Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101128052 is supported by the
European Cybersecurity Competence Centre

CYDERCO - CYber DEtection, Response and COllaboration

D7.1- Dissemination and Communication Plan

Deliverable date: 2024-01-31

Status: Released

Version: 01

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them

List of changes

Version	Date	Description	Author(s)
01	30.01.2024	First version	Eva Maia

Contributors

Role	Contributor's Name	Entity Name - Beneficiary
Deliverable Lead	Eva Maia	ISEP
Contributor	Catalina Popescu	Eviden Technologies SRL
Contributor	Mircea Avram	Eviden Technologies SRL
Contributor	Aljosa Pasic, Rodrigo Diaz Rodriguez	Atos Spain S.A.
Contributor	Isabel Praça	ISEP
Contributor	Christine DEMETER	DNSC
Contributor	Marius Duta	DNSC

Approvers

Entity Name - Beneficiary	Project Manager	Signature
Eviden Technologies SRL	Catalina Popescu	X Catalina-Mihaela Popescu Digitally signed by Catalina-Mihaela Popescu Date: 2024.01.31 13:36:21 +02'00'
Instituto Superior De Engenharia Do Porto	Isabel Praça	X Assinado por: Isabel Cecília Correia da Silva Praça Gomes Pereira Identificação: BI09480460 Data: 2024-01-31 às 09:57:05
Directoratul National De Securitate Cibernetica	Christine Demeter	Semnatar: Demeter Christine Data si ora semnarii: 31-01-2024 12:13:40 SERVICIUL DE TELECOMUNICAȚII SPECIALE ROMÂNIA X
Atos Spain SA	Rodrigo Diaz Rodriguez	X Rodrigo Diaz Rodriguez Digitally signed by Rodrigo Diaz Rodriguez Date: 2024.01.31 11:23:41 +01'00'

Contents

Glossary: Acronyms, Terms and Abbreviations

Acronyms

AI	Artificial Intelligence
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
EC	European Comission
EU	European Union
GA	Gant Agreement
IEEE	Institute of Electrical and Electronics Engineers
IPR	Intellectual Property Rights
RTO	Research and Technology Organisations
SOC	Security Operation Center
SME	Small and Medium-sized enterprises

Introduction

The threat landscape has been increasing exponentially as the adoption of new technologies such as IoT, Big Data, Cloud computing are expanding the attack surface and cyber criminals are becoming more organized.

CYDERCO project aims to develop, test, and validate two different platforms that will support and enhance the detection and response capabilities of relevant entities, including private and national SOC's, to fight against cyber threats that affect network and information systems across the European Union: Detection and Response HUB and Threat Intelligence Platform.

The Detection and Response hub includes 4 main building blocks that will provide detection of malicious activities and incidents at network and host level using both traditional detection techniques and advanced AI-based detection. The platform will be fast and flexible and should provide SOC engineers with the needed info to efficiently detect, triage, investigate and respond to threats.

The Threat Intelligence platform will provide SOC's with critical info about threat actors and their TTPs, IoCs, improving collaboration, efficiency and proactivity in dealing with cyber-attacks. It will securely share and analyze large data sets among entities dealing with cyber detection and threat analysis, always supporting the increased availability, quality, usability and interoperability of threat intelligence data among the entities. Using the platform and showing its efficiency CYDERCO aim to bridge cooperation between various cybersecurity communities.

