a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

Deliverable D8.7

Report on connections with stakeholders and European CERTs/CSIRTs – final version

Grant Agreement number:	833685
Project acronym:	SPIDER
Project title:	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
Start date of the project:	01/07/2019
Duration of the project:	36 months
Type of Action:	Innovation Action (IA)
Project Coordinator:	Name: Pier Luigi Polvanesi Phone: +39 010 600 2662 e-mail: pierluigi.polvanesi@ericsson.com

Due Date of Delivery:	30/06/2022
Actual Date of Delivery:	30/06/2022
Work Package:	WP8
Type of the Deliverable:	Report (R)
Dissemination level:	Public (PU)
Main Editors:	George HATZIVASILIS (FORTH)
Version:	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

List of Authors, Contributors, Reviewers

Name	Role	Organization
GEORGE HATZIVASILIS, MANOS ATHANATOS, DIMITRIOS KARNIKIS, NIKOS PETROULAKIS, PANOS CHATZIADAM, EFTYCHIA LAKKA, PARASKEUI FRAGKOPOULOU, MARIOS PAPAMIXALOPOULOS	Authors	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
KONSTANTINA PAPACHRISTOPOULOU	Contributor	EIGHT BELLS
PIERLUIGI POLVANESI, ANGELA BRIGNONE	Contributors	ERICSSON TELECOMUNICAZIONI
FILIPPO REBECCHI, ERIC WEBER	Contributors	THALES SIX GTS FRANCE
ANTONIO ALVAREZ ROMERO	Contributors	ATOS SPAIN SA
CHRISTOS XENAKIS	Contributor	UNIVERSITY OF PIRAEUS RESEARCH CENTRE
MAURIZIO GIRIBALDI, GUERINO LAMANNA	Contributors	INFOCOM S.R.L
GEORGE KAKAMOUKAS	Contributor	K3Y LTD
KONSTANTINA PAPACHRISTOPOULOU	Reviewer	EIGHT BELLS
IRENE KARAPISTOLI	Reviewer	CyberLens

History of changes

Version	Date	Change History	Authors	Organization
0.1	01/06/2022	First Draft, ToC	George Hatzivasilis, Nikos Petroulakis, Manos Athanatos, Dimitrios Karnikis, Panos Chatziadam, Eftychia Lakka, Paraskeui Fragkopoulou, Marios Papamixalopoulos	FORTH
0.2	22/06/2022	Second Draft	Konstantina Papachristopoulou	8Bells
0.3	22/06/2022	Review by 8Bells	Konstantina Papachristopoulou	8Bells
0.4	24/06/2022	Comments addressed	George Hatzivasilis	FORTH
0.5	26/06/2022	Review by CyberLens	Irene Karapistou	CyberLens
0.6	28/06/2022	Comments addressed	George Hatzivasilis	FORTH
1.0	29/06/2022	Final version	George Hatzivasilis	FORTH

Disclaimer

The information, documentation and figures available in this deliverable are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability.

Glossary

Acronym	Explanation
5G	FIFTH Generation cellular networks
B2B	Business to Business
CERTs	Computer emergency response teams
CRST	Cyber Ranges and Security Training workshop
CSIRTs	Computer security incident response teams
CTF	Capture the Flag
CyberHOT	Cybersecurity Hands -On -Training
DG-CONNECT	Directorate-General for Communications Networks, Content and Technology
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
HRB	Horizon Results Booster
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
ISACs	Information Sharing and Analysis Centres (ISACs)
KPI	Key Performance Indicators
MANO	Management and Orchestration
MWCapital	Mobile World Capital
ML	Machine Learning
NMIOTC	NATO Maritime Interdiction Operational Training Centre
NMRG	Network Management Research Group
OSM	Open Source MANO
PG	Project Group
REA	Research Executive Agency
RCIS	Research Challenges in Information Science Conference

SMEs	Small and Medium Enterprises
WP	Work Package

Table of Contents

Executive Summary 10
1 Introduction 12
1.1 Relation to the project work 12
1.2 Structure of the document 12
2 Methodology and Liaison Opportunities 14
2.1 Liaison opportunities with CERTs/CSIRTs 14
2.2 Liaison opportunities with SMEs / Public sector 14
2.3 Liaison opportunities with EU PROJECTS / ACADEMIA 15
3 Participation in Events 16
4 Report on activities, outcomes, and future plans 23
4.1 Report on EU CERTs / CSIRTs liaison activities 23
4.2 Report on SMEs/Public Sector Liaison activities 26
4.2.1 Report on SMEs liaison activities 26
4.2.2 Report on Public Sector liaison activities 27
4.3 Report on liaison activities with EU projects and academia 29
4.3.1 Joint activities with projects from CONCORDIA Project Group 29
4.3.2 The Cyber-Range Network 30
4.3.3 Federation of cyber-range platforms 31
4.3.4 The joint IEEE Cyber Ranges and Security Training (CRST) workshop 32
4.3.5 Collaboration with 5G projects 32
4.3.6 The knowledge transfer event with the PANDORA-EDIDP project 33
4.4 Reports on other stakeholders' events 34
4.4.1 Liaison with the Hellenic Cyber Security Team 34
4.4.2 Support the CyberHOT summer school 34
4.4.3 Participation in NATO's NMIOTIC conference 35
4.4.4 Participation in OSM Ecosystem Research 35
5 Conclusions 37
6 References 38
ANNEX I – EU CERTs/CSRITS events 41
Invitation sent to EU CERTs/CSIRTS 41
SPIDER Information sent to EU CERTs/CSIRTS 42
Questionnaire Results for EU CERTs/CSIRTS 44
ANNEX II – SMEs event 47
Invitation sent to SMEs 47
SPIDER Information sent to SMEs 48
Questionnaire Results for SMEs 50

ANNEX III – CONCORDIA PG JOINT EVENT 55
Joint event announcement 55
Post event Report 57
Takeaways from Panel Discussion 59
QUESTIONNAIRE RESULTS FOR CONCORDIA PG 60
ANNEX IV – PANDORA-EDIDP Project event 65
Invitation sent to PANDORA-EDIDP 65
SPIDER Information sent to PANDORA-EDIDP 66
Questionnaire Results for PANDORA-EDIDP 68

List of Tables

Table 1. Performed events for Liaison activities 22
Table 2. Liaison KPIs as defined in SPIDER GA 23
Table 3. EU CERTs/CSIRTs liaison status. 24
Table 4. EU CERTs/CSIRTs workshop logistics. 25

List of Figures

Figure 1. CERTs/CSIRTs workshops 26
Figure 2. SMEs Knowledge Transfer event 27
Figure 3. ENISA NIS summer school 28
Figure 4. Joint webinar "Training the European workforce of tomorrow: cyber ranges in practice" . 30
Figure 5. Cyber Range Network and online Webinar 31
Figure 6. Collaboration towards the technical federation between SPIDER, THREAT-ARREST, KYPO (CONCORDIA) 32
Figure 7. IEEE CSRT workshop – SPIDER presentation 32
Figure 8. Knowledge transfer event for the EU project PANDORA-EDIDP 34
Figure 9. Collaboration with the Hellenic Cyber Security Team 34
Figure 10. CyberHOT summer school 35
Figure 11. NATO's NMIOTIC conference 35
Figure 12. OSM Ecosystem Research 36

EXECUTIVE SUMMARY

This document represents the deliverable *D8.7 "Report on connections with stakeholders and European CERTs/CSIRTs – final version"*. It is the final version of the report concerning the liaison activities of WP8, which describes the work plan, material, and communication activities that were pursued during the project lifetime, as well as the means used to accomplish the objectives set for this reporting period. These activities concur to achieve partially **project objective #8 "**To **ensure (a) wide communication and scientific dissemination** of the SPIDER results to the research, academic, and ICT community**, (b) efficient exploitation and business planning** of the SPIDER concepts and tools to the market, and **(c) contribution of specific project results to relevant standardisation bodies**, namely: "[…] *The project will pursue dissemination of its results through (ii) participation and communication activities (participation in scientific conferences /workshops, coordination/communication with similar projects, etc.), (iii) community building activities (presence on social media platforms, communication with industry stakeholders, etc.), (iv) liaison activities (collaboration and knowledge interchange with CERT/CSIRT networks around Europe), […]"* of the SPIDER Grant Agreement (GA) [1].

The deliverable describes in detail all the rationale behind all completed and planned activities as well as the results of the liaison activities. The work described in this deliverable is the final outcome of Task 8.4: "*Liaison with Stakeholders and Creation of Operational Links with European CERTs/CSIRTs*" of the GA [1] which enhances the dissemination, exploitation, and innovation capacity of the project by creating live operational liaisons with external cybersecurity stakeholders like other R&D initiatives, projects, SMEs, Public Sector, and EU CERTs/CSIRTs. The establishment of these links is twofold. Firstly, it provided useful insights on the efficacy and added value of the SPIDER platform through its hands-on experience and the feedback received, and secondly, it will assist the adoption and longevity of SPIDER's outcomes even after the project's end.

We must underline the fact that some of the planned activities, such as face-to-face interaction through participation to meetings and workshops since Month 8 of the project were hindered due to COVID-19 impact. The WP8 task leaders took all mitigation actions possible for ensuring that the work done within the context of this task would be not compromised.

To summarize, the main accomplishments of this task were:

- The organizing of 3 *workshops for EU CERTs/CSIRTs*.
- The organizing of 1 *knowledge transfer event for SMEs*.
- The organizing of 1 *knowledge transfer event for the PANDORA-EDIDP project*.
- The engagement in the *CONCORDIA Project Group (PG)* (part of the Horizon Results Booster), the participation in the webinar *'Training the European workforce of tomorrow: cyber ranges in practice'*, and the collaboration with the included projects.
- The establishment of the *Cyber-Range Network* along with the projects *Cyber-MAR* and *FORESIGHT*, and the conduction of a *webinar for cyber-ranges and cyber-security training*.

- The collaboration with the projects *CONCORDIA* and *THREAT-ARREST* towards a *roadmap for the technical federation of cyber-range platforms*.
- The collaboration with other 8 cyber-range projects (*THREAT-ARREST*, *FORESIGHT*, *CyberMAR*, *SPARTA*, *ECHO*, *CyberSec4Europe*, *CONCORDIA*, and *SECANT*) and the establishment of the *'Workshop on Cyber Ranges and Security Training (CRST)'* that has been conducted two times (2021 and 2022) under the conference IEEE CSR.
- The collaboration with *5 projects in the 5G domain* (*5GMED*, *5GCroCoCo*, *5G-VINNI*, *5G-VICTORI*, and *5G-PICTURE*).
- The support of the *summer school CyberHOT* under the auspices of *NATO NMIOTC*.
- The support of the *ENISA's NIS summer school*.
- The involvement with the *OSM Ecosystem Research where SPIDER became part*.
- The engagement with more than 50 *communication, dissemination, and/or liaison events*, including events with *ENISA*, *NATO*, *CONCORDIA*, and *ECSO*.

Finally, the on-time delivery of D8.7 designates the completion of Task 8.4. The related dissemination KPIs were accomplished (workshops, knowledge transfer events, as well as liaison with other projects and external stakeholders), as presented in D8.4 [2].

1 INTRODUCTION

Within the SPIDER project, WP8 is responsible for dissemination, exploitation, standardization, and activities related with establishing liaisons with stakeholders. The first period of the project focused on maturing the technical work of SPIDER as well as on creating visibility for the SPIDER's outcomes and focusing on dissemination. The second period of the project has been concentrated on the liaison and knowledge transfer activities with the targeted external stakeholders. The current deliverable describes the overall outcomes of *Task 8.4 "Liaison with Stakeholders and Creation of Operational Links with European CERTs/CSIRTs".* The aims of the task as described in the GA [1] are the following:

(i) Establish liaisons with a number of security related stakeholders from Industry, SMEs, and Public Sector;

(ii) Pursue Liaison activities within the academic domain and cooperation with related R&D initiatives and other projects;

(iii) Create operational links between SPIDER and numerous EU CERTs/CSIRTs in order to interchange arising threats' information, training tools and material.

In the context of the liaison activities of this task, SPIDER consortium aims, through its cyber range training platform, to provide a holistic security training that can be used by different stakeholders and more specifically, by EU CERTs/CSIRTs. The main outcome of this task is validated through KPI number 9 in Table 2-6 of the GA [1], which refers to the number of achieved liaisons with EU CERTs/CSIRTs and other projects.

This deliverable is the final report of all the activities and milestones achieved under the Task 8.4. It also provides the successful establishment of active liaisons during the second half of the project's lifetime and beyond. Additionally, it includes a detailed description of the produced material and information on all communications between the consortium and external stakeholders. Detailed results based on the KPIs and achievement in relation to the original plan are also provided.

1.1 RELATION TO THE PROJECT WORK

The work of this Task was directly related with all tasks and work under WP8, as it enhanced most the activities pursued under WP8 like dissemination, exploitation, and communication. Moreover, it was directly dependant on the technical advances of the project pursued under the technical work packages namely: WP2, WP3, WP4, WP5, WP6, since a mature version of SPIDER was needed in order to be used, exploited, and validated through the liaison activities of Task 8.4. Furthermore, the feedback received from this task assisted on the validation activities of the WP7 project and created a feedback loop between WP7 and the technical work the project.

1.2 STRUCTURE OF THE DOCUMENT

The reminder of the document includes:

Section 2. Methodology: In this section, we describe the methodology that was used in order to identify the liaisons and we provide the plan and main outcomes from the liaison activities;
Section 3. Participation in events: In this section, we list the liaison events that SPIDER members performed or participated in;
Section 4. Reported Activities and Outcomes: In the fourth section of the document, we provide a report of the completed activities and the outcomes so far;
Section 5. Conclusions: This section concludes the document.
Annexes: The annexes of this document include the invitation letter and information sheet that was sent to the EU CERTs/CSIRTs, a cluster of SMEs, and other projects in order to invite them to the liaison activities of SPIDER, as well as the detailed feedback that we received via on-line questionnaires.

2 METHODOLOGY AND LIAISON OPPORTUNITIES

A simple methodology was followed by the liaison activities of SPIDER, which consisted of the following five (5) phases: i) *Identify* the potential liaison activities, ii) *Contact* the identified liaison links, iii) *Connect* with them and disseminate project-related information, iv) *Participate* in organized liaison activities, and v) *Maintain* collaboration. The stages were detailed in the first deliverable D8.6 [4]. In the first stage of Task 8.4 and D8.6, we focused on the first three (3) steps of the aforementioned methodology, while the main steps and rest activities were performed afterwards (documented here in D8.7).
Therefore, during the first half of the project we have set the initial plan, the processes, and the relevant files, and managed to identify various stakeholders for our liaison activities. Then, we prepared and sent out invitations focusing mostly on the difficult task of creating links with the largest possible number of CERTs/CSIRTs and SMEs. Liaison with EU projects was an easier task.

2.1 LIAISON OPPORTUNITIES WITH CERTS/CSIRTS

In order to recognize all the existing links with EU CERTs/CSIRTs, the CSIRTs list inventory by ENISA [3] was provided to the partners in order to find all the connection points that can be exploited for the purposes of Task 8.4. Through that process, twelve CERTs were identified. Only, FORTHCert which is FORTH's internal CERT team did not receive a formal invitation, as it operates under the same organization and personnel that handles this task. FORTH is part of FIRST.org a global forum of responders with the participation of most CERTs/CSIRTs teams from all over the world.
Eventually, we established liaison with five external CERTs, three of which are national CERTs. Partners from *GR-CSIRT*, *Cy-CERT*, *CZNIC-CSIRT*, and *BU-CERT* participated in the overall liaison activities (as well as *FORTHcert* members). These included: i) ***three dedicated workshops*** where the SPIDER project, its platform, and the use cases were presented and discussed, and ii) the ***some of the use cases*** under WP7 were validated. These main outcomes are presented in Section 4.1.

2.2 LIAISON OPPORTUNITIES WITH SMES / PUBLIC SECTOR

Concerning SMEs, we planned to reach out to SMEs' communities, e.g., through the PRAXI network [5] and Mobile World Capital (MWCapital) [6]. The contact began at a later stage of the project, when the prototype and a more mature version of the SPIDER platform were released. Public sector initiatives were also examined in order to promote SPIDER's outcomes and create operational links via the participation of individual partners or bilateral cooperation with SPIDER consortium.

Eventually, we ***contacted several SMEs*** via the PRAXI network, MWCapital, and other partners' contacts, and we ***organized a Technology Transfer event*** where the SPIDER project was presented and the platform was demonstrated, receiving fruitful comments that were considered for the finalization of the overall solution. Thereupon, a cluster of 8 SMEs (ITML, Focal Point, PDMFC, AEGIS, Zelus, Synelixis, CZNIC, and SEA) from 6 countries (Greece, Belgium, Portugal, UK, Czech Republic, and Germany) was established.

Moreover, we achieved ***collaboration with ECSO, ENISA, EOS, and NATO*** with the participation in several events that were organized by them. These events enhanced our knowledge concerning various cutting-edge issues on security training and cyber ranges, like the legal framework and the security posture after the extensive use of remote working during the COVID-19 pandemic. Also, we had the chance to familiarise with policies and rationales that are included in the establishment of the EU-ISACs community, the cooperation scheme between ENISA and CERT-EU, the CSIRTs Network in Europe, as well as the relevant structures of the European Union. All these aspects influenced the development of the platform and the overall progress of the SPIDER project. Furthermore, we supported and co-organized two cyber security summer schools of ENISA and NATO, respectively.

The detailed list of events that SPIDER members took part is presented in Table 1. Performed events for Liaison activities, as well as the main liaison results with SMEs and Public bodies are summarized in Section 4.2.

