Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

Project: 101190232 - aSIEMmetry
D1.3 - Communication, Dissemination and Exploitation Plan

expertware VUB ARTIFICIAL INTELLIGENCE RESEARCH GROUP DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICĂ

Document Control

Title	**D1.3 - aSIEMmetry Communication, Dissemination and Exploitation Plan**
Version:	0.3
Release Date:	30/06/2025
Author:	Expertware, DNSC
Total Pages:	24
Security Class:	PU
Distribution:	This document is intended for public distribution. It may be shared, cited, or published without prior approval, provided that the content is not altered and proper attribution is maintained.
Disclaimer:	

Document Approval

Expertware Approver	Lucian Vizeteu	Project coordinator
DNSC Approver	Valeria Popescu	Project Manager
VUB Approver	VUB	Project Manager

Revision History

Version	Date	Issued By	Status	Comments (Update this history table for each version)
0.1	15/05/2025	@aSIEMmetry Project Management	Draft	Initial draft
0.2	16/06/2025	@aSIEMmetry Project Management	Draft	Contributions to sections
0.3	20/06/2025	@aSIEMmetry DNSC Beneficiary Partner	Edited	Editing, format and Introduction changes.
0.4	30/06/2025	@aSIEMmetry Project Management	Final for approval	Final corrections and approval
0.5				
0.6				
0.7				
0.8				
1.0				

Contents

1 Introduction 3
1.1 Background 3
1.2 Executive summary 4
2 Communication, Dissemination and Exploitation Strategy 5
2.1 Communication and Dissemination and Exploitation main goals 5
2.2 Communication and Dissemination main activities 6
2.3 Partner Engagement for Model Validation & Exploitation 6
2.4 Partners Engagement Channels for cyber sec research and training 7
2.5 Target Audiences and Stakeholder Mapping 7
3 Communication, Dissemination & Engagement Channels 9
3.1 Project Intranet web site 9
3.2 Project Public Website 10
3.3 Social Media Channels 12
3.4 Newsletters 14
3.5 Conferences and Events 14
3.6 Webinars & Demo Workshops 15
3.7 Demonstrations in EU related events & forums 16
3.8 Media Relations & Print 16
3.9 Engagement with EU Cybersecurity Ecosystem 16
4 Communication, Dissemination & Engagement activities 18
4.1 Project Visibility Toolkit 19
5 Dissemination, Communication and partner engagement KPIs 20
5.1 Communication and Dissemination KPIs 20
5.2 Enhanced SOC processes 20
6 Glossary of Acronyms and Abbreviations 22

1 Introduction

1.1 Background

The **aSIEMmetry project** aims to reinforce the operational capabilities of Security Operation Centers (SOCs), both private and national, by introducing advanced workflows built on artificial intelligence (AI) and machine learning (ML). Funded under the **DIGITAL-ECCC-2024-DEPLOY-CYBER-06** call by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), DIGITAL JU Simple Grants (contract no. 101190232), the project is coordinated by **EXPERTWARE SRL** (Romania), in collaboration with **Vrije Universiteit Brussel** (Belgium) and the **Romanian National Cyber Security Directorate (DNSC)**.

Through the research of two innovative AI-driven models— **"security entropy"** and the **"LLM SOCagent"**—aSIEMmetry intends to complement and enhance existing SIEM systems, enabling proactive threat detection, reducing analyst burden, and increasing the response efficiency. The project directly addresses critical challenges faced by SOC teams: increasing data volume and complexity, the urgent need for rapid incident containment, and the shortage of high-skilled cybersecurity professionals.

The aSIEMmetry project aims to enhance the capabilities of Security Operation Centers (SOCs), both private and national, through the development of advanced processing workflows based on machine learning (ML) and artificial intelligence (AI). The project focuses on proactively detecting new risks associated with assets monitored by SIEM (Security Information and Event Management) systems, improving SOC processes and analyst activities by leveraging AI capabilities.

aSIEMmetry represents a novel approach enabling machine learning and AI models as a complement of existing SIEM information to proactively detect novel threats and empower the SOC analysts with AI capabilities.

The project enriches the capabilities for the SOC teams to pinpoint risky actions combing huge data sets collected by various agents into the SIEM data lake with UEBA analytics, enhance their capabilities to respond to security incidents using a specialized "LLM SOCagent".

It addresses three pain points faced today by the Security Operating Centers:

a. High(er) volume of security related events/information and the inherent complexity
b. Time to contain security attacks is critical
c. Shortage of highly skilled individuals/resources

aSIEMmetry aims to leverage new generation detection methods and continuously improve the detection speed starting from a "security entropy" mathematical model, refining the alerts so it better addresses false positives, scale and simplify the discovery of previously unseen anomalies.

The project approaches these challenges (pain points a and b) from a different angle reducing the dimensionality of the model, identifying significant properties which impact the overall security posture of an asset and its surroundings.

1.2 Executive summary

The aSIEMmetry dissemination and exploitation plan aims to maximize the impact of the project's innovations in enhancing the capabilities of Security Operations Centres (SOCs).

To ensure the visibility, trustworthiness, and adoption of these technologies, this document defines a targeted dissemination and communication strategy, along with concrete actions and measurable objectives to actively engage key stakeholders, including SOC teams, cybersecurity researchers, and public sector institutions throughout Europe.