Objectives

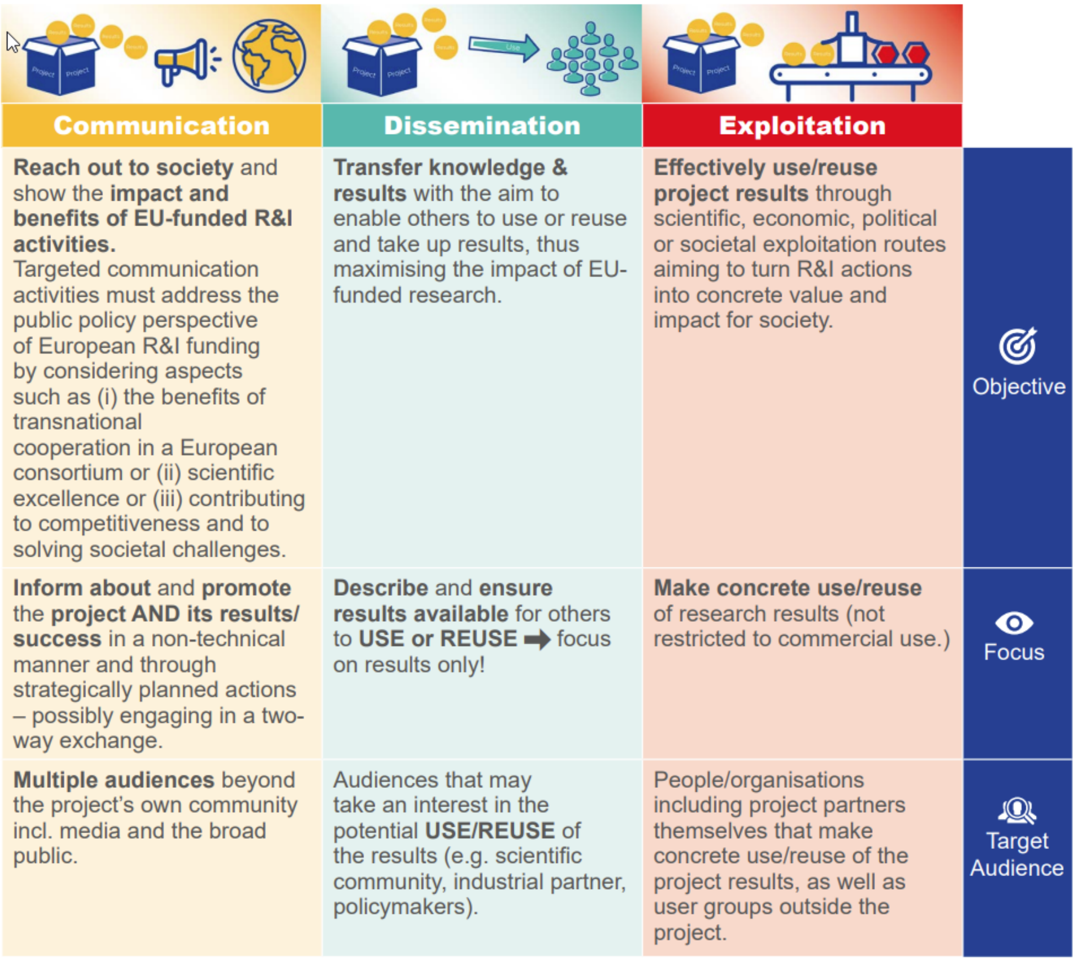
This document follows the definition of the communication, dissemination and exploitation provided by The European IPR Helpdesk for Horizon Europe projects[1]. Figure 1 summarizes the referred definitions.

The Gant Agreement (GA) sections pertaining to project exploitation, dissemination, and communication provide a very good basis for the planning. Consequently, this document leverages the GA content, incorporating updates where necessary. Specifically, it refines the selection of events and publications to reflect the latest information and delivers the initial version of pertinent dissemination materials. Tailored dissemination activities will be crafted for distinct audiences based on the primary groups of key end-users and stakeholders identified for results exploitation. This involves identifying and coordinating actions to:

- Engage end-users and influential figures representing industry, academia, responders, and policymakers.
- Ensure an optimal approach to enhance the project's visibility.
- Heighten awareness among attendees regarding the issues addressed by CYDERCO.
- Influence the development process by incorporating feedback from end-users and key representatives.

