D4.7 - Dissemination and exploitation deliverable

NGSOTI Project: 101127921
DIGITAL-ECCC-2022-CYBER-03

Team CIRCL/NGSOTI

CIRCL
Computer Incident
Response Center
Luxembourg

Co-funded by
the European Union

2025-09-14

Contents

1 Dissemination and exploitation deliverables

1.1 Disclaimer

Words displayed in red indicate hyperlinks. These links can be clicked or viewed by hovering over the text.

1.2 Distribution and License

The document is distributed as TLP:CLEAR.

1.3 Deliverable definition

The identifier of the deliverable is **D4.7** and it adheres to the definition outlined in the grant agreement written in **bold**. **Dissemination and exploitation deliverable**.

1.4 Introduction

This section provides an overview of the NGSOTI (Next Generation Security Operator Training Infrastructure) project and the importance of dissemination and exploitation activities. The project entails a comprehensive document encompassing a communication and dissemination plan, structured with several key sub-sections. These include objectives, key messaging, target audiences, communication channels, social media plan, planned budget, and relevant indicators for monitoring and evaluation. Additionally, the document features a section dedicated to post-action exploitation strategies, detailing the sustainability program for platform operation beyond the project's duration. It is structured to include sections on Dissemination Plan, Exploitation Plan, Budget, Risk Management, and concludes with a summary emphasizing the significance of effective dissemination and exploitation strategies for the success and longevity of the NGSOTI project.

In the midst of burgeoning efforts to enhance Security Operation Center (SOC) capabilities through the development of toolsets, acquisition of data feeds, and integration of artificial intelligence, the NGSOTI project prioritizes the human dimension of SOC operations. While current SOC environments may have ample potential operators, many lack access to robust toolsets and comprehensive data

feeds. The NGSOTI project looks beyond the present landscape to cultivate a new generation of SOC operators primed to tackle emerging challenges. Presently, SOC operators typically transition from IT roles or pursue academic paths specializing in cybersecurity. However, existing academic curricula often rely heavily on the experiences of educators and may benefit from industry input. To address evolving training needs, the NGSOTI project outlines the establishment of a real-world operational infrastructure dedicated to training the next wave of SOC operators. This infrastructure will provide hands-on training opportunities essential for preparing SOC professionals for the dynamic threat landscape. Collaboration between educational institutions and industry partners will drive teaching and training initiatives, ensuring alignment with evolving industry standards and best practices.

2 Dissemination Plan

This section describes the objectives, the key messaging, social media plan, target audience, communication channels, communication materials, and timeline.

2.1 Objectives

The NGSOTI objectives are specific, measurable, achievable, relevant, and time-bound goals within the NGSOTI project that the NGSOTI consortium aims to achieve in the between 1/1/2024 to 31/12/2026. The objectives provide a clear direction and purpose for actions and serve as benchmarks for assessing progress and success. They help to focus efforts, allocate resources efficiently, and prioritize tasks effectively. The NGSOTI objectives try to be clearly defined, realistic, and aligned with broader goals or strategies to ensure that they contribute to overall success. They are enumerated below grouped by workpackage.

2.1.1 Project Management Objectives

- Ensure timely execution of project work.
- Facilitate smooth coordination between project partners.
- Record necessary project management data for reporting to the funding agency.
- Set up agreements for using NGSOTI for teaching and research.

2.1.2 Technical Infrastructure Objectives

- Set up the technical infrastructure.
- Maintain infrastructure agility to adapt to new SOC paradigms.
- Collect data from the infrastructure.
- Implement an independent satellite task for URL checking within Restena edu.lu service.

2.1.3 Training and Education Objectives

- Evaluate NGSOTI data to create up-to-date training materials.
- Conduct training sessions using NGSOTI.
- Collect feedback from existing training sessions to improve future ones.

2.1.4 Outreach and Engagement Objectives

- Make NGSOTI attractive for schools and students.
- Enable teachers to use NGSOTI for creating training materials.
- Maintain blog posts related to components used within NGSOTI.

2.2 Key messaging

The Key messaging refers to the core, essential information or points that NGSOTI project aims to communicate to its target audience. These messages are carefully crafted to convey specific themes, ideas, or objectives effectively and consistently. Key messaging ensures that stakeholders receive clear and cohesive information that aligns with the NGSOTI project's, values, and priorities. It is intended to help to shape perceptions, influence opinions, and guide decision-making among the audience. Key messaging is often developed based on audience analysis, communication objectives, and brand positioning, and it serves as the foundation for all communication materials and activities.