The plan covers:

- Identification of relevant audiences and stakeholders,
- Selected channels and formats for outreach (e.g. Website, social media, newsletters, technical webinars, workshops),
- Timing and sequencing of dissemination and engagement activities,
- Key performance indicators (KPIs) to monitor communication impact.

Activities are synchronized with the project's technical milestones to ensure timely and effective communication of progress. Stakeholder engagement efforts include promoting the "security entropy" model to SOC practitioners, raising awareness about the development of the "LLM SOCagent" model, and facilitating collaboration with cybersecurity analysts and research organizations across the EU for validation and refinement.

Continuous coordination with other EU-funded cybersecurity initiatives will ensure that aSIEMmetry's results are interoperable, relevant, and contribute meaningfully to strengthening cybersecurity across Europe.

2 Communication, Dissemination and Exploitation Strategy

The aSIEMmetry project includes specific communication, dissemination, and stakeholder engagement activities aimed at raising awareness, promoting project results and impact.
The Communication and Dissemination Strategy of the aSIEMmetry project is designed to ensure that the project's goals, progress, and results are clearly conveyed to key stakeholders across the cybersecurity and AI ecosystem. It also aims to maximize the project's impact by facilitating understanding, knowledge transfer, adoption of results, and long-term sustainability.

This strategy is guided by the distinction between:

- **Communication**, which focuses on raising awareness about the project among broader, non-specialist audiences, and on making the project visible at European and international levels;

- **Dissemination & Exploitation** which targets more specialized groups (e.g., SOC operators, researchers), with the goal of promoting and transferring project results knowledge, and tools developed during the project that can be reused, implemented, or further developed, creating long-term value beyond the project's duration.

The strategy adopts a multi-channel, audience-centric approach aligned with AI and cybersecurity topics, and also focuses on fostering a collaborative ecosystem among project partners, industry stakeholders, and the broader cybersecurity community to drive knowledge sharing and accelerate adoption of aSIEMmetry outputs.

2.1 Communication and Dissemination and Exploitation main goals

Considering the duration of the project and the Work Packages assigned to every stage of the project, the main objectives of the communication and dissemination activities are correlated to the **WP1 dissemination and communications** for the duration of the whole project:

- To ensure coordinated communication within the project consortium and alignment across all partners.
- To disseminate project results—including AI models, anomaly detection queries, and integrated HI+AI (human + AI) blueprints—towards relevant technical and key stakeholders.
- To engage with cybersecurity actors such as other **CSIRTs**, **SOCs**, **NIS2-regulated organizations**, **and MSSPs**, in the validation, feedback, and co-development of aSIEMmetry outputs.
- **To attract interest from academic and research organizations,** facilitating collaboration on use case exploration, testing, and knowledge transfer.
- **To increase visibility and awareness** of the project's goals, progress, and relevance to key societal and technological challenges in cybersecurity and AI,
- **Raise awareness about the EU's investments** and active role in promoting cybersecurity and innovation and how the project contributes to safer digital environments for citizens, businesses, and institutions.

- **To promote the project's results** and enable their uptake by target stakeholders such as SOC teams, AI researchers, industry partners, and national/international cybersecurity authorities.
- **To support engagement and collaboration** with relevant EU-funded initiatives, networks, and communities.
- **To facilitate knowledge sharing** and two-way communication between the consortium, technical experts and the public.
- **To contribute to the sustainability and exploitation** of project outcomes by ensuring results are understandable, accessible, and well-positioned in the cybersecurity and AI domains.

This communication framework will evolve in parallel with the project's work packages, ensuring that strategic messages, tools, and actions are deployed in an impactful, and stakeholder-centric manner.

2.2 Communication and Dissemination main activities

Communication and dissemination activities in aSIEMmetry are focused on informing a wide range of audiences about the project's objectives, progress, results, and their relevance to the evolution of Security Operations Centres (SOCs).

These efforts will highlight the project's AI/ML-driven innovations, such as the *"security entropy"* multi-agent model and the *"LLM SOCagent"*, which are designed to continuously detect cybersecurity anomalies and support advanced decision-making in SOC environments.

The aSIEMmetry team will utilize multiple communication channels to ensure consistent messaging and maximize reach. These include:

- The project website, offering updates, publications, and news items.
- Social media (LinkedIn) for broader outreach and engagement.
- Technical webinars and presentations at conferences.
- Academic publications and\or white papers targeting research communities.

Content will be curated and reused across formats and platforms to boost visibility (e.g., re-share, re-post, amplify via project partners).

2.3 Partner Engagement for Model Validation & Exploitation

This section focuses on engagement activities that aim to onboard and collaborate with partners interested in validating the *"security entropy"* and *"LLM SOCagent"* models developed within the project. These efforts are crucial for ensuring real-world relevance and operational adoption of aSIEMmetry's technological outputs.

Engagement will be promoted via:

- The project website and internal collaboration tools;
- Webinars/content targeting SOC teams across the EU;

- Participation in cybersecurity working groups \EU forums\conferences;
- Online forms and opt-in mechanisms for validation partners to share anonymized feedback or event data.

2.4 Partners Engagement Channels for cyber sec research and training

This section covers engagement activities aimed at expanding the network of partners contributing to the validation and improvement of the aSIEMmetry models, as well as the population of the research environment with anonymized SOC data.

