DIGITAL-ECCC-2022-CYBER-B-03-SOC
DIGITAL JU Simple Grants
Grant Agreement No.: 101145874

Next Generation Security Operation Centres

D7.2 Business Plan			
Report Identifier:	D7.2		
Work-package:	WP7	**Task:**	T7.2
Responsible Partner:	European Dynamics Luxembourg SA (ED)	**Version Number:**	1.0
Due Date	31/06/2025	**Document Date:**	17/09/2025
Distribution Security:	PUB	**Deliverable Type:**	R
Keywords:	Dissemination, Communication, Exploitable Results, Market Positioning		
Project website: https://ng-soc.eu			

Document History

Version	Content & Changes	Issue Date
0.1	**Document created**	**13/06/2025**
0.2	**Document sent for review**	**17/09/2025**
0.3	**Document reviewed**	**18/09/2025**
0.4	**Document reviewed**	**18/09/2025**
0.5	**Reviews are combined**	**19/09/2025**
0.6	**Sent for Quality Assurance**	**22/09/2025**
1.0	**Quality Assurance and Submission**	**25/09/2025**

Quality Control

	Name	Organisation	Date
Editor	Effrosyni Pechlidou, Apostolos Gkletos	ED	**13/06/2025**
Peer review 1	Konstantinos Maliatsos	INS	18/09/2025
Peer review 2	Constantinos Lambrinoudakis	UPRC	18/09/2025
Authorised by (Technical Coordinator)	Mateusz Zych	CYEN	24/09/2025
Authorised by (Quality Manager)	Themis Kolyvas	ED	25/09/2025
Submitted by (Project Coordinator)	Anastasia Garbi	ED	25/09/2025

Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The NG-SOC Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Figures

List of Tables

Abbreviations

Acronym	Description
BPD	Business Plan Development
CA	Consortium Agreement
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
EC	European Commission
EU	European Union
G2M	Go-To-Market Support
GA	Grant Agreement
HRB	HORIZON Results Booster
IoC	Indicator of Compromise
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
KER	Key Exploitable Result
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
OCA	Open Cybersecurity Alliance
PDES	Portfolio Dissemination and Exploitation Strategy
PG	Project Group
SDO	Standards Development Organization
SOP	Standards Operating Procedure
STIX	Structured Threat Information eXpression
SW, S/W	Software
TAXII	Trusted Automated eXchange of Intelligence Information
TRL	Technology Readiness Level
WP	Work Package

Executive Summary

The Next Generation Security Operations Centres (NG-SOC) project is a pan-European flagship initiative co-funded by the European Union to strengthen cyber resilience across critical and essential sectors. Its mission is to deliver a modular, standards-based, and open SOC platform that supports national CSIRTs, operators of essential services, and private SOC providers in building stronger defence capabilities, ensuring compliance with EU regulations, and fostering trusted cross-border cooperation.

NG-SOC directly responds to the rapidly evolving threat landscape and the rising regulatory expectations of the NIS2 Directive, the Cyber Solidarity Act, the Digital Operational Resilience Act (DORA), and the EU Cybersecurity Strategy. Against this backdrop, the project offers a compliance-ready, interoperable, and sustainable solution that reduces fragmentation in Europe's cybersecurity ecosystem and contributes to Europe's ambition for digital sovereignty.

At the technical level, NG-SOC integrates a broad set of advanced capabilities. These include behaviour-based intrusion prevention and dynamic risk management for proactive detection and mitigation, next-generation SIEM and SOAR automation for real-time monitoring, orchestration and response, collaborative incident case management and cyber threat intelligence sharing to enhance information exchange and crisis coordination, and immersive cyber range environments with sector-specific training programmes to address the acute cybersecurity skills gap across Europe. Together, these elements form a comprehensive platform that enhances both the technological and human dimensions of cybersecurity.

The project's impact is reinforced through real-world validation in three distinct pilot domains: banking, energy, and digital infrastructure/academia. CaixaBank, ELES/INFORMATIKA, and CYNET lead these pilots, demonstrating NG-SOC's capacity to deliver tangible improvements in cyber resilience across heterogeneous environments. By situating its pilots in highly regulated and strategically significant sectors, NG-SOC ensures that its outcomes are directly aligned with European policy priorities and operational realities.

Beyond technological innovation, NG-SOC places strong emphasis on sustainability and exploitation. The project builds upon open-source principles, which reduce vendor lock-in, foster interoperability, and encourage community-driven innovation, while at the same time creating pathways for commercial exploitation through service models such as SOC-as-a-Service, consultancy and integration offerings, tailored training and certification, and sector-specific solution packages. By combining community engagement with structured business models, NG-SOC positions itself as a long-term contributor to the European cybersecurity ecosystem rather than as a transient research effort.

Through this comprehensive approach, NG-SOC delivers immediate operational benefits and long-term systemic impact. It strengthens Europe's ability to anticipate, detect, and respond to cyber threats, enhances preparedness for cross-border incidents, and ensures that thousands of entities falling under NIS2 and related frameworks can comply with new regulatory requirements. At the same time, it contributes to workforce development and knowledge transfer, addressing one of the most pressing challenges in the field: the shortage of skilled cybersecurity professionals. By combining technological excellence, regulatory alignment, sectoral validation, and sustainable exploitation pathways, NG-SOC establishes itself as a cornerstone of Europe's collective cyber defence and resilience agenda.

In business terms, NG-SOC is designed not only as a technological platform but as a market-ready solution that can sustain itself beyond the project. By combining open-source components with targeted service offerings, NG-SOC establishes viable revenue streams through SOC-as-a-Service for SMEs, integration and consulting services for large operators, and training and certification programmes for professionals.

1 Introduction

1.1 Project Introduction

NG-SOC is a three-year project (2024 - 2026) applied by a consortium of ten partners from seven European countries. It is co-funded under the Digital Europe Programme to address one of the most pressing challenges in the EU today: ensuring that essential and important entities can detect, analyse, and respond effectively to cyber threats in an increasingly interconnected and regulated digital environment.

The project's overarching goal is to design and deploy a joint, interoperable, and multi-service SOC platform. This platform combines leading-edge detection and response capabilities with advanced training environments, enabling national and cross-sector operators to:

- Achieve situational awareness across complex threat environments.
- Coordinate incident detection, response, and recovery across borders.
- Build cybersecurity capacity through tailored educational programmes and simulations.

NG-SOC adopts an open-standards and open-source approach, ensuring scalability, modularity, and sustainability. This design choice not only facilitates integration with existing infrastructures but also ensures alignment with current and forthcoming EU regulatory frameworks, including NIS2, CRA, CSA, and DORA.

1.2 Deliverable Purpose

Deliverable D7.2 represents the first comprehensive business plan of the NG-SOC project. While the primary mission of NG-SOC is to strengthen Europe's cyber resilience, the long-term success of the platform depends on its ability to sustain itself beyond the project lifetime. This requires a clear, evidence-based exploitation and sustainability strategy.

The deliverable therefore aims to:

- Identify and characterise Key Exploitable Results (KERs), ranging from advanced software modules and services to training programmes and sector-specific knowledge.
- Define exploitation routes for scientific, commercial, and policy-driven uptake.
- Analyse market dynamics and policy drivers, including the impact of NIS2, the Cyber Solidarity Act, and sector-specific regulations.
- Develop the initial business model and risk analysis to guide future commercialisation and community-driven sustainability.
- Outline individual partner exploitation plans to capture the diverse opportunities across industrial, academic, and public-sector stakeholders.

By doing so, D7.2 lays the foundation for the project's exploitation pathway and provides a structured response to Horizon Europe requirements for impact and sustainability. It also prepares the ground for D7.3 (final business plan, due M36), which will refine the strategy with updated market insights, exploitation agreements, and consolidated sustainability measures.

1.3 Deliverable Structure

The deliverable is structured as follows:

- **Section 2** presents the overall exploitation strategy, including its three phases: pre-marketing, ramp-up, and market penetration.
- **Section 3** details the business model, market analysis, regulatory drivers, risk analysis, and NG-SOC's positioning.
- **Section 4** identifies and characterises the project's Key Exploitable Results (KERs).
- **Section 5** provides the individual exploitation plans of each consortium partner.
- **Section 6** sets out the Intellectual Property Rights (IPR) strategy.
- **Section 7** describes NG-SOC's contributions to standardisation activities.
- **Section 8** concludes with next steps towards impact realisation and sustainability.

2 Initial Exploitation Strategy

As outlined in D7.1, NG-SOC's exploitation framework is structured across three phases: pre-marketing, exploitation ramp-up, and market penetration. The initial plan defined the approach, preliminary Key Exploitable Results (KERs), and partner-level intentions.

Additionally, D7.2 builds directly on this foundation by moving from strategy definition towards a concrete **business model and market positioning**. It introduces measurable KPIs, sustainability pathways, and partner-specific plans reflecting the updated consortium composition. In particular, the inclusion of **FUNITEC** (training and education focus) and **ELES/INFO** (energy sector pilot) extends the scope of exploitation beyond the initial version.

2.1 Exploitation Routes

The exploitation routes first introduced in D7.1 remain valid:

- **Scientific**: dissemination through academic publications, conferences, and roadmaps.
- **Commercial**: industrial exploitation through partner networks and market channels.
- **Networks and Policy Groups**: engagement with associations, initiatives, and regulators.

D7.2 extends these routes by explicitly integrating the perspectives of **energy operators** (via ELES/INFO) and **training providers** (via FUNITEC). As a result, the consortium now addresses a wider set of stakeholders:

- Banking & financial services (CaixaBank pilot)
- Energy operators & regulators (ELES/INFO pilot)
- Digital infrastructure & research networks (CYNET pilot)
- Training and education providers (FUNITEC)
- Research partners (UPRC)
- SMEs and managed SOC clients (INSIGHIO)
- Technology providers & SOC operators (ED, SPH, CYEN).

This framing ensures that NG-SOC is not only technically robust but also positioned for diverse sectoral uptake.

2.2 Exploitation Phases

The phased approach described in D7.1 continues to guide exploitation activities:

- **Phase A (Pre-marketing)** focused on mapping technologies, market drivers, and early KERs.
- **Phase B (Ramp-up)**, now underway, emphasizes strategic analysis, partner plans, and initial business modelling.
- **Phase C (Market penetration)** will consolidate exploitation agreements and financial models in D7.3.

In this deliverable, Phase B is elaborated with updated **market analysis**, **risk assessment**, and **partner KPIs**. The addition of ELES/INFO and FUNITEC ensures that exploitation activities cover both a **new critical sector (energy)** and a **horizontal enabler (training/skills)**. These updates strengthen the overall strategy and demonstrate how NG-SOC evolves in line with consortium composition and EU policy developments. Furthermore, **Figure 1 has also been updated to include ELES/INFO and FUNITEC within the consortium landscape**, ensuring that the exploitation strategy visually reflects the revised partner composition and their respective roles.

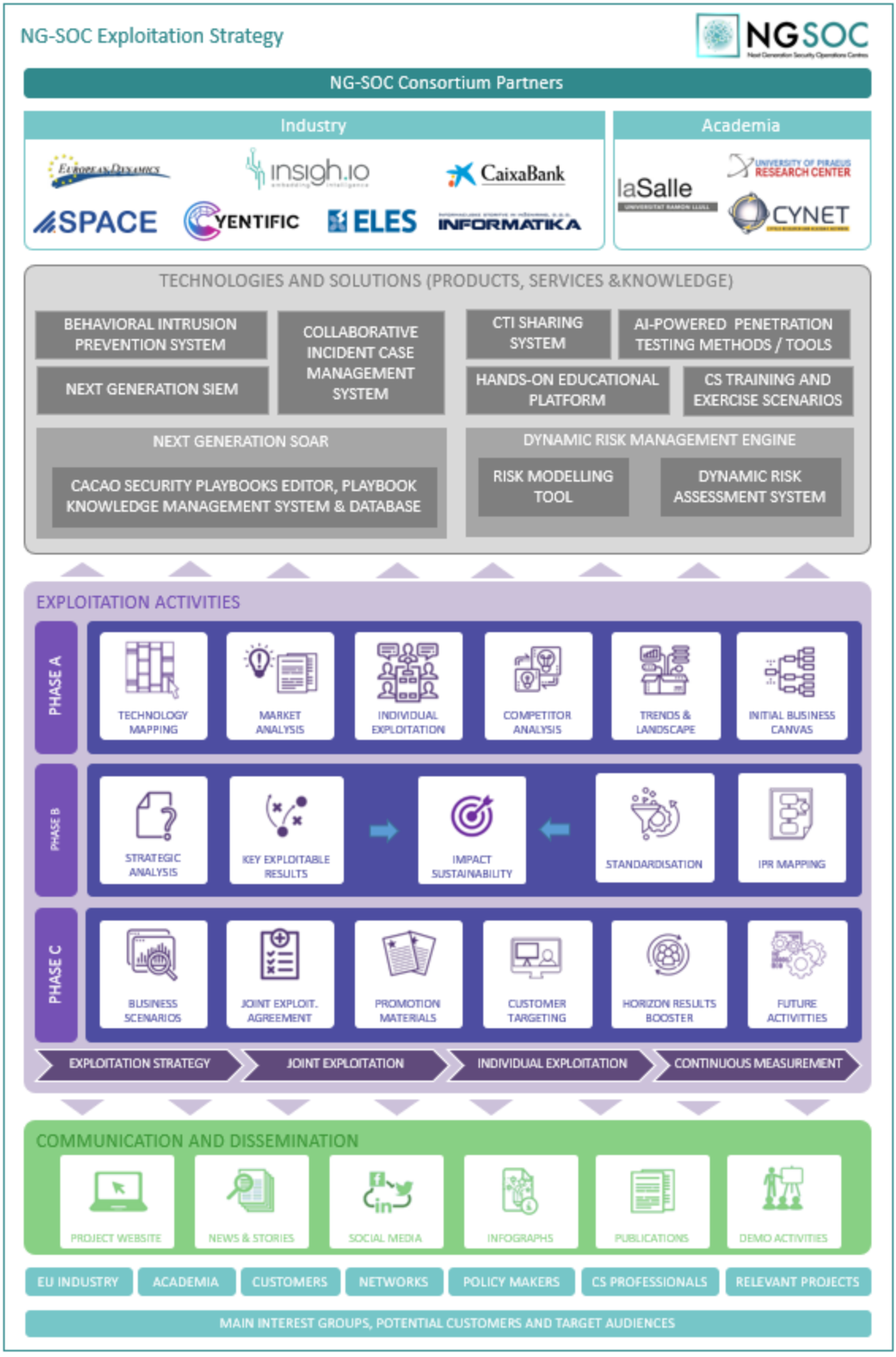

Figure1.NG-SOC Exploitation strategy overview

3 Business Model

NG-SOC's business model is designed to address the growing cybersecurity challenges faced by European organisations, particularly Operators of Essential Services (OES), national CSIRTs, critical infrastructure providers, private SOC operators, and cybersecurity training entities. The model reflects both the technical ambitions of the project and its alignment with market realities, European policy objectives, and the need for long-term sustainability.

