Ref. Ares(2025)4936564 - 20/06/2025

expertware

SIEMBIOT
Project review 1
Summary report

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

Document Control

Title	**SIEMBIOT Project review 1 summary report**
Client:	Internal
Reference:	2025-189
Version:	1.3
Release Date:	26/02/2025
Author:	Expertware, DNSC
Total Pages:	
Security Class:	Sensitive
Distribution:	Cannot be distributed without prior agreement from Expertware & DNSC.
Disclaimer:	

Document Approval

Expertware Approver	Lelcu Ion Didel	General Manager
DNSC Approver	Catalin Cristescu	Project Manager

Revision History

Version	Date	Issued By	Status	Comments (Update this history table for each version)
1.0	24/02/2025	@SIEMBIOT Project Management	Draft	Initial draft
1.2	28/02/2025	@SIEMBIOT DNSC Beneficiary Partner	Final version	Updated draft review & document validation
1.3	16/06/2025	@SIEMBIOT Project Management	Revision request update	New Chapter (7) added: *to include additional details on client onboarding KPIs, targets and plans as set out in D1.3 *adoption risks to the risk registry *market analysis update (competitor scenarios) *update of the progress regarding all 13 KPIs as defined in the DoA *Information on specific key CSIRT organizations and their contributions to the validation and enhancement of the platform, liaison activities with EU initiatives such as ENISA and European

				Digital Innovation Hubs (EDIH) as well as engagement with cybersecurity bodies and educational institutions *Include information/documentation on the repository of deployment integration templates, as mentioned by the project and statistics/information on the customer deployments, number of devices, processes and operations.

Contents

1 Introduction 4
1.1 Scope 4
1.2 Executive Summary 4
2 Milestones achieved & reviewed 5
3 Status of Deliverables 8
4 Status of Work Packages 9
4.1 Completed Work packages 9
4.2 Ongoing Work packages 10
4.2.1 Status Work Package 1 10
4.2.2 Status Work Package 4 11
4.2.3 Status Work Package 5 11
4.2.4 Status Work Package 6 12
5 Metrics & KPIs 13
5.1 KPI 1: Number of Customers Onboarded on the SIEMBIOT Platform 13
5.2 KPI 2: Industrialization Feasibility of SIEMBIOT Central Services 13
5.3 KPI 3: number of NIS2 Directive sectors onboarded on SIEMBIOT 14
5.4 KPI 12: % of project tasks delivered on time and on budget 15
6 Communication & Dissemination results 16

7 Revised after Review 19
7.1 Client Onboarding KPIs, Targets, and Plans (as outlined in D1.3) 19
7.2 Adoption Risks – Updates to Risk Registry 19
7.3 Market Analysis Update 21
7.3.1 SIEM/SOCaaS market analysis 21
7.3.2 Cyber Academy training & research portal 23
7.4 Progress on all 13 KPI's (as defined in the DoA) 24
7.5 CSIRT Involvement and EU Liaison Activities 25
7.6 Repository of Deployment Integration Templates 26
7.7 Customer Deployment Statistics and Operations 27

1 INTRODUCTION

1.1 Scope

This report provides a comprehensive summary following the first project review, conducted 18 months into the project's timeline. The review aimed to assess the progress and achievements of all work packages in relation to the project's overall objectives and milestones. It highlights the key outcomes, budget consumption, challenges, the strategies implemented to address them.

Additionally, the report outlines the next steps and adjustments planned to ensure continued success in the remaining phases of the project. This document serves as a critical reflection of the project's initial phase and provides valuable insights for ongoing and future activities.

1.2 Executive Summary

The consortium achieved all deliverables and milestones as per the original project plan and we are fully committed to disseminate the results to European entities helping them to improve the security posture and comply with cyber security regulations (NIS2, CRA, DORA). More details regarding the milestones and the deliverables submitted are present in section 2 and section 3.

We deployed the IT infrastructure, completed the development for SIEMBIOT SOCaaS tenants (https://demo.siembiot.eu), the shared cyber security services and the Cyber security training & research portal (https://cyber-academy.siembiot.eu) and we are currently continuing to onboard beneficiaries into their dedicated SIEMBIOT tenant. We also started the communication and dissemination process to cyber security partners who can contribute with training content or research playbooks or can train their personnel against the anonymized cyber security events data lake.

All the work packages are on track with respect to activities, deliverables and budgets (detailed in section 4). Section 5 describes the KPIs which have been already achieved as well as indicating what we expect at the end of the projects

The budget was managed with careful planning and strategic allocation, ensuring that resources were used efficiently and without unnecessary waste. We notice a genuine interest from organisations to onboard into the SIEMBIOT platform and to use the SIEMBIOT training & research portal (Cyber Academy) but many times their internal project approval and resource allocation if time consuming hence bringing them into the platform takes slightly longer than we initially anticipated. Therefore, we would like to propose that the savings are re-allocating to the dissemination activities. As you can see later in this document, section 6 the most efficient communication & dissemination channel is active presence to Cyber Security conferences and Fairs. We believe that increasing the participation to European Cyber Security conferences & trade fairs will boost the adoption rate and the impact for our solutions.

2 MILESTONES ACHIEVED & REVIEWED

The consortium strived to achieve the milestones detailed in the original project plan. The table below provides a chronological summary indicating the delivery date, details regarding the review & approval process and the repository where supporting documents are stored.

The document repository is hosted in Expertware's intranet where the DNSC partner has been invited (Guest accounts with Edit/Modify authorizations).

M. No	Name	WP No	Due date	Delivered	Status	Details & supporting documents
M1	Kick-off meeting	WP1	30-Sep-23	01-Mar-24	Done	Meeting held @Experwtare, recurring weekly meetings setup for dissemination and Technical topics
M2	Project plan & risk register	WP1	31-Oct-23	28-Oct-23	Done	Deliverable D1.1 reviewed & submitted SIEMBIOT_ProjectPlan_v1.1.docx SIEMBIOT_Risk Management -baseline.docx
M6	SIEMBIOT platform requirements and high-level design document	WP2	30-Nov-23	30-Nov-23	Done	Deliverable D2.1 reviewed and submitted SIEMBIOT HLD v1.0.docx
M7	SIEMBIOT security architecture blueprint	WP2	31-Dec-23	29-Dec-23	Done	Deliverable D2.1 reviewed and submitted SIEMBIOT HLD v1.0.docx
M4	Elaborate awareness and dissemination plan and toolkit	WP1	29-Feb-24	29-Feb-24	Done	Project web site https://siembiot.eu Project LinkedIn profile https://www.linkedin.com/showcase/siembiot/ 2024 -2025 conferences 2024 EU Conferences to consider.docx Conferences 2025.xlsx

