Cyber Security for Europe

Work Package Descriptions (with contact details)

Document Identification	
Date	6 January 2020
Version	1.0

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Table of Contents

Work package 1 – Project Management and Coordination

Contact: Kai Rannenberg (cybersec4europe@m-chair.de)

WP1 takes care of the administrative, financial, technical and quality management of the project; ensuring that the project achieves its commitments on schedule and within budget. It will coordinate the efforts of the consortium using the governance models developed where possible and establish the means of cooperation and communication among the participants. The Project Coordinator (PC) leads this WP and is the formal contact with the EC Project Officer.

Objectives

- **[Obj. 1.1]** Perform and maintain an efficient overall project government and set up and maintain the communication, control and reporting infrastructure.
- **[Obj. 1.2]** Monitor and report development tasks and resource usage, risks, identify deviations and propose corrective action when needed.
- **[Obj. 1.3]** Perform administrative coordination incl. financial reporting supervision and funding distribution
- **[Obj. 1.4]** Provide the scientific and technical coordination of the project.
- **[Obj. 1.5]** Assure the required quality standard of the project activities and results.

Description of work

Task 1.1 Overall Project Management [M01-M42]

This task will carry out overall project management as described in Section 3.2.

Outcomes: Progress reports, management procedures, risk assessment and plans (D1.1, D1.3, D1.4, D1.5).

Task 1.2 Scientific and Technical Management [M01-M42]

This task will assess and report the scientific relevance and excellence of the project research lines and results. The following activities will be performed:

- Ensure the scientific excellence of the project and the trialling of the governance models.
- Drive the scientific and technical activity coordinating relevant discussion among participants, ensuring consistency and complementarity of development and settling conflicts using the governance model where possible.

Outcomes: Technical and scientific progress report and assessment (D1.3, D1.4, D1.5).

Task 1.3 Quality Assurance [M01-M42]

This task will be responsible for the overall Quality Assurance of the project as described in Section 3.2.3.

Outcomes: Quality assurance and Project Quality Plan (D1.2).

Deliverables

D1.1 Project Handbook [M01] details project management and reporting procedures.

D1.2 Quality Assurance Plan [M02] describes the quality system and procedures.

D1.3 First Periodic Report [M14] provides a management report for project review.

D1.4 Second Periodic Report [M28] provides a management report for project review.

D1.5 Final Report [M42] summarizes the project results.

Work package 2 – Governance Design and Pilot

Contact: Tobias Fiebig (T.Fiebig@tudelft.nl)

Description of work

WP2 will design the governance model for the future "Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre" (NCCC) by combining two inputs: requirements, empirical best practices. WP2 collects each of these inputs, bring them together in an integration phase and then implement and validate them in a pilot. Stakeholders input (T2.1) input will be instrumental from T2.2 to build a V1.0 Governance model (D2.1). The V1.0 model will be validated in T2.3 and T2.4, leading to D2.2. This input will then be broadened to larger and possibly complementary or conflicting visions of the stakeholders identified from the pilots (T2.4) and will be instrumental to build the V2.0 Governance model (D2.3).

Task 2.1 Stakeholders Viewpoints [M01-M24] Requirements for the NCCC will be elicited from key stakeholders at different phases by qualitative research methods (e.g. semi structured, "grand tour" interviews, etc.) in close alignment with the community activities of WP10, the demonstration cases in WP5, the educational cases of WP6, and the design and validation tasks of WP2. In the first round we will consider the input of key players for the demonstration cases, education and research activities of the project. This task will also look at the "concept validation" by those very stakeholders involved into the piloting of the first governance model.

Task 2.2 Assessing Best Governance Practices [M01-M24] We will identify current best practices via quantitative methods, leveraging different data sources, such as academic publications, patents, LinkedIn, interviews and site visits. The results will be included in D2.1, D2.2 & D2.3. We will look for best practices around five research activities that help to scale up research for the benefit of the Digital Single Market:

A: Aligning research & teaching competencies across institutions, due date M6. To fight the current fragmentation of research competencies across many institutions, we will study successful forms of alignment across multiple institutions and boundaries. We do this by building and analysing research publications in the highest, most competitive scientific venues.

B: Data sharing between academic research and industry, due date M12. Breakthroughs in security research are often tied to the availability of valuable data. This makes data sharing a key driver for increasing the impact and value of research for the Digital Single Market. Data sharing is valuable in both directions, from researchers to firms and vv.

C: Researching new solutions for securing products and services, due date M17. Research can benefit the European market by developing new solutions for improving the security of products and services. Finding best practices around transitioning scientific solutions towards commercial adoption will be undertaken by looking at patent data, but also by looking at social network data (e.g., LinkedIn), and the careers of alumni of the universities etc.

D: Researching new solutions for security products, due date M22. Innovative research can also give rise to new security services. In fact, some companies are direct spin-offs from security groups at EU universities. Using market data on the EU cybersecurity market, and complementing this with social

network data, we will identify a range of companies that have taken an innovation in security research and brought it to market.

E: *Capability Building of cybersecurity competences across institution*. Since one of the major end-results of the CyberSecurity4Eurpe project is a governance model for a future NCCC the final activity of T2.2 consists of liaising with related projects in the SU-ICT-03-2018 call and with the commission to collect and prepare operational data necessary for the implementation of the NCCC.

Task 2.3 Governance Structure Design [M01-M24] Core design choices will be explored in workshops, where we present different possible designs and assess their strengths and weaknesses. Potential legal structures, fitting into the existing European and/or national legal framework will be investigated. This task will develop two versions of the governance structure: V1.0 at M12, and V2.0 at M24. By M6, WP6.3 will provide a "MOOC" case to WP2, which is the identification of the top ten topic channels and the quality assurance process for MOOC to be branded a CyberSec4EU MOOC. Also by M6, T2.3 will establish a specific governance process for the MOOC case: i) a decision process for the selection of MOOC channels, and ii) a decision process for the quality criteria for MOOCs.

Task 2.4 Operation and Testing of the Governance Structure [M01-M36] Governance model V1.0 as described in D2.1 will be validated by applying the model to a number of demonstration cases of WP5 and education cases of WP6. WP5 & WP6 will be responsible for implementing the decision processes and policies proposed by the governance model but WP2 will be responsible for the assessment of the proposals. The results of the analysis will be laid down in D2.2. Similarly, governance model V2.0 as described in D2.3 will be partially validated on a selection of cases from WP5 and WP6. The validation results will be included in D2.3. By M6, T2.4 will develop a validation process for the MOOC case mentioned under T2.3. The validation process will be executed and the results will be included by M12 in D2.1.

Task 2.5 Preparation for the future Cybersecurity Competence Network [M30-M42] This task will contribute to the actual set-up of the NCCC by the European commission. Combining efforts from WP10, other tasks in WP2, WP3, and results from WP5 and WP6, this task will build a roadmap for the set-up of the NCCC. The roadmap is in effect V3.0 of the governance structure. The best in class concepts from all SU-ICT-03 projects will be combined into different options to be included in the roadmap as well (WP10 concertation). Benchmarking and measurement against results will be used to determine key success factors for the governance model. The task is also focused upon the preparatory efforts for the next steps in the process to set up the NCCC after the completion of this project.

Deliverables

D2.1: Governance structure 1 [M12] report describing governance model 1.0
D2.2: Internal validation of governance structure [M24] of demonstration cases / educational cases
D2.3: Governance structure 2 [M24] revised version of governance model 1.0
D2.4: Roadmap for the Set-Up of the NCCC [M42] A report describing how governance model 2.0 compares to related models developed by other SU-ICT-03 projects.