2.3 LIAISON OPPORTUNITIES WITH EU PROJECTS / ACADEMIA

SPIDER envisioned to create a number of active connections with other H2020 project that can cooperate and benefit from SPIDER and vice versa. An initial list of projects was compiled based on the participation of SPIDER partners to other funded projects and initiatives were created. This list was also populated with projects that were identified/contacted during participation to clustering events, conferences, info days, and webinars. Moreover, through partners' links we promoted SPIDER propositions, receiving feedback and creating joint initiatives like webinars. D8.6 [4] lists the affiliated projects in which partners directly participated, as well as projects that are relevant to our objectives and scope. Throughout the project's duration we tried to establish operational links with them.

Collaboration with several EU funded projects was also achieved, including, CONCORDIA, Cyber-MAR, FORESIGHT, THREAT-ARREST, PANDORA-EDIDP, and several 5G projects. We also accomplished to become part of the Open Source MANO (OSM) Ecosystem Research. Furthermore, we participated in numerous activities promoting SPIDER objectives and identifying potential liaison links.

Eventually, we managed to have active collaborations with almost all these projects. These included: i) ***co-organization of workshops*** under popular conferences, ii) ***knowledge transfer events***, iii) support of ***cyber-security summer schools***, and iv) technical discussions in order to support the ***federation with other cyber-ranges***. These results are analysed in Section 4.3.

3 PARTICIPATION IN EVENTS

This section includes all the events that were identified, and partners were able to participate in. Participation in events allowed us to propagate the vision of SPIDER outside the confines of the consortium. Moreover, it allowed the exchange of ideas and the recognition of potential exploitation and collaboration activities. Partners from the consortium participated in these events, providing a summary back to the task. All events conducted by the consortium during the period M19-M36 are presented in Table 1. A similar table in D8.6 summarizes the events that were performed during the period M01-M18.
The main liaison activities and results are summarized under the subsections of Section 4. At this point, we need to note that the travelling and working restrictions due to CoVID-19 affected the number of events held, and thus attended, by the consortium partners. Moreover, the liaisons activities are more easily done in a face-to-face manner, than through teleconferencing and virtual meetings.

Performed Events	External Stakeholder	Date	Partner	Description
M19-M36				
CYBERWISER.eu training event [7]	CYBERWISER.eu	March 25, 2021	8BELLS	CYBERWISER.eu organized a training event, entitled 'Effective cybertraining in the era of staff remotisation'. The event was attended by experts from all across Europe, including SPIDER members, setting the scene on the state of the art in cybersecurity training, presenting existing solutions and opportunities. Some of these ideas were also incorporated in the overall SPIDER training approach.
Territory and Infrastructure Security in the Digital Age workshop [8]	System of Systems and Intelligent Automation (SOSIA) Hub [9]	April 7, 2021	INFOCOM	SOSIA hub gathers industrial companies (mainly SMEs and some large companies) that provide ICT solutions for Environmental Security, Critical Infrastructure protection and Smart Industries. During the workshop, the SPIDER project was also presented in

				this broad audience.
EUCNC2021 WS8 [10]	EUCNC and 6G Summit	June 8, 2021	UPM	UPM gave a presentation entitled 'SPIDER: ML Applied to 5G Network Cyber Range at EUCNC's 'WS8: From 5G to 6G Automated and Intelligent SecuriTy: FAST'.
IEEE CSR Workshop on Cyber Ranges and Security Training (CRST) [11]	THREAT-ARREST, FORESIGHT, CyberMAR, SPARTA, ECHO, CyberSec4Europe, CONCORDIA	July 26, 2021	CYBERLENS	This workshop was co-organized along with other 7 EU funded cyber-ranges projects (THREAT-ARREST, FORESIGHT, CyberMAR, SPARTA, ECHO, CyberSec4Europe, and CONCORDIA). Also, CYBERLENS gave a presentation entitled 'The SPIDER Cyber Security Component', which was a joint work with CITY and 8BELLS.
Cybersecurity Hands-On Training (CyberHOT) Summer School [12]	NATO Maritime Interdiction Operational Training Centre	September 27-28, 2021	FORTH	FORTH represented SPIDER as a sponsor of the event, which was under the auspices of NMIOTC.
Career Day: Meet the companies	University of Crete	October 18, 2021	STS	STS participated in the virtual event, organized by the Graduate Student's Association of Computer Science Department of the University of Crete. There, SPIDER was disseminated in an audience of more than 90 participants of academic and industry fields.
CONCORDIA Open Door 2021 (COD2021) [13]	CONCORDIA	October 21, 2021	All	SPIDER participated as an exhibitor at COD2021 virtual event.
IEEE International Workshop on Computer Aided	IEEE	October 26, 2021	UPRC	UPRC participated in the workshop and gave a presentation entitled as 'Unveiling the user

Modeling and Design of Communication Links and Networks (CAMAD 2021) [14]				requirements of a cyber range for 5G security testing and training'. The related paper was a joint effort of UPRC, TID, and Ericsson.
Ericsson R&D Italy Innovation Event	Ericsson	December 1, 2021	Ericsson	The SPIDER concept and solution was presented during the event, giving an overview of SPIDER as a 'cyber-range training centre'
Open Source MANO (OSM) Ecosystem Research [15]	OSM and ETSI	January 17, 2022	All	SPIDER became part of the OSM Ecosystem Research. SPIDER integrates ETSI OSM framework to orchestrate scenarios deployments for different cybersecurity training and testing exercises.
Technology transfer event with PANDORA-EDIDP project	PANDORA-EDIDP	February 22, 2022	ERICSSON, UBITECH, 8BELLS, THALES	A targeted working session took place where partners from PANDORA-EDIDP consortium have been acquainted with the technologies of SPIDER 5G Cyber Range and how these can support their operations both as individual organizations and as the whole project.
Security Research Event (SRE 2022) [16]	EC and French Presidency of the Council of the European Union	March 1-2, 2022	UBITECH, THALES, FORTH, and UNISYSTEM	SPIDER was planning to participate as an exhibition event in SRE 2022 in Paris, France. However, *the event was postponed*.
OSM-MR#12 Ecosystem Day [17]	OSM Ecosystem	March 9, 2022	CNIT	In the event, CNIT shared SPIDER's OSM experience by demonstrating 'The SPIDER Platform – deployment and management of virtual topologies in 5G

				programmable environments'.
Doctoral School on CSDP Research Methodology Course [18]	European Security and Defence College (ESDC)	March 14-16, 2022	UPRC	UPRC participated in the course, organized by ESDC in Piraeus, Greece. UPRC member was among the speakers, presenting the research goals of SPIDER.
Promo video of CONCORDIA Project Group (PG) [19]	CONCORDIA and Horizon Results Booster	April 20, 2022	All	CONCORDIA PG, including SPIDER, produced a short promo video, with the support of the Horizon Results Buster service of EC. The video focuses on cyber ranges and innovative cyber security training. It is also included in SPIDER's YouTube channel.
1st International workshop on Technologies for Network Twins (TNT 2022) [20]	IEEE/IFIP	April 25-29, 2022	TID and UPM	TNT 2022 was co-allocated with IEEE/IFIP NOMS 2022, in Budapest, Hungary. TID and UPM gave a presentation entitled 'B5GEMINI: a Digital Twin Network for 5G and Beyond'.
Layer123 Reunion 2022: Intelligent Network Automation Congress [21]	ETSI ZSM	April 26-28, 2022	TID	TID participated in the meeting, which took place in Madrid, Spain. It included presentation and talks in four thematic areas of: i) cloud native networks, ii) AI/ML, iii) cybersecurity, and iv) edge computing. TID gave a presentation entitled 'Trustworthy networks in the days of zero-trust'. The SPIDER's Machine Learning Lab and orchestration, and the STA toolbox were also demonstrated.
ECSO's Cybersecurity Awareness Calendar – May 2022 [22]	ECSO	May 1, 2022	All	ESCO's Awareness Calendar Initiative provides some basic facts on selected subjects as well as associated solutions, services, courses,

				and best practices from ECSO Members and the community. May 2022 edition hosted the topic 'Cyber ranges & range-enabled services', where SPIDER Cyber Range was being featured.
Technology transfer event with SMEs		May 5, 2022	FORTH, UBITECH, ERICSSON	During this event, the project was presented in a group of external SMEs. The platform was also demonstrated, and the participants had the chance to see some of the mature results of SPIDER. The participants provide fruitful feedback and it was agreed to continue the collaboration in the future.
"Training the European workforce of tomorrow: cyber ranges in practice" webinar [23]	CONCORDIA and FORESIGHT	May 17, 2022	UBITECH	The webinar focused on a set of cyber ranges simulating realistic domain environment, equipment, infrastructures, and data developed by three EU funded initiatives (CONCORDIA, SPIDER, and FORESIGHT). Each project presented current progress, best practices, and technical insights together with a practical demonstration.
IETF 113 standardization meeting [24]	Internet Engineering Task Force (IETF) Network Management Research Group (NMRG)	May 24, 2022	TID	TID participated at the IETF 113 standardization meeting. The result was the agreement upon a first draft on 'Digital Twin Network: Concepts and Reference Architecture'. SPIDER contributed actively to this achievement with several application scenarios related to security and ML.
1st Open Annual Workshop on	8BELLS	May 27, 2022	8BELLS	The event was organized and promoted by 8BELLS. The

Future ICT [25]				project was presented along with other presentations concerning the state of the art related to ICT and aspects like 5G/6G, cyber security, IoT and Cloud. The event was attended by around 50 participants, who had the chance to explore the latest technologies, results, and outcomes of cutting-edge research as realised via EU Research Projects.
First European Defence Innovation Day Conference & Exhibition [27]	European Defence to High Representative for Foreign Affairs, European Defence Agency	May 31, 2022	UBITECH	Demonstration of SPIDER Cyber Range and how this can be utilised in supporting European Defence to High Representative for Foreign Affairs / Head of the European Defence Agency, Josep Borrell, and CEO of European Defence Agency, Jiry Sedivy, who had the chance to see the platform and its capabilities.
1st International Workshop on Massive Digital Twins for the Computer-Networks Evolution (TwinNets 2022) [26]	The event was sponsored by the European 6G Flagship project HEXA-X	June 14, 2022	THALES	TwinNets 2022 was co-allocated along with the 23rd IEEE International Symposium on a World of Wireless, Mobile and Mutlimedia Networks (WoWMoM). There, THALES present the SPIDER platform through the paper 'A Digital Twin for the 5G Era: the SPIDER Cyber Range', which was a joint effort by THALES, TID, UPM, CNIT, UNISYSTEMS, FBK, UBITECH, ATOS, and UPRC.
1st International Cybersecurity Challenge (ICC) [27]	ENISA	June 14-17, 2022	UPRC, UBITECH	SPIDER members participated in this challenge. Also, members of the Hellenic Cyber Security Team had the chance to participate

				in a CTF exercise in the SPIDER platform.
IEEE CSR Workshop on Cyber Ranges and Security Training (CRST) [28]	FORESIGHT, CyberMAR, SPARTA, ECHO, CONCORDIA, SECANT	July 27-29, 2022	FORTH	This is the second iteration of the workshop that will be conducted after the end of the SPIDER project. Nevertheless, SPIDER members are co-organizing and actively supporting this initiative.

Table 1. Performed events for Liaison activities

In total, SPIDER partners participated in around 38 main events reaching a wide audience of stakeholders and entities interested in SPIDER results. In these events, we had the chance to discuss with other experts in the field and exchange fruitful information that was incorporated during the development activities of the project. The overall list of events that SPIDER partners participated, including events related to Communication activities, presenting project results in wider audiences and the public, is included in D8.4 [2].

4 REPORT ON ACTIVITIES, OUTCOMES, AND FUTURE PLANS

In this section, we will report all the work done and the liaisons achieved under this task. In the next sections, we will describe what we finally achieved in each of the categories of targeted liaisons. In order to measure the success of the main liaison activities, we have set the following KPIs in the GA [1]:

Liaison with other projects	*"The SPIDER consortium will collaborate as much as possible with other ongoing projects accepted in the call to exploit opportunities for knowledge exchange and for improving dissemination among the target audience." [1]*	***Number of collaborations with other projects ≥ 2***	***Final number of active collaborations with other projects: 14***
Liaison with CERTs/CSIRTs network across the EU	*"The SPIDER consortium will strive to ensure collaboration and knowledge interchange with CERTs/CSIRTs. The communication will be achieved either via the creation of direct channels between projects or via the participation and collaboration of mandated SPIDER representatives to ECSO technical Working Groups (e.g., WG1, WG3, WG5, and WG6) and ENISA meetings." [1]*	***Number of collaborations with CERTs/CSIRTs networks across the EU ≥ 3***	***Finally organized workshops and knowledge transfer events: 3***

Table 2. Liaison KPIs as defined in SPIDER GA

The first KPI is both related to the task T8.4 and the dissemination task T8.1 and as such, it has been reported in the respective dissemination deliverables (D8.2 [31], D8.3 [32], and D8.4 [2]) while this deliverable focuses mostly on the second KPI concerning the liaison with the CERTs/CSIRTs community.

4.1 REPORT ON EU CERTS / CSIRTS LIAISON ACTIVITIES

As mentioned in Section 2, we identified twelve (12) CERTs/CSRITs established in EU, based on ENISA's Inventory [3] and one (1) global forum for incident responders. We sent out eleven (11) invitations, describing SPIDER proposition and our requesting their participation in SPIDER's liaison activities. Totally, six (6) organizations from four (4) countries decided to support the SPIDER project (FORTHcert is part of FORTH and no official invitation was sent). Table 3 presents the status of each invitation accompanied with some details on the dates of the communication and some brief explanation where needed. The Invitations that were sent are depicted in ANNEX I – EU CERTs/CSRITS events of this deliverable, as well as the file with the presentation of SPIDER that was shared, and the feedback received via an on-line questionnaire. SPIDER directly aimed to collaborate with teams and initiatives inside the EU, while reaching out to a broader audience was out of the scope of the project at this point.

Based on the final results, we have met the number of CERTs/CSIRTs needed to fulfil the Liaison activities KPI. We arranged a series of knowledge transfer events and hands-on workshops, further enhancing SPIDER's validation, exploitation, and sustainability activities, resulting to a mature product ready to reach the market and enhance 5G security throughout EU.

Full name	Country	Contacted on	Status(date)
GRNET-CERT	**Greece**	**29/09/2020**	Accepted (13/10/2020)
National CSIRT-CY	**Cyprus**	**29/09/2020**	Accepted (12/11/2020)
Hellenic Cyber Security Incident Response Team (CSIRT)	**Greece**	**29/09/2020**	Accepted (13/10/2020)
FORTHCert	**Greece**	**N/A**	Not contacted by default Accepted as part of FORTH
BU CERT	**UK**	**01/03/2021**	Accepted (01/04/2021)
CZ.NIC-CSIRT	**Czech Republic**	**01/04/2022**	Accepted (01/05/2022)
Greek National Authority Against Electronic Attacks	**Greece**	**29/09/2020**	No confirmation received
CERT POLSKA	**Poland**	**29/09/2020**	No confirmation received
CERT-EU	**European Union**	**29/09/2020**	No confirmation received
Computer Emergency Response Team Austria	**Austria**	**29/09/2020**	No confirmation received
CSIRTMalta	**Malta**	**29/09/2020**	No confirmation received
CSIRT.CZ	**Czech Republic**	**29/09/2020**	No confirmation received
NASK CSIRT, Nationally appointed CSIRT	**Poland**	**29/09/2020**	No confirmation received
Forum of Incident Response and Security Teams.	**Global Forum**	**N/A**	It was finally decided not to exploit this channel, due to lack of time to examine all the related legal issues of SPIDER usage outside EU

Table 3. EU CERTs/CSIRTs liaison status.

Thereupon, ***three (3) dedicated Workshops*** were organized during the various phases of the project, involving two workshops at an early stage of the implementation/integration activities, as well as a third one at the final phase of the project, where the most mature results were demonstrated. Table 4 summarizes the logistics of these workshops.

CERT/CSIRT	Country	Persons
1st workshop (21/04/2021)		
GRNET-CERT	Greece	1
National CSIRT-CY	Cyprus	1
Hellenic Cyber Security Incident Response Team (CSIRT)	Greece	2
BU CERT	UK	3
FORTHCert	Greece	1
2nd workshop (13/05/2021)		
GRNET-CERT	Greece	1
National CSIRT-CY	Cyprus	1
Hellenic Cyber Security Incident Response Team (CSIRT)	Greece	2
BU CERT	UK	1
FORTHCert	Greece	1
3rd workshop (26/05/2022)		
Hellenic Cyber Security Incident Response Team (CSIRT)	Greece	3
BU CERT	UK	3
CZ.NIC-CSIRT	Czech Republic	2

Table 4. EU CERTs/CSIRTs workshop logistics.

At the end of each event, there was a discussion session where the participants provided feedback for the main SPIDER activities and the potential collaboration with CERTs/CSIRTs communities. Attendees from the CERTs/CSIRTs answered a relevant on-line questionnaire. In general, the events made good impression to the participants. The *demo session* was the most interesting item that gained the most attention. Also, the attendees were interested in the *5G training scenarios*, the *underlying technical aspects*, as well as the *topic suggestions for CERTs particularities*. The detailed answers are mentioned in the Annex I.

Finally, it was agreed to maintain an open collaboration between SPIDER and the CERTs/CSIRTs teams, extending even beyond the lifecycle of the project (after M36). Also, these teams could act as potential future customers/users of the SPIDER platform, enhancing their internal training programmes concerning 5G security.