M8	Platform deployment	WP3	31-Mar-24	31-Mar-24	Done	Platform deployment report reviewed by consortium members SIEMBIOT Platform Deployment v1.0.docx
M9	Platform validation	WP3	30-Jun-24	28-Jun-24	Done	Platform validation (performance & high availability) report reviewed by consortium members SIEMBIOT Performance - HA.docx Shared Services configuration review SIEMBIOT OpenCTI Configuration.docx SIEMBIOT MISP Configuration.docx
M12	Complete development for the cybersecurity research data lake (including ingestion)	WP5	31-Aug-24	31-Aug-24	Done	Reviewed data lake anonymization HLD: SIEMBIOT Data Lake anonymization.docx Validated anonymized process: SIEMBIOT Data Lake anonymization.docx
M10	Completion of training and certifications plan for additional SOC roles	WP4	31-Oct-24	31-Oct-24	Done	Updated training & certification plan reviewed by consortium members SIEMBIOT Training & certification schedule and report .docx
M13	Collaborative portal development completion	WP5	28-Feb-25	27-Feb-24	Done	SIEMBIOT tenant demo portal https://demo.siembiot.eu SIEMBIOT collaborative portal https://cyber-academy.siembiot.eu Penetration Test Reports Siembiot Penetration Test Report 2.docx Cyber Academy Penetration Test Report .docx

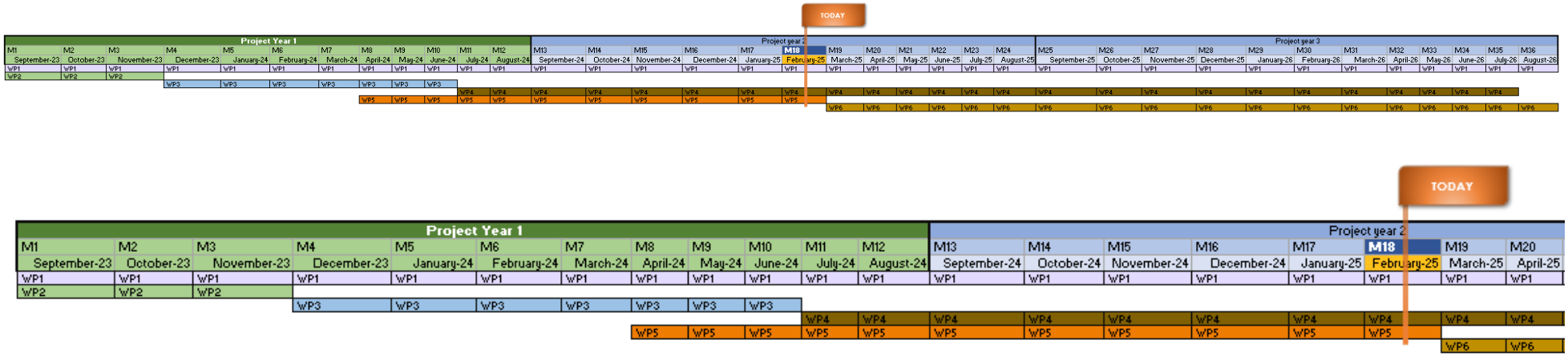
M3	Project review 1	WP1	28-Feb-25	28-Feb-25	Done	This document reviewed by the consortium members

3 STATUS OF DELIVERABLES

Until now all the deliverables envisaged have been submitted on time & on budget.

Deliverables					
WP	**Del.No**	**Deliverable Name**	**Lead**	**Due Date**	**Status**
WP1	D1.1	Project Plan	Expertware	31 Oct 2023	Submitted
WP1	D1.2	Risk register and mitigation	Expertware	31 Oct 2023	Submitted
WP1	D1.3	Dissemination strategy and communication plan, partner engagement	DNSC	29 Feb 2024	Submitted
WP1	D1.4	Project review 1 summary report	Expertware	28 Feb 2025	Submitted
WP1	D1.5	Project review 2 summary report	Expertware	31 Aug 2026	Pending
WP2	D2.1	High level solution design, requirements, use cases	Expertware	30 Nov 2023	Submitted
WP3	D3.1	Platform deployment report	Expertware	31 Mar 2024	Submitted
WP4	D4.1	Training and certification schedule report	Expertware	31 Oct 2024	Submitted
WP5	D5.1	Collaborative web portal pilot (including penetration testing done by an external supplier).	Expertware	28 Feb 2025	Submitted
WP6	D6.1	Partner and beneficiaries onboarding web site & manuals	Expertware	30 Jun 2025	Pending
WP6	D6.2	Summary research updates report/dashboard	Expertware	31 Jul 2026	Pending

4 STATUS OF WORK PACKAGES



4.1 Completed Work packages

Work package	Completed activities	Milestones	Deliverables	Status
WP2: SIEMBIOT System design [Sept 2023] - [Dec 2023]	T2.1 Define platform requirements and target use cases. T2.2 Platform system architecture T2.3 CTI system architecture T2.4 Continuous vulnerability assessment system architecture T2.5 Security architecture including data segregation and privacy	Achieved	Delivered	Ontime & on-budget
WP3: SIEMBIOT Platform build [Dec 2023] - [Jun 2024]	T3.1 IT equipment Acquisition T3.2 Hardware and software deployment T3.3 Configure central threat intelligence services T3.4 Configure central vulnerability scanning services T3.5 Platform validation	Achieved	Delivered	Ontime & on-budget

Effort Allocation vs. Consumption

Participant	Work package	Allocation (months)	Consumption (%)	Assessment
EXPT	WP2	12	98.23%	On track
DNSC	WP2	3	0.00%	Lower consumption
WP 2 Total	WP2	15	78.58%	
EXPT	WP3	30	110.80%	Higher consumption
DNSC	WP3	10	31.63%	Lower consumption
WP3 Total	WP3	40	91.01%	

4.2 Ongoing Work packages

4.2.1 Status Work Package 1

[September 2023] - [August 2026]

WP1 Effort Spent vs Allocation

	Resources WP 1			
Participant	**Tasks**	**Allocation (months)**	**Spent (%)**	**Assessment**
EXPT Marketing & communication	T1.2 Dissemination and targeted communication T1.3 Engagement with CSIRT organizations	18	49.81%	On track
DNSC Project Management		8	58.75%	On track
Total		26	52.56%	On track (as we are in M18)

The overall effort utilization for WP1 stands at **52.56%**, Participant-wise, **EXPT** has used **49.81%** utilization. Meanwhile, **DNSC** has consumed **58.75%** utilization. DNSC has a higher relative usage.

4.2.2 Status Work Package 4

[July 2024] – [July 2026]

In Work Package 4, T4.2, we decided to pursue CompTIA certifications instead of SANS, as originally planned. Expertware became CompTIA partner, hence the decision to find similar relevant cyber security courses. The training has been ongoing for the past four months, led by our internal SOC team under the coordination of Viorel Horga.