Work package 3 – Blueprint Design and Common Research

Contact: Antonio Skarmeta (skarmeta@um.es)

Objectives

- **[Obj. 3.1]** Definition of a common set of technology and methodologies for cybersecurity that will enable the building of a whole set of cybersecurity services and components
- **[Obj. 3.2]** Innovative research in the main research topics of cybersecurity providing and supplying of European products and solutions adapted to different sectors' needs, as well as with a sufficient level of trust among market players.
- **[Obj. 3.3]** Reach an interdisciplinary cybersecurity know-how for developing a next-generation digital technologies to support innovative products and services.
- **[Obj. 3.4]** Continuous scouting on advanced an relevant new techniques and research contributions to identify innovative approaches

WP3 is responsible for definition of common research, development and innovation in next generation cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies and cybersecurity in critical sectors (e.g. energy, transport, health, finance). WP3 will provide the common research support for the different WPs especially coordinated with WP4 and WP5 to connect the research and innovation with the demonstration and industrial sector to be covered. The WP will create synergies between experts from various cybersecurity domains, providing a mass of researchers and results strengthening its scientific and technological bases by achieving a European research area of cybersecurity. WP3 will run aligned with the two cycles design of CyberSec4Europe providing a first result to be used on the first deployment of WP5 and feedback providing an enhancement on its outcomes.

Task 3.1 Common Framework Design [M03-M28]

This task addresses the project lifecycle and how the activities, results and community built and gathered by the project compose into an overall CyberSec4Europe ecosystem of cyber-security development. The working technical space of this task is in structuring progress and features to emerge as components of the developed systems. These activities are to be distributed throughout the project as timely efforts, diverse disciplines and results rendered and formulated by the initiatives of the community engaged via CyberSec4Europe. The task aim to assess the level of originality, detail, sustainability and conformity of the models and results towards the CyberSec4Europe vision, providing a common ground for their development. Hence, this task will formulate the realistic progress of the project, impact potential, define the feedback for the project activities and communicate and organise the progress behind the building blocks of the CyberSec4Europe ecosystem.

Outcomes: Technical and scientific coordination of the common framework (D3.1, M9, and D3.12, M28).

Task 3.2 Research and Integration on Cybersecurity Enablers and underlying Technologies [M03-M36]

This task will oversee the identification of the horizontal cross sectoral security and privacy enablers, the design of the operational technological components and the identification and research on common technologies like blockchain, identity management, PET and the advance over state of art. The main objective is to develop core innovative cybersecurity building blocks for the CyberSec4Europe project, providing pioneering technologies on top of innovative tools to enhance the security and privacy of services. This task also includes identity management and authentication solutions over multiple non-federated providers, security and privacy services to deploy a basic Edge Computing platform, identify technologies to reduce the system attack surface, design security mechanisms based on Trusted Execution Environments (TEE) and design a framework for TEE-based cloud data processing, IoT Privacy Preserving Middleware Platform, improve integrated Security & Privacy by Design approaches,

decentralized evidence-based authorization and distributed access control using blockchain, addressing applications in IoT and investigate approaches that achieve extreme privacy- and integrity-preserving storage and processing of critical data with long-term protection requirements.

Outcomes: Cross sectoral cybersecurity building blocks release (D3.2, M11), Definition of Privacy by Design, Privacy Preserving enablers (D3.11, M20), Updated version of enablers and components (D3.13, M30), Final cybersecurity enablers and underlying technologies components (D3.20, M36)

Task 3.3 SDL – Software Development Lifecycle [M03-M32]

This task aims at identifying research challenges, requirements and approaches in all stages of the lifecycle of software: early stages (security requirements, modelling and analysis, security design patterns); risk analysis and management (including tool support and empirical methodologies to validate the efficacy in practice); implementation (programming and code, testing and tool support); and deployment (configuration, operations, monitoring). The task will focus on secure-by-design and proactive methodologies, supported by (semi)automated tools reduce security vulnerabilities and risks, and paving the way to the reactive security solutions used in late stages. We will also consider certification of security products to cope with the dynamicity of security. We will further focus on the issue of the software supply chain and identify screening methods (and tools) to identify vulnerabilities in previous versions of industry deployment of open source software. Special focus will be put on software components for the enablers of Task 3.2, namely software for improved privacy and trust in pervasive infrastructures and technologies such as the IoT, cloud and fog, edge.

Outcomes: Research challenges and requirements for secure software development (D3.9, M14), Proactive approaches for secure software development (D3.15, M32).

Task 3.4 Security Intelligence [M03-M30]

We will enhance the state of the art for reliability, safety and privacy guarantees of security intelligence techniques based on artificial intelligence, machine learning and data analytics. The objective is to define the requirements and mechanisms to share digital evidence between the different expert systems, providing solutions to allow interoperability, either through the unification of languages, formats and interfaces, or through trusted intermediate translators systems respecting the privacy, business requirements and the regulations of the different countries. We will investigate mechanisms capable of interacting with Threat Intelligence Information Services to capture evidence of malware activity at early stages. We will also address research challenges on log and event management, threat detection and security analytics with privacy-respecting big-data analytics. Additionally the goal is to enable security intelligence in defensive systems, by making sure the underpinning intelligence systems are fortified.

Outcomes: Research challenges to manage digital evidence (D3.3, M12), Cooperation and interaction with Threat Intelligence Services for deploying adaptive honeypots. Proof-of-concept implementation (D3.14, M30).

Task 3.5 Adaptive Security [M03-M36]

This task will explore the development of flexible security solutions that can quickly adapt security controls in response to security changes such as new attacks or changes in security requirements. To improve the modelling and analysis of dynamic systems, we will provide tools and techniques to support elicitation and representation of assets, security requirements and threats, focusing on interconnected systems in various domains (e.g., cloud systems and Internet of Things). This task will also provide scalable architectures supporting security situation computation and risk assessment, and also selection and deployment of security controls that could satisfy security requirements and policies, also enabling awareness of the current system status. Finally, the acceptance of adaptive systems by stakeholders will be addressed developing techniques to provide explanations (assurances) about why certain security controls should be adapted.

Outcomes: Analysis of research challenges for adaptive security (D3.4, M12). Framework to design and implement adaptive security systems (D3.21, M36).

Task 3.6 Usable Security (Human-centred Cybersecurity) [M03-M32]

This task formulates and develops recommendations and guidelines on how to incorporate usability requirements in security design, as well as a tool-supported method for assessing the effectiveness factor of usability. We will specify a unified validation framework to test both usability and security requirements of biometric-based and multimodal user authentication mechanisms and we will design of new behavioural-based user authentication mechanisms including countermeasures and defences against attackers, validated through some of the demonstration cases. The task will also provide users and administrators with awareness mechanisms to support visualisation of the system status and security risks, enabling effective and usable security controls. Key challenges include automation and AI to help users on their security and privacy decisions, secure and usable authentication, complexity assessment for new security policies, user informed consent on privacy policies and best ways to visualise security and privacy information.

Outcomes: Usable security & privacy methods and recommendations (D3.5, M12); Usability requirements validation (D3.7, M13); Security requirements and risks conceptualization (D3.16, M32); Integration to demonstration cases (D3.17, M32)

Task 3.7 Regulatory Sources for citizen-friendly Goals [M03-M34]

With the intent to drive innovation, the goal of the task includes the design of best practices for innovative and GDPR compliant user experience (Task 3.6) and the investigation of the compliance for identity technologies interoperability (e.g. eIDAS, GDPR, ePrivacy). We will also investigate legitimacy of technologies used and processing of personal data in cross-border and cross-sector dimensions and contribute to the design of a common "blueprint", making reference to other regulations relevant for the market. Dynamically changing environments will lead to the investigation of compliance issues of personal data processing purpose limitation (Task 3.5). An adequate development methodology can address those issues, so the investigation of compliance of proposed software development lifecycle (SDL) methods with EU regulation in light of privacy by design (Task 3.3) and privacy by default requirements is required.

Outcomes: Guidelines for GDPR compliant user experience (D3.6, M12), Analysis of interoperability and cross-border compliance issues (D3.18, M34).