Influence opinions and decision-making within Security Operation Centers (SOCs) is pivotal for ensuring effective cybersecurity measures. This influence hinges on comprehensive documentation of best practices, guiding the selection of solutions deployed in a SOC. By meticulously outlining proven methodologies and criteria, SOC teams can make informed decisions that bolster their defenses and mitigate risks effectively.

Moreover, the availability of practical, usable software tailored for SOCs is instrumental in streamlining operations and enhancing response capabilities. These software solutions, meticulously designed to address SOC-specific needs, empower teams to proactively detect and respond to threats with agility and precision.

Addressing the challenge of handling large volumes of data within SOC environments is paramount. Through innovative approaches and scalable solutions, SOC teams can efficiently manage and analyze vast amounts of data, extracting actionable insights to fortify their defenses and thwart emerging threats effectively.

Furthermore, interconnecting with other SOCs fosters collaboration and information sharing, amplifying collective defense efforts. Establishing robust communication channels and protocols enables seamless exchange of threat intelligence, enabling SOC teams to stay ahead of evolving threats and bolster their resilience.

Lastly, collaboration with Information Sharing and Analysis Centers (ISACs) enriches SOC capabilities by leveraging collective expertise and resources. By participating in ISACs, SOC teams gain access to valuable threat intelligence, industry-specific insights, and collaborative initiatives, strengthening their cybersecurity posture and resilience against emerging threats.

Together, these themes underscore the importance of informed decision-making, collaboration, and innovation in SOC operations, ultimately enhancing cybersecurity resilience and safeguarding organizations against evolving cyber threats.

2.3 Potential Audience Analysis

In this paragraph, the demographics, interests, and behaviors of the target audience are summarized, followed by an analysis of their social media usage.

- **Threat Analysts**: These are typically professionals working in cybersecurity or information security roles. They often have a background in computer science, information technology, or related fields. They can vary in age but often fall within the range of mid-20s to mid-40s. They tend to have a high level of technical expertise and knowledge of cybersecurity tools and techniques. The geographic location may vary, but they are commonly found in regions with a strong presence of technology companies or cybersecurity firms.
- **Bachelor / Master students**: They are Enrolled in academic programs related to cybersecurity, information security, or computer science. Their age range may vary widely, from undergraduate students in their late teens to graduate students in their late 20s or beyond. They often have a strong interest in technology and computer systems. Their geographic location may vary based on the location of the educational institution they attend. They can come from diverse backgrounds, but many have prior experience or education in cybersecurity or software engineering fields.
- **Open Source Enthusiasts**: They are individuals with a passion for open source software and the principles of open collaboration and transparency. Their age range can vary widely, from young enthusiasts to seasoned professionals. They often have technical backgrounds in software development, engineering, or computer science. They are geographically dispersed but often clustered in regions with a strong technology industry or open source community presence. They tend to be highly engaged in online communities, forums, and platforms dedicated to open source software.
- **Engineering Students**: Enrolled in undergraduate or graduate programs in engineering disciplines such as cybersecurity or software engineering. Age range typically falls within the late teens to mid-20s, but can vary depending on the level of education. Have a strong interest in STEM (Science, Engineering, Technology and Mathematics) subjects and problem-solving. Ge-

ographically diverse, attending universities and colleges around the world. May come from various socioeconomic backgrounds, with a common interest in technology and innovation.

- **Security Professionals and SOC operators**: They are working in various roles within the cybersecurity field, including security analysts, engineers, consultants, and managers. Their age range can vary widely, from early career professionals to seasoned veterans. They often hold degrees or certifications in cybersecurity, computer science, or related fields. They are geographically dispersed but concentrated in regions with a strong technology industry or cybersecurity sector. They have diverse backgrounds and experiences, ranging from IT professionals transitioning into cybersecurity to specialists with years of dedicated experience in the field.

