Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D6.3: Capacity Building Programme and Planning

Document Summary Information

Grant Agreement No	101020416	**Acronym**	ERATOSTHENES
Full Title	Secure management of IoT devices lifecycle through identities, trust and distributed ledgers		
Start Date	01/10/2021	**Duration**	42 months
Project URL	www.eratosthenes-project.eu		
Deliverable	Capacity Building Programme and Planning		
Work Package	WP6		
Contractual due date	30/09/2022	**Actual submission date**	7/10/2022
Nature	Report	**Dissemination Level**	Public
Responsible author	DBC	**Lead Beneficiary**	DBC
Authors	George Athanasiou, Anastasia Panousi, George Sidiras (DBC)		
Internal reviewers	INLE, IDIADA, ATOS		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101020416.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V1	20/06/2022	40%	Initial Deliverable Structure & Basic Processes.	George Athanasiou, Anastasia Panousi, George Sidiras (DBC)
V2	25/07/2022	70%	Collection of information from the corresponding partners	George Athanasiou, Anastasia Panaousi, George Sidiras (DBC)
V2.1	30/09/2022	100%	Almost Final version	George Athanasiou, Anastasia Panousi, George Sidiras (DBC)
V3	10/10/2022	100%	Final version	George Athanasiou, Anastasia Panousi, George Sidiras (DBC), George Baroutas, Konstantinos Loupos (INLE)

Disclaimer

Copyright message

Table of Contents

List of Tables

1 Executive summary

The current deliverable reports on the outcome of Task 6.2 *"Capacity building and workshops"*. It presents all the different types of capacity building/training activities undertaken in the context of the ERATOSTHENES project. Those activities include:

- The capacity building process action plan: Capacity building in ERATOSTHENES focuses mainly on fostering of knowledge exchange between the IoT industry and the research community in the EU and beyond, by offering training programs through online modules to improve capabilities/skills of researchers, SW developers, technical experts and end users.
- The method followed to elicit training requirements: In the project, the training needs analysis method (TNA) will be followed. TNA is the methodology for the identification and analysis of the gap between employees' training and training requirements.
- Training sessions to be conducted: ERATOSTHENES training process is split into two phases: 1. *"Train the trainers"* phase referring to stakeholders and pilot representatives' end-users training of the ERATOSTHENES system and its accompanying components and *"Train the pilot end-users"* phase referring to the training of the internal and external pilot participants (end-users) of the ERATOSTHENES system and its accompanying components.
- The capacity building material provided to educate the pilot end-users and stakeholders on the use and operations of the ERATOSTHENES system together with its components which assisted in preparing the pilot end-users properly for the pilot operations.

The purpose of Task 6.2 is to provide efficient training capabilities to capture all training requirements of the pilot end-users (retrieved from a pilot end-users survey and from various data sources).

Description of the utilized training material and means of supporting the training process are presented in the current report.

2 Introduction

2.1 Mapping ERATOSTHENES outputs

The purpose of this section is to map ERATOSTHENES Grant Agreement (GA) commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to ERATOSTHENES GA Deliverable & Tasks Descriptions

ERATOSTHENES GA Component Title	ERATOSTHENES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.3 - Capacity Building Programme and Planning	Report on the planning and organisation of the capacity building programme, strategy and implementation plan	*1-7*	*Chapters 1-7 provide an extensive description of all the activities, proposed plans, material, partners and the general means to be engaged in the training process of the ERATOSTHENES system.*
WP/TASKS			
WP6/T6.2	T6.2 - Capacity building and Workshops	*1-7*	*Chapters 1-7 provide an extensive description of all the activities, proposed plans, material, partners and the general means to be engaged in the training process of the ERATOSTHENES system. The presented training process along with the associated material aimed for allowing pilot end-users and stakeholders to get familiarized with the ERATOSTHENES system and its components, leveraging their knowledge incident handling, increasing their security awareness and raising their awareness on how to improve protection on their infrastructures.*

2.2 Deliverable overview and report structure

The present report is structured around 8 Sections as follows:

- Section 1: Executive summary of the deliverable.
- Section 2: General overview of the requirements of the deliverable in comparison to what is mentioned in the Grant Agreement.
- Section 3: Introduction.
- Section 4: Capacity building/Training needs analysis method and other sources used.
- Section 5: Training process.
- Section 6: Training material.
- Section 7: Monitoring and evaluation.
- Section 8: Conclusions.
- Annex 1: 1st workshop evaluation template