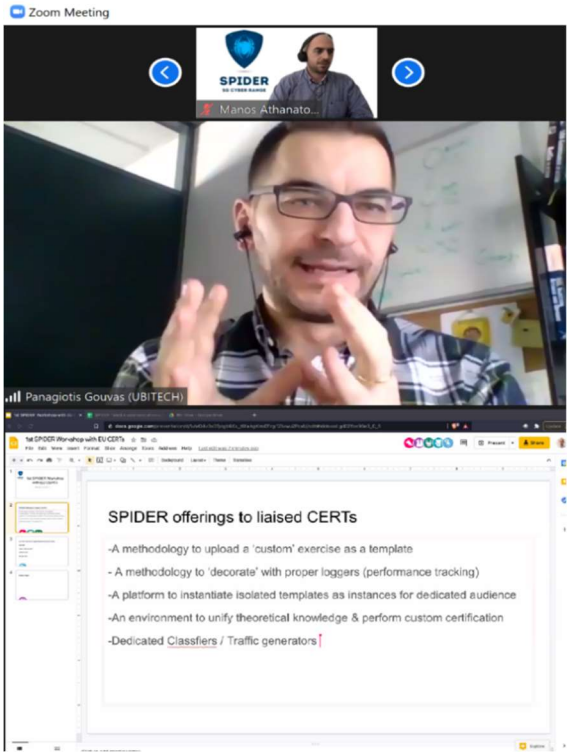


Figure 1. CERTs/CSIRTs workshops

4.2 REPORT ON SMES/PUBLIC SECTOR LIAISON ACTIVITIES

We identified a number of links that could be exploited throughout the lifespan of SPIDER in D8.6. Once the Beta release of SPIDER became available, we exploited these liaison links to further promote the technical advances and capabilities developed in SPIDER to the SME community and Public sector, providing a compelling offer for enhancing their security awareness of the 5G sector.

The aforementioned links are also utilised by the standardisation, dissemination, and exploitation tasks of the project, insuring interoperability, and coordination between all tasks under WP8.

4.2.1 Report on SMEs liaison activities

The main result of this activity was the organization of a **knowledge transfer event** for **8 SMEs**. The event took place at **05/05/2022** and the following companies were finally joined:

1. [Germany] Social Engineering Academy – https://socialengineeracademy.com/
2. [UK & Germany] AEGIS IT Research – https://aegisresearch.eu/
3. [Belgium] Focal Point – https://focalpoint-sprl.be/
4. [Portugal] PDMFC – https://www.pdmfc.com/
5. [Greece] Information Technology for Market Leadership (ITML) – https://itml.gr/
6. [Greece] Zelus – https://www.zelus.gr/
7. [Greece] Synelixis – https://synelixis.com/
8. [Czechia] CZ.NIC – https://www.nic.cz/

Also, the following 4 other SMEs did not manage to join eventually:

1. [Germany] SimPlan AG – https://www.simplan.de/en/
2. [Portugal] SONAE MC – https://mc.sonae.pt/
3. [Greece] Optimum – https://www.optimum.gr/el/
4. [Slovenia] XLAB – https://www.xlab.si/

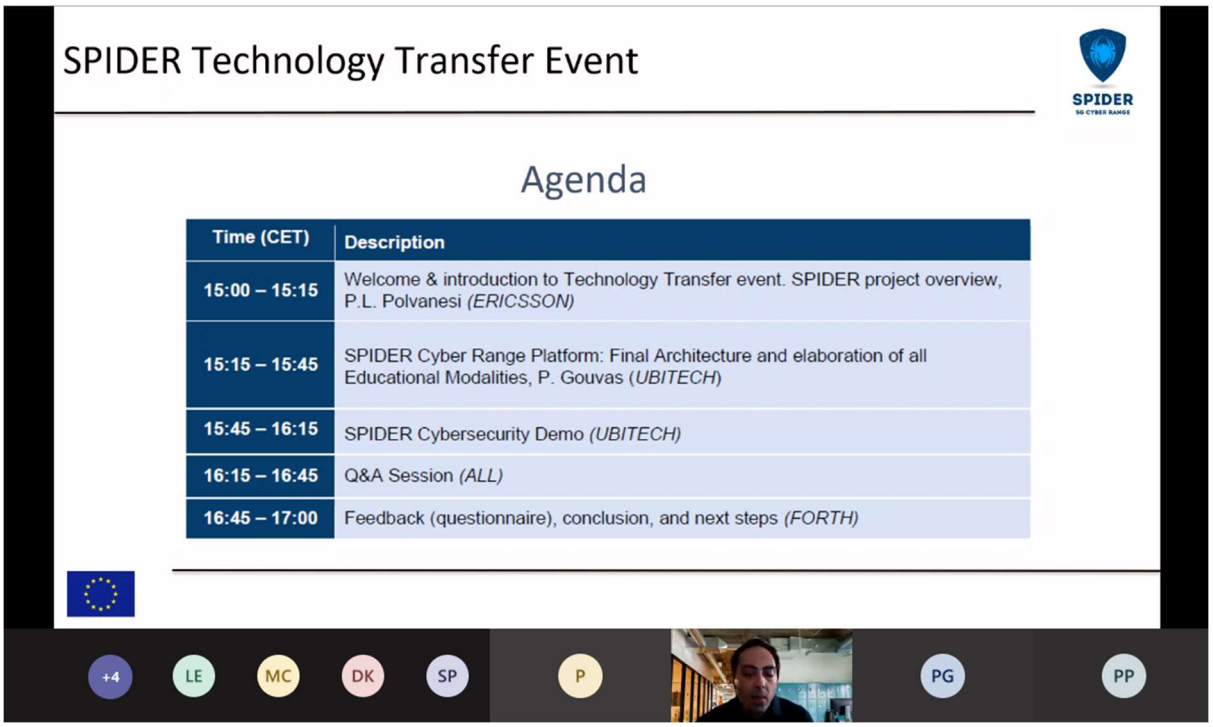


Figure 2. SMEs Knowledge Transfer event

At the end of the main presentation/demonstration, there was a discussion session where the participants had the chance to provide feedback for the main SPIDER activities. Moreover, 11 attendees from the SMEs answer a related on-line questionnaire. In general, the event made good impression to the participants. The overall *5G scenarios* was the most interesting item that gained the most attention. Also, the attendees were interested in the *seamless scenario creation*, the *platform itself*, the *serious gaming* part, as well as the *continuous risk assessment methodology*. The detailed answers are mentioned in the ANNEX II – SMEs event.

Finally, participants from the involved SMEs expressed their interest in retaining communication and get informed periodically concerning SPIDER progress and updates. Some of them could be also actively involved in the potential exploitation of the platform after the end of the project, acting either as additional technical partners or customers.

4.2.2 Report on Public Sector liaison activities

The SPIDER project participated in several liaison activities with Public bodies, mainly with ECSO and ENISA. In particular, SPIDER members participated in the EU-ISACs Conference. In this Kick-Off meeting of EU-ISACs community, 179 participants from 34 countries were present, holding a conference online allowing broad discussions on the topic of Information Sharing and Analysis Centres (ISACs). In this conference, we were able to enhance our

knowledge on information sharing, identify the key stakeholders, EU parties, policies, and rationales to be included in the creation of the EU-ISACs community.

SPIDER also participated in the 9th ENISA-EC3 Workshop. It was privilege to get invited in this meeting as it allows to get in touch with numerous CERTs and look inside the CERT community. Moreover, we were able to see cybersecurity from the point of legal authorities and how the cybercrime is treated. More specifically, the changes and increases in cybercrime and how it has been affected by the coronavirus and teleworking were discussed. Various governmental CERTs presented information about the events detected by or reported to them. Discussions on the effects of attacks on information systems in the health sector were held. The new joint EU Cybersecurity unit was presented. Some information that will be in the new IOCTA 2020 report of Europol were presented. The cooperation scheme of ENISA with CERT-EU, the CSIRTs Network and the structures of the European Union was presented. The EU blueprint was introduced for the common European policy of responding to large-scale cyber-attacks. Special mention was also made of shifting our focus from the various assets to the human factor in a cyber-attack.

SPIDER also supported the ENISA's *6th Network and Information Security (NIS'19) Summer School*, which took place in Crete in September 2019. The special theme for this year was "Security Challenges of Emerging Technologies". Towards this objective, ENISA and FORTH, brought together to this Summer School a distinguished faculty from around the world with the purpose to identify current trends, threats, and opportunities against the background of recent advances on NIS measures and policies. The SPIDER project was included -among other projects in the event flyer that was disseminated in the NIS'19 summer-school and was enlisted among the event sponsors.

Figure 3. ENISA NIS summer school

Due to COVID-19 restrictions, this was the last time that this event took place. Therefore, SPIDER supported the cyber security summer school CyberHOT, which is mentioned in the subsection 4.4.2.

4.3 REPORT ON LIAISON ACTIVITIES WITH EU PROJECTS AND ACADEMIA

The initial list of identified projects is presented in D8.6. Overall, we have identified around twenty (20) related projects; in fifteen (16) of them, partners from SPIDER's consortium are also full partners in the respective project creating a directly communication and collaboration link when possible.

4.3.1 Joint activities with projects from CONCORDIA Project Group

SPIDER project has been a member of CONCORDIA Project Group (PG) in Horizon Results Booster [29] since July 2021. Through CONCORDIA PG, SPIDER made use of two modules from Service: Portfolio Dissemination & Exploitation Strategy, namely Module A: "Identifying and creating the portfolio of R&I project results" and Module B: "Helping projects from the portfolio to design and execute a portfolio dissemination plan" [30]. Apart from SPIDER, projects CONCORDIA [33] and FORESIGHT [34] are members of the PG. Joining forces for all three projects, along with the support of the experts appointed from HRB, led to a fruitful collaboration that had a positive impact in implementing joint activities which reached a wider audience of targeted stakeholders.

The outcome of Module A concerned the availability of the *"Portfolio Dissemination and Exploitation Strategy (PDES)"* which identifies the collective results of the PG to be disseminated, their characteristics and the target stakeholders that can benefit from these results and are ultimately the target audience for the PG dissemination activities. The main objectives of the various projects that served in the PG dissemination effort are:

- Objective 1 - Increase awareness of the PG results.
- Objective 2 - Identify stakeholders potentially interested in the project and its outcomes, engage them in the projects' activities and encourage them to regularly interact with the involved projects.
- Objective 3 - Find new ways of dissemination to mitigate COVID-19 restrictions and ensure an effective engagement.

The portfolio, following an in-depth analysis of the Project Group, provided the following conclusions/recommendations:

1. The PG's results deliver innovations in the field of the cybersecurity training sector, especially dealing with cyber ranges.
2. The PG's stakeholders are, by order of priority:
    a. Industry and Security professionals.
    b. Research and Academia.
3. The barriers to dissemination are:
    a. Disseminating the PG results in a way that they can stand out from the oversaturated cyber security stream of information.

   b. Mitigating the negative effect of COVID-19 on dissemination and stakeholder engagement.
4. The recommended dissemination channels to be used by the PG to reach its newly identified common stakeholders are:
   a. The organisation of digital events with a practical hands-on approach.
   b. The Dissemination Network proposed by the experts to support the PG to structure its community targets and define its virtual engagement plan.

Project members of CONCORDIA PG followed the recommendations of experts and opted for Module B, so they proceeded with joint dissemination activities to reach all identified common stakeholders. In this framework, the following joint activities took place:

1. Joint information flyer, published and circulated in March 2022 (Available at SPIDER website [35]).
2. Joint short promo video in the form of video pill, produced and published in April 2022 (Available at SPIDER's YouTube channel [36]).
3. Organisation and planning of a joint webinar entitled "Training the European workforce of tomorrow: cyber ranges in practice", which took place virtually on May 17th, 2022. In total, 89 attendees from 27 countries participated from various technological backgrounds, most of them having some knowledge of Cyber Ranges. The event has been moderated by ECSO and hands on training presentations were given by representatives from all three projects of the PG. More information on the event can be found in ANNEX III – CONCORDIA PG JOINT EVENT. Additionally, the related dissemination material are presented in D8.4 [2].

Figure 4. Joint webinar "Training the European workforce of tomorrow: cyber ranges in practice"

4.3.2 The Cyber-Range Network

We established the "Cyber-Range Network" [38] which is a collaborative initiative/platform created jointly from three EU funded projects: FORESIGHT (GA# 833673), Cyber-MAR (GA# 833389) and SPIDER with the aim of: (i) promoting collaboration and to facilitate exchange of knowledge among them; (ii) showcasing their respective project results to a wider audience; (iii) performing joint dissemination activities; (iv) improving overall awareness regarding cybersecurity preparedness and cybersecurity training. In order to kick start these joint activities, a joint webinar was held on November 26th where the three projects were introduced along with their key objectives and the current progress. Additionally, the concept of cyber-ranges as virtual training environments and how they can be used for

cyber warfare was presented. Furthermore, a Q&A session with the webinar participants was held exchanging views and clarifying future collaboration plans. Finally, in the wider context of the organisation of this webinar, through the communications of the three projects, future collaboration activities' plans were discussed and agreed upon.

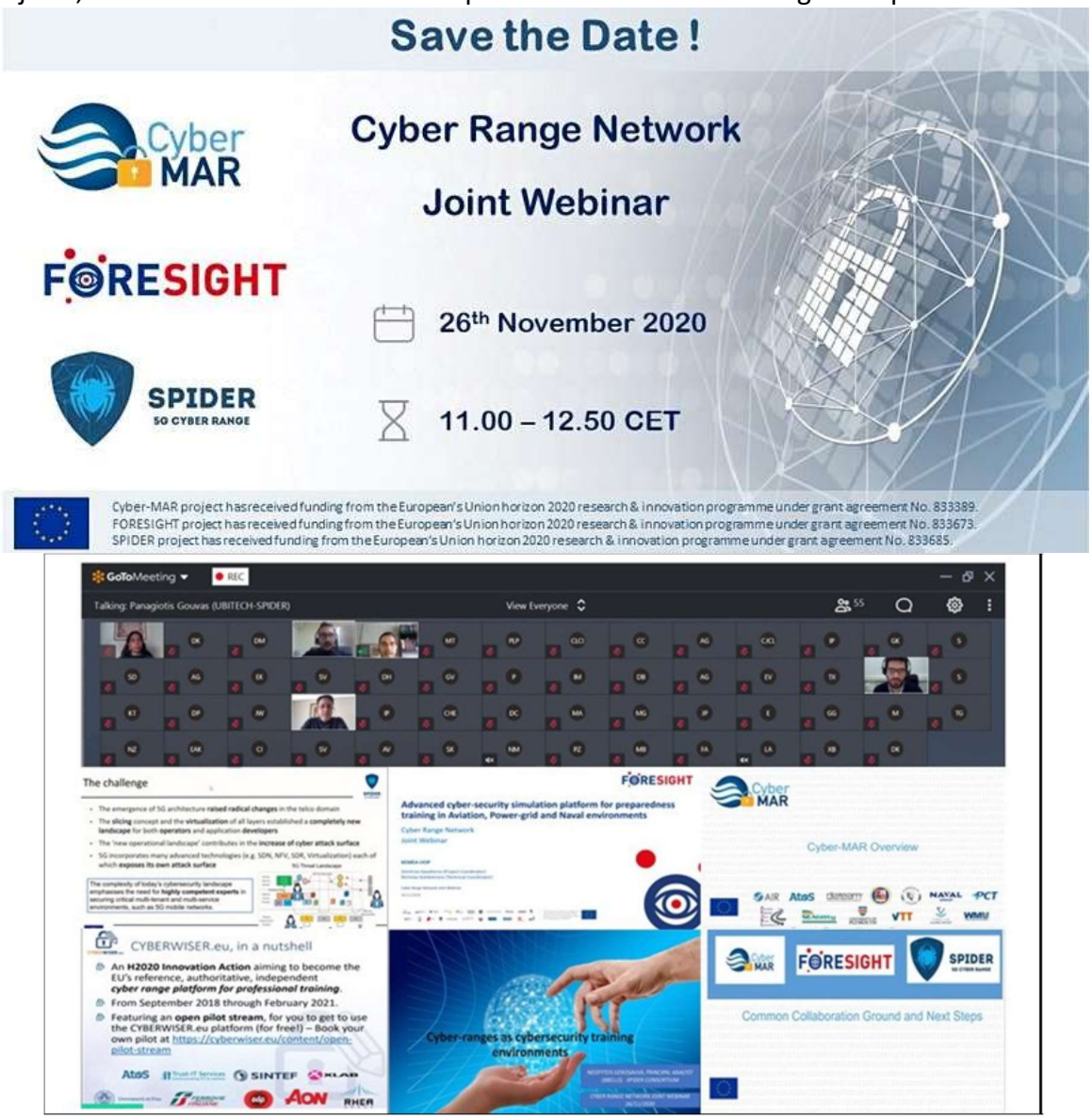


Figure 5. Cyber Range Network and online Webinar

4.3.3 Federation of cyber-range platforms

SPIDER has initiated a collaboration with THREAT-ARREST (GA# 786890) which is also developing a general-purpose Cyber Range. The collaboration has started in July 2020 with the aim to provide a common output concerning the Cyber Ranges and their Models. The output of this collaborative activity will be provided as input to the cyber range activities of the EU Cybersecurity pilot project CONCORDIA (GA# 830927). An early presentation of the SPIDER project has been provided to CONCORDIA project in September 2020 including technical discussion on the *"A modelling of the training activities for Cyber Ranges"*. The main goal is to design a ***unified way to design and populate training scenarios*** among the three cyber-ranges platforms. From the technical point of view, all three solutions are using

OpenStack to produce virtual environments for cyber-ranges training. The emulated components for a specific scenario are defined as Virtual Machines (VMs). Thus, the three projects are close to an agreement of defining a common model for: i) the scenario description, ii) the instantiation of a relevant virtual environment with emulates components and pre-installed software modules, and iii) the automated evaluation of the trainee with on-line questionnaires.

