European Commission

Horizon 2020
European Union funding
for Research & Innovation

Cyber Security PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi- Layer, end-to-end Simulation and Training

D8.7: The Stakeholders' Engagement & Online Channels Report v.2[†]

Abstract: This deliverable provides the final report of the Communication activities executed by the Consortium for the full duration of the project and the engagement of stakeholders. These activities have been performed under the task "T8.1 – Communication and Engagement of Stakeholders".

Contractual Date of Delivery	28/02/2021
Actual Date of Delivery	28/02/2021
Deliverable Security Class	Public
Editor	*Fulvio Frati, Chiara Braghin (UMIL)*
Contributors	All partners
Quality Assurance	*Vassilis Prevelakis (TUBS),* *George Leftheriotis (TUV)*

[†] *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786890.*

The *THREAT-ARREST* Consortium

Foundation for Research and Technology – Hellas (FORTH)	Greece
SIMPLAN AG (SIMPLAN)	Germany
Sphynx Technology Solutions (STS)	Switzerland
Università Degli Studi di Milano (UMIL)	Italy
ATOS Spain S.A. (ATOS)	Spain
IBM Israel – Science and Technology LTD (IBM)	Israel
Social Engineering Academy GMBH (SEA)	Germany
Information Technology for Market Leadership (ITML)	Greece
Bird & Bird LLP (B&B)	United Kingdom
Technische Universitaet Braunschweig (TUBS)	Germany
CZ.NIC, ZSPO (CZNIC)	Czech Republic
DANAOS Shipping Company LTD (DANAOS)	Cyprus
TUV HELLAS TUV NORD (TUV)	Greece
LIGHTSOURCE LAB LTD (LSE)	Ireland
Agenzia Regionale Strategica per la Salute ed il Sociale (ARESS)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *Vassilis Prevelakis (TUBS),*
2. *George Leftheriotis (TUV)*

Revisions

Version	Date	By	Overview
0.9	25/02/2021	Editor	Internal reviewers' comments addressed. Version for PCC review
0.5	20/01/2021	Editor	Version ready for internal review
0.2	15/01/2021	Editor	Updated Section 1 and Section 2
0.1	01/12/2020	Editor	First Draft

Executive Summary

Deliverable "D8.7 – The Stakeholders' Engagement & Online Channels Report v.2" is the final output of task "T8.1 – Communication and Engagement of Stakeholders". Since it is delivered at M30, the activities performed in the last six months of the project will be reported in a specific section of deliverable "D8.8 – THREAT-ARREST Dissemination and Exploitation report v.2", due at M36, given the close interplay between Dissemination, Exploitation and Communication.

This document provides a report of the Communication activities executed by the consortium after M18. Unfortunately, this period corresponds to the Covid-19 pandemic, which restricted the type and the number of activities we were able to engage. However, whenever possible, we participated, organized and promoted meetings and events to engage possible stakeholders of the project. In particular, we focussed on establishing a solid networking with other European projects and security-concerned industries to foster future Dissemination and Exploitation activities. Online channels then became even more important in this period.

The document describes the activities executed by partners in the second part of the project, and of the result of social media campaign.

Table of Contents

List of Figures

1 Introduction

This deliverable reports the Communication activities executed by the consortium within task "T8.1 – Communication and Engagement of Stakeholders". This task aims at addressing and implementing strategies to extend the project's offerings to a multitude of audiences, including non-scientific audiences such as the media and the public.

This document is the follow-up of deliverable "D8.1 – The stakeholders' engagement plan and online channels development", where the plan for the stakeholders' engagement and for establishing online channels for communication has been identified, and of deliverable "D8.4 – The Stakeholders' Engagement & Online Channels Report v.1". Since the Consortium took an integrated approach to effectively carry out Communication, Dissemination, and Exploitation activities, this deliverable is closely connected also to task "T8.3 – Dissemination plan and activities".

According to the Communication plan, after defining the purpose of the Communication, Dissemination, and/or Exploitation measures, we identified possible project stakeholders, which could be a target of Communication actions, and the means to reach them. Multiple online channels have been exploited in order to reach the largest audience in the context of cyber-security training community. Each channel targets a different category of stakeholders and has its own Communication policy in terms of posted messages and moderator's work.

The Covid-19 pandemic restrictions on travel, gatherings, and meetings limited the in-person events and activities we were able to engage in the second half of the project. Nevertheless, physical meetings have been converted into virtual ones and the Consortium continued to build a network of connections with key players from industry, academia, and potential business partners, to be used to communicate the project's results and to disseminate the technological and business-related knowledge acquired during the project.

In this deliverable, we describe the activities executed by the partners in the second half of the project until M30, and the result obtained so far by the social media campaign. It is important to note that the analysis of further Communication activities carried out in the last six months of the project will be reported in the deliverable "D8.8 – THREAT-ARREST Dissemination and Exploitation report v.2", due at M36.

The structure of the deliverable is as follows: Section 2 analyses the activities with respect to the stakeholders previously identified. Section 3 reports on the results of the Communication activities executed through online channels, i.e., the project website and Twitter, Facebook, and LinkedIn project pages. Section 4 presents the activities and synergies the Consortium has carried on with other major projects funded by the European Commission in the cybersecurity area. Finally, Section 5 provides our conclusions, and in the Appendix I we list and describe the specific Communication actions which have been performed so far.

2 Stakeholders' Engagement Activities Report

The aim of the Communication strategy is to focus on the creation and support of a dynamic innovation ecosystem around THREAT-ARREST's results, targeting to achieve maximum market visibility for the technologies and services developed. Moreover, THREAT-ARREST tried to ensure that the research activities – both the action and its results – were made known to society at large in such a way that they could be understood by non-specialists, thereby improving the public's understanding of science.

One of the goals of THREAT-ARREST Exploitation strategy is to interact with and influence the rapid evolving market of cybersecurity and cyber training. To reach this objective, it is important that the project partners follow and continuously improve and modify the Communication strategy depicted in "D8.1 – The stakeholders' engagement plan and online channels development". To this aim, TREAT-ARREST started with an initial survey of the stakeholders, results and channels through which information is to be disseminated. Then, Communication and Dissemination activities were split into two streams: awareness and knowledge transfer. The strategy applied to the former was based on first recruiting audiences through the website and social media channels, ready to be exploited during the project as results mature and take shape. In parallel, knowledge transfer was achieved through the standard publishing of results in conferences and in journals.

In the following subsections, we briefly review the most relevant stakeholders that we identified for THREAT-ARREST, whose interaction can maximize the impact of the Communication strategy and the diffusion of the project vision and results. Then, we report and analyse the activities performed so far. The liaisons with running H2020 projects are also discussed in Section 4, since we believe that establishing dialogue and collaboration with related projects is important both to identify commonalities and to highlight THREAT-ARREST important outcomes.

2.1 THREAT-ARREST Stakeholders

Stakeholders in the European cybersecurity landscape, and in the internal national markets are unquantified and very heterogeneous. The heterogeneity of project partners helps the Consortium to reach an increasing number of stakeholders, which by nature have different objectives and needs. As reference framework, we referred to the ecosystem defined in the *European Cybersecurity cPPP Strategic research and Innovation Agenda* (ECSO, 2016), that is graphically depicted in Figure 1.

From the schema proposed, we identified the following macro-categories of stakeholders to target the Communication activities:

- S1: Start-up and SMEs,
- S2: Universities and R&D organizations,
- S3: Policy makers,
- S4: Critical Infrastructure providers (in particular Healthcare, Energy, and Maritime),
- S5: Large companies,
- S6: General public.

The "General public" category is meant to include non-expert possible users of the THREAT-ARREST platform, such as high school students or technology users unaware of their possible security risks and vulnerabilities.

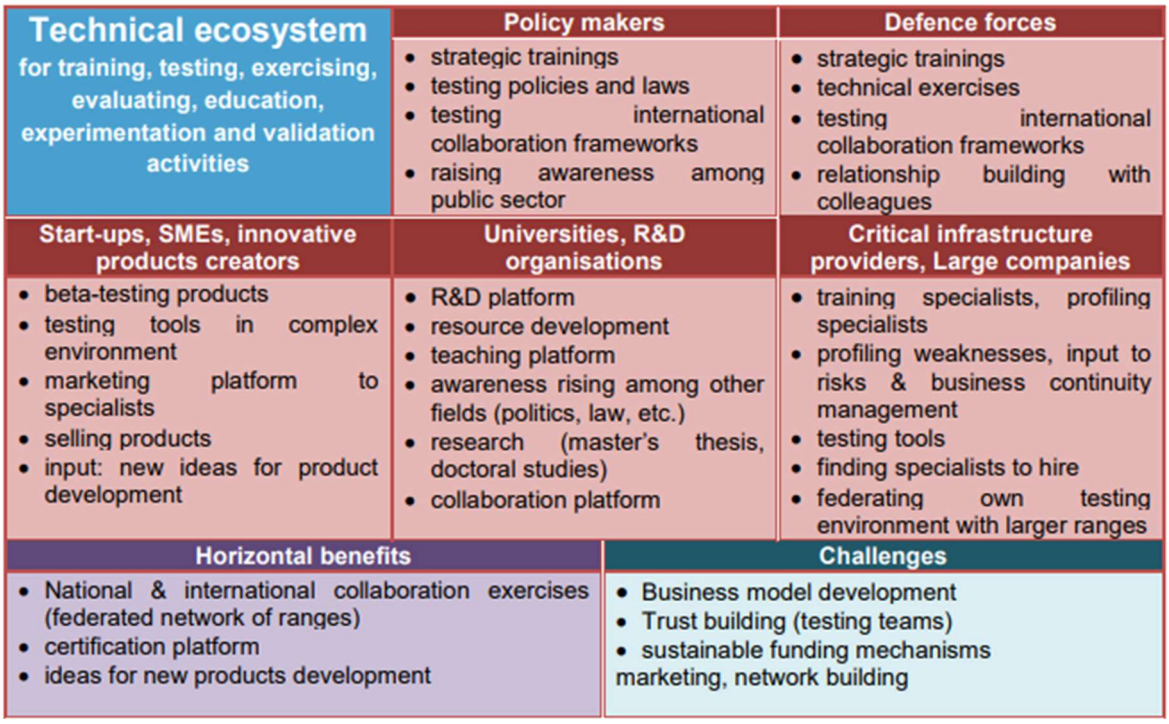

Figure 1: Potential stakeholders groups and beneficiaries (ECSO, 2016)

2.2 Engagements Activity Inventory

In order to keep track of engagement activities with respect to the identified stakeholder categories, a specific event reporting form has been provided to partners to collect data and feedback after the activities (see Appendix I).