The analysis of the social media platforms used by the target audience for NGSOTI is described below:

- **X** (formerly known as Twitter): X provides real-time updates and discussions on various topics, including cybersecurity threats and incidents. Many security researchers and organizations share relevant information and analysis on X. X is is widely used by cybersecurity students to follow cybersecurity experts, organizations, and news outlets, as well as to participate in cybersecurity-related discussions and share relevant articles and resources. X is popular among engineers for staying updated on the latest news, innovations, and trends in their respective fields. Many engineering organizations, professionals, and industry influencers share valuable content and engage in discussions on X. X is used by open source enthusiasts to follow open source projects, developers, and organizations, as well as to participate in discussions using relevant hashtags like #opensource and #FOSS (Free and Open Source Software). X is widely used by SOC analysts and security professionals to follow cybersecurity experts, organizations. It provides real-time updates on security incidents, vulnerabilities, and threat intelligence, and allows professionals to engage in discussions using relevant hashtags like #cybersecurity and #infosec.
- **LinkedIn**: LinkedIn is used by threat analysts to network with other professionals in the cybersecurity field, share insights, and stay updated on industry news and trends. It is also popular platform for cybersecurity students to build professional networks, connect with industry professionals, join cybersecurity groups, and access job opportunities in the field. LinkedIn also is widely used by engineers for professional networking, job searching, and sharing industry insights. Engineers often join LinkedIn groups related to their field of expertise to connect with peers and participate in discussions. LinkedIn is used by threat analysts to network with other professionals in the cybersecurity field, share insights, and stay updated on industry news and trends. LinkedIn is used by open source enthusiasts to showcase their contributions to open source projects, connect with other professionals in the open source community, and stay updated on open source job opportunities and events. Many cybersecurity organizations and professionals share articles, research papers, and job opportunities related to cybersecurity on LinkedIn.

- **Reddit**: Reddit hosts a variety of cybersecurity-related communities (subreddits) where threat analysts can engage in discussions, share information, and seek advice from peers. Students can ask questions, share knowledge, and discuss cybersecurity topics with peers and professionals. Subreddits such as r/cybersecurity and r/netsec are particularly popular among cybersecurity enthusiasts. Subreddits like r/netsec and r/AskNetsec are popular among cybersecurity professionals for sharing insights and asking technical questions. Subreddits such as r/opensource and r/linux are popular among open source enthusiasts for discussions, news, and sharing resources related to open source.
- **Facebook Groups**: There are several private and public Facebook groups dedicated to cybersecurity and threat intelligence where analysts can share information and collaborate with others in the field. There are numerous Facebook groups focused on cybersecurity education, certifications, and career opportunities where students can connect with peers, seek advice, and share resources. Engineers may join Facebook groups focused on specific engineering topics, industries, or professional organizations to connect with like-minded individuals, share resources, and discuss relevant issues.
- **Information Security Forums**: Threat analysts may participate in specialized online forums and discussion boards focused on information security, such as the SANS Internet Storm Center (ISC) Forum or the Malwarebytes
- **Open Source Forums and Mailing Lists**: Online forums and mailing lists dedicated to open source software, such as the Linux Kernel Mailing List (LKML) and the Apache Software Foundation mailing lists, provide platforms for open source enthusiasts to ask questions, share knowledge, and discuss open source topics with peers and experts.
- **GitHub**: GitHub is a popular platform for hosting and sharing open source code repositories. Open source enthusiasts use GitHub to collaborate on projects, contribute code, report issues, and discover new projects to work on.
- **Security Blogs and Forums**: Online security blogs and forums, such as the SANS Internet Storm Center (ISC) Forum and the Krebs on Security blog, are valuable resources for SOC professionals to stay updated on security trends, research, and incident reports. These platforms allow professionals to discuss security issues, share insights, and seek advice from industry experts.
- **Engineering Blogs and Websites**: Engineers may follow blogs and websites dedicated to engineering news, projects, and innovations. Platforms like Medium, Engineering.com, and IEEE Spectrum feature articles, blog posts, and opinion pieces relevant to various engineering disciplines.
- **Threat Intelligence Platforms**: Some threat intelligence platforms have their own community forums or social media channels where analysts can discuss threats, share indicators of compromise (IOCs), and collaborate on research.

- **Engineering Forums and Communities**: There are numerous online forums and communities dedicated to engineering disciplines where engineers can ask questions, share knowledge, and seek advice from fellow professionals. Examples include Engineering Stack Exchange, Reddit's engineering-related subreddits, and various specialized forums.
- **YouTube**: YouTube hosts channels dedicated to open source software, development tutorials, and project showcases. Open source enthusiasts use YouTube to learn new skills, discover open source projects, and stay updated on the latest developments in the field. Engineers often use YouTube to access educational videos, tutorials, and demonstrations related to engineering concepts, tools, and technologies. Many engineering channels offer valuable insights and practical advice for engineers at all career stages. Students often use YouTube to access educational content, tutorials, and training videos on cybersecurity topics such as ethical hacking, penetration testing, and network security.
- **Discord**: Discord servers dedicated to cybersecurity provide SOC professionals with opportunities to collaborate in real-time, participate in Capture The Flag (CTF) competitions, and share threat intelligence. Many cybersecurity communities and organizations host Discord servers for their members to engage in discussions and networking.Discord servers dedicated to cybersecurity provide students with opportunities to engage in real-time discussions, participate in CTF competitions, and collaborate on cybersecurity projects with other students and professionals.
- **Information Security Conferences**: While not traditional social media platforms, information security conferences and events, such as Black Hat and DEF CON, provide opportunities for SOC professionals to network, learn about the latest security technologies and trends, and engage with industry leaders and peers.
- **Mastodon**: Mastodon is an open source decentralized social network that allows users to create and join communities (instances) based on shared interests. There are several Mastodon instances focused on open source software and technology where enthusiasts can connect with like-minded individuals.