Task 3.8 Conformity, Validation and Certification [M09-M36]

This task will support the rest of the projects by analysing technologies, system designs and implementations to determine whether the combination of cybersecurity technologies in use achieve the desired security goals, allowing to compare different systems. The task will design a security framework capable of formally defining cyber-physical attack incidents, detecting an intrusion at different levels (physical or cyber), provide a resiliency policy and generate a forensics analysis. It will be based on the work of meta-schema for certification defined by ECSO, the ARMOUR project methodology and the NIST CPS. The testing and validation work will be also coordinated with WP7 infrastructure to define a common strategy. Finally, combing Task 3.3 with other methods, we can prove the security of the whole system.

Outcomes: Framework and Toolset for conformity (D3.8, M13). Validation and Certification Methodology and evaluation (D3.22, M36).

Task 3.9 Continuous Scouting [M09-M36]

This task will monitor the trends in the cybersecurity field to identify innovative approaches that could change the rules of the game or at least provide a competitive advantage to the early adopters. This will impact the roadmap development in WP4 and provide to demonstration cases in WP5 food for thoughts and for benchmarking. The task will rely on the expertise of the participants, voluntary contributions from researchers all over the world and cooperation with other cybersecurity competence centres (e.g., ENISA,

Europol, national cybersecurity agencies, NIST). Finally, we will experiment with automatic text analysis to identify innovations.

Outcomes: Cybersecurity outlook (D3.10 (M18) and D3.23 (M36)).

Task 3.10 Impact on Society [M15-M34]

The objective of this task is to advance the state of the art by developing a novel security awareness conceptual model, monitoring and enhancement methods with international applicability. This task will be devoted to analyse and identify efficient measures and methods for the continuous enhancement of societal security awareness, which should be held regularly to ensure that the staff is knowledgeable regarding the up-to-date security solutions, referring to private usage of digital technologies, human aspects of information security, professional practice and competence-development, governance, management and achievement of results and use of serious games for privacy and security awareness rising.

- **Outcomes**: Guidelines for enhancement of societal security awareness across critical indicators and targeted societal groups (D3.19, M34)

Deliverables

D3.1 Common Framework Handbook 1 [M09] common framework versions
D3.2 Cross sectoral cybersecurity building blocks[M11] first release of components
D3.3 Research challenges and requirements to manage digital evidence [M12] stakeholder analysis
D3.4 Analysis of key research challenges for adaptive security [M12] advanced threats and needs
D3.5 Usable security & privacy methods and recommendations [M12] general guidelines
D3.6 Guidelines for GDPR compliant user experience [M12] Identification of user impact aspects
D3.7 Usability requirements validation [M13] design methodology for usability requirements validation
D3.8 Framework and Toolset for conformity [M13] Complex system modelling and analysis
D3.9 Research challenges and requirements for secure software development [M14] new challenges
D3.10 Cybersecurity outlook 1 [M18] New trends monitoring versions
D3.11 Definition of Privacy by Design and Privacy Preserving enablers [M20] privacy solutions details
D3.12 Common Framework Handbook 2 [M28] common framework versions
D3.13 Updated version of enablers and components [M30] second released based on feedback
D3.14 Cooperation with Threat Intelligence Services for deploying adaptive honeypots. [M30] Proof-of-concept implementation
D3.15 Proactive approaches for secure software development [M32] methodologies and tools
D3.16 Security requirements and risks conceptualization[M32] Modelling and visualization techniques
D3.17 Integration to demonstration cases [M32] final development
D3.18 Analysis of interoperability and cross-border compliance issues [M34] Evaluation and end results
D3.19 Guidelines for enhancement of societal security awareness [M34] Continuous societal impact
D3.20 Final cybersecurity enablers and underlying technologies components [M36] final version
D3.21 Framework to design and implement adaptive security systems [M36] complete processing
D3.22 Validation and Certification Methodology [M36] Evaluation of the methodology
D3.23 Cybersecurity outlook 2 [M36] New trends monitoring versions

Work package 4 – Research and Development Roadmap

Contact: Evangelos Markatos (markatos@ics.forth.gr)

Objectives

- [Obj. 4.1] To develop a common Research and Innovation Roadmap for the cybersecurity of critical sectors of Europe covering the entire spectrum of research and development.
- [Obj. 4.2] To reduce fragmentation of cybersecurity research in Europe by providing an alignment of research activating and linking them to industrial demonstration cases.

Description of work

Over the past few years we witnessed that Europe's capacities in the area of cybersecurity are widely fragmented among Member States. To reduce this fragmentation and capitalize on the collective expertise that exists among the individual Competence Centers in Member States, WP4 aims to create a common roadmap that will represent the join investment of the community – the join commitment to their research – the join commitment to their future.

Task 4.1 Vertical stakeholders engagement and consultation [M01-M12]

This task will focus on engaging all vertical stakeholders (end users and industrial participants) so as to collect their requirements, to help them define their important problems and to lay the foundation for the roadmap. Through a diverse set of approaches including targeted questionnaires, one-on-one interviews, and common brainstorming workshops, this task will collect feedback (i) on the important problems that stakeholders face and (ii) on realistic approaches to deal with them. This task will also provide feedback to task 3.1 for the methodology definition on the research topics.

Task 4.2 Legal and regulatory requirements [M01-M12]

This task will map the legal and regulatory framework of the roadmapping process. Two are the main goals of this task: (i) define a framework within which the roadmapping work will proceed, and (ii) identify the unique European Legal and Regulatory Requirements (such as the GDPR, the NIS directive and the ePrivacy Regulation, PSD2 and eIDAS) that will offer a unique advantage to the roadmapping work compared to roadmaps possibly produced in a different geographic and/or legal context.

Task 4.3 Mapping and roadmap design [M01-M42]

This task will focus on creating the Research and Innovation roadmap of the project. Based on the results of Task 4.1, this task will closely collaborate with tasks 4.4-4.10, will integrate their results, and will cover any areas not covered by the proposed demonstration cases and mapped also to WP3 research areas. All roadmapping work in Tasks T4.4 to T4.9 will consist of the following steps:

(i) Collect existing roadmaps published by European Organizations (such as **ENISA** and Europol), European Associations (such as **ECSO** and the associated **cPPP** on cybersecurity), European Activities (such as the **Scientific Advice Mechanism**), and Academic Networks (such as **Networks of Excellence**, CSAs and concertation activities). The participants of the project have been contributing to (and in some cases leading) most of the above mentioned activities.

(ii) Identify Major Research Challenges that need to be addressed in this area. Explain what is at stake, and what can go wrong if problems are left unsolved, with attention to the results of task 4.1.

(iii) Collaborate with WP3 in the mapping of the identified research challenges that will be addressed in the context of the project and their impact on solving the different security and privacy needs of the sectors considered in the project. Clearly pinpoint what can be solved in the duration of the

project and what can be considered a **grand challenge problem** that needs to be solved as part of a larger programme.

(iv) Produce a roadmap with clear milestones that enable the regular progress checking.

(v) Update the roadmap in regular intervals based on its progress and possible updates of the requirements and needs, and taking into account the two phases defined in the project.

Task 4.4 Roadmap for industrial challenge 5.1 (e-Commerce) [M6-M36]

Create a roadmap for Challenge 5.1 (e-Commerce) based on the methodology explained in Task 4.3.

Task 4.5 Roadmap for industrial challenge 5.2 (Supply Chain) [M6-M36]

Create a roadmap for Challenge 5.2 (Supply Chain) based on the methodology explained in Task 4.3.

Task 4.6 Roadmap for industrial challenge 5.3 (Privacy-preserving Identity Management) [M6-M36]

Create a roadmap for Challenge 5.3 (Privacy-preserving Identity Management) based on the methodology explained in Task 4.3.

