ARCADIAN–IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D5.6: Training and security and privacy awareness activities report

Revision: v.1.0

Work package	WP5
Task	Task 5.6
Due date	30/04/2023
Submission date	27/04/2023
Deliverable lead	MARTEL
Version	1.0

Abstract

The ARCADIAN-IoT project focuses on addressing privacy, security, and trust challenges in IoT ecosystems. A series of training sessions will be conducted, targeting both ICT and non-ICT end-users, to provide knowledge and skills for testing and validating the framework. The training activities will cover use cases across three domains, promoting a secure and trustworthy IoT ecosystem for diverse applications.

Keywords: ARCADIAN-IoT, IoT, Internet of Things, Privacy, Security, Trust, Training sessions, Use cases, Stakeholders

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	16.03.2023	ToC	Valentin Popescu (MARTEL)
V0.2	11.04.2023	Content production	Valentin Popescu (MARTEL)
V0.3	13.04.2023	Feedback on the content	Paulo Silva (IPN)
V0.4	14.04.2023	Final review based on the feedback	Valentin Popescu (MARTEL)
V0.5	26.05.2023	Feedback on the content	Adriana Peduto (E-Lex)
V1.0	26.05.2023	Final review based in the comments from E-lex	Valentin Popescu (MARTEL)

Project co-funded by the European Commission under SU-DS02-2020		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ARCADIAN-IoT project and Commission Services	

* R: Document, report (excluding the periodic and final reports)
DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.
OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

The ARCADIAN-IoT project aims to develop a framework that addresses key challenges related to privacy, security, and trust in the context of the Internet of Things (IoT). To ensure the success of the project, a set of training session will be developed to engage stakeholders associated with the use cases in testing and validating the ARCADIAN-IoT framework. The training sessions will be conducted in two rounds, engaging both ICT and non-ICT end-users involved in the piloting scenarios.

The training objectives are to provide ICT and non-ICT end-users with the knowledge and skills needed to test and validate the ARCADIAN-IoT framework and to gather initial feedback on the ARCADIAN-IoT solutions. The training topics will cover the use cases of the three domains of the project.

The training sessions will be delivered online with remote presentations and will be open to the public. Recipients of the training include partners from the consortium, stakeholders, cluster projects, and users of the solutions.

Overall, the ARCADIAN-IoT project and its training activities aim to contribute to the development of a secure and trustworthy IoT ecosystem that can support a wide range of applications in various domains.

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS

DGA	Digital Guardian Angel
IoT	Internet of Things
IPN	Instituto Pedro Nunes
RISE	Research Institutes of Sweden
UC	University of Coimbra
UWS	University of the West of Scotland

INTRODUCTION

The ARCADIAN-IoT framework is a comprehensive approach to address the cybersecurity challenges faced by the Internet of Things (IoT) devices and networks. The framework consists of various components that work together to provide a secure and resilient IoT infrastructure. To ensure that the framework is adopted and implemented effectively, it is important to provide training to the relevant stakeholders.

1.1 Purpose and scope

The deliverable focuses on providing a clear understanding of the objectives and extent of the ARCADIAN-IoT training sessions. The primary purpose of these sessions is to enhance security and privacy awareness among stakeholders associated with the use cases in testing and validating the ARCADIAN-IoT framework. This is achieved by offering comprehensive training materials, engaging presentations that enable participants to effectively utilize the framework.

The scope of the deliverable encompasses various aspects, including the development of training materials, the organization of training sessions, and the collection of participant feedback. These sessions target ICT end-users, emphasizing the most advanced components and valuable aspects of the ARCADIAN-IoT framework. By addressing both the vertical and horizontal planes of the framework, the training sessions aim to empower participants with the knowledge and skills necessary to test, validate, and provide feedback on the ARCADIAN-IoT solutions.

