Co-funded by the European Union

Ref. Ares(2024)6854142 - 27/09/2024

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

CYDERCO - CYber DEtection, Response and COllaboration

D6.1 Community building

Deliverable date: 2024-09-26

Status: Final

Version: 1.0

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

List of changes

Version	Date	Description	Author(s)
0.1	01.06.2024	First Version	Christine Demeter
1.0	26.09.2024	Quality Assurance	Liana Predut, Ioana-Andreea Craciun

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

Contributors

Role	Contributor's Name	Entity Name - Beneficiary
Deliverable Lead	Christine Demeter	DNSC
Contributor	Mihaela Dan	DNSC
Contributor	Antonio Radu	DNSC
Contributor	Marius Duta	DNSC
Contributor	Darius Tica	DNSC
Contributor	Razvan Stoica	DNSC
Contributor	Eva Maia si	ISEP
Contributor	Isabel Praça	ISEP
Contributor	Rodrigo Diaz	ATOS
Contributor	Ovidiu Calancea	Eviden Technologies
Contributor	Alexandru Rusandu	Eviden Technologies
Contributor	Andrei Chipaila	Eviden Technologies
Contributor	Mircea Avram	Eviden Technologies

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

Approvers

Entity Name - Beneficiary	Project Manager	Signature
Directoratul National De Securitate Cibernetica	Christine Demeter	X Semnatar: Demeter Christine Data si ora semnarii: 2024.09.27 09:52:38 +0300
Instituto Superior De Engenharia Do Porto	Isabel Praça	X Assinado por: Isabel Cecília Correia da Silva Praça Gomes Pereira Identificação: BI09480460 Data: 2024-09-27 às 12:16:24
Eviden Technologies SRL	Ovidiu Calancea	X Ovidiu Calancea Digitally signed by Ovidiu Calancea Date: 2024.09.27 15:14:36 +03'00'
Atos Spain SA	Rodrigo Diaz Rodriguez	X Rodrigo Diaz Rodriguez Digitally signed by Rodrigo Diaz Rodriguez Date: 2024.09.26 17:52:14 +02'00'

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

Contents

1 Glossary: Acronyms, Terms and Abbreviations 6

1.1 Acronyms 6

2. Introduction 7

2.1 Deliverable Purpose 8

3. Methodology 10

4. Key target stakeholders 11

4.1 Expert landscape 11

4.2 Identify Key Stakeholders & Define target audience 12

4.3 Analyze Expertise Areas 13

5. Needs and Motivations Identification 18

6. Building Community 20

6.1 Mission and Vision in the CYDERCO Community 20

6.2 Outreach and Invitation Initiatives 21

6.3 Strengthening Community dynamics 22

6.4 Categories of engagement efforts 22

6.5 Communication channels for the CYDERCO Community 24

6.6 Proposed activities for Community engagement 25

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

1 Glossary: Acronyms, Terms and Abbreviations

1.1 Acronyms

CERT	Computer Emergency Response Team
DoS	Denial of Service
ENISA	The European Union Agency for Cybersecurity
EU	European Union
IoC	Indicator of Compromise
IT	Information Technology
NIST	National Institute of Standards and Technology
SOC	Security Operations Center
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures

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

2. Introduction

CYDERCO (CYber DEtection, Response and COllaboration) project aims to develop, test, and validate components that will support and enhance the detection and response capabilities of relevant entities, including private and national SOCs. This initiative aims to combat cyber threats impacting network and information systems throughout the European Union.

The project delivers two core components: a Detection and Response Platform and a Threat Intelligence Hub, designed to enhance cybersecurity capabilities across European Security Operations Centers (SOCs).

Detection and Response Platform

The Detection and Response Platform is engineered for real-time cyber threat monitoring and analysis, enabling advanced detection of malicious activities and incidents. It integrates traditional signature-based detection with AI-driven techniques, providing a robust and adaptive response to evolving threats.

The platform operates as a data lake, intelligently correlating and filtering events to prioritize high-risk incidents. Designed for seamless integration via DevOps processes, it ensures rapid deployment and operational efficiency, equipping SOC engineers with essential tools for threat detection, triage, investigation, and response.

Threat Intelligence Hub

The Threat Intelligence Hub facilitates secure sharing and analysis of actionable threat intelligence across SOCs and public authorities. It aggregates critical data on threat actors, TTPs, and IoCs, enhancing the detection of unknown threats and improving SOC collaboration and proactivity.

By covering the entire attack surface and providing industry-specific threat insights, the hub supports a comprehensive, interoperable threat intelligence framework, crucial for preemptive defense strategies and efficient incident response.