With respect to their working context and relationships, the partners identified specific events where stakeholders could be engaged. During these events, THREAT-ARREST results and achievements have been presented.

The event reporting process collected the following data:

- The person who was in charge of executing the engagement activity.
- The project unit responsible of the activity.
- When the activity took place.
- The name of the event where the activity took place.
- A description of the event, which can be the name of the workshop or conference attended, the performed activity, the name of the website or social forum used to communicate, etc.
- The addressed stakeholder categories, depending on the type of audience the communication was expected to be able to reach.
- The number of attendees, namely the number of people attending the event or, if it was possible to give an estimation, the number of people that can be affected by the action.
- The cost of the Communication action, that can be represented by the cost needed to participate to it, to register to the conference or workshop, or the cost for the partner to implement the activity.
- The expected coverage that the Communication activity can have, being worldwide, Europe-wide, or at regional or country-level.

- The Communication channel exploited for the Communication activity, namely Conference, Industry event, H2020 projects meetings or EC events, Poster presentation, Newsletter, Press release, General news, Magazines, Web site, Blogs, or other.
- The overall feedback received by the audience participating to the event (if any), that will be used and discussed in project meetings to improve the quality of the product.

The detailed list of the event data collected, describing all the Communication activities performed and reported by partners from M18 to M30, is included in Appendix I. This list is then analysed in subsection 2.3.

2.3 Communication Activities Results Analysis

The dataset consists of ***15 Communication events***, covering a total of ***49 stakeholders***, at the date this deliverable has been produced. Since some of the stakeholders are consortia or networks, this greatly increased number of individual stakeholders. As mentioned above, the list of events together with a detailed description of the event, is reported in Appendix I.

Data are further examined in the diagram in Figure 2 to give a deeper view of the coverage of the Communication actions. The actions were targeted especially to large companies, Universities and R&D departments, and start-ups and SMEs, due in particular to the nature of the pilots and the Consortium members.

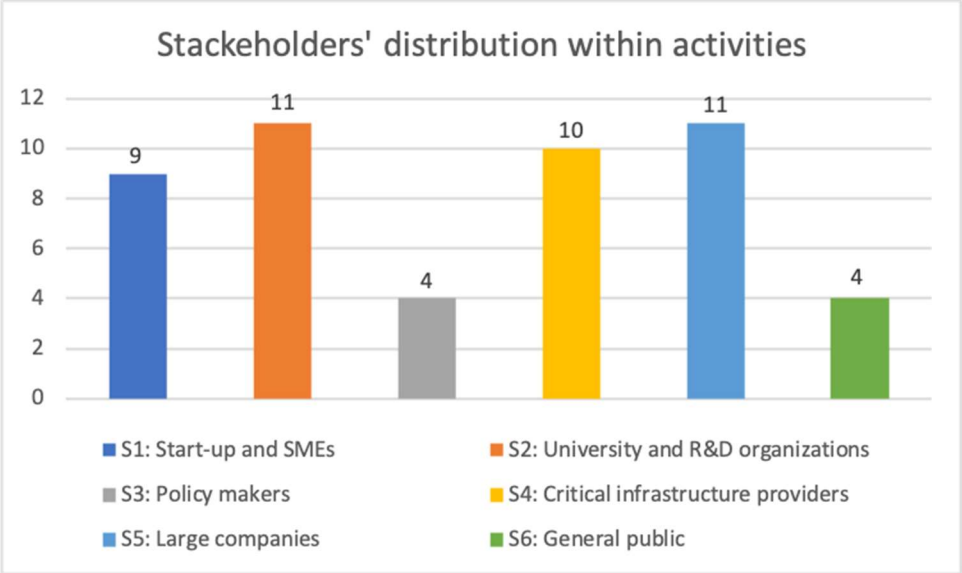

Figure 2: Stakeholders' distribution

Unfortunately, the COVID19 outbreak did not allow the Consortium to improve the outreach to the General Public, since most of the in-presence activities have been canceled or virtualized. On this respect, the Consortium is making effort in producing promoting material that will describe the final version of the infrastructure, with the objective to increase the visibility of the platform on the website.

2.4 Network with other organizations

As the maturity of the platform improved, the Consortium was able to promote its functionalities also to specific Organizations that are willing to produce their own cyber range infrastructure.

In particular, the research connections with researchers in the Robotics and Intelligent Systems Institute at Khalifa University (UAE), provided the opportunity to present the THREAT-

ARREST platform and its capabilities, that were considered a valuable support and research background for the following upcoming projects:

1. Project with *Emirates Nuclear Energy Corporation* (ENEC).

   Project Title: NPP-Cyber Range Framework for the Nuclear Threats and Mitigation in OT Environment.

   Project Description:

   The project proposes an NPP-Cyber Range solution for a specific high-risk organization, Nuclear Power Plants, to provide cyber-tests, training, and hardening its architecture. NPP-Cyber Range provides a mechanism to automatically prepare and manage the OT cyber ranges based on Security Experts' specifications in the Nuclear Power plants.
2. Project with *Emirates Steels*.

   Project Title: A Cyber Range-based Solution to Investigate IT Threats on OT environment.

   Project Description:

   Due to the complex nature of industrial operations, the evaluation of cyber threats from the IT to OT systems is a strenuous task to consider all possible attack vectors. Thus, virtualizing the IT and OT systems through a Cyber Range platform is a safe practice to examine the impact of those threats and evaluate the recommended countermeasures.
3. Project with *Abu Dhabi National Oil Company* (ADNOC).

   Project Title: DE-KNOV: Distillating Expert KNOwledge for Training and Verification.

   Project Description:

   Human expertise is a very important part of companies' intellectual capital. When experts retire, it is not easy to replace them at the same level of expertise. This project aims to extract ADNOC's expertise skills through a gamification tool to be used as a reference to training employees within an augmented reality environment.

3 Online Channels Reports

According to the Communication strategy, also in the second part of the project, the Communication team exploited multiple online channels trying to reach the largest audience possible. The strategy followed aimed at giving visibility to all the project-related activities carried on by the partners, and to news and events that might be important for the cyber-security training community. Each channel targeted a different category of readers, that led to a differentiation of the messages posted by the moderators.

The Communication team opened also a YouTube account, were videos showing the first prototype of the platform have been uploaded.

3.1 Website

The THREAT-ARREST website[1] (see Figure 3) is the central access point to information on the project objectives, team, and achievements. At the same time, it is used also to inform about events organized by the Consortium, like the *2nd Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC) workshop*[2], co-located with the ESORICS 2020 Conference in Guildford, United Kingdom – but actually held online due to Covid-19 (Figure 4).

The project has also released and published, under the Publications section of the website, other six periodic newsletters, highlighting the achievements and the status of the project at the time. The newsletters will be presented in deliverable D8.8.