[1] European IP Helpdesk - Publications Office of the EU (europa.eu)

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them



Communication	Dissemination	Exploitation	
Reach out to society and show the **impact and benefits of EU-funded R&I activities.** Targeted communication activities must address the public policy perspective of European R&I funding by considering aspects such as (i) the benefits of transnational cooperation in a European consortium or (ii) scientific excellence or (iii) contributing to competitiveness and to solving societal challenges.	**Transfer knowledge & results** with the aim to enable others to use or reuse and take up results, thus maximising the impact of EU-funded research.	**Effectively use/reuse project results** through scientific, economic, political or societal exploitation routes aiming to turn R&I actions into concrete value and impact for society.	Objective
Inform about and **promote** the **project AND its results/ success** in a non-technical manner and through strategically planned actions – possibly engaging in a two-way exchange.	**Describe** and **ensure results available** for others to **USE or REUSE** ➡ focus on results only!	**Make concrete use/reuse** of research results (not restricted to commercial use.)	Focus
Multiple audiences beyond the project's own community incl. media and the broad public.	Audiences that may take an interest in the potential **USE/REUSE** of the results (e.g. scientific community, industrial partner, policymakers).	People/organisations including project partners themselves that make concrete use/reuse of the project results, as well as user groups outside the project.	Target Audience

Figure 1. Communication, dissemination and exploitation definition by The European IPR Helpdesk[2]

In the initial months, efforts will concentrate on preparatory activities, including:

- Identifying the most relevant dissemination channels and topics for publication.
- Establishing a timed roadmap for publication and dissemination events.
- Providing guidelines and rules for content approval and dissemination policy.
- Creating dissemination templates to guarantee a proper understanding of the project.
- Developing plans for event participation, publications, and the adaptation of communication channels.

[2] European IP Helpdesk - Publications Office of the EU (europa.eu)

Internal Communication and Dissemination Plan

In this section, a concise overview is provided of the internal communication strategy employed by the Consortium partners, aligning with the stipulations outlined in the project's Grant Agreement.

Dissemination Activities

Notification of all dissemination activities to other beneficiaries, unless otherwise agreed, must be made with a minimum lead time of **30 days**. This notification should be accompanied by adequate information regarding the results intended for dissemination. In the event that any partner perceives potential harm to their interests, they reserve the right to object within **20 days of receiving the notification**. Additionally, all partners are required **to facilitate open access to all peer-reviewed scientific publications** associated with their results.

The following outlines the standard procedure for implementing dissemination activities within the CYDERCO project, with a particular emphasis on the creation of scientific publications. It is important to note that this procedure is applicable to all forms of dissemination actions.

- Advanced notice of any scheduled dissemination action/publication must be provided to other partners a minimum of 30 calendar days before submission.
    - This information should be communicated through the project's mailing list, with the T7.1 leader copied.
    - Associated materials for dissemination should be uploaded to the document management and sharing platform, accompanied by all pertinent details about the dissemination action for the consortium.
- Objections to the planned dissemination action/publication should be raised within 20 calendar days of receiving the notice. If no objection is raised within this timeframe, the publication is considered approved.
- The specified notification and objection periods can be adjusted (including shortened) on a case-by-case basis, contingent upon obtaining consent from the Project Coordinator after a request from the partner responsible for the dissemination action/publication. Any modification to the notification/objection period must be justified.
- An objection is deemed justified if:
    - The protection of the objecting Party's Results or Background would be adversely affected.
    - The objecting Party's legitimate interests related to the Results or Background would be significantly harmed.
- The objection has to include a precise request for necessary modifications.
- The objecting Party can request a delay of the dissemination action/publication for up to 90 calendar days from the time the objection is raised. After 90 calendar days, the publication is allowed.
- Parties are prohibited from including another Party's Results or Background in any dissemination activity without obtaining the owning Party's prior written approval unless they are already published.

- Explicit acknowledgment of EC support is required:
  - Display the EU emblem.
  - Include the following text "*The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre*".
- A disclaimer excluding Agency responsibility needs to be included,
  - For convenience, the following example disclaimer is provided here: "*Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them"*
- An accepted copy of the publication should be sent to the project leader for the project archive and website.

The above list is for dissemination actions. For communication actions the general procedure is provided below.