Task 4.7 Roadmap for industrial challenge 5.4 (Incident Reporting) [M6-M36]

Create a roadmap for Challenge 5.4 (Incident Reporting) based on the methodology explained in Task 4.3.

Task 4.8 Roadmap for industrial challenge 5.5 (Maritime Transport) [M6-M36]

Create a roadmap for Challenge 5.5 (Maritime Transport) based on the methodology explained in Task 4.3.

Task 4.9 Roadmap for industrial challenge 5.6 (Medical Data Exchange) [M6-M36]

Create a roadmap for Challenge 5.6 (Medical Data Exchange) based on the methodology explained in Task 4.3.

Task 4.10 Roadmap for industrial challenge 5.7 Smart cities [M6-M36]

Create a roadmap for Challenge 5.7 (Smart Cities) based on the methodology explained in Task 4.3

Deliverables

D4.1 Requirements Analysis from Vertical Stakeholders [M6] collects vert. stakeholder's requirements

D4.2 Legal Framework [M12] and its impact on the Research and Development Roadmap

D4.3 Research and Development Roadmap 1 [M12] First version of the roadmap. Each industrial challenge will have its own chapter (its own "roadmap" in D4.3.1), and the deliverable will tie all challenges together into a bigger roadmap that provide the big picture.

D4.4 Research and Development Roadmap 2 [M24] Updated version of the roadmap

D4.5 Research and Development Roadmap 3 [M36] Second update of the roadmap

D4.6 Evaluation of the Research and Innovation Roadmap [M42] Final evaluation of roadmap/process.

Work package 5 – Demonstration cases

Contact: Alessandro Sforzin (Alessandro.Sforzin@neclab.eu)

Objectives

- **[Obj. 5.1]** To effectively manage the WP and the alignment with WP3 to ensure meeting deadlines in the two phases appropriately.
- **[Obj. 5.2]** To identify use cases as demonstration cases with a high impact that sufficiently supports or if possible enhances the intentions of EU regulations and directives, such as GDPR, eIDAS and PSD2.

Description of work

WP5 is responsible for defining demonstration cases and use cases that identify the common research, development and innovation concepts to be developed by WP3 and to ensure their integration in demonstration cases in each of the project phases. Each of the tasks will develop specific use cases and demonstration cases, and the overall WP5 coordination will make sure that as many common technologies as possible are identified. The target is to maximize the resources allocated to each of the research items.

Task 5.1 E-Commerce [M01-M42]

This task is responsible for:

the specification and design of the demonstration case for e-commerce, including the identification of the relevant research challenges for WP3, the definition of validation scenarios and the identification of the corresponding criteria for the validation of the demonstration case;

the integration and deployment of the technologies and infrastructure required to set up a demonstration case based on the design and the validation cases as defined;

the validation by the stakeholders involved and the analysis of results.

These three activities are conducted around two demonstration case iterations and therefore, deliverables and workplan are defined accordingly.

Specifically, this task addresses the various security issues associated with PSD2 with the intention of resolving key inhibitors for AISPs, ASPSPs, PISPs and PSUs from moving forward with open banking with confidence. It will also give a boost to the strategic aspects of the EU's ambitions to establish a vibrant, open digital market, and in so doing facilitate the potential to enable innovation within the traditional financial community as well as in the newer Fintech companies, create jobs and opportunities for new citizen-oriented services.

Potential cybersecurity challenges to be addressed are in the area of:

Vulnerabilities emerging from social engineering and malware attacks

Providing protection for bank administration security policies

Potential weaknesses in the design and/or implementation of the API (i.e. not adequate design in terms of encryption, authentication, transport and application level security);

Fraud and data loss prevention in relation to the access and request of payment by TPPs;

TPP identification/certification/authorization, i.e. verification (and revocation) of certificates issued by national certification authorities to PISPs/AISPs;

Transaction risk analysis in the open banking environment, i.e. measurement of fraud risk in the presence of TPPs;

Risks and vulnerabilities exposed when obtaining account information, also under contingency state;

Coherence between GDPR and PSD2 requirements.

Outcomes: Requirements Analysis of e-commerce demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of e-commerce demonstration case (D5.2, M15 and D5.5, M39) and Validation of e-commerce demonstration case (D5.3, M24 and D5.6, M42)

Task 5.2 Supply Chain Security Assurance [M01-M42]

This demonstration case will result in a supply chain that allows components and the goods to be traced during all stages of the supply chain. The demonstration case will show how attempts at attacking the supply chain at various points, such as providing low-quality components or cheap counterfeits will be detected and prevented. The demonstration case might also show how conflicts can be resolved very quickly to save time and cost as compared to traditional systems.

It will further be shown how the various players will only reveal essential data and be able to conceal all other data than may be confidential.

Besides providing a generic blueprint to be applied is several domains, the demonstration case will specifically show an energy use case that involves transformers that are used for power distribution as a part of critical infrastructure. It will look at the supply chain for the delivery of components towards the construction of transformers.

Outcomes: Requirements Analysis of Supply Chain demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of Supply Chain demonstration case (D5.2, M15 and D5.5, M39) and Validation of Supply Chain demonstration case (D5.3, M24 and D5.6, M42)

Task 5.3 Privacy-preserving Identity Management [M01-M42]

This demonstration case focuses on developing a distributed and scalable platform for privacy-preserving self-sovereign identity management in the context of the public sector (education, smart city, healthcare). The platform will allow users to collect and manage attributes and claims from identity service providers, authenticate to service providers, provide consent for and control the personal data usage in a seamless and privacy-preserving fashion.

The demonstrated use case is the secure and trustworthy exchange of higher education certificates between organizations: educational institutes, universities, state agencies, private sector organizations, and individuals. The demonstration case will allow higher education graduates to, easily and in a verifiable way, share their certificates and prove their expertise during a preselection stage.

This task includes the following subtasks: (i) developing specification and design of the demonstration case for privacy-preserving identity management, including the identification of the relevant research challenges for WP3, the definition of validation scenarios and identification of the corresponding criteria for the validation of the demonstration case designed, (ii) developing and integrating the technologies and infrastructure required to set-up a demonstration case based on the design and the validation cases defined, (iii) the execution of the validation by the stakeholders involved and the analysis of results.

Outcomes: Requirements Analysis of privacy-preserving identity management demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of privacy-preserving identity management demonstration case (D5.2, M15 and D5.5, M39) and validation of privacy-preserving identity management demonstration case (D5.3, M24 and D5.6, M42)

Task 5.4 Incident Reporting [M01-M42]

This task is in charge of (i) the specification and design of the demonstration case for Incident Reporting, including the identification of the relevant research challenges for WP3, the definition of validation scenarios and identification of the corresponding criteria for the validation of the demonstration case designed, (ii) the integration and deployment of the technologies and infrastructure required to set-up a demonstration case based on the design and the validation cases defined, (iii) the execution of the

validation by the stakeholders involved and the analysis of results. These three activities are conducted around two demonstration case iterations and therefore, deliverables and work-plan are defined accordingly.

Outcomes: Requirements Analysis of Incident Reporting demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of Incident Reporting demonstration case (D5.2, M15 and D5.5, M39) and Validation of Incident Reporting demonstration case (D5.3, M24 and D5.6, M42)

Task 5.5 Maritime Transport [M01-M42]

The task will focus on the Maritime Transport vertical. The characteristics of the maritime transport, such as the interconnectivity of modern ships' and ports' systems and relative field devices (e.g. RFID, IoT), the use of wireless and special purpose communication protocols, the need for cost-effectiveness and the potentially hostile sea environment, generate very targeted security needs. This demonstration case will take advantage of the synergies that already exist among the competence network participants and the key maritime stakeholders, like port and ship operators, to assist the identification, collaboration and deployment of cyber-security services for this vertical. System interconnectivity and the interdependencies between various systems both at the ship side and at the shore side are some of the key features that need to be examined in order to model the novel cybersecurity threats in the maritime transport sector and assess their risk. Apart from threat modelling and risk assessment, other security domains that will be dealt with in this task, with the combined knowledge of the participants involved – from both academia and the industry of cybersecurity in the maritime sector – include situational awareness and intrusion detection & response, secure ship-ship and ship-shore communications, protection of autonomous navigation and collision avoidance systems from attacks like Man-in-the-Middle, and security hardening and forensics-by-design approaches for ship and port information systems. As for all demonstration cases, this task will have a strong link both with WP3, for research topics, and WP2 for the governance strategy. In the end, the task is in charge of (i) the specification and the design of the demonstration case for the maritime transport vertical and (ii) the design and deployment of novel cybersecurity tools as well as the modification and integration of existing security tools that come from the wide background knowledge of the participants, to address the identified cyber-security challenges and (iii) the execution and the validation of the demonstration case, applying the two iterative phases envisaged by the project.