WP4 Effort Spent vs Allocation

	Resources WP 4			
Participant	**Activities**	**Allocation (months)**	**Spent (%)**	**Assessment**
EXPT SOC Analysts (L1,L2,L3)	T4.1 SIEMBIOT beneficiary selection T4.2 Continuous Training & certifications (According to CompTIA) T4.3 Configure automation Template for SIEMBIOT tenant deployment	120	31.52%	On track
DNSC Security Experts	T4.4 SIEMBIOT onboarding T4.5 SIEMBIOT continuous collaborative and threat intelligence sharing	24	6.87%	Lower consumption
Total		144	27.41%	On track

WP4 effort consumed is **27.41%** of the initial allocation. EXPT has used **31.52%,** as the work package is running until month 25. DNSC has used just 6.87% indicating underutilization. The low utilization is mainly due to the early stages of the project, requiring focused resource allocation and acceleration in upcoming phases to meet WP 4 objectives. Close monitoring of both EXPT and DNSC is essential.

4.2.3 Status Work Package 5

[April 2024] - [February 2025]

WP5 Effort Spent vs Allocation

Participant		**Allocation (months)**	**Spent (%)**	**Assessment**

EXPT BI Developers Web Developers	T5.1 Develop research data lake T5.2 Populate the research data lake T5.3 Develop collaborative research web portal T5.4 Research data lake and collaboration portal validation	48	100.09%	Ontime & on-budget
DNSC Security Experts		15	35.71%	Lower consumption
Total		63	84.76%	On track

WP 5 is related to the development of the cybersecurity research data lake. We consumed 84.76% of the allocated efforts (EXPT near 100% utilization), indicating efficient resource use. DNSC used only (35.71%), suggesting underutilization and the need to reassess their role and redistribute responsibilities. While WP 5 is progressing well, adjustments in resource allocation, particularly for DNSC, will be necessary to accelerate progress on key tasks such as the data lake, web portal, and validation. Effective coordination will be crucial to meeting remaining objectives.

4.2.4 Status Work Package 6

[March 2025] - [August 2026]

Task No	Task Name
T6.1	Interoperability with CSIRTs members
T6.2	Continuous research
T6.3	Collaborative portal training sessions

WP6 Effort Spent vs Allocation

Not yet started.

5 METRICS & KPIS

We provide below the value of envisaged KPIS as of February 2025, 18 months since we started working on the SIEMBIOT platform. The KPIs will be updated quarterly and the final SIEMBIOT report will contain updated values and more KPIs/ KRIs.

5.1 KPI 1: Number of Customers Onboarded on the SIEMBIOT Platform

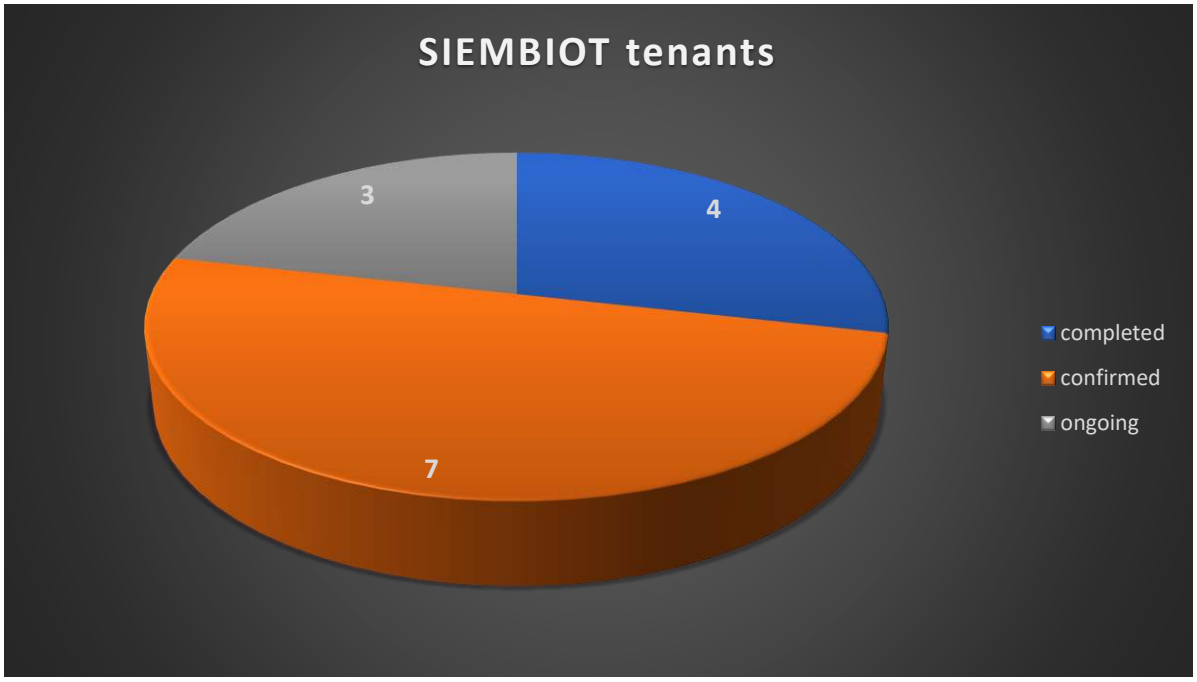
Target: Minimum 10 customers onboarded

Measurement: Track the number of customers successfully onboarded to the SIEMBIOT platform.

Current value: 12/10 120%

As we still have 18 months, we are confident that we will go beyond the initial target of 10 distinct SIEMBIOT tenants.

Current list includes multiple beneficiaries located in various European countries: Romania, Luxembourg + The Netherlands + United Kingdom, Belgium.