Communication Activities

Partners unanimously agree to implement a "common-sense" policy for communication actions related to online presence. This policy is applicable to the project website, social media (SM) accounts, and individual partner websites/social media accounts. The following procedure will be observed:

- For communication materials solely derived from already approved dissemination materials (e.g., project standard materials), notification to the T7.1 leader is required, providing information solely on the communication effort.
- If the materials in question have the potential to raise security concerns, details about the planned communication effort must be initially communicated to the dissemination task leader (T7.1). The dissemination and exploitation work package leader (WP7) and the project coordinator should be copied on this communication. The purpose is to either gain clearance for content publication or determine whether the communication effort's content should:
  a) Be forwarded to the project Coordinator,
  b) Be submitted to the Security Advisory Board for clearance, or
  c) Follow the same procedure as dissemination activities, including partner notification and screening by the Security Advisory Board.

Communication activities should include information on EU funding and disclaimer excluding European Union and Granting Authority responsibility, as mentioned already for the dissemination actions:

- Include EU emblem
- For communication activities: "*This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101128052*".

- For infrastructure, vehicles, supplies or major result funded by the grant must acknowledge EU support and display the European flag (emblem) and funding statement (translated into local languages, where appropriate):
    - *"This [infrastructure][equipment][insert type of result] is part of a project that has received funding from the European Cybersecurity Competence Centre under Grant Agreement No. 101128052"*

External Communication and Dissemination Plan

Dissemination and communication activities are performed throughout the whole project duration, in different forms, e.g. scientific and industry publications, attendance to the conferences and events, organizing project awareness events etc. For that multiple dissemination and communication activities will be identified and organized to promote widest dissemination of knowledge from the project and engagement from the target audiences. Such dissemination opportunities will be constantly monitored in order to present CYDERCO project results as widely as possible.

The strategy is expanded in three directions towards:

1. Raising awareness and exchange of information. As well as ensuring maximum visibility of the project key facts, outputs and findings among different entities that can support cyber threat detection and CTI sharing;
2. Supporting transfer of project results and engagement from key stakeholders;
3. Increase the number of entities benefitting from the project outputs.

The strategy is structured into three main steps:

1. Creating synergies with relevant stakeholders and open-source communities;
2. Positioning CYDERCO at the intersection of technology communities and stakeholder groups; and
3. Use appropriate channels to reach target audience, disseminate results and communicate value proposition.

Target Audience and Stakeholders Group

Stakeholders are individuals or entities that have a vested interest in the project's outcomes, and their active involvement is crucial for the success and impact of CYDERCO initiatives. Therefore, it is crucial to identify the key stakeholder groups associated with CYDERCO project, providing insights into their roles, interests, and potential contributions. Understanding the dynamics of these groups will guide the development of communication strategies that foster collaboration, address concerns, and maximize the impact of our dissemination efforts. Moreover, recognizing the unique perspectives and expectations of each stakeholder group is vital for tailoring communication strategies that resonate effectively.

Table 1 provides an overview of CYDERCO's stakeholders groups, examining their potential benefits from the CYDERCO project and outlining the objectives and expected feedback from each group. By comprehensively addressing these needs and expectations of our diverse stakeholders, we aim to build strong partnerships, enhance project visibility, and ultimately drive the successful dissemination of our project's outcomes.

Table 1. Stakeholders Group Table

Stakeholder Groups	Key Message (How can they benefit from the project)	Objectives and expected feedback
Governments CSIRTs & CERTs	Security Tools, Detection & Response Platforms, Citizen Participation	DNSC will lead the direct engagement with CERTs. The team will promote sharing the project results and incorporating CERT partner feedback.
SMEs & Industry & End-users	CYDERCO framework	Project consortium will start discussions, explain the methodology and showcase the tools. Feedback will be gathered and considered for CYDERCO framework development.
RTO, University	New Publications and Patents	Get the results disseminated in the working groups that will then consider methodology and results while drafting future guidelines and standards
ENISA	ENISA aims to achieve a high common level of cybersecurity across Europe. Therefore, CYDERCO developments can actively contribute to the European Detection and Response capabilities.	ISEP will disseminate through AI Cybersecurity working group CYDERCO developments. Since the group is composed by highly skilled AI specialists, they can advise the CYDERCO developments, as well as use them to influence regulation and standards in the European cybersecurity field.
CLAIRE	CLAIRE seeks to strengthen European excellence in AI research and innovation. Therefore, AI developments in CYDERCO project will contribute to the innovation of AI in cybersecurity field.	ISEP will establish the connection with CLAIRE research network to spread the results of CYDERCO project.