Collaboration will be promoted via the project website, partner intranet, and other communication channels detailed in this document.

2.5 Target Audiences and Stakeholder Mapping

To ensure that communication and dissemination activities are effective and impactful, the aSIEMmetry project identifies and categorizes its key target audiences. These audiences represent the main communities that will benefit from, contribute to, or support the project's objectives during and beyond its execution.

Internal Audiences

Direct communication among aSIEMmetry partners will be maintained through:

- Stakeholder coordination groups
- Project management and technical work package teams
- Secure collaboration environments (intranet, repositories)

External Communication & Dissemination Audiences

- EU-based public and private SOC teams involved in the validation phase
- Cybersecurity EU research centres and academic partners
- Innovation clusters and cybersecurity communities
- EU institutions and peer organizations: ENISA, ECSO, ENDR
- SMEs across Europe aiming to strengthen their cybersecurity posture
- Key Stakeholder groups, including CSIRTs, SOCs, organizations in sectors specified by NIS 2 Directive, members of the Computer Security Incident Response Teams (CSIRTs) network and other MSSPs
- Digital innovation hubs / clusters

Partner Engagement audiences

- EU peered organizations: ENISA, ENDR, ECSO
- EU SMEs looking to uplift their security posture
- SOC and CSIRT teams interested in the adoption of ML/AI-driven detections
- Organizations contributing to open threat intelligence and cybersecurity knowledge
- Other EU projects and cybersecurity initiatives seeking interoperability and synergy with aSIEMmetry's findings

General Public and Media:

Communication efforts targeting the general public and media aim to increase understanding of how European investments in cybersecurity and artificial intelligence contribute to safer

digital environments. Through accessible messaging the project will highlight the benefits of trustworthy, human-centred technologies, helping to build public confidence in the ethical use of AI and demonstrating the tangible outcomes of EU support in securing the digital future.
This mapping will be regularly reviewed and refined throughout the project lifecycle to include new stakeholders and adjust approaches based on feedback and project developments.
Each stakeholder group will be engaged through tailored communication formats and frequency, ensuring relevance and maximizing participation. For instance:

- SOCs and CERTs will be reached via technical briefings, hands-on demos, and secure knowledge exchange environments;
- Researchers and academics through scientific publications, open-access datasets, and collaborative events;
- Policy makers through white papers, policy briefings, and participation in EU cybersecurity forums;
- Broader audiences via social media, public-friendly content, media coverage, and visual storytelling.

This mapping will be regularly reviewed and refined throughout the project lifecycle to include new stakeholders and adjust approaches based on feedback and project developments.

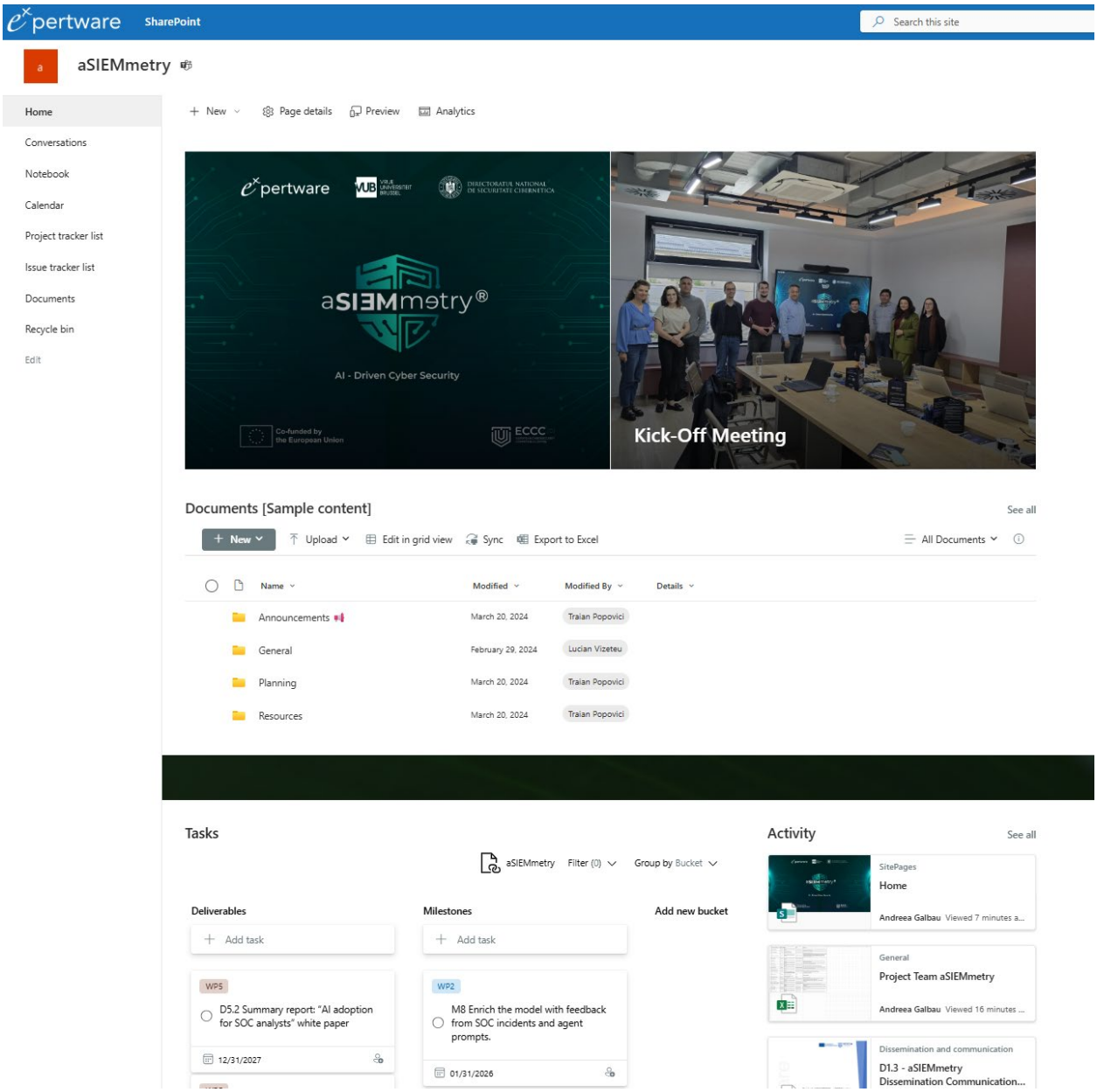
3 Communication, Dissemination & Engagement Channels

