**SPARTA**

Task T9.4 Plan

Date: 07.01.2020

**Task-specific WP9 information:**

Any changes to data in the proposal:

Main contact for T9.4 WP9: Jérôme JACOB jerome.jacob@securitymadein.lu

Partners involved in T9.4 WP9: TUM, UBO, DEM, PU, M30, KTU, YWH, CINI, CNIT, L3CE, ANSSI, ISCOM

**Plan for T9.4:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Quarter** | **Activity** | **Output** | **Partner Responsible** |
| Q1 - 2020 | Task Plan Creation | **Report** (This Document) | SMILE |
| Q2 - 2020 | Overview of the cyber threats | **Exhaustive report** of the cyber threats with classification (threat measurement scale) | ? |
| Q2 - 2020 | Overview of the standard cybersecurity leaks / vulnerabilities | **Exhaustive report** of the general cyber leaks / vulnerabilities with classification (leak measurement scale) | UBO |
| Q2 - 2020 |  Overview of mass/generic cybersecurity solutions / controls | **Exhaustive report** of the mass/ generic cybersecurity solutions / controls – Create a document which explain to user what to do to protect ourself | ? |
| Q3-2020 | Overview of the field for cyber security training | **Report presenting** how cybersecurity training is organized in EU countries and in the world. | CNIT |
| Q3 - 2020 | Define objectives to be achieved by a training program | **Report presenting** content of a global cybersecurity program, targets and goals | CNIT |
| Q4 -2020 | Based on the previous report, define and develop a structured reference model for cybersecurity training program – from basic hygiene rules for non-specialists to complex technical training for cyber specialist | **Document** **presenting exhaustive** adapted and structured cybersecurity training program (content must be exhaustive) | PPHS |
| Q1 - 2021 | Based on the previous report and documents, define a mechanism for the maximal diffusion – ad/mass info campaign/social network | **Document presenting a media program** describing the mechanism for the maximal diffusion – ad/mass info campaign/social network | ? |
| Q2 - 2021 | Study how to promote a virtuous model of cooperation between private/public/3rd sector = cooperation based on existing actions | **Document presenting a model of cooperation** between private/public/3rd sector | ? |
| Q1 - 2022 | Based on the results of each activities, reports and documents create an infrastructure dedicated to cyber security training at multiple consortium partners | **Deliverable (D9.4):** Pilot of Cyber training and exercice Framework (Ct&eF): **An Infrastructure** for technical realization of training activities at multiple consortium partners. | DEM, PU, M30 KTU |

**Risks:**

|  |  |
| --- | --- |
| **Risk** | **Mitigation strategy** |
| Unavailability of information in English | Use of partner knowledge (best) – own network – machine translation (worst) |
| Large volume of information | Be focused on official documentation and national agencies |
| Complexity of misunderstood to build an infrastructure | Follow the results of the reports and documention produced in the 9.4 task plan |
| Diffulties to involve partners | Improve communication to WP9 partners |

**KPIs:**

 **Description Target**

 # ? ?

**Dissemination strategy:**

Some elements of our reports should be published, in particular:

* **Report presenting** the overview of the global cyber world, benefits, constraints and risks
* **Exhaustive report** of the cyber threats with classification (threat measurement scale)
* **Exhaustive report** of the general cyber leaks / vulnerabilities with classification (leak measurement scale)
* **Exhaustive report** of the mass/ generic cybersecurity solutions / controls

For the others outcomes, they should be accessible through the Deliverable of the T9.4.