Recognizing that different stakeholders have distinct preferences and communication styles, our strategies are designed to be adaptable and targeted. By understanding the preferences of each group, we can choose channels that optimize engagement and encourage meaningful interactions. Table 2 provides a concise overview of the different communication channels designated for each stakeholder group.

Table 2. CYDERCO's Communication Channels

Channel	Information to be shared	Targeted Audience
Working Groups	Methodology and early results will be disseminated in working groups, aiming at creating momentum on the approach that would finally result in a wider approach	Governments CSIRTs & CERTs SMEs & Industry & End-users RTO, University
Web communication: presence of CYDERCO with a project website and through presence on the social networks.	Project deliverables and publications are made regularly available to the general public through public channels	General Public
e-Newsletters and Email Campaigns	e-newsletters will provide a snapshot of main activities and achievements of CYDERCO, whereas broadcasting messages to a target pool of contact points via email is a highly effective measure of engagement, especially when promoting events and outcome among different domains.	Governments CSIRTs & CERTs SMEs & Industry & End-users RTO, University ENISA CLAIRE

Also, different dissemination channels were defined (Table 3). These channels serve as the conduits through which we share project updates, outcomes, and relevant information with our stakeholders. Hence, our dissemination channels are thoughtfully designed to be adaptable, ensuring that information reaches our audience through methods that resonate most effectively.

Table 3. CYDERCO's Dissemination Channels

Channel	Information to be shared	Targeted Audience
Cybersecurity conferences/journal	Participation and presentation at cybersecurity conferences aimed at informing about project results, methods, tools, etc	Security and Resilience Research Community
Participations to workshops and dissemination events	The consortium partners will present CYDERCO approach and results to workshops and event to further promote	Scientific and technical experts

	the project results and collect feedbacks to drive the next steps.	
Standards & Policies	CYDERCO aims at influencing standards and policy-making presenting project's results.	CLAIRE, ENISA, National and European CERTs
Horizon Results Platform (HRP)	Intermediate and final results of the project.	Policy-makers, investors, entrepreneurs, researchers, innovation/ legal/ business development or financing expert
Horizon Results Booster Services	Dissemination and exploitation strategy	Policy-makers, investors, entrepreneurs, researchers, innovation/ legal/ business development or financing expert

Scientific Dissemination

In order to publish the work done in the project, CYDERCO strives to consolidate results and project outcomes in several journals and magazines. Table 4 lists relevant journals in the scope of project activities, which are candidates to receive papers from our consortium. The Consortium will ensure an open access to publications through the Self-archiving / 'green' scheme to all peer-reviewed scientific publications relating to the project results.

Table 4. Academic and industry journals

Topic	**Name**
Cyber security	Computers and security (open-access); International Journal of Cybersecurity and Digital Forensics (IJCSDF); Journal of Cybersecurity (Oxford University); IEEE Security and Privacy.
Data analytics	IEEE Transactions on knowledge and Data Engineering; European Journal of Operational Research; International Symposium on Intelligent Data Analysis.
Data privacy	European Data Protection Law Review; International Data Privacy Law; International Journal of Law and Information Technology.
Machine learning	Foundations and Trends in Machine Learning; IEEE Transactions on Neural Networks and Learning Systems;; Expert Systems; Advances in Distributed Computing and Artificial Intelligence Journal.

Communication activities

CYDERCO project, its objectives, results, and achievements will be presented also during international events, including scientific and industry conferences. Table 4 presents the list of already identified events although it is not exhaustive and other relevant events will be monitored and considered during the project.