To ensure the effective reach and visibility of the aSIEMmetry project, a diverse and strategically selected set of channels and formats will be used throughout the project lifecycle. These actions are aligned with the identified audiences and messages, and will evolve as the project progresses.

3.1 Project Intranet web site

URI	https://expertware.sharepoint.com/sites/ aSIEMmetry General | aSIEMmetry | Microsoft Teams
Audience	Internal only [Expertware + DNSC +VUB)
Data residency	EU
Status	Live since January 2025
Authentication	Required. Supports Microsoft 365 federations. Supports guest accounts for trusted entities.
Communication Content	Project Management documents. aSIEMmetry KPI reporting see. aSIEMmetry deliverables drafts & final documents. aSIEMmetry Technical documents. aSIEMmetry Use case definitions (see HLD) aSIEMmetry Partner Exchange libraries Research papers How-to' s Communication KPIs Engagement KPIs

Intranet Home page



3.2 Project Public Website

The public website will serve as the project's main communication and dissemination hub. It will be launched in the early stages of the project and will provide clear, user-friendly, and regularly updated content for a variety of audiences: disseminating news, project results, partner engagement and activities related to aSIEMmetry.

It will offer curated links to publications, blog articles, or cross-project news that are relevant to the AI/cybersecurity community.

Figure 2 gives an overview of the layout for the public web site and below you can find the main functionalities which are to be implemented before M6 when the dissemination and partner engagement activities are planned to start.

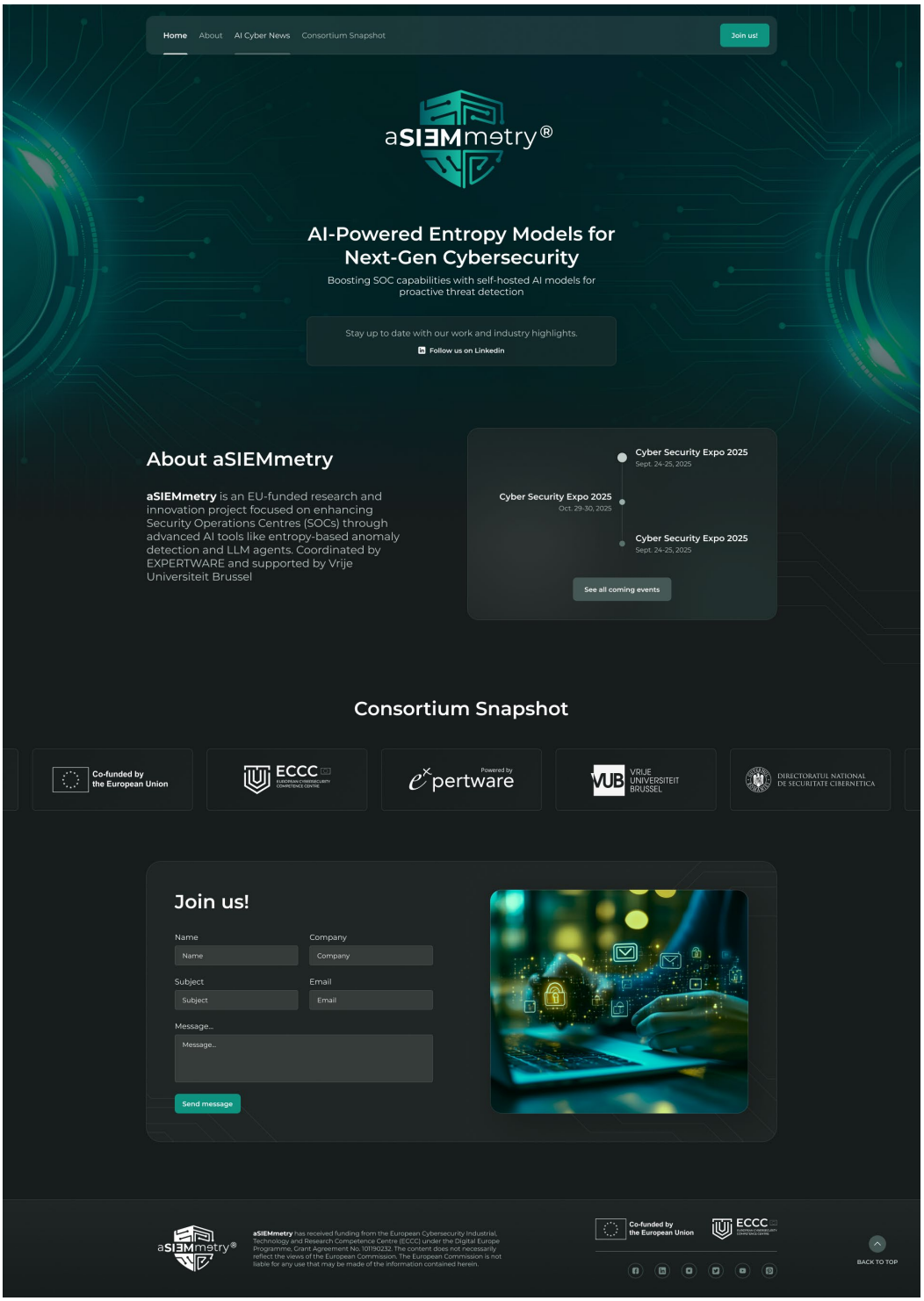
The site structure will enable continuous updates of news and technical achievements and will facilitate use case collaboration.