The primary focus is to deliver a modular, interoperable, and standards-based SOC platform that enhances cyber resilience while enabling compliance with the NIS2 Directive and the Cyber Solidarity Act. NG-SOC reduces the reliance on proprietary, fragmented solutions by offering an open-source alternative built specifically for the diverse operational needs of Europe's critical sectors.

Customer segments include:

- National SOC operators and CSIRTs responsible for threat detection, incident response, and information sharing.
- Operators of Essential Services in the banking, energy, and digital infrastructure sectors who require enhanced SOC capabilities.
- Private SOC providers seeking to expand their service offerings with modular, interoperable tools.
- Cybersecurity training providers, including academic institutions, aiming to improve hands-on skills development.
- SMEs that could adopt NG-SOC through future SOC-as-a-Service offerings: include those operating in sectors covered by NIS2 and related regulations, such as digital infrastructure providers, managed service providers, healthcare facilities, water supply and wastewater management companies, manufacturing of critical products (e.g. medical devices, pharmaceuticals, chemicals), postal and courier services, food production and distribution, and entities in the banking and financial market infrastructure sectors.

Added Value is delivered by NG-SOC through:

- Reduced vendor lock-in via open standards and open-source software.
- Enhanced detection, response, and threat intelligence sharing capabilities.
- Integrated cyber range and training modules to build workforce capacity.
- Future scalability through modular architecture.
- Modular end-to-end architecture, which can be used to guide decisions for complementing existing services of an organisation.

Revenue generation for commercial exploitation includes:

- Support and maintenance packages tailored to different user needs.
- Consulting and integration services to facilitate NG-SOC deployment.
- SaaS deployment models for non-governmental entities.

- Custom development of sector-specific modules and service extensions.
- Comprehensive training and certification programmes on cyber range [9], including setting up and deploying custom infrastructures and tailored scenarios to individual organisations' needs.

By offering interoperability through open standards and modularity, NG-SOC reduces vendor lock-in, strengthens incident detection and response capabilities, and facilitates compliance with regulatory frameworks such as NIS2. The integration of training and education components further addresses Europe's cybersecurity workforce challenges.

3.1 Market and Policy Update-Requirements for NG-SOC

The cybersecurity landscape in the European Union is undergoing a major transformation driven by the rapid expansion of digital services, the growing interdependence of critical sectors, and the increasing sophistication of cyber threats. In response, the EU has introduced an updated and more comprehensive regulatory framework, notably through the NIS2 Directive (EU) 2022/2555, the proposed Cyber Solidarity Act, the Digital Operational Resilience Act (DORA), and the EU Cybersecurity Strategy.

The **NIS2 Directive**, in force since January 2023, expands the scope of the original NIS Directive by including more sectors (e.g., public administration, wastewater, space) and introduces stricter supervisory and enforcement measures. More precisely, NIS2 adopts an "all hazards" approach that mandates the implementation of cybersecurity risk management measures, incident reporting, business continuity planning, supply chain security checks, situational awareness processes, preparedness measures, and regular security testing, including penetration testing. For NG-SOC, this regulatory framework implies a demand for cross-sectoral monitoring and detection capabilities that align with diverse threat environments, scalable and interoperable SOC components that can serve both large and smaller operators across critical sectors, such as banks, energy, and academia, and enhanced compliance support and auditability features to enable operators to meet regulatory obligations efficiently.

The **Cyber Solidarity Act**, currently under legislative negotiation, proposes the creation of a European Cyber Shield, a network of national and cross-border SOCs that would jointly detect, analyze, and respond to large-scale cyber incidents. The initiative will supply advanced detection platforms, real-time data sharing mechanisms, and mutual assistance protocols, fostering collective preparedness, emergency response, and pan-European defence capabilities. NG-SOC is uniquely positioned to contribute to this vision by providing a modular SOC platform that is aligned with EU values of collaborative cybersecurity, transparency, and technological sovereignty.

Additionally, **DORA**, which came into force in January 2025, is of particular relevance to the financial sector, where NG-SOC's banking pilot partner, CaixaBank operates. It introduces harmonised requirements for ICT risk management, incident reporting, operational resilience testing and third-party risk management across EU financial entities and their critical ICT service providers. NG-SOC's architecture, with its interoperability, automation, and compliance-ready features, directly supports these obligations.

Complementing these efforts, the **EU Cybersecurity Strategy** underscores the importance of building trusted security solutions, fostering cyber resilience across supply chains, and enabling public-private collaboration. NG-

SOC addresses these goals by embedding European innovation, sector-specific threat intelligence, and co-creation with operators at the heart of its platform design.

However, despite growing awareness of cybersecurity risks, **a significant number of entities remain underprepared to meet these new expectations**. Many mid-sized and sectoral operators, including SMEs in regulated sectors, lack the operational maturity and resources to comply with NIS2, DORA, or to participate in cross-border collaboration mechanisms under the **Cyber Solidarity Act**. So far, the market has failed to provide accessible and regulation-ready solutions for the stakeholders. Therefore, NG-SOC fills this gap by offering a **European-built, modular, open-source and scalable SOC solution** designed to operationalise regulatory frameworks while supporting interoperability with future EU-level initiatives.

Regarding the NG-SOC project, it is situated within a rapidly maturing cybersecurity policy landscape shaped by the NIS2 Directive, the proposed Cyber Solidarity Act, and the evolving EU Cybersecurity Strategy. Key requirements include:

- **Comprehensive Risk analysis and information system security policies** that are often updated to reflect evolving threat landscapes. NG-SOC's Dynamic Risk Management Engine supports this requirement by continuously assessing asset risk profiles, correlating threat intelligence, and providing decision-support dashboards that help organisations prioritise mitigations in line with sectoral risk appetites.
- **Effective handling of incidents, business continuity, and crisis management**, making sure that organisations have established processes for detecting, responding and recovering from cyber incidents. NG-SOC's integrated Next Generation SIEM and SOAR components automate threat detection, orchestrate coordinated responses, and provide post-incident forensic analysis, reducing recovery times and maintaining service continuity during crises.
- **Strengthened supply chain security and secure development practice**, requiring organisations to assess and mitigate risks posed by third-party service providers and suppliers. NG-SOC facilitates this through its CTI Sharing System and interoperability with multiple threat intelligence sources, enabling early detection of supply chain-related threats and aligning with secure-by-design principles in SOC integration.
- **Timely and clear reporting obligations and coordinated vulnerability disclosure** that ensure incidents with significant impact are reported to the relevant national authorities within the mandated timeframes. NG-SOC's Collaborative Incident Case Management System standardises incident documentation, supports CACAO-compatible reporting, and integrates with national CSIRTs, ensuring compliance with both reporting deadlines and coordinated vulnerability disclosure requirements.

The **Cyber Solidarity Act** (COM/2023/209) introduces the vision of a "European Cyber Shield," proposing a network of national and cross-border Security Operations Centres (SOCs) that can share threat intelligence in real time. This initiative is designed to address large-scale cross-border incidents and support a rapid operational response.

The **EU Cybersecurity Strategy** emphasizes digital sovereignty, sectoral preparedness, and interoperability across the Union. It encourages both innovation and compliance and highlights the need for platforms that

bridge national infrastructures with EU-level capabilities. Aligned with this is the NG-SOC envisaged strategic impact:

- ✓ Aligns with EU Cybersecurity Strategy & NIS2 Directive
- ✓ Enhances cross-sector preparedness & operational resilience
- ✓ Supports transition from reactive to proactive cybersecurity

In response to these regulatory trends, NG-SOC has been designed to provide a compliance-ready, scalable, and modular SOC framework. Its key features align with legal obligations from NIS2 (e.g., incident escalation, threat monitoring, secure communications) and are extensible to anticipated requirements from the Cyber Solidarity Act. Its technical framework includes:

- Early detection & classification of cyber threats
- Automated detection, investigation, and response
- Interoperable open-source SOC toolkit
- Orchestration of incident response workflows
- Links for cross-border and cross-organizational cooperation and collaboration across EU institutions

The NG-SOC (Next-Generation Security Operations Center) project is designed to meet the evolving cybersecurity needs of organizations of all sizes, from small businesses to large enterprises and critical infrastructure providers. Its key strengths include:

- **Comprehensive Security Solution:** NG-SOC delivers an end-to-end cybersecurity framework that integrates detection, response, and prevention capabilities into a unified platform.
- **Reference Implementation:** It serves as a benchmark model for deploying modern SOC architectures, helping organizations align with best practices and industry standards.
- **Modular Toolset:** Offers a flexible suite of off-the-shelf components that can be easily integrated into existing systems, reducing deployment time and complexity.
- **Open Standards for Interoperability:** Built on open standards to ensure seamless adaptability and interoperability across diverse environments and technologies.
- **Innovation Testbed:** Provides a controlled environment for validating new cybersecurity concepts, tools, and methodologies before full-scale implementation.
- **Cybersecurity Upskilling:** Supports workforce development by offering hands-on training and resources to enhance cybersecurity expertise across roles.

3.2 Target groups and their needs

NG-SOC addresses the cybersecurity needs of both **essential** and important entities, as defined under the NIS2 Directive. According to the directive, essential entities are those whose operations are critical to societal or

economic activities, such as energy providers, banks, healthcare institutions, and public administrations. Important entities may not have the same systemic impact but are nonetheless subject to cybersecurity obligations due to their role in maintaining services of public interest. These classifications apply to both public and private actors, including key suppliers and service providers operating within or across EU Member States.

The **NIS2 Directive** (Directive (EU) 2022/2555) significantly broadens the scope of cybersecurity regulation across the European Union, impacting a wide array of sectors deemed essential or critical to societal and economic stability. NG-SOC is strategically designed to support this expanded landscape with a modular, scalable architecture that adapts to the unique needs of each stakeholder. NIS2 applies primarily to **medium-sized and large organizations** operating in sectors classified as:

Figure 2: NIS2 Sector Categories and Examples of Affected Entities

Sector Category	Examples of Affected Entities
Highly Critical	Energy, banking, finance, healthcare, transport, water
Other Critical	Digital infrastructure, public administration, space

Based on insights from NG-SOC's pilot use cases and alignment with the NIS2 scope, the following target groups and needs have been identified:

- **Banking & Finance Sector (Pilot: CaixaBank)**: Includes banks, fintechs, payment institutions, and investment services. As essential entities, they require high-assurance threat detection, robust data protection, secure transaction oversight, and automation of compliance workflows to meet stringent regulatory timelines.
- **Digital Infrastructure Sector (Pilot: CYNET)**: Covers NRENs, DNS services, and cloud platforms. These can be essential or important depending on their size and service footprint. Their needs focus on interoperability with CSIRTs, federated threat intelligence sharing, and maintaining secure access for diverse stakeholders.
- **Energy Sector (Pilot: ELES/INFORMATIKA)**: Includes transmission and distribution operators (TSOs/DSOs) and energy IT vendors. These are essential entities requiring deep OT/IT integration, monitoring, anomaly detection in ICS environments, and tools that support both NIS2 compliance and resilience planning.

Figure 3: NIS2 Directive: Classification of Critical and Very Critical Sectors

NG-SOC's architecture has been built to enable a tiered and flexible deployment model, ensuring it can effectively support critical operators across the NIS2 spectrum, both large and small—while enabling future integration with EU-level cybersecurity initiatives.

The market Size of these target groups in EU is vast:

Over 160,000 entities across the EU are estimated to fall under the scope of NIS2, a dramatic increase from the few thousand covered under the original NIS Directive. This includes:

- **Thousands of hospitals and healthcare providers**
- **National and regional public administrations**
- **Energy and water utilities**
- **Financial institutions and digital service providers**

The directive also indirectly affects **SMEs** operating within the supply chains of regulated entities, creating ripple effects across the broader economy.

3.3 Market Needs and Size

The European cybersecurity landscape is rapidly evolving, driven by regulatory reforms and a rising frequency of complex cyber threats. The NIS2 Directive (Directive (EU) 2022/2555)[1] mandates comprehensive requirements for risk management, business continuity, incident response, and cross-border cooperation across an expanded scope of critical and important entities. Yet, many organisations, especially mid-sized or sectoral operators, remain under-equipped due to fragmented cybersecurity infrastructure, lack of preparedness protocols, and poor interoperability with national CSIRTs and EU-level coordination networks.

As noted by ENISA (2023) in its Best Practices for Cyber Crisis Management, significant challenges persist across the cyber crisis response lifecycle, particularly for critical infrastructure operators. These include:

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

- **Unclear escalation paths:** Many organisations lack predefined decision trees or chain-of-command protocols, delaying time-sensitive incident containment and cross-sector communication.
- **Absence of situational dashboards**: The inability to visualise, correlate, and act upon real-time threat intelligence hampers the coordination of stakeholders during a live incident.
- **Inconsistent communication formats:** Without harmonised formats and vocabularies, the transmission of alerts and updates between entities (e.g., CSIRTs, regulators, SOCs) is error-prone and fragmented.
- **Under-tested response protocols:** Many operators have not validated their crisis workflows through regular simulations or red-team exercises, resulting in procedural gaps during real-world attacks.
- **Lack of affordable, regulation-ready platforms:** Existing SOC solutions often do not align with the specific requirements of NIS2 and other EU regulations, especially for small-to-medium public entities and sectoral CSIRTs.

3.3.1 Rising Demand Across Sectors

The European cybersecurity market is forecasted to grow strongly, reaching around USD 56.96 billion in 2024 and expected to surpass USD 107.5 billion by 2030, at a compound annual growth rate of 11.2 percent [9]. The Banking, Financial Services and Insurance (BFSI) sector currently accounts for the largest share, while healthcare and SMEs are among the fastest-growing segments [9]. NG-SOC's pilots in banking, energy, and digital infrastructure are therefore well aligned with present market needs, while an expansion into healthcare and SME offerings would further strengthen its positioning in high-growth segments.

3.3.2 Skills Shortage & Managed Services Uptake

Europe continues to face a critical cybersecurity workforce gap, estimated at more than 300,000 professionals [18]. This shortage has been highlighted in policy analyses, such as the OECD (2024), which stresses the importance of building advanced cyber skills across Europe, and ENISA (2023), which emphasises the role of simulation environments and structured training in enhancing resilience. NG-SOC's integrated training modules, including the CYNET pilot, and its open-source design, directly respond to these needs by supporting both workforce development and the growing uptake of managed services.

3.3.3 Consolidation & Interoperability

Organisations are increasingly consolidating vendors and prioritising interoperable, standards-based solutions to manage costs and reduce complexity [9]. At the same time, ENISA (2023) has underscored the necessity of interoperability between SOCs and CSIRTs to strengthen cross-border preparedness and incident response. NG-SOC, through its modular architecture and adherence to open standards, is designed to address these challenges, enabling adaptability, compliance with EU-level initiatives such as the NIS2 Directive and the proposed Cyber Solidarity Act [3],[4] and long-term sustainability.

3.3.4 Risk Analysis

NG-SOC faces several identifiable risks, Table 1, in its path to exploitation. Market adoption risks stem from competition with established vendors and potential inertia within targeted sectors. Regulatory delays could affect market timing, while technical integration challenges and sustainability concerns around open-source components present additional risks. Mitigation measures include robust pilot demonstrations, ongoing policy

engagement with relevant EU bodies, a modular and flexible technical architecture, and the establishment of a dedicated governance model to oversee long-term platform maintenance and community-driven development.