Together, these components strengthen the EU's cybersecurity posture through enhanced detection, response, and collaborative intelligence sharing.

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

2.1 Deliverable Purpose

Within the project's framework, Work Package 6 (WP6), titled "Ecosystem Building, Collaboration & Sustainability Strategy," plays a pivotal role in laying the foundation for a sustainable and engaged community around the CYDERCO platform.

The main objective of WP6 is to bring together a diverse group of stakeholders and experts, creating an ecosystem where knowledge, expertise, and resources can be exchanged and leveraged to advance the goals of the CYDERCO platform.

The focus of this document is to provide an in-depth analysis of the different types of stakeholders and outline a strategic methodology for engaging these stakeholders effectively. It is essential for the construction of the CYDERCO community, as it sets the stage for identifying and engaging the right individuals and organizations that can contribute meaningfully to the platform's development and long-term sustainability.

The work carried out in Task 6.1 and presented in this document is not an isolated effort. It is closely interlinked with other critical components of the CYDERCO project, particularly with Task 6.2, which focuses on the Sustainability and Exploitation Strategy.

The insights gained from the stakeholder landscape and engagement methodology directly feed into the strategies developed in Task 6.2, ensuring that the community building efforts are aligned with the broader goals of sustainability and exploitation of the CYDERCO platform's outputs.

Additionally, this document is informed by the findings from Deliverable 2.1, which is dedicated to Stakeholders' Analysis & Requirements Elicitation. Deliverable 2.1 provides a detailed summary of the stakeholders' analysis conducted earlier in the project and outlines the specific requirements necessary to ensure that the project's activities and proposed technical solutions are feasible and aligned with stakeholder expectations.

The information from Deliverable 2.1 plays a critical role in shaping the engagement strategies outlined in this document, ensuring that the community building efforts are grounded in a solid understanding of stakeholder needs and project requirements.

Furthermore, WP6 activities are also connected to the broader efforts of Work Package 7 (WP7), which is focused on Dissemination and Communication Plans. The primary goals of WP7 are to disseminate the project's results to relevant communities and to promote the project's activities and outputs.

The stakeholders' engagement strategies developed in WP6, particularly those detailed in this document, provide an important foundation for the dissemination and communication efforts in WP7.

By establishing a well-defined and engaged community, WP6 ensures that there is a receptive audience for the project's outputs, thereby enhancing the overall impact and visibility of the CYDERCO platform.

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

In conclusion, this document is a cornerstone of the CYDERCO project's community building efforts. It provides a detailed roadmap for identifying, engaging, and sustaining a diverse group of stakeholders and experts who will form the backbone of the CYDERCO community.

Through a systematic approach that includes landscape analysis, needs identification, and strategic engagement, the project aims to create a dynamic and sustainable ecosystem that will continue to thrive and contribute to the field well beyond the project's initial phases.

Therefore, our focus is to provide a comprehensive framework for identifying, engaging, and sustaining a diverse community of stakeholders and experts around the CYDERCO platform, ensuring the development of a dynamic and sustainable ecosystem aligned with the project's long-term goals.

3. Methodology

Initiating a community around the CYDERCO platform involves laying the foundation for collaborative engagement and knowledge exchange. The methodology for community building is structured into several key phases, as follows:

- ✓ identifying and analyzing key stakeholders
- ✓ understanding their needs and motivations
- ✓ developing strategies for outreach, engagement, and retention

The main goal is to establish a vibrant, sustainable community that supports the CYDERCO platform's objectives.

The activities required to accomplish the objectives of Task 6.1 consist of several key stages, outlined as follows:

The first stage, within **Key target stakeholders Chapter**, involves a comprehensive landscape analysis, where the focus is on identifying the key target audience who could potentially become part of the CYDERCO community. This analysis goes beyond merely listing potential members; it seeks to understand the different types of expertise that are necessary to address the challenges and opportunities associated with the CYDERCO platform. This stage is foundational, as it helps to define the scope and diversity of the community, ensuring that it includes a broad range of perspectives and skills that are essential for its success.

Following the landscape analysis, the next stage, under **Needs and Motivation Identification Chapter,** is dedicated to the identifying the needs and motivations of these potential community members. Understanding what drives these experts to participate in a community like CYDERCO is crucial for designing an engagement strategy that resonates with them. This involves exploring their professional interests, the challenges they face in their fields, and the value they perceive in being part of a collaborative ecosystem. By aligning the community's objectives with the specific needs and motivations of its members, the project can foster a sense of ownership and commitment among the participants, which is key to the long-term success of the CYDERCO platform.