The platform will facilitate dialogue with external experts and allow exploration of the project's tools and results for broader relevance.

Communications & engagements shared via the public web site

URL	
Audience	Public with authenticated module for partners
Data residency	EU
Status	Planned launch M6
Authentication	Anonymous & authenticated Supports federation based on Microsoft Azure guest
Communication & Dissemination Content	Project Management news labelled as public. ASIEMmetry Project Progress Milestones aSIEMmetry Project description aSIEMmetry Technologies aSIEMmetry deliverables, white papers, public documents webinars aSIEMmetry Results & public KPIs
Engagement Content	aSIEMmetry partner onboarding aSIEMmetry Training partner onboarding aSIEMmetry Cyber Security News / Feeds ASIEMmetry Discussion Forums / Q&A Section Events Calendar Resource Center

Entry website home page



Expression of Interest form (for demonstrations, testing, feedback, exploitation)

3.3 Social Media Channels

Social media is an essential tool to promote project updates, connect with cybersecurity and AI communities, and amplify project results. The main social media presence will be on

LinkedIn, where a dedicated project page has already been created. The content includes weekly posts highlighting progress, news items, event participation, partner meetings, and general content related to cybersecurity and AI. To improve visibility, content will be regularly reshared via the partners' social media accounts and amplified via tagging, mentions, and cross-posting. Visual content such as infographics, quote cards from technical leads, or short demo videos will be included to increase engagement.

Twitter/X and Discord will be evaluated as additional platforms depending on the evolution of the project. Twitter/X may support outreach to the innovation community, while Discord may enable deeper technical conversations with students or open-source communities if community interest is demonstrated. These may be activated depending on the partner's capacity and engagement needs. The team will also monitor platform metrics (followers, impressions, engagement rate) to decide where to allocate resources.

Content calendar: A simple content calendar will guide weekly or bi-weekly posts, including major project milestones, consortium meetings, technical deliverables, and participation in events. The calendar will also help synchronize posts with relevant cybersecurity awareness days or EU-level campaigns.

The engagement strategy involves promoting the aSIEMmetry partnership offering via the dedicated web site and the social media accounts managed by the project partners: Expertware, DNSC and VUB (Vrije Universiteit Brussel). During the project lifecycle we aim to broader the federation ecosystem resharing and reposting relevant messages with other entities interested in the aSIEMmetry results. Each partner will commit to resharing core content at predefined project milestones (e.g., demos, deliverables, events), ensuring broader outreach through distributed visibility.

Hashtags such as #aSIEMmetry, #AI, #Cybersecurity, #MachineLearning, #EUfunded or #AIsecuriy will be adopted to connect with relevant online conversations and make posts easier to find.

The initial list of social media channels which will be used to promote the project and engage research & training partners:

Platform	URI	Owner	Status	Followers
LinkedIN	aSIEMmetry: Prezentare generală | LinkedIn	Consortium	Active	81
LinkedIN	Directoratul Național de Securitate Cibernetică: Anunțuri | LinkedIn	DNSC	Active	24.610
LinkedIN	https://www.linkedin.com/company/expertware/	Expertware	Active	2068
LinkedIN	Vrije Universiteit Brussel: Anunțuri | LinkedIn	VUB	Active	120.620
LinkedIN	(10) ERIS VUB TechTransfer: Anunțuri | LinkedIn	VUB		1.162
Instagram	https://www.instagram.com/expertware_net/	Expertware	Active	395
Facebook	https://www.facebook.com/expertware.net	Expertware	Active	637
Instagram	DNSC (@dnsc.ro) • Instagram photos and videos	DNSC	Active	3.599
Facebook	Facebook	DNSC	Active	70.060

3.4 Newsletters

Periodic communication tool targeting subscribed stakeholders, industry, and research followers. Periodic newsletters will keep internal and external stakeholders informed about project developments, achievements and upcoming events.

The newsletter will be maintained on the project intranet and public website or via LinkedIn, or via an opt-in email list. The updates will cover information regarding the project progress, results, threat intelligence news, research communities, partner organization engagements, spotlights on consortium partners, upcoming events etc. Starting in Month 15, the project team will distribute the aSIEMmetry newsletter on a triannual basis (every four months).