Table 1: Risk Analysis

Risk ID	Category	Description	Likelihood	Impact	Mitigation	Responsible Partner
R1	Market Adoption	Resistance from large operators preferring incumbent vendors	Medium	High	Highlight compliance-ready features, leverage pilots for credibility, targeted outreach to regulators	ED, CXB
R2	Regulatory	Delay in adoption of Cyber Solidarity Act or divergence in national NIS2 transposition	Medium	Medium	Maintain active liaison with ENISA/ECCC; adjust positioning to align with national regulatory timetables	ED, INS
R3	Technical Integration	Interoperability issues between NG-SOC modules and legacy systems	High	High	Modular architecture, open standards, pilot validation, integration toolkits	SPH, CYEN
R4	Sustainability	Lack of funding for open-source maintenance post-project	Medium	High	Establish governance board, explore SOC-as-a-Service model, pursue Horizon follow-up and CEF funding	ED, INS, CYNET
R5	IPR/Legal	Ambiguity in ownership of joint results or conflicting licenses	Low	High	Define licenses per KER (Apache 2.0, GPL, proprietary add-ons), clarify in Consortium Agreement addendum	ED, All partners
R6	Skills/Workforce	Insufficient uptake of training modules due to limited awareness	Medium	Medium	Partner outreach via universities, ECSO, sector associations; certifications and micro-credentials	FUNITEC, UPRC

R7	Competition	Rapid evolution of commercial SOC-as-a-Service offerings (Atos, IBM, Microsoft Sentinel)	High	Medium	Differentiate via EU compliance, open source, modularity, community trust	ED, All

This structured risk register will be updated bi-annually and integrated with the project's overall risk management framework, ensuring alignment between technical, business, and exploitation risks.

3.4 NG-SOC market positioning

NG-SOC positions itself as a European cybersecurity operations platform designed to meet the regulatory, operational, and technological needs of critical entities in the NIS2 era. Its market differentiation is defined by the following pillars:

- **Compliance-Driven Design**: NG-SOC offers out-of-the-box features aligned with EU directives, particularly NIS2, including incident reporting modules, audit logs, and role-based access control.
- **Modular and Scalable Architecture**: The platform supports adaptation to various operational scales, from large national SOCs to small sector-specific operators, making it suitable for deployment across the spectrum of critical and important entities. This architecture can be used as a reference for the entities that need to comply with the directives, but also to enhance their cyber protection measures by integrating missing features (and tools) and adopting standardised interfaces to facilitate their integration towards a holistic cybersecurity solution.
- **Cross-Sectoral Flexibility**: NG-SOC has been piloted in finance, energy, and research/education sectors, demonstrating its capability to address heterogeneous threat landscapes through configurable detection and response workflows.
- **European Trust and Governance**: Built and validated within an EU-funded framework, NG-SOC adheres to principles of data sovereignty, transparency, and collaborative threat sharing, reinforcing its suitability for sensitive infrastructures.
- **Integrated Escalation Frameworks:** Built-in decision trees and incident workflows aligned with NIS2 and EU-CyCLONe protocols.
- **Real-Time Situational Dashboards:** Visual correlation of threat intelligence, asset impact, and stakeholder roles for rapid response.
- **Standardized Communication Modules:** Harmonized alert formats and vocabularies to streamline coordination across CSIRTs, SOCs, and regulators.
- **Simulation & Training Environments** Red-team automation and crisis simulation tools validated through pilots (e.g., CaixaBank, CYNET).
- **Regulation-Ready Architecture:** Affordable, open-source SOC components tailored for SMEs, public entities, and sectoral CSIRTs.

In contrast to generic or highly centralised cybersecurity solutions, NG-SOC offers a strategic fit for the European cybersecurity ecosystem, addressing fragmented capabilities while supporting shared situational awareness, operational coordination, and trust among Member States. NG-SOC supports the translation of EU-level strategic

goals into practical and deployable tools, NG-SOC bridges the gap between high-level policy and ground-level implementation. Its value lies in enabling compliance, enhancing resilience, and supporting Europe's ambition for digital sovereignty.

3.5 Go-To-Market Strategy

The NG-SOC go-to-market strategy is carefully designed to leverage the project's strengths, align with market needs, and ensure broad uptake across Europe. A phased, targeted approach ensures that early adopters in key sectors validate the platform's capabilities, laying the groundwork for wider market entry.

- At the core of this strategy is real-world validation through the project's three pilots:
- **CaixaBank (Financial Sector):** Demonstrating NG-SOC's effectiveness in fraud detection, red team automation, and compliance with banking-sector cybersecurity requirements.
- **CYNET (Academic/Digital Infrastructure Sector):** Showcasing the platform's utility for SOC operations within research networks and its integration with advanced hands-on training environments.
- **ELES/INFORMATIKA (Energy Sector):** Validating NG-SOC for critical infrastructure protection, advanced threat detection, and resilience testing within the energy sector.

These pilots provide tangible proof of NG-SOC's functionality, sectoral applicability, and ability to address both technical and organisational cybersecurity needs.

The **initial market focus** targets:

- National SOC operators and CSIRTs.
- Operators of Essential Services (banking, energy, digital infrastructure).
- Cybersecurity training providers, including universities and specialised academies.

NG-SOC will actively pursue strategic partnerships with:

- European standards bodies such as ETSI and OASIS, to enhance market credibility and promote interoperability.
- Sector-specific associations and forums to facilitate targeted outreach.
- EU regulatory authorities, including ENISA [5] and relevant DGs of the European Commission, to align with policy developments and funding instruments.

3.5.1 Market Drivers

- **Regulatory Momentum** NIS2 Directive and Cyber Solidarity Act create urgent demand for scalable, compliant cybersecurity solutions.
- **Open-Source Adoption** Growing preference for transparent, community-driven security frameworks across public and private sectors.
- **Digital Transformation** Increasing reliance on digital infrastructure heightens the need for robust SOC capabilities.

Regulatory momentum, particularly the implementation of NIS2 and the Cyber Solidarity Act, is a key market driver. NG-SOC is positioned as a practical enabler of compliance, supporting essential service providers and national authorities in meeting their legal and operational obligations.

Beyond the initial project lifecycle, NG-SOC's go-to-market strategy anticipates scalability through:

- Expansion beyond the pilot sectors.
- Development of a SOC-as-a-Service offering for SMEs.
- Continued engagement with the open-source community to foster innovation and widespread adoption.

This multi-faceted strategy ensures that NG-SOC does not merely remain a research output, but becomes a sustainable, impactful cybersecurity solution embedded within Europe's digital ecosystem.

3.5.2 Open-Source Distribution & Reference Architecture Promotion

- **GitHub Repository** NG-SOC's modular components, reference implementation, and documentation will be published on GitHub under a permissive open-source license to encourage adoption, contribution, and integration.
- **Reference Architecture Publication** A formalized, standards-aligned reference architecture will be disseminated via:
    - Technical whitepapers
    - ENISA-aligned implementation guides
    - Sector-specific deployment templates
- **Digital Promotion** Targeted advertising and content marketing via:
    - LinkedIn, and cybersecurity forums
    - EU-funded project showcases and Horizon Europe platforms
    - GitHub trending and developer community engagement

3.5.3 Sector-Specific Outreach via Partner Channels

Each consortium partner will activate their existing networks to promote NG-SOC within their operational domains, as presented in Table 2:

Table 2: Partner Operational Domains

Partner	Sectoral Reach	Outreach Strategy
ED	Banking, healthcare, public sector	Leverage existing client relationships and sectoral influence to promote NG-SOC as a compliance and resilience solution.
CaixaBank	Financial services	Demonstrate NG-SOC's fraud detection and red-team automation capabilities through industry events and banking associations.

CYNET	Academic and research networks	Promote NG-SOC as a training and SOC operations platform via university alliances and cybersecurity education forums.
ELES/INFORMATIKA	Energy and utilities	Showcase NG-SOC's threat detection and resilience testing in energy sector conferences and regulatory briefings.

3.5.4 Strategic Alliances & Capability Extension

To ensure NG-SOC offers a complete solution across diverse use cases, partners will form **alliances and service agreements** to fill capability gaps and extend functionality:

- **FUNITEC:** Provide novel, tailored cybersecurity simulation environments, combining theory and hands-on, for advanced training.
- **CYEN:** Lead the development of executable CACAO playbooks for automated incident response, aligned with NIS2 and EU-CyCLONe protocols.
- **UPRC:** Innovative cutting-edge ML enhanced dynamic risk management, alongside state-of-the-art educational material for training Europe's next generation SOC analysts.
- **SPH:** Provide cross-border SOCaaS bundles by integrating NG-SOC with existing custom and off-the-shelf solutions.
- **INS:** Dissemination of project results to enhance SMEs' capabilities to handle cyber incidents/threats.
- **Other Consortium Members:** Offer integration support, training services, and sector-specific customization to ensure NG-SOC meets operational and regulatory needs.

3.5.5 Integration with EU Cybersecurity Ecosystem

NG-SOC will actively pursue integration into broader EU cybersecurity initiatives:

- **REWIRE project collaboration** NG-SOC is aligned with the REWIRE project Blueprint and the methodology provided. Moreover, NG-SOC is extending the REWIRE legacy creating new training materials and new training environments on the Cyber Range (powered by CyberRangeCZ Platform, also known as KYPO Cyber Range).
- **ENISA & ECCC Collaboration** Position NG-SOC as a reference implementation for EU-wide SOC capabilities and cyber crisis coordination.
- **Participation in EU Cyber Exercises** Demonstrate NG-SOC's operational readiness and interoperability in cross-border simulations.
- **Alignment with EU Funding Instruments** Leverage Digital Europe Programme, Horizon Europe, and Connecting Europe Facility (CEF) for scaling and sustainability.
- **Collaboration with the EU-iNSPIRE Project** for delivering micro credential course on SOC operation, as well as on the proposed Master courses.
- **Synergy with CY-TRUST project:** Joint workshop & training event pertinent to topics such as SOC infrastructures, Threat intelligence, Incident Response, Playbooks, Artificial Intelligence and Security.

3.6 NG-SOC Solution Response

The NG-SOC platform delivers a coherent and technically mature response to key structural challenges identified in the evolving EU cybersecurity landscape. By aligning its architecture with the NIS2 Directive, the Cyber Solidarity Act, and ENISA's crisis management best practices, NG-SOC addresses both regulatory and operational fragmentation. The project's solution directly contributes to the expected results outlined in the Horizon Europe call by ensuring scalability, interoperability, and demonstrable security impact across sectors, as presented in Table 3.

Table 3: NG-SOC Solution Response

Expected Result	Policy Challenge	NG-SOC Contribution	Policy Reference
Improved coordination between cybersecurity actors at EU and national levels	Fragmented incident reporting chains and inconsistent communication formats impede coordinated cyber crisis response across borders and sectors.	- Role-based incident workflows - Escalation trees and multilingual notification templates - Real-time integration with national CSIRTs	NIS2 Article 21, Recital 57; ENISA (2023), pp. 24–25
Effective incident response and recovery capabilities at scale	Absence of tested playbooks and limited simulation capacity across sectors weakens crisis preparedness.	- Integrated crisis playbook and simulation support - Audit-ready logs - Regulatory conformance tools	NIS2 Articles 23, 32
Situational awareness and shared threat intelligence capabilities	Lack of real-time situational awareness tools and sector-specific dashboards among critical infrastructure operators.	- Threat intelligence engine with log correlation - Sector-specific dashboards - Contextual risk analysis tools	NIS2 Article 21(2)(d); ENISA (2023)
Practical tools for compliance and cybersecurity capability building	Smaller and mid-sized operators lack affordable, regulation-aligned platforms tailored to their operational needs.	- Modular SOC toolkit - Built-in compliance indicators and audit support - Validation across banking, energy, infrastructure pilots	NIS2; Cyber Solidarity Act COM/2023/209

By addressing both policy-driven challenges and technical implementation gaps, NG-SOC contributes to a European cyber defense architecture that is resilient, inclusive, and legally compliant. Its cross-sector validation ensures broad applicability and future alignment with evolving EU policy frameworks.

These capabilities have been piloted and validated across banking, energy, and research sectors, showcasing NG-SOC's cross-sectoral applicability and deployment maturity. Table 5 present a comparison of NG-SOC vs vendor solutions.

Table 4: Competitor Benchmarking Table

Vendor / Solution	Core Offering	Strengths	Weaknesses vs. NG-SOC	NG-SOC Differentiation
Splunk (Enterprise Security)	Commercial SIEM & analytics	Strong brand, advanced analytics, integrations	High licensing costs, vendor lock-in, limited EU regulatory tailoring	Open-source, compliance-ready, cost-effective
Palo Alto Cortex XSOAR	SOAR platform	Mature automation, ecosystem integrations	Proprietary playbooks, limited CACAO support	CACAO v2 native, open sharing of playbooks
Atos Prescriptive SOC	Managed SOC-as-a-Service	Global reach, managed services	Centralised, limited modularity, less transparent	Decentralised, modular, adaptable to SMEs
IBM QRadar	SIEM + threat detection	Advanced analytics, integration	Expensive, heavy infrastructure footprint	Lightweight, EU-focused compliance
Microsoft Sentinel	Cloud-native SIEM/SOAR	Scalable, cloud-native, strong AI	Locked to Azure ecosystem, US-based governance	EU-built, data sovereignty, multi-cloud interoperability
NG-SOC (proposed)	Modular SOC platform, training, CTI sharing	Open standards, interoperability, EU regulatory compliance, pilot validation	New entrant, requires community growth	Positioned as EU reference SOC platform bridging regulation & practice

4 Key Exploitable Results

The following Table 5 represents the identification of the Key Exploitable Results (KERs), as they were mutually agreed by the consortium. The generated list represents the most innovative results that have been achieved or will be delivered by the end of the project. Their exploitation potential is expected to have either commercial, social, or scientific value. Here, exploitable results can include equipment, hardware, processes, products, services, knowledge & IP, and other forms of knowledge (publications, patents, etc.). In NG-SOC, the following types of results have been outlined:

- **Software/Application**: Innovative IT solutions that are integrated into the NG-SOC architecture and that enable either unique, ground-breaking, or beneficial functionalities.
- **Service**: The envisioned capacity-focused, AI-enhanced SOC service together with the dedicated training sessions and educational programmes in digital infrastructure security represent unique services focusing on increasing the level of automation in SOC/CSIRT operations while delivering multidisciplinary and realistic training and knowledge testing in multiple domains.
- **Knowledge/Use case**: provides a better understanding or otherwise not readily available information about specific use case scenarios within the banking, energy, and educational domains, which will, in turn, help to create a more realistic and useful SOC service and hands-on training.

For each Key Exploitable Result (KER), the consortium will pursue a dual exploitation pathway: (1) open-source release of baseline functionalities under a permissive license (e.g., Apache 2.0 or GPLv3), and (2) value-added commercial extensions provided through service, support, or consulting. This ensures both broad community adoption and sustainability through revenue generation. Each KER will be characterised by TRL, IPR measures, target customers, and market readiness, with periodic updates feeding into the final business plan (D7.3).