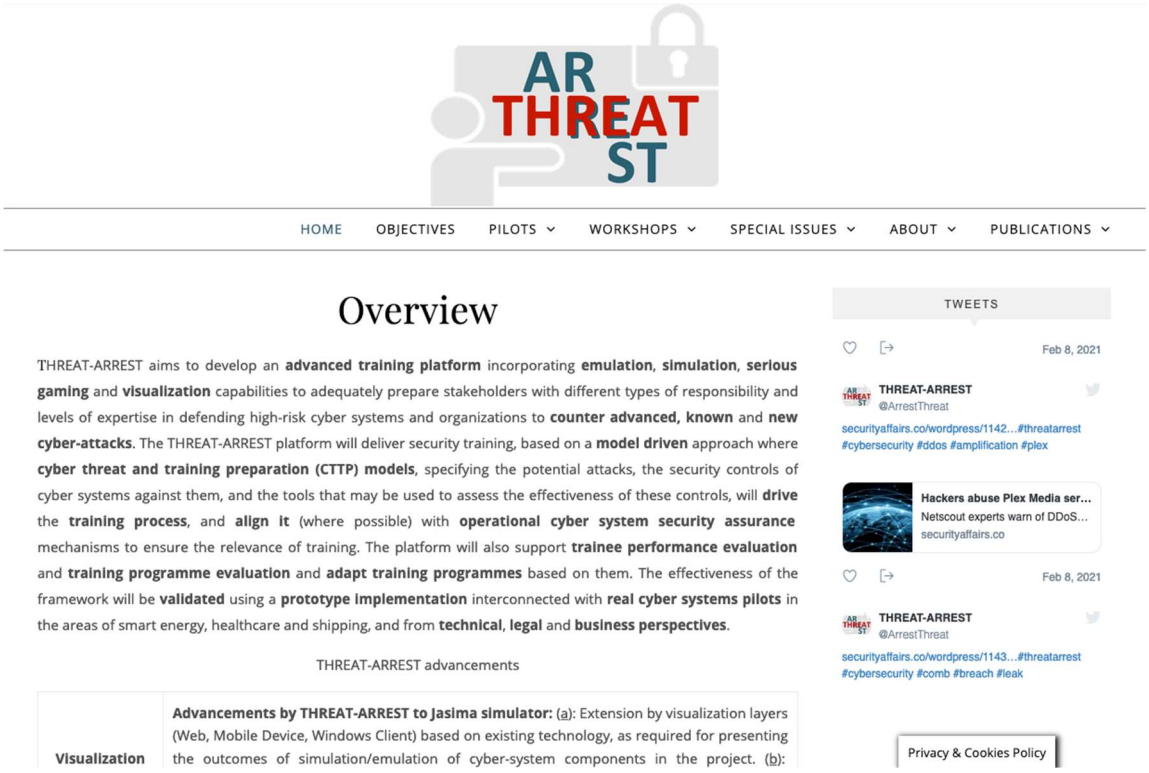

Figure 3: THREAT-ARREST Homepage

[1] THREAT-ARREST – Website: https://www.threat-arrest.eu/
[2] THREAT-ARREST – MSTEC page: https://www.threat-arrest.eu/html/mstec/

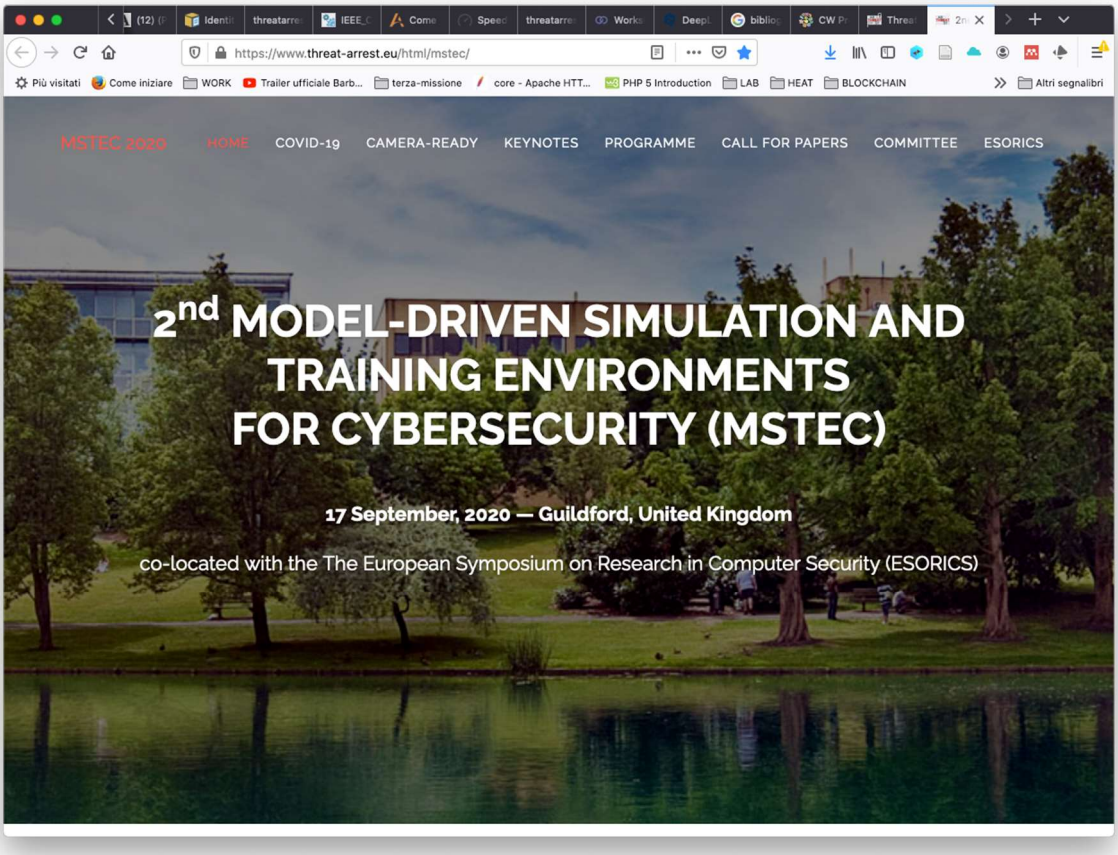

Figure 4: MSTEC Homepage

Due to GDPR restrictions, the administrator of the website has limited the information that is monitored and maintained by the server, and the amount of time data are kept. In particular, only data related to the last 30 days are available. In addition, cookies are not activated by default anymore, as users must give their consent first.

Statistics of data collected during the period Jan 17 – Feb 16, 2021 show the following trends (see Figure 5):

- Total access requests (number of visits): 14.574
- Unique visitors: 2.563

Even if it is limited to 30 days, this data shows a good ratio of visits per day, about 480, indicating a good interest for the project itself and the topics it explores. However, the number of hits may include also page requests done by web crawlers, scrapers, and spiders, since it is not possible to identify the origin of the request. By considering the number of unique visitors per day, it is possible to get a more accurate value, with an average of 85 visitors per day, which, together with the statistics of the pages mostly viewed per day (Figure 6), show an active interest in the project and in the documentation published in the website. Naturally enough, the front page of the website dominates the page views, although also the sections on the project objectives, the ones with the description of the consortium, or the Publications section receive a good level of attention. In addition, Figure 7 shows the geographic origin of visitors, showing interest in the project also from outside Europe. Figure 8 and Figure 9 show the age groups and the gender of visitors, respectively.

Figure 5: Website statistics in the period Jan 17-Feb 16, 2021

Top 10 Pages

ID	Title	Link	Visits
1	Home Page	/	9,731
2	Publications	/downloads/	1,084
3	Objectives	/objectives/	660
4	Consortium	/consortium/	626
5	Healthcare Cyber-Security Training	/healthcare-cyber-security-training/	514
6	Public Deliverables	/public-deliverables/	405
7	Smart Shipping Management	/smart-shipping-management/	304
8	Smart Energy System	/smart-energy-system/	294
9	Home Page	/?xxxxxxxxxxx_loads=1&xxxxxxxxxxxx_filename=info.txt&xxxxxxxxxxxx_filecontent=INF0	94
10	Home Page	/?q=user/login	66

Figure 6: Pages mostly viewed per day

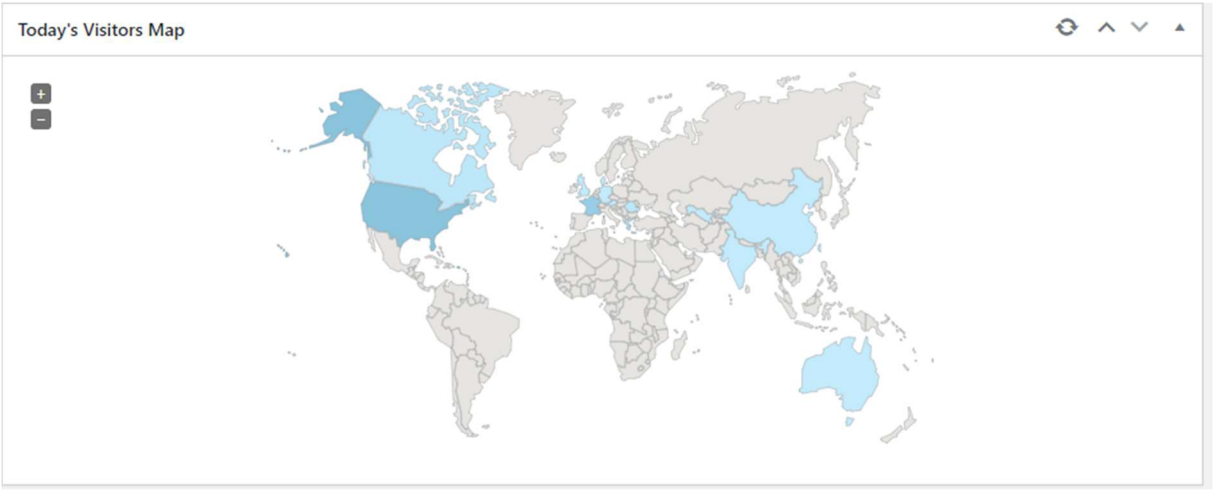

Figure 7: Geographic origin of requests

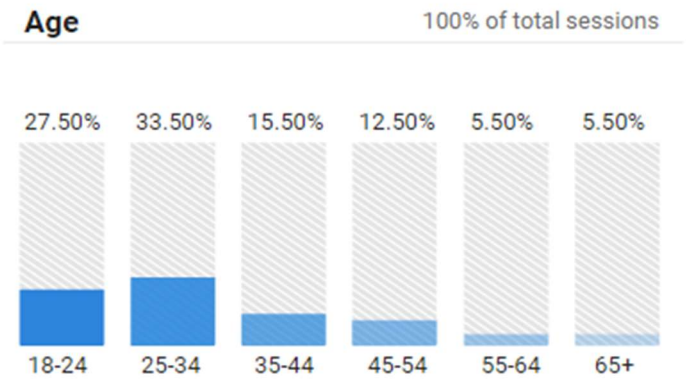

Figure 8: Age groups of visitors

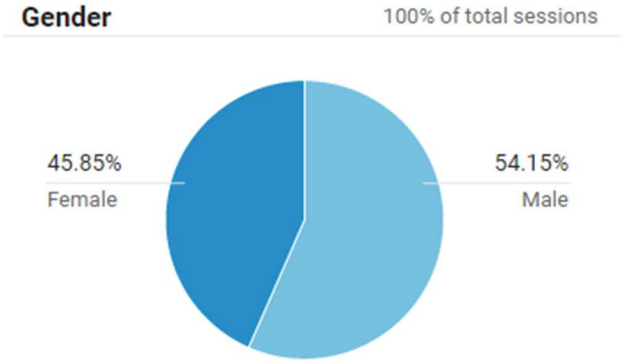

Figure 9: Gender of visitors

3.2 Facebook

THREAT-ARREST's Facebook page[3] is managed by the Communication team and targets the general audience of people that are interested in the context of the cybersecurity, even if it does not involve directly their working interests. The project page is shown in Figure 10.