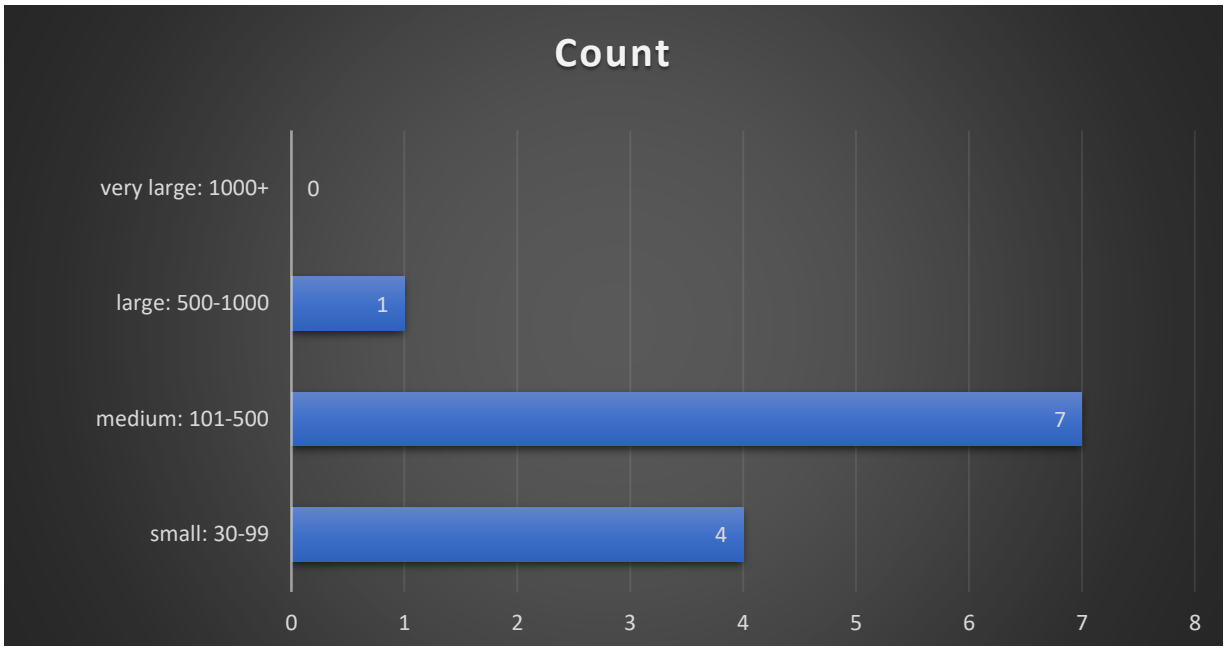
Based on the current data, we are on track to exceed the KPI 1, which targets a minimum of 10 customers onboarded to the SIEMBIOT platform. Out of the 14 total customers, 4 are marked as "completed," 7 as "confirmed," and 3 as "ongoing." With 11 customers either completed or confirmed, we are already exceeding the target of 10 customers/tenants.
The number of ongoing customers indicates that additional onboarding is still in progress, and once completed, the total will exceed the target. This suggests that the project is progressing well and is likely to meet or surpass the initial KPI by the end of the reporting period.

5.2 KPI 2: Industrialization Feasibility of SIEMBIOT Central Services

Target: 1 customer per category (small, medium, large, very large organizations)

Measurement: Ensure SIEMBIOT central services are tested and deployed successfully across different sized user organizations (small: 30-99, medium: 101-500, large: 500-1000, very large: 1000+).

Current KPI2: 3 out of 4, 75%



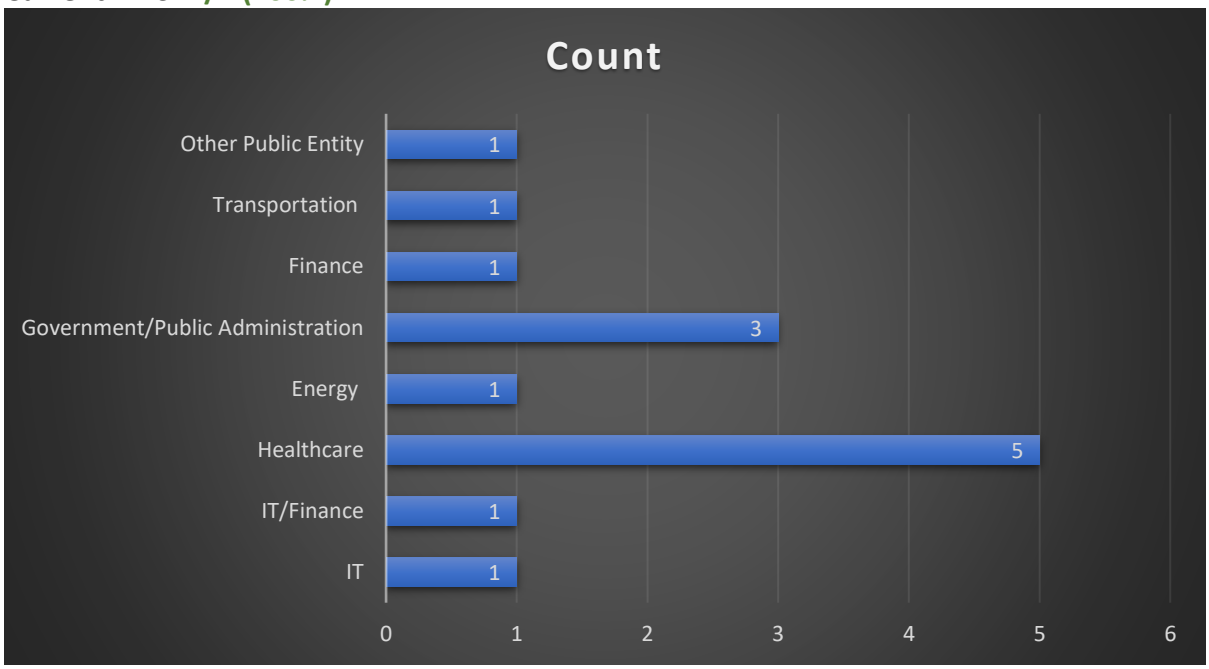
Based on the current data, the project is progressing towards meeting KPI 2, which targets onboarding at least 1 customer per category (small, medium, large, very large organizations). As of now, the distribution of customers across categories is as follows: 4 customers in the "small" category (30-99), 7 customers in the "medium" category (101-500), 1 customer in the "large" category (500-1000), and 0 customers in the "very large" category (1000+). The target of having 1 customer in each category has already been met for small, medium, and large organizations, which indicates strong progress in these areas. However, no customers have been onboarded yet in the "very large" category, which could indicate a need for additional focus or strategy to onboard such organizations before the project ends in August 2026. Given that the project began in September 2023, there is still ample time to onboard customers in the "very large" category, and efforts can be adjusted to ensure all targets are met by the project's conclusion.

5.3 KPI 3: number of NIS2 Directive sectors onboarded on SIEMBIOT

Target: at least 1-2 customers from the 4 different sectors (IT, Finance, Health, Government)

Measurement: Track the number of entities from the NIS2 Directive sectors (Essential and Important Entities) onboarded on SIEMBIOT within each of the four sectors. The goal is to have at least one to two customers per sector (IT, Finance, Health, Government) to ensure broad sectoral representation and alignment with NIS2 requirements.

Current KPI3: 4/4 (100%)



As of the latest reporting period, the onboarding of customers across various sectors on SIEMBIOT shows a diverse range of participation. The breakdown by sector is as follows: 1 customer from the IT sector, 1 customer from the IT/Finance sector, 5 customers from Healthcare, 1 from Energy, 3 from Government/Public Administration, 1 from Finance, 1 from Transportation, and 1 from Other Public Entities. This distribution highlights strong engagement across multiple sectors, with a particularly notable uptake in the Healthcare sector. These figures demonstrate SIEMBIOT's broad applicability and successful onboarding across key industries as part of NIS2 compliance efforts.

5.4 KPI 12: % of project tasks delivered on time and on budget

Target: Ensure that 100% of project tasks are completed within the planned timeline and budget constraints.

