call-digital-eccc-2022-cyber-b-03 (accessed on Feb. 22, 2024).

[4] K. Ala-Mutka, "Dissemination and Exploitation in Horizon 2020", EC, https://ec.europa.eu/research/participants/data/ref/h2020/other/events/2017-03-01/8_result-dissemination-exploitation.pdf (accessed Feb. 23, 2024).

[5] HORIZON 2020 – WORK PROGRAMME 2014-2015, General Annexes, G. Technology readiness levels (TRL), https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf (accessed Feb. 26, 2024)

[6] "Intellectual property," Your Europe. https://europa.eu/youreurope/business/running-business/intellectual-property/index_en.htm (accessed Feb. 26, 2024).

[7] "Horizon Results Booster." https://www.horizonresultsbooster.eu/ (accessed Feb. 26, 2024).

[8] "Cybersecurity," Trust-ITServices, https://www.trust-itservices.com/ict-expertise/cybersecurity (accessed Feb. 26, 2024).

[9] "MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing" https://www.misp-project.org/ (accessed Mar. 12, 2024).

[10]"MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing" https://www.misp-project.org/ (accessed March. 12, 2024).

[11]OpenCTI, https://docs.opencti.io/latest/ (accessed Mar. 12, 2024).

[12]Structured Threat Information Expression (STIX™) https://oasis-open.github.io/cti-documentation/stix/intro.html (accessed Mar. 12, 2024).

[13]Trusted Automated Exchange of Intelligence Information (TAXII™), https://oasis-open.github.io/cti-documentation/taxii/intro.html (accessed Mar. 12, 2024).

[14] "MISP Default Feeds." https://www.misp-project.org/feeds/ (accessed Mar. 13, 2024).

[15]SpiderFoot https://github.com/smicallef/spiderfoot (accessed Mar. 13, 2024).

NGSOC

Next Generation Security Operations Centres

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874