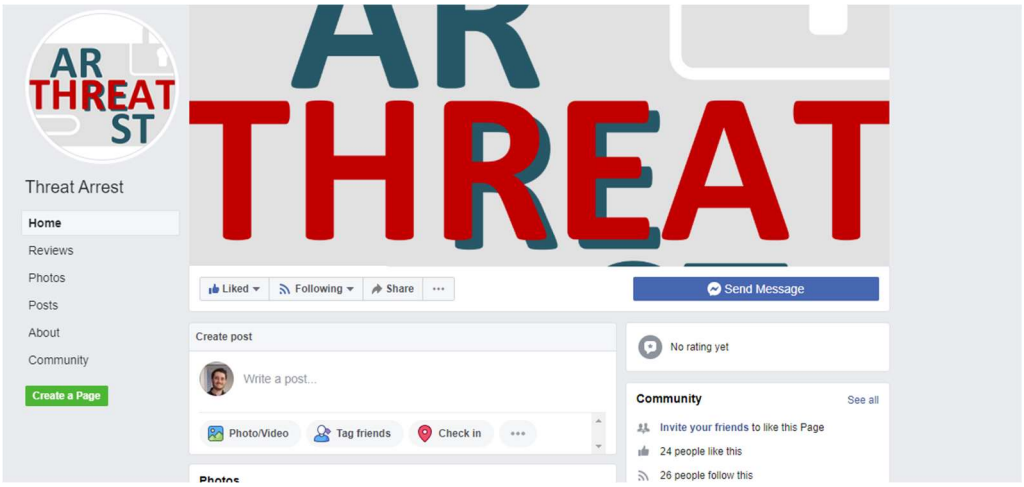

Figure 10: THREAT-ARREST Facebook page

[3] THREAT-ARREST – Facebook page: https://www.facebook.com/Threat-Arrest-266454357324031/

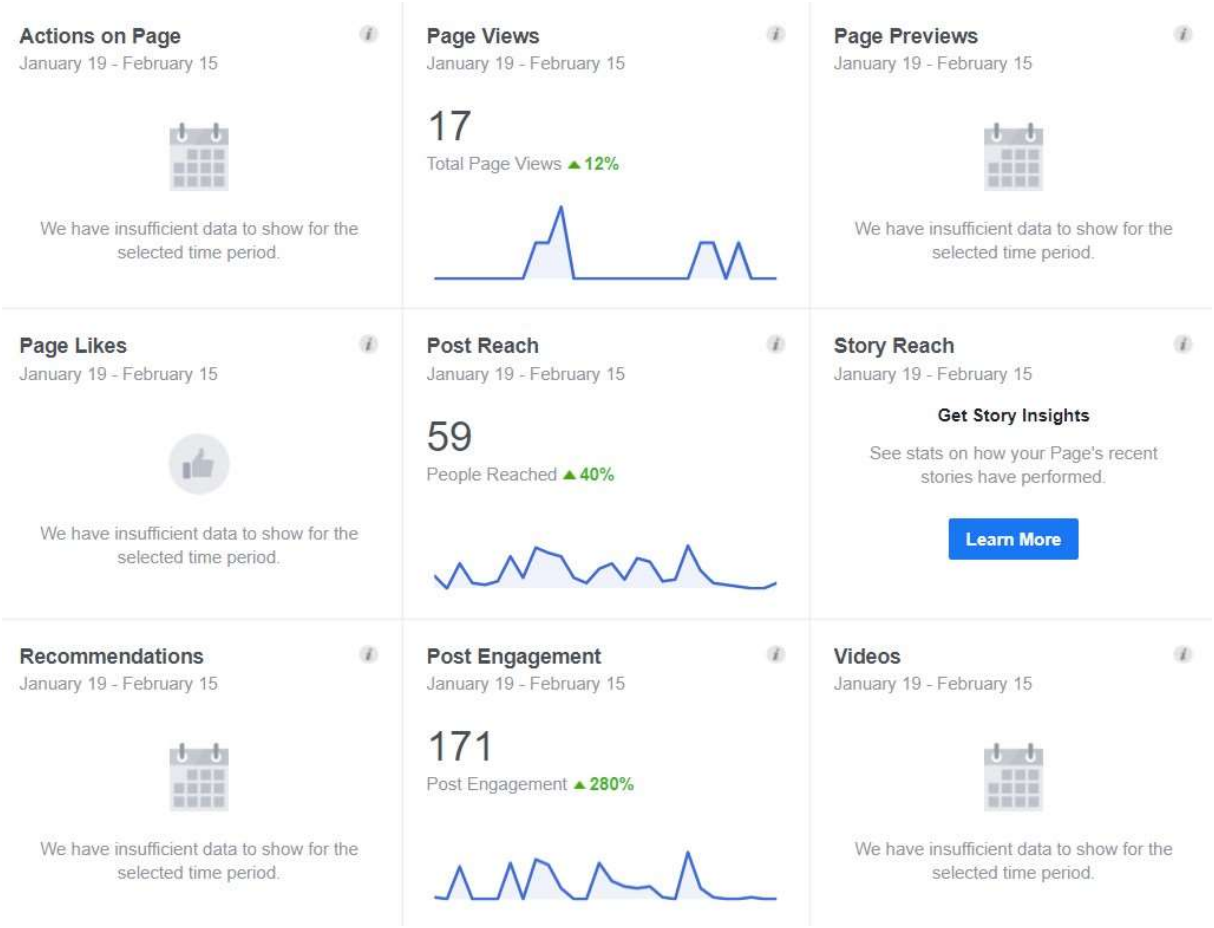

Figure 11: THREAT-ARREST Facebook page data (January 19 – February 15, 2021)

Figure 11 shows the monitoring panel of Facebook depicting the data relative to the last 30 days (from January 19, 2021, to February 15, 2021). Even if the number of followers is not so high (*around 40*), the web site shows a good level of post reach (number of views the users had on the posts) and post engagement (the number of actions, for example like, the user did on the posts).

3.3 Twitter

The twitter channel (**@ArrestThreat**)[4] has been exploited to target an audience that is more related to the cybersecurity context. The homepage is shown in Figure 12.

[4] THREAT-ARREST – Twitter page: https://twitter.com/ArrestThreat

Figure 12: THREAT-ARREST Twitter Homepage

The number of *followers* of THREAT-ARREST Twitter profile has increased since last year, from 104 to 169. In addition, the other Twitter metrics available (see Figure 13 and Figure 14) have also increased with respect to the ones that have been collected one year ago for the previous deliverable. Also in this case, they are relative to the last 28 days (from January 21, 2021, to February 14, 2021), however, their values indicate a good reach in the cybersecurity community. For example, the profile earned a total of 13.4K impressions. This metric describes how many times a post has been seen by users (not only the times it has appeared in the timeline of one of THREAT-ARREST followers, but also the times it has appeared in a search or as a result of someone liking the tweet).

Figure 13: THREAT-ARREST Twitter account statistics (January 21 – February 14, 2021)

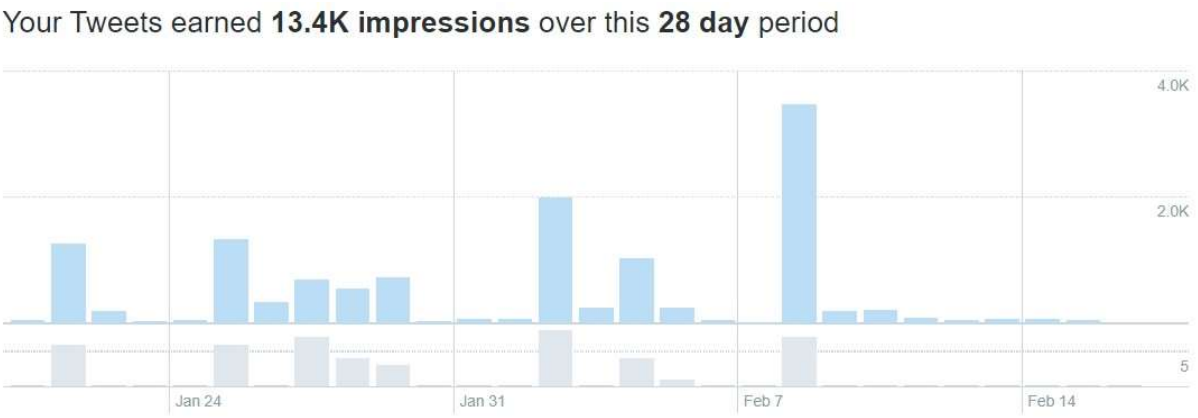

Figure 14: THREAT-ARREST Twitter impressions

3.4 LinkedIn

The LinkedIn page[5] targets an audience of professionals focused on the cybersecurity context. The project page is shown in Figure 15. Currently, the page has *80 connections* (a 35% increase over last years numbers) and posted *more than 100 posts and articles* in the last 12 months of activities.