Once the needs and motivations of the stakeholders are well understood, the project moves into the building community phase, as presented in the **Community Building Chapter**. In this phase, identified experts and stakeholders are invited to join the CYDERCO community. The engagement strategy is designed to facilitate active participation, encouraging members to share their opinions, expertise, and knowledge on topics that are closely aligned with the objectives of the CYDERCO platform. This phase is not just about building membership; it's about creating an interactive and collaborative environment where participants feel valued and are motivated to contribute actively. To ensure the community's long-term success, a sustainability strategy will be implemented, involving regular activities that align with members' professional interests. The goal is to establish a vibrant, enduring community that enhances the detection, response, and collaboration capabilities of cybersecurity entities across the European Union.

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

4. Key target stakeholders

To establish a robust community, it is crucial to identify and actively engage key stakeholders who are integral to the cybersecurity ecosystem. These stakeholders will encompass government agencies, CERTs, industry leaders, technology providers, academic institutions, SMEs, startups, and end-users. Each group contributes distinct expertise and resources essential for the success and long-term sustainability of the CYDERCO platform.

The community-building efforts within CYDERCO will be detailed across two key subchapters: "Expert Landscape" and "Identifying Key Stakeholders/Defining Target Audience." This document will delineate various roles within the cybersecurity ecosystem and the strategies for engaging key stakeholders to ensure the platform's success. Collectively, these initiatives will foster a strong and sustainable community, significantly enhancing cybersecurity capabilities throughout the European Union.

4.1 Expert landscape

The expert landscape within CYDERCO is diverse and complex, reflecting the varying responsibilities and expertise of different stakeholder groups. To effectively build the community, it is crucial to understand the specific role each group plays in the cybersecurity ecosystem. These roles can be categorized into three main responsibilities:

- ✓ incident reporting
- ✓ incident handling
- ✓ expertise production

Incident reporting is a responsibility typically held by individuals or teams on the front lines of cybersecurity within their organizations. They are tasked with monitoring systems and identifying potential security breaches. By providing timely and accurate reports, they enable the broader community to respond effectively to threats.

Incident handling involves specialized teams, such as SOCs and CERTs, who manage and resolve incidents. Their role is critical in containing threats and mitigating damage. Within CYDERCO, these stakeholders are essential for refining the platform’s response capabilities and ensuring that it meets real-world needs.

Expertise production includes researchers and analysts who contribute to the broader knowledge base in cybersecurity. They provide insights that inform both the strategic direction of CYDERCO and the day-to-day operations of incident handlers. Their work ensures that the community remains at the cutting edge of cybersecurity practices.

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

4.2 Identify Key Stakeholders & Define target audience

Identifying key stakeholders is crucial for the community's foundation. Primary stakeholders include governmental entities, regulatory bodies, cybersecurity companies, and IT service providers. These groups play critical roles in shaping the platform's capabilities and ensuring alignment with national security standards.

Secondary stakeholders, such as academic institutions and industry associations, contribute through research, innovation, and broader community engagement.

These stakeholders are divided into primary and secondary groups, each with a unique role in supporting the platform's success.

Primary stakeholders:

- Governmental entities and regulatory bodies - include national CERTs and law enforcement agencies. Their involvement is important for ensuring that CYDERCO aligns with national security standards and can respond quickly to cyber incidents. Engaging these stakeholders early and continuously is essential for establishing credibility and operational effectiveness.
- Cybersecurity companies and IT service providers - contribute to the technical development of the platform. Their feedback during the iterative design and testing phases will help ensure that CYDERCO meets the practical needs of the industry. Early adopters from this group will also play a key role in refining the platform's features and functions.

Secondary stakeholders:

- Academic institutions and research organizations - universities and research institutions help to advance the platform's capabilities and train the next generation of cybersecurity professionals. Collaborations with these institutions will furnish CYDERCO with fresh insights and potential breakthroughs in cybersecurity technologies.
- Industry associations and non-profit organizations - help to expand CYDERCO's reach and foster engagement across different sectors. By leveraging their networks, CYDERCO can disseminate information more effectively and build a broader, more inclusive community.

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

4.3 Analyze Expertise Areas

Analyzing the expertise areas within the CYDERCO community is crucial for mapping the diverse skills, knowledge, and capabilities of stakeholders involved in cybersecurity. This analysis provides insight into how different entities can collaborate, enhancing the overall effectiveness of the community. By examining these areas, CYDERCO can identify key synergies, gaps, and opportunities for growth.

This empirical analysis is grounded in findings from the *D2.1 Stakeholders' Analysis & Requirements Elicitation*. It emphasizes the identification and involvement of key stakeholders with technical profiles that align with the project's objectives. By classifying these stakeholders and understanding their roles, as detailed in *Table 1*, CYDERCO can better address their specific needs and expectations, ensuring a successful development process.