2.4 Social media plan

The social media plan focuses on the audience analysis, the platform selection, the content strategy, the engagement strategy, the promotion and advertising, the monitoring and analytics, The social media plan is structured by an introduction, audience analysis, platform selection, content strategy, engagement strategy, promotion and advertising, monitoring and analytics, Team Roles and Responsibilities, Risk Management and Crisis Communication, Evaluation and Reporting. Only a subsection of the structure is used as parts of them are overlapping with the sections of this deliverable. In NGSOTI, a federated approach is utilized, relying on the existing communities and audience of the platforms of each partner within NGSOTI.

2.4.1 Platform Selection

This section describes the social media platforms used by the audience. The selection of social media platforms is based on audience demographics and platform suitability. In NGSOTI multiple platform will be used.

- NGSOTI is hosted on GitHub, where it will utilize the platform's features for community management. Additionally, a complementary open source platform like ForgeJo may be employed during the project. This is to ensure a mirrored version of the git repositories and to handle very large materials that cannot be accommodated on GitHub.
- X will continue to be utilized as long as it remains functional, taking into account future usage terms and community engagement.
- In addition to platform X, we will establish a list of Mastodon servers where communities can present their content as a backup option.
- Technical content will be published in blog posts, which will then be shared across other social media platforms and available newsletter.
- The participation in academic conferences is prioritized to enhance academic impact, including citation by other researchers, although acceptance is contingent upon community and reviewer evaluation.

2.5 Content Strategy

The content strategy includes the key messaging, the types of content to be shared such as articles, images, videos and infographics. Furthermore it includes a content calendar outlining posting frequency and schedule.

The Key Messaging of the NGSOTI project encapsulates essential information tailored to its audience, aiming to convey themes, ideas, and objectives consistently. It serves as a foundation for communication activities, influencing opinions and guiding decision-making within Security Operation Centers (SOCs). Through comprehensive documentation, practical software solutions, and effective data management strategies, SOCs can enhance their response capabilities and bolster cybersecurity measures. Collaboration with other SOC and ISACs further strengthens collective defense efforts, highlighting the importance of informed decision-making and collaboration in mitigating evolving cyber threats.The details are elaborated in the section of key messaging. In NGSOTI the focus is put on technical blog posts, academic publications and documentation on the progress of the NGSOTI infrastructure.

The content calendar, which outlines posting frequency and schedule, is linked to the table below. It delineates the tasks of the NGSOTI project, with each quarter denoted by 'Q' indicating the timeframe when the content can be published.

Dissemination task	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
NGSOTI components blog posts		✓		✓		✓		✓		✓		✓
Research publications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Lectures / Seminars	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
General endorsement of cybersecurity competence in present and future research agenda	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

2.6 Engagement Strategy

The approach to engaging with the audience, such as responding to comments, initiating discussions, and running polls, is integral to NGSOTI's outreach strategy. Multiple opportunities exist for interaction with the audience, whether through social media channels or during trainings, events, and conferences. During NGSOTI trainings, polls are conducted using services like Mentimeter to gauge participant capacity. Additionally, as NGSOTI components are open source, they encourage community interaction and involvement. Strategies for increasing follower engagement include regularly communicating about the different stages of the NGSOTI platform's creation, allowing the community to track its progress. Furthermore, NGSOTI will be referenced in training and teaching materials, which are encouraged to be reused under attractive open source licenses to foster community growth and accessibility for learning curiculum.

2.7 Monitoring and Analytics

NGOSTI relies on the tools and metrics available from the used platforms for monitoring social media performance, including engagement rates, reach, and impressions. These metrics are continuously monitored, and the social media plan may be adjusted based on insights gained. Key Performance Indicators (KPIs) are used to measure the effectiveness of the social media strategy.