Figure 6. Collaboration towards the technical federation between SPIDER, THREAT-ARREST, KYPO (CONCORDIA)

4.3.4 The joint IEEE Cyber Ranges and Security Training (CRST) workshop

Another main outcome of these collaborations was the co-organization of a dedicated joint workshop for cyber-ranges and security training. This is the *'Cyber Ranges and Security Training (CRST)' workshop* that has been co-located along with the conference *'IEEE International Conference on Cyber Security and Resilience (IEEE CSR)'* for 2021 and 2022. The two workshop iterations have been supported by SPIDER, THREAT-ARREST, FORESIGHT, CyberMAR, SPARTA, ECHO, CyberSec4Europe, CONCORDIA, and SECANT.

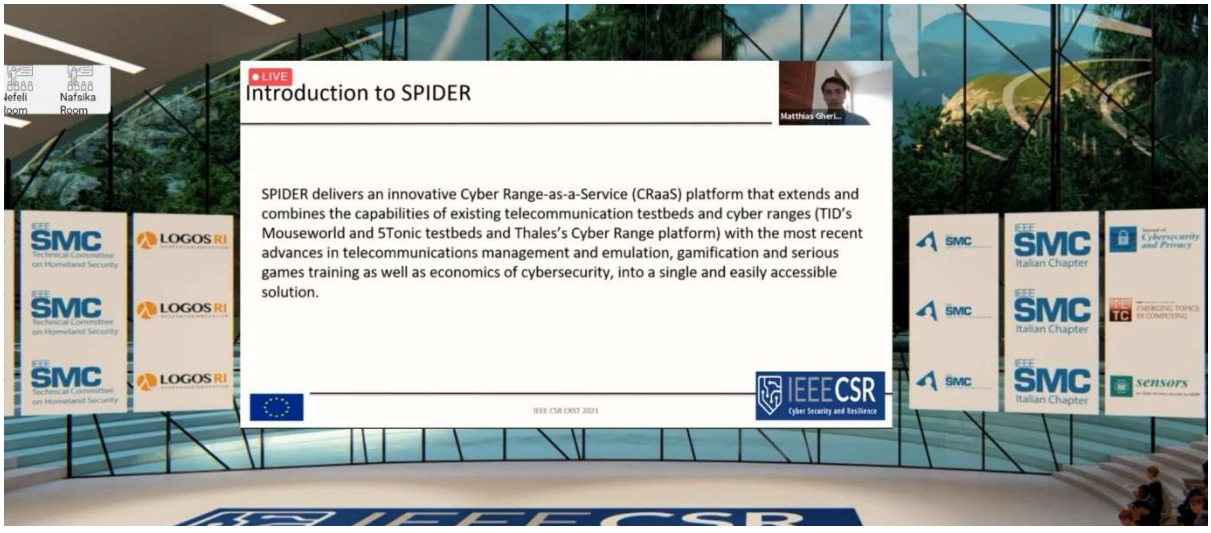


Figure 7. IEEE CSRT workshop – SPIDER presentation

4.3.5 Collaboration with 5G projects

Finally, through the participation in the events presented in Table 1 and D8.6, like 5G TECHRITORY [37], and exploitation of partners' internal connections, we had the opportunity to interact with projects developing solutions in the area of 5G, like 5GMED (GA# 951947), 5GCroCoCo (GA#825050), 5G-VINNI (GA# 815279), 5G-VICTORI (GA#

857201), and 5G-PICTURE (GA# 762057). Thereupon, we have had official and unofficial discussions with partners from these projects, and we were keen to participate in hands-on workshops, info days and other events involving SPIDER. Their aim is to exploit the capabilities offered by SPIDER to enhance their security awareness in developing their 5G solutions. Through, their participation in these liaison activities of SPIDER, we were able to receive valuable feedback on the developed platform and be more aligned with the requirements of the 5G community. Moreover, their involvement not only enhanced the validation of SPIDER but also amplified the exploitation, business, and dissemination activities of SPIDER. The liaisons created with these 5G projects were treated with the same way as the ones of the EU CERTs/CSIRTs, taking part in hands-on workshops, info days, and gaining access to the SPIDER platform.

4.3.6 The knowledge transfer event with the PANDORA-EDIDP project

The PANDORA-EDIDP project aims at contributing to the EU cyber defence capacity building, by designing and implementing an open technical solution for real-time threat hunting and incident response, focusing on endpoint protection, as well as information sharing. The PANDORA-EDIDP system aims also to promptly detect and classify known and unknown threats, enforce policies on-the-fly to counter these threats, and also exchange threat intelligence information with third parties, at both national and international level.

A targeted working session took place where it was demonstrated the technologies of SPIDER 5G Cyber Range and how these can support the operations of the PANDORA-EDIDP's consortium members, both as individual organizations and as the whole project. The event was attended by 22 persons. The attendees were interested about some *technical features of the SPIDER platform*, as well as the *5G scenarios*. They considered that the *gamification aspects* could be of interest to their project, and they also suggested that some of the *features should be provided as a service in the cloud*. The invitation and information sheet that were sent before the knowledge transfer event, as well as the detailed answers and feedback for the online questionnaires are presented in ANNEX IV – PANDORA-EDIDP Project event.

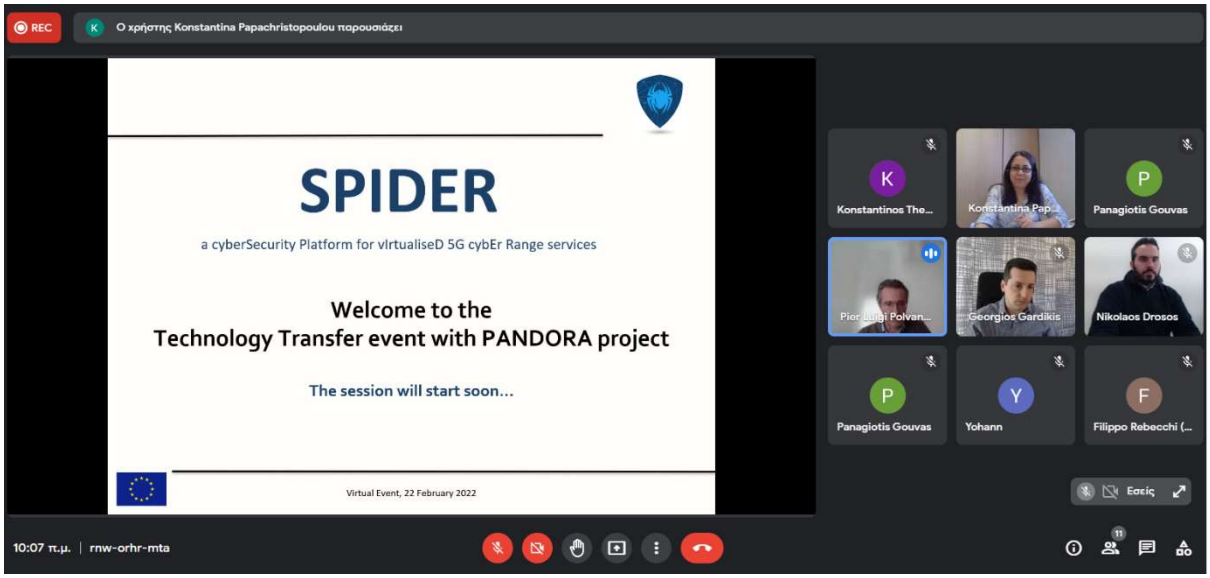


Figure 8. Knowledge transfer event for the EU project PANDORA-EDIDP

4.4 REPORTS ON OTHER STAKEHOLDERS' EVENTS

In this section, we are describing the rest events that partners from SPIDER participated and the outcomes of them in relation to creation liaison activities.

4.4.1 Liaison with the Hellenic Cyber Security Team

The Hellenic Cyber Security Team has close collaboration with UPRC. The team was engaged often in various SPIDER activities. At an early phase of the project, they assisted us in setting the validation aspects of the platform and extending the defined user requirements. Also, the team was engaged in the evaluation of the SPIDER platform during the last phase of the project by joining the cyber security experts training activities under WP7. Both the Hellenic Cyber Security Team and SPIDER members participated in the ICC event On June 2022.

Figure 9. Collaboration with the Hellenic Cyber Security Team

4.4.2 Support the CyberHOT summer school

The Cybersecurity Hands-On -Training (CyberHOT) Summer School took place on 27-28 of September 2021 under the auspices of NMIOTC. The 5th NMIOTC Cyber Security Conference in the Maritime Domain followed on 29-30 September 2021, where several of the attendees continued the collaboration there. The SPIDER project supported the organization of the summer school and members of the FORTH team had the chance to participate in the event.

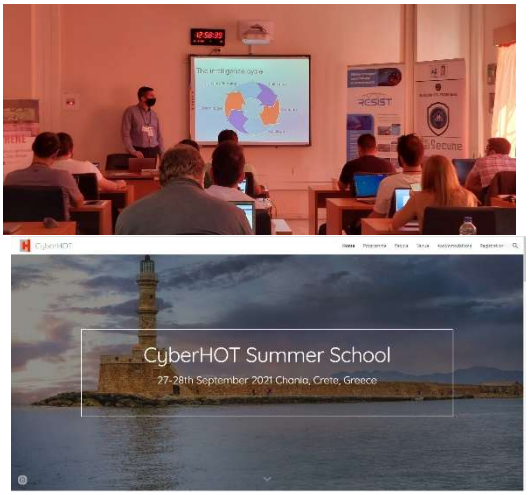


Figure 10. CyberHOT summer school

4.4.3 Participation in NATO's NMIOTIC conference

Every year NMIOTC holds its Annual Conference which aims at providing opportunities to discuss issues and share perceptions related to the contribution of the international community to improved security and in projecting stability and to path forward proposals and solutions in achieving enhanced Capabilities and Operational Effectiveness. In 2021, Prof. Sotiris Ioannidis presented "Cyber-ranges and security training for the maritime Sector" in the session of "Secure Maritime Value and Supply Chains, Infrastructures & Services". There, we had also the chance to check the proposed Cyber Range solution of THREAT-ARREST project, deepen our collaboration and discuss our common path for developing the models of training that are to be delivered to the CONCORDIA project.

Figure 11. NATO's NMIOTIC conference

4.4.4 Participation in OSM Ecosystem Research

In January 2022, SPIDER became part of the OSM Ecosystem Research. This was a main achievement of the technical efforts of the project. The consortium has decided to integrate the ETSI OSM framework and orchestrate scenarios deployments for different cybersecurity training and testing exercises. Moreover, OSM Ecosystem Days allows participating organizations to share their Open Source MANO experience and how OSM is helping them to accomplish their goals. In March, and OSM-MR#12 Ecosystem Day, SPIDER share its OSM experience, by demonstrating the platform to this audience. During these events,

presentations and demos cover a wide range of aspects from research activities in academia to production deployments and commercial initiatives, many of them focused on 5G and MEC use cases.

Figure 12. OSM Ecosystem Research

5 CONCLUSIONS

This document is the final report of *Task 8.4 "Liaison with Stakeholders and Creation of Operational Links with European CERTs/CSIRTs"*. With the participation of all involved partners, we managed to setup all the appropriate connection links and create active collaborations with various stakeholders, R&D and public sector initiatives, as well as many H2020 funded projects that allowed easily to fulfil the project objective and KPIs set by the Grant Agreement.

We have managed to get in touch with numerous CERTs/CSIRTs teams and we engaged six (6) of them in various project activities. Also, a cluster with eight (8) SMEs was set, promoting the SPIDER solution to the market. Through our partners and participation to well-known EU events, we got in contact with numerous EU projects (around 20), mostly from the fields of cyber-security and 5G, and engaged around fourteen (14) of them in various SPIDER's activities. We have active cooperation with a project developing a general-purpose cybersecurity cyber range (THREAT-ARREST) and the largest cybersecurity pilot project (CONCORDIA), designing a common roadmap towards technical federation of EU cyber-ranges platforms. We became part of the CONCORDIA PG where we have the chance to co-organize a webinar and further promote the project's results and collaborations. We have setup the "Cyber-Range Network" with CyberMAR and FORESIGHT projects and held a joint Webinar for cyber security training. A dedicated cyber-ranges workshop has been established under the conference IEEE CSR and is co-organized along with other eight (8) projects (THREAT-ARREST, FORESIGHT, CyberMAR, SPARTA, ECHO, CyberSec4Europe, CONCORDIA, and SECANT). Through our participation in 5G TECHRITORY, we got in contact with MWCapital Barcelona, two (2) additional 5G projects, and we have created links with five (5) 5G projects in total that took part in the hands-on workshops and webinars that followed concerning the SPIDER solution, providing valuable feedback to our consortium. Through a knowledge transfer event, the project PANDORA-EDIDP was also engaged, setting another potential opportunity for collaboration after the end of the project. Concerning training, except from the aforementioned webinars, we supported the organization of two summer schools by ENISA and NATO, respectively. One main technical liaison activity was the inclusion of SPIDER in the OSM Ecosystem Research. Finally, the consortium participated in several events that was organized by ECSO, ENISA, EOS, and NATO.

Based on all aforementioned activities, we were able to fully fulfil the objectives of the task creating a live ecosystem around the SPIDER project (including CERTs/CSRITs, SMEs, EU projects, as well as national and international organizations and initiatives) that can drive the longevity of the project, assisting in the promotion, validation, and exploitation of our project's outcomes.

6 REFERENCES

[1] Grant Agreement **NUMBER** 833685 — SPIDER

[2] SPIDER D8.4 "Final report on dissemination, communication, standardisation and exploitation", 2022

[3] ENISA CSIRT Inventory – "CSIRTs by Country - Interactive Map", https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[4] SPIDER D8.6 "Report on connections with stakeholders and European CERTs/CSIRTs - initial version", 2020

[5] PRAXI Network, https://praxinetwork.gr/en/

[6] Mobile World Capital Barcelona, https://mobileworldcapital.com/

[7] CYBERWISER.eu training event, https://www.cyberwiser.eu/content/effective-training-cybersecurity-new-era-staff-remotisation-6

[8] Report Seminar "Territory and infrastructures security in the digital age", https://www.polososia.siitscpa.it/en/news/653-report-seminar-territory-and-infrastructures-security-in-the-digital-age.html

[9] System of Systems and Intelligent Automation (SOSIA) Hub, https://www.polososia.siitscpa.it/en/

[10] EUCNC and 6G Summit, https://www.eucnc.eu/

[11] IEEE CSR Workshop on Cyber Ranges and Security Training (CRST), 2021, https://echonetwork.eu/2021-ieee-csr-workshop-on-cyber-ranges-and-security-training-crst/

[12] Cybersecurity Hands-On Training (CyberHOT) Summer School, https://www.cyberhot.eu/home

[13] CONCORDIA Open Door 2021 (COD2021), https://www.concordia-h2020.eu/news/concordia-open-door-cod2021-save-the-date/

[14] IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2021), https://camad2021.ieee-camad.org/

[15] Open Source MANO (OSM) Ecosystem Research, https://osm.etsi.org/wikipub/index.php/Research

[16] Security Research Event (SRE 2022), https://www.sre2022.eu/

[17] OSM-MR#12 Ecosystem Day, https://osm.etsi.org/wikipub/index.php/OSM-MR12_Ecosystem_Day

[18] European Security and Defence College (ESDC), https://issat.dcaf.ch/Share/People-Organisations/Organisations/European-Security-and-Defence-College-ESDC

[19] Promo video of CONCORDIA Project Group (PG), https://youtu.be/d_4hyiwB5ZQ

[20] 1st International workshop on Technologies for Network Twins (TNT 2022), https://sites.google.com/view/tnt-2022/home)(https://noms2022.ieee-noms.org/

[21] Layer123 Reunion 2022: Intelligent Network Automation Congress, https://congress.layer123.com/event/f6bbdefe-7441-4e9c-bcb8-9ae25cf1877b/websitePage:2baa15cf-2ef0-4cff-8004-47bbe0664a09

[22] ECSO's Cybersecurity Awareness Calendar – May 2022, https://ecs-org.eu/initiatives/cybersecurity-awareness-calendar

[23] "Training the European workforce of tomorrow: cyber ranges in practice" webinar, https://www.cyberwatching.eu/projects/1484/concordia/news-events/training-european-workforce-tomorrow-cyber-ranges-practice

[24] IETF 113 standardization meeting, https://datatracker.ietf.org/meeting/113/session/nmrg/#autoid-3

[25] 1st Open Annual Workshop on Future ICT, https://www.8bellsresearch.com/workshop/

[26] 1st International Workshop on Massive Digital Twins for the Computer-Networks Evolution (TwinNets 2022), http://www.twinnets22.unipi.it/

[27] 1st International Cybersecurity Challenge (ICC), Athens, Greece, June 2022, https://www.enisa.europa.eu/topics/cybersecurity-education/international-cybersecurity-challenge-icc

[28] IEEE CSR Workshop on Cyber Ranges and Security Training (CRST), 2022, https://www.ieee-csr.org/crst/

[29] Horizon Results Booster, https://www.horizonresultsbooster.eu/

[30] Horizon Results Booster > Service: Portfolio Dissemination & Exploitation Strategy, https://www.horizonresultsbooster.eu/ServicePacks/Details/6

[31] SPIDER D8.2 "Initial report on dissemination, communication, standardisation and exploitation", 2020

[32] SPIDER D8.3 "Interim report on dissemination, communication, standardisation and exploitation", 2021

[33] CONCORDIA Horizon 2020 Project, https://www.concordia-h2020.eu/

[34] FORESIGHT Horizon 2020 Project, https://foresight-h2020.eu/

[35] HRB CONCORDIA PG Joint Flyer, March 2022, https://spider-h2020.eu/wp-content/uploads/2022/04/hrb_concordia_flyer_web_mar2022.pdf

[36] Joint short promo video for CONCORDIA PG, https://youtu.be/d_4hyiwB5ZQ

[37] 5GTECHRITORY, 3rd-annual Baltic Sea Region 5G ecosystem forum, https://www.5gtechritory.com/

[38] Cyber Range Network, https://www.cyber-mar.eu/event/cyber-range-network-joint-webinar/

ANNEX I – EU CERTS/CSRITS EVENTS

INVITATION SENT TO EU CERTS/CSIRTS

SPIDER 5G CYBER RANGE

Dear «Name»,

*I am writing to invite **«organisation»** to participate in the creation of an operational link between your organization and "SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range"* [1] *EU-funded project. Through that link, we will be able to interact, cooperate and exchange valuable information for arising security threats, new tools and training material, with the focus on preventing future incidents and raising security awareness overall.*

*Moreover, being part of the **SPIDER** ecosystem will give you the chance to get updated with the major developments of **SPIDER** platform, test and provide valuable feedback that will assist us in the creation of the final **SPIDER 5G Cyber Range**.*

Please respond to this letter, via email, stating that you are interested in collaborating with our project and we can contact you, or any other contact person that you will provide, in the future for discussions and common collaborative actions.