4.3.1 Stakeholder categories and their involvement

Stakeholders in the CYDERCO community are categorized into four main groups:

- stakeholder roles
- internal stakeholders
- external stakeholders
- collaborative partners

Each group contributes specialized technical insights essential for developing and implementing the CYDERCO platform.

Table 1 below outlines the stakeholder categories and their respective roles and contributions. Each stakeholder plays a vital role in the project, from ensuring compliance with national cybersecurity standards to developing innovative solutions.

Table 1 - Technical stakeholders and their involvement

Stakeholder Category	Stakeholder Role	Involvement and Contributions
Stakeholder Roles	Chief Information Security Officer (CISO)	Ensures alignment of platform requirements with strategic security objectives.
	Security Analysts	Monitors, detects, and responds to security incidents; vital for defining operational functionalities of the platform.
	Network Administrators	Ensures network security and integrates the platform with existing infrastructure.

	Incident Response Team	Manages and mitigates security incidents; essential for developing incident management features.
	Threat Intelligence Team	Identifies emerging threats and contributes to requirements for threat intelligence gathering and analysis.
	IT Operations Team	Collaborates with SOC to implement security measures and ensures system integrity.
	Chief Information Officer (CIO)	Aligns SOC activities with organizational goals; guides prioritization of development efforts.
	Audit and Compliance Teams	Ensures adherence to industry standards and contributes to compliance-related functionalities within the platform.
Internal Stakeholders	National CERTs and Government Entities	Defines national-level security and collaboration requirements for the platform, especially for critical infrastructure.
	Law Enforcement Agencies	Provides input on requirements for incident reporting and investigative cooperation during severe cyber incidents.
External Stakeholders	Critical Infrastructure Organizations	Key in establishing the platform's capabilities to protect and respond to threats within EU critical infrastructure sectors.
	For-Profit Organizations	Offers insights into security challenges and needs specific to various organizational domains.
	Regulatory Bodies	Ensures platform compliance with industry-specific security regulations and standards.
Collaborative Partners	External Security Researchers	Provides insights into emerging threats and vulnerabilities; shapes threat research and information-sharing capabilities of the platform.
	IT and Security Service Providers	Offers feedback on requirements related to service integration and security, particularly for outsourced services working with SOCs.

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

4.3.2 Mapping stakeholder relationships

Mapping stakeholder relationships highlights how different entities interact and how their expertise can complement each other. For instance, national Computer Emergency Response Teams (CERTs) often work closely with governmental regulatory bodies to ensure compliance with cybersecurity standards.

Additionally, cybersecurity companies may partner with academic institutions for research and development, leading to innovative solutions.

Table 2 illustrates the specific roles of various stakeholders and their potential collaboration opportunities. By visualizing these connections, CYDERCO can clarify the roles of each stakeholder and identify key players, fostering collaboration.

Table 2 - Stakeholder Roles and Collaboration Opportunities in the CYDERCO Platform

Stakeholder Category	Roles	Collaboration Opportunities
Governmental Entities & Regulatory Bodies	Oversight, ensuring regulatory compliance, policy enforcement	Collaborate with CERTs, law enforcement, and critical infrastructure organizations to align regulations with industry needs
National CERTs & SOCs	Real-time threat monitoring, incident response, intelligence sharing	Work with governmental bodies, law enforcement, and private sector to exchange threat intelligence and coordinate responses
Cybersecurity Companies & IT Service Providers	Provide tools and solutions for threat detection and incident mitigation	Collaborate with CERTs and SMEs for platform integration and sharing of best practices
Academic Institutions & Research Organizations	Conduct research, develop new cybersecurity methods, train workforce	Partner with cybersecurity firms, CERTs, and government agencies for joint research projects and workforce development
Critical Infrastructure Organizations	Ensure operational continuity, comply with cybersecurity regulations	Collaborate with governmental bodies and CERTs for real-time monitoring and incident response

Law Enforcement Agencies	Investigate cybercrimes, collaborate on cybercrime prevention	Work with CERTs, governmental entities, and cybersecurity firms to access intelligence and prosecute cybercrimes
SMEs & Startups	Implement affordable, scalable cybersecurity solutions	Partner with cybersecurity firms and academic institutions for testing new solutions and developing affordable cybersecurity measures
End-Users (Private Sector & General Public)	Ensure data protection, maintain operational safety	Collaborate with service providers and government agencies for protection against cyber threats and guidance on best practices
Industry Associations & Non-Profit Organizations	Advocate for cybersecurity best practices, raise awareness	Work with various stakeholders to promote cybersecurity standards and organize community outreach initiatives

4.3.3 Segmentation of stakeholders

Once the relationships among stakeholders are mapped, the next step is to segment the community based on shared characteristics, interests, and behaviors.