For the trainings, two NGSOTI training performance reports are scheduled. The first report is due on 28/02/2025, and the second on 31/8/2025. Additionally, two maturity analyses, conducted before and after implementation, will measure changes in cybersecurity. The first analysis will be conducted at the beginning of the project, and the second at the end, to assess the impact of NGSOTI initiatives.

2.7.1 Key Performance Indicators (KPI)

Considering the current budget constraints, the table below presents the dissemination and communication KPIs. Lower KPI targets are proposed for newly piloted communication channels, allowing time to collect feedback and evaluate their relevance for future use.

Channel	KPI
LinkedIn	10
Facebook Groups	1
Information Security Forums	2
Open Source Forums and Mailing lists	1
Github	150
Engineering forums and Communities	10
Youtube	2
Information Security Conference	10
Mastadon	1

2.8 Team Roles and Responsibilities

The assignment of roles and responsibilities for social media management such as content creation, community management and analytics tracking are shown in the tale below:

Profile	Role in NGSOTI
Project manager	In the NGSOTI project, project managers are responsible for planning, organizing, and overseeing the execution of NGSOTI, ensuring its successful completion within the constraints of time, budget, and scope. In the dissemination phase, they are involved in coordinating between various profiles and also contribute to the writing aspects. They will contribute the community management and analytics tracking

Profile	Role in NGSOTI
Senior researcher	The senior researchers in NGSOTI are experienced professionals in the field of research who lead and conduct advanced studies, manage projects, and significantly contribute to the advancement of knowledge in their area of expertise. They play a crucial role in participating in seminars regularly organized within Work Package 4. Additionally, they are involved in writing academic papers that they present at highly ranked conferences or publish in reputable academic journals.
Senior engineer	An engineer is a professional who applies scientific knowledge, mathematics, and creativity to design, develop, and analyze solutions for various technical challenges and projects. Their role is to develop the technical content of the NGSOTI platform components. They are also disseminating the material within open-source communities.
Communication officer	Communication officers are responsible for overseeing and executing communication strategies, managing public relations, and maintaining positive relationships with stakeholders on behalf of an organization. Communication officers are typically bound by the policies and guidelines of their organizations. Their role in NGSOTI involves reviewing produced materials and distributing them across established communication channels that are not exclusive to NGSOTI.

2.9 Target Audiences

This section describes the groups or individuals who will benefit from the project's results

- **Security Operation Center (SOC) operators**. SOC operators are professionals responsible for monitoring, detecting, investigating, and responding to security incidents within an organization's SOC. Their primary role is to ensure the security and integrity of the organization's information systems and networks by continuously monitoring for potential security threats and vulnerabilities.
- **Security professionals**. They are individuals who specialize in ensuring the security, integrity, and confidentiality of information systems and networks. They typically possess expertise in various aspects of cybersecurity, including risk assessment, vulnerability management, incident response, and security architecture design. Security professionals may work in a variety of roles and industries, including cybersecurity consulting firms, government agencies, financial institutions, healthcare organizations, and technology companies. They are responsible for safeguarding sensitive data, identifying and mitigating security threats, and implementing security measures to protect against cyberattacks.
- **Engineering students**. They are individuals enrolled in academic programs focused on the study of engineering, a discipline that applies scientific principles and mathematical methods to design, develop, and innovate solutions to real-world problems. These students typically possess a strong aptitude for math and science and are passionate about understanding the physical world and creating practical solutions to complex challenges. Within NGSOTI they have access to solid practical background with real data in for their work as future SOC operators. This background consists of components from NGSOTI, allowing them to reuse it in their future professional activities.
- **Bachelor and master students**. They are individuals pursuing undergraduate and graduate degrees, respectively, at universities or higher education institutions. These students are typically enrolled in academic programs that offer a comprehensive curriculum in various fields of study. Within NGSOTI, they will gain ready-to-use knowledge of state-of-the-art open-source technology that they can apply in their future professional life. They will also have the opportunity to participate in internships to practice on the NGSOTI operational platform.
- **Threat analysts**. They are professionals responsible for identifying, assessing, and mitigating potential cybersecurity threats to an organization's systems, networks, and data. They utilize various tools, techniques, and threat intelligence sources to proactively detect and respond to security incidents, safeguarding the organization against cyberattacks.
- **Open source enthusiasts**. They are individuals who are passionate about open source software and the principles of open collaboration, transparency, and community-driven development. They actively contribute to open source projects, advocate for the adoption of open source so-

lutions, and engage in discussions and activities that promote the growth and sustainability of the open source ecosystem.