Table 5. Conferences, congresses and external events

Topic	Name
Cyber security	International Conference on Cyber Technology in Automation, Control, and Intelligent Systems; IEEE Symposium on Security and Privacy; International Cyber Security Forum; Cyber Security Week; International Symposium on Research in Attacks, Intrusions and Defenses; Security Mission Information & Innovation Group (SMI2G), IEEE International Symposium on Hardware-Oriented Security and Trust.
Data analytics	Big Data Value Forum; International Symposium on Intelligent Data Analysis.
Data privacy	Annual Privacy Forum; Computers, Privacy and Data Protection Conference.
Machine Learning	International Joint Conferences on Artificial Intelligence; IEEE Symposium Series on Computational Intelligence; European Conference on the Impact of AI and Robotics.

Web Presence

The CYDERCO website stands out as a crucial communication and dissemination channel, serving as a central hub for sharing project concepts, status updates, and achievements with a broad audience. It will be ready by end of Month5. The primary objective is to engage a wide range of stakeholders and foster collaborative discussions between the consortium and external parties. The website plays a crucial role in maximizing the project's impact on multiple fronts:

1. Enhancing project visibility, online presence, and identity on the web;
2. Amplifying dissemination through the informative capacity of the website, offering up-to-date project information, public deliverables, open-access papers, dissemination materials (e.g., leaflets, brochures), and details about project demonstrations;
3. Providing regular updates through a dynamic and attractive interface;
4. Facilitating the collection of end-users' feedback via diverse channels, such as open forums, two-way communication campaigns, face-to-face meetings, targeted events, and questionnaires. Social media platforms like LinkedIn will also be utilized.

The impact of the website and social networking efforts will be meticulously monitored through relevant analytics platforms, such as Google Analytics. Content moderation will be implemented to optimize website outreach.

Visual material

The creation of the corporate CYDERCO project identity through the use of the common visual/graphical elements is one of the tasks in the project's communication strategy. Visual materials are being prepared in WP7: Slides template; Document deliverable templates, General project presentation; Flyers; Posters.

Measurable indicators

In evaluating the effectiveness of our communication and dissemination strategies, the implementation of Key Performance Indicators (KPIs) becomes instrumental. These KPIs serve as measurable benchmarks, allowing us to gauge the impact and reach of our efforts. Table 6 summarizes the KPIs for Communication and Dissemination activities.

Table 6. Key Performance Indicators about Communication and Dissemination

Channel	Indicators and Targets
Working Groups	Number of working groups to contribute >5
Web communication: presence of CYDERCO with a project website and through presence on the social networks.	Unique Visitors from M12: > 1,000; Unique Visitors from M30: > 2,500. Size of online community (by M30): >2,500
e-Newsletters and Email Campaigns	e-Newsletters contributed/released: 4
Cybersecurity conferences/journal	Number of journal papers > 4
Participations to workshops and dissemination events	Number of workshops and events to participate > 5
Standards & Policies	Standards Influence to different Organisations >2
Horizon Results Platform (HRP)	Contact requests > 5

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them

Actions Planned

In this section we are providing some of the initiatives we can foresee by now, although, this list will be updated.

Event	Date	Partners	Role
Focus Group with external Stakeholders	January 19, 2024	ALL	Organizer Participant
Internal Focus Group	February 22, 23, 2024	ALL	Organizer Participant
Other projects interactions	February 2024	ALL	Participant
Launching the project web page	February 2024	Eviden RO	Coordinator
Launching the first press release	January-February 2024	ALL	Contributor

Exploitation Plan

The project's exploitation strategy guides the dissemination and communication plan, to leverage the outcomes, capabilities, and demonstrators generated throughout the project's lifecycle. The Exploitation Plan serves as a guiding framework, aiming to maximize the impact of our project results across diverse sectors. We begin by identifying key assets within the project and specifying target audiences poised to benefit from our innovations. The plan delves into joint exploitation strategies, market uptake considerations, and individualized plans for each project partner. Additionally, a dedicated task within the Work Package 6 structure has been established to define a roadmap for the future exploitation of project outcomes.