This segmentation allows for the categorization of stakeholders into distinct groups, such as incident response professionals, threat intelligence analysts, researchers, and policymakers.

Each group will have specific expertise areas and operational focuses, enabling CYDERCO to tailor engagement strategies effectively.

For example, cybersecurity professionals specializing in incident response may require access to real-time threat intelligence and training on new detection techniques. In contrast, academic researchers may seek opportunities to publish findings and collaborate on projects that advance cybersecurity knowledge.

Understanding these unique needs allows CYDERCO to create targeted programs and resources that enhance engagement and participation.

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

4.3.4 Recognizing interdependencies

Another critical aspect of analyzing expertise areas is recognizing the interdependencies among stakeholders. The success of incident handling teams, for example, often relies on timely intelligence provided by researchers and analysts. Ensuring that incident responders receive accurate and actionable insights can significantly improve the efficiency of the incident response process.

Similarly, academic institutions depend on input from cybersecurity companies to align their research with industry needs. Nurturing these interdependent relationships strengthens the entire CYDERCO community, making it more resilient and agile in responding to emerging threats.

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

5. Needs and Motivations Identification

Identifying the needs and motivations of stakeholders involves a systematic approach that includes various methods of research, analysis, and engagement.

The CYDERCO community aims to create a collaborative environment where various stakeholders can come together to enhance cybersecurity measures and share valuable insights. Understanding the diverse needs and motivations of these stakeholders is essential for fostering engagement and ensuring the success of the project.

Each stakeholder group, including governmental entities, cybersecurity companies, SMEs, academic institutions, and end-users has unique requirements and goals. By addressing these needs, the CYDERCO initiative seeks to provide tailored solutions that empower stakeholders to improve their cybersecurity posture and adapt to evolving threats.

In terms of identifying and developing incentives to attract and retain members within the CYDERCO community, we plan to establish a series of activities, such as webinars and workshops led by cybersecurity experts. These sessions will be designed to address the specific needs identified in our survey, such as advanced threat intelligence and hands-on threat simulation exercises.

We aim to introduce a recognition program that highlights member contributions through awards and certifications. For example, members who actively contribute to community discussions or lead successful collaborative projects will receive recognition that they can showcase on their professional profiles.

Table 3 below presents key needs, motivations, and incentives that stakeholders can expect when joining the CYDERCO community, highlighting key aspects such as: the need for access to collaborative platforms, affordable security solutions, and opportunities for research collaboration.

It also outlines the motivations driving stakeholders to participate, including the desire to stay informed about the latest trends and the chance to influence industry standards and policies.

Moreover, the incentives offered to stakeholders, such as networking opportunities, financial support identification, and recognition within the community, are designed to encourage active participation and collaboration.

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

Table 3 - Needs, motivations, and incentives for stakeholders

Needs	Motivation	Incentives
Access to a collaborative platform for threat intelligence	Enhance cybersecurity posture and protect critical assets	Opportunities for networking and collaboration
Affordable cybersecurity solutions tailored for SMEs	Improve security measures without straining budgets	Financial support or discounts for services
User-friendly tools for effective threat response	Minimize downtime and risks associated with cyber threats	Training programs and resources
Regular updates on project developments and best practices	Stay informed about the latest cybersecurity trends	Access to exclusive content and early insights
Opportunities for research collaboration with academic institutions	Contribute to innovative cybersecurity solutions	Grants or funding for joint research initiatives
Participation in working groups and workshops	Influence the direction of cybersecurity practices	Recognition as a thought leader in the community
Sharing experiences and challenges with peers	Gain insights and learn from others' successes	Access to case studies and success stories
Influence standards and policies through active involvement	Shape the future of cybersecurity practices	Opportunities to participate in policy discussions
Visibility and recognition in the cybersecurity community	Enhance reputation and credibility	Certificates, awards, or public recognition
Access to EU funding visibility and support	Ensure alignment with EU policies and initiatives	Inclusion in promotional materials and reports

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

6. Building Community

Building a community is a fundamental aspect of fostering collaboration, engagement, and knowledge-sharing among stakeholders in any given field. In the context of the CYDERCO project, community building involves creating a network of individuals and organizations united by a shared interest in enhancing cybersecurity practices.

This process begins with outreach and invitation initiatives designed to raise awareness of the project's benefits, encouraging diverse participation.