Measurement: Track the total number of project tasks and assess the percentage of those that have been delivered according to schedule and budget. The goal is to maintain a high level of efficiency and resource management throughout the project lifecycle.

Current KPI4: 100%

As of the latest reporting period and pointed in the previous points within this report, all project tasks have been successfully delivered on time and within budget. This achievement reflects strong project planning, efficient resource allocation, and effective execution. Maintaining this level of performance ensures that SIEMBIOT continues to meet strategic milestones while optimizing costs and timelines. Continuous monitoring and proactive risk management will be key in sustaining this success moving forward.

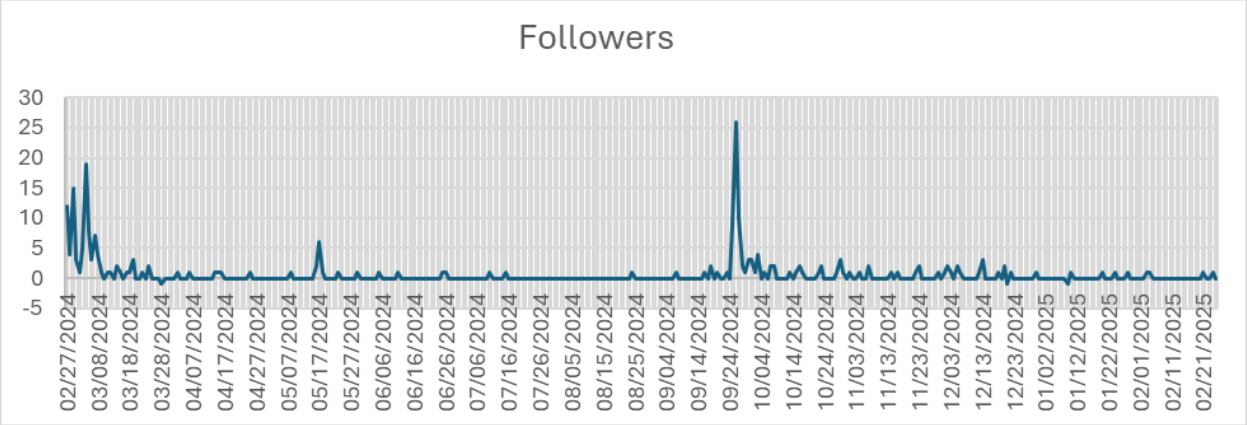
6 COMMUNICATION & DISSEMINATION RESULTS

Engaging in a wide variety of events, from international conferences and trade fairs to workshops and educational sessions, provides a unique opportunity to amplify the awareness of SIEMBIOT's project and its impact. Through active participation, SIEMBIOT gains increased visibility for its innovative cybersecurity solutions, while simultaneously promoting the EU grant and showcasing its commitment to contributing to European technological advancement.

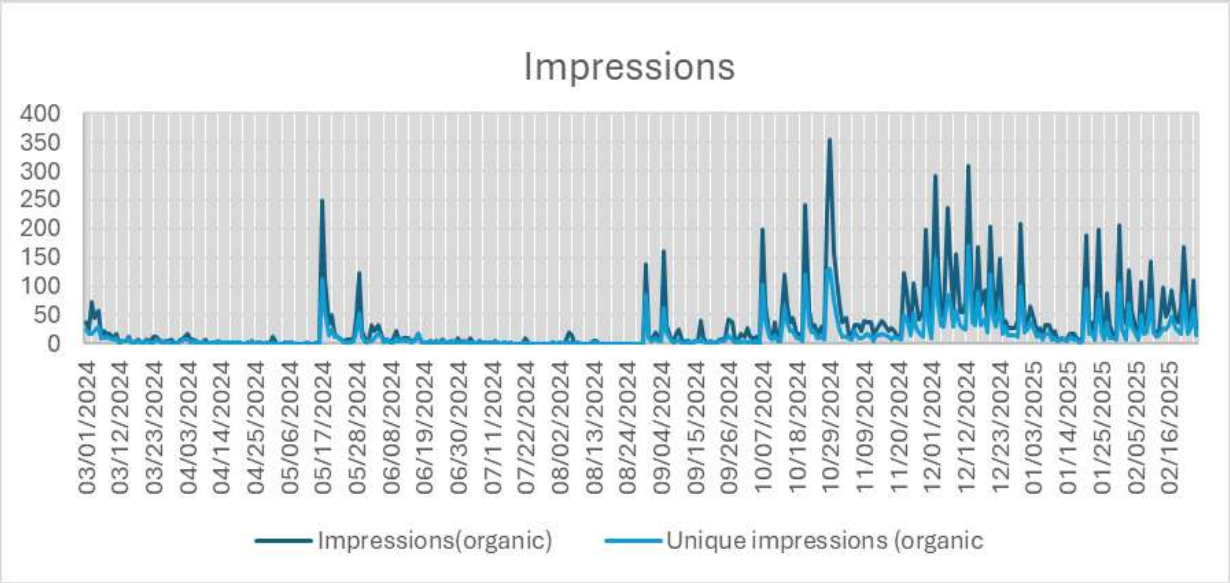
Event type	Event name	Location	Event date	Estimate event footfall	Estimated no of visitors at booth
Conference	DIGITAL INNOVATION ZONE 2024	Iasi, (Romania)	28-Mar-24	over 400	approx. 200
Cybersecurity Conference & Expo	DefCamp Cluj-Napoca 2024	Cluj-Napoca (Romania)	16–17 May-24	over 400	approx. 200
Cybersecurity Conference &Expo	Cybersec Europe 2024	Brussels (Belgium)	29–30 May-24	over 1500 participants and over 100 exhibitors from more than 30 countries	approx. 500 visitors and 57 leads
Education and training	Hackout Talks#3 (Live hacking & defense demo)	Bucharest, (Romania)	11-Oct-24	aprox.100	
Cybersecurity Conference & Expo	Bucharest Cybersecurity Conference 2024 (Live hacking & defense demo)	Bucharest, (Romania)	29–31 Oct-24	over 1,500 in-person participants and 350 online attendees from more than 50 countries.	approx. 400
Education and training	International Industry Engagement Workshop on Cybersecurity - Deep Tech Skills Day	On-line	13-Nov-24	approx. 25	
Open Demo Day	Open Demo Day (Suceava County Council Meeting)	Suceava, (Romania)	26-Jan-25	approx. 40	
Open Demo Day	Open Demo Day (Falticeni Municipality Meeting)	Falticeni, (Romania)	4-Feb-25	approx. 30	
Clustering Activities	DIZisITDays - Digital Innovation Hub	Iasi, (Romania)	28-Feb-25	approx. 30	

