**The concept of methodology D9.3 Training Pilot Evaluation**

Lead participant: PPHS

Deliverable 9.3 was originally planned to:

This deliverable will contain recommendations from trainees toward improvements in the training that will take place at involved universities and professional training facilities in the form of hands-on training. Recommendations will be written down during pilot tests of the trainings, basing on thematic analysis of trainees experiences. Pilot evaluation will be done through in-depth interviews and focus groups.

After consideration of current circumstances, the WP9 team decided upon a new approach to the deliverable. Succinctly, as the ‘pilot tests’ are not feasible in an academic environment from a time perspective (the process of launching new pilots and courses would exceed the timings for the deliverable and the efforts of SPARTA in WP9) and not possible in the professional sphere due to the current COVID pandemic.

Therefore, the team will work only with academic institutions in the project that believe they are currently following – in the most part – the recommendations of SPARTA, outlined in Deliverable 9.2 (D9.2).

The work will help confirm which universities are following the SPARTA recommendations and also help highlight any gaps between their current approach and the best practices included in D9.2. Furthermore, by also gathering data directly from students, the team can compare the results between the parties and highlight where perceptions differ.

In addition, WP9 can help highlight – where necessary - which ‘competencies’ are missing from the learning paths that will enable students to fill three entry-level roles: **Technical Support Specialist, Cyber Defense Incident Responder and Cyber Defense Forensics Analyst.**

Finally, the WP9 team considers creating a ‘focus group’ (FG), comprising selected survey participants from each of the universities. The FG will review the high-level findings of the surveys and discuss the areas related to the **SPARTA Best Practices** that could help boost the value offered by courses. For example, the FG will debate some of the identified gaps, linking them to possible solutions such as the use of practical workshops and simulations that can aid education.

To achieve the aforementioned deliverable, the team will implement two questionnaires to capture data from the course providers and students, respectively. The intends to use a ‘reusable template’, that, with minimum alterations can be reused to capture and highlight similar information from other universities and course providers. Moreover, the team will provide a ‘framework’ for the Focus Group that can also be followed to replicate similar outputs.

Finally, the team will summarise all the information captured, showing clear visualisations of the results and where possible, mapping the materials to the previously delivered reports D9.1 and D9.2.

## **Questionnaire 1 – for Administrators**

### Purpose

To gain an understanding of the current courses/programs covered by the universities that are dedicated to cybersecurity and to ascertain whether they align to the SPARTA guidelines/best practices detailed in Deliverable 9.2

For the applicable courses/programs, the goals are to capture the opinion of the university which of **SPARTA’s Cybersecurity Skills Framework** topics are covered in the courses/programs and to ascertain the delivery ratio between theory and practical teachings.

Moreover, the team would like to gain the opinions of course providers on the competencies and knowledge areas they intend to transfer to students sitting the courses/programs.

#### Questions

1. Which courses/programs ‘dedicated’ to cybersecurity do you provide (e.g. Cryptography, Security, Privacy but not general programs like Computer Science)?

*Entry via ‘short text field’ with a selection boxes:* ***1)*** *B (Bachelor’s) or Ms (Master’s) and* ***2)*** *Officially accredited course/program at the university (Yes/No)*

Entry 1, 2, 3 etc..

1. For ‘Entry 1’ please define the ratio of practical-based to theory-based based training

*(numerical selectors that equal 100. For examples 20 / 80)*

**IF, Practical = more than 0**

* 1. Please list the practical techniques you use (e.g. in Laboratory work, programming, etc.)
	2. Please list the modern technologies for training you use (e.g. CTF, CyberRanges, visualization, etc.)
1. Please select the skills your course/program covers

*Drop down checklist of SPARTA Skills*

1. Please select the work roles that most suit your course/program structure and syllabus

*Drop down checklist of NICE roles (use the target roles and others to enrich their data)*

1. Please list the novel trends in security (e.g. blockchain, (post)quantum, privacy by design, etc.)

*Entry via ‘short text field’*

1. Please list the basic topics: Computer Science, Cryptology, Humanistic and Social Science, Mathematics, Privacy, Security

*Entry via ‘short text field’*

1. What changes are on the horizon for this course/program?

*Entry via ‘short text field’*

 *(****Repeat questions 2 – 7*** *for each of the courses/programs they provide)*

Additional questions - optional

1. Are the Technical Support Specialist supported by the course/program?

*(Primary/Secondary/No)*

1. Are the Cyber Defense Incident Responder supported by the course/program? *(Primary/Secondary/No)*

1. Are the Cyber Defense Forensics Analyst supported by the course/program? *(Primary/Secondary/No)*
2. What are the unsupported roles according to Curricula Designer? (https://informacni-bezpecnost.cz/curricula-designer/, instruction video in progress)

## **Questionnaire 2 – for Students**

### Purpose

To capture the opinions of students sitting the courses/programs provided at the university.