Once established, the focus shifts to strengthening community dynamics through active engagement, communication, and collaborative activities.

By promoting interaction and facilitating the exchange of ideas, the CYDERCO community aims to cultivate a sustainable ecosystem where members can continuously learn, innovate, and address the evolving challenges in cybersecurity together.

This guide outlines practical strategies and activities to effectively build and maintain such a vibrant community, ensuring long-term success and resilience in the face of cyber threats.

6.1 Mission and Vision in the CYDERCO Community

6.1.1 Mission

The mission of the CYDERCO Community is to create a resilient and collaborative cybersecurity ecosystem that enhances the detection, response, and mitigation of cyber threats.

By fostering strong horizontal and vertical communication among public and private stakeholders, we aim to facilitate real-time information sharing, improve cross-sector cooperation, and establish standardized best practices. Our goal is to enable organizations, regardless of size or industry, to strengthen their cybersecurity postures through joint initiatives, shared resources, and continuous learning.

Key components of the mission:

- Empowering organizations with tools and knowledge to manage cyber incidents effectively
- Promoting collaboration between SOCs, CERTs, and relevant stakeholders
- Driving innovation and adaptability through ongoing feedback, simulations, and collaboration
- Supporting both horizontal (internal) and vertical (external) communication for faster, more coordinated responses to cyber incidents.

6.1.2 Vision

The vision of the CYDERCO Community is to become a leading force in shaping a secure digital environment across Europe, where public and private entities work together to mitigate cybersecurity risks.

We envision a future where collaboration, transparency, and shared best practices lead to a robust and unified defense system that can swiftly respond to the evolving threat landscape.

Through CYDERCO, we strive to set a standard for cybersecurity collaboration that transcends industries and borders, ensuring a safer digital ecosystem for all.

Key aspects of the vision:

- A harmonized cybersecurity network across sectors that enables swift and effective responses to cyber threats
- A culture of continuous improvement, where stakeholders engage in proactive learning and cooperation
- An integrated, Europe-wide platform that leverages both artificial intelligence and human expertise to enhance cybersecurity measures
- The establishment of CYDERCO as a model for cross-sector cooperation, driving policymaking, standardization, and technological advancements in cybersecurity.

6.2 Outreach and Invitation Initiatives

The outreach and invitation initiatives are essential for creating a practical and engaged community surrounding the CYDERCO project. This phase consists of three key steps:

1. **Creating Awareness and Invitational Materials**

The initial step involves developing user-friendly materials that clearly articulate the CYDERCO project's value proposition. These materials should emphasize the benefits of participating in the CYDERCO community and adhere to best practices in marketing.

The first set of materials will be adaptable to various formats to maximize the outreach and dissemination efforts. All materials will be informed by empirical analysis and will be refined as more market input is collected.

2. **Identifying Relevant Communication Channels**

The second step focuses on identifying and prioritizing communication and dissemination channels for outreach and invitation. This includes differentiating between direct and indirect outreach methods, small-scoped or wide-scoped strategies, and formal or informal approaches.

Multiple channels, such as the project website, social networks, e-newsletters, and email campaigns, will be utilized to ensure diverse outreach. These channels are selected based on their

effectiveness in reaching different groups, maximizing the visibility of the project's key outputs and findings.

3. **Implementing Course-Correction Mechanisms**

The third step involves establishing mechanisms to track the performance of outreach efforts over time. This allows for timely adjustments if certain strategies underperform. For instance, if one communication channel yields poor results, resources can be redirected to a more effective channel. These mechanisms ensure that all stakeholder outreach efforts are continuously optimized.

After the outreach campaign, interested stakeholders will be invited to join the community built around the CYDERCO platform. Although outreach efforts may continue in the background, the focus will shift to engaging these stakeholders through various activities.

6.3 Strengthening Community dynamics

Once the outreach and invitation phase is complete, the next step is to solidify and enhance the CYDERCO community. This involves boosting engagement and information flow between the project implementation team and stakeholders, as well as among the stakeholders themselves. The goal is to create a sustainable and vibrant community that can support itself over time.

The engagement efforts are guided by two core principles:

- **Sustainability**: the community should thrive independently without constant oversight from consortium partners.
- **Active engagement**: community activities should encourage active participation from members rather than relying solely on passive contributions.

These principles must be incorporated into the overall strategy, with activities designed to promote them.

6.4 Categories of engagement efforts

- **Consortium-lead engagement activities**

This category includes activities organized by the consortium to boost interaction within the community through information sharing and workshops. Examples of activities include:

- **Specialized training sessions**: focused on practical applications of the CYDERCO project components and tools.