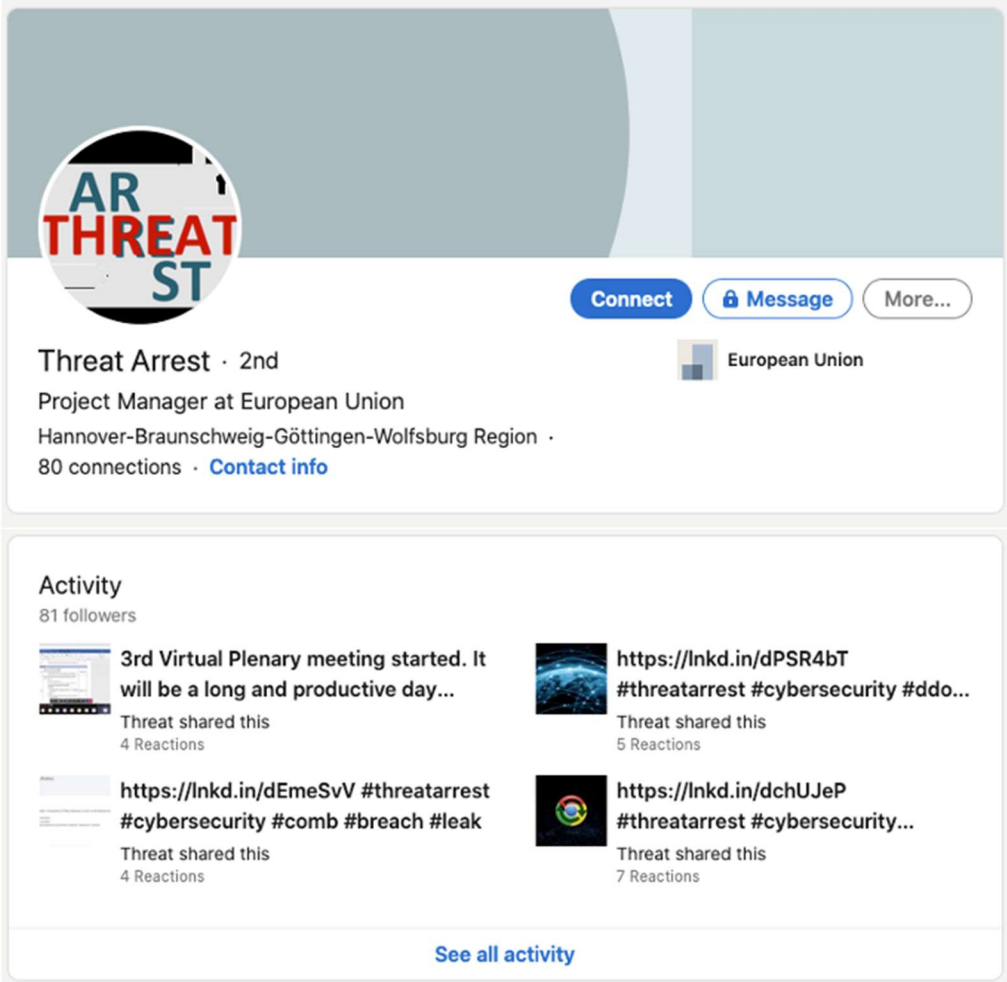

Figure 15: THREAT-ARREST LinkedIn page

[5] THREAT-ARREST – LinkedIn page: https://www.linkedin.com/in/threat-arrest-706485175/

3.5 YouTube

The YouTube channel[6] has been opened as soon as the project had the first version of the THREAT ARREST platform ready and running. Targeted video tutorials on the tools and use-case scenarios have been produced and posted. With this specific channel, the Communication group aimed to engage with software developers and cyber communities, who may not normally have access to academic papers and reports.
This channel was of great use especially during the restrictions given by the Covid-19 pandemic, that limited traveling, meetings, and gatherings.

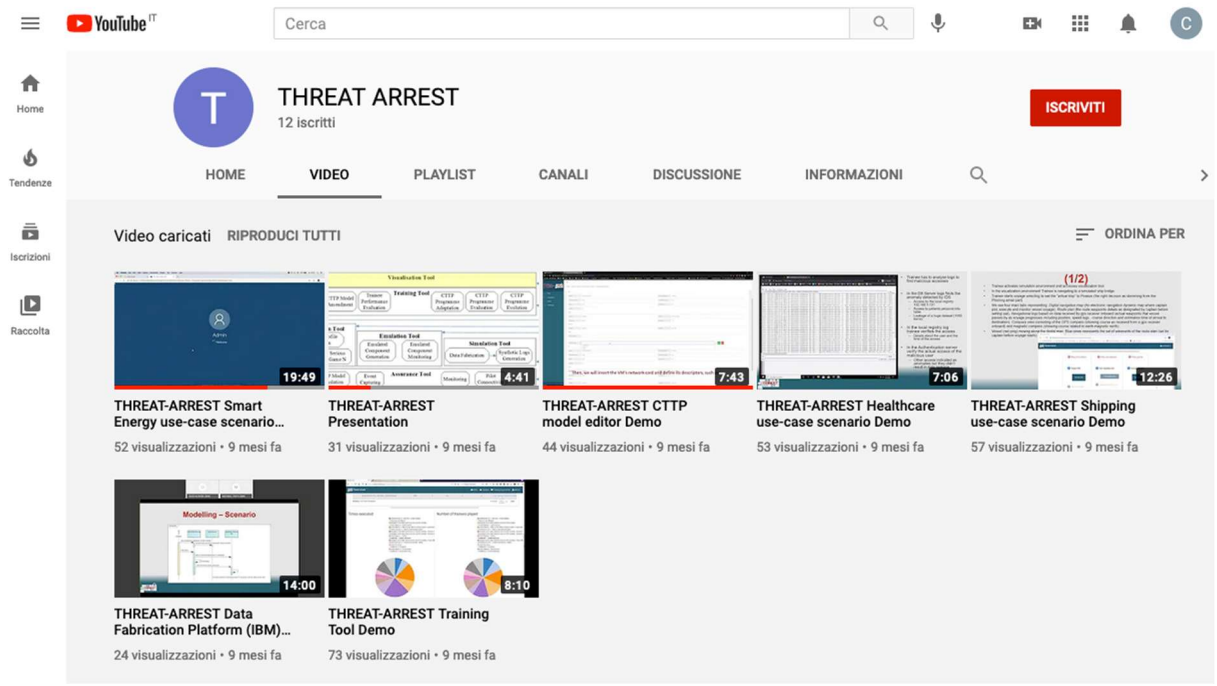

Figure 16: THREAT-ARREST YouTube channel

The 7 video tutorials posted so far are the following:

- *THREAT-ARREST Presentation:* a presentation of the project goals and of the overall architecture of the platform.
- *THREAT-ARREST CTTP Model Editor:* a demo of the editor for building CTTP models and programmes.
- *THREAT-ARREST Training Tool Demo:* a short demo of the first version of the Training Tool (both for trainer and trainee access).
- *THREAT-ARREST Data Fabrication Demo:* a description of the tool used for data fabrication in simulated and emulated training environments.
- *THREAT-ARREST Smart Energy use-case scenario demo:* this video presents a demonstration of a training session for the Smart Energy use-case scenario, using the THREAT-ARREST integrated platform.
- *THREAT-ARREST Shipping use-case scenario demo:* this video presents a demonstration of a training session for the Shipping use-case scenario.
- *THREAT-ARREST Healthcare use-case scenario demo:* this video shows a demonstration of a training session for the Healthcare use-case scenario.

[6]THREAT-ARREST – YouTube page: https://www.youtube.com/channel/UCBUClnDkE6cjYtw7cEgP0vQ/featured

4 Liaisons with running H2020 Projects

Part of the activities addressed in task T8.1 included the active participation to events and activities funded by the H2020 Framework Programme, or other European Commission's instruments.

Since the beginning of the project, the Consortium started an active cooperation with the H2020 projects *CONCORDIA, Cyberwatching.eu*, *SPIDER*, *SmartShip*, *SEMIoTICS*, *Ideal-Cities*, and *CE-IoT* in order to share knowledge, and to build a network of connections to support Dissemination and Exploitation of the project's findings. In the last year, thanks to the existence of a first prototype of the THREAT-ARREST platform, collaborations with some European projects have been consolidated with focussed meetings and small workshops aiming at exchanging experience, and at establishing a cyber-ranges federation. Meetings were fruitful for the Consortium from different points of views: we were able to present THREAT-ARREST platform and have a feedback from people working in the same filed, we have been introduced to other tools owners or to use-cases different from smart energy, healthcare, and shipping, being involved into the building of a cyber ranges federation.