3 Introduction to Capacity building

This deliverable aims at presenting all the information related to the processes that will be undertaken, the method that will be followed and the training material that will be utilized to enlighten end-users on the operation and use of the ERATOSTHENES system and each accompanying component. The Deliverable D6.3 *"Capacity Building Programme and Planning"* is the outcome of task T6.2 "Capacity Building and Workshops". The ultimate purpose of the capacity building processes is to familiarize end-users with the ERATOSTHENES system and prepare pilot participants to use its environment towards the three pilot demonstrations:

- **Pilot 1: Connected vehicles**
- **Pilot 2: Healthcare**
- **Pilot 3: Industry 4.0**

The main purpose of this document is to increase awareness and familiarize the ERATOSTHENES proposed solution in the pilot domains. Furthermore, the present deliverable acts as an on-going assessment of the challenges and barriers that exist in the capacity building aspects within the selected domains. Three versions of the document (first version entitled "Capacity building, Programme and Planning", second and third version entitled "Workshops and Capacity building programme") are expected to be produced within the 42 months of the project.

The first version of this document (i.e., D6.3 due at M12) will focus on a diagnostic analysis of the current situation in training needs and capacity building activities in pilot sectors, having a particular interest in identifying challenges and gaps that would be potential barriers in the successful accomplishments of the training activities. The next versions will refine the analysis and provide training activities, presented material and implemented training activities throughout the course of the project.

As stated in the GA, to maximize the use and impact of the project outputs, a **Capacity Building Programme** is designed and delivered to expand and support the project solution across Europe. Capacity building in ERATOSTHENES focuses mainly on fostering of knowledge exchange between IoT industry and researchers in the EU and beyond, by offering training programs through online modules to improve capabilities/skills of researchers, SW developers, technical experts and end users, including:

- **Distributed, and dynamic Trust Management for IoT devices and networks** (Trust Agents, Virtualization techniques, trustful services, security/privacy mechanisms etc.).
- **Decentralised and scalable identity management approaches** (IoT devices enrolment and registration, hierarchical identification approaches, context-aware identities, privacy preserving self-sovereign identity (SSI) management models, Zero-Knowledge Proof concepts etc.).
- **Lifecycle management and the overall governance layers of trust in networks** (distributed ledgers, trusted IoT transactions, sharing and tracking cyber security in IoT, secure bootstrapping, software defined networks, federated learning loop for achieving intelligent and trustworthy IoT application, etc.).
- **Methodological Trust Frameworks scenarios and Architectures for distributed heterogeneous IoT networks.** The ERATOSTHENES challenge is to establish a mechanism that will keep participants' knowledge and capabilities sharp during and after the project. Innovations and processes that will be introduced to address this challenge include: i) Assessment of the **heterogeneity** of existing cyber-security schemes, ii) Analysis of **standardization** approaches, iii) Consideration of **dynamic nature** of IoT networks and iv) Consideration of **scalability** of IoT networks.

More details on the capacity building program and the training material are presented in the forthcoming sections.

4 Capacity building/Training needs analysis method

In the present section we present and analyse the main methods and sources used in view of:

- The target group identification per training session
- The capacity building priorities and needs articulation

4.1 Introduction to the methods & other cybersecurity training needs reports

Training needs analysis method (TNA) is the methodology for the identification and analysis of the gap between employees' training and training requirements. The capacity building/training process is considered the process during which "the acquisition of skills, concepts or attitudes that result in improved performance within the job environment" are obtained [1].

Training analysis delves into an operational domain recognizing all the initial skills, concepts and attitudes of the human elements of a system and specifying the appropriate training for them.

This chapter describes the TNA that will be adopted to conduct and implement the ERATOSTHENES capacity building programs as part of T6.2. The adopted TNA addresses the following features:

- Review of initial training needs;
- Task analysis;
- Identification of training gaps;
- Statement of training requirements.

Training Analysis is usually carried out as part of the system development process. Due to the close tie between the design of the ERATOSTHENES system and the training needs, the analysis run alongside the development.

The main scope of the TNA for the ERATOSTHENES project is to capture all the appropriate information that will organize and drive the ERATOSTHENES training process. The adopted TNA meets the following characteristics:

- Context specific: Relevant to the ERATOSTHENES Project and the Organisations participating in the project(both as Technical Partners & Stakeholders) taking into consideration the personnel skills/experience, requirements and expectations;
- Relevant to the trainees: Training process should guide and assist the trainees how to implement their tasks when using the ERATOSTHENES platform;
- Appropriate in terms of structure, timing and learning styles: ERATOSTHENES training process should be conducted in a way (i.e. structure, timing, and method of training) that facilitates the learning of the target group.