1.2 Trainings objectives

As we strive to create a comprehensive and impactful training experience, the following objectives have been carefully designed to ensure the success of the ARCADIAN-IoT training sessions:

1. **Enhance knowledge and skills:** Equip the ICT end-users with the necessary knowledge and skills to understand, test, and validate the ARCADIAN-IoT framework. This includes a comprehensive understanding of the framework's components, their interactions, and their significance in addressing security and privacy challenges in IoT environments.
2. **Foster collaboration and knowledge sharing:** Facilitate an interactive learning environment that promotes collaboration and knowledge sharing among participants, enabling them to exchange ideas, experiences, and best practices related to the ARCADIAN-IoT framework. This objective aims to foster a community of stakeholders who can collectively work towards improving the security and privacy aspects of IoT solutions and contribute to the continuous refinement of the ARCADIAN-IoT framework.
3. **Collect valuable feedback:** Gather initial feedback from the ICT end-users on the ARCADIAN-IoT solutions to identify areas of improvement, potential modifications, and enhancements. This feedback will help refine the framework and ensure its effectiveness in addressing the security and privacy needs of the IoT domain, ultimately leading to more successful deployment and adoption of the ARCADIAN-IoT framework in various use cases.

1.3 Trainings structure

To provide effective training for the ICT end-users of the ARCADIAN framework, a well-structured and comprehensive training program should be designed. The best structure for these training sessions could consist of the following components:

1. **Introduction**: Begin the session with a brief introduction to the ARCADIAN-IoT framework, its purpose, and the goals of the training sessions.
2. **Framework overview**: Provide an overview of the ARCADIAN-IoT framework, covering the vertical and horizontal planes, the components, and their interactions.
3. **In-depth component exploration**: Delve deeper into the most advanced and significant components of the framework, discussing their functionalities, use cases, and benefits.
4. **Real-world scenarios**: Present real-world scenarios and case studies that demonstrate the practical application of the framework and its components in various IoT environments.
5. **Group activities and discussions**: Encourage group activities and discussions that promote collaboration, knowledge sharing, and problem-solving related to the framework's components and use cases.
6. **Feedback and improvement**: Allocate time for participants to share their feedback, suggestions, and potential improvements or modifications for the ARCADIAN-IoT framework.
7. **Q&A Session**: Conclude the training sessions with a dedicated Q&A session to address any remaining questions, concerns, or clarifications participants may have.

By following this structured approach, the training sessions will ensure that ICT end-users acquire a comprehensive understanding of the ARCADIAN-IoT framework, build the necessary skills to apply it effectively, and contribute to its continuous improvement through valuable feedback.

2   FIRST ROUND OF TRAININGS: ICT END USERS

2.1   Trainings session structure

The training program will consist of three sessions, each lasting one and a half hours. The sessions will be conducted online and will be interactive, with opportunities for the participants to ask questions and provide feedback.

2.2   Topics and use cases covered

The training will be structured based on a selected subset of the identified use cases of the Arcadian framework for IoT security, with priority given to those that consider security or privacy incidents. The aim is to demonstrate the importance of each component and how they work together to provide an effective solution for IoT security.

The lead technical partners for each use case play a vital role in driving the activities related to the technical components. However, it is essential to note that the responsibility for constructing the training activities is not solely theirs. Rather, it is a collaborative effort that involves support from other technical partners who are also engaged in the use case implementation and demonstration.

This collaborative approach is particularly important for the first round of trainings, as the target end-users will primarily be the domain leaders. In essence, while the lead technical partners may spearhead the process, the training development is a collective endeavor that requires input and cooperation from various technical partners to ensure its success.

Table 1: Overview of the use cases

Domain	Use case	Lead partner
A1	Person registration at DGA service	ATOS
A2	Person authentication at the DGA service	RISE
A3	Person retrieving and editing personal data	XLAB
A4	Person requesting a DGA service	UWS
A5	DGA service	LOAD
A6	Drone security or privacy incident	RISE
A7	Personal device security or privacy incident	XLAB
B1	New device registration	IPN
B2	GMS IoT device data gathering and transmission process	BOX2M
B3	Service request from third-party IoT monitoring platforms	BOX2M

B4	GMS IoT device security or privacy incident	IPN
B5	GMS middleware security or privacy incident	MAR
B6	External data audit to grid infrastructure	UC
C1	MIoT kit delivery - Patient registration and authentication	TRU
C2	MIoT Capturing and sending vital signs and perceived health status	MAR
C3	Personal data processing towards health alarm triggering	XLAB
C4	Monitor a patient and update a patient monitoring protocol	ATOS
C5	Patient MIoT devices security or privacy incident	RISE
C6	MIoT Cloud services security or privacy incident	UWS
C7	Medical 3rd party security or privacy incident	RGB

In the development of the training sessions, it is important to recognize that not all use cases will be included or considered as part of the curriculum. Instead, a focused selection of use cases will be chosen, with an emphasis on those that address security or privacy incidents, if possible. By prioritizing these specific use cases, the training sessions will provide participants with a more targeted and relevant learning experience, ensuring they acquire the necessary skills and knowledge to handle security and privacy challenges in the IoT domain effectively.