4.1 EU Cyber Competence Network

THREAT-ARREST and its members are actively participating in the EU efforts to establish a *Cyber Competence Network* and develop a *Cyber-Ranges Federation*.

The Cyber Competence Network is mainly supported by the 4 umbrella projects: CyberSec4Europe, SPARTA, CONCORDIA, and ECHO. We produce a policy brief for ***"Cyber-Security Training and Cyber-Ranges"*** and attend in relevant ***discussions*** that were made by this network (Figure 17) as well as a training ***Workshop on Education for Cybersecurity professionals***, made by CONCORDIA (Figure 18).

Figure 17: Cyber Competence Network

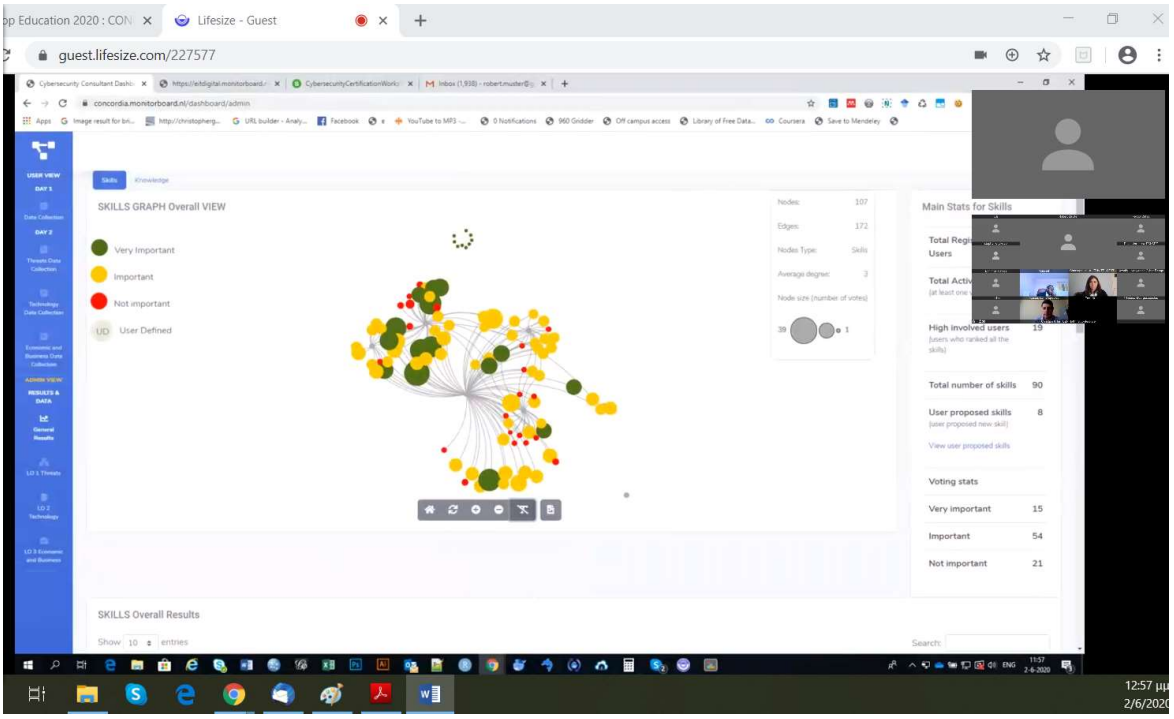

Figure 18: Workshop on Education for Cybersecurity professionals

Moreover, THREAT-ARREST took part in two related surveys conducted by the European Cyber Security Organization (ECSO) – ***"Understanding cyber ranges: From hype to reality"***; and Cyber Security for Europe (CyberSec4Europe) – ***"Report on existing cyber ranges, requirements"***; respectively.

There, they identified two types of federation:

- **Operational Federation (OF):** Sharing of operative cyber exercise or scenario data, or cyber range configuration data in machine-readable format, between cyber range operators or parties using them. Operational Federation can be achieved "offline", without integrating or performing any technical federation of cyber ranges.
- **Technical Federation (TF):** Enables the federated parties to utilize or consume specified functionalities, services, capabilities or resources from another party or parties of the federation. Once the technical federation is established, the usage of the resources or services may happen seamlessly, i.e. transparently from end user perspective.

Thereupon, for the operational federation the ECHO designed a ***cyber-ranges marketplace*** where cyber-ranges platforms can offer their training programmes and attract potential customers (Figure 19). THREAT-ARREST is planning to join this marketplace and promote the three full training programmes that have been developed (see "D3.5 – Reference CTTP Models and Programmes Specifications v2").

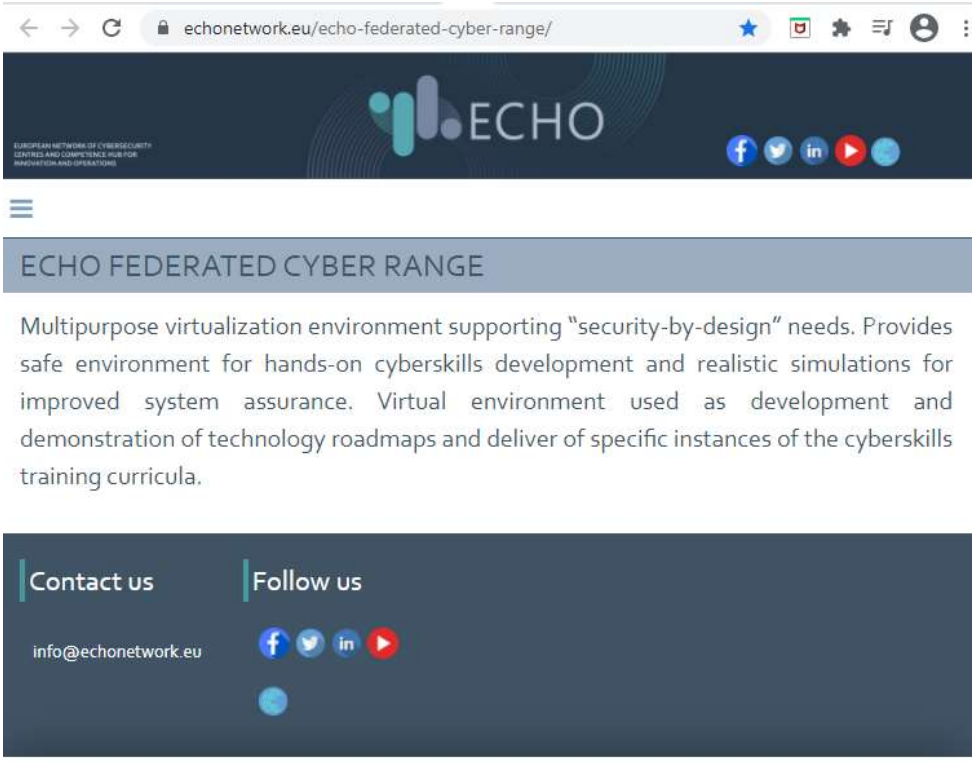

Figure 19: ECHO Federated Cyber-Range

Furthermore, THREAT-ARREST is co-organizing the ***Workshop on Cyber Ranges and Security Training (CRST)*** under the conference IEEE Cyber Security and Resilience (CSR), supported also by ECHO, CONCORDIA, SPARTA, CyberSec4Europe, SPIDER, FORESIGHT, and CyberMAR (Figure 20).

Figure 20: Workshop on Cyber Ranges and Security Training (CRST)

Several efforts have been also performed towards the technical federation of the European cyber-ranges. These initiatives were driven by CONCORDIA. The initial meetings and discussions among the platforms THREAT-ARREST, SPIDER, and KYPO are detailed in the following subsections. The main goal is to design a unified way to design and populate training scenarios among the three cyber-ranges solutions.

4.2 CONCORDIA

The CONCORDIA project[7] has the goal of defining a Cybersecurity Competence Network with leading research, technology, industrial and public competences to build the European Secure, Resilient, and Trusted Ecosystem (Figure 21).

[7] https://www.concordia-h2020.eu/

Figure 21: CONCORDIA Homepage

CONCORDIA will strongly liaise with ENISA, to leverage its expertise and knowledge, exploiting it as interface to other cybersecurity actors and networks within the EU institutional framework and with established industry networks in the private sector.

The goals of the project, as defined by its Consortium, are the following:

1. Define a Cybersecurity Competence Network;
2. Using an open, agile and adaptive governance model and processes that combine the agility of a start-up with the sustainability of a large center;
3. Devise a cybersecurity roadmap to identify powerful research paradigms, to do hands-on experimental validation, prototype and solution development;
4. Develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach;
5. Scale up existing research and innovation with CONCORDIAs virtual lab and services;
6. Identify marketable solutions and grow pioneering techniques towards fully developing their transformative potential;
7. Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators;
8. Launch Open Calls to allow entrepreneurs and individuals to stress their solutions with the development;
9. Establish a European Education Ecosystem for Cybersecurity;
10. Provide expertise to European policy makers and industry.

4.2.1 Interactions with THREAT-ARREST

CONCORDIA and THREAT-ARREST have been actively cooperating in the definition of the requirements for including cyber-security training, based on cyber-ranges, in the CONCORDIA Ecosystems.

In particular, the model-based architecture of THREAT-ARREST is of interest for this definition, and CTTP Models can be taken as basis for the requirements collection. Furthermore, THREAT-ARREST's training scenarios have been examined and discussed, since they cover important application aspects of the industry (maritime sector), public services (healthcare sector), and final users (smart home sector).