Apart from the TNA methodology and within the scope of T6.2 a desktop research and analysis of the following cybersecurity sources has been implemented:

- European Cybersecurity Skills Framework, September 2022, ENISA[2] : An analysis of the main cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, competences. It facilitates the identification of training needs per cybersecurity professional profile and consequently in bridging the gap between work and learning environments.
- European Cybersecurity Education and Professional Training: Minimum Reference Curriculum, November 2021, ECSO[3]: The report is dedicated in formulating a cybersecurity training curriculum and follows the JRC

[1] *How to Conduct a Training Needs Analysis*. Directory Journal. Available online: https://www.dirjournal.com/blogs/how-to-conduct-a-training-needs-analysis/ . Accessed: 2022-01-28.
[2] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
[3] https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf

cybersecurity taxonomy. It also presents a body of knowledge (being an outcome of an EU project, namely CyBOK[4]) for cybersecurity training purposes.

- Global Cybersecurity Index 2020, ITU[5]: This report aims to measure the cybersecurity maturity status of ITU Member States; The capacity development metric used in it, facilitates the identification of capacity development differences between each EU MS in their cybersecurity strategies and therefore contributes in tailoring the training needs for different EU MS audiences.
- EU funded projects outputs and recommendations on cybersecurity training. The cyberwatching radar[6] was used to extract the funded EU projects belonging to the JRC Cybersecurity Taxonomy domain: Education and Training. The selected list includes 20 EU funded projects. Each of them can be accessed in the provided link.

4.2 Description and analysis of the methods

This section describes the main areas of enquiry and the TNA method used to conduct and implement the ERATOSTHENES training process.

As described previously, the TNA is used to assess organisations and/or project's training needs following a gap analysis. The aim is to identify the gap between the knowledge, skills and attitudes that people in the organisation currently possess and the knowledge, skills and attitudes that they require to meet the organisation's objectives.

The application of the TNA depends on the current situation each time. One size does not fit all. The purpose of the assessment of the training needs is to:

- Lead into a design of a specific purpose improvement initiative (e.g. user claim reduction)
- Enable the design of the Project's training calendar
- Identify training and development needs of individual staff during the performance appraisal cycle.

To perform the TNA analysis, we considered the training needs at the organisation level, at the project level and at the department level of specific employees. These considerations help to determine:

- Who will conduct the TNA
- How the TNA will be conducted
- What data sources will be used.

To capture the training, education and development needs of ERATOSTHENES stakeholders, a number of methods were utilized. This ensured that the data gathered was unbiased/identified gaps and balances under different perceptions. The approaches adopted to explore the ERATOSTHENES training needs, have been assessed to consider the time constraints of those involved; costs involved if any; available resources; and the preferences of those involved.

A part of the **training needs/capacity assessment** was conducted during the execution of Task 1.2. Furthermore, a survey was set up for stakeholders that will participate in the ERATOSTHENES training process. In this vein, information was collected from pilot end-users through questionnaires, to capture the stakeholders training requirements. The training needs assessment was obtained from pilot end-users answers and feedback to the following questions:

- Are there skilled and trained personnel on security and incident handling practices?

[4] https://www.cybok.org/
[5] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[6] https://radar.cyberwatching.eu/radar

- Does your organisation offer / is willing to offer training programs on its employees about security awareness? If yes, how long is the average duration of each training program?
- Are drills conducted frequently? What is the duration of the training?
- Do you see any addressed security requirement to engage a capacity building program in your organisation?

The output of the survey related to the training needs assessment showed that:

- The organisations of most pilot end-users have some skilled and trained personnel on security and incident handling practices
- More than half of the responders, answered positively that their organisations offer a training program about security awareness. In most cases occasionally and in few cases on an annual basis. In most cases the organisations offer daily training programs and in few cases with 2-3 days duration

As a consequence, the employees of the pilot end-users organisations is partially trained. A considerable number of responders have attended a training program in their organisation related to security awareness, nevertheless, most of them occasionally. According to the results, there is a considerable requirement to train the pilot's end-users on security and incident handling practices and raise their security awareness and consciousness on the involving threat landscape and help them to improve their incident handling capabilities and skills.