Project team will ensure that the content is informative, fresh, accessible, and relevant for the cyber security communities. Partners organisations engaged will be encouraged to repost, re-share so results are disseminated, and benefits shared with broader audiences.

3.5 Conferences and Events

Participation in relevant conferences and industry events will form a major component of the project's dissemination strategy.

An important dissemination and engagement channel is presence to European conferences and exhibitions related to cyber security field. This will include not only large pan-European events but also specialized niche conferences and workshops where targeted communities gather.

Identify key cybersecurity conferences, events, exhibitions in the EU and at the national level, ensuring participation to showcase aSIEMmetry's features through live demonstrations. This hands-on approach can effectively communicate the project's value to potential users and partner entities. Demonstrations will be designed to be interactive where possible, encouraging questions and direct feedback from attendees to better understand user's needs.

Participation at these events can include speaking engagements, panel discussions, network with stakeholders or having a dedicated booth. This will increase visibility and networking opportunities for aSIEMmetry within the cybersecurity community. Additionally, preparing clear takeaway materials (e.g., brochures, one-pagers, demo videos) will support follow-up discussions after events.

Based on the perceived dissemination and engagement impact, we have shortlisted key events and conferences. From these, we will select those most aligned with the project's evolution and with the potential to maximize visibility and stakeholder engagement throughout the aSIEMmetry project lifecycle. Event participation will be regularly reviewed and adjusted according to project milestones and feedback from previous engagements to optimize impact.

Event	Location	Calendar
Cybersec Europe https://www.cyberseceurope.com/	Brussels, Belgium	Yearly (May 2025, 2026, 2027)
Cyber security & Cloud Expo Europe https://cybersecuritycloudexpo.com/europe/	Amsterdam, The Netherlands	Yearly (September 2025, 2026, 2027)
Barcelona Cybersecurity Congress https://www.barcelonacybersecuritycongress.com/	Barcelona, Spain	Yearly (2026, 2027)
Cloud Security Expo https://www.cloudsecurityexpo.de/	Frankfurt, Germany	Yearly (2026, 2027)

Black Hat Europe https://www.blackhat.com/upcoming.html	London, United Kingdom	Yearly (Dec 2025, 2026, 2027)
Cyberwisecon https://cyberwisecon.eu/	Vilnius, Lithuania	Yearly (May 2025, 2026, 2027)
EU Cyber Acts https://eucyberact.org/	Brussels, Belgium	12-13 Mar 2024
Conference on Science of Cyber Security https://scisec.org/	Copenhagen, Denmark	Yearly (Aug 2025, 2026, 2027)
Defcamp https://def.camp/	Bucharest, Romania	Yearly (Nov 2025, 2026, 2027)
Websummit https://websummit.com/	Lisbon, Portugal	Yearly (Nov 2025, 2026, 2027)
ENISA events & conferences https://www.enisa.europa.eu/events#b_start=0	Brussels, Belgium	Tbd
DNSC Cybersecurity Conference	Bucharest, Romania	Yearly (Oct 2025, 2026, 2027)
National Conference in the field of Cyber Security organized by ISACA and Romanian National Bank	Bucharest, Romania	Yearly (Dec 2025, 2026, 2027)
Bucharest Tech Week https://www.techweek.ro/	Bucharest, Romania	Yearly (June 2025, 2026, 2027)
GoTech Work https://www.gotech.world/	Bucharest, Romania	Yearly (Nov 2025, 2026, 2027)

The list is not limited to the conferences mentioned above and it will be extended if other relevant events are identified. aSIEMmetry project team intends to spread participation to different events each year, nationally or at European level, so we ensure broad results dissemination and engagement for European partners.

3.6 Webinars & Demo Workshops

Besides the already established events and conferences, we will organize project specific webinars & workshops to facilitate regional information dissemination and engagements (demo for novel SOC detection methods, Walkthrough HI+AI use cases in SOC, best practices identified etc.).
Two events will be organized by the project — one mid-term to showcase early results and gather feedback, and one final event to demonstrate full capabilities and encourage uptake. These actions will help build credibility, generate interest, and support cross-project collaboration.

Event	Locations	Calendar
aSIEMmetry Demos – Webinars	Expertware Suceava, Romania Expertware Suceava, Romania VUB, Brussels	May-Aug 2026, 2027 tbd
aSIEMmetry Regional Partners engagements	DNSC Bucharest, Romania Expertware Suceava, Romania VUB, Brussels	Sept-Nov 2026, 2027 tbd

aSIEMmetry project results event will be organized in a hybrid manner, to ensure a wider audience and will be announced via the project web site and the social media channels and enrolment will be free so interested entities can subscribe and participate.

To maximize the effectiveness, we will complement the open registration with a personalized invitation process, sending direct engagement email to relevant actors from the cybersecurity

industry and representatives of the essential sectors, SMEs, public organizations, other cybersecurity MSPs potential users.

3.7 Demonstrations in EU related events & forums

aSIEMmetry will actively seek visibility and alignment within the broader European cybersecurity landscape by participating in relevant EU-level events and conferences, engage in events and forums specifically focused on EU cybersecurity initiatives and projects. Participation will be carefully selected to align with project milestones and ensure relevance to ongoing EU cybersecurity priorities.