Table 5: NG-SOC Key Exploitable Results (KERs)

No	KER	Type	Partner(s)
1.	Behavioural Intrusion Prevention System	Software / Application	SPH
2.	AI-Powered Penetration Testing Methods and Tools	Software / Application / Service	EDGR, SPH
3.	CTI Sharing System	Software / Application	EDGR
4.	Dynamic Risk Management Engine	Software / Application	UPRC, INS, EDGR
5.	Next Generation SIEM	Software / Application	SPH
6.	Next Generation SOAR	Software / Application	CYEN
7.	Collaborative Incident Case Management System	Software / Application	EDGR
8.	Hands-on Educational Platform	Software / Application	EDGR, ED
9.	Cybersecurity Training and Exercise Scenarios	Software / Application /Service	ED, EDGR, UPRC, FUNITEC

10.	Sectorial Training Programs	Knowledge / Use cases	CXB, CYNET-CSIRT, ELES/INFO

The next step is to carry out the characterisation of the identified results using a systematic approach. Here, the characterisation focuses on the assessment of the results' technological maturity (in their current phase) using the Technology Readiness Level (TRL) framework, as shown in Table 6. In any case, after the end of the project, the identified results will potentially need further development, refinement, optimisation, or investment before they can be fully exploited commercially. Furthermore, several additional parameters are used to define the results in the context of innovation, uniqueness, market potential and IPR measures:

- **Description**: Brief description about the result.
- **What problems are solved**: What problems does the result solve? / Why has this result been achieved in NG-SOC?
- **Innovativeness/new approach**: What is the new element/approach/innovation of the result that distinguishes it from the state of the art?
- **Unique selling point**: In what way is the solution better (faster, cheaper, more reliable, more efficient, with less undesired effects)?
- **Competitors (solutions)**: Who are the main competitors of the result?
- **Target users / customers**: Who will potentially use the result?
- **Benefits for users / customers**: What benefit will the result bring to end users? Why should the end users invest in or adopt the result?
- **TRL level**: Estimation of the result's technology maturity.
- **Main technical challenge(s)**: What are the main technical challenges which need to be or were solved?
- **Legal / ethical requirements**: Legal, normative, or ethical requirements (Is there a need for authorisations, compliance to standards, norms, etc.?).
- **Involved partners**: Who are the principal partners involved in the delivery of the result?
- **IPR protection**: Does the result need to be protected? How? When?

Table 6: Overview of TRL levels and their descriptions

TRL	Description
TRL 1.	basic principles observed
TRL 2.	technology concept formulated
TRL 3.	experimental proof of concept
TRL 4.	technology validated in lab
TRL 5.	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)

TRL 6.	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7.	system prototype demonstration in operational environment
TRL 8.	system complete and qualified
TRL 9.	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

4.1 Behavioural Intrusion Prevention System

KER 1: Behavioural Intrusion Prevention System	
Description	The BIPS aims to enhance the security posture of the organization by proactively detecting and mitigating potential threats in real-time. It implements data engineering processes on system logs, including collection, pre-processing, as well as pattern recognition and anomaly detection. The latter are realised via AI algorithms trained using supervised and unsupervised models. The outputs of this AI-based component will generate alerts to the SOC analyst, providing details on the anomaly's nature, impact, and mitigation strategies. Those alerts will be used to guide incident response processes, including system isolation, anomaly investigation, and future incident prevention. Finally, continuous learning of BIPS will be implemented by iteratively refining AI models based on new data and incident responses towards improving accuracy and effectiveness in threat detection.
What problem(s) are solved	Overall, the BIPS component plays a crucial role in mitigating cybersecurity risks, protecting sensitive data, and safeguarding the organisation's assets and reputation. Particularly, the following problems are expected to be solved: **Early Insider Threat Detection**: By continuously monitoring network and system behaviour of in-house assets and actors in real-time, the BIPS can identify anomalies and potential threats before they escalate into full-blown security breaches. This approach helps prevent unauthorised access, data breaches, and other cyberattacks. **Enhanced Accuracy**: Using AI-driven algorithms and continuous learning techniques, the BIPS can accurately detect both known and novel threats. By extracting key features from data and training models, the system can distinguish between normal behaviour and suspicious activities, reducing false positives and negatives. **Timely Alerting**: The generation of comprehensive alerts upon detection of anomalies enables security analysts to respond promptly to potential security incidents. These alerts provide detailed information about the nature of the threat, its potential impact, and recommended mitigation strategies, facilitating rapid decision-making and incident response. **Incident Response Improvement**: By guiding incident response processes, including system isolation, anomaly investigation, and future incident prevention, the BIPS component helps streamline the organisation's response to security incidents. This leads

	to quicker resolution times, reduced impact on operations, and improved overall security posture. **Adaptability to Evolving Threats**: Continuous learning mechanisms allow the BIPS to adapt and evolve alongside emerging cybersecurity threats. By iteratively refining AI models based on new data and incident responses, the system can stay ahead of evolving attack techniques and maintain its effectiveness in threat detection over time.
Innovativeness / new approach	A transparent and explainable AI framework for intrusion prevention, analysing the systems' behaviour tailored to the organisation's business activity.
Unique selling point	The AI-enabled behavioural threat detection will timely capture abnormal patterns within the organisation's digital infrastructure, match them with known vulnerabilities and propose tailor-made remedies. In this regard, particularly insider threats will be prevented and/or mitigated.
Competitors (solutions)	In terms of relevant commercial solutions, there are numerous vendors offering products and services in the field of intrusion prevention systems, many of which incorporate behavioural analysis and AI-driven techniques. Some well-known commercial solutions include Cisco Firepower, Palo Alto Networks' Next-Generation Firewall with Threat Prevention, Check Point Intrusion Prevention System, and IBM QRadar. These solutions typically offer a range of features, including real-time monitoring, threat detection, alerting, and incident response capabilities, tailored to meet the security needs of organizations across various industries.
Target users / customers	**SOCs** to proactively identify vulnerabilities before they are exploited by attackers. **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts.
Benefits for users / customers	Higher efficiency for SOC teams and security analysts in terms of events and issues handling; increased visibility of threat landscape; fortification against insider threats
TRL level (1-9)	TRL 4
Main technical challenge(s)	Model training, data availability.

4.2 AI-Powered Penetration Testing Methods and Tools

KER 2: Semi-Automated Penetration Testing Methods and Tools	
Description	*The Semi-Automated penetration testing methods and tools serve two purposes: a) assessing the robustness of the behavioural intrusion prevention system using comprehensive, realistic threat simulations, and b) streamlining the workflow, thereby reducing human intervention, time and costs while increasing test frequency and entry point coverage, by automating critical aspects of penetration testing.*

What problem(s) are solved	*It automates repetitive tasks and augments human capabilities, freeing up pen testers to concentrate on higher-level strategic analysis and decision-making, allowing for faster and more scalable security assessments. It prioritizes vulnerabilities based on their potential impact, optimizing testing efficiency. Simulates and replicates advanced attack techniques, providing a more realistic assessment of an organization's security defences. Provides insights back into the intrusion prevention system for continuous learning and improvement.*
Innovativeness / new approach	*Introducing a new generation of vulnerability assessment by combining intelligent algorithms, automation scripts, and the MITRE Caldera adversary emulation framework. This innovative approach moves beyond static, rule-based scanning to a dynamic, adaptive model that continuously learns from vast streams of security data. Automated workflows accelerate the detection-to-response cycle, while Caldera simulates advanced, multi-stage attack scenarios to expose weaknesses that traditional tools overlook. By uncovering hidden patterns, zero-day threats, and custom malware, this method not only prioritizes the most critical risks but redefines how security testing is conducted.*
Unique selling point	*It introduces automation, intelligent analysis, and continuous adaptation, significantly enhancing the effectiveness and efficiency of cybersecurity efforts. By leveraging machine intelligence we can uncover hidden weaknesses, adapt to new threats, and optimize the testing process for a more secure future. It's a proactive approach that anticipates and adapts to the evolving threat landscape.*
Competitors (solutions)	*Numerous self-hosted platforms that can potentially provide a similar solution like Deepwatch Arc, PenTest (by Rapid7), Nixeus, BreachLock (by Cymulate), AttackIQ, Cymulate. However, they are not easy to extend.* *Research groups that incorporate AI in penetration testing and vulnerability identification.*
Target users / customers	*The module can be used by a) **Penetration Testers** to automate tedious tasks, allowing them to focus on crafting complex attacks, analysing results, and applying their critical thinking and social engineering skills; b) **Security Teams** to gain a more comprehensive vulnerability assessment, identify sophisticated threats, and prioritize risks, allowing them to make informed decisions about resource allocation and remediation efforts; c) **SOCs** to proactively identify vulnerabilities before they are exploited by attackers, giving them a head start in shoring up defences; d) **Compliance and Risk Management Teams** to ensure compliance by identifying vulnerabilities that could lead to data breaches; e) **DevOps Teams** to identify and address security vulnerabilities early in the development lifecycle, resulting in time and resources reduction compared to fixing vulnerabilities discovered later in the production stage; f) **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.*

Benefits for users / customers	*AI-powered penetration testing streamlines the testing process, enhances vulnerability detection, and equips teams with the knowledge to prioritize risks and make data-driven security decisions. Furthermore, it empowers users and customers with a faster, more effective way to identify and address security weaknesses. It's a proactive approach that helps organizations stay ahead of evolving threats and strengthen their overall cybersecurity posture.*
TRL level (1-9)	*TRL-3*
Main technical challenge(s)	*AI can generate both false positives (flagging non-existent vulnerabilities) and false negatives (missing real vulnerabilities), resulting in wasting time and resources investigating non-issues or leaving critical gaps in security. Fine-tuning AI models and incorporating human expertise are crucial to minimize these errors. Additionally, biased or incomplete data sets used to train the models can lead to biased results, potentially overlooking certain attack vectors or vulnerabilities specific to certain systems. Ensuring high-quality, unbiased training data is essential. Finally, ensuring seamless integration, interoperability and data sharing with existing security infrastructure (such as SIEM or IDS/IPS) and workflows is essential for maximizing the effectiveness of AI-driven security assessments.*

4.3 CTI Sharing System

KER 3: CTI Sharing System	
Description	The CTI Sharing System serves two purposes: a) collecting, storing and sharing of structured Cyber Threat Intelligence (CTI), including indicators of compromise (IoCs) and contextual information related to cybersecurity incidents, campaigns, and intrusion sets and b) managing, correlating, visualizing and analysing CTI in a structured and collaborative manner, enhancing the understanding of cyber threats.
What problem(s) are solved	The CTI Sharing System addresses a common problem in the cybersecurity field: limited visibility and information sharing regarding cyber threats, lack of efficient management and sharing of CTI, lack of a standardized and centralized platform for collaborative threat analysis in the dynamic and complex field of cybersecurity.
Innovativeness / new approach	This module uses and enhances: the MISP sharing platform [9], a platform that has several built-in functionalities that can ease the collection, storage, correlation, and sharing of cyber security indicators and threats. Using MISP in a CTI sharing system reflects innovativeness through open collaboration, adherence to standards, centralized management, scalability, automation, community involvement , and a commitment to continuous development. Furthermore, the module introduces new advanced correlation techniques through automated workflows that analyse data from MISP (focusing on IoCs and IoAs) to identify connections between threats and attacker campaigns.

Unique selling point	This solution advances MISP by introducing new advanced correlation techniques with MISP's rich graph layouts to provide a more comprehensive picture of the threat landscape.
Competitors (solutions)	Other CTI gathering tools, such as MISP with its default feeds [14], SpiderFoot [15] that supports the collection of information from various sources including the Dark Web, commercial thread intelligence feeds from different cybersecurity companies, and more. However, our module supports the automatic collection and the extraction of CTI from additional sources compared to our competitors. Other CTI sharing platforms, either open-source or commercial. However, they do not utilise advanced correlation techniques.
Target users / customers	The module can be used by a) **SOC teams** to share and analyse threat indicators (IOCs and IoAs) and attacker Tactics, Techniques, and Procedures (TTPs) to proactively identify and respond to threats; b) **CTI Teams** to gain a comprehensive understanding of the threat landscape (by monitoring and extracting CTI from multiple sources) and produce actionable intelligence; c) **Information Sharing Communities** (ISCs) to facilitate collaboration and information exchange within these communities; d) **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts; e) **Managed Security Service Providers** (MSSPs) to cater to the specific needs of their diverse client base; f) **Security Researchers** to identify new threats and develop better defensive strategies; g) **Law Enforcement Agencies** (LEAs) to share and analyse threat intelligence related to cybercrime investigations. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.
Benefits for users / customers	By combining data from MISP (IoCs, IoAs) users can identify connections between indicators and attacker tactics, providing them with a more comprehensive picture of potential threats (broader threat visibility). Furthermore, by automating data ingestion, enrichment, and correlation we can streamline (by highlighting connections) and automate some aspects of threat analysis reducing manual effort for security analysts while enabling them to focus on more strategic tasks. Finally, enhanced threat visibility allows users to identify potential threats before they cause harm, enabling proactive threat hunting.
TRL level (1-9)	TRL-7
Main technical challenge(s)	Since information sharing within CTI communities can be susceptible to inaccurate or misleading data, mechanisms to assess data quality and trust must be implemented (such as reputation scoring or manual review processes) before feeding it into analysis workflows.

4.4 Dynamic Risk Management Engine

KER 4: Dynamic Risk Management Engine	
Description	The Dynamic Risk Management Engine (DRME) identifies, analyses and assigns threats and vulnerabilities to the infrastructure's assets, aiming to minimise risks with minimal intervention by risk analysts. To accomplish that, DRME will: a) Explore possibilities for automatic asset identification; b) Use an ontology-based knowledge representation to depict the various system services and the assets associated with these services, distinguishing them to composite and basic assets; c) Utilise ML approaches to accurately and automatically correlate identified threats with the Common Weakness Enumeration (CWE) list and other high-level vulnerabilities; d) Help analysts adopt c technical countermeasures based on MITRE ATT&CK and MITRE D3FEND and automatically correlate them with the threats and vulnerabilities associated with the ontology's assets; e) Leverage stochastic approaches and existing relationships between CWEs and CVEs in conjunction with their scoring systems (CWSS and CVSS) towards reliable automated risk predictions regarding the identified cascading threats on assets and their interconnections.
What problem(s) are solved	DRME addresses the issue of cascading threats, over or under estimation of risks for complicated cyberphysical systems due to insufficient threat modelling, and static risk assessments. Introduces an accurate calculation of the composite risk value for complicated cyberphysical systems with correlated and cascading threats; Use of third-party sources and AI tools for zero-day attacks identification and accurate calculation of threat occurrence probabilities; Interconnection with other threat intelligence engines and SIEMs; DRME is adaptable to any sector.
Innovativeness / new approach	DRME proposes hierarchical modelling of multi-layered cyberphysical systems that include multiple assets and users; a new cascading threat and risk estimation engine; new AI-based techniques for risk value recalculation and automated asset identification; a new ontology for risk and threat modelling.
Unique selling point	Accurate, detailed, and dynamic risk modelling and assessment for complicated, multi-asset, multi-layered systems with significantly reduced requirement for deep technical system knowledge by the risk analysts.
Competitors (solutions)	Many risk assessment and analysis solutions exist; however, they generally lack intelligent or dynamic features, and/or they are not provided as open source. The list of solutions includes the following: Riskrecon, UpGuard, Security Scorecard, NormShield, BitSight, Microsoft Security Assessment Tool 4.0, CounterMeasures, EAR / PILAR, eBIOS Risk Manager, MEHARI Expert, Modulo Risk Manager™, Risk Management Studio, SimpleRisk, CORAS, Verinice ISMS, Practical Threat Analysis, Cyber Security Evaluation Tool (CSET), ZenGRC, CIS RAM, vsRisk, OneTrust GRC, MONARC.