Apart from the stakeholders' survey, the training requirements were gathered through consultation from the ERATOSTHENES Project's Pilot Sites and through open discussions with senior staff during dedicated teleconferences of T1.2. Thereby, the team and gathered samples of work relating to the range of training activities delivered in the past (past deliverables, presentations, meetings) were considered.

This approach provides the following benefits:

- Quick, low-cost approach using information already available
- Provides information about individual, organisation and future needs
- Assists alignment of activities with organisational goals
- Demonstrates to staff that action is being taken to address issues they have identified
- Provides information to support and compare to other information sources (past security projects, etc.).

Apart from the survey implemented under Task 1.2 and the recent ITU's GCI report[7] presents interesting findings in the capacity development matters per country. The report reflects the gap between the capacity development between different EU MS countries, hence a different training level shall be followed in case of offering the same training session in different MS. Equally important, the recent publication from ENISA on European Cybersecurity Skills Framework (ECSF) Role Profiles[8] will facilitate the filtering and final formulation of the target audiences for the ERATOSTHENES training sessions that will be realized.

4.3 Target groups identification

This section encompasses the identification of the main stakeholders that are directly or indirectly interested/affected by the ERATOSTHENES project. To identify the target groups that will participate in the ERATOSTHENES training process, the training requirements must be considered. This information is captured from the pilot end-users' requirements retrieved from the implementation of Task T1.2. To this end, the initial target groups of ERATOSTHENES are:

- Scientific/ Research Community, Students
- Technical Software and System Developers, IoT Communities

[7] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
[8] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

- Business SMEs/other from IoT using technical outputs, Investors
- Standardization entities (AIOTI, ETSI, ECSO, etc.)
- Legislative Public admin, Policymakers
- Social General public - Citizens

Following the TNA and report analysis that has been implemented a more detailed positioning of the cybersecurity training target audiences has been defined. A first grouping is among the internal consortium stakeholders and the external ones, including cybersecurity and technology actors in the healthcare, industry and connected vehicles domains.

With regards to the internal stakeholders, the Research and Academia entities will mostly contribute towards the training aspects of the project. The technology providers and end-users will facilitate the implementation of training sessions to more experienced cybersecurity professionals working either for the public or the private sector. A short representation of the initial roles for the training sessions for the consortium partners is provided in the table below:

Table 2: Internal stakeholder and competencies

ERATOSTHENES PARTNERS PROFILES	RESEARCH AND ACADEMIA	TECHNOLOGY PROVIDERS / END-USERS
Partners	**UMU, SINTEF, KUL, TUG, UPRC**	**INLE, ATOS, AIRBUS, ENG, DWG, EUL, IDIADA, TEL**
Description	They will act as the main training providers to audiences within the cybersecurity sector and potentially in the cross-section of cybersecurity and healthcare, IIoT and automated vehicles.	They will contribute to the ERATOSTHENES training activities through their expertise and knowledge in parts of the software and hardware technologies used for the overall technical solution.
Target Audience – Organisational level	Academic and Research Institutes specialised in the cybersecurity domain either on a sector-specific direction (Healthcare, IIoT, connected vehicles) or on cybersecurity generic direction; Research laboratories working in the field of applied cybersecurity	SMEs with a special focus on Identity Management & Privacy solutions, in different settings (health, industry etc.). Technology centric-SMEs especially in technologies used in Eratosthenes (Ledger, PUF etc.) are also within the target audience. Cybersecurity public agencies, legislative public entities, standardisation entities with active participation in WG on IoT/cybersecurity
Target Audience – Individual level (following ECSF profiling classification as provided in ENISA's document)	Cybersecurity Educator Cybersecurity Researcher Cybersecurity Architect	Chief Information Security Officer (CISO) Cybersecurity Risk Manager Cybersecurity Architect

		Cyber Threat Intelligence Analyst Cybersecurity Implementer
Target Audience – Individual level	Cybersecurity Postgraduate, PhD Students & Researchers, preferably in the Identity & Privacy domain.	CISOs, threat intelligence specialists, risk managers, cybersecurity architects

With regards to the external stakeholders, they are categorized in four separate categories: cybersecurity, healthcare, connected vehicles and industry actors. In the following pages we present each of these categories and the initial approach to get engaged in ERATOSTHENES training activities:

Cybersecurity stakeholders: This category includes international organizations, market companies, international initiatives, public authorities, as well as policy and decision makers.