2.2.1 First training: Domain A

The first training session will concentrate on Domain A, which addresses a range of use cases related to the DGA service. The primary objective of the DGA service is to offer a secure and privacy-preserving solution for the registration, authentication, and management of personal data within IoT environments. In this session, the use cases to be considered, and their corresponding lead partners are as follows:

1. A1 - Person registration at DGA service (ATOS)
2. A2 - Person authentication at the DGA service (RISE)
3. A3 - Person retrieving and editing personal data (XLAB)
4. A4 - Person requesting a DGA service (UWS)
5. A5 - DGA service (LOAD)
6. A6 - Drone security or privacy incident (RISE)
7. A7 - Personal device security or privacy incident (XLAB)

ARCADIAN-IoT

By focusing on a select subset of use cases, rather than incorporating all of them, the training session will prioritize those that are particularly relevant to security or privacy incidents, if possible. This approach will provide participants with a comprehensive understanding of the DGA service's role in enhancing security and privacy within IoT ecosystems. As a result, attendees will acquire the necessary skills to effectively implement and utilize the ARCADIAN-IoT framework, ensuring a more targeted and relevant learning experience. The primary goal of this training session is to provide participants with an understanding of the various components and interactions involved in certain Domain A use cases. To achieve this goal, the session will be structured as follows:

1. Introduction to Domain A: The session will begin with an overview of Domain A, its relevance to the ARCADIAN-IoT framework, and the specific use cases to be covered during the training.
2. In-depth exploration of the selected use cases: Each use case will be presented in detail, highlighting its significance, objectives, and the specific components involved. The lead partner for each use case will guide the participants through the process, ensuring a thorough understanding of the component interactions and their role in addressing security and privacy challenges.
3. Hands-on activities and demonstrations: Practical exercises and demonstrations will be incorporated throughout the session, allowing participants to apply their newfound knowledge to real-world scenarios. This hands-on approach will help reinforce the concepts presented during the training and encourage active engagement from the participants.
4. Collaborative discussions and problem-solving: Participants will be encouraged to engage in group discussions and problem-solving activities, promoting knowledge sharing and collaboration. This interactive approach will allow participants to learn from one another, exchange ideas, and collectively work towards improving the security and privacy aspects of the ARCADIAN-IoT framework.
5. Feedback and improvement: Time will be allocated at the end of the session for participants to share their feedback, suggestions, and potential improvements for the ARCADIAN-IoT framework as it relates to Domain A use cases. This feedback will be invaluable for refining the framework and ensuring its effectiveness in addressing the security and privacy needs of IoT environments.

By focusing on Domain A use cases, the first ARCADIAN-IoT training session aims to equip participants with the necessary knowledge and skills to effectively implement and utilize the framework within this specific domain. Through a combination of in-depth exploration, hands-on activities, and collaborative discussions, participants will gain valuable insights and experience, contributing to the continuous improvement and refinement of the ARCADIAN-IoT framework.

2.2.2   Second training: Domain B

The second training session will concentrate on Domain B, which involves various use cases related to the registration, data gathering, transmission, and service requests of IoT devices. The primary objective of these use cases is to ensure a secure and privacy-preserving environment for IoT device interactions and data management. The use cases to be considered, and their corresponding lead partners are as follows:

1. B1 - New device registration (IPN)
2. B2 - GMS IoT device data gathering and transmission process (BOX2M)
3. B3 - Service request from third-party IoT monitoring platforms (BOX2M)
4. B4 - GMS IoT device security or privacy incident (IPN)
5. B5 - GMS middleware security or privacy incident (MAR)
6. B6 - External data audit to grid infrastructure (UC)

As in the first training, ARCADIAN-IoT second training will focus on a select subset of use cases, rather than incorporating all of them To provide participants with an in-depth understanding of the various components and interactions involved in Domain B use case. The session will be structured the same as the first training (see above section 2.2.1).