- **Communication materials**: In this section, the types of materials, such as reports, articles, presentations, and videos, that will be developed for dissemination are listed in the table below:

Communication material	Use cases
NGSOTI github repository	It is a public repository that includes data on the project management aspects of NGSOTI including its deliverables.
NGSOTI website	All the open source contribution available to the community are published on the NGSOTI website
Blog posts websites	Specific techniques, tooling or practices for SOC users
Videos	The videos produced in NGSOTI mainly focuses on cornerstones of NGSOTI platform such as MISP, AIL and D4.
Academic publications	Improved techniques or materials which advance the state-of-the-art
Presentations	Presentations will be performed at cybersecurity events whose objectives overlap with NGOSTI
Reports	During NGOSTI, multiple deliverables, milestones, and reports related to dissemination will be published

The produced material is listed below along with the date of publication.

Deliverable,milestones,reports	Due date
NGSOTI training performance #1	28/02/2025
NGSOTI training performance#2	31/08/2025
NGSOTI Internship announce	30/06/2024
NGSOTI deployment status report 1	31/12/2024

Deliverable,milestones,reports	Due date
Technical requirement analysis report collected	31/12/2024
NGSOTI data key findingsreport #1	30/11/2024
NGSOTI data key findings repory #2	30/11/2025
NGSOTI sustainability report	30/06/2026
References of training material updates #1	31/03/2025
References of training material updates #2	30/06/2026
Reports on NGSOTI training experience and WP3 data set	30/06/2026
Reference to lectures given at master courses on cybersecurity and cybersecurity practices	31/12/2026
References of training materials	31/12/2026
NGSOTI architecture document	31/03/2024
NGSOTI data collection blog post	30/09/2024
NGSOTI training experience blog post	30/06/2025
NGSOTI information sharing blog post	31/12/2025
Annual report on seminar and talks	31/12/2026
Research Agenda activity report	30/06/2026
Dissemination and exploitation deliverable	29/02/2024

2.10 Exploitation Plan

The main arguments for the significance of the effective dissemination and exploitation strategies are listed below.

2.10.1 Stakeholder Engagement

Effective stakeholder engagement is pivotal to the NGSOTI project, focusing on utilizing dissemination strategies that engage stakeholders throughout the project's lifecycle. By fostering dialogue, feedback, and collaboration, this approach enhances the relevance, credibility, and sustainability of the project outcomes.

The NGSOTI GitHub repository serves as a central hub for stakeholder interaction. It offers stakeholders the opportunity to access, reuse, and contribute to the project materials. This open-access model allows stakeholders to provide valuable feedback, suggest improvements, and engage in active dialogue, thereby fostering a collaborative and responsive development environment.

Forking a repository on GitHub is a key feature that benefits the NGSOTI project. It allows users to create a personal copy of the repository, enabling them to contribute to the project by experimenting with and modifying this copy, without affecting the original codebase. This process not only facilitates collaboration but also encourages community-driven development, allowing for experimentation and innovation in a controlled and safe environment. Forking also provides a means for backup and preservation of the code, ensuring its longevity and accessibility.

Creating issues on the GitHub repository is another crucial aspect of stakeholder engagement. It allows stakeholders to report bugs, suggest new features, or discuss improvements related to the project. This feature serves as a centralized platform for tracking, managing, and prioritizing tasks, promoting transparent and effective collaboration among contributors.

Furthermore, stakeholders are encouraged to create pull requests on GitHub. This feature allows them to propose changes to the repository, including bug fixes, new features, or improvements to existing code. Pull requests facilitate a collaborative review process, ensuring that all contributions align with the project's standards and goals before being integrated into the main codebase.

Finally, documentation and public project deliverables will also be made available on GitHub. This ensures that the community has access to the same interaction possibilities, maintaining a consistent and open platform for engagement and contribution.

In summary, the stakeholder engagement strategy for the NGSOTI project is built on a foundation of active and open participation, leveraging GitHub's features to foster a collaborative and dynamic development environment.

2.10.2 Influence and Policy Impact

The dissemination of the NGSOTI project's outcomes plays a crucial role in influencing policy development, decision-making, and implementation processes. By informing policy agendas, shaping legislative initiatives, and driving positive change, the project aims to have a substantial impact on the landscape of cybersecurity policies and practices.

