D4.1 "TRANSVERSAL TECHNICAL CYBERSECURITY CHALLENGES REPORT"

The main objective of Work Package 4 (WP4) is the development of cybersecurity technology roadmaps as a result of analysis related to current and emerging cybersecurity challenges and associated technologies. These roadmaps will create the foundations for new industrial capabilities, and assist towards the development of innovative technologies that will aim to address these cybersecurity challenges. To this end, early prototypes research and development which will target specific, high-priority opportunities identified in these roadmaps will be performed.

To achieve these objectives, the roadmaps will be developed in accordance with the challenges identified in the analysis performed in T4.1 "Detailed analysis of transversal technical cybersecurity challenges" and its associated deliverables. The challenges were identified through the following multistep process:

1. review and analysis of the latest cybersecurity reports from a variety of sources, including research articles and industry reports;
2. identification of threats and concerns based on the analysis of these reports which were subsequently converted into technical challenges (where appropriate); and
3. categorisation of these challenges based on already existing taxonomies, including the latest JRC taxonomy, which was published in 2019.

To avoid bias, the contributors of this deliverable were involved in all phases of the analysis, thus offering different perspectives on the most pressing technical challenges. The variety of the sources that were analysed allowed for a comprehensive identification, since the reports that were gathered originated from organisations representing a wide variety of sectors and disciplines.

The analysis resulted in the identification of a total of 86 technical cybersecurity challenges: 57 transversal challenges (reviewed in this deliverable) and 29 inter-sector challenges. Each of the identified challenges are broadly presented across three dimensions: (i) the detailed description of each specific challenge, (ii) the mitigation techniques currently existing either as a commercially available product or as the state-of-the-art on a research level, and (iii) the opportunities that can be derived based on the availability of mitigation techniques and solutions.

The deliverable D4.1 “Transversal technical cybersecurity challenges report” will be updated on M45 to include the latest developments in the cyber threat landscape, enhance its study through questionnaires answered by cybersecurity practitioners and professionals, and also use the input of dedicated workshops specifically held for this purpose. Also, given the timeline of the second iteration of the technology roadmaps, the second version of D4.1 will shift its focus more on the emerging challenges, rather than the currently existing ones.

Overall, this section provided a detailed review of the identified transversal technical cybersecurity challenges, while the discussion on the potential opportunities that arise touched upon multiple facets of required solutions that would need to leverage a combination of advanced technology (including the latest advances in AI/ML technologies), clear processes, and qualified and informed people. Moreover, solutions that are customisable and adaptive to particular environments are often needed.

Finally, such a systematic review has the potential to address the fragmentation often observed in the cybersecurity domain, and also form the basis for additional meta- analyses that will provide further insights into the current landscape and potential opportunities.