Target users / customers	The module can be used by a) **SOC teams** for various technological domains monitoring cyberphysical systems; b) **CTI Teams**; c) **Information Sharing Communities**; d) **Incident Response Teams**; e) **Managed Security Service Providers**; f) **Security Researchers**. Additionally, the module can be used as part of the NG-SOC platform to facilitate the training process of the NG-SOC users.
Benefits for users / customers	DRME is a semi-automated tool that can be exploited by users without deep technical knowledge of the underlying system. It provides accurate risk score calculations considering cascading risks, security controls and risks, and interconnects with third party feeds and applications to ensure dynamic reconfiguration.
TRL level (1-9)	TRL-7
Main technical challenge(s)	The interfacing and interconnection with the SIEM and threat intelligence engines for the recalculation of threat occurrence probabilities and mainly for the identification of zero-day attacks. The integration of the automated asset identification procedures since they may be considered invasive from the perspective of a security officer. The integration with the overall NG-SOC solution.

4.5 Next Generation SIEM

KER 5: Next Generation SIEM	
Description	This KER will implement novel functionalities that are poorly or not at all implemented in current SIEM solutions. The next generation SIEM will offer automation in data collection from different sources within the digital infrastructure. Moreover, data aggregation, correlation and categorisation capabilities are included. Finally, cyber threats' related operations will be implemented, including detection and investigation.
What problem(s) are solved	**Advanced Threat Detection:** Traditional SIEM systems may struggle to detect sophisticated and evolving cyber threats. Next-generation SIEM will leverage advanced analytics, machine learning, and behavioural analysis to identify anomalies and potential security incidents more effectively. **Increased Data Volume and Variety:** With the proliferation of digital assets and the rise of cloud computing, organizations are generating vast amounts of diverse data. Next-generation SIEM will handle large volumes of structured and unstructured data from various sources, including logs, network traffic, endpoint telemetry, OSINT data on cyber threats and vulnerabilities (i.e. MITRE ATT&CK, CVE). **Real-Time Monitoring and Response:** Traditional SIEMs often provide retrospective analysis of security events, which may not be sufficient for detecting and responding to threats in real-time. Next-generation SIEM will offer real-time monitoring capabilities, enabling organizations to detect and respond to security incidents promptly. **Integration with Threat Intelligence:** Next-generation SIEM will integrate with external threat intelligence feeds, via CTI Sharing System, to enrich security event data. By

	correlating internal security events with external threat intelligence, Next Generation SIEM can identify indicators of compromise and emerging threats more effectively. **User and Entity Behaviour Analytics (UEBA):** Next-generation SIEM will incorporate UEBA capabilities to analyse the behaviour of users and entities within the organization's network. By identifying deviations from normal behaviour patterns, these systems can detect insider threats, compromised accounts, and other malicious activities. This is also associated with the Behavioural Intrusion Prevention System KER. **Automation and Orchestration:** By automating repetitive tasks and orchestrating response actions, organizations can improve the efficiency and effectiveness of their security operations. **Compliance and Reporting:** Next-generation SIEM will provide advanced reporting and compliance features to help organizations meet regulatory requirements and industry standards. This component can generate customized reports, conduct forensic analysis, and demonstrate compliance with security policies and regulations.
Innovativeness / new approach	The main innovative aspects of the NG-SOC Next Gen SIEM are its integrations with BIPS and CTI Sharing System. Those integrations offer **advanced threat hunting and investigation tools** that empower security analysts to proactively search for and investigate potential security threats. These tools leverage advanced search capabilities, visualization techniques, and threat intelligence integrations to streamline the threat hunting process. It also improves **UEBA capabilities** by leveraging advanced machine learning algorithms to analyse user and entity behaviour patterns. This will enable more accurate detection of insider threats, compromised accounts, and other anomalous activities. Moreover, autonomous response mechanisms help organizations respond to threats more rapidly and efficiently, reducing the impact of security breaches. Finally, **continuous improvement through self-learning** improves threat detection capabilities, analysing feedback from security incidents, user interactions, and threat intelligence feeds to refine their algorithms and adapt to evolving threats over time.
Unique selling point	The ability to provide advanced threat detection and response capabilities, leveraging advanced analytics, machine learning, behavioural analysis, real-time monitoring, integration with threat intelligence, scalability, flexibility, automation, orchestration, and compliance reporting features. These capabilities help organizations enhance their security posture and effectively defend against a wide range of cyber threats.
Competitors (solutions)	CrowdStrike's Falcon Next Gen SIEM, Stellar Cyber, Gurucul SIEM,
Target users / customers	**SOCs** to proactively identify vulnerabilities before they are exploited by attackers. **Managed Security Service Providers** (MSSPs) to deliver comprehensive security assessments, threat detection, and incident response services to their clients. **Incident Response (IR) Teams** to identify the scope of the incident, implement mitigation strategies, and accelerate remediation efforts.

Benefits for users / customers	Higher efficiency for SOC teams and security analysts in terms of events and issues handling; increased visibility of threat landscape; fortification against insider threats
TRL level (1-9)	TRL 4
Main technical challenge(s)	Interfacing and integration with BIPS; data availability so that the automation features are properly validated.

4.6 Next Generation SOAR

KER 6: Next Generation SOAR	
Description	The next generation SOAR comprises standards based interoperable and modular orchestration and automation components to assist and enhance cybersecurity operations and different operational roles. Our SOAR is based on the CACAO v2 playbooks standard. A Minimum Viable Product (MVP) version of the solution will be open sourced whereas NG-SOC will maintain and commercialise a version with enhanced features such as the sharing component, the Generative AI based import module, and the knowledge management system which allows establishing and monitoring playbook oriented KPIs and searching, indexing, and filtering capabilities.
What problem(s) are solved	Currently SOAR solutions are utilizing proprietary formats for playbooks making them non-shareable and -interoperable across organizational boundaries and solutions. The NG-SOAR allows designing and creating CACAO playbooks in a no-code manner and provides an execution engine in support of automation and orchestration. In addition, our solution will introduce a CACAO-based Generative AI component for importing playbooks traditionally documented in human natural language or graphical non-machine-readable formats, allowing defenders to seamlessly upgrade their playbooks capability while providing a clear path to automation. In addition, defenders will be able to exchange playbooks and create trusted and open sharing communities; a capability highly desired by the cybersecurity community but not yet materialised.
Innovativeness / new approach	Full CACAO-based (distributed) SOAR solution providing both an editor for designing and creating playbooks and an execution engine. A playbooks knowledge management system for advanced analytics, tracking KPIs, indexing, filtering, and searching based on a rich set of metadata. Sharing playbooks capability and integration with CTI. Generative-AI-based CACAO transformer to automatically transform playbooks to CACAO from unstructured sources.
Unique selling point	The cybersecurity industry will swift to standards-based interoperable SOAR since it has been researched and to a certain extent demonstrated through PoCs that they can offer certain benefits compared to existing siloed and proprietary approaches. Benefits include the ability to design and exchange playbooks across organizational boundaries and solutions and coupling them with CTI for threat informed defence. Ultimately, NG-SOC is

	entering this market at a very early stage and has the know-how since consortium partners have been actively involved in developing the CACAO technical standard and demonstrated very early-stage implementations.
Competitors (solutions)	Currently, the industry is developing to a certain extent CACAO compliant solutions but none of the "competitors" provide the full set of features that described above. In fact, the CACAO Roaster[2] that we have open sourced is the first open source and known solution for creating CACAO playbooks to date.
Target users / customers	SOCs, MSSPs, and most operational cybersecurity roles, including, threat hunters, red teams, and IR, compliance, and vulnerability management teams.
Benefits for users / customers	Enhanced cybersecurity by exchanging defensive tradecraft in addition to CTI. Enhanced cybersecurity by enabling orchestration and automation. Fully interoperable product that can seamlessly integrate with any other solution of interest. Efficiency in converting IR processes and proprietary playbooks to machine readable CACAO playbooks. A knowledge management playbooks system to increase the efficiency and effectiveness on the use of playbooks.
TRL level (1-9)	TRL 4
Main technical challenge(s)	Complying fully with the CACAO specification and complexity in integrating with the Collaborative Incident Case Management System which is also based on a standards-based approach.

4.7 Collaborative Incident Case Management System

KER 7: Collaborative Incident Case Management System	
Description	The CICMS is based on the DFIR-IRIS (Digital Forensics and Incident Response – Incident Response Investigation System) which is an open-source platform that centralizes and streamlines digital forensics and incident response operations. It provides a collaborative environment where SOC analysts, incident responders, and forensic investigators can manage incidents, store and correlate evidence such as logs, memory dumps, disk images, and other artifacts, and document every step of the investigation within structured case files. By supporting role-based access control, DFIR-IRIS enables multiple team members to work simultaneously on the same case, while its integration capabilities allow automation of evidence ingestion, enrichment, and reporting. Designed as a central hub for evidence management and case tracking, it helps organizations respond to incidents

[2] https://github.com/opencybersecurityalliance/cacao-roaster

	faster, with greater consistency, and with the detailed documentation necessary for legal, regulatory, or internal review.
What problem(s) are solved	✓ Addresses non-interoperability across systems and components regarding incident representation. ✓ Enables sharing incidents and relevant CTI with different teams and organisations. ✓ Provides the required capacity for teams from different organizations to collaborate in the context of incident resolution and requests for information and takedown.
Innovativeness / new approach	CICMS represents the first incident case management system to natively integrate threat intelligence within case records, enabling enriched context for investigative and response activities. It provides a robust API that allows automatic case creation directly from the NG-SIEM, thereby streamlining incident intake and triage processes. Additionally, CICMS supports real-time indexing of NG-SOAR playbooks, with the capability to execute these playbooks directly from within the system. This integration of intelligence, automation, and orchestration functionality establishes CICMS as a comprehensive platform for managing and accelerating incident response workflows.
Unique selling point	The unique selling point of CICMS lies in its seamless fusion of incident case management, integrated threat intelligence, and automated response capabilities. Unlike traditional systems, CICMS not only embeds enriched threat intelligence directly into case records but also enables automatic case creation via API integration with SIEM platforms, reducing response time from detection to investigation. Its real-time indexing and native execution of NG-SOAR playbooks within the same environment eliminate the need for multiple tools, delivering a unified, intelligence-driven, and automation-enabled incident response solution.
Competitors (solutions)	Existing incident case management systems providers and open-source tools like The Hive.
Target users / customers	SOCs and MSSPs
Benefits for users / customers	Benefiting by enabling collective defence; in this context the ability of defenders within and across organizational boundaries to collaborate and create clusters for incident response. Seamless integration with CTI systems. Integration with SOAR solutions via a tailored API.
Readiness level	TRL 4
Main challenge(s)	Integration with the NG-SOAR platform to be able to correlate automatically the cases with the relevant playbooks and their automated execution.

4.8 Hands-on Educational Platform

KER 8: Hands-on Educational Platform	
Description	A hands-on educational platform that will host multidisciplinary and realistic training sessions and educational programmes in cybersecurity across multiple domains, based on the merged principles of Massive Open Online Course (MOOC) tools and explicit use of cyber ranges as a regular hands-on learning method.
What problem(s) are solved	By integrating cyber ranges and hands-on learning methods, NG-SOC provides immersive experiences in realistic training environments, bridging the skills gap and preparing individuals for real-world cybersecurity challenges. Offering a multidisciplinary curriculum, flexible self-paced learning, and interactive assessments, the platform promotes active, experiential learning while democratizing access to high-quality, practical cybersecurity education, empowering learners from diverse backgrounds to acquire essential cybersecurity skills, meet industry demands, and contribute to global cybersecurity resilience.
Innovativeness / new approach	While both MOOCs and cyber ranges exist independently, the platform combines them and provides a holistic approach to cybersecurity education. This allows learners to gain theoretical knowledge through MOOC modules and then immediately apply it through practical exercises in the cyber range. This cohesive approach reinforces learning and enhances skill development. By integrating collaborative learning features, flexible self-paced learning options, and offering content and exercises across multiple domains, it promotes skill development, fosters community engagement, and democratizes access to quality training resources. This innovative approach not only addresses current challenges in cybersecurity education but also anticipates the evolving needs of the industry, preparing learners to navigate complex cyber threats and contribute effectively to cybersecurity initiatives worldwide.
Unique selling point	The platform's unique selling point lies in its fusion of immersive, hands-on learning experiences with comprehensive, multidisciplinary cybersecurity education. By integrating cyber ranges and practical exercises into its curriculum, the platform offers learners the opportunity to engage in realistic simulated scenarios, enabling them to develop practical skills and problem-solving abilities crucial for success in the cybersecurity field. Additionally, its flexible self-paced learning options, collaborative features, and open-source accessibility not only addresses the skills gap in cybersecurity but also empowers individuals from diverse backgrounds to pursue careers in this rapidly evolving industry.
Competitors (solutions)	Traditional academic programs, online course providers like Coursera, edX and Udemy, cybersecurity training firms such as SANS Institute, dedicated cyber range providers. While traditional academic programs offer structured education, they may lack hands-on experiences. Online course providers offer convenience but may not provide the required depth of practical learning. Cybersecurity training firms offer comprehensive programs

	but at a higher cost. Dedicated cyber range providers focus on immersive experiences but may lack educational content.
Target users / customers	The platform targets a diverse audience including aspiring and current cybersecurity professionals, IT professionals seeking career transitions, academics, educators, security enthusiasts, and organizations looking to enhance their cybersecurity capabilities.
Benefits for users / customers	It empowers users to gain a deeper understanding of cybersecurity, develop practical skills, and stay ahead of the curve in this ever-changing landscape. It offers a flexible, comprehensive, practical, and accessible learning experience that can benefit anyone interested in building a strong foundation in cybersecurity, enhancing their skills, and advancing their careers in this ever-growing field.
TRL level (1-9)	TRL-7
Main technical challenge(s)	Deploy them in a private cloud solution like Openstack

4.9 Cybersecurity Training and Exercise Scenarios

KER 9: Cybersecurity Training and Exercise Scenarios	
Description	To develop the training framework aligned with the vision of NG-SOC - to provide an advanced, hands-on educational platform to guide conversations around cybersecurity workforce skills development that goes beyond policies.
What problem(s) are solved	✓ Understand organisational needs for cybersecurity training based on the merged principles of online education tools and cyber ranges. ✓ Identify training and learning objectives. ✓ Develop an innovative framework for training and evaluation.
Innovativeness / new approach	Offer an innovative training framework, incorporating characteristics such as multidisciplinary, varying levels of difficulty, different training modes, real-world attacks scenarios, individual and team skills.
Unique selling point	An innovative training framework with the abovementioned characteristics, tailored to identified training goals and objectives and delivered via different training delivery methods.
Competitors (solutions)	Existing cybersecurity training platforms
Target users / customers	✓ Beginner level for non-technical users (with no relevance to information Technology) who want to be aware of cybersecurity and the basic concepts behind this.