From a policy/decision-making perspective the most important actors to be engaged with ERATOSTHENES training activities are the following:

- European Commission: Digital Society, Trust & Cybersecurity, DG CNECT
- ECSO: Working Group 5: Education, Training, Awareness, Cyber Ranges[9]
- ENISA
- ETSI: Cybersecurity Technical Committee[10]
- ISO: ISO/IEC 27001 related technical committees mainly JTC1
- Cybersecurity national officers and agencies: All official national MS CERT/CSIRT teams and sector-specific CERT/CSIRTs[11]

All policy /decision-makers are expected to contribute towards a more effective cybersecurity training profile as well as provide their expertise in the successful establishment of the training activities vis-à-vis the reported and identified training needs from the corresponding organisations.

The industries and companies (SMEs) that will be targeted are mainly: engineering/consultancy companies with services on the network performance & security; risk monitoring and control. Such enterprises are key partners on matters of information selection and visualization due to their needs to interpret and link the information to configure and secure IT infrastructure assets and endpoints. Large ICT enterprises with a portfolio including Trust & Identity Management solutions will also be invited to selectively attend some of the training sessions offered by ERATOSTHENES. A non-exhaustive list of such private companies is provided below: Thales, IBM, Cisco, Ping identity, tenfold, Microsoft.

In addition to the private companies, IoT related associations will be invited to attended ERATOSTHENES training activities. In Europe, the Alliance for Internet of Things Innovation (AIOTI) or the Big Data Value Association (BDVA) are interested in expanding the adoption of IoT technology as well as creating alliance between several domains to develop and use common IDM architectures.

Pilot Sectors

As mentioned in previous sections, the training sessions will be organised back-to-back with the pilot activities of the project. Hence, several entities acting not in the cybersecurity domain per se but in selected sectors will be also invited

[9] https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges
[10] https://www.etsi.org/committee/cyber
[11] For a full list of MS CERT/CSIRTs: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

to follow the offered training activities. The table below attempts to present in a comprehensive manner the key entities for each training session, taking into consideration all previously mentioned reports as well as the TNA.

Table 3: Key entities for each training session

	Policy Actors / Decision makers	Companies / SMEs	Regulatory / Standardisation landscape	Research and Academia	End-users	Individual profiles
Cybersecurity	DG CNECT - EC ENISA ECSO WG5	Industries offering IDM solutions SMEs active in components of ERATOSTHENES or offering IDM solutions	ETSI – Cybersecurity TC ISO/IEC 27001 TCs AIOT BDVA	Cybersecurity R&I departments in Universities and ROs	CERTs CSIRTs	CISOs Cybersecurity Risk Manager Cybersecurity Architect Cyber Threat Intelligence Analyst Cybersecurity Implementer Cybersecurity Researcher
Healthcare	ENISA DG SANTE – EC	Companies active in security of IoT medical devices (hardware & software)	ISO/IEC 27001 TCs	Universities and departments with programmes on eHealth applications / medical IoT devices	Healthcare CERTs / CSIRTs	
IIoT	ENISA	IIoT security-driven SMEs, Smart manufacturing solution providers	IIoT consortium – Security WG	IIoT, smart manufacturing cybersecurity research teams	Industry actors CERT teams	
Connected Vehicles	ENISA	V2X cybersecurity based solution SMEs OEMs	ISO/SAE 21434:2021 related TCs	Connected vehicles research teams	Monitoring authorities	

Based on the specific training sessions that will be offered this list of target audiences will be dynamically updated and further filtered in order to formulate a case-by-case approach for the invited attendees while at the same time a continuity in the offered training activities will be ensured.

5 Training process

The ERATOSTHENES training process is split into two phases:

- *"Train the trainers"* phase referring to stakeholders and pilot representatives end-users training of the ERATOSTHENES system and its accompanying components
- *"Train the pilot end-users"* phase referring to the training of the internal and external pilot participants (end-users) of the ERATOSTHENES system and its accompanying components.

The phases of the ERATOSTHENES training process are presented in the following sections.

The ERATOSTHENES training process follows a composite approach integrating different training types:

- Self-instruction utilizing training materials (e.g. manuals, online training videos, etc.)
- Face-to-face training by skilled technical experts of the project
- Online training sessions instructor lead which are organized by consortium members and presented in the following sections
- Remote support from the technical partners via e-mails and teleconferences.

The following sections describe the action plan of the training process decided by the consortium and analyses its distinct training phases.