Members of THREAT-ARREST participated in CONCORDIA meetings and in the CONCORDIA Open Door event[8] to discuss the cooperation between the two projects (see Appendix II for some pictures of the event, showing all the exhibitors involved). In particular, a CONCORDIA-THREAT ARREST internal workshop has been organized to concretely discuss the possibility of establishing a cyber-ranges federation.

4.3 Cyberwatching.eu

Cyberwatching.eu[9] is the European observatory of research and innovation in the field of cybersecurity and privacy.

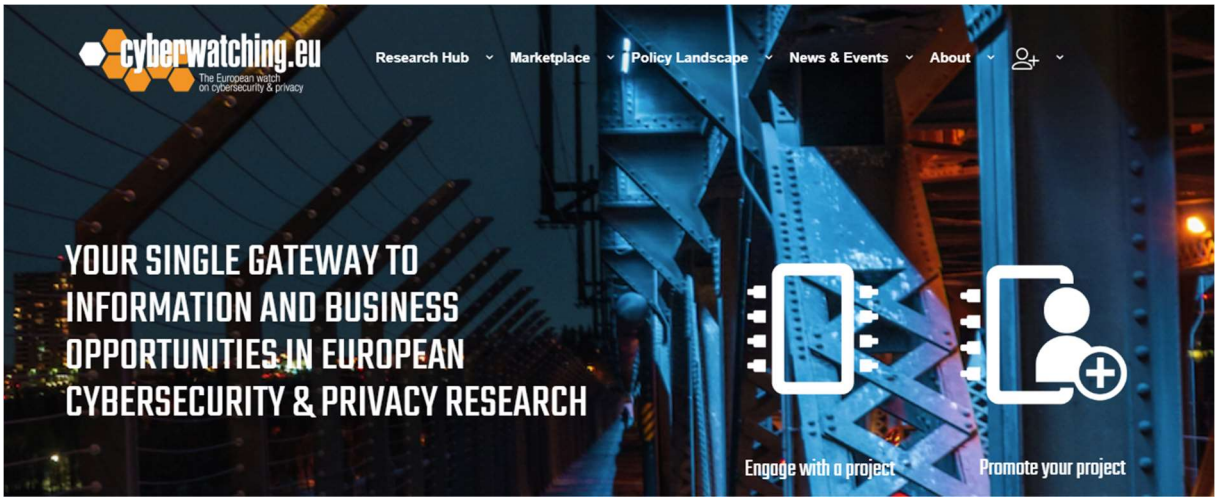

Figure 22: CyberWatching.eu homepage

Funded under the European Commission's H2020 programme, the project will contribute to secure the Digital Single Market promoting the uptake and understanding of cutting-edge cybersecurity and privacy services which emerge from Research and Innovation initiatives across Europe.

First to benefit are SMEs, which will have unlimited access to project information, and also to a Marketplace of services to help improve their cybersecurity offering.

As an online hub for research and innovation in cybersecurity & privacy in Europe, the Cyberwatching.eu website offers European citizens a single gateway to innovative and trustworthy ICT products, services and software which take fundamental rights, such as privacy, into consideration.

4.3.1 Interactions with THREAT-ARREST

THREAT-ARREST has been included in the Cyberwatching.eu Radar Data[10] in the Secure System section, in the ASSESS category (see Figure 23), since the project is still under development. Radar depicts the state of the art of the EU-funded projects active in the context

[8] CONCORDIA EU project: https://www.concordia-h2020.eu/concordia-open-door-event/
[9] Cyberwatching.eu EU project: https://www.cyberwatching.eu/
[10] Cyberwatching.eu Radar: https://radar.cyberwatching.eu/

of the cybersecurity, as a means to maintain an oversight of the larger European Cybersecurity research landscape.

The Consortium will update the information sent to Cyberwatching.eu in order to give an actual and real view of the project.

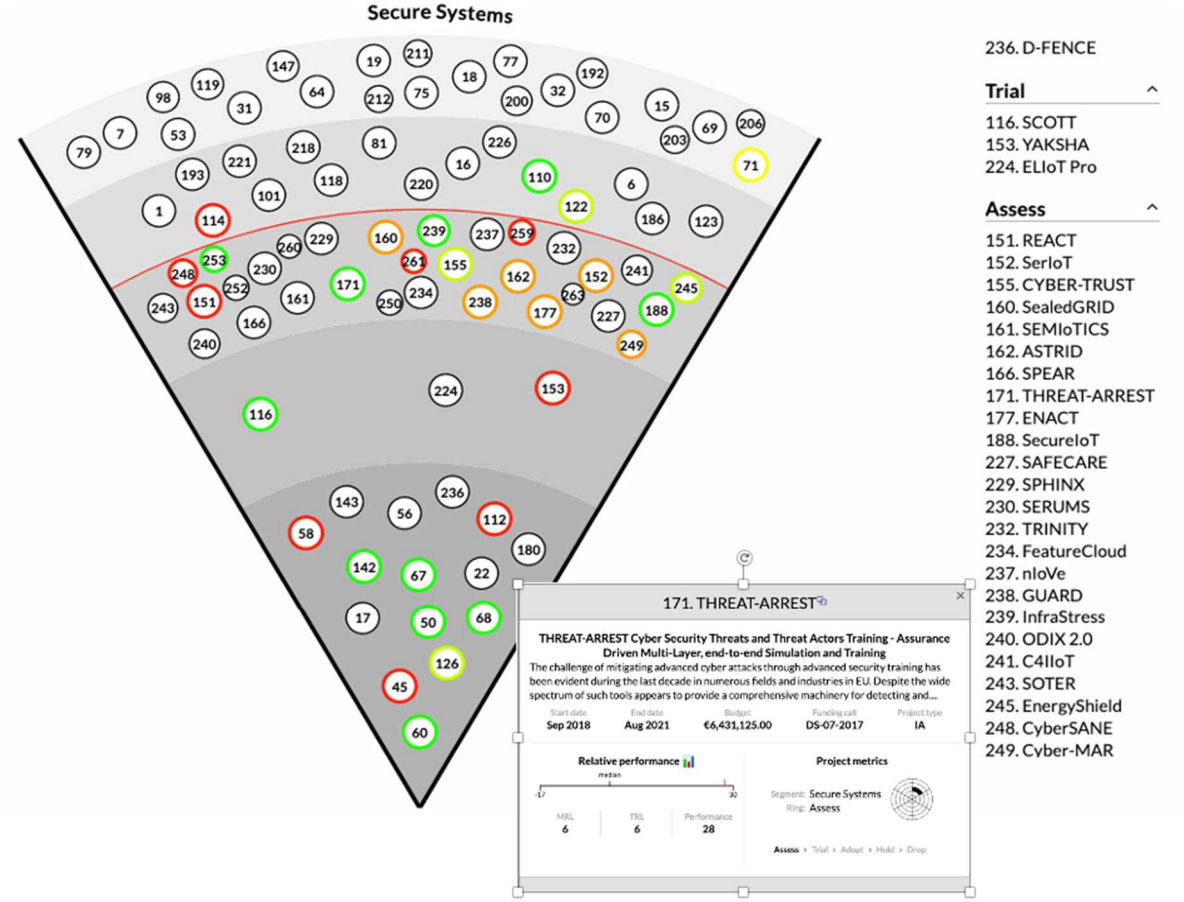

Figure 23: THREAT-ARREST in the Cyberwatching.eu Radar Data

4.4 SPIDER

SPIDER[11] (a cybersecurity Platform for virtualised 5G cyber-range services) aims to deliver an innovative cyber-range as a service platform that extends and combines the capabilities of existing telecommunication testbeds and cyber-ranges with the most relevant advances in telecommunication management and emulation, gamification and serious games training as well as economics of cybersecurity.

SPIDER's main goal is to propose a cyber-range model targeting the provision of a set of risk assessment methodologies, security assurance and certification tools, econometric models for forecasting the evolution of cyber-attacks and their associated impact.

4.4.1 Interactions with THREAT-ARREST

Some of THREAT ARREST partners (i.e., FORTH and STS) are also in the SPIDER consortium. We expect to have a fruitful cross-fertilization among the THREAT-ARREST model-based architecture and the SPIDER proposed framework. Moreover, we are closely

[11] SPIDER EU project: https://spider-h2020.eu

collaborating with CONCORDIA and the KYPO cyber-ranges platform towards the aforementioned technical federation of the platforms (Figure 24).