2.2.3   Third training: Domain C

The third training session will be centred   around Domain C, which encompasses various use cases related to the delivery, registration, authentication, and data management of medical IoT (MIoT) devices. The primary objective of these use cases is to ensure a secure and privacy-preserving environment for IoT devices within the healthcare sector. The use cases to be considered, and their corresponding lead partners are as follows:

1. C1 - MIoT kit delivery - Patient registration and authentication (TRU)
2. C2 - MIoT Capturing and sending vital signs and perceived health status (MAR)
3. C3 - Personal data processing towards health alarm triggering (XLAB)
4. C4 - Monitor a patient and update a patient monitoring protocol (ATOS)
5. C5 - Patient MIoT devices security or privacy incident (RISE)
6. C6 - MIoT Cloud services security or privacy incident (UWS)
7. C7 - Medical 3rd party security or privacy incident (RGB)

To provide participants with a comprehensive understanding of the selected use case, the session will be structured the same as the first training (see above section 2.2.1).

2.3 Participants

The training sessions will be delivered to various recipients including:
1. **Partners from the consortium**: The training sessions will be provided to all the partners of the consortium who are involved in the ARCADIAN-IoT project. These partners will receive training on the various components of the framework and how to use them effectively.
2. **Stakeholders from WP2 surveys**: WP2 (Work Package 2) conducted a series of surveys to gather information from stakeholders about their needs and requirements for IoT solutions. The training sessions will also be provided to stakeholders who have participated in these surveys. This will help ensure that the ARCADIAN-IoT framework meets the needs of the stakeholders.
3. **Cluster projects**: The training sessions will also be open to other projects or initiatives that are related to IoT solutions. This will help to disseminate knowledge and promote collaboration between different projects in the same field.
4. **Users of the solutions**: The training sessions will be provided to users who will be using the ARCADIAN-IoT framework to implement IoT solutions. These users

may come from various industries such as healthcare, transportation, agriculture, etc. and will receive training on how to implement and use the framework effectively to meet their specific needs.

2.4 Outcomes and feedback

The outcomes of the ARCADIAN-IoT training sessions can be evaluated based on several factors, including participant satisfaction, knowledge gain, and practical application of the framework. These outcomes can be measured using both qualitative and quantitative approaches, such as participant surveys, post-training assessments, and feedback from the actual implementation of the framework in real-world scenarios.

2.4.1 Participant satisfaction

Participant satisfaction is an essential outcome of the ARCADIAN-IoT training sessions. Ensuring that the training content is relevant, engaging, and informative will contribute to a positive learning experience for the participants. Surveys and questionnaires can be used to gauge participant satisfaction, allowing trainers to identify areas of improvement and adjust the training content and delivery accordingly.

2.4.2 Knowledge gain

One of the main objectives of the ARCADIAN-IoT training sessions is to enhance the knowledge and skills of the ICT end-users regarding the framework and its components. Assessing knowledge gain can be achieved through pre- and post-training assessments, as well as monitoring the participants' ability to apply the acquired knowledge to real-world IoT scenarios. This assessment will help determine the effectiveness of the training sessions in equipping participants with the necessary knowledge to effectively utilize the ARCADIAN-IoT framework.

2.4.3 Practical application

The practical application of the ARCADIAN-IoT framework by the participants is another critical outcome of the training sessions. By observing how the participants apply the framework in real-world scenarios, trainers can assess the effectiveness of the training and identify areas where further guidance or support may be required. This information can be used to refine and improve the training sessions, ensuring that they remain relevant and effective in addressing the ever-evolving challenges faced by IoT environments.

2.4.4 Feedback collection

Collecting valuable feedback from the participants is essential for the continuous improvement and refinement of the ARCADIAN-IoT framework. Feedback can be gathered through various means, such as surveys, interviews, and open discussions during or after the training sessions. This feedback can help identify potential modifications, enhancements, or areas of improvement for the framework, ultimately leading to a more effective and successful implementation of the ARCADIAN-IoT framework in various use cases.

In conclusion, the ARCADIAN-IoT training sessions play a vital role in ensuring the successful adoption and implementation of the ARCADIAN-IoT framework by providing comprehensive training materials, fostering collaboration, and collecting valuable

feedback from the participants. By carefully designing the training sessions to achieve the outlined objectives, and consistently evaluating their outcomes, the ARCADIAN-IoT project can contribute significantly to improving the security and privacy aspects of IoT solutions across various industries and use cases.