Outcomes: Requirements Analysis of Maritime Transport demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of Maritime Transport demonstration case (D5.2, M15 and D5.5, M39) and Validation of Maritime Transport demonstration case (D5.3,M24 and D5.6, M42)

Task 5.6 Medical Data Exchange [M01-M42]

This task is in charge of (i) the specification and design of the demonstration case for secure and privacy-preserving medical data exchange, including the identification of the relevant research challenges for WP3, the definition of validation scenarios and identification of the corresponding criteria for the validation (ii) the integration and deployment of the technologies and infrastructure required to set-up a demonstration case based on the design and the validation cases defined (iii) the execution of the validation by the stakeholders involved and the analysis of results. These three activities are conducted around two demonstration case iterations and therefore, deliverables and work-plan are defined accordingly.

For this task, Dawex will set up a private data exchange platform, specific to this demonstration case, to integrate the toolkit developed in WP3, and prove it through live medical data exchange use cases.

Outcomes: Requirements Analysis of Medical Data Exchange demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of Medical Data Exchange demonstration case (D5.2, M15 and D5.5, M39) and Validation of Medical Data Exchange demonstration case (D5.3, M24 and D5.6, M42)

Task 5.7 Smart Cities [M01-M42]

The task will focus on the Smart City vertical. The demonstration case will move around personal data exchange among citizens and other city stakeholders, mainly the Municipalities (as key player in the delivery of public services and citizens' data management). New arising business and government models can be enabled only by user data exchange, so this will highlight several privacy and security challenges going to identified and analysed with the support of the participants involved and the additional city stakeholders who will be engaged by the project. Here, the Personal Data Store will represent a key asset offered by CyberSec4Europe to enable the demonstration case. Besides, Smart Cities are structurally facing to budget issues that avoid them to improve their cyber-security infrastructure/capabilities. The demonstration case will take advantage of Open Innovation tools in order to enable needs, ideas, best practices and lesson learned exchange among city stakeholders and the competence network to ease the identification, uptake, collaboration and deployment of cyber-security services for Smart Cities, including novel business models to pool resources and decrease the individual cost each city will have to provide. This environment then will also act as a trusted market place for cybersecurity services, using a "pooling" delivery model of services and resources. This will be a key goal for the demonstration case and for the whole project for this reason the task will have a strong link with WP3 and WP4.

In the end, the task is in charge of (i) the specification and the design of the demonstration case for the vertical and (ii) the set up and deployment of all the required and focused tools and methods (as the already mentioned GDPR compliant tool to manage personal data, lifelong learning approaches and online platform, cyber-security risk assessment tools, social engineering penetration testing tools and processes and Open Innovation process for cybersecurity novel pooling models) to address the main cyber-security challenges identified and (iii) the execution and the validation of the identified demonstration case, applying the two iterative phases envisaged by the project

Outcomes: Requirements Analysis of Smart Cities demonstration (D5.1, M3 and D5.4, M26), Specification and set-up of Smart Cities demonstration case (D5.2, M15 and D5.5, M39) and Validation of Smart Cities demonstration case (D5.3, M24 and D5.6, M42)

Deliverables

D5.1 Requirements Analysis of Demonstration case Phase1 [M04] will be produced as a documentation

D5.2 Specification and set-up Demonstration case Phase1 [M15] will be produced as a documentation

D5.3 Validation Demonstration case Phase 1 [M24] is the fully documented demonstration case

D5.4 Requirements Analysis of Demonstration case Phase 2 [M26] will be produced as a documentation

D5.5 Specification and set-up Demonstration case Phase 2 [M34] will be produced as a documentation

D5.6 Validation of Demonstration cases Phase 2 [M42] is the fully documented demonstration case

Work package 6 – Cybersecurity Skills and Capability Building

Contact: Fabio Massacci (fabio.massacci@unitn.it)

Objectives

- **[Obj. 6.1]** A formal education cybersecurity skills framework for HE for reference curricula development;
- **[Obj. 6.2]** A professional, continuing education framework for employers to train and assess the cyber-security capability of their workforce
- **[Obj. 6.3]** A virtual education strategy and offering for students, citizens and workers to reskill themselves and reach beyond formal education
- **[Obj. 6.4]** The development of innovative strategy based on distributed Cyber Ranges

Description of work

WP6 is responsible for setting an education and training framework and related instruments in order to support continuing education and lifelong learning in the area of cybersecurity and is organized to demonstrate the effectiveness of WP2 Governance Models and the full transfer of the pilot results to the future centres' operations. WP6 specifies learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles. It specifies knowledge units and curricula, training and awareness to achieve such objectives and competences. It sets activities to apply and test such competencies. WP6 implements the CyberSec4Europe education strategy for citizens, students, and professionals through creation and promotion of the CyberSec4Europe brand and of the guidelines and procedures to produce and consume content from platforms developed in WP7. The aim of WP6 is not to produce all possible content required to implement the specified educational and training programmes, but instead to set and run its platforms as a capability building instrument open to external sources and third-party material outside the consortium (if they meet guidelines and quality standards). This allows to bootstrap the programme into the future beyond the project.

WP6 runs full synchronized cycles on review (M12), design (M24) and pilot delivery (M42).

Task 6.1 University Education [M01-M42]

Identify and prioritize the cyber skills needed for education at University level, and investigate existing cyber-security curricula (e.g. ACM CyberSecurity Curriculum, DHS, etc.). Mapping of the national requirements for Cybersecurity Competences at the level of EU Member States and other nations) to identify the cybersecurity skills framework to be used as a reference by education providers. The project will leverage on the existing cooperation between participants such as EIT Digital CSE and SEECLO. *Each WP6 participant will be in charge for specific countries*.

Outcomes: Review, Design and Pilot Delivery of Formal Education Reference Framework

Task 6.2 Professional Training and Workforce Assessment [M01-M42]

Identification and prioritization of the cyber skills needed for security professionals and professionals in general. Specification of training programmes and professional assessment for different target groups in comparison to already existing industry programmes (ISACA, CISSP, ISC2, etc.) Design of a methodology to develop such programmes. Implementation of the capabilities (i.e. training and skill assessment) required to run such programmes. One Partner will lead the task and be responsible for the initial review of existing programs at European Level and the final development of assessment mechanisms for the general cybersecurity capabilities of the workforce across all Demonstration cases. Another partner will design and provide content and assessment approaches for the specific areas of Security Intelligence, Adaptive Security and Cross-Border Authentication. A third partner will provide

workforce assessment methods through serious games for PSD Demonstration cases. A forth partner will provide assessments mechanism for non-ICT workforce (lawyers etc.). A sixth partner will provide workforce assessment for Federated IdM scenarios on Public Sector.