- **Collaborative workshops**: allow stakeholders to share insights and provide feedback to contribute to the project's development.
- **Working groups**: focus on specific areas such as AI-driven detection methods, threat landscape analysis, and response protocols.

➢ **Ongoing community communication**

Maintaining high levels of intra-community communication is essential for sustaining engagement. This includes both consortium-led and community-led initiatives:

- **Regular update meetings and webinars**: to keep the community informed about project progress and developments.
- **Online platform or forum**: for ongoing discussions, knowledge sharing, and collaboration among stakeholders.
- **Recognizing contributions**: promoting and acknowledging the efforts of community members to encourage participation.
- **Joint projects and shared resources**: encouraging collaboration on research initiatives and resource sharing among members.
- **Monitoring engagement levels**: continuously evaluating community participation and adjusting strategies to maintain interest.

➢ **Future exploitation strategies**

To ensure the longevity of the community beyond the project's duration, the consortium must develop strategies for resource exploitation:

- **Identifying key deliverables**: such as AI algorithms, detection tools, and training materials that can be further utilized.
- **Commercialization strategies**: developing plans for licensing, commercialization, or open-source release of relevant components.
- **Engagement with industry partners**: exploring opportunities for collaboration with potential investors or industry partners to scale project results.

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

6.5 Communication channels for the CYDERCO Community

Effective communication is essential for ensuring the success and sustainability of the CYDERCO Community. A multi-channel approach will be utilized to facilitate communication, engagement, and collaboration among all stakeholders. The following outlines the key communication channels:

CYDERCO website

The Web Communication channel (https://page.eviden.com/cyderco-eviden-project.html) aims to establish a central platform for sharing key information, project updates, and resources with a diverse audience, ensuring transparency and broad accessibility.

Through a dedicated CYDERCO project website, stakeholders, including the general public, governments, CSIRTs, CERTs, SMEs, industry professionals, and academic institutions will have access to deliverables, publications, event details, and news. This website will serve as the primary information hub, fostering engagement and knowledge dissemination.

Social Media

The Social Media Presence channel is designed to engage the cybersecurity community and increase awareness of CYDERCO's activities and achievements. Through our active profile on LinkedIn (https://www.linkedin.com/company/cyderco/) we will share regular updates on project milestones, cybersecurity insights, and upcoming events.

This platform will foster interaction, discussion, and knowledge exchange, while targeted social media campaigns will enhance visibility and encourage audience engagement. The target audience includes cybersecurity professionals, researchers, SMEs, industry experts, and the general public.

E-Newsletters and Email Campaigns

The e-Newsletters and Email Campaigns channel aims to keep key stakeholders informed about CYDERCO's progress, upcoming events, and significant developments through personalized communication. Quarterly e-newsletters will highlight the project's activities and achievements, while targeted email campaigns will focus on promoting specific events and outcomes to a carefully selected audience.

Cybersecurity conferences and journals

The objective of this communication channel is to disseminate CYDERCO's findings and innovations within the broader cybersecurity research and industry communities, enhancing recognition and support for the project.

CYDERCO representatives will present research results at leading cybersecurity conferences and publish in respected journals, thereby increasing the project's visibility and fostering collaborations

with industry professionals, academic leaders, and policymakers. This will strengthen the project's presence and contribute to the development of new partnerships.

6.6 Proposed activities for Community engagement

To build a strong, sustainable, and collaborative cybersecurity community across Europe, the CYDERCO project will implement a series of targeted activities designed to enhance communication, optimize processes, and foster collaboration among stakeholders.

1. **Workshops on horizontal communication**

The workshops will focus on improving internal communication within organizations, addressing common challenges that hinder effective collaboration between different departments and teams. By facilitating open discussions and sharing best practices, these workshops aim to break down silos and promote seamless information flow across various functions. The outcome will be enhanced cooperation and more coordinated efforts in responding to cybersecurity threats.

2. **Training sessions on vertical reporting**

To improve the accuracy and efficiency of reporting incidents to sector-specific CERTs, the project will organize specialized training sessions. These sessions will cover best practices for clear and timely communication, ensuring that all necessary details are conveyed to the appropriate regulatory bodies. By enhancing vertical reporting, organizations can ensure compliance with regulatory requirements and contribute to a more robust cybersecurity ecosystem.

3. **Forums for process optimization**

The project will establish forums where stakeholders can come together to identify and address inefficiencies in their current cybersecurity processes. These forums will encourage participants to share their experiences and collaborate on solutions that streamline workflows, reduce redundancy, and enhance overall coordination. The goal is to create more efficient and effective operations within and between organizations, ultimately strengthening the cybersecurity infrastructure.