3 TRAINING MATERIALS DEVELOPMENT

3.1 Partner contributions

In order to ensure the successful implementation of the ARCADIAN-IoT framework, the project has planned for two rounds of training and knowledge sharing activities linked with the planned use cases. These training sessions will provide the stakeholders associated with the use cases with the necessary knowledge and skills to test and validate the framework.

The contributions from the partners are crucial to the success of the training sessions, and their involvement will help ensure that the ARCADIAN-IoT framework is properly tested and validated by the stakeholders associated with the use cases.

3.2 Presentations

The presentations in the training sessions should be clear, concise, and informative. They should include visuals such as diagrams, graphs, and images to help participants understand the concepts being presented.

Presentations should be structured logically, with a clear introduction and conclusion, and should cover the topics outlined in the training objectives. They should also provide examples and case studies to illustrate the use of the ARCADIAN-IoT framework in real-world scenarios.

The pace of the presentations should be moderate, allowing participants enough time to absorb and understand the information being presented. Presenters should also encourage interaction and questions from participants to ensure that everyone is engaged and has a clear understanding of the topics covered.

Overall, the presentations should be engaging, informative, and easy to understand, and should effectively convey the knowledge and skills needed to test and validate the ARCADIAN-IoT framework.

3.3 Demonstrations

During the training sessions, demonstrations should be interactive and hands-on to allow participants to see the practical application of the concepts covered in the presentations. The demonstrations should be well-prepared and presented in a clear and concise manner to ensure that participants can easily follow along.

Examples of demonstrations could include:

1. Setting up a verifiable credential: In this demonstration, the presenter could walk participants through the process of creating and issuing a verifiable credential using the ARCADIAN-IoT framework. Participants could follow along and practice creating their own credentials.

2. Conducting a remote attestation: This demonstration could show participants how to use the ARCADIAN-IoT framework to conduct a remote attestation of a device. The presenter could walk participants through the process step-by-step, highlighting important considerations and best practices.

3. Using federated AI: The demonstration could show participants how to use federated AI to analyse data in a privacy-preserving way. The presenter could use a simple example to illustrate the concept, and participants could practice running their own federated AI analysis.

4. Conducting behaviour monitoring: This demonstration could show participants how to use the monitoring components of the ARCADIAN-IoT framework to detect

anomalous behaviour on a network or on devices. The presenter could use a simulated network to show participants how the components work and how to interpret the results.

Overall, the demonstrations should be engaging, informative, and relevant to the training objectives. Participants should have opportunities to practice using the ARCADIAN-IoT framework themselves to reinforce their learning.

3.4 Hands-on exercises

Potential hands-on exercises:

1. **Setup of the ARCADIAN-IoT framework**: Participants could be guided through the setup process of the framework, including installation of necessary software and configuration of the components.
2. **Configuration of the components**: Participants could be given a scenario and tasked with configuring the appropriate components of the framework to meet the requirements of the scenario.
3. **Use case simulations**: Participants could be given a specific use case scenario and asked to simulate the use of the ARCADIAN-IoT framework to solve the problem. This could involve setting up and configuring components, troubleshooting issues, and providing feedback on the experience.
4. **Threat modeling**: Participants could be given a hypothetical scenario involving a security threat and asked to use the ARCADIAN-IoT framework to address the threat. This could involve identifying vulnerabilities and implementing security measures.
5. **Troubleshooting exercises**: Participants could be given a set of problems to solve related to the ARCADIAN-IoT framework, such as connectivity issues or configuration errors. They could work in small groups to diagnose and resolve the issues.
6. **Feedback and improvement exercises**: Participants could be asked to provide feedback on the usability, effectiveness, and overall experience of using the ARCADIAN-IoT framework. They could then work in groups to brainstorm and propose improvements to the framework based on their feedback.

The feedback could be collected through online surveys or in-person discussions. The feedback gathered could be analysed and categorized into different areas, such as usability and effectiveness of the ARCADIAN-IoT framework. The consortium could use this feedback to identify potential modifications or enhancements to the framework, which could be incorporated into the technical development of the project. The technical partners could analyse the feedback, identify the common themes, and prioritize the modifications and enhancements based on their impact and feasibility.