	✓ Intermediate and advanced level for professionals in a specific domain or experts who are not domain specific.
Benefits for users / customers	✓ Offering theoretic and hands-on offensive/defensive training. ✓ Complex cross-domain/hybrid scenarios jointly built with the IoT domain. ✓ The realistic and dynamic training and exercise scenarios enable cybersecurity professionals to rapidly adapt to the evolving threat landscape.
TRL level (1-9)	TRL 4
Main challenge(s)	Compete with existing cybersecurity training programmes with professional accreditation.
Developing scenarios	Available on GitHub repository: redtrace-kypo (at: https://github.com/NG-SOC-eu/redtrace-kypo). riskmanagement-kypo (at: https://github.com/NG-SOC-eu/riskmanagement-kypo). malwarecontain-kypo (at: https://github.com/NG-SOC-eu/malwarecontain-kypo). incidentresponse-kypo (at: https://github.com/NG-SOC-eu/incidentresponse-kypo).

4.10 Sectorial Training Programs (CYNET-CSIRT)

KER 10: Sectorial Training Programs	
Description	Adaptive and proactive training programmes for research and education. More specifically the training program will incorporate: a) a comprehensive cyber security training plan focused on studying online materials, that covers various aspects of cyber security, assuming beginner to intermediate levels of knowledge, using a scenario-based approach to educate participants on identifying and mitigating phishing threats and b) hands-on training activities designed to enhance participants' skills in ethical hacking, in recognizing and defending against social engineering attacks, with a specific focus on phishing, in handling and mitigating a cybersecurity incident involving automated malware attacks, in developing and implementing effective incident handling and response procedures, and in handling an Advanced Persistent Threat (APT) incident.
What problem(s) are solved	Test participants' ability to recognize and respond to a variety of attacks in a controlled environment, fostering a proactive approach to cybersecurity and improving their ability to i) detect, analyse, and respond to social engineering threats and sophisticated cyberattacks, ii) utilize/leverage automation tools and incident response techniques to detect, contain, eradicate, and recover from an incident, iii) create, refine, and execute incident response plans to mitigate and recover from the incident. Enhance participants' skills in ethical hacking and improve their understanding of security vulnerabilities and countermeasures.

Innovativeness / new approach	Scalable architecture of mostly virtualized components, with some physical equipment for more realistic training experience. Question based training scenario. Proposed approach is scalable for very similar business (i.e., other research and education organisations) and based on best practise
Unique selling point	The unique selling point of the adaptive and proactive training program lies in its combination of theoretical and practical training, focusing on real-world scenarios and current threats. Through scenario-based learning and hands-on activities, learning becomes practical and engaging. Participants of varying expertise levels learn to identify and mitigate phishing threats, handle automated malware attacks, and respond effectively to Advanced Persistent Threats (APTs). The program's focus on proactive defence and comprehensive incident handling equips participants with the skills needed to anticipate and address cybersecurity challenges effectively, making it an invaluable resource for individuals and organizations seeking to enhance their cybersecurity posture.
Competitors (solutions)	Traditional cybersecurity courses offered by universities and online platforms. However, they often lack the adaptive learning element and focus heavily on theory without enough practical exercises. Moreover, the self-paced nature of MOOCs can lead to lower engagement and lack of hands-on activities. Expensive and time-consuming certification programs (like CompTIA Security+ or Certified Ethical Hacker (CEH)) that may prioritize theoretical knowledge over practical application. Affordable security awareness training platforms able to deliver regular awareness training updates, however, focusing primarily on basic awareness, and lacking in-depth training on specific topics like ethical hacking or incident response. Vendor-specific training programs that although beneficial for in-depth knowledge of a specific platform/solution, they lack broader applicability.
Target users / customers	Overall, the program targets a diverse range of users, including individuals seeking to build a strong foundation in cybersecurity, enhance their existing skillset, or gain practical knowledge for their specific roles, professionals advancing their careers, students preparing for future roles, organizations strengthening their defences, and security teams improving their capabilities.
Benefits for users / customers	The cybersecurity training program offers a comprehensive and adaptable approach to educating users at all skill levels, providing practical skills development and theoretical knowledge across various cybersecurity domains. Participants benefit from a tailored learning path, gaining expertise in identifying and mitigating real-world threats such as phishing attacks and malware incidents. This program not only enhances individual career prospects but also strengthens organizational security postures, fostering a culture of cybersecurity awareness and readiness. With its cost-effective and accessible online format, users receive expert guidance and support while enjoying the flexibility to learn at their own pace. Overall, the program

	empowers users with the skills and resources needed to navigate the evolving cybersecurity landscape effectively, making it a valuable investment for both personal and professional growth.
TRL level (1-9)	TRL 4
Main challenge(s)	Complexity of the subject matter, technical requirements for hands-on activities, maintaining participant engagement and retention, addressing skill level disparities among users, addressing limited time or resources of busy professionals, evaluating progress accurately, resource constraints, staying adaptable to emerging threats and attack methods. Overcoming these challenges requires continual updates to content, ensuring accessibility to necessary resources, fostering engagement through innovative methods, and maintaining flexibility to accommodate diverse skill levels and evolving cybersecurity landscapes.

5 Individual Exploitation Plans

This section presents the updated individual exploitation plans of all consortium partners. A similar description has been given in D7.1 but is repeated here for ease of reference. As the project progresses, partners could potentially identify different exploitation opportunities and goals. As such, this reporting activity will also be repeated for D7.3 *Business plan – M36,* where only significant changes with partner's individual exploitation will be incorporated and described. Individual exploitation plans include results that are exploited by partners and which market sector and customer segments they target. Moreover, exploitation channels, expected sales, and current achieved exploitation goals are presented. To assist the partners with the drafting of their individual exploitation plans, the following questions were provided as a guideline:

- **Results to exploit**: Which aspects (technology, services, knowledge, experience, know-how, network, etc.) of NG-SOC do you plan to exploit, and for what purpose?
- **Market Sectors**: Are you / do you plan to collaborate with any local, national, EU, or international sectors? Which stakeholders (research, industry, academia, authorities, decision-makers, etc.) are you connected with? How many people can potentially be reached?
- **Channels/Actions**: Which channels and actions will you use to exploit NG-SOC results?
- **Expected Sales**: How is NG-SOC going to provide an added value for your organisation? (This can include financial gains, gained know-how, development portfolio, widen networks, etc.)

By following the guidelines and answering the proposed questions, the consortium partners created the basis for setting up their exploitation plans of NG-SOC outputs, as identified in this early stage of the project. Each partner defined the major exploitable items and outlined the appropriate business strategy, as shown in the following sections.

5.1 EUROPEAN DYNAMICS LUXEMBOURG SA (01 ED)

European Dynamics (ED) will actively pursue the exploitation of key results and innovations emerging from the NG-SOC project, with a focus on maximizing impact across commercial, educational, and strategic domains. The exploitation strategy is designed to leverage open-source assets, extend service offerings, and build long-term market visibility and partnerships.

Results to exploit:

a) CTI Sharing System Built on MISP ED will enhance and operationalize the threat intelligence sharing system built atop MISP, integrating it into broader cybersecurity offerings. This includes:

- Custom connectors and enrichment pipelines
- Sector-specific threat feeds
- Integration with national CSIRTs and SOCs

b) Open-Source Tools and Frameworks Most NG-SOC components are released as open-source, enabling ED to:

- Reuse and adapt tools for commercial deployments
- Contribute to ongoing development and community engagement

- Package selected modules into tailored solutions for clients

c) Training Programs and Exercises ED will further develop and commercialize the training curricula and simulation environments co-created during the project. These will be offered as:

- **Professional certification courses** in cybersecurity, threat hunting, and SOC operations
- **Custom exercises and red-team scenarios** for clients in banking, healthcare, and public administration
- **Joint training programs** with partners such as CYNET and FUNITEC, leveraging KYPO and RITA integration

- **Value-Added Services & Commercial Opportunities**

ED will expand its portfolio by offering specialized services built around NG-SOC technologies:

- **Cybersecurity Consulting** Advisory services for NIS2 compliance, SOC design, and cyber crisis management.
- **Infrastructure Deployment** Turnkey SOC installations using NG-SOC's modular architecture, including AI-based inspection and monitoring tools.
- **Custom Feature Development** Enhancements to NG-SOC components (e.g., advanced analytics, CACAO playbook automation, sector-specific dashboards).
- **Integration Services** Seamless deployment of NG-SOC tools into existing enterprise environments, including hybrid cloud and sovereign infrastructure.

Market Sectors: NG-SOC tools may find applications in academia, industry stakeholders, law enforcement agencies, European Union agencies, or public organisations where we mainly provide services, or other leading experts in the field of cyber-security technologies. ED will explore individually but also jointly with other project partners and external experts or national authorities the possibility of establishing: a) national, regional, or sectorial SOCs, within and across EU member states that can actively communicate, cooperate, share information, and respond to cyber threats effectively and b) training courses and educational programmes for professionals that are active in the field of cybersecurity.

Channels/Actions: ED will exploit the results of NG-SOC by enlarging its products and services with genuinely needed solutions for cyber security. ED will exploit the project results in three ways: a) will enlarge its technical know-how and services within the cyber security sector with new products and services that are complementary to its own, b) will obtain new and innovative as well as competitive services that can reach public organisations where ED mainly provides services, and c) will expand its alliances with other global players of the consortium in the cyber security market.

Expected Sales: Increased revenues based on gained know-how and strategic alliances with other NG-SOC partners, which will allow us to expand our cyber-security services portfolio.

5.2 INSIGHIO IKE (02 INS)

Results to exploit: INS will pursue the exploitation of the Dynamic Risk Management Engine (DRME), which is co-developed with UPRC and integrated with ED solutions. The three partners will prepare, agree on, and follow

a collaboration agreement for the joint exploitation of the developed tools, while special agreements with NG-SOC partners may be drafted in case of integration of tools and functions from other NG-SOC systems. Moreover, INS is eager to explore the utilization of the developed tools in its systems and its IoT-related use cases/products for proofing and securing their cyber physical system.

Market Sectors: As a company, INS is developing IoT, communications, and automation solutions for various verticals, namely: vehicular communications and connected/autonomous vehicles, industrial automation and robotics, precision agriculture, emergency response and disaster relief, smart cities, smart grids, and more. As a tool, DRME is vertical agnostic and is adaptable to any sector, medium, or large company. Moreover, the solution is usable and exploitable by academia (for research and innovation), authorities and law enforcement agencies, European Union agencies or public organisations, or other leading experts in the field of cyber-security technologies.

Channels/Actions: INS will exploit the project results in the following ways: a) pursue new collaborations and participation in new research and innovation actions; b) enhance its technical expertise in cyber security leading to new products and services; c) establish relations and alliances in the cybersecurity market; d) establish a permanent channel for development and exploitation with the Greek academia (UPRC); e) proceed to commercial exploitation of the solution. Commercial exploitation will be feasible using the freemium model (offering the basic version for free, while charging is applied for premium features and services), using dual licensing (users can choose between open-source and commercial licensing), providing managed hosting or cloud services for the open-source tool, taking care of installation, updates, and maintenance for clients who prefer a hassle-free solution, and offering custom development services based on the open-source tool.

Expected Sales: Increased revenues based on the exploitation of the DRME tool using the aforementioned channels and activities, including direct commercial exploitation, participation in new collaborative projects, utilization of the gained know-how and the newly acquired strategic alliance with the NG-SOC ecosystem.

5.3 University of Piraeus Research Center (03 UPRC)

Results to exploit: UPRC will pursue the exploitation of: a) the Dynamic Risk Management Engine (DRME) that is co-developed with INS and integrated with ED solutions, b) the developed training programs and exercises for the design and implementation of new university courses (under and postgraduate), and seminars (offered as professional-level online training; c) the research outcomes generated during the development, improvement, and optimisation of the risk management system. As far as DRME is concerned, the three involved partners will prepare, agree on, and follow a collaboration agreement for the joint exploitation of the developed tools.

Market Sectors: As a research and academic organization, UPRC focuses on academic channels for the provision of novel and efficient educational and training tools, as well as tools to produce new research and innovation results and algorithms. Simultaneously, UPRC and Security Systems Laboratory members are involved in relevant regulation and law enforcement authorities, where UPRC, through its reliability and prestigious profile, will provide consultancy services. Moreover, for the full exploitation of the DRME potential, UPRC will cooperate with INS utilizing its established industrial channels, while UPRC will investigate the potential of a spin-off company that will pursue industrial-commercial aspects of the solution.

Channels/Actions: UPRC will exploit the project results in the following ways: a) pursue new collaborations and participation in new research and innovation actions; b) enhance its technical expertise in cyber security leading

to new products and services; c) establish relations and alliances in the cybersecurity market; d) utilize the educational and training course and material to improve the curricula for undergraduate and postgraduate courses or develop new courses and professional training solutions; e) exploit the creation of a stable channel with Greek SMEs (INS); f) proceed to commercial exploitation of the solution. As far as the latter point is concerned, UPRC and INS will propose a joint commercialization plan.

Expected Sales: Increased revenues based on the exploitation of the new training programs, the exploitation of the DRME tool using the channels and activities, participation in new collaborative projects, utilization of the gained know-how, and the newly acquired strategic alliance with the NG-SOC ecosystem.

3.1 SPACE HELLAS (04 SPH)

Results to exploit: the KERs to be exploited by SPH are the BIPS and Next Generation SIEM. Stemming from background assets of SPH, the enhancement of those KERs will be pursued. This will happen with their deployment in sectors additional to the military domain, where the initial deployments and validations were performed (i.e., financial via the Caixa Bank pilot). New data pipelines will be explored, new business processes will be considered, and the new SIEM automation features will be leveraged to introduce a scientifically sound and technologically robust solution for a SOC team.

Market Sectors: the main target will be the Greek national SOC. SPH is a member of the EL-SOC project that implements the national SOC and is coordinated by the Greek Ministry of Digital Governance. The existing clientele of the SOC services of SPH comprised of private organisations will also be leveraged. Finally, SPH will enhance its established position in national cyber-defence by improving its current offerings with the NG-SOC outcomes. More specifically, SPH envisions deploying the NG-SOC results to military cyber ranges following national and European initiatives (i.e., CYBER RANGES[3], CapTech Cyber[4]). Finally, selected components of the two KERs will be properly tailored to be included in solutions delivered to LEAs. Such components may be AI-enabled classifiers and feature extraction capabilities that can facilitate LEA investigations that involve high data volumes (i.e., financial corruption cases, cybercrime, etc.).

Channels/Actions: SPH will leverage its existing clientele and business network around SOC services and cyber defence. It will also pursue new alliances in research and commercial contexts, stemming from the NG-SOC consortium and expanding to the EU cybersecurity and cyber defence community (e.g., EDA, DG-HOME, etc.).