5.1 Train the Trainers

The current training sessions are mainly focused on the consortium end-users and internal pilot participants. The "Train the Trainers" phase involves the training conducted by the technical experts of the project's consortium who have overseen the development of the ERATOSTHENES system. These technical experts will organize the following training sessions to train pilot representatives (trainers) assigned to each pilot site:

- The **1st ERATOSTHENES platform training session** will be organized for the pilot end-users representatives and other consortium's end-users through a **remote webinar.** It will be a **2-hour training session** dedicated to the project's end-users (pilot sites and supporting partners). During the training session, a detailed presentation of the ERATOSTHENES platform will be provided by the technical representative from INLE, UMU and DBC showing online the ERATOSTHENES system and each different module, screen and feature that will be used during the three ERATOSTHENES pilot demonstrations.
- The **2nd ERATOSTHENES platform training session** will be organized mainly for the Advisory Board, consortium end-users, pilot representatives and other stakeholders via a virtual workshop. The duration of the session will be approximately 1 hour and a half, where the ERATOSTHENES technical experts will illustrate the ERATOSTHENES system functionalities directly from the platform online in real-time. Within this session, cybersecurity specialists and industry experts will be trained on the ERATOSTHENES system and incident handling process.

5.2 Train the Pilot End-Users/Representatives

The current phase is mainly focused on pilot end-users (internal and external). This training phase is performed in parallel with the pilot period.

According to the training calendar and action plan, training sessions are scheduled close to the pilot implementation period and will be conducted by the ERATOSTHENES technical team. In addition, during the three pilots ERATOSTHENES trainers (pilot representatives), who were trained by the project's consortium technical experts

during the previous period, undertake the responsibility to train other pilot end-users (both internal and external) on the ERATOSTHENES environment to get them familiarized with it and be in position to evaluate the ERATOSTHENES system and each accompanying components under the scope of the ERATOSTHENES pilot reference scenarios.

5.3 Training calendar and action plan

During WP6 and T6.2 devoted meetings, the consortium proposed a series of training sessions to capture the training requirements, analysed before and educate properly all target groups. The aim of the current training action plan is to help pilot end-users deeply comprehend the ERATOSTHENES system and its operations and get properly prepared for the pilots, raise the awareness of a group of stakeholders and project's end-users on the incident handling process and therefore increase their preparedness, response and decision-making capabilities. Upon these perspectives and considering that stakeholders' training is a continuous process, the consortium decided to undertake the action plan presented in the following table (workshop to be organized):

Table 4: ERATOSTHENES planned workshops

M (estimated)	Location	Leading Partner	Key Objective - Related Task	Audience
M3	Madrid, Spain	**ATOS**	Present the ERATOSTHENES Strategy and validate related impact assesment indicators (KPIs), gathering end-user requirements and feedback from the related stakeholders. Input to T1.1 and T1.2.	Scientific Community (30), IoT companies, SMEs and start-ups (25), potential end-users (use-cases) (15), Policy Makers and EC (5)
M21	IoT Week 2023, Berlin, Germany	**UMU**	Presentation of ERATOSTHENES first outcomes and feedback from the related stakeholders on the Methodological Trust Framework and Ref. Trust and Identity Management Arch. Input to T1.4.	Scientific Community and project representatives (70), IoT companies and stakeholders (70)
M30	Oslo, Norway	**SINTEF**	Presentation of ERATOSTHENES technological developments. Results from the second development cycle of ERATOSTHENES feedback from pilots.	Scientific Community and project representatives (50), Open call participants (20), IoT companies and SMEs (20)
M42	Athens, Greece	**INLE**	Final dissemination event, involving also international actors, to showcase the final project implementations including interactive presentations and system demonstrations to potential up-takers and tech. users	Scientific Community (30), IoT companies, SMEs and start-ups (35), potential end-users (use-cases) (35), Policy Makers, EC (10)

Each workshop mentioned before will include a training session. In total, the topics that will be covered in those sessions are the following (each workshop will include part of those topics):