Attendees could have evidence of these modifications and enhancements through regular updates on the project's website or direct mailing. The technical partners could also communicate the changes made based on the feedback through release notes, documentation, and training materials, ensuring that attendees are aware of the changes and how they impact the framework's functionality.

3.5 Roadmap and plan

This roadmap and plan for the first round of training scheduling should help ensure that the training sessions are delivered effectively and efficiently, providing the necessary knowledge and skills to the ICT end-users to test and validate the ARCADIAN-IoT framework.

June:
- Develop training materials for the selected use cases and components of the ARCADIAN-IoT framework
- Finalize the agenda for the training sessions
- Invite and confirm the participation of the partners from the consortium, stakeholders from WP2 surveys, and cluster projects
- Set up the necessary tools for the training sessions

September and October:
- Deliver the first three training sessions for the ICT end-users
- Conduct evaluations after each session to gather feedback and identify areas for improvement.
- Incorporate feedback and adjust the training materials and sessions as needed

November:
- Analyse the feedback and evaluation forms to identify areas for improvement
- Refine the training materials and sessions based on the feedback received
- Develop a plan for the second round of training sessions, which will focus on engaging non-ICT end-users involved in the piloting scenarios.

4   SECOND ROUND OF TRAININGS: NON-ICT END USERS

The second round of training sessions, scheduled around M33, will focus on engaging non-ICT end users who will be involved in the piloting scenarios. This round will build upon the experiences and feedback gathered from the first round of training sessions, implementing improvements and modifications to ensure a more effective and impactful learning experience for the non-ICT end users.

To address the unique needs and requirements of non-ICT end users, the training sessions will be structured as follows:

1. Recap and review of the ARCADIAN-IoT framework: Begin the session with a brief recap of the ARCADIAN-IoT framework, its purpose, and the primary components. This will help non-ICT end users understand the foundation of the framework and its relevance to their respective domains.

2. Tailored training content: Adjust the content of the training sessions to be more accessible and relevant for non-ICT end users, focusing on the practical application of the framework and its impact on their specific scenarios. This approach will help ensure that the training sessions resonate with the non-ICT end users and provide them with the necessary information to effectively utilize the ARCADIAN-IoT framework.

3. Simplified technical explanations: Present the technical aspects of the ARCADIAN-IoT framework in a simplified and easy-to-understand manner, ensuring that non-ICT end users can comprehend and appreciate the value and benefits of the framework in their respective scenarios.

4. Real-world case studies and demonstrations: Incorporate real-world case studies and demonstrations that showcase the practical application of the ARCADIAN-IoT framework in various non-ICT end user scenarios. This will help participants visualize the potential benefits and effectiveness of the framework in their own contexts.

5. Interactive activities and discussions: Encourage group activities and discussions that promote collaboration, knowledge sharing, and problem-solving related to the framework's components and use cases. This interactive approach will enable non-ICT end users to gain insights from their peers and contribute to the continuous improvement of the ARCADIAN-IoT framework.

6. Feedback and improvement: Allocate time for participants to share their feedback, suggestions, and potential improvements or modifications for the ARCADIAN-IoT framework, particularly from the perspective of non-ICT end users. This feedback will help refine the framework, ensuring its effectiveness in addressing the security and privacy needs of a diverse range of use cases.

By incorporating the lessons learned from the first round of training sessions and adapting the content to better suit the needs of non-ICT end users, the second round of ARCADIAN-IoT trainings will provide a more impactful and relevant learning experience. This approach will empower non-ICT end users with the knowledge and skills necessary to effectively utilize the ARCADIAN-IoT framework, ultimately leading to more successful deployment and adoption across various domains.

5 CONCLUSIONS AND NEXT STEPS

The ARCADIAN-IoT project's training sessions play a crucial role in ensuring the successful implementation and adoption of the framework. By engaging relevant stakeholders and end-users in both ICT and non-ICT domains, the project aims to provide them with the necessary knowledge and skills to test, validate, and provide feedback on the ARCADIAN-IoT solutions. The first round of training sessions will focus on the specific use cases across three domains, targeting the ICT end-users. The second round, scheduled around M33, will engage non-ICT end-users involved in the piloting scenarios, taking into account the valuable feedback and lessons learned from the first round.