Expected Sales: sales from new cybersecurity solutions incorporating the NG-SOC results; new R&D projects where NG-SOC results will be introduced as background assets.

5.4 CYENTIFIC AS (05 CYEN)

Results to exploit: the KERs to be exploited by CYEN is, the NG-SOAR, and the know-how acquired while developing these tools both from a research, standardization, and implementation perspective. This will allow CYEN to increase its product (and service) portfolio by providing trustworthy state-of-the-art tools and enable the SME to be onboarded and collaborate with other European projects. In addition, the pertinent activities in

[3] https://eda.europa.eu/news-and-events/news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

[4] https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

NG-SOC will allow CYEN to become a major player in cybersecurity standardization and a trusted knowledge provider for EU policymaking.

Market Sectors: CYEN collaborates closely with academia and industry within and outside the EU. It is a trusted knowledge hub for cybersecurity information modelling, automation, and standardization activities and a big contributor to open source. Thus, it will use its extensive network, including national security authorities and CSIRTs, critical infrastructure operators, MSSPs, large and small organizations, universities and research institutes, standards-developing organizations, governments, ENISA and other EU cybersecurity-focused stakeholders, and formal cybersecurity communities such as FIRST to raise awareness about the developed tools and their provision.

Channels/Actions: as mentioned above, CYEN has direct contact with governments, national and sectorial CSIRTs, national security authorities, ENISA through the participation in different ad hoc working groups and policymaking groups, standards-developing organizations, and MSSPs and thus will aim to exploit these channels to disseminate NG-SOC results, including the developed tools and know-how. CYEN will proceed to provide demos and consult the stakeholders on how they can address specific use cases and the benefits derived from NG-SOC tools. In addition, CYEN will engage in public and academic talks, and presentations in conferences and workshops and continue supporting standardization while raising awareness about the NG-SOC tools. Finally, CYEN, to attract potential customers, will create a global community around NG-SOC where minimum viable versions of specific tools will become available and maintained as open-source.

Expected Sales: Increased revenues based on the exploitation of the tools, know-how, and the market sectors and channels identified. In addition, it is expected that CYEN will be able to participate in more EU projects as it becomes a major EU knowledge hub and tool provider in the domains of CTI, collective threat defence, automation, and AI.

5.5 CAIXABANK SA (06 CXB)

CXB plans to exploit the pilot and use cases developed in NG-SOC during and beyond the lifespan of the project. The approach for taking profit from the pilot after the project unfolds in two types of Exploitation plans: Internal exploitation plan and External Exploitation plan.

Internal exploitation plan: First, CXB employees from the Digital Security department, CSIRT and SOC plan to evaluate the usage of the tools and models extracted from finance use cases in its day-to-day operations. In a second phase, CXB plans to deploy part of the NG-SOC platform and use cases in its Security Innovation sandbox, an isolated infrastructure designed to evaluate innovative tools' integration into the Digital Security department's day-to-day operations. The deployment of some of those tools in CXB premises, even in a laboratory environment, will allow to refine and align the tools' requirements, to streamline and facilitate eventual integration with CXB systems in production. More concretely, the objective is to undertake an extended evaluation of NG-SOC tools and platform and the use cases in that environment, allowing a higher integration with some of CXB systems and allowing to use realistic confidential data that cannot leave CXB premises. Third, supposing the second evaluation is positive, CXB would integrate NG-SOC platform (as a whole or the specific subset of tools that allows to deploy tested finance use cases) inside the premises of the entity, replicating the resources and security processes tested in the Security Innovation sandbox and defining the governance model of the tool within the entity. That will open the platform to be used by other CXB teams, when necessary.

External exploitation plan: Due to the fact that the use cases related to finance sector explored within NG-SOC address very common problems within the Financial sector, once we can measure the benefits of the set of tools developed and models, CXB can show these benefits outside the Organization, in national and international Security Workgroups CXB is part of and whose members are mostly bank and pairs with the same necessities as CXB. To name some of these Forums and workgroups:

- EPC (European Payments Council)
- ENISA EGFI (ENISA's Experts Group in Financial Sector)
- AEB (Asociación Española de Banca)

5.6 Cyprus Research and Academic Network (07 CYNET)

Results to exploit: Cyprus Research and Academic Network will exploit a) the CTI sharing system that is built on top of MISP, b) the developed training programs and exercises for the design and implementation of new training courses for its members/constituents, and seminars offered to higher management. Furthermore, CYNET will explore possibilities for cooperation with new partnerships at a national, regional and international level.

Market Sectors: CYNETs mission is the provision of an advanced network infrastructure and related innovative networking services, including efficient educational and training tools, to educational and research institutions/organizations, along with the wider promotion of innovative Internet applications with the participation of relevant national and communal research projects and the promotion of national initiatives for the benefit of the Cypriot Educational and Research community.

Channel/Actions: CYNET will exploit the project results in the following ways: a) pursue new collaborations and participation in new research and innovation actions; b) enhance its technical expertise in cyber security leading to new products and services. c) utilize the educational and training course and material to improve the training courses for its members.

Expected Sales: Increased revenues based on the exploitation of the new training programs and future collaborations.

3.2 ELES/INFO

Results to exploit: ELES and INFORMATIKA will jointly exploit the NG-SOC components validated in the energy sector pilot, specifically the Behavioural Intrusion Prevention System (BIPS), the Next Generation SIEM, and the Dynamic Risk Management Engine (DRME). The organisations will also leverage the operational experience, sector-specific threat models, and technical know-how gained through pilot deployment to enhance their cybersecurity offerings and infrastructure protection services for the national and European energy sectors.

Market Sectors: As Slovenia's transmission system operator and an established IT service provider for the energy sector, ELES and INFORMATIKA focus primarily on critical energy infrastructure protection at both national and EU levels. The results will be promoted within Slovenia's energy sector, to other EU grid operators, utilities, and energy stakeholders. Close collaboration with national authorities, regulatory bodies, and energy sector associations will also be pursued.

Channels/Actions: The project results will be exploited by:

- Enhancing ELES's cybersecurity capabilities and operational procedures.

- Offering advanced cybersecurity services to energy operators through INFORMATIKA.
- Contributing to national and European cybersecurity initiatives in the energy sector.
- Engaging with relevant sector associations such as ENTSO-E and EE-ISAC.
- Exploring opportunities for collaboration with Slovenian and EU energy regulators.

Expected Sales: Improved cybersecurity posture for ELES operations, enhanced service offerings from INFORMATIKA to energy sector customers, and strategic positioning as key players in EU energy sector cybersecurity initiatives. Potential revenue increase through consultancy services, operational improvements, and expanded IT service portfolios.

5.7 FUNITEC

Results to exploit: FUNITEC will exploit the hands-on cybersecurity training platform, self-paced educational modules, and research outcomes developed within NG-SOC. These assets will be integrated into FUNITEC's existing academic curriculum (La Salle Campus BCN - Ramon Llull University) and continuing education programs for students and professionals. In addition, FUNITEC will utilise the acquired know-how to strengthen its research capabilities and partnerships in cybersecurity education.

Market Sectors: FUNITEC operates in the higher education sector, providing advanced technical education and training. The NG-SOC outcomes will be used to strengthen cybersecurity education for students, young researchers, and professionals, with a focus on practical, real-world skills development in both academic and industrial contexts.

Channels/Actions: FUNITEC will:

- Integrate NG-SOC results into existing undergraduate and postgraduate courses in cybersecurity and IT.
- Expand professional training offerings for industry stakeholders.
- Explore collaboration with other academic, research, and industry partners in Europe.
- Promote NG-SOC results through academic conferences, workshops, and educational networks.
- Participate in EU-funded projects to further develop and exploit the NG-SOC educational components.

Expected Sales: Increased enrollment in FUNITEC's cybersecurity programs, new partnerships with academic and industry stakeholders, enhanced institutional reputation in cybersecurity education, and potential revenue from professional training and collaboration agreements.

5.8 Partner Exploitation KPIs

To complement the qualitative exploitation plans of individual partners, the consortium has defined measurable KPIs that each organisation will deliver by M36, as presented in Table 7. These ensure alignment with the consortium-wide impact indicators presented in Section 3.6.6.

Table 7: Partner Exploitation KPIs

Partner	Exploitation Focus	KPI (by M36)
European Dynamics (ED)	Lead exploitation and integration of NG-SOC platform; SOC consulting and integration services; exploitation of SOAR/CTI modules; business model coordination.	3 client deployments outside pilots; 2 commercial contracts for integration/consulting; 100 GitHub forks of NG-SOC modules coordinated by ED.
INSIGHIO (INS)	SME-focused SOC-as-a-Service offer; risk management engine exploitation; SME engagement and onboarding.	5 SMEs onboarded into SOC-as-a-Service; 2 commercial SaaS contracts signed; 1 whitepaper on SME adoption.
University of Piraeus Research Center (UPRC)	Academic research exploitation; further development of risk modelling and analytics; contribution to skills/training curricula.	2 scientific publications; 200 students trained in NG-SOC methods; 1 open training module published.
Space Hellas (SPH)	Behavioural Intrusion Prevention System (BIPS) and SIEM exploitation; commercial cybersecurity service extension.	2 commercial deployments of BIPS/NG-SIEM; 1 new SOC service offering integrated into portfolio; 1 patent or proprietary licensing pathway explored.
Cyentific (CYEN)	CTI sharing and SOAR playbook exploitation; open-source contributions; engagement with OASIS CACAO and standardisation.	1 open-source SOAR module released; 3 contributions to OASIS standards; Advancement of the architect tool.
CaixaBank (CXB)	Banking sector pilot; exploitation of NG-SOC modules in finance sector; regulatory alignment (DORA/NIS2).	2 validated banking SOC deployments; internal adoption of NG-SOC modules; dissemination to at least 3 EU banking fora/associations.
CYNET (Cyprus Research & Academic Network)	Academic SOC and CSIRT exploitation; training and awareness in research and education sector; OpenEdX training platform adoption.	350 students/trainees reached; 2 SOC/CSIRT deployments in academic sector; 2 joint training programmes with EU NRENs.

ELES / Informatika (INFO)	Energy SOC pilot; integration of NG-SOC modules in power sector operations; dissemination to EU energy associations; alignment with NIS2/DORA for operators.	2 sectoral SOC deployments in energy domain; 1 exploitation agreement with energy association; 100 operators/engineers trained or engaged.
FUNITEC (La Salle – Ramon Llull University)	Training and cyber range exploitation; commercialisation of educational platform; certification programmes.	200 professionals trained; 2 new certified training programmes launched; 1 joint exploitation agreement with industry for training use.

5.9 Synthesis of Partner Exploitation KPIs

The partner-level KPIs presented in Table 7, provide a granular view of how each consortium member will translate its role into measurable outcomes by M36. By explicitly linking partner-level actions with consortium-level outcomes, NG-SOC ensures traceability from individual commitments to overall project impact. This layered approach also enables more effective monitoring: partners are accountable for their specific KPIs, while the PMO consolidates progress into the overarching business and impact framework. As a result, the consortium can demonstrate both the breadth (number of partners contributing) and depth (market uptake, training reach, regulatory alignment) of NG-SOC's exploitation pathway.

5.10 Dissemination & Communication KPIs (from D7.1)

In D7.1 (Initial Dissemination and Exploitation Plan), the consortium established a set of Key Performance Indicators (KPIs) to monitor dissemination and communication activities. These KPIs remain the baseline framework for tracking visibility and awareness. D7.2 now provides an update on their current status, presented in Table 8. Notably, during the course of the project, the consortium decided to reduce activity on Twitter/X and place greater emphasis on LinkedIn. The main reason is that LinkedIn is a more suitable channel for our objective: attracting professionals in the field of cybersecurity. Through targeted posts and high-value content, LinkedIn enables us to connect with experts, researchers, organisations, and potential end-users of the project results, ensuring greater professional impact compared to more general social media platforms.

Table 8: Dissemination & Communication KPIs (as defined in D7.1, updated in D7.2)

KPI ID	KPI Description	Target (D7.1)	Current Progress (D7.2)
1	Visibility of the public NG-SOC website	Website online by M03	Achieved – NG-SOC website launched on M03 (https://ng-soc.eu)
2	Visibility of the public NG-SOC website	~2000 visitors/year, 900 downloads/year	In progress – Visitor tracking enabled, download tracking pending

3	Number of articles, press releases and journal publications	>10	8 publications delivered: additional in pipeline
4	Number of news items presented on the website and other social media	≥15 per year	Ongoing – More than 30 Initial posts active on LinkedIn
5	Number of presentations (in external events i.e. symposiums, meetings, conferences)	>8	Ongoing – 8 presentations
6	Number of # hashtag used on Twitter	≥1200	Ongoing – Hashtags used in every post: #eu #cybersecurity #dep #ngsoc #technology #information #cybersecurityawareculture #AI #EUCyber – currently 544 hashtags on LinkedIn
7	Number of followers on LinkedIn	≥600	Ongoing – Currently 288 followers
8	Online presence in social media channels such as LinkedIn, Twitter, spreading news about the project	>1000 stakeholders, 200 monthly impressions	In progress – On average, achieved 1,406 impressions/month, exceeded the KPI in 7 out of 13 months
9	Multimedia video podcasts presenting the project, its innovation, and its key outcomes	>3 videos, >2000 views	Planned – not yet released
10	Number of Thematic Workshops Organisation	>3	1 workshop and more planned – under design
11	Number of Cluster of European projects and other initiatives	>5	Planned – engagement with ECSO & ECCC underway
12	E-newsletters	>6 newsletters, >1000 contacts, 30% open rate	In progress
13	Brochures, leaflets, flyers in events, roll-up banners, posters,	>2000 copies, >4 roll-ups	In progress – first materials prepared

	also available online for printing through the project's website		
14	Promotion of periodic non-technical reports (publications) to fora and blogs to create awareness on NG-SOC potential and features	>5 publications to blogs >5 blogs/for a to post	Planned – content pipeline under preparation

These KPIs originate from D7.1 and focus on communication and visibility. They will continue to be monitored across the project lifecycle, with results consolidated in the final D7.3 Business Plan.

6 Intellectual Property Rights (IPR)

Establishment of a proper IPR strategy is an essential requirement for a successful exploitation, high impact and the protection of the identified key exploitable results produced during the NG-SOC project. Therefore, it is important that all NG-SOC consortium partners jointly develop and agree upon a strategy, which will define the collaboration framework as well as commercial or industrial exploitation aspects protected through Intellectual Property Rights. Such an agreement will be formalised within a legal document known as **IPR (Intellectual Property Rights) Agreement**. The IPR Agreement, based on the Consortium Agreement (CA) already signed by all the partners, will provide obligations and rights related to NG-SOC foreground IP (Intellectual Property) ownership and exploitation. As such, it will focus on:

- raising participants' awareness regarding IP issues
- contributing to the resolution of disagreements between participants
- assisting in the drafting of the plan for the use and dissemination of foreground
- tracking down results that should be protected and advise individual partners on the means of protection
- assisting participants in evaluating their contribution to the jointly owned foreground and establishing their respective shares
- decisions regarding third parties joining the consortium with the intention to receive ownership of the Foreground of a specific Party

NG-SOC partners will have several potential options to protect the Intellectual Property they have generated during the project [6]. These can include **trademarks** (exclusive rights over distinctive signs), **patents** (exclusive rights over an invention for a limited period, normally 20 years), **copyright** (rights over literary, scientific and artistic works, computer programs, and database structure), **trade secrets** (valuable information on technology or on any other business aspect), etc. Furthermore, the exploitable foreground of the NG-SOC project could be categorised in the following 3 main groups:

For further research (e.g., architecture module designs, algorithms, parts of software applications…)

For creating and commercializing marketable products (e.g., application, tool, component, simulation hardware…) or **services** (e.g., cybersecurity situational awareness, coordinated incident handling/response, cybersecurity training, consultancy, NG-SOC technical support, etc.)