4. **Collaboration meetings for cross-sectoral best practices:**

Regular meetings will be held to bring together representatives from different industry sectors to discuss common cybersecurity challenges and share best practices. These meetings will promote consistency in approaches to cybersecurity across sectors, helping to build a more unified and cooperative defense against threats. Participants will gain valuable insights from other sectors, which can be applied to their own practices, fostering a culture of continuous improvement.

5. **Simulation exercises for incident response and reporting**

To ensure that all stakeholders are prepared to handle real-world cyber incidents, the project will develop and conduct simulation exercises. These exercises will provide participants with hands-on experience in both horizontal communication within their organizations and vertical reporting to CERTs. By simulating real-world scenarios, participants can identify weaknesses in their current practices and develop strategies to improve their response capabilities.

6. **Feedback sessions for continuous improvement:**

Regular feedback sessions will be implemented to gather input from end-users, service providers, and other stakeholders on the effectiveness of the CYDERCO platform. These sessions will be critical for ensuring that the platform evolves in line with the real-world needs of its users. By continuously refining the platform based on user feedback, the project can maintain its relevance and effectiveness in the face of changing cybersecurity challenges.

By implementing these activities, the CYDERCO project will build a resilient and collaborative cybersecurity community across Europe. The focus on improving communication, optimizing processes, and fostering cross-sectoral collaboration will not only enhance the immediate response to cyber threats but also contribute to the long-term sustainability of the community.

This proactive approach will ensure that the CYDERCO community remains at the forefront of cybersecurity innovation, driving continuous improvement in the field while effectively adapting to new challenges.

The table below outlines the activities we have planned to keep the community vibrant, responsive, and in tune with the changing needs of its members.

Table 4 - Proposed activities for community development

Event Type	Goal	Specific Objectives	Practical Activities	Expected Outcomes	Participant Roles
Workshop	Promote efficient internal communication within organizations	- Break down departmental silos - Encourage cross-functional collaboration	- Presentations on cybersecurity communication protocols - Interactive sessions on real-time data sharing	- Improved horizontal communication - Unified response across departments	IT Managers, Risk Officers, Legal Advisors, Operations Managers
Training Session	Improve vertical reporting to sector-specific CERTs	- Enhance reporting accuracy - Ensure compliance with	- Training on step-by-step incident reporting - Best practices for	- Accurate and timely vertical reporting to CERTs - Compliance	IT and Security Officers, Compliance Managers

		regulatory standards	communication with sectoral CERTs	with regulatory requirements	
Forum	Identify and address inefficiencies in cybersecurity workflows	- Streamline internal processes - Reduce redundancies in reporting and threat response	- Collaborative sessions to benchmark and optimize processes - Discussions on CYDERCO tool integration	- Optimized processes - Reduced operational redundancy - Better coordination with CERTs	Cybersecurity Experts, Operational Managers
Collaboration Meetings	Foster cross-sectoral knowledge exchange	- Share best practices across industries - Develop unified cybersecurity standards	- Discussions between representatives from finance, healthcare, government, etc. - Common cybersecurity strategies	- Cross-sector adoption of best practices - Harmonized cybersecurity approaches across sectors	Sector Leaders, IT Managers, Policy Advisors
Simulation Exercises	Strengthen incident response capabilities	- Test horizontal and vertical communication channels - Identify response weaknesses	- Real-world cyber incident simulations - Evaluation of communication speed and accuracy	- Identified gaps in incident response - Improved collaboration and communication during incidents	IT Security Teams, Incident Response Teams
Feedback Sessions	Continuous improvement of CYDERCO platform	- Gather user input for platform development - Address operational needs in communication features	- Stakeholder feedback gathering - Discussions on horizontal and vertical communication tools	- Platform improvements aligned with operational needs - Enhanced communication features	IT Managers, End-Users, Developers
Establishment of Reporting Protocols	Ensure organizations follow clear incident reporting guidelines	- Refine roles and responsibilities for incident reporting - Introduce automated escalation tools	- Workshops on creating incident escalation protocols - Hands-on tool training for automated reporting	- Clear, predefined reporting roles - Faster and more efficient incident escalation	IT Directors, Security Experts, CERT Representatives

Working Groups for SOC/CERT Collaboration	Develop joint operational procedures for SOCs and CERTs	- Standardize operational procedures for threat detection and response - Support horizontal/vertical info flow	- Working groups for SOC/CERT collaboration - Development of joint procedures for vulnerability management	- Harmonized SOC and CERT operations - Efficient collaboration between SOCs and CERTs	SOC Analysts, CERT Operators, IT Experts