A key strength of the NGSOTI project lies in the active involvement of its consortium members in prominent open-source security communities, such as the MISP project, AIL, and D4. This engagement ensures that the outcomes and findings of NGSOTI are regularly shared within these influential communities, fostering a broader reach and encouraging the integration of these insights into policy and practice.

Moreover, the open-source nature of NGSOTI's training materials is a pivotal aspect of its policy impact strategy. Education centers, trainers, and other stakeholders in the field of cybersecurity can freely reuse and adapt these materials to their specific needs. This accessibility not only facilitates the widespread dissemination of knowledge and best practices but also allows for flexibility and customization, ensuring that the training materials are relevant and effective in diverse contexts.

By adopting an approach that combines active community involvement with the provision of open-source educational resources, the NGSOTI project positions itself as a key contributor to the evolution of cybersecurity policies and practices. Its influence extends beyond immediate project outcomes, fostering an environment of continuous learning, adaptation, and improvement in the field.

2.10.3 Commercialization and Exploitation

Effective exploitation strategies are essential for converting research findings and innovations from the NGSOTI project into practical applications with commercial viability. These strategies are pivotal in supporting economic growth, enhancing competitiveness, and ensuring sustainability.

A significant advantage of the NGSOTI project is that its materials are distributed under an open-source license, which permits commercial use. This approach effectively removes barriers to exploitation and commercialization, making it easier for various stakeholders to adopt and adapt these resources for their own commercial endeavors.

The open-source licensing model adopted by NGSOTI greatly facilitates the exchange of information. It eliminates the need for complex contractual agreements, thereby streamlining the process of knowledge sharing and collaboration. This approach not only simplifies access to valuable resources but also accelerates the pace of innovation and application in the field.

Furthermore, the project leverages cross-publication with commercial vendors, utilizing the open-source tooling from NGSOTI. This collaboration highlights the industrial relevance and applicability of NGSOTI's contributions. By showcasing how these tools are used in commercial settings, the project demonstrates real-world value and encourages broader adoption and adaptation in various industrial contexts.

In conclusion, the NGSOTI project's approach to commercialization and exploitation, centered around open-source licensing, not only fosters a culture of open innovation but also paves the way for widespread application of its findings and tools in the commercial sector. This strategy is integral to maximizing the project's impact and contributing to the advancement of the cybersecurity field.

2.10.4 Intellectual Property Considerations

The NGSOTI project is committed to fostering collaboration and ensuring the reusability of its materials. To achieve this, all deliverables from the project will be licensed under an open-source li-

cense. This strategic approach is designed to streamline collaboration and enhance the accessibility of project outcomes.

The specific open-source licenses selected for NGSOTI materials will be those approved by the Open Source Initiative (OSI), listed as free software licenses by the Free Software Foundation, or classified as 'Compatible Licenses' in accordance with Article 5 of the EUPL (European Union Public Licence). These licenses are recognized for their compliance with established standards of open-source distribution, offering clarity and consistency in terms of intellectual property rights.

This licensing framework underpins the project's commitment to open innovation. By adopting licenses that are widely acknowledged and respected in the open-source community, NGSOTI ensures that its intellectual property is managed in a way that encourages sharing, adaptation, and further development. This approach not only aligns with the project's ethos of collaboration and transparency but also maximizes the impact and reach of its deliverables.

In summary, the intellectual property strategy of the NGSOTI project is carefully structured to promote widespread use and adaptation of its materials. By embracing recognized open-source licenses, the project paves the way for seamless collaboration and contributes to the advancement of knowledge and innovation in the field.

2.10.5 Sustainability

Sustainability is a crucial aspect of the NGSOTI project, focusing on how the results and contributions will be maintained and developed further beyond the project's lifespan. A key element of this sustainability strategy involves the integration of NGSOTI's outputs into various ongoing open-source projects.

A significant portion of the contributions made by the NGSOTI project are designed to have a lasting impact, persisting well after the project concludes. This enduring presence is achieved through the incorporation of NGSOTI's deliverables into established open-source projects like MISP and Tenzir. These platforms will serve as repositories and continuance vehicles for the innovations and tools developed by NGSOTI.

By embedding its contributions within these respected and widely-used open-source projects, NGSOTI ensures that its results not only remain accessible but also continue to evolve and improve with the broader open-source community's input. This approach not only extends the life of the project's outcomes but also enriches the ecosystem of tools available for cybersecurity, benefiting a wider audience and promoting continuous development.

In essence, the sustainability plan for the NGSOTI project is built on a foundation of long-term integration into the open-source community. This strategy ensures that the valuable work and advancements made by the project will be preserved, enhanced, and utilized well into the future, making a lasting contribution to the field of cybersecurity.