For creating and providing a service for others:

- Joint exploitation of the NG-SOC solution developed under the project, based on the joint ownership terms and conditions.
- Individual exploitation of the individual contributions of the parties in the NG-SOC solution developed under the project.

This deliverable presents the updated identification of new intellectual property generated within NG-SOC. At this stage, the partners have assessed potential foreground technologies and know-how, but no final decisions have yet been made regarding the most appropriate protection strategies. The consortium is currently evaluating options such as open-source licensing, patenting, or joint ownership models, in alignment with the project's

exploitation routes. The optimal route for protecting foreground IP will be consolidated during the next project phase, and finalised results will be reported in D7.3 – Final Business Plan (M36).

Here, as previously stated, the basis has been initially setup in the NG-SOC Consortium Agreement, where among other, several relevant sections related to the management of IPR as well as ownership, transfer of results and exploitation rights are defined:

Ownership of Results (Section 8.1 of the CA): There are rules in place that handle the ownership of results, where results are owned by the party that generates them.

Joint Ownership of Results (Section 8.2 of the CA): In the case of joint ownership of results it is covered by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results, managing the legal aspects of the exploitation and protection of the IPR.

Transfer of Results (Section 8.3 of the CA): Each party may transfer ownership of its own results following the procedures of the GA Article 16.4 and its Annex 5, Section Transfer and licensing of results, sub-section "Transfer of ownership.

Access Rights to Results for Exploitation (Section 9.4 of the CA):

- Access Rights to Results if Needed for Exploitation of a Party's own Results shall be granted on Fair and Reasonable conditions.
- Access rights to Results for internal research and for teaching activities shall be granted on a royalty free basis.

6.1 Background Technologies / Know-How

Background as defined on The European Participant Portal glossary [1]:

"Any data, know-how and/or information, whatever its form or nature (tangible or intangible) including any rights such as intellectual property rights which are needed to carry out the project or exploit its results".

Table 9 shows all background technologies and know-how that the consortium partners have used for the implementation of the NG-SOC project, with particular emphasis on the associated Intellectual Property Rights, as identified in the Consortium Agreement.

Table 9: IPR Ownership of Background Technologies and Know How used

Background Technology / Know-How	IPR Ownership
Risk analysis and impact assessment engine (RITA)	ED (100%)
Risk Modelling Tool (RMT)	UPRC, INS (100%)
Features from PANDORA components: cyber threat intelligence; network anomaly detection; rule-based threat mitigation; SIEM environment and relevant UI components; OSINT services considering MISP, MITRE ATT&CK, Lockheed Martin Cyber Kill Chain etc	SPH (100%)
ML models for events classification and reduction of false positives	SPH (100%)
CYENTIFIC CACAO Editor	CYEN (100%)

CYENTIFIC Playbook Management System	CYEN (100%)

6.2 Foreground Technologies / Know-How

Foreground as defined on The European Participant Portal glossary [1]:

"*Any tangible or intangible output of the action (such as data, knowledge and information, whatever their form or nature, whether or not they can be protected), which are generated in the action, as well as any attached rights, including intellectual property rights*".

Table 10 shows preliminary information regarding IPR ownership of the NG-SOC outcomes. This information should be considered as an initial identification since it will be updated and finalised towards the end of the project. IPR ownership is based on the development of relevant outcomes by specific partners, during the development of the project.

Table 10: IPR Ownership of Foreground Technologies and Know How

Partner	No.	Project Outcome
ED	1	AI-powered Penetration Testing Methods and Tools
	2	CTI Sharing System
	3	Part of the Dynamic Risk Management Engine contributed by ED
	4	Hands-On Educational Platform
	5	Cybersecurity training and exercise scenarios
	6	Cybersecurity market analysis and landscape mapping
	7	Exploitation strategy
INS	1	Part of the Dynamic Risk Management Engine contributed by INS
	2	Part of the threat landscape and domain modelling relevant to the NG-SOC project, contributed by INS
	3	Part of the strategy for skills development of cybersecurity professionals, contributed by INS
UPRC	1	Part of the Dynamic Risk Management Engine contributed by UPRC
	2	Part of the threat landscape and domain modelling relevant to the NG-SOC project, contributed by UPRC
	3	Part of the strategy for skills development of cybersecurity professionals, contributed by UPRC
SPH	1	Behavioural Intrusion Prevention System
	2	Next Generation SIEM
	3	Part of the AI-powered Penetration Testing Methods and Tools contributed by SPH

CYEN	1	Part of the CTI Sharing System contributed by CYEN
	2	Part of the Next generation SOAR contributed by CYEN
CXB	1	Banking domain modelling
	2	Risk Assessment models in banking domain
	3	Caixa Bank Risk Register
CYNET	1	CYNET-CSIRT training use cases
	2	Training material that is provided by CYNET-CSIRT
ELES/INFO	1	ELES/INFO use cases
FUNITEC	1	Cybersecurity trainings and hands-on exercises (cyber range scenarios)
	2	Syllabus of the training materials designed

The consortium has agreed that baseline NG-SOC components (SIEM-core, SOAR, CICMS, CTI) will be released under the Apache 2.0 license to maximise adoption. Advanced modules (e.g., CACAO-based SOAR enhancements, training scenario packages, NG-SOC SIEM[5]) will be offered under dual licensing: open-source baseline plus commercial extensions. This model balances openness with sustainability, avoiding vendor lock-in while enabling revenue streams.

[5] A reduced version of the SIEM, namely without the AI-models developed for the project end-users is referred to us 'SIEM-core'

7 Standardisation Activities

As part of its strategic objective to ensure interoperability, sustainability, and alignment with broader European cybersecurity efforts, **NG-SOC** has actively engaged with key international standardization bodies and community-driven initiatives. The project recognizes that adherence to open standards is crucial for enabling seamless information sharing, automating response actions, and integrating with existing and future cybersecurity ecosystems. During the reporting period, NG-SOC focused on aligning its technical developments with ongoing work in standards such as **CACAO, STIX, and TAXII**, while also participating in knowledge exchange through collaborative forums, including the **Open Cybersecurity Alliance (OCA)** and **FIRST Special Interest Groups**. This section outlines the progress made in these engagements and highlights the impact of standardization activities on the design and implementation of the NG-SOC platform.

OASIS CACAO TC[6]

The Collaborative Automated Course of Action Operations (CACAO) Technical Committee defines a standardized, vendor-agnostic, machine-readable playbook schema and taxonomy. Throughout the reporting period, NG-SOC has actively participated in the development and refinement of CACAO. CACAO is adopted within NG-SOC as the foundation for encoding and sharing executable playbooks, supporting internal orchestration logic and cross-organizational collaboration. Notably, NG-SOC makes a significant contribution to the evolution of the CACAO standard through its consortium partner, CYEN, which holds co-chair and secretary roles in the committee. Leveraging feedback from NG-SOC use cases and pilot activities, the CACAO specification is undergoing a major upgrade v3[7], aimed at strengthening its operational robustness and interoperability.

OASIS CTI TC[8]

NG-SOC leverages the STIX and TAXII standards developed by the OASIS CTI TC to represent and exchange structured threat intelligence. In selected use cases, NG-SOC has extended STIX objects to better model threats relevant to critical infrastructures covered under NIS2 (banking, energy, academia).

OASIS TAC TC[9]

The Threat Actor Context (TAC) TC develops an ontology to enrich CTI with context-aware semantics. NG-SOC has integrated TAC concepts into its CTI Sharing System and Graph-based knowledge layer, enabling enhanced reasoning and cross-source correlation. CYEN has contributed to proof-of-concept implementations of agentic workflows for CTI extraction from prose reports, storing results in a GraphRAG to support complex, low-hallucination queries.

Open Cybersecurity Alliance (OCA)[10]

NG-SOC strengthened collaboration with the OCA by contributing to Playbook Architect, the next-generation version of the CACAO Roaster tool by CYEN. NG-SOC partners enhanced the application with new capabilities for

[6] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=b75cccb8-adc6-4de5-8b99-018dc7d322b6

[7] https://docs.google.com/document/d/17BvgyEhoXK78lQ4P-vX9FD54vTbskOrcm8UEnfCiEIg/edit?tab=t.79bxgnyg46d

[8] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=c6c33da0-d1ee-42dd-9427-018dc7d32277

[9] https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=33f0d182-232a-4c56-aba6-018dc7d3f415

[10] https://opencybersecurityalliance.org/

creating, parsing, validating, visualizing, and executing CACAO playbooks. These enhancements were merged into OCA's official repositories, further supporting adoption of open cybersecurity standards across the community.

FIRST CTI SIG[11] and FIRST Automation SIG[12]

NG-SOC has actively participated in discussions hosted by FIRST's CTI and Automation Special Interest Groups. These forums provided insights into current best practices and emerging trends in threat intelligence representation and response automation. NG-SOC partners have also contributed updates on the project's adoption of open standards and interoperability practices, ensuring alignment with the global incident response community.

[11] https://www.first.org/global/sigs/cti/

[12] https://www.first.org/global/sigs/automation/

Conclusion

This deliverable has presented the first iteration of the NG-SOC Business Plan, building upon the initial exploitation and dissemination strategy defined in D7.1. It has outlined the exploitation framework, updated market analysis, and partner-specific plans, while also identifying risks, sustainability measures, and preliminary KPIs to monitor progress.

A key development since the project's initiation has been the enlargement of the consortium with ELES/INFO and FUNITEC, which has significantly strengthened the project's coverage. The addition of ELES/INFO as leader of the energy pilot broadens the applicability of NG-SOC to another highly critical sector, while FUNITEC brings dedicated expertise in training, education, and skills development, ensuring that the platform's impact will extend to workforce capacity building and long-term knowledge transfer.

The business plan presented here is not static but a living document. As the project matures and further results are validated through the pilots, exploitation activities will be refined, IPR strategies consolidated, and commercial pathways clarified. These updates will be captured in D7.3 – Final Business Plan (M36), which will integrate final market positioning, joint exploitation agreements, and Horizon Results Booster outcomes.

Through this iterative process, NG-SOC aims to ensure that its exploitable results not only achieve technical excellence but also deliver sustainable impact across critical sectors, supporting Europe's resilience and sovereignty in cybersecurity.

References

[1] **European Commission. (2025).** "Glossary of the Funding and Tenders Portal - European Union" https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/glossary (accessed Aug. 26, 2025).

[2] **European Commission. (2023).** NIS2 Directive: securing network and information systems. Shaping Europe's Digital Future.

[3] **European Commission (2023)** *Proposal for a Regulation of the European Parliament and of the Council on the establishment of the Cyber Solidarity Act*. COM(2023) 209 final. Available at: https://eur-lex.europa.eu

[4] **European Union (2022)** *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, L333/80. Available at: https://eur-lex.europa.eu

[5] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed Aug. 26, 2025).

[6] **Hessel, S., & Schneider, M. (2025).** The NIS2 Directive: a new era of cybersecurity regulation in the European Union. International Bar Association. https://www.ibanet.org/NIS-2-Directive-EU-cybersecurity (accessed Aug. 26, 2025).

[7] **(ISC)². (2025, January 16).** EU Cyber Solidarity Act – What You Need to Know. (ISC)² Insights. https://www.isc2.org/Insights/2025/01/EU-Cyber-Solidarity-Act (accessed Aug. 26, 2025).

[8] **ENISA (2023)** *Best Practices for Cyber Crisis Management*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications

[9] **European Union Agency for Cybersecurity (ENISA). (2023).** ENISA Threat Landscape 2023. ENISA Report.

[10] **Grand View Research (2025)** *Europe Cyber Security Market Size & Outlook, 2024–2030*. Available at: https://www.grandviewresearch.com/industry-analysis/europe-cybersecurity-market

[11] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed Aug. 26, 2025).

[12] **Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., & Kim, H. (2024).** Sharing cyber threat intelligence: Does it really help? In Proceedings of the Network and Distributed System Security Symposium (NDSS) 2024.

[13] https://www.ndss-symposium.org/ndss-paper/sharing-cyber-threat-intelligence-does-it-really-help/ (accessed Aug. 26, 2025).

[14] **Vargas, J. (2023, April 7).** Standardizing cybersecurity: The need for interoperability. Solutions Review. https://solutionsreview.com/network-monitoring/standardizing-cybersecurity-the-need-for-interoperability (accessed Aug. 26, 2025).

[15] **Wiz Experts Team. (2025, February 4).** 10 open-source SOC tools. Wiz Academy Blog. https://www.wiz.io/academy/open-source-soc-tools (accessed Aug. 26, 2025).

[16] **Glas, M., Messmann, G., & Pernul, G. (2024).** Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises. Computers & Security, 144, 103965.

[17] **Grand View Research (2025)** *Europe Cyber Security Market Size & Outlook, 2024–2030*. Available at: https://www.grandviewresearch.com/industry-analysis/europe-cybersecurity-market

[18] https://doi.org/10.1016/j.cose.2024.103965 (accessed Aug. 26, 2025).

[19] **Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K., & Khater, H. M. (2025).** Empowering Security Operation Center with Artificial Intelligence and Machine Learning—A Systematic Literature Review. IEEE Access.

[20] https://doi.org/10.1109/ACCESS.2025.3532951 (accessed Aug. 26, 2025).

[21] **Rebuffi, L. (2024).** Cybersecurity Market Analysis and Recommendations (Version 1.1). European Cyber Security Organisation (ECSO).

[22] **OECD (2024)** *Building a Skilled Cyber Security Workforce in Europe*. Organisation for Economic Co-operation and Development. Available at: https://www.oecd.org.

[23] https://ecs-org.eu/publications/ecso-cybersecurity-market-analysis-and-recommendations (accessed Aug. 26, 2025).

[24] **Source Group International (2025)** *A Forensic Analysis of the Cyber Skills Gap in Europe*. Available at: https://www.sourcegroupinternational.com/insights/cyber-skills-gap-europe

[25] **Crowley, C., Filkins, B., & Pescatore, J. (2023).** 2023 SANS SOC Survey. SANS Institute White Paper.

[26] https://www.claranet.com/de/assets/misc-sans-2023-soc-survey.pdf (accessed Aug. 26, 2025).

[27] **Car, P. (2025, July 11).** Cyber Solidarity Act [EU Legislation in Progress] (3rd edition). European Parliamentary Research Service.

[28] https://epthinktank.eu/2025/07/11/cyber-solidarity-act-eu-legislation-in-progress/ (accessed Aug. 26, 2025).

NGSOC

Next Generation Security Operations Centres

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874