The goals range from establishing whether the students feel the current delivery method provides the appropriate balance of practical-based vs theory-based based learnings. To various matters connected to the skills and knowledge areas. Including:

* The roles that they would like to start following qualification (if applicable)
* The (SPARTA) skills they believe the course/program provides
* The knowledge areas they believe they will attain through the course/program
* If they believe any improvements can be gained through changes to the course/program structure

#### Questions

1. What course/program are you currently studying?

*Drop down checklist from the universities’ answers* ***OR*** *Entry via ‘short text field’*

1. Is this the first course/program you have studied dedicated to cybersecurity?

*(Yes/No)*

**IF No**

* 1. Please provide the names of other courses/programs and state where you have completed them.

*Entry via ‘short text field’ with a selection boxes:* ***1)*** *B (Bachelor’s) or Ms (Master’s) and* ***2)*** *Officially accredited course/program at the university (Yes/No)*

1. Which of the next steps best represents your current feeling towards your move after completing the current course/program?

***Options***

*Option 1: Leave university and find a work*

*Option 2: Start a new course/program*

*Option 3: Other*

**IF Option 1**

* 1. Do you know the role you will apply for?
	Which selection best represents your current thinking?
1. *Currently, I have no idea*
2. *I am still considering, but I have several thoughts*
3. *I am fairly sure*
4. *I would love to… (provide role field)*

**IF *selections 2-4***

* + 1. Please select the work roles you would like

*Drop down checklist of work roles*

* + - 1. Do you think your current course/program will provide the skills necessary for your possible future role?

*(Yes/No)*

* + - 1. Which of the following knowledge areas do you think you will need for this work role?

*List of Knowledge areas: The KSA for the roles* ***Technical Support Specialist, Cyber Defense Incident Responder and Cyber Defense Forensics Analyst****. PLUS, other skills for specialist roles (this can be used to determine whether the students’ choices are realistic).*

1. In your current course/program, what is the ratio between practical and theory based learning?

*(numerical selectors that equal 100. For examples 20 / 80)*

* 1. Which statement best matches your opinion for the selection above?

***Options***

 *Option 1: The current approach is well balanced*

 *Option 2: I would prefer more practical training*

 *Option 3: I would prefer more theory training*

**IF Option 2 or 3**

* + - 1. Please provide your preferred ratio mix

*(numerical selectors that equal 100. For examples 20 / 80)*

* + - 1. Also, please help with providing more details

*Entry via ‘short text field’*

**IF Option 2**

* + 1. Which techniques would you like to be used in the course/program?

*Entry via ‘short text field’*

**IF Option 3**

* + 1. *Which topic would you like to study more of?*

*Entry via ‘short text field’*

1. From your current course/program, please select the statement next to each of the following skills that best matches your current feeling:

*List of SPARTA Cyber Security Skills with the selections underneath:*

1. *I feel I have already gained this skill*
2. *We are planning to cover this topic later in the course/program*
3. *My course/program does not cover this topic*

## **Conclusion**

The questionnaires will hopefully provide a plethora of information regarding the courses and the skills and knowledge areas covered.

Once all the information is captured and returned, we intend to link the ‘feelings’ of the universities to the opinions of the students. Moreover, the data will hopefully allow us to determine which of the courses match the SPARTA best practices. For the students, we can highlight the current gaps (if any) between their desired role and the course they are currently sitting. In addition, it will allow us to compare the expected learning outcomes provided by the universities to the competencies and roles provided in the CSF.

Finally, the information will allow us to continue discussions around the practical-based and theory-based approaches, and the items that could strengthen the courses and potentially increase the value for students. If there is appetite, we can also propose FG meetings to uncover more in-depth content.