On behalf of SPIDER Project,
Manos Athanatos,
athanat@ics.forth.gr

SPIDER Contact details:
Website: https://spider-h2020.eu/
Project Coordinator: **Pier Luigi Polvanesi**
e-mail: **pierluigi.polvanesi@ericsson.com**

[1] https://spider-h2020.eu/

SPIDER INFORMATION SENT TO EU CERTS/CSIRTS

SPIDER 5G CYBER RANGE

SPIDER: a cybersecurity Platform for virtualised 5G cyber Range

SPIDER 5G Cyber Range in a nutshell

SPIDER's proposed solution takes into account all relevant advancements and latest trends capitalizing on current state of the art in order to offer eventually a **synthetic and sophisticated war-gaming environment** that will provide to the training users the ability of playing the part either of the attacker either of the defender (following a red vs blue team format). The main features of the SPIDER solution include advanced simulation and emulation tools, novel training methods towards active learning as well as generation of improved risk analysis and econometric models based on real-time emulation of modern cyber-attacks. **The goal of SPIDER is to deliver a novel 5G cyber-range CRaaS platform** which targets 5G deployment and will be eventually in place to assist security professionals of various levels to enhance their skills being trained under realistic conditions.

The SPIDER platform will be in place offer to its intended users a digital gamified and serious game-based learning environment capable of training experts and non-experts.

SPIDER will offer two types of exercises:

i) **Self-paced exercises:** SPIDER implements self-paced exercises through the provision of a selection of Virtual Machines that will be loaded upon user-request. Each VM will be equipped with the appropriate tools and confirmation mechanisms in order to detect the progress and the proper completion of a specific cybersecurity exercise.

ii) **Team-based exercises** including Red Team vs. Blue Team exercises, Capture the Flag (CTF) competitions, King-of-the-Hill, Force-on-force exercises, etc. Through several different types of scenarios, players are required to both attack and defend network and infrastructure components by utilizing skills developed in the security challenges, and in a manner, that closely matches the real-world networks.

SPIDER's basic Functionalities

A basic characteristic of SPIDER is that it incorporates **both a simulation environment and an emulation environment**. The *Emulation environment* is used for hands-on exercises while the simulation is tailored to non-expert users. More specifically the emulation environment provides the ability to interact with a real 5G infrastructure spanning from the bare-metal to configured antennas while the *Simulation environment* is configured to execute virtual scenarios (also addressed as serious games) which are affected by the decisions of the trainees.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

SPIDER 5G CYBER RANGE

The combination of both environments delivers a unique value proposition which includes the automated performance tracking of trainees, the extraction of their learning gaps and the provision of self-paced educational material regarding theoretical concepts of security. Another basic feature of the SPIDER functionality is to provide the users with the capability of **predicting the evolution of cyber-threats and furthermore to analyse the associated economic impact** and cost that is brought with the respective attack.

SPIDER ARCHITECTURE[1]

The **SPIDER reference architecture** consists of a proper componentization along with proper interaction and dependency tracking among these components. The functional goals of SPIDER will be materialized by an integrated platform which will be "de-composed" in several architectural modules. The decomposition process by itself aims at the enhancement of conceptualization, the acceleration of development and the proper analysis of the entire platform.

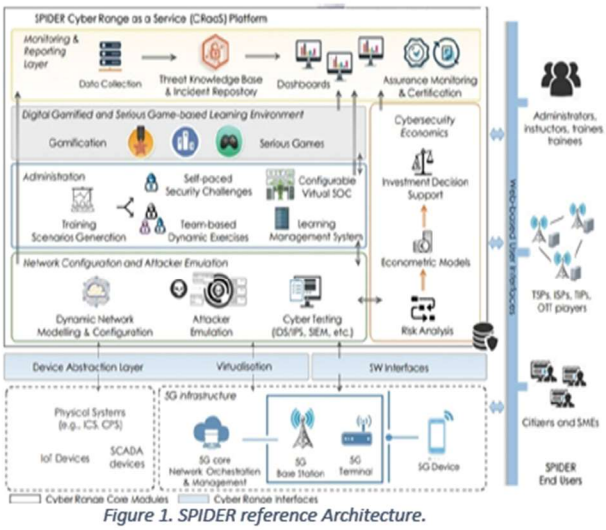


Figure 1. SPIDER reference Architecture.

The output of the componentization process resu different groups representing the various environments. These environments include: a) Emulation environment; b) Programmable 5G infrastructure; c) vSOC (Virtual Security Operations Centre) environment; d) Machine Learning Lab e) Simulation Environment and f) Operational Dashboards.

We could refer also to the Knowledge base component that monitors and keeps track of the various 5G asset types, vulnerabilities, potential threats etc, the Risk Calculation Engine component that calculates risks based on the given assets, asset relationships, vulnerabilities, controls and threat appetites , and the Decision Support component that selects the optimal cyber security investment strategy based on the calculated risks provided by the Risk Calculation Engine.

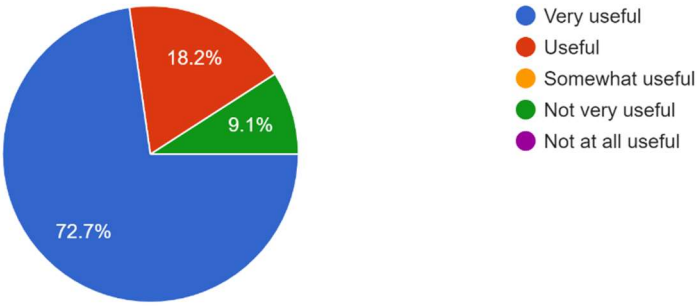
[1]"The SPIDER concept: A Cyber Range as a Service platform" - https://doi.org/10.5281/zenodo.4030473

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

QUESTIONNAIRE RESULTS FOR EU CERTS/CSIRTS

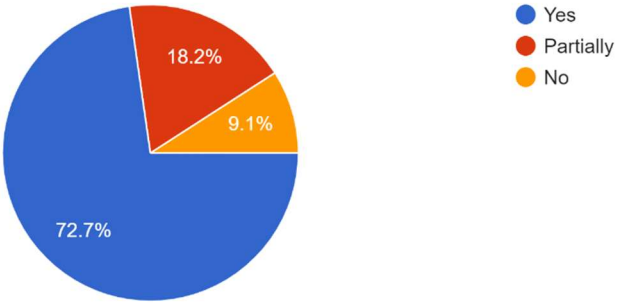
1. This workshop was

11 responses



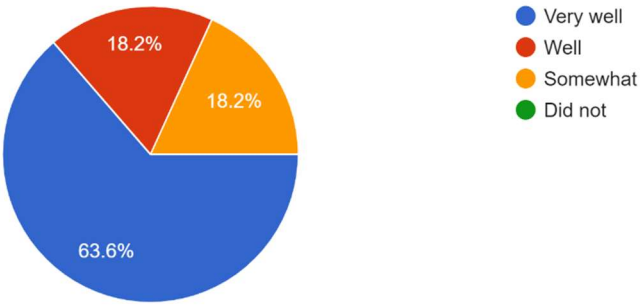
2. Were your expectations fulfilled?

11 responses



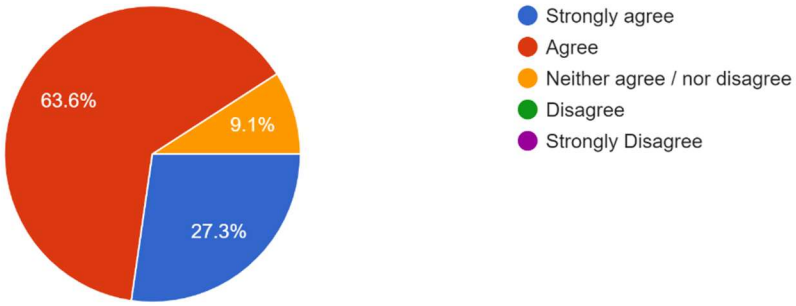
3. Did the organizers clearly explain the objectives of the workshop and sustain interest and participation of the group?

11 responses



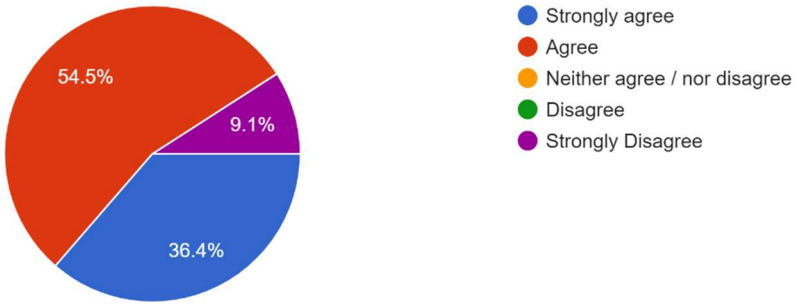
4. The presentations were explanatory and interesting

11 responses



5. The content of the workshop was relevant for you and your organisation?

11 responses



6. What was the best part of the workshop for you/ What did you liked more ?

10 responses

- The demo session
- Not thrilled on any part of it!
- The detailed presentation of the demos
- The training scenarios
- Topic suggestions by CERTs
- Technicalities
- DEMOS
- All the presentations were interesting
- The demo presentation on the first workshop

7. Do you have any suggestions for improvement?

4 responses

- -
- No, I am waiting for the actual CTF exercise
- An open access to the platform would be much appreciated
- Collaboration with other cyber-ranges or security training solutions

ANNEX II – SMEs EVENT

INVITATION SENT TO SMEs

SPIDER 5G CYBER RANGE — SMEs Technology Transfer Event

Invitation - Save the Date!

SPIDER Project is glad to invite you to a specialised Technology Transfer Event that will take place online, on **05/05/2022, at 15.00-17.00 CET**, via Teams teleconference platform.

What is SPIDER Project?

SPIDER's proposed solution takes into account all relevant advancements and latest trends capitalizing on current state of the art in order to offer eventually a **synthetic and sophisticated war-gaming environment** that will provide to the training users the ability of playing the part either of the attacker either of the defender (following a red vs blue team format). The main features of the SPIDER solution include advanced simulation and emulation tools, novel training methods towards active learning as well as generation of improved risk analysis and econometric models based on real-time emulation of modern cyber-attacks. **The goal of SPIDER is to deliver a novel 5G CyberRange-as-a-Service (CRaaS) platform** which targets 5G deployment and will be eventually in place to assist security professionals of various levels to enhance their skills being trained under realistic conditions.

What is the Technology Transfer Event about?

This virtual event is customized to meet the interests of SMEs, focusing on the presentation of SPIDER cyber range technologies. The aim is to introduce participants in the technology behind SPIDER, presenting the concept of cyber-ranges as virtual training environments and how they can be used for cyber warfare.

Who is the Target Audience?

The event is addressed to SMEs and end users. The event can be attended from stakeholders of all backgrounds that are interested in cybersecurity technological advancements.

Please mark your calendar with the SPIDER Technology Transfer Event. An invitation should have been sent to you. Otherwise, you can access the event directly via the link:
https://teams.microsoft.com/l/meetup-join/19%3ameeting_NTFhNik2ZTEtY2Y5Yi00ZGVmLWI1OWYtMik1MDc1ZmViOTM3%40thread.v2/0?context=%7b%22Tid%22%3a%22add98d93-11de-4dae-bd3a-3f2477c4d058%22%2c%22Oid%22%3a%226a064488-e59e-42b9-8232-210e2176dcbb%22%7d .
It will be a great honor for us to welcome you virtually on **05/05/2022**.

Additional information on the connection details will be sent to you, via email, prior to the event.

By entering the event, you confirm that you have read and agree with our Privacy Policy.

For more information on SPIDER project please visit:

- SPIDER Project website: https://spider-h2020.eu/
- A wealth of information on SPIDER technology in the form of publications (Research papers, Deliverables) can be found at: https://spider-h2020.eu/publications/
- Join us at LinkedIn, Twitter, Facebook, YouTube

Funded by the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

SPIDER INFORMATION SENT TO SMES

SPIDER 5G CYBER RANGE — SMEs Technology Transfer Event

Information Sheet

SPIDER: a cybersecurity Platform for virtualised 5G cyber-Range

SPIDER 5G Cyber Range in a nutshell

SPIDER's proposed solution takes into account all relevant advancements and latest trends capitalizing on current state of the art in order to offer eventually a synthetic and sophisticated war-gaming environment that will provide to the training users the ability of playing the part either of the attacker either of the defender (following a red vs blue team format). The main features of the SPIDER solution include advanced simulation and emulation tools, novel training methods towards active learning as well as generation of improved risk analysis and econometric models based on real-time emulation of modern cyber-attacks. The goal of SPIDER is to deliver a novel 5G CyberRange-as-a-Service (CRaaS) platform which targets 5G deployment and will be eventually in place to assist security professionals of various levels to enhance their skills being trained under realistic conditions.

SPIDER's Basic Functionalities

A basic characteristic of SPIDER is that it incorporates both a simulation environment and an emulation environment. The *Emulation environment* is used for hands-on exercises while the simulation is tailored to non-expert users. More specifically the emulation environment provides the ability to interact with a real 5G infrastructure spanning from the bare-metal to configured antennas while the *Simulation environment* is configured to execute virtual scenarios (also addressed as serious games) which are affected by the decisions of the trainees. The combination of both environments delivers a unique value proposition which includes the automated performance tracking of trainees, the extraction of their learning gaps and the provision of self-paced educational material regarding theoretical concepts of security. Another basic feature of the SPIDER functionality is to provide the users with the capability of predicting the evolution of cyber-threats and furthermore to analyse the associated economic impact and cost that is brought with the respective attack.

SPIDER Architecture

The SPIDER reference architecture consists of a proper componentization along with proper interaction and dependency tracking among these components. The functional goals of SPIDER will be materialized by an integrated platform which will be "de-composed" in several architectural modules. The decomposition process by itself aims at the enhancement of conceptualization, the acceleration of development and the proper analysis of the entire platform.

The output of the componentization process resulted on 19 distinct components that were aggregated in different groups representing the various environments. These environments include: a) Emulation environment; b) Programmable 5G infrastructure; c) vSOC (Virtual Security Operations Centre) environment; d) Machine Learning Lab e) Simulation Environment and f) Operational Dashboards.

We could refer also to the Knowledge base component that monitors and keeps track of the various 5G asset types, vulnerabilities, potential threats etc, the Risk Calculation Engine component that calculates risks based on the given assets, asset relationships, vulnerabilities, controls and threat appetites, and the Decision Support component that selects the optimal cyber security investment strategy based on the calculated risks provided by the Risk Calculation Engine.

Example Demonstration Scenario

SPIDER 5G CYBER RANGE — SMEs Technology Transfer Event

SMS overhearing on a vulnerable Operation Support System (OSS)

You belong to a black-hat hacking group that aims to disrupt the business of SPIDER Telecom organisation. Your group is conducting social engineering campaigns in order to bypass the security perimeter of the organisation. After many months your group has achieved to acquire a valuable reverse shell from an IT administrator of the organisation.

Your mission is to:

a) Explore the network visibility of this person and identify valuable assets that belong to the telco's OSS in order to find a vulnerability and try to penetrate in this asset as stealthy as possible (avoid bruteforce)
b) Perform privilege escalation in order to be able to intercept traffic from the access network
c) Intercept an SMS sent to user, and
d) Use the content of the SMS in order to unzip the encrypted zip file flag.zip that exists in the root filesystem of the OSS virtual machine.