Outcomes: Review, Design and Pilot Delivery of Professional Training and Assessment Programmes

Task 6.3 Virtual Education [M01-M42]

Implementation of the CyberSec4Europe virtual education strategy used to promote, disseminate and provide the capabilities built in Task 6.1, 6.2 and 6.3. It sets guidelines and format for all courses (specifying logos, format and look-and-feel) provided through the platform. It sets and implements the quality and assurance process and the process for the participant contribution to the virtual education platform. The task must also specify and implement the process to become a producer of a course and the process and access policies of subscribing and consuming single courses, seminars or entire predefined cyber skills programmes. Rather than developing yet another platform, it will leverage on the successful experience of EIT Digital and establish a negotiation to use one of the existing platforms (e.g., Coursera) for the actual delivery and the previous experience of one partner on delivering MOOC on the topic. Additionally the task will define and establish approaches to consolidate a federation of virtual platform interoperability in order to facilitate the broad coverage at European level and ERA. The partner will be responsible for the first initial review of MOOC offering at EU level and the process related to credit bearing courses for academic programmes, another partner will be responsible for the process for Continuous Education courses, a third partner for courses based on the use of the CyberRange. A forth partner will integrate the offering of EIT Digital on Security and Innovation, a fifth partner will contribute to the definition of educational capabilities and federation aspects (content and process for research & technology transfer courses).

Outcomes: Review, Design and Delivery of Virtual Educational Offers for citizens and professionals

Task 6.4: Cyber Ranges as platform for education, training and exercises [M01-M48]

Use of cyber ranges (Blue/RedTeam exercises, Capture the Flag challenges etc.) as both a professional and educational tool. The project will leverage on the most advanced cyber range in Europe called RGCE (Realistic Global Cyber Environment). It is an isolated and controlled environment, which offers a risk-free environment for use of attacks, known vulnerabilities and real malware. It enables the implementation of operator, company, government or other environments for demonstration, training or exercise. One partner will organize at least two cyber exercises during the project to be the "official" CyberSec4Europe flagship challenge and design a course on infrastructure use for teachers. Another partner will design a full course (syllabus, exercise and schedule) based on a third partners infrastructure. A forth partner will provide course on infrastructure use for PSD2 staff training. A fifth partner will create as full training set for CyberRangers for a summer school format.

Outcomes: Review, Design and Delivery of Cyber Range Instruments, Including the actual delivery of at least two CyberSec4Europe Co-Branded Cyber Ranges Exercises.

Deliverables

D6.1 Case Pilot for WP2 Governance [M06]
D6.2 Education and Training Review [M12]
D6.3 Design of Education and Professional Framework [M24]
D6.4 CyberSec4Europe, 1st flagship challenge [M24]
D6.5 CyberSec4Europe, 2nd flagship challenge [M36]
D6.6 Final Educational and Assessment Framework [M42]

Work package 7 – Open tools and infrastructures for certification and validation

Contact: Vaclav Vashek Matyas (matyas@fi.muni.cz)

Objectives

- **[Obj. 7.1]** to examine and provide open tools for certification and validation, in a close relation to education and standardization.
- **[Obj. 7.2]** to provide a completely open cyber range – a portable, lightweight virtual lab environment.
- **[Obj. 7.3]** to map existing cyber ranges, requirements from industry and requirements of connections and services including specification for implementation, including sample integration.
- **[Obj. 7.4]** to examine the role of certification for cybersecurity and its implementations, incl. governance structure and implementations over a virtual security certification centre.

Description of work

Working in a close relation with other WPs, namely 8 and 6, this WP takes the path from tooling, through infrastructures, to methodology for certification. Task 7.1 addresses open tools and open cyber range, task 7.2 aims at supporting access to infrastructures for testing and validation. Task 7.3 focuses on methodology, governance, supporting infrastructures and services for security certification.

Task 7.1 Open tools and common portable virtual lab [M02-M40]

Our first goal is to map the landscape of open tools in cybersecurity, to provide a portal exploiting this mapping and directing users to open tools, and to provide clear illustration of the benefits on selected concrete case(s). This task will develop in a close coordination with task 7.3 and WP8 (Standardization). One partner will leverage its experience in development and operations of KYPO, a complex cyber range, with numerous exercise sessions. The overarching ambition is to construct a portable, lightweight virtual lab environment from existing proven building blocks – modern virtual engines and containers, technologies for software provisioning, configuration, application management and deployment, interoperability standards including REST APIs, available datasets and testing data generators as well as virtual learning environments.

Within task T7.1, we will develop a prototype of the lab that will facilitate not only the actual deployment of open-source tools, but also will support hands-on learning with gamification features for engaging and efficient learning. We will provide sample training materials, as well as guidelines for developers describing how to prepare their tools and other supplementary materials (documentation, user interface, testing data, APIs).

Outcomes: Virtual lab for open-source tools education and research (D7.2, M23, with M12 – Architecture of the virtual lab – A technical report detailing the selection of existing modern proven SW technologies as building blocks for virtual lab development.). Common virtual lab with open-source tools for research and development (D7.4, M39, with M33 – Open-source tools, data, and use-cases deployed and demonstrated in the lab). Open tool portal (D7.5, M40 with M18 – Open tool taxonomy with proposed portal structure and selection of tools for D7.5).

Task 7.2 Federated infrastructures for cyber range and testing [M07-M41]

The European cybersecurity market is fragmented and not growing fast enough compared to other regions of the world. This task includes following activities:

- collecting data and assessing/comparing the features functionalities and services of existing cyber ranges in Europe. (cooperation with WP6 T6.4);
- gathering testing & certification requirements from cybersecurity industry and from vertical industry sectors. (cooperation with WP3, WP4 and WP5);
- defining requirements and conditions for cyber range federation and implementation:
- defining shareable services and selecting services for demonstration;
- implementing and demonstrating selected interconnections and services;

- collecting feedback, finalizing the services, preparing agreements and publishing of guidance documentation.

Outcomes: Report on existing cyber ranges, requirements from industry and vertical sectors and requirements of connections and services including specification for implementation (D7.1, M19); Evaluation report on integration demonstration (D7.3, M31); Collection of agreements, guidance documentation and dissemination materials (D7.6, M40).

Task 7.3 Certification – methodologies, tools and infrastructures [M07-M41]

To define governance and supporting services for security certification, with research, support, guidance and training for validation and certification of security properties of devices and systems for the EU industry.

- Partner1: Will investigate the certification role and objective for critical infrastructure components in the situation, where certification would not discover major vulnerabilities, in relation to task 7.1. Considering the ROCA case, states may not want to accept certified security products automatically. In addition to certification, states may consider developing their technical competence of developing and executing additional tests of the critical security features of certified products.
- Partner 2: Will align the work package efforts with the policy work related to the definition of the framework from T7.2 within the scope of ENISA and ECSO. This work is also needed as a starting point for Cloud Security Certification, a European initiative to associate certification concepts to cloud environments.
- Partner 3: Will examine how to reduce the time to certification of critical sector cyber physical systems (CPS) by designing its core components (architecture, communication and operating system) with a novel certified by-design framework. The overarching goal is to design a unified certified-by design IoT-enabled CPS framework where overall assurance is guaranteed for the complete system.
- Partner 4: Will follow the modification and approval of the EU Cybersecurity Act, and also assess the role of certifications based on ISO/IEC 27001 and GDPR for privacy compliance.
- Partner 5: Will be the key link to ECSO (as chair of ECSO WG1.4, WG2.3) and will ensure that Task 7.3 builds upon the work already accomplished and at the same time reflecting the reality of how certification and the harmonisation of certification will be done into the future, including governance structures and aspects of the further global penetration of the cybersecurity certification scheme.

The task will involve close cooperation with tasks that examine or provide tools or services (tasks 7.1 and 7.2), with the standardization WP (task 8.1 and 8.2), and with conformity and validation (task 3.8).

Outcomes: Report on the role of the certification and its implementations (the first version (month M14) with state of the art of the role of certification as a starting point for all participants, an update to this report in M28. The final version of the report (D7.3.1, M41) will also cover the implementation of the certification and governance structure and implementations over a virtual security certification centre.