LinkedIn Growth and Engagement Analysis for SIEMBIOT Project Page

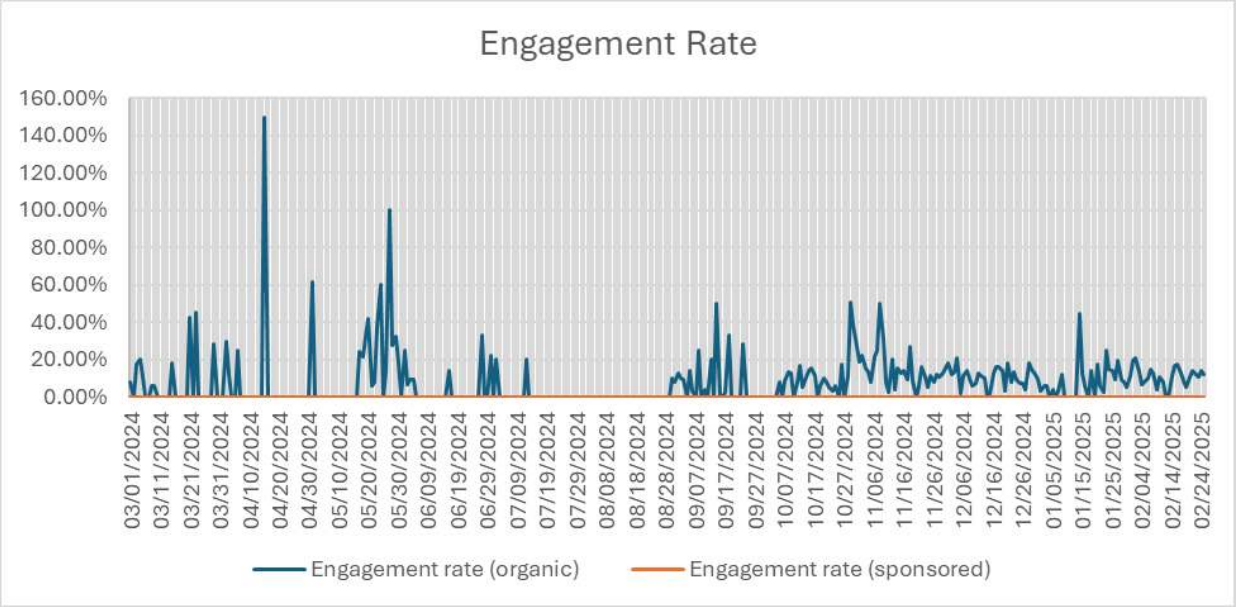
The dedicated LinkedIn project page has experienced a gradual growth in its followers and engagement over the course of year reaching a total number of 265 followers up to date with no paid sponsorship, fully organic.



The other metrics like impressions and engagement rate have shown a steady increase, with notable spikes recorded, particularly around specific events and content types. This period with growth surges coincides with the participation in international and national cybersecurity conferences, which is a critical indicator that major events and visibility can significantly impact page growth. This also suggests that industry-related exposure contributes to audience engagement, which will be leveraged further for visibility.

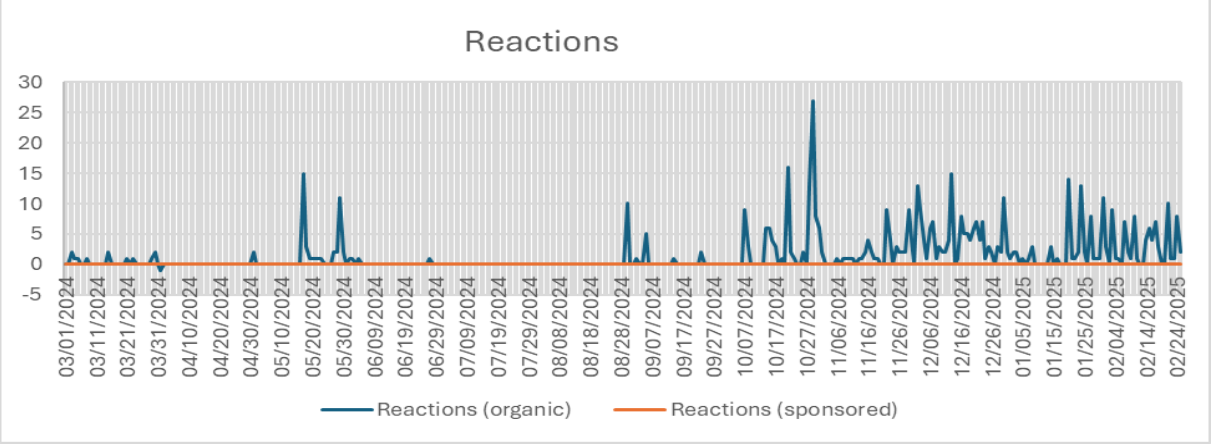


The project's overall engagement rate stands at an average of 11%, which is considered quite good on LinkedIn, especially in the B2B sector. Specific posts such as conferences and content related to SIEMBIOT's presentations show much higher engagement, with 47.19% engagement rate during for example the BBC 2024 Conference and 25% during CyberSec Europe 2024. This indicates that event-based content drives high engagement and may appeal significantly to the audience when it's aligned with the consortium's core business and expertise.



Posts focusing on the benefits of SIEMBIOT functionalities and the solutions provided to fight against cybercriminals and types of behaviour of attackers, have been performing reasonably well, with an average engagement rate of 15%. This suggests that educational and solution-oriented content resonates with our audience (B2B and B2C). Content providing actionable tips has also shown notable engagement, highlighting the value of providing informative, actionable insights that meet the needs of both business clients and individual consumers.

31 individual posts have been made throughout the page lifetime, supplemented by 11 reposts from the beneficiaries' pages (Expertware - 1.870 followers and DNSC - 21.727 followers). These shares suggest cross-promotion and an expanding network of industry connections, which is beneficial for increasing reach and visibility.



From 1/03/2024 to 2/24/2025, the engagement levels were strong, with 535 reactions, indicating a positive response from the audience. In addition, the content prompted 3 comments and 3 reposts, reflecting meaningful interaction and further amplification within professional networks. These metrics demonstrate that the posts are effectively engaging the target audience, enhancing both visibility and interaction, and contributing to the overall outreach efforts.

7 REVISED AFTER REVIEW

This revised section of Deliverable D1.4 incorporates additional details requested during the project review, including updates on client onboarding KPIs, risks, market analysis, KPI progress, collaboration with CSIRTs, liaison with EU cybersecurity initiatives, and deployment statistics.

7.1 Client Onboarding KPIs, Targets, and Plans (as outlined in D1.3)

The onboarding KPIs reported below are aligned with the strategy defined in D1.3 and detailed in the project's dissemination, communication, and partner engagement plan. In line with D1.3 Section 5.2, the SIEMBIOT project tracks partner onboarding KPIs per use case and reports progress in two formal reporting cycles: M18 and M35.