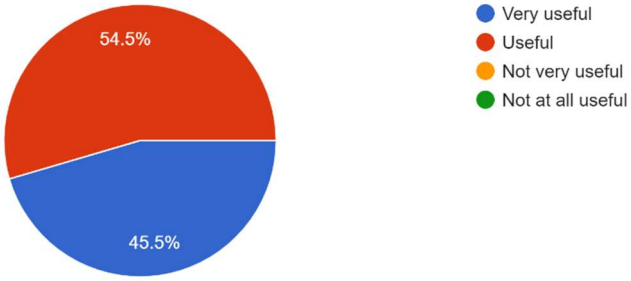
Funded by the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

QUESTIONNAIRE RESULTS FOR SMES

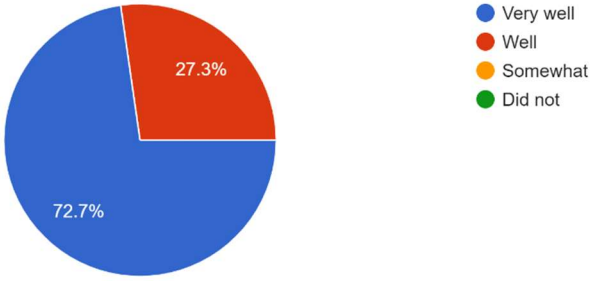
1. SPIDER Technology Transfer Event was

11 responses



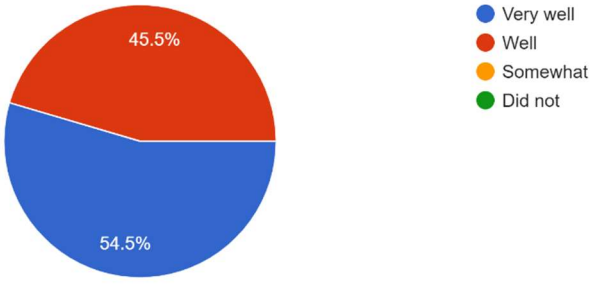
2. Did the organisers from SPIDER project clearly explain the objectives of the event?

11 responses



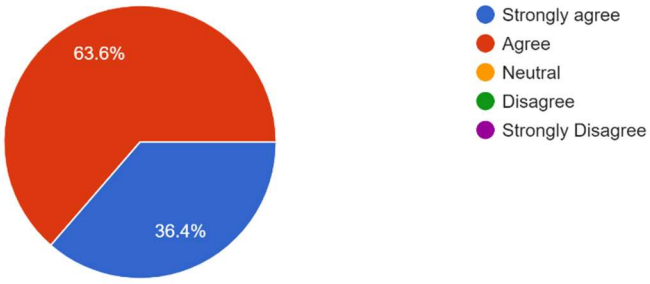
3. Did the organisers sustain interest and participation during the event?

11 responses



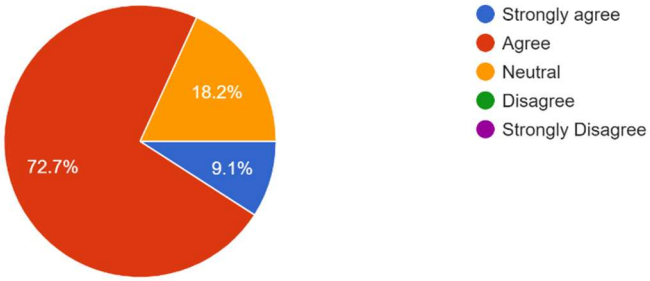
4. Technology presentation/ demonstration were explanatory and interesting?

11 responses



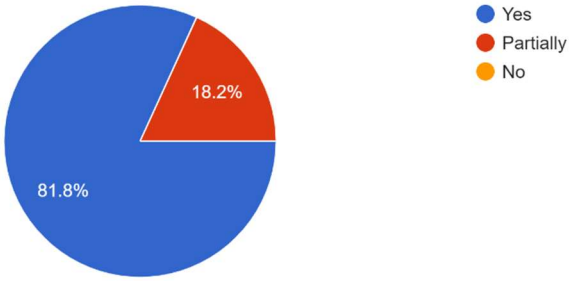
5. The content of the Technology Transfer event was relevant for you and your organisation?

11 responses



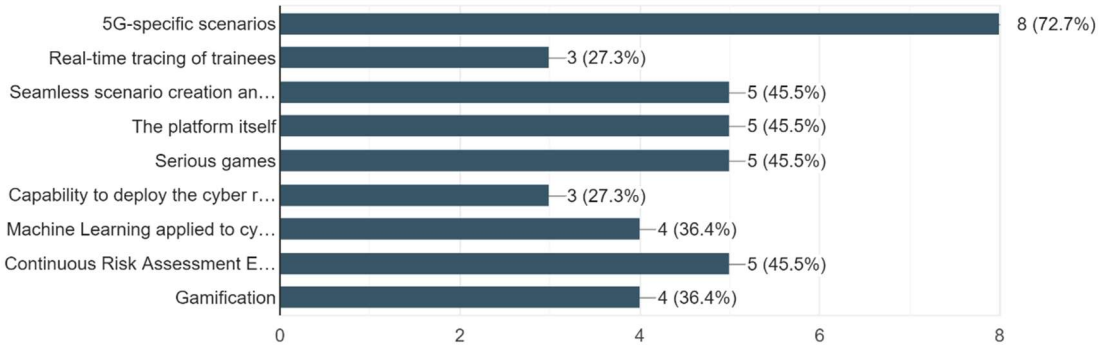
6. Were your expectations fulfilled?

11 responses



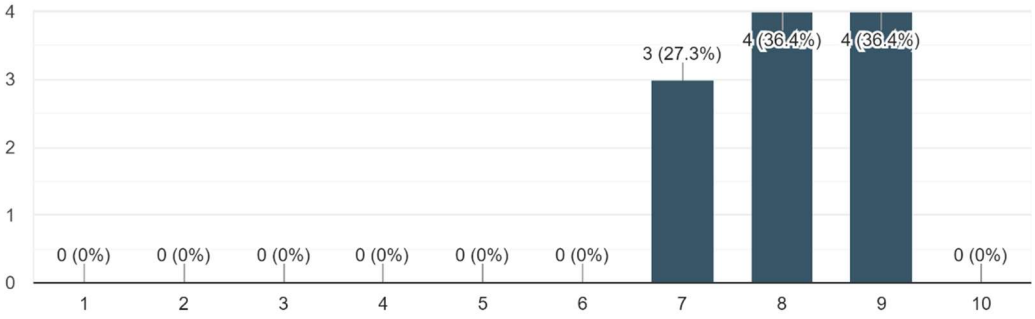
7. What do you think are the most innovative set of feature(s) of the SPIDER platform presented today?

11 responses



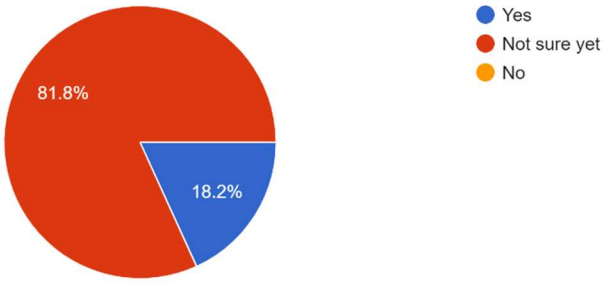
8. How likely is to suggest SPIDER Cyber Range to your peers?

11 responses



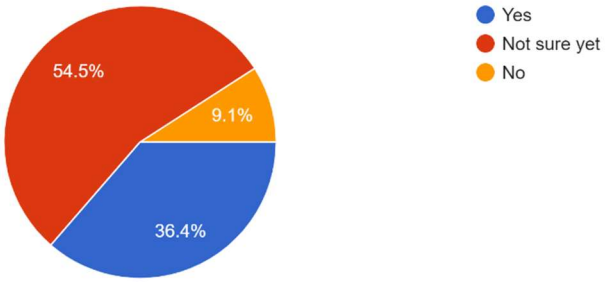
9. Do you plan to exploit SPIDER offerings within your organisation?

11 responses



10. Think about how cyber security awareness is taught in your current organisation, do you think a platform like SPIDER could be beneficial to improve the current situation?

11 responses



11. Why? please motivate your previous answer

6 responses

Not sure if there are cyber-security concerns related to 5G networks

We are not active within 5G.

We're not focused on 5G. Generally it's really difficult to provide such training tailored to each company requirements.

Because it provides close-to-real-life scenarios through an intuitive platform that can greatly enhance the 5G security knowledge of the personnel.

Could be beneficial since we don't have enough experience and information regarding 5G security scenarios.

I am not an expert, would have to consult with the experts in my team

12. Considering what you saw today (including the presentation, the demonstration, and the discussion), what could we improve to make the SPIDER platform better?

3 responses

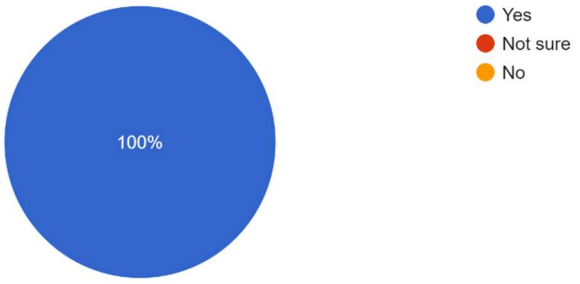
Change the password for user trainer in https://spider.euprojects.net/ login :)

Provide online open demos that anyone could play with the platform so that we could provide more precise feedback. Also more general security scenarios would be beneficial.

so far everything looked alright

12. Would you suggest similar events from SPIDER project to your peers?

11 responses



ANNEX III – CONCORDIA PG JOINT EVENT

Permanent website address, including the event announcement, the agenda, the available presentations, and the webinar recording is available at https://www.cyberwatching.eu/projects/1484/concordia/news-events/training-european-workforce-tomorrow-cyber-ranges-practice

JOINT EVENT ANNOUNCEMENT

Context - A fast evolving cyber threat landscape

Over the past years, malicious cyber activity has evolved and substantially increased with the ongoing coronavirus pandemic and now the Ukraine crisis. Cyber criminals are taking advantage of this situation, constantly boosting their attacks to exploit vulnerabilities and flaws to acquire sensitive information, infiltrate private networks to steal data, or disrupt critical infrastructures.

As Europe is accelerating its path toward the shift to a digital economy, the need for cybersecurity skilled staff has never been higher.

A collaborative EU response

The last years have seen the development of a number of cyber range technologies, products, national and international initiatives to tackle the evolving cyberthreat landscape thanks to innovative but realistic forms of training to emulate real environments that fully replicate what can be faced in daily life.

The webinar focussed on a set of cyber ranges simulating realistic domain environments, equipment, infrastructures and data developed by three EC funded initiatives: CONCORDIA, SPIDER and FORESIGHT.

Each project presented current progress, best practices and technical insights together with a practical demonstration of the respective cyber ranges as virtual training environments and how they can be used to simulate cyber incidents and attacks so IT professionals can hone their skills and prepare for real-world circumstances.

Finally, a panel discussion moderated by ECSO looked at how Europe is bringing together different initiatives with the aim of tackling the cybersecurity skills gap and how R&I projects can play an active role producing practical tools and services to address it quickly and comprehensively.

Target Audience

Given that cybersecurity is not just an IT issue, the event will cater for both IT specialists and a wider audience including employees from all departments and at all levels of seniority.

Agenda

Duration (min)	Topic and Speaker
10:00 - 10:05	Introduction and framework overview | *Csaba Virag, Chair of Cyber Range Focus Group, ECSO*
10:05- 10:20	*ECSO WG5 and Cyber Range Focus Group activities | Csaba Virag, Chair of Cyber Range Focus Group, ECSO*
10:20- 10:40	*CONCORDIA Project - Development of open a cybersecurity training and exercise | Jakub Čegan, Masaryk University* The talk will demonstrate how to develop cybersecurity training and exercise. There are three key components needed. The platform. The basic building blocks. And the know-how. The first two are freely available. We can't easily give you the last one, but we can show you hints and tips during this talk. We also will show several success stories of exercises and training at the KYPO Cyber Range Platform. **Download the presentation**
10:40- 11:00	*Introducing a novel 5G specific Cyber Range: The case of SPIDER project | Panagiotis Gouvas, UBITECH* The presentation focuses on the main features of the SPIDER 5G CyberRange-as-a-Service solution, which includes advanced simulation and emulation tools and novel training methods towards active learning, aiming to assist security professionals of various levels to enhance their skills, being trained under realistic conditions.
11:00- 11:20	*FORESIGHT Project – Development of a federated cyber range platform and innovative training curricula | Nicholas Kolokotronis, University of the Peloponnese* This talk will provide a brief overview of the current advances in FORESIGHT project, final architecture and federation concept, functionalities and novel services, automation and integration with external platforms, as well as, training curricula and certification. **Download the presentation**
11:20- 11:50	Panel and Q&A | *All Speakers*
11:50- 12:00	End of Webinar

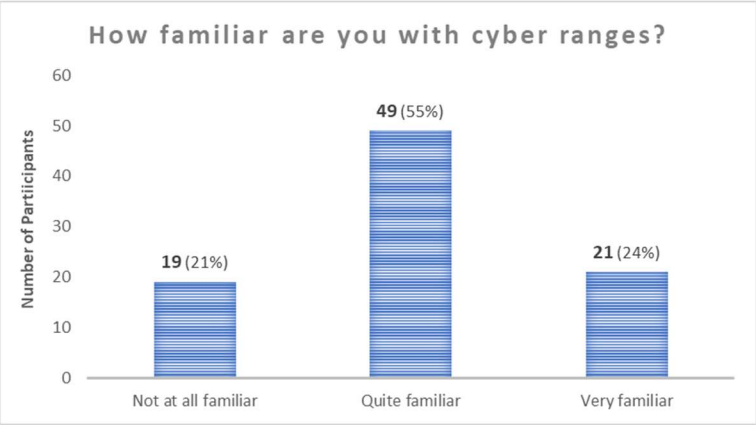
POST EVENT REPORT

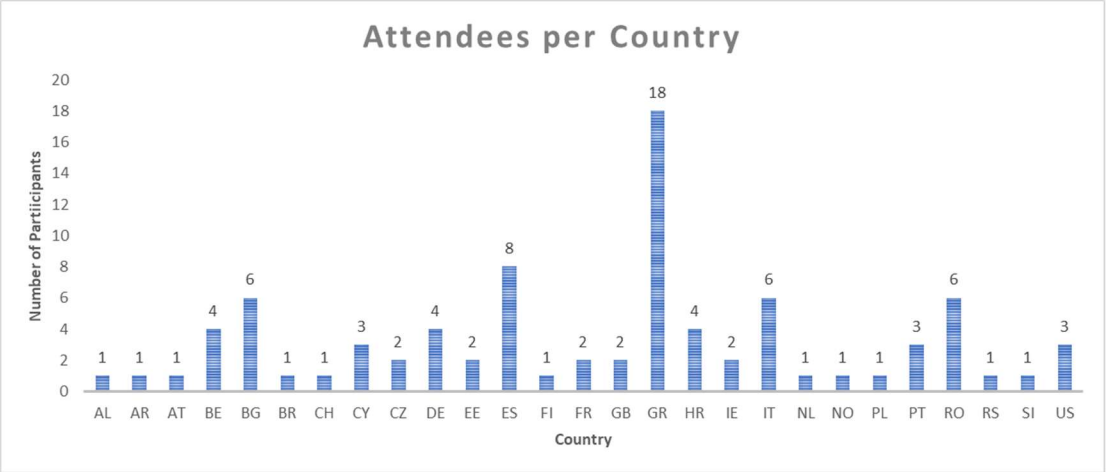
On 17 May 2022, CONCORDIA, SPIDER, and FORESIGHT, three EU projects advancing cyber ranges, came together under the umbrella of the European Commission's Horizon Results booster for a joint webinar showcasing their complementary results.

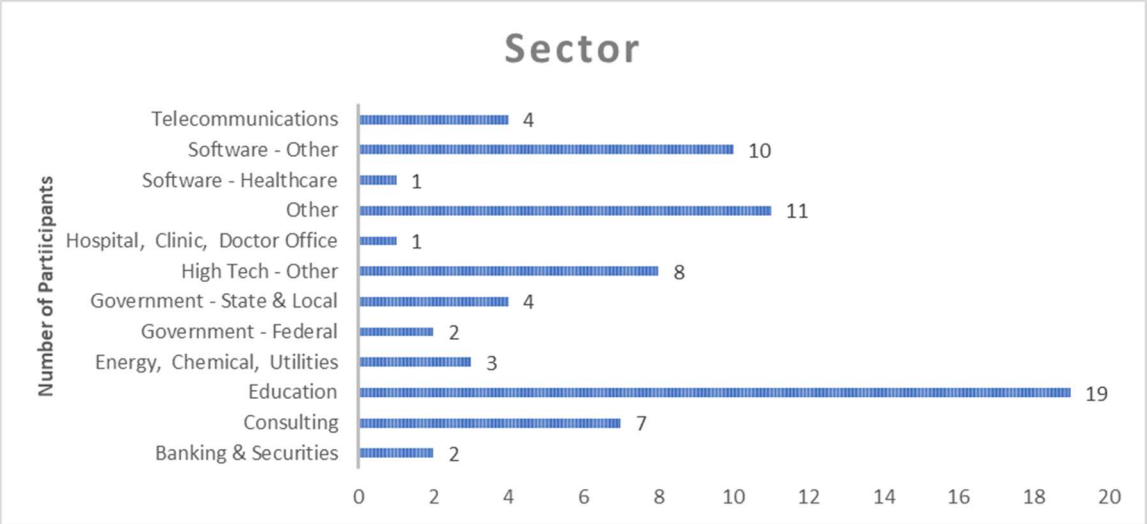
They were joined by Csaba Virag, cyber range expert, Director of Capacity Building at Talgen Cybersecurity and Chair of the Cyber Range Focus Group at the European Cyber Security Organisation (ECSO). He walked participants through actions the Focus Group is planning to implement, such as the set-up of a Cyber Range Alliance with a Best Practice Guide and Use Case Portfolio for academia. Another action is defining a benchmark with core competences and capabilities. He also highlighted the work within the European Union Agency for Cybersecurity (ENISA) in the human resource space, guiding organisations on cybersecurity from a training and skills perspective while also encouraging more women to get involved.

Csaba chaired this highly interactive webinar, which featured many questions from the audience, reflecting the high-level of interest in cyber ranges and their relevance in building resilience against a growing threat landscape.

During registration, attendees were asked a few questions for the organisers to understand their technological background and their knowledge about cyber ranges. A total of 89 participants, from 27 countries, attended the joint event, most of them being familiar with cyber ranges, coming from various sectors.




Attendees per Country
Number of Partiicipants
Country
AL AR AT BE BG BR CH CY CZ DE EE ES FI FR GB GR HR IE IT NL NO PL PT RO RS SI US
1 1 1 4 6 1 1 3 2 4 2 8 1 2 2 18 4 2 6 1 1 1 3 6 1 1 3


Sector
Number of Partiicipants
Telecommunications 4
Software - Other 10
Software - Healthcare 1
Other 11
Hospital, Clinic, Doctor Office 1
High Tech - Other 8
Government - State & Local 4
Government - Federal 2
Energy, Chemical, Utilities 3
Education 19
Consulting 7
Banking & Securities 2

TAKEAWAYS FROM PANEL DISCUSSION

Advances in cyber ranges – user perspective, open source, and federation

The CONCORDIA user-driven approach revolves around the use of Open Source (OS). On top of this, it is essential to build a community to enable us to be on a par with commercial solutions. SPIDER brings together users both virtually and physically as some exercises can only be performed with dedicated equipment. Repopulating and open sourcing some complex attacks can amplify the advances of the SPIDER platform. FORESIGHT combines the unifying benefits of federation, system definition and trainee evaluation The FORESIGHT OS approach means other platforms can join. SPIDER combines end-to-end virtualised scenarios and open-source approaches for critical mass with no obligation to be bound to the platform. The open format used in CONCORDIA, centres on using the same language and technologies rather than a fully-fledged federated approach.

The evolution of cyber ranges – an EU funding perspective

For CONCORDIA, service definition at federation level is a key evolution. More enabling technologies like blockchain, machine learning (ML) and artificial intelligence (IA) will need supporting moving forward. From a SPIDER perspective, the competitor analysis has been a constant during the project, checking for gaps. There are monetisation opportunities from the use of cyber ranges and physically-based exercises (hybrid formats), such as in water management systems complemented with virtual models. In terms of simulating network slicing and being specifically directed at the telecommunications sector, SPIDER is one step ahead of the competition.

Making content creation easier, faster, and more flexible

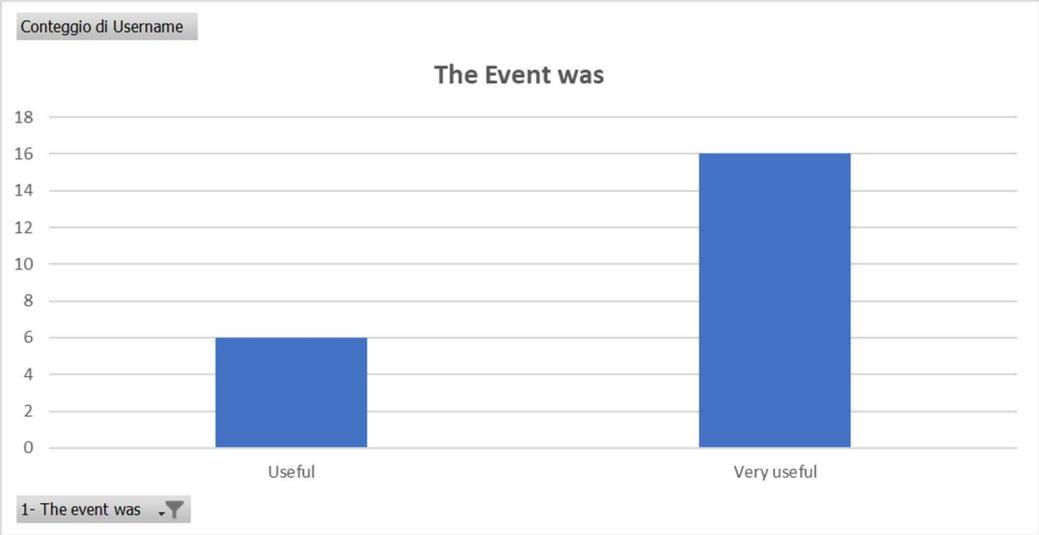
Being ahead of the knowledge accumulated by attackers is essential. This is especially true for content creators, techniques, and meeting trainee exercise needs, which all need to be updatable in as little time as possible. A key requirement moving forward is therefore ensuring we have enough skilled specialists able to create content on the highly multi-faceted topic of cybersecurity. Without this it will be hard to stay ahead of cyber attackers and keep up with the growing demand. Another essential requirement is having real interoperability across cyber ranges to ensure exercises are transferrable.

Envisioning future market development and how to achieve it

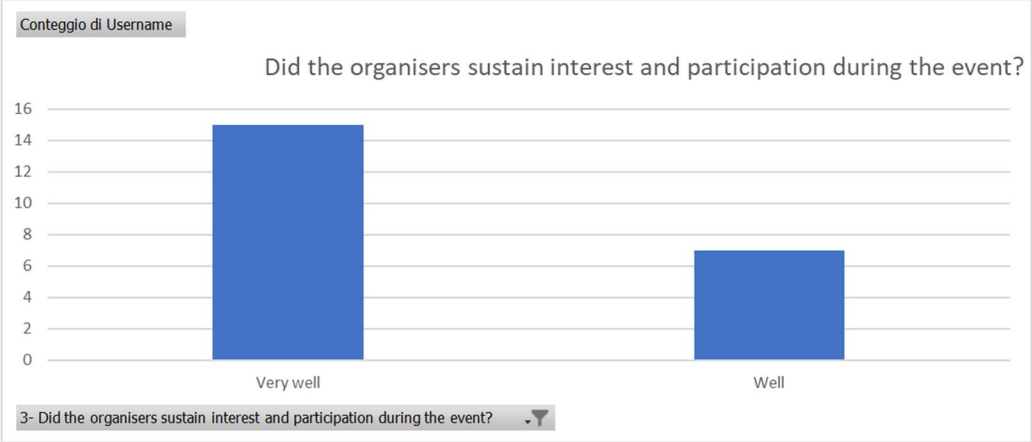
SPIDER highlights two key directions in the future hybrid and interplay of cyber physical aspects. From a booming of virtualised cyber ranges to a flourishing of hybrid cyber ranges, where the interplay with physical objects will practically be mandatory. Tackling the skills gap will be a real driver towards the growth in hybrid models. CONCORDIA sees a lot of growth in terms of specialisation with a separation of cyber ranges and scenario development. Hence training and exercises will be on software within the cyber range with organisations covering the development of single scenarios. It is important that cyber ranges are available to SMEs and European Member States. FORESIGHT believes we will witness a move to specialised solutions, available to a wider range of cybersecurity professionals. The use of Digital Twins will also help broaden the use of cyber ranges.

QUESTIONNAIRE RESULTS FOR CONCORDIA PG

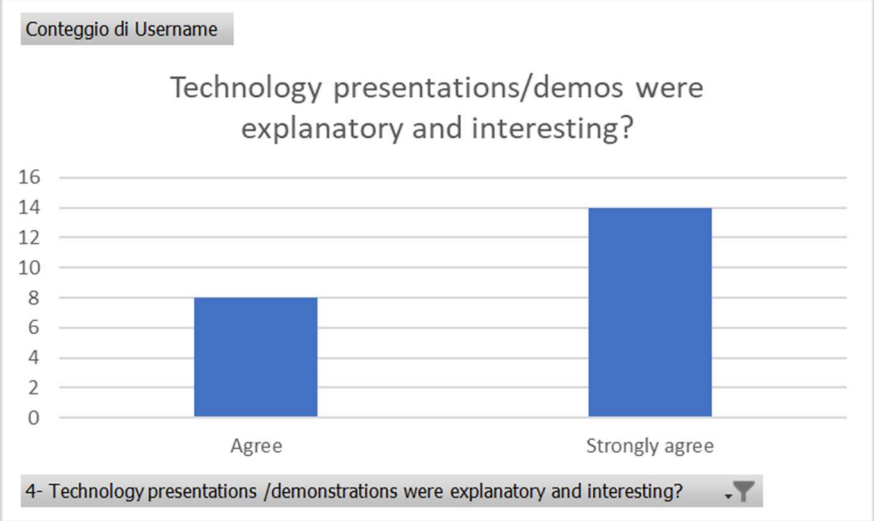
Q1 The Event was



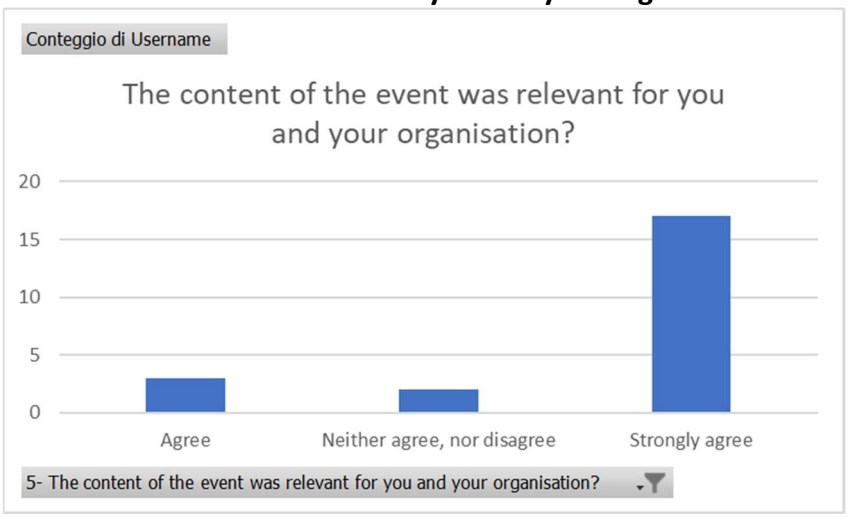
Q2 Did the organisers sustain interest and participation during the event?



Q3 Technology presentations/demos were explanatory and interesting?

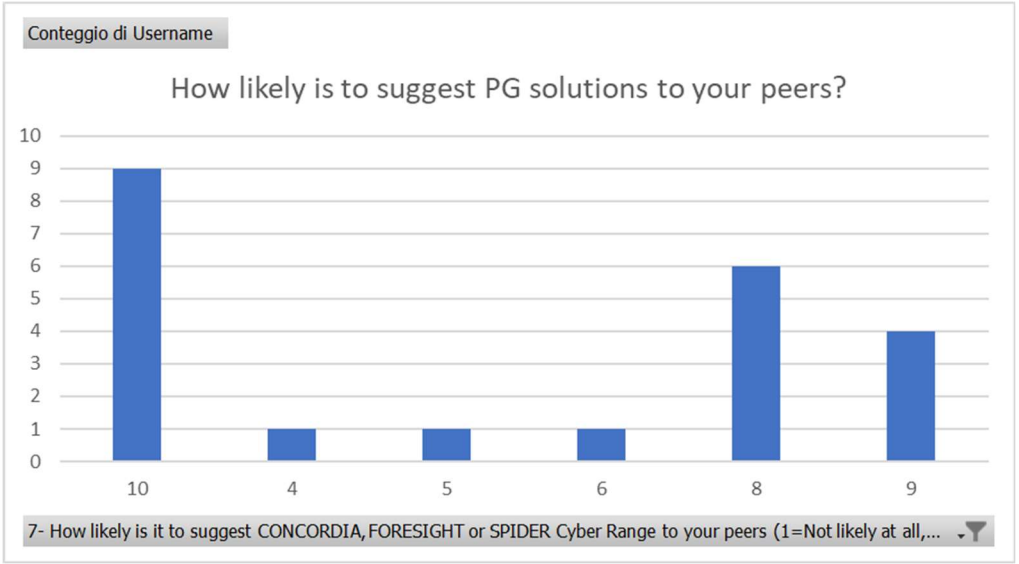


Q4 The content of the event was relevant for you and your organisation?

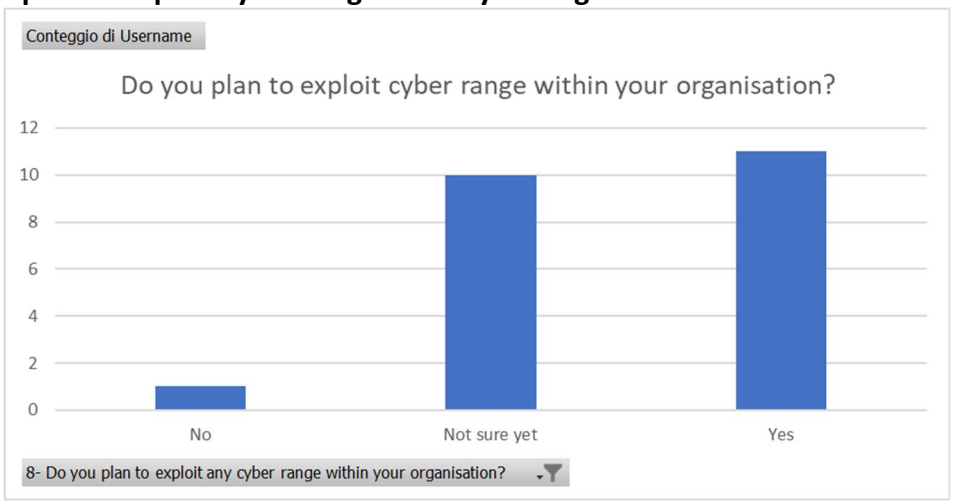


Q5 Where your expectations fullfilled?

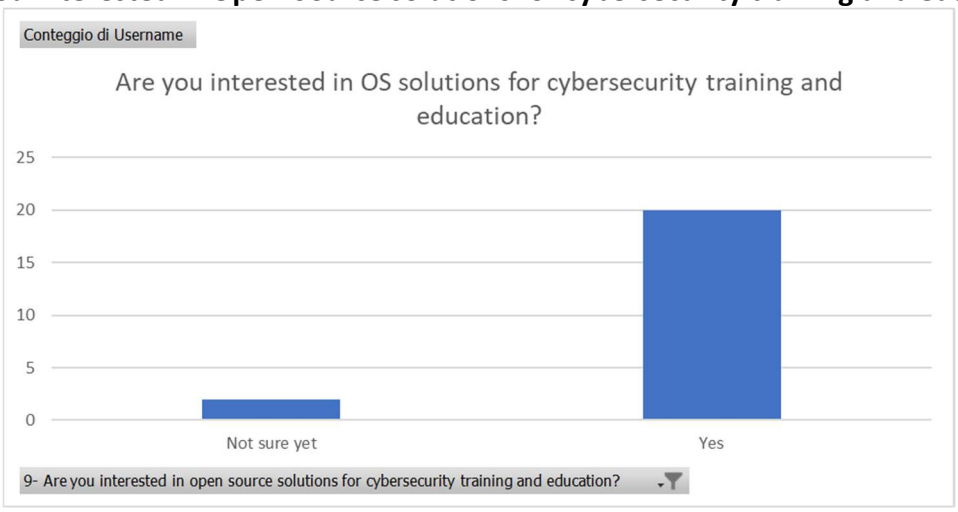
Q6 How likely is to suggest PG solutions to your peers (1=Not likely at all, 10=Very likely)?



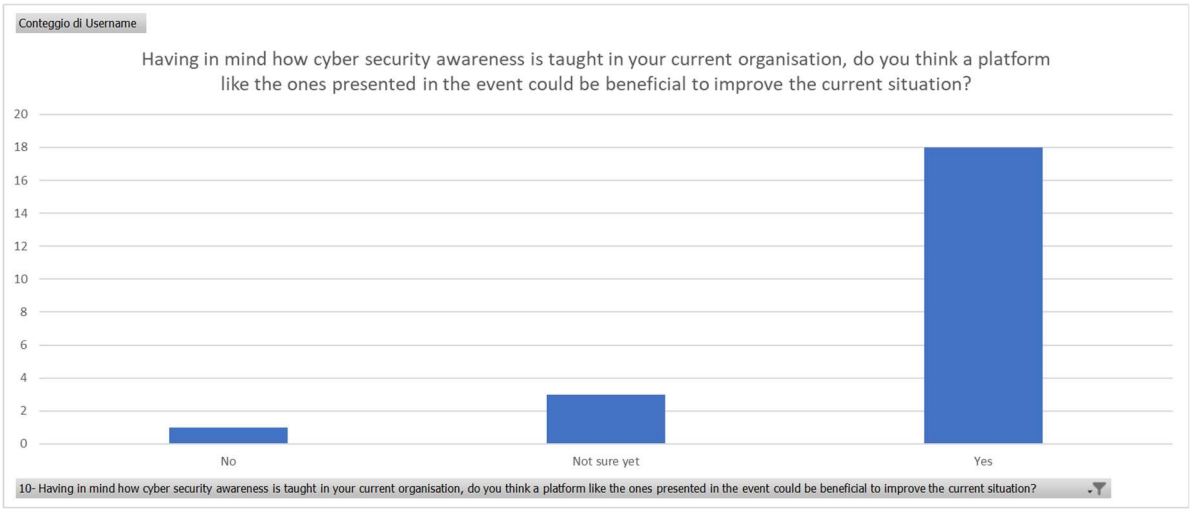
Q7 Do you plan to exploit cyber range within your organisation?



Q8 Are you interested in Open-Source solutions for cybersecurity training and education?



Q9 Having in mind how cyber security awareness is taught in your current organisation, do you think a platform like the ones presented in the event could be beneficial to improve the current situation?



Yes Motivations:
1) hands on training for various level of cybersecurity expertise
2) Organizing training on open sources platforms solves a lot of issues
3) We are implementing KYPO in open stack environment to be prepared for scenario exchange (be more independent as in special dedicated Cyber Ranges)
4) Improve the organizational culture regarding the cybersecurity and adapt the actual procedures and guidelines of security management within the company.
5) Because a platform like the ones presented at the event would be an asset in the way of raising cyber security awareness.
6) Cybersecurity is a topic that every organization should manage nowadays
7) Higher level of interaction and realism can help to acquire and retain useful knowledge for trainees at all levels of experience and expertise.
8) Practical training in a safe environment that is similar to real system is very useful exercise.
9) Due to its architecture
10) The cyber security workforce training is the most important component of the cyber security. Acquisition of technologies and even best practices is faster and more straight forward process than selection and development of the necessary staff.
11) Yes, it will support to improve abstract thinking
12) Those platforms can be used to run a CTF to prove skills acquired during training.
13) I am from Power Grid domain so FORESIGHT definitely will be useful for us.
14) For many reasons: Ethics, awareness, employment behaviour and management understanding and budgeting.

Not sure Motivations:
1) There are different needs on the market and each product and service should consider these needs. It can't exist a solution that fits all requirements and specifics.
2) Depends on required resources as we are constrained with number of people.

Q10 Considering what you saw today (including the presentations, the demonstrations, and the discussion), what could we improve to make the CONCORDIA, FORESIGHT and SPIDER platforms better?
1) all are good
2) Include Law Enforcement :)
3) "Thanks again for presentations.
4) Perhaps, as a proposal, to be more specific in architecture and functionalities (esp. what are differences of possible use cases in der Cyber ranges and what are the synergies in CRFG)"
5) We don't refer to the technological approaches and technical solutions proposed, but all the projects in this field must be oriented to the real needs of end-users and reflect / comprise the UX (User Experience) aspects.
6) Its very inappropriate for me to suggest enhancements. I actually got in touch with the subject for the first time.
7) Nothing all is good
8) Nothing to add.

9) No comments
10) Align the visual identity and UI across the multiple modules, allowing a more seamless experience (users need to have a feeling that they are using a single product).
11) Continuing working expanding the CRs with new functions, communication protocols and devices. To improve users' confidence preparing CRs environment as much as possible to real live systems.
12) Course for the educator with hands on and certification
13) I am impressed by the presentation and by the solutions. Will be very glad to have more events like this and to see more products. It will be interesting to see comparison of our - EU solutions to other solutions from America, Asia ... It is also important to see roadmaps for development. We would like to join in these projects and will be important to see the current level but also plans for the development."
14) I am not an expert on this, so honestly, I don't know/have a clue
15) It was not clear to me how these efforts can be combined. Maybe some longer demos would help. During the short amount of time the event lasted we had to digest a lot of information and I'm sure I missed some. So, a follow up email with links to tutorials, examples, etc. would help.
16) More use cases and validation cases are needed to exploit those great R&I results.
17) No suggestions.
18) More events like this.

ANNEX IV – PANDORA-EDIDP PROJECT EVENT

INVITATION SENT TO PANDORA-EDIDP

2 INVITATION

Uploaded at https://www.eventbrite.com/e/spider-technology-transfer-event-tickets-256985319007
Used in the e-mail invitation sent to Dr. Gardikis, PANDORA project coordinator, main contact point of PANDORA consortium

Invitation - Save the Date!

SPIDER Project is glad to invite you to a specialised Technology Transfer Event that will take place online, on **22/02/2022, at 10.00-12.00 EET**, via Google Meet teleconference platform.

What is SPIDER Project?

SPIDER's proposed solution takes into account all relevant advancements and latest trends capitalizing on current state of the art in order to offer eventually a **synthetic and sophisticated war-gaming environment** that will provide to the training users the ability of playing the part either of the attacker either of the defender (following a red vs blue team format). The main features of the SPIDER solution include advanced simulation and emulation tools, novel training methods towards active learning as well as generation of improved risk analysis and econometric models based on real-time emulation of modern cyber-attacks. **The goal of SPIDER is to deliver a novel 5G CyberRange-as-a-Service (CRaaS) platform** which targets 5G deployment and will be eventually in place to assist security professionals of various levels to enhance their skills being trained under realistic conditions.

What is the Technology Transfer Event about?

This virtual event is customized to meet the interests of PANDORA consortium partners, focusing on the presentation of SPIDER cyber range technologies. The aim is to introduce participants in the technology behind SPIDER, presenting the concept of cyber-ranges as virtual training environments and how they can be used for cyber warfare.

Who is the Target Audience?

The event is addressed to PANDORA consortium partners and end users. The event can be attended from stakeholders of all backgrounds that are interested in cybersecurity technological advancements.

Please mark your calendar and register at https://www.eventbrite.com/e/spider-technology-transfer-event-tickets-256985319007 to join SPIDER Technology Transfer Event. It will be a great honor for us to welcome you virtually on 22/02/2022.

Additional information on the connection details will be sent to you, via email, prior to the event.

By clicking "Register", you confirm that you have read and agree with our Privacy Policy.

For more information on SPIDER project please visit:

- SPIDER Project website: https://spider-h2020.eu/
- A wealth of information on SPIDER technology in the form of publications (Research papers, Deliverables) can be found at: https://spider-h2020.eu/publications/
- Join us at LinkedIn, Twitter, Facebook, YouTube

SPIDER INFORMATION SENT TO PANDORA-EDIDP

4 SPIDER INFORMATION

SPIDER: a cybersecurity Platform for virtualised 5G cyber-Range

SPIDER 5G Cyber Range in a nutshell

SPIDER's proposed solution takes into account all relevant advancements and latest trends capitalizing on current state of the art in order to offer eventually a synthetic and sophisticated war-gaming environment that will provide to the training users the ability of playing the part either of the attacker either of the defender (following a red vs blue team format). The main features of the SPIDER solution include advanced simulation and emulation tools, novel training methods towards active learning as well as generation of improved risk analysis and econometric models based on real-time emulation of modern cyber-attacks. The goal of SPIDER is to deliver a novel 5G CyberRange-as-a-Service (CRaaS) platform which targets 5G deployment and will be eventually in place to assist security professionals of various levels to enhance their skills being trained under realistic conditions.

SPIDER's Basic Functionalities

A basic characteristic of SPIDER is that it incorporates both a simulation environment and an emulation environment. The *Emulation environment* is used for hands-on exercises while the simulation is tailored to non-expert users. More specifically the emulation environment provides the ability to interact with a real 5G infrastructure spanning from the bare-metal to configured antennas while the *Simulation environment* is configured to execute virtual scenarios (also addressed as serious games) which are affected by the decisions of the trainees. The combination of both environments delivers a unique value proposition which includes the automated performance tracking of trainees, the extraction of their learning gaps and the provision of self-paced educational material regarding theoretical concepts of security. Another basic feature of the SPIDER functionality is to provide the users with the capability of predicting the evolution of cyber-threats and furthermore to analyse the associated economic impact and cost that is brought with the respective attack.

SPIDER Architecture

The SPIDER reference architecture consists of a proper componentization along with proper interaction and dependency tracking among these components. The functional goals of SPIDER will be materialized by an integrated platform which will be "de-composed" in several architectural modules. The decomposition process by itself aims at the enhancement of conceptualization, the acceleration of development and the proper analysis of the entire platform.

The output of the componentization process resulted on 19 distinct components that were aggregated in different groups representing the various environments. These environments include: a) Emulation environment; b) Programmable 5G infrastructure; c) vSOC (Virtual Security Operations Centre) environment; d) Machine Learning Lab e) Simulation Environment and f) Operational Dashboards.

We could refer also to the Knowledge base component that monitors and keeps track of the various 5G asset types, vulnerabilities, potential threats etc, the Risk Calculation Engine component that calculates risks based on the given assets, asset relationships, vulnerabilities, controls and threat appetites, and the Decision Support component that selects the optimal cyber security investment strategy based on the calculated risks provided by the Risk Calculation Engine.

Example Demonstration Scenario

SMS overhearing on a vulnerable Operation Support System (OSS)

You belong to a black-hat hacking group that aims to disrupt the business of SPIDER Telecom organisation. Your group is conducting social engineering campaigns in order to bypass the security perimeter of the organisation. After many months your group has achieved to acquire a valuable reverse shell from an IT administrator of the organisation.

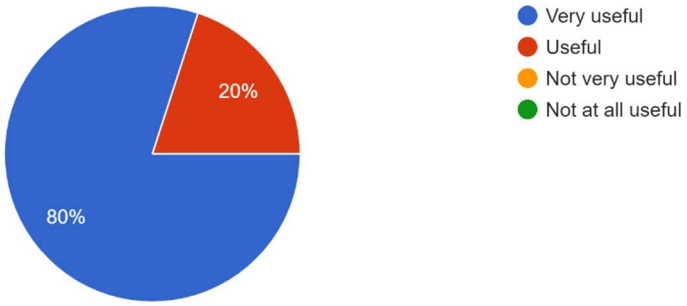
Your mission is to:

a) Explore the network visibility of this person and identify valuable assets that belong to the telco's OSS in order to find a vulnerability and try to penetrate in this asset as stealthy as possible (avoid bruteforce)
b) Perform privilege escalation in order to be able to intercept traffic from the access network
c) Intercept an SMS sent to user, and
d) Use the content of the SMS in order to unzip the encrypted zip file flag.zip that exists in the root filesystem of the OSS virtual machine.

QUESTIONNAIRE RESULTS FOR PANDORA-EDIDP

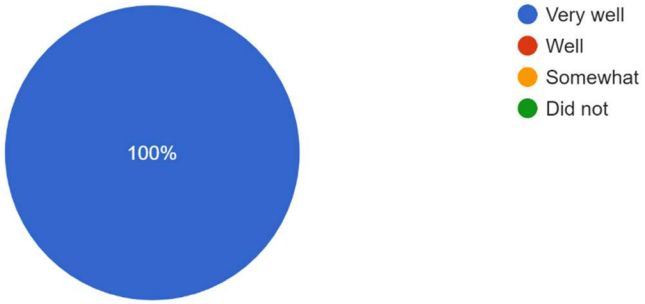
1. SPIDER Technology Transfer Event was

5 responses



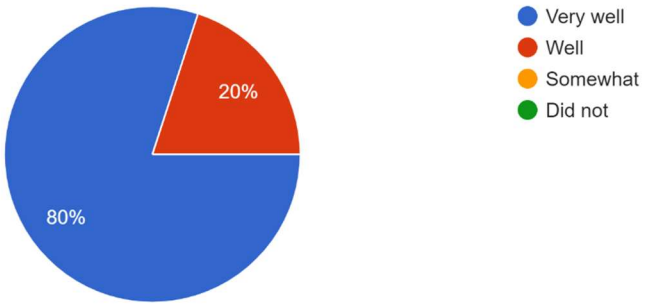
2. Did the organisers from SPIDER project clearly explain the objectives of the event?

5 responses



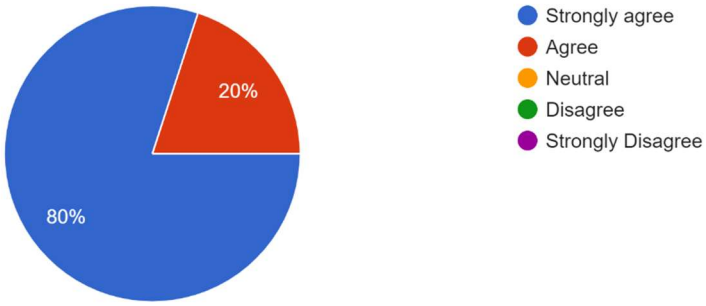
3. Did the organisers sustain interest and participation during the event?

5 responses



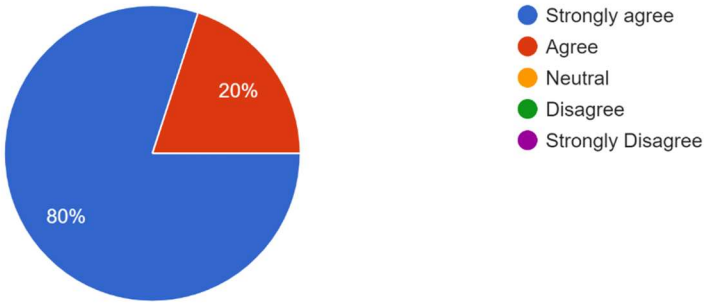
4. Technology presentation/ demonstration were explanatory and interesting?

5 responses



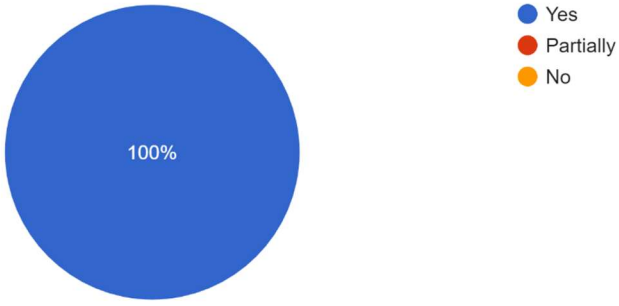
5. The content of the Technology Transfer event was relevant for you and your organisation?

5 responses



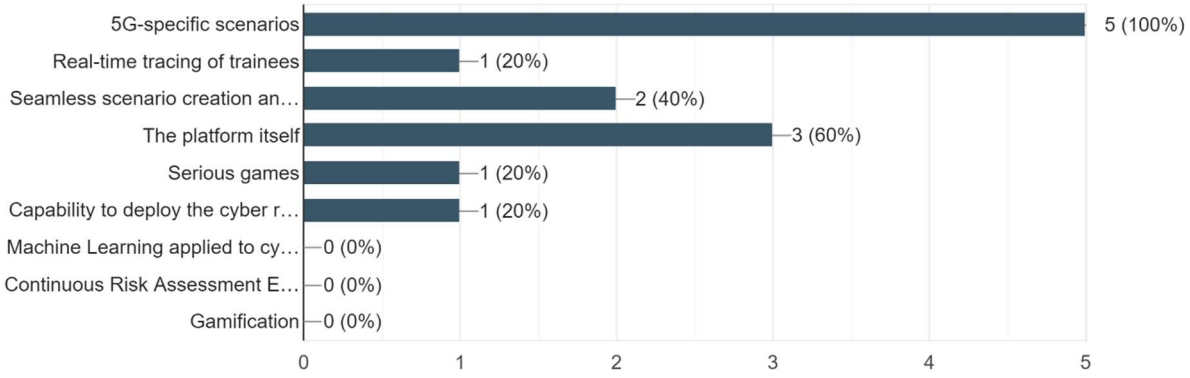
6. Were your expectations fulfilled?

5 responses



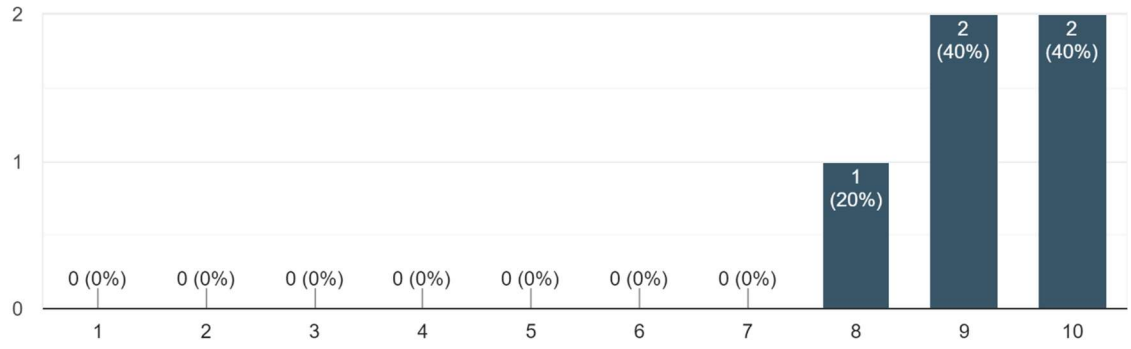
7. What do you think are the most innovative set of feature(s) of the SPIDER platform presented today?

5 responses



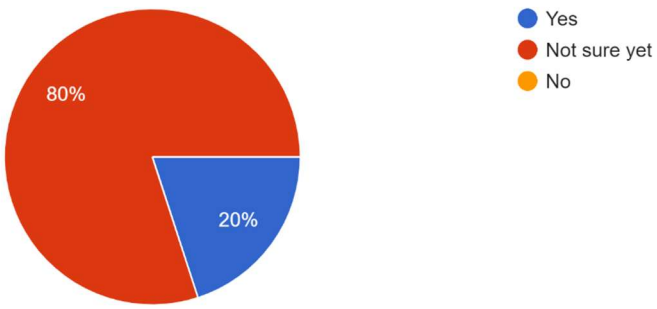
8. How likely is to suggest SPIDER Cyber Range to your peers?

5 responses

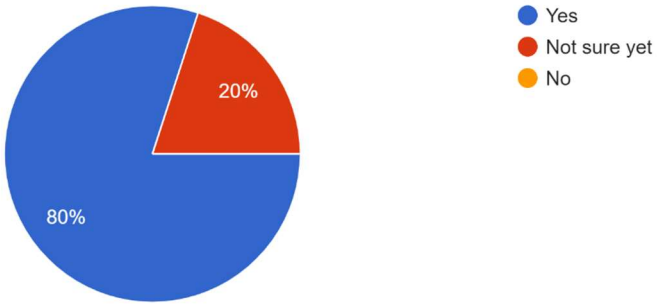


9. Do you plan to exploit SPIDER offerings within your organisation?

5 responses



10. Think about how cyber security awareness is taught in your current organisation, do you think a platform like SPIDER could be beneficial to improve the current situation?
5 responses



Why? please motivate your previous answer
1 response
The gamification concept seemed quite relevant indeed

11. Considering what you saw today (including the presentation, the demonstration, and the discussion), what could we improve to make the SPIDER platform better?
1 response
Offering some of its components as-a-Service in the cloud.

12. Would you suggest similar events from SPIDER project to your peers?
5 responses