The project aims to **demonstrate key technical results and AI-driven innovations** at EU projects **community workshops and academic events**. These demonstrations will not only showcase the project's scientific and technological progress but will also serve to foster dialogue with cybersecurity practitioners, and representatives of other EU-funded initiatives. Demonstrations will be designed to encourage interactive discussions, including Q&A sessions and feedback collection, supporting potential collaborations and synergies across projects.
Engagement in such events will help position aSIEMmetry as a contributor to Europe's cybersecurity resilience and ensure that project results are visible, credible, and potentially reusable by the wider EU ecosystem. This ongoing engagement will also support sustainability efforts, helping to integrate aSIEMmetry's outputs into future EU cybersecurity frameworks and initiatives.

3.8 Media Relations & Print

Media engagement will ensure that project developments reach wider public and sector audiences. Press releases will be issued at major milestones (e.g. project launch, pilot deployment, final demonstration), and will be adapted for both specialist and non-specialist media. Special attention will be given to local and regional coverage in countries where the project partners are based.

The aSIEMmetry marketing team will develop a range of high-quality visual and written materials to support communication, education, and reuse.
Where relevant, materials will be translated into the languages of the consortium partners to support national dissemination, otherwise will be created in English.

3.9 Engagement with EU Cybersecurity Ecosystem

To amplify its impact and ensure alignment with other EU-funded efforts, aSIEMmetry will engage with the broader EU cybersecurity and AI ecosystem. The project will establish connections with other EU cybersecurity initiatives and projects, fostering collaboration and knowledge sharing.

Active collaboration will be pursued through webinars, partnerships, mailing lists, or participation in collaborative projects, strengthening the overall cybersecurity ecosystem. Regular joint activities, such as co-hosted webinars or shared workshops, will be organized to maintain momentum and foster continuous dialogue.

In particular, the project will seek opportunities for interoperability, data sharing, or pilot alignment with other projects in areas like threat intelligence, LLM safety, or explainable AI for security. Collaboration approaches will be adjusted based on feedback and emerging needs within the ecosystem to maximize relevance and impact.

These conferences/forums represent key opportunities to demonstrate technical results, gather stakeholder feedback, explore exploitation pathways, and connect aSIEMmetry with the broader EU cybersecurity strategy. Sharing tools, datasets, and best practices with other projects will help avoid duplication and accelerate innovation.

4 Communication, Dissemination & Engagement activities

The aSIEMmetry project will implement an integrated set of communication and dissemination actions to ensure its visibility, build stakeholder engagement, and support the uptake of its results across the cybersecurity and AI communities. These actions will be tailored to the needs of target audiences and aligned with the project's objectives and phases. A balanced mix of digital tools, physical presence, and content formats will be used to reach both expert and non-expert stakeholders. For each activity type we established clear targets which will be measured and reported as per aSIEMmetry project reporting targets.

Activity	Audience	Channels & methods	M1-M18	M19-M36
Kick-off Meeting	All partners	Kick-off meeting with all partners	M1	
Project Website	All EU interested entities	Social Media	By M3 aSIEMmetry website created, monthly updates	
aSIEMmetry project Intranet platform launch	Internal only (DNSC+Expertware)	Newsletter, direct communication	M1 weekly updates	-
Social Media - LinkedIn,	Public announcements - All interested entities	DNSC, VUB, Expertware to announce the aSIEMmetry pages to their followers	By M3 aSIEMmetry pages created, monthly updates	-
aSIEMmetry results dissemination, partner engagement, Community Dialogs, SOC Runbooks, project results	EU Cybersec national and international communities (ECCC, ENISA, EDF, SMEs associations)	Participation to national and international Cyber Security conferences showing the results and promoting aSIEMmetry	Start WP4 + 1M	4 international conferences
Academic publications/ Scientific journals	All interested entities	Article publications in scientifical journals in the fields of cyber security and/or ML/AI, indexed in international database	Start WP 5 targeting minimum 2 articles	
aSIEMmetry webinars & workshops	All interested entities	Demo for novel SOC detection methods, organized by DNSC & Expertware. Registration via project web site and Social Media channels.		As of M24 - 2 webinars As of M33 – 1 workshop
aSIEMmetry research results/ newsletter	All EU interested entities	Social Medial channels Project Website	1 update	5 updates
Intermediate project reports	Restricted to partners	Separate report	M12	M24
Intermediate dissemination report	Restricted to partners	Separate report		M24

Final project report	Restricted to partners			M36
aSIEMmetry project closure	All EU Interested entities	Press Conference, An event organized by EXPERTWARE, DNSC to announce overall results		Until 31 dec 2027

4.1 Project Visibility Toolkit

To support partners in promoting the aSIEMmetry project effectively and consistently, a comprehensive Dissemination Toolkit has been developed and stored in the project intranet.

The toolkit will include:

- Project logo and visual identity guidelines
- Branded templates for PowerPoint presentations, flyers, roll-ups, event posters, and social media cards
- A partner briefing pack for event participation and partner onboarding

These resources are hosted on the internal SharePoint portal (https://expertware.sharepoint.com/sites/aSIEMmetry) and are periodically updated to reflect project needs and partner feedback. Consortium members are encouraged to use the toolkit to ensure coherent messaging and professional branding throughout all communications.