As next steps, the ARCADIAN-IoT project should focus on refining the training materials and ensuring they cover the selected use cases and components effectively. It is crucial to prioritize use cases that consider security or privacy incidents, as well as foster collaboration among technical partners, ensuring the training development is a joint effort. The project team should also actively encourage interaction and knowledge-sharing during the training sessions, promoting an environment that facilitates feedback collection, improvements, and refinements to the framework.

After the completion of the first round of trainings, the project team should analyse the feedback received from participants, including their responses to the evaluation forms. This will help identify areas of improvement, potential modifications, and enhancements to both the training sessions and the ARCADIAN-IoT framework itself. The second round of trainings should be adjusted accordingly to address these findings, ensuring a more effective and impactful training experience for non-ICT end-users.

The second round of training sessions will build upon the experiences and feedback gathered from the first round of training sessions, implementing improvements and modifications to ensure a more effective and impactful learning experience for the non-ICT end users.

Regarding comparing results from both rounds, the project partners will to compare the feedback received from both rounds to evaluate the effectiveness of the modifications and improvements made in the second round.

As for final conclusions and lessons learned, the project partners aim to have a post-project evaluation phase that includes analysing the feedback received from the training sessions and identifying lessons learned to improve future projects.

APPENDIX A

Training evaluation form

Evaluation Form: ARCADIAN-IoT Training Session

Thank you for participating in the ARCADIAN-IoT Training Session. Your feedback is essential for us to improve future training sessions. Please take a few minutes to complete this evaluation form.

Please mind that your data will be processed exclusively for the project' purposes. For further information you may write to the following e-mail address: info@arcadian-iot.eu

***

Participant Information:

Name:

Organization:

Role/Position:

Date of Training:

Organisation of the trainings:

Please rate the following aspects of the training session on a scale of 1 to 5 (1: Strongly Disagree, 2: Disagree, 3: Neutral, 4: Agree, 5: Strongly Agree):

- The training objectives were clearly defined. Rating: _____

- The training content was well-organized and easy to follow. Rating: _____

- The training materials (presentations, exercises, etc.) were helpful and relevant. Rating: _____

- The trainers were knowledgeable and effectively communicated the material. Rating: _____

- The balance between theory and hands-on exercises was appropriate. Rating: _____

- The training session met my expectations. Rating: _____

- The training session will help me apply the ARCADIAN-IoT framework in my work. Rating: _____

- I would recommend this training session to others. Rating: _____

Cybersecurity aspects covered in the trainings:

1. How well did the training materials cover the key cybersecurity aspects in the context of the ARCADIAN-IoT framework?

    a. Poorly

    b. Adequately

    c. Well

       d. Very well

       e. Exceptionally well

2. To what extent did the training address the ARCADIAN-IoT planes (identity, trust, privacy, security, recovery, and common) in a comprehensive manner?

       a. Not at all

       b. Somewhat

       c. Moderately

       d. Very much

       e. Completely

3. How effective were the training materials in providing a clear understanding of the relationship between the ARCADIAN-IoT planes and their impact on cybersecurity?

       a. Not effective

       b. Slightly effective

       c. Moderately effective

       d. Very effective

       e. Extremely effective

4. How relevant and up-to-date did you find the information and materials related to cybersecurity aspects in the ARCADIAN-IoT framework?

       a. Not relevant or outdated

       b. Somewhat relevant or outdated

       c. Relevant and up-to-date

       d. Very relevant and up-to-date

       e. Exceptionally relevant and current

5. Did the training provide sufficient practical examples and case studies demonstrating the application of the ARCADIAN-IoT planes in addressing cybersecurity challenges?

       a. Not at all

       b. A few examples

       c. Some examples

       d. Many examples

       e. A wealth of examples

6. How confident do you feel in applying the concepts and principles learned in the training to address cybersecurity aspects related to ARCADIAN-IoT framework?

       a. Not confident

       b. Slightly confident

       c. Moderately confident

       d. Very confident

       e. Extremely confident

7. Please provide any suggestions or feedback on how the training could be improved to better address the ARCADIAN-IoT planes and their relationship with cybersecurity aspects:

a. [Open-ended response]

Please provide your thoughts on the following:

1. What did you like most about the training session?
2. What areas of the training session could be improved?
3. What additional topics or would you like to see covered in future training sessions?
4. Any other comments or suggestions?

b. [Open-ended response]

Thank you for completing this evaluation form. Your feedback is greatly appreciated and will help us improve our future training sessions.