Table 5: ERATOSTHENES technologies and partners offering it

ERATOSTHENES technology	Partners Involved
Blockchain based ledger development; Application of an SSI approach • Implementation of DID Communication protocols • Identity Management for Eratosthenes Framework, including the IoT devices • Integration with Hyperledger Aries framework	ATOS, TUG
Blockchain Traceability Platform	ATOS
p-ABC • Attribute-Based-Credentials and Zero-Knowledge proofs (concept/research) • Self-Sovereign Identity throguh p-ABCs (concept/research) • Integration of p-ABC crypto with Hyperledger ARIES framework (technical presentation)	UMU
Trust Manager Deployer	SINTEF
DLT, Smart Contracts and PoX protocols • Blockchain for IoT Security, Privacy, Data Integrity and Interoperability (industry oriented) • Blockchain-based data management in IoT (concept/research) • Decentralised identity management in IoT (concept/research) • Integration of Hyperledger Aries agents with Hyperledger Fabric (technical presentation	INLE
IoT Intrusion Detection System • Security monitoring and anomaly detection on local to IoT devices perimeter traffic with real time information • Application of Federated Learning techniques to enhance the underlying model results while improving privacy preservation. • Traceability and auditability of models and datasets through a DLT network. • Signature-based Detection for Known threats • Anomaly-based detection for unknown threats and misbehaviour with ML techniques • IoT-based Detection	ENG, ATOS

Security microVisor	KUL
Self —sovereign ID management platform • Authentication and ID management protocols and platforms (hands on) • Strong security authentication protocols (FIDO) (hands on) • Decentralized authentication based on VCs, DIDs and digital wallet • Self-sovereign identity for authentication and authorization on web3 applications and verticals of distributed IoT networks	UPRC
Interoperability layer for trust management	AIRBUS
Cybersec. validation mechanism	ATOS
Threat modeling framework	KUL
IoT Security certification • MUD standard and IoT security certification: extensions and applicability (concept/research) • Eratosthenes lifecycle security of IoT devices (technical presentation)	UMU
Context-aware Trust Management for IoT • Trust Management models from web of trust to zero trust architectures • Context-awareness and adaptive trust score calculation based on IoT hardware, software and operational characteristics • Implementation models and platforms for reliable and robust Trust Management	UPRC
PUF-based technologies for IoT trust networks • Industry oriented Root of Trust • Multi connectivity secure ecosystem • PUF Based Certification authority • Self Sovereign Identity compatible secure ecosystem	EUL
Cybersecurity Exercises/Training platrofm • Hands on exercises with "capture-the-flag" scenarios including challenges related to IoT authentication and Trust	UPRC, SINTEF, ATOS
Ledger uSelf • Ledger uSelf Context identity: Add a new factor of authentication to the end user (person or device) using the context information used for the communication with the Identity Provider and Service Provider • Ledger uSelf Mobile app: Mobile app devoted to allow to the end user to use the Self-Sovereign Identity functionality from his/her mobile.	ATOS

• Ledger uSelf Broker: Middleware to simplify the adoption of a SSI solution for the Service Provides • Ledger uSelf IoT: new module of the Ledger uSelf (decentralized identity system) which will support manage identity of IoT devices	

The training action plan shall be managed & executed by all participating stakeholders.

In addition, the training process shall combine theory and hands-on practice. Therefore, a set of training materials will be available to the trainers, to facilitate the training activities.

6 Training material

To facilitate the training activities, educational material and tutorials are utilised within the training process. The material that is provided to help the pilot end-users and stakeholders get familiarized with the ERATOSTHENES system and its components is the following:

- The **"Crash course on cybersecurity for organisations"**, which is a cybersecurity awareness documentation, it provides guidance on Information Security and explores various aspects of cybersecurity, involving business entities and following a technologically neutral approach for the implementation of protection against cyber-attacks within companies.
- The **"ERATOSTHENES System User Manual"**. A document describing the ERATOSTHENES system User Interface with showcases wherever required. It presents all ERATOSTHENES usage flows as a guide to the ERATOSTHENES users to indicate how they can take advantage of the ERATOSTHENES system and its accompanying components to make proper decisions for the incident handling process.
- **Specialized training material in PowerPoint presentation format illustrating the ERATOSTHENES system** components for better comprehension Screenshots from the auxiliary material.
- **Video recording & Multimedia** from conducted training session. A video will be recorded during each online training sessions illustrating all the main functionalities of the ERATOSTHENES system directly through the platform. The videos will be available in the ERATOSTHENES website and the YouTube channel.
- **Training Agenda** helps the user to get an idea of the training session and feature walkthrough
- **Public version Deliverables** of the ERATOSTHENES project related to the ERATOSTHENES system and its components
- **E-mails, online Frequently Asked Questions (FAQs) and online helpdesk** are available for responding to inquiries.