Deliverables

D7.1 Report on existing cyber ranges, requirements [M19]
D7.2 Virtual lab for open-source tools education and research [M23]
D7.3 Evaluation report on integration demonstration [M31]
D7.4 Common virtual lab with open-source tools for research and development [M39]
D7.5 Open tool portal [M40]
D7.6 Collection of agreements, guidance documentation and dissemination materials [M40]
D7.7 Report "The role of the certification and its implementations" [M41].

Work package 8 – Standardisation

Contact: Liina Kamm (liina.kamm@cyber.ee)

Objectives

- **[Obj. 8.1]** to maintain contacts with standardisation organisations;
- **[Obj. 8.2]** to link the technical work of the project to the standards;
- **[Obj. 8.3]** to bring together standards projects and relevant cybersecurity experts;
- **[Obj. 8.4]** to assess the existing standardisation procedures in context of cybersecurity;
- **[Obj. 8.5]** to help increase the economic impact of European research and development by disseminating European technologies into international standards.

Description of work

Task 8.1 Maintaining contacts with the (European) SDOs and the relevant cybersecurity committees [M01-M42]

Task 8.1 will be undertaken hand in hand with the collaboration work in WP10, however, this task is specifically focused upon certification aspects. A close working relationship with ECSO Working Group 1 (standardisation/certification/supply chain) is implied with a number of the CyberSec4Europe participants being very active participants and contributors to the work of ECSO WG1. Furthermore, close relationships with SDOs (and especially CEN/CENELEC) are envisaged including the work associated with the ECSO MoU. Furthermore, one partner will be in charge of generalisation and integration towards other domains such as CIGRE (WG B5.66 and WG D2.46).

This task will create a cybersecurity standardisation engagement plan that sets up the plans and communication channels.

Outcome: Cybersecurity Standardisation Engagement Plan

Task 8.2 Linking the technical work of the project to standards and standards to the project [M06-M42]

The goal of this task is to study existing standards and ongoing standardisation projects in the context of the project topics and to connect experts to the standardisation process where they are needed. The skill sets of the consortium (and other competence centres) will be mapped out and a directory of ongoing cybersecurity standards projects will be kept. This will make it possible to connect the relevant experts to the standardisation topics. The task also aims to identify the cases where new standards can and should be proposed based on the work done during the project.

Outcome: Project Standards Matrix

Task 8.3 Assessing the appropriateness of the existing standardisation procedures for the cybersecurity goals [M18-M42]

This task is twofold – it will look at cybersecurity standards themselves and cybersecurity concerns in other relevant standards. The goal of this task is to assess the existing standardisation procedures, to document their appropriateness for cybersecurity goals and their exploitation of open tools, and to suggest improvements. The task also aims to give guidelines on how to better integrate cybersecurity considerations into the procedures of standardisation of various kinds of activities, possibly with the use of open tools and certification.

The turnaround time of a standard in different SDOs is often quite long but cybersecurity concerns are critical and need to be dealt with swiftly. This task will compare turnaround, procedures and usage of standards from different SDOs within the EU. This task will also estimate which SDOs have had the biggest im-pact on EU legislation.

Outcome: Standardisation Procedure Assessment Document

Deliverables

D8.1: Cybersecurity Standardisation Engagement Plan [M06] plans/communication channels to SDOs
D8.2: Project Standards Matrix [M12] describing standards projects and their relevance to project topics
D8.3: Cybersecurity Standardisation Engagement Plan [M24] updated document
D8.4: Standardisation Procedure Assessment Document [M36] considering cybersecurity goals.
D8.5: Project Standards Matrix [M42] updated document

Work Package 9 – Dissemination, outreach, spreading of competence, raising awareness

Contact: David Goodman (david@trustindigitallife.eu)

WP1 Objectives

- **[Obj. 9.1**] Maximise dissemination of the project results to a wide audience of researchers and technolgists within the relevant cybersecurity communities and initiatives. Run dissemination as a necessary step before and during exploitation
- **[Obj. 9.2]** Promote the project achievements and results taking strategic and targeted measures for communicating the education and training cybersecurity framework and the service infrastructure to all potential users, including the media.
- **[Obj. 9.3]** Spread excellence and guidance on best practices in next generation industrial and civilian cybersecurity technologies, applications and services
- **[Obj. 9.4]** Raise cybersecurity awareness by establishing the value of new integrated secure and trust-aware services where possible involving end-users in piloted activities.
- **[Obj. 9.5]** Identify the exploitation strategy of the CyberSec4Europe results at a consortium and participant level relating to the comprehensive suite of novel cybersecurity products and services as well as in the context of implementing a common cybersecurity research and innovation roadmap
- **[Obj. 9.6]** Make policy recommendations based on the results of the conclusions and roadmaps associated with the demonstration activities in order to define a sustainable path for the technologies developed in CyberSec4Europe

Description of work

The main goal of WP9 is to disseminate the findings of the project effectively, to engage key stakeholders for knowledge sharing, to launch an effective internal and external communications strategy, while assisting other WPs to meet their outreach objectives.

WP9 will make project-related information available and easily accessible, promote widely the project's milestones, raise awareness and visibility, encourage stakeholder participation, manage the dissemination of the project's achievements, as well as achieve widespread adoption of cybersecurity best practices across Member States, industry, public authorities, research institutes and the general public.

T9.1 Dissemination activities & reporting [M01-M42]

T9.1 will provide a website and social media accounts for CyberSec4Europe to share and distribute information about the project. The website and social media will continuously be updated to reflect project news, events and to serve as a dissemination and communication channel with external communities. T9.1 will develop a plan for all WP9 dissemination activities in terms of location, scheduling, target, organizations involved, expected impact and a strategy with T9.3 to define channels and target stakeholders. T9.1 also deals with the annual reporting of the dissemination activities

Outcomes: D9.1, D9.3, D9.4, D9.9, D9.15, D9.22;

T9.2 Outreach [M03-M42]

T9.2 will promote the project activities and results going beyond the traditional dissemination means, taking strategic and targeted measures to communicate among a multitude of audiences, including the media and the public. T9.2 will also ensure that CyberSec4Europe research activities are made known to society at large in such a way that they can be understood by non-specialists. T9.2 will also make sure to reach target audiences in the field of security and trust by the organization of specific workshops and events including a final conference in collaboration with WP10 where researchers and members of existing cybersecurity and technological initiatives will be involved to maximise inputs on exploitation issues and give the project results the widest possible visibility.

Outcomes: D9.2, D9.5, D9.10, D9.21, D9.23

T9.3 Spreading of excellence [M03-M42]
Through T9.3, CyberSec4Europe aims to spread excellence and offer guidance on best practices in next generation industrial and civilian cybersecurity technologies, applications and services. This task will focus on publications in high-quality scientific journals and influential, high impact conferences, talks at industry events, presentations in specific events related to cybersecurity and organization of workshops, such as the International Symposium on Engineering Secure Software & Systems (ESSoS), and special sessions using dissemination through several summer schools and collocating workshops with conferences that several participants co-chair regularly.
Outcomes: D9.7, D9.16, D9.24
T9.4 Raising cybersecurity awareness [M03-M42]
T9.4 will raise cybersecurity awareness across industry and society by establishing the value of new integrated secure and trust-aware services involving where possible end-users in piloted activities. One essential target group is SMEs constitute the overwhelming majority of enterprises (approximately 99%, over 20 million), which accounts for two out of every three jobs (Eurostat 2016) in the EU. Many SMEs are subcontractors to large enterprises operating in industrial sectors, critical for the security maintenance of national supply infrastructures. One focus will be on the potentially serious cybersecurity problems that these SMEs may generate for a whole supply chain. Especial attention will be paid to the exploitation of the CyberSec4Europe solution for supporting the strategy behind GDPR, eIDAS, and other regulations.
Outcomes: D9.6, D9.11, D9.12, D9.13, D9.17, D9.18, D9.25, D9.26
Task 9.5 Exploitation & Sustainability [M06-M42]
T9.5 will identify the exploitation of the CyberSec4Europe results at a consortium and participant level relating to the comprehensive suite of novel cybersecurity products and services as well as the implementation of a common cybersecurity research and innovation roadmap also taking into consideration advice from the advisory board. T9.5 will also identify the sustainability strategy of the CyberSec4Europe framework in the context of building a network of competence centres in Europe beyond the completion of the project. Project participants will develop individual business plans and joint exploitation strategies using tested business models to show how they will use the outcomes of the project for future products and activities as well as patents and the generation of IPRs.
Outcomes: D9.14, D9.19, D9.27
Task 9.6: Policy recommendations [M13-M42]
T9.6 will identify and prioritise policy recommendations based on the results of the conclusions and roadmaps associated with the demonstration activities, to define a sustainable path for the technologies developed in CyberSec4Europe. The policy recommendations will also take into account the development of a legal and regulatory framework which can contribute to the evolution of the (upcoming) EU Cybersecurity Act and the wider context of comparative legislations in other domains. This task will be coordinated with WP10 in order to identify and plan the possible policy areas to be covered.
Outcomes: D9.8, D9.20, D9.28