This section provides a first overview into our strategies for ensuring the sustained and impactful utilization of the project's contributions, aligning with our broader objectives and creating pathways for real-world application. Each partner within the consortium will develop its own exploitation plan, and the final versions could contribute to their product management, aiding in the development of business cases for their decision-making processes.

Strategic Overview

The strategic perspective will unfold in two primary phases:

- Phase 1 involves conducting a comprehensive market analysis and formulating tailored business models to effectively exploit the project's results.
- In Phase 2, leveraging the research findings of CYDERCO, industrial partners within the consortium will initiate or expand their product and security portfolios to address the challenges associated with a fast and efficient detection and response and increased cybersecurity resilience strategy.

These strategic initiatives are encapsulated in Task 6.2. The forthcoming Deliverable D6.2, titled " Sustainability and exploitation strategy" and scheduled for Month 18, and the final version for Month 36, will succinctly encapsulate the rapid achievements in exploitation accomplished during the project's execution. Furthermore, it will outline the blueprint for continued exploitation beyond the project's conclusion.

Exploitation of project results and tools

Table 7 presents the exploitation strategy as it applies to each asset.

Table 7. Exploitable assets and exploitation strategy

Asset	Partners	Business model for exploitation
AI Data analytics	ISEP Eviden ATOS SP	Utilization in cybersecurity operations, offering advanced data processing services. Scalable solutions for handling large data

module	DNSC	volumes provide a competitive edge. Possible revenue streams from licensing or consultancy services to allied organizations. Utilizes open-source technologies like Apache Hadoop for data processing and analytics. Exploitation: Enhanced data analysis capabilities for SOC teams, aiding in efficient threat detection and response. Scalable to handle large datasets typical in national, regional or sectorial cybersecurity efforts.
Network Traffic Analysis (NTA) module	ISEP Eviden ATOS SP DNSC	Deployment in cyber defense infrastructures. Real-time traffic monitoring and anomaly detection services could be offered to other public entities or allied nations under a service agreement. Implements tools like Suricata, Snort, Zeek or Wireshark for comprehensive monitoring of network traffic. Exploitation: Enables real-time detection of anomalies and potential threats in network traffic, crucial for maintaining national cybersecurity. Zeek's scriptable framework offers deep traffic analysis, while Wireshark provides full packet capture capabilities for detailed network traffic inspection.
Host Intrusion Detection Service	Eviden ATOS SP	Integration in cybersecurity infrastructures. Offering HIDS as a service to government agencies and critical national infrastructure entities. Potential for collaboration with private sector for advanced security solutions, creating a public-private partnership model. Exploitation: Strengthens endpoint security by detecting unauthorized changes or activities, essential for safeguarding critical national infrastructure systems.
Detection and **Response Hub**	ISEP Eviden DNSC	Centralized service for SOC teams , offering AI-enhanced detection and response capabilities, as well as non-AI data analytics, creating avenues for technology transfer and shared cybersecurity initiatives leveraging data lake solutions. Exploitation: Provides a central hub for detection and response, facilitating quick and informed decision-making in threat mitigation. Enhanced by AI for advanced detection capabilities.
CYDERCO Threat **Intelligence Platform**	Eviden ATOS SP	Provision of enriched threat intelligence to national security agencies and allies, including custom threat analysis and reporting. Exploitation: Delivers enriched threat intelligence, crucial for predicting and preventing cyber-attacks. Integration with frameworks like MITRE ATT&CK enhances contextual understanding of threats.

Partners Individual Exploitation Plan

Every industrial partner will formulate an individualized exploitation plan, and the conclusive versions of these plans could serve as valuable inputs for their respective product management teams in crafting robust business cases for strategic development decisions. Table 8 presents a first draft of partners individual exploitation plan.