7 Monitoring and evaluation

The purpose of Monitoring and Evaluation (M&E) of the capacity building/training program is to answer questions on progress, whether the implementation of certain activities have the intended result, to allow for the overall results assessment and whether something can be done differently to achieve the prescribed goals and objectives. The generic technical definitions of M&E could be provided:

- Monitoring uses systematic collection of data on specified indicators to provide management and to also provide the main stakeholders of an ongoing intervention with indications of the extent of progress and achievement of objectives and progress in the use of allocated funds.
- Evaluation is a systematic and objective assessment of the ongoing or completed interventions (actions/policies), their design, implementation and results according to the following criteria: relevance, effectiveness, efficiency, sustainability, impact, coherence and EU added-value.

The basis of the M&E of the capacity building/training program is the following lists of KPIs, used to measure the current status of the program.

- KPI1: Training requirements fulfillment (TNA method)
- KPI2: Attendance to the training sessions
- KPI3: Satisfaction level of the end-users (questionnaires)
- KPI4: Quality of the live presentations
- KPI5: Quality of the training material uploaded on the website
- KPI6: Downloads of the training material

As a first evaluation exercise but also building the monitoring templates, the first ERATOSTHENES workshop was used to collect user requirements but at the same time to start building the competence list of required capacity building items. In the frame of this task, the related monitoring template (annex 1) was created and collected by all participants (the results of this is out of the scope of this deliverable and will be reported in a later release)[12].

DBC together with the entire consortium will be responsible for the M&E of the capacity building/training program at a periodic basis. The results will be reported in the corresponding deliverables in WP6.

[12] https://eratosthenes-project.eu/1st-workshop-iot-lifecycle-security-requirements-and-first-architecture-15-february-2022-register-and-save-the-date/

8 Conclusions

The present deliverable provided an extensive description of all the activities, proposed plans, material, human resources and the general means to be engaged in the training process of the ERATOSTHENES system. It is the first deliverable on training implementation under the project setting the ground on the most important aspects in successfully planning and organising the training activities of the project.

To conduct the training process efficiently, the ERATOSTHENES consortium follows well known methods and practices to collect information regarding potential gaps between the end-users training and the training requirements. In particular, with the conduction of a TNA method, the ERATOSTHENES consortium will perform an assessment on the end-users training requirements. Scope and objectives of undertaking this TNA method, its content and training target groups (e.g. key users, administrators, technical personnel) are described in Section 4. In addition, the section justifies the conditions under which the TNA is performed and the data sources that are used (e.g. initiate a pilot end-users training survey by disseminating questionnaires to end-users related to training and gathering their responses, explore information from various sources (e.g. from public reports of past projects, etc.).

Section 5 describes the training process that is undertaken by the ERATOSTHENES consortium to train pilot end-users and stakeholders on the use and operations of the ERATOSTHENES system. This process falls into two phases; the *"Train the trainers"* phase and the *"Train the pilot end-users"* phase. An action plan to organize training sessions, is to be followed in an efficient manner that will capture the identified end-users' training requirements. Different types of training are realized during the training execution and respectively reported.

Training means and educational material associated and support to the training process facilitating the courses and allowing trainees to better understand the content is presented and analysed in section 6.

The presented training process along with the associated material aimed for allowing pilot end-users and stakeholders to get familiarized with the ERATOSTHENES system and its components, leveraging their knowledge incident handling, increasing their security awareness and raising their awareness on how to improve protection on their infrastructures.

Annex 1 – 1st Workshop Evaluation Template

ERATOSTHENES - 1st Project Workshop

Disclaimer

The European Commission is not responsible for the content of questionnaires created using the EUSurvey service - it remains the sole responsibility of the form creator and manager. The use of EUSurvey service does not imply a recommendation or endorsement, by the European Commission, of the views expressed within them.

ERATOSTHENES

Company/Entity name:

Type of entity (SME, industry, academic/research, end-user, policy maker):

Country:

Expertise (topic of activities):

Please include below further challenges in the area of IoT Security that our project should consider. Try to be specific on the domain (use-case) identified and the challenge itself.

Please fill in your answer:

Please include comments over our project architecture and system components in mind of particular requirements and capabilities.

Please fill in your answer:

Please describe the gaps in standards that relate to our project and concept. Also please described any expected future requirements.

Please fill in your answer:

What functionality of the architecture do you find most interesting for its adoption/use?

Please fill in your answer:

Do you see any potential security or privacy conflict that you want to highlight?

Please fill in your answer:

Submit