Deliverables
D9.1 Website and Social media accounts [M03]
D9.2 Dissemination material: Brochures, poster [M04]
D9.3 Dissemination and awareness plan [M06]
D9.4 Website and Social media accounts [M12]
D9.5 Report on the outreach and dissemination activities 1 [M12]
D9.6 SME cybersecurity awareness program 1 [M14]
D9.7 CyberSec4Europe summer schools 1 [M18]
D9.8 Policy recommendation reports 1 [M18]
D9.9 Website and Social media accounts [M24]

D9.10 Report on the outreach and dissemination activities 2 [M24]
D9.11 SME cybersecurity awareness program 2 [M24]
D9.12 Supply chain security recommendations 1 [M24]
D9.13 Awareness effectiveness study 1 [M24]
D9.14 Exploitation strategy reports 1 [M24]
D9.15 Website and Social media accounts [M36]
D9.16 CyberSec4Europe summer schools 2 [M36]
D9.17 SME cybersecurity awareness program 3 [M36]
D9.18 Awareness effectiveness study 2 [M36]
D9.19 Exploitation strategy reports 2 [M36]
D9.20 Policy recommendation reports 2 [M36]
D9.21 Final conference on the project results [M40]
D9.22 Website and Social media accounts [M42]
D9.23 Final report on the outreach and dissemination activities [M42]
D9.24 CyberSec4Europe summer schools 3 [M42]
D9.25 Supply chain security recommendations 2 [M42]
D9.26 Awareness effectiveness study 3 [M42]
D9.27 Exploitation strategy reports 3 [M42]
D9.28 Policy recommendation reports 3 [M42].

Work package 10 – Community empowerment and innovation fostering

Contact: Mark Miller (mrmiller@conceptivity-switzerland.com)

Objectives

- **[Obj. 10.1]** Concertation and clustering with related and concurrent projects for joint learning, information sharing, cooperation, benchmarking and achieving significant impact
- **[Obj. 10.2]** Cooperation with existing cybersecurity ecosystems and communities (also including innovators and entrepreneurs) building upon important experience and capabilities developed over time
- **[Obj. 10.3]** Collaboration with EU bodies and agencies to address the strategic research and innovation agenda elements (cPPP) and to contribute effectively to the work of ENISA, Europol, EU agencies and bodies in relation to cybersecurity.

Description of work

WP10 is focused upon significant collaboration with other SU-ICT-03 projects, existing other cybersecurity projects, communities & ecosystems and EU bodies and agencies in order to achieve a fully sustainable competence network and comprehensive integrated European cybersecurity ecosystem for the benefit of European Industry, the European Research Community and ultimately benefitting the European Citizen.

Task 10.1 Clustering and collaboration activities with funded projects from SU-ICT-03 and other EC cybersecurity projects [M01-M42]

Subtask 10.1.1 - Identification and development of natural clusterings of activities within cybersecurity domains such as, but not limited to: *Certification/Assurance/Audit, Cryptography, Data Privacy and Security, Education/Training, Incident Handling/Forensics, Human Factors, Identity and Access Management, Governance/Security Management, Networks, Hardware/Software Security Engineering, Measurement/Analysis of Security, Legal Elements, Theory, and Trust Management & Accountability.*

Subtask 10.1.2 - CONCERTATION activities with the SU-ICT-03 funded projects and other cybersecurity projects: 1) initial contact with other SU-ICT03 projects, 2) information sharing and exchange agreements with other SU-ICT-03 projects (formal or informal), 3) annual CONCERTATION conference (x3) with other cybersecurity projects and related networks.

Task 10.2 Collaboration with existing cybersecurity communities and ecosystems innovation [M01-M42]

Subtask 10.2.1 – Direct collaboration and integrated work streams with the European Cybersecurity Organisation, including, but not limited to: ECSO Working Group 1.4 (standardisation/certification/supply chain), ECSO Working Group 2.3 (international), ECSO Board of Directors (direct representation and participation of CyberSec4Europe participants), ECSO Working Groups 1, 2, 3, 4, 5, 6 with ECSO Strategic Research and Innovation Agenda contributions and work (via ECSO Working Group 6)

Subtask 10.2.2 – Active participation in the work of the Cybersecurity PPP - cPPP Board Member representation from CyberSec4Europe consortium participants.

Subtask 10.2.3 – Active collaboration with existing project communities and associations (including international elements such as USA, EU/Japan, etc.), for example: cyberwatching.eu, EUNITY, AEGIS, HPC, IoT, AI, SmartX, etc. Cooperation with the Digital Innovation Hubs and Networks of Excellence including, but not limited to: FIDIS, SysSec, NESSOS, eCRYPT. Direct interaction with associations including: Trust in Digital Life, Digital SME Alliance, and the European Organisation for Security, among many others. Also including national, regional and other clusters of cybersecurity excellence.

Task 10.3 Cooperative efforts and interactions with EU bodies [M01-M42]
Subtask 10.3.1 – Collaboration with ENISA and DG CNECT including active participation in ENISA workshops and conferences and providing input and feedback for Commission Communications, legislative and regulatory recommendations, working papers and impact assessments.
Subtask 10.3.2 – Collaboration with EUROPOL - involvement in the work of EUROPOL EC-3 (IoT Cybersecurity+ and CyberSec4Europe participants as EC-3 experts) and participation in EUROPOL workshops and conferences (including SU-ICT-03 presentations)
Subtask 10.3.3 – Contribution to the work efforts of CEN/CENELECT, including, but not limited to participation via the ECSO Working Group 1 activities and efforts and active participation and contribution to CEN/CENELECT Workshops

Deliverables

D10.1 Clustering results and SU-ICT-03 project CONCERTATION conference year 1 [M12] proceedings and reporting of collaboration efforts results year 1 (including but not limited to ECSO (and Working Groups), cPPP, ENISA, DG CNECT, EUROPOL, EOS, CEN/CENELECT, ISO, international cooperation)
D10.2 SU-ICT-03 project CONCERTATION conference year 2 [M28] proceedings and reporting of collaboration efforts results year 2 (including but not limited to ECSO (and Working Groups), cPPP, ENISA, DG CNECT, EUROPOL, EOS, CEN/CENELECT, ISO, international cooperation) – due month 24
D10.3 SU-ICT-03 project CONCERTATION conference year 3 [M42] proceedings and reporting of collaboration efforts results year 3 (including but not limited to ECSO (and Working Groups), cPPP, ENISA, DG CNECT, EUROPOL, EOS, CEN/CENELECT, ISO, international cooperation) – due month 42 (in order to include all project liaison results)