Table 8. Partners Individual Exploitation Plan

Partner	Exploitation Plan
Eviden	Developing commercial Eviden XDR commercial solution(s) with features such as auto-scaling for data ingestion. In order for the technologies in the proposal to be future-proof and process large volumes of data, modern features such as auto-scaling which do not need human interaction and are able to scale the initial ingestion pipeline automatically will be added to the ingestion pipeline. The project will provide Eviden a competitive advantage by mapping to an increased customer base such as national CSIRTs. Enhancing existing Eviden Threat Intelligence service with features that benefit the beneficiaries of the project, map to the industry needs as well as attempt to match external stakeholders The enhancement of the Threat Intelligence (TI) service will include enrichment of the TI info through standard frameworks like MITRE ATT&CK (in terms of context and interrelationships), advanced visualization, dashboards and scoring to make easier, intuitive, efficient and faster the investigation activities. From the business standpoint, Eviden will merge all feasible-to-be-added newly developed features which also map to the portfolio and product roadmap.
ISEP	ISEP will further improve its methods, especially those addressing the security of using AI, and bringing the vision on working for increased explainability, robustness, and trust of AI. With CYDERCO we intend to explore our work in different AI-based techniques applied to cybersecurity context, to boost the development and integration of innovative AI techniques to detect & respond to cybersecurity threats, fostering the development of CYDERCO Network Traffic Analysis module and CYDERCO Detection and Response Hub. We will work both at scientific level and to strengthen collaboration with industry actors, in particular, with EVIDIEN and ATOS. We intend to exploit project results by leveraging open-source library on robust and explainable AI for IDS, as the basis for new projects and PhD works.
DNSC	Developing a customized solution, specifically tailored to meet the unique needs of macro cybersecurity. This solution will be equipped with robust data processing capabilities, including auto-scaling for data ingestion, to handle the vast amounts of information typically encountered in national and regional operations. A key aspect of this development is ensuring that the technology remains adaptable and responsive to evolving threats. This adaptability is crucial for maintaining an effective defense against

	the constantly changing of cybersecurity threats, ensuring that national security infrastructures are always one step ahead. In parallel, we are committed to enhancing our Threat Intelligence operations. This enhancement involves integrating the service with security databases and frameworks, thus ensuring that the intelligence gathered and analyzed is relevant and specific to the cybersecurity challenges. A significant part of this enhancement will be the development of advanced visualization tools and dashboards. These tools are designed to facilitate quicker and more efficient threat assessment by Security Operations Center (SOC) teams, enabling them to respond to potential threats with greater speed and accuracy.
ATOS SP	Detection tools require both rule-based and behavior-based approaches to cope with the new attack patterns. However, most detection tools (IDS, IPS, SIEMs, etc.) are very limited in behavior analytics capabilities and do not cover context specific protocols and network traffic. The exploitation plan for the NTA and HIDS solutions developed in CYDERCO will follow a maturation and customization path, before packaging and positioning phase starts. We plan to adapt our existing solutions for sector specific uses and improve detection of specific types of attacks. For instance, the current version is trained with dataset generated on a small-scale process scenario, and additional data is needed to improve machine learning models to progress in the asset maturity roadmap. The second exploitable result is the outcome of ATOS SP contribution to the CYDERCO Threat Intelligence Platform. This contribution will leverage on an existing asset named TINTED (Threat Intelligence Node inTEgrated with Data enrichment services) which has two potential exploitation paths within the CYDERCO project. The first is focused on the secure exchange of CTI and targets existing cybersecurity threat intelligence ecosystems. The second one refers to CTI enrichment with user specific information and targets individual organizations. In the short term, the focus will be on packaging with documentation. The following actions are planned to be executed in the project: • Packaging of CYDERCO results and the incubation of market ready solution • Production of training, deployment, marketing and other material. • Contacting with CTI sharing communities and CTI providers and exploration of possibility to partner with the other offerings or sharing ecosystems. • Commercial activities through presentation to account managers of existing clients • Impact creation activities, such as organization of workshops or inputs to policy or white paper. • Participation in the joint exploitation activities of CYDERCO.