KPI 1 – Customers Onboarded (UC1: SIEMBIOT Operations)

- **Target:** >9 entities
- **Status (May 2025): 10** fully onboarded, 4 in progress, 11 in planning
- **Outlook:** Target met, and pipeline remains active

KPI 2 – Distinct Users & Devices Onboarded (UC1)

- **Target:** >3000 users/devices
- **Status:** 1,515 users/devices onboarded as of M18; full target expected to be met progressively with ongoing tenant expansion.

KPI 3 – Sectoral Coverage (UC2: SIEMBIOT Research Data Lake)

- **Target:** ≥5 sectors
- **Status: 8 sectors** with SEIMBIOT tenants: Administration, Education, Energy, Finance, Health, ICT, Telecom, Transport:

KPI 4 – Research Engagement (UC3: Research Portal)

- **Target:** >5 research partners, >100 advanced queries
- **Status:** In progress; initial contributions onboarded, full metrics to be presented in M35

KPI 5 – Training Usage (UC4: Training Portal)

- **Target:** >100 students, >50 cyber exercises
- **Status:** Ongoing training activities under WP6, aligned with CompTIA content and purple team labs.

Observations: The onboarding process has been refined and accelerated. Partner support, targeted onboarding sessions, and participation in cybersecurity trade fairs have proven critical to converting interest into deployments. Engagement remains strong across public and private entities. Dissemination through LinkedIn, live demos and workshops ensures visibility, while the Project Intranet provides up-to-date reporting for all internal stakeholders.

7.2 Adoption Risks – Updates to Risk Registry

New entries in the risk registry:

1. Delayed Onboarding Due to Internal Client Processes
    a. Likelihood: Medium
    b. Impact: Medium
    c. Mitigation: Extend engagement through executive briefings, onboarding support and technical workshops, initiated multiple parallel onboarding activities.
2. Underrepresentation of Very Large Enterprises
    a. Likelihood: Medium
    b. Impact: High
    c. Mitigation: Tailored incentives and direct outreach to C-level decision-makers

7.3 Market Analysis Update

SIEMBIOT project has two distinct solutions:

1. an integrated end-to-end SIEM / SOCaaS
2. a Research and training portal based on anonymized data lake containing real live security events captured from selected tenants.

7.3.1 SIEM/SOCaaS market analysis

The integrated SIEM/SOCaaS offers the following features:

- Vulnerability Management
- Multi source Threat Intelligence & Enrichments
- Asset and Software Inventory (with snapshots)
- Advanced Threat Hunting capabilities
- Alert Automatic Creation & Triage
- Security Incident Management (ITSM)
- Security Incident Response (SOAR integrations)
- Policy Evaluation and Reporting
- AI integration

This integrated approach reduces vendor fragmentation, accelerates deployment, and increases visibility — making SIEMBIOT especially attractive for public institutions and regulated entities in Europe.

Some Key Market Segments:

- Global SOC Platforms (e.g., Crowdstrike MDR, Rapid7, Microsoft Sentinel, IBM QRadar, Palo Alto Cortex XSIAM). We did not identify similar EU only solutions.
- EU-native CTI and threat analysis platforms (e.g., T-SOC, Sekoia.io, HarfangLab)
- Vertical-focused solutions (e.g., solutions targeting health or finance sectors)

We made a feature comparison to identify SIEMBIOT go-to-market strengths and weaknesses:

	Sovereignity	SIEM	UEBA	VM	CTI	ATH	ASM	CIS/compliance	AI	ITSM	Onprem	Cloud	SOC 24x7	Pricing
Siembiot	EU	Yes	Limited	Yes	Yes	Yes	Limited	Yes	Yes	Yes	Yes	Yes	Yes	€
Wazuh (open source)	US	Yes	No	Yes	Limited	Limited	No	Self-service	No	No	Yes	Yes	No	€€
SOCRadar	US	Yes	Limited	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	€€€
Microsoft MDR	US	Yes	Add-on	Yes	Add-on	Self-service	No	Self-service	Add-on	No	No	Yes	No	€€€€
Qradar	US	Yes	Yes	Yes	Add-on	Yes	Limited	No	Add-on	No	Yes	Yes	No	€€€€€
Crowdstrike MDR	US	Yes	Yes	Yes	Add-on	Yes	Add-on	Yes	Yes	No	No	Yes	Add-on	€€€€€
Rapid7	US	Yes	No	Yes	Limited	Yes	Yes	Yes	Limited	No	Yes	Yes	Add-on	€€€
Cortex Xsiam	US	Yes	Yes	Yes	Yes	Yes	Add-on	Yes	Yes	No	Yes	Yes	No	€€€€€

We compared our solution with other integrated established solutions from top tier vendors.

Analysis Criteria

SIEM: Security Information and Event Management UEBA: User Entity and Behaviour Analytics VM: Vulnerabilities Management capabilities CTI: Cyber Threat Intelligence feeds ATH: Advanced Threat Hunting capabilities ASM: Attack Surface Management evaluation	CIS: Center for Internet Security policy evaluation AI: Artificial Intelligence capabilities ITSM: Onprem: hosting on-premises Cloud: hosted in the cloud as SaaS Pricing: estimated ownership costs

Our evaluation is that SIEMBIOT SIEM/SOCaaS has several distinct advantages: EU sovereignty, deep integration with simple pricing (no add-ons, no hidden costs), offers services together with the platform and aims a very competitive pricing.

The European cybersecurity platform landscape includes global enterprise solutions, EU-based threat analysis tools, and vertical-specific SOCaaS offerings. Based on ongoing market observation (e.g., Cybersec Europe 2024, DefCamp 2024), the demand is shifting toward integrated, policy-aligned, and sovereign platforms capable of supporting NIS2 compliance and multi-sector onboarding.

Criteria	**SIEMBIOT (All-in-One)**	**Global Vendors (e.g., Crowdstrike, Microsoft, IBM, SOCRadar, Rapid7)**	**EU-Based Vendors (e.g., Sekoia.io, HarfangLab)**
Platform Architecture	Fully integrated (SOCaaS, CTI, VM, Incident Response)	Modular (separate add-ons/modules)	CTI-focused, often partial SOC integration
Data Sovereignty & GDPR	100% EU-hosted, GDPR-aligned	Often US/Global hosting with compliance layers	EU-based, GDPR-aligned
Onboarding Automation	Preconfigured templates, auto-deploy PODs	Manual onboarding or separate tools	Partial automation
Multi-sector Support	8 sectors onboarded, templates per vertical	Enterprise-focused, less sectoral granularity	Sector-limited (finance, gov., etc.)
NIS2 & ENISA Alignment	Built-in features mapped to NIS2 requirements	Limited or generic EU alignment	Emerging alignment
Threat Intelligence	Integrated OpenCTI, MISP, Cortex, Wazuh	Proprietary or premium CTI options	Strong CTI tools, limited integration
Response & Remediation	Built-in SOAR-like capabilities	External SOAR platforms required	Limited or in development
TCO & Scalability	Optimized for EU SMEs and public orgs	High cost, enterprise scale	Moderate cost, focused coverage

Unlike most competitors that require customers to stitch together tools for asset management, vulnerability scanning, CTI, alert triage, and policy enforcement, SIEMBIOT consolidates all these in a single, modular platform.