2.11 Budget

This section provides a breakdown of the resources allocated for dissemination and exploitation activities, including personnel, materials, and any external costs.

For the dissemination activities, mainly personnel costs are planned to be used. The total estimated costs anticipated for these personnel expenses are 172.270,00 EUR. The breakdown of person-months over 36 months is shown in the table below.Additional costs might arise for conference registrations, conference execution and journal publications.

Partner	Number of PM
LHC	2
Restena	4
University of Luxembourg	9
Tenzir	1

The allocated budget enables us to engage in regular dissemination activities.

2.12 Risk Management and Crisis Communication

Below is the table containing identified risks along with their corresponding mitigation strategies:

Risk Number	Risk description	Proposed mitigation
1	Changes in the platform's terms of use may render it unusable within NGSOTI.	Track the usage of platforms used by the target audience and engage with them accordingly. Additionally, cross-post items on multiple platforms.
2	Limited Reach. Risk that the dissemination channels chosen may not reach the intended audience effectively, resulting in low engagement or awareness.	Monitor the reach, record, and evaluate the data to promptly identify any issues and implement countermeasures as necessary.

Risk Number	Risk description	Proposed mitigation
3	Message Misinterpretation. Risk that the message conveyed through dissemination activities may be misinterpreted or misunderstood by the audience, leading to confusion or misinformation.	Involve strategies to ensure that the intended message is understood accurately by the audience. This includes using clear and concise language, supplementing text with visual aids, disseminating the message through multiple channels, encouraging feedback from the audience, providing additional educational resources, facilitating interactive engagement activities, testing the message with a sample audience, and offering training to stakeholders involved in dissemination. By employing these countermeasures, organizations can mitigate the risk of message misinterpretation and enhance the effectiveness of their communication efforts.
4	Resource Constraints: Risk that limited resources, such as budget or personnel, may hinder the execution of dissemination activities as planned.	Involve optimizing resource allocation, prioritizing key activities, and seeking alternative funding or collaborative opportunities to ensure the successful execution of dissemination activities despite limited resources.

Risk Number	Risk description	Proposed mitigation
5	Competing Priorities: Risk that competing priorities within the organization or project may divert attention and resources away from dissemination efforts, impacting their effectiveness.	Countermeasures for competitive priorities involve effective time management, clear prioritization of tasks, regular communication and coordination among team members, delegation of responsibilities, and flexibility in adapting to changing priorities. Additionally, establishing clear project objectives and aligning them with organizational goals can help mitigate the impact of competing priorities and ensure that dissemination activities remain on track. The priorities outlined in the grant agreement must take precedence.
6	Regulatory Compliance: Risk that dissemination activities may inadvertently violate regulatory requirements or ethical guidelines, resulting in legal or reputational consequences.	Countermeasures include thorough compliance with regulations, regular policy reviews, robust monitoring, staff training, clear reporting channels, prompt issue resolution, and seeking legal guidance as needed.

3 Conclusion

In conclusion, the NGSOTI project's success hinges significantly on an effective communication plan and dissemination strategy, particularly highlighting its commitment to utilizing open-source tools in training the next generation of SOC operators. This emphasis on open-source resources not only showcases the project's innovative approach to cybersecurity training but also aligns with the broader goal of making high-quality, accessible tools available for skill development in key areas like detection engineering, incident response, and threat intelligence analysis. Collaborations with partners such as CIRCL, Restena, Tenzir, and the University of Luxembourg underscore the project's dedication to creating a real operational infrastructure for hands-on training, blending academic curricula with practical industry insights.

The open-source nature of NGSOTI enables a dynamic and collaborative learning environment, encouraging contributions and feedback from a global community of cybersecurity experts and learners. This aspect will be a focal point in our communication and dissemination efforts, leveraging various channels such as social media, industry forums, and academic networks. Highlighting the open-source tools and methodologies used in the project not only promotes transparency and inclusivity but also inspires innovation and continuous improvement in cybersecurity practices.

Regular updates, featuring both the progress of the project and success stories, will further illustrate the practical application and impact of open-source tools in cybersecurity training. By articulating the benefits and achievements of NGSOTI, the communication plan aims to attract a wide range of participants and stakeholders, positioning the project as a leader in open-source cybersecurity education. Ultimately, the successful execution of this communication strategy will play a crucial role in preparing a new generation of SOC operators, equipped with the open-source skills and knowledge necessary to address the evolving challenges in cybersecurity.