The project's dissemination strategy emphasizes visibility and engagement through established digital channels:

- LinkedIn: The central communication channel, with regular project updates via the aSIEMmetry Showcase page and partner cross-posts from DNSC, VUB and Expertware.
- Facebook and Instagram: Used by Expertware to share visual content, key milestones, and partner-focused messages.
- News Updates: Published on the project website to consolidate announcements, events, and results.
- Event Amplification: Online posts synchronized with aSIEMmetry's presence at major cybersecurity events (e.g., CyberSec Europe, DNSC conferences), reinforcing visibility across platforms.
- Performance Monitoring: Engagement is tracked via website analytics, LinkedIn Analytics and Meta Business Suite (impressions, clicks, shares, reach).

5 Dissemination, Communication and partner engagement KPIs

To ensure that communication and dissemination efforts are effective, measurable, and aligned with the project's objectives, the aSIEMmetry project defines a set of KPIs (Key Performance Indicators). KPIs will help the team track progress, identify areas for improvement, and demonstrate the project's impact to stakeholders. KPIs are organized by communication tools or activity, and are linked to the project's target audiences, outreach goals, and innovation impact expectations. They will be reviewed periodically to ensure they remain relevant throughout the project lifecycle and adapt to evolving communication needs.

This document section highlights also the reporting KPIs, the expected date from when they are available and the communication channel where the KPIs will be published.

5.1 Communication and Dissemination KPIs

The results for the communication and dissemination activities will be reported based on the following KPIs:

Name	Activity	Target metrics
Project Intranet	Internal Project web site total number of visits.	1000+ visits.
Project Public web sites	Public Web site total number of visits	2500+
Social media posts	Regular posts on social; media (LinkedIn)	100+
Brochure / Flyers / Posters	Electronic and printed brochure to be distributed during events	3 designs
Conferences, exhibitions	Participation to national and international conferences to promote aSIEMmetry	4+
aSIEMmetry webinars	Interactive demo LLM	>=2 webinars: At least 2, From Month 18 onward
aSIEMmetry research updates	Publish research results on the project portal	5+

KPI Benchmarks:

- Minimum 1 LinkedIn post/month via the aSIEMmetry showcase page
- Bi-quarterly cross-posting on DNSC, VUB and Expertware corporate accounts
- Monthly news updates on the project website
- Target of 1,000+ views per quarter across channels

5.2 Enhanced SOC processes

The project team will monitor the progress and will report the results on the public web site.

Sharing the metrics and KPIs publicly will ensure transparency for the activities and results.

As o month 19, after the creation and the design of the AI model we will publish a set of metrics on the project intranet and public website.

Enhanced SOC metrics

Use case aSIEMmetry	**Details**	**Metrics and dissemination channel**
Enhance SOC processes detecting anomalies based on “security entropy” baseline	Develop and validate proactive security incidents detections based on “security entropy model”	Number of novel detections established based on the entropy model published Publishing: project site
Enhance SOC processes detecting anomalies detecting patterns and anomalies based on “shifting windows / time-based aggregations”	Develop and validate of proactive alerts based on “shifting windows / time-based aggregations”	Number of new alerts designed based “shifting window/ time-based aggregations” Publishing: project site
deep learning classifications dashboards	Research and evaluate models for security posture classifications	Number of security posture classification categories Publishing: project site
Enhance SOC processes leveraging the use of AI models (“AI enhanced SOC”)	Develop playbooks leveraging the use of AI platforms in SOC analysts ‘activities.	Number of AI powered SOC analysts’ playbooks Publishing: project site
Subscribers for aSIEMmetry newly discovered threat indicators	New threat indicators and observables discovered thanks to the AI enhanced SOC processes will be shared with vetted organizations	Number of organizations enrolled for the aSIEMmetry news feed Publishing: project site

As we progress, we will update the current document twice in M24 and M36

- M24 (update 1) and
- M36 (update 2)

6 Glossary of Acronyms and Abbreviations

AD	Active Directory
AI	Artificial Intelligence
API	Application Programming Interface
AV	Antivirus
CTI	Cyber Threat Intelligence
DNS	Domain Name System
EDR	Enhanced Data Rate
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
GVM	Greenbone Vulnerability Management
HA	High Availability
HDD	Hard Disk Drive
HTTPS	Secure Hypertext Transfer Protocol
IoA	Indicator of Attack
IoC	Indicator of Compromise
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KVM	Kernel-based Virtual Machine
M[1-35]	Project Month [1-35]
ML	Machine Learning
MISP	Malware Information Sharing Platform
NTP	Network Time Protocol
NVMe	Non-Volatile Memory
OS	Operating System
PAM	Privileged Access Management
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
S2S	Site-to-Site Virtual private network
SAN	Storage Area Network
SIEM	Security Information and Event Management
SIRP	Security Incident Response Platform
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOAR	Security orchestration, automation and response
SOC	Security Operation Center
SOCaaS	Security Operations Center-as-a-Service
SPOF	Single Point Of Failure
SQL	Structured Query Language
SSD	Solid State Drive
SSL	Secure Sockets Layer
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TLP	Traffic Light Protocol

TLS	Transport Layer Security
UC	Use Case
VDI	Virtual Desktop Infrastructure
VM	Vulnerability Management
VMDR	Vulnerability Management Detection & Response
VPN	Virtual Private Network
XSS	Cross-Site Scripting