From our view, SIEMBIOT fills a strategic gap in the European cybersecurity landscape, providing scalable, sovereign, and transparent SOCaaS capabilities. It aligns with the digital and resilience goals outlined in the European Cybersecurity Strategy and supports adoption across public and private sectors.

7.3.2 Cyber Academy training & research portal

We consider that the anonymized data lake and the training & research portal built on top of it is unique.

SIEMBIOT Cyber Academy portal offers access to an entire data set which is updated daily based on the newly anonymized events captured from various tenant.

Our research did not find any data set contain anonymized security events from multiple entities, sectors and countries.

There are separate solutions (TryToHackMe, HackTheBox) but they focus on purpose built isolated environments where attackers can learn Red Team techniques. The platform do not offer a decent size data set where blue team engineers can be trained, learn investigation techniques or perform research identifying new attack methods or discovering new detection rules.

7.4 Progress on all 13 KPI's (as defined in the DoA)

This section tracks SIEMBIOT's progress against the KPIs defined under both objectives of DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE, including maturity assessment, stakeholder engagement, data management, cross-sector coordination, and capacity-building activities.

KPI	Description	Target	Status (May 2025)
1	Number of onboarded customers on the SIEMBIOT platform	≥10	10 onboarded, 4 in progress, 9 in planning
2	Industrialization feasibility (customers by organization size)	1 per category Small (30-99), Medium (101-500), Large (500-1000) XL very large (1000+) users	3/4 achieved (S/M/L)
3	Number of advanced threat queries published/month	≥20/month	**41** de threat queries, more to be created.
4	Number of CSIRTs/SOCs onboarded	≥3	**2** Confirmed (DNSC, CERT-RO), **1** in onboarding phase (CSIRT Energy sector)
5	Number of alerts + trending	Track trends, volume	**93K** alerts (Jan–Jun 2025)
6	Number of security incidents + trending	Track trends, volume	**22K** incidents (Jan–Jun 2025)
7	% incidents resolved in SLA	≥95%	**97.28%** SLA (Jan–Jun 2025)
8	Number of daily events/alerts processed	NA	**4.684M** events and **93K** alerts over 6 months
9	Number of NIS2 Directive sectors onboarded on SIEMBIOT	≥4	**8** sectors onboarded
10	Number of cyber research and training partners onboarded	≥10	**2** (DNSC, TU Iasi) Ongoing, part of WP6
11	Number of training courses and/or cybersecurity exercises supported by SIEMBIOT for public or private organizations	≥5	**25** training courses published Ongoing, part of WP6
12	% of project tasks delivered on time and on budget	100% on time and budget	Achieved

13	Number of trainings & certifications performed by the SIEMBIOT project	≥10	**9** achieved, 3 ongoing (CompTIA-based)

7.5 CSIRT Involvement and EU Liaison Activities

Key CSIRTs integrations:

- Completed: DNSC(Romania), Technical input, scenario validation, operational reviews, MISP CTI API integration
- Completed: Circl.lu, MISP CTI API integration
- Completed: CISA America: CTI information ingested in SIEMBIOT daily
- Ongoing: CERT-RO: Alignment with JTAN and MeliCERTes initiatives
- Ongoing: CERT-EU via DNSC

Liaison with EU Initiatives:

SIEMBIOT architecture and functionalities follow key ENISA recommendations from early design stages, including CTI source integration, SOC structuring, Vulnerability management automation.

The **Cyber-Academy portal** (https://cyber-academy.siembiot.eu) delivers ENISA-aligned training mapped to the European Cybersecurity Skills Framework (ECSF), featuring courses such as: Incident Response, Threat Intelligence, SOC Operations, Vulnerability Management (aligned with ENISA's Guidelines on Coordinated Vulnerability Disclosure)

The VM module integrates TLP tagging, remediation workflows, and post-patch verification, fulfilling ENISA-aligned standards.

Collaboration and synergies established with other EU projects: JTAN, MeliCERTes, EDIHs (DIZ, Merit), ECYBRIDGE, OCCTET

Training & research results:

- 25 Cyber Academy courses,
- 41 advanced threat hunting queries,
- 4 anonymized playgrounds, collaborative CTI testing.

Academic partnerships agreed:

- Technical University "Gheorge Asachi", Iasi where the university agreed to onboard their lab devices (~60) and use SIEMBIOT anonymized data lake for cyber security learning & research.
- University "Stefan cel Mare" Suceava, enrolled in dual program, (Învățământul Dual – „Performanță în formarea profesională prin parteneriat cu mediul economic pentru dezvoltarea rutei complete de învățământ dual la USV), 5 students who will be trained by Expertware based on SIEMBIOT Cyber-Academy in the academical year 2025-2026. Collaboration likely to extend beyond 2026.

Other Planned Engagement Activities for M19-M35:

- Liaison with ENISA, EDIHs, ECCO, CyberHub, and others
- Educational partnerships (Technical University Iasi) and threat-sharing collaboration via the SIEMBIOT MISP platform.

7.6 Repository of Deployment Integration Templates

CTI information is being shared bi-directionally with partner CSIRTs using MISP integration template already published at: https://www.misp-standard.org/rfc/misp-standard-object-template-format.html

A centralized, version-controlled repository is maintained to standardize onboarding and operations across tenants. It contains over 40 reusable templates and automation scripts categorized by function, including:

- Integration with Azure, Fortinet, Cisco, Windows, and Linux
- VLAN and VRF configuration blueprints
- Firewall policy setup, DNS integration, and identity provider onboarding (LDAP, PAM)
- SIEM/CTI connectors and Cortex analyzers preconfigured per tenant

These templates are maintained under WP3 coordination and used in over 75% of production deployments with minimal customization. Documentation and configuration examples are accessible to all project partners and referenced in Deliverable D3.1 and the shared Git-based deployment toolkit.

APIs for programmatic sharing of Cyber Academy results are still being developed during WP6 based on partner ‘feedback.

7.7 Customer Deployment Statistics and Operations

Expertware developed a life PowerBI workspace fed with information from all the SIEMBIOT tenants deployed:



As of May 2025:

- 10 onboarded, 9 postponed, 4 in progress
- 1,515 users/devices onboarded
- 8 NIS2 Sectors onboarded

Operational Coverage:

- Infrastructure provisioning:
- Security services:
- Threat intelligence
- Monitoring
- Training environments

All tenants leverage the shared SOCaaS framework, supported by platform-wide alerting, SLA enforcements, and tenant-isolated CTI processing.