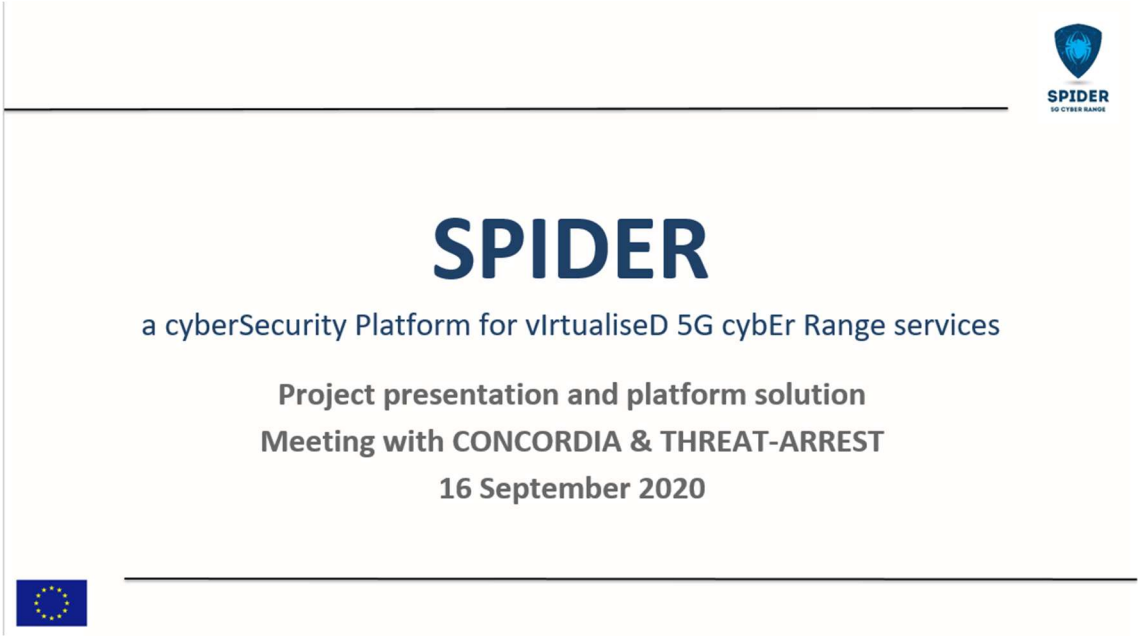

Figure 24: THREAT-ARREST, SPIDER, and CONCORDIA platforms' presentations

4.5 SmartShip

SmartShip[12] project aims to bring together Information and Communication (ICT) Technologies of focused Universities, Research Institutions, and Companies oriented in the maritime sector in order to build a holistic integrated ICT-based framework for a sustainable, individualized and completely automated energy management of ships.

4.5.1 Interactions with THREAT-ARREST

Given that SmartShip has more than two years before completion, we envisage that the project will take advantage of the THREAT-ARREST output to augment its cyber-training activities. The fact that THREAT-ARREST partners (i.e., DANAOS, ITML, and TUBS) are also involved in SmartShip, will facilitate such integration.

4.6 SEMIoTICS, Ideal-Cities, and CE-IoT

The three collaborating EU projects, namely the SEMIoTICS[13], Ideal-Cities[14], and CE-IoT[15], deal with security and privacy issues in smart environments and IoT settings (e.g. (Alexandris et al., 2018; Hatzivasilis et al., 2019a; Hatzivasilis et al., 2019b; Hatzivasilis et al., 2019c; Lakka et al., 2019; Soultatos et al., 2019)). They develop novel secure and dependable technologies in smart sensing, machine learning and artificial intelligence, software-defined networking and cloud management, as well as data-driven circular economy aspects, and bring together stakeholders from the ICT, healthcare, industry, and IoT sectors.

4.6.1 Interactions with THREAT-ARREST

Some of THREAT ARREST partners are also part of the related consortiums (i.e., FORTH and STS in SEMIoTICS, FORTH in Ideal-Cities and in CE-IoT). We are in close collaboration with all these members in order to co-organize workshops and conferences with higher impact to the

[12] SmartShip EU project: https://smartship2020.eu
[13] SEMIoTICS EU project: https://www.semiotics-project.eu/
[14] Ideal-Cities EU project: https://www.ideal-cities.eu/
[15] CE-IoT EU project: https://www.ce-iot.eu/

targeted audience. At the moment, we successfully co-organized the *"Special Session on Security & Privacy for Intelligent, 5G-Enabled IoT Ecosystems"*[16], in conjunction with the IEEE CAMAD 2019 conference, in Limassol, Cyprus. The Covid-19 pandemic limited our plans of workshops/conferences for 2020. We are currently deciding planning for the second half of 2021.

[16] Special Session in IEEE CAMAD 2019: http://camad2019.ieee-camad.org/wp-content/uploads/sites/51/2019/04/SS05.pdf

5 Conclusions and Future Steps

This document presented the activities executed by partners and the results of social media campaign in the second part of the THREAT-ARREST project. The list of engagement activities put in place by partners has been presented, along with the analysis of their impact in the overall Exploitation strategy. Furthermore, a report on the impact of the social media and channels has been presented, highlighting our effort in disseminating the project achievements and progress.

The activities that will be carried out in the last six months of the project will be documented at M36, in the deliverable “D8.8 – THREAT-ARREST Dissemination and Exploitation report v.2”.

6 References

[1] Alexandris, G., et al., 2018. Blockchains as enablers for auditing cooperative circular economy networks. 23rd IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2018), IEEE, Barcelona, Spain, 17-19 September 2018, pp. 1-7.

[2] ECSO, 2016. *European Cybersecurity Strategic Research and Innovation Agenda for a Contractual Public-Private-Partnership (cPPP).* [Online] Available at: https://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

[3] Hatzivasilis, G., et al., 2019a. Review of Security and Privacy for the Internet of Medical Things (IoMT). 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-8.

[4] Hatzivasilis, G., et al., 2019b. The CE-IoT Framework for Green ICT Organizations. 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-7.

[5] Hatzivasilis, G., et al., 2019c. Cyber Insurance of Information Systems. 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), IEEE, Limassol, Cyprus, 11-13 September 2019, pp. 1-7.

[6] Lakka, E., et al., 2019. End-to-End Semantic Interoperability Mechanisms for IoT. 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), IEEE, Limassol, Cyprus, 11-13 September 2019, pp. 1-6.

[7] Soultatos, O., et al., 2019. Pattern-Driven Security, Privacy, Dependability and Interoperability Management of IoT Environments. 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), IEEE, Limassol, Cyprus, 11-13 September 2019, pp. 1-6.

Appendix I: List of Engagement Activities

Time period: March 2020 – February 2021

Activity #1	
Person in Charge	George Hatzivasilis, Fulvio Frati, Michael Smyrlis, Hristo Koshutanski, George Tsakirakis, George Leftheriotis
Unit	ALL Partners
Time	June 10, 2020
Place	Online
Event name	THREAT-ARREST & CONCORDIA meeting
Event Description	THREAT-ARREST project and platform presentation.
Type of Audience	S2: University and R&D organizations S5: Large companies
No. attendees	20
Cost of the activity	--
Coverage	Europe
Communication channel	H2020 projects meetings or EC events
Overall Feedback	Participants discussed the possibility of establishing a cyber-ranges federation. The integration issues between the THREAT-ARREST platform and KYPO cyber range platform were investigated.

Activity #2	
Person in Charge	George Hatzivasilis, Sotiris Ioannidis, Marinos Tsandekidis, Michalis Smyrlis, Chiara Braghin, Fulvio Frati, Martin Kunc, Ludger Goeke, Sebastian Pape
Unit	FORTH, TUBS, STS, UMIL, CZNIC, SEA
Time	September 2020
Place	Online
Event name	The European Symposium on Research in Computer Security (ESORICS)
Event Description	THREAT-ARREST organized the workshop MSTEC-2. In addition to research papers, the overall project was briefly presented in the main workshop event.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S4: Critical Infrastructure providers (in particular Healthcare, Energy, and Maritime) S5: Large companies S6: General public
No. attendees	300
Cost of the activity	--
Coverage	Worldwide
Communication channel	Conference
Overall Feedback	Papers were presented during the MSTEC-2 workshop, detailing the model-driven approach based on CTTP modelling, system assurance technologies, emulated components, digital forensics analysis, and serious gaming. The attendees were interested in all the topics. The presentations were made by FORTH, UMIL, STS, TUBS, CZNIC, and SEA.

Activity #3	
Person in Charge	George Hatzivasilis, Fulvio Frati
Unit	FORTH, UMIL
Time	September 2020
Place	Online
Event name	THREAT-ARREST & SPIDER meeting
Event Description	THREAT-ARREST & SPIDER meeting
Type of Audience	S2: University and R&D organizations S5: Large companies
No. attendees	10
Cost of the activity	--
Coverage	Europe
Communication channel	H2020 projects meetings or EC events
Overall Feedback	The participants discussed the possibility of establishing a cyber-ranges federation. The integration issues between the THREAT-ARREST platform and SPIDER were investigated.

Activity #4	
Person in Charge	Sotiris Ioannidis, George Hatzivasilis, Fotis Oikonomou
Unit	FORTH, DANAOS
Time	September 30 – October 1, 2020
Place	Souda Bay, Chania, Greece
Event name	4th NMIOTC Conference on Cyber Security in Maritime Domain, NATO
Event Description	Presentation of the THREAT-ARREST platform and the Smart Shipping scenario in the annual NATO's conference in Greece concerning the Maritime domain.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S4: Critical Infrastructure providers S5: Large companies
No. attendees	100
Cost of the activity	--
Coverage	Regional
Communication channel	Conference
Overall Feedback	Attendees were interested in the training capabilities of the THREAT-ARREST platform and in the ability to provide realistic emulation of maritime scenarios.

Activity #5	
Person in Charge	George Hatzivasilis, Fulvio Frati, Michael Smyrlis
Unit	FORTH, UMIL, STS
Time	October 28-29, 2020
Place	Online
Event name	Presentation of the THREAT-ARREST project and platform in the CONCORDIA Open Doors event
Event Description	Presentation of the THREAT-ARREST project and platform in the CONCORDIA Open Doors event.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	300
Cost of the activity	--
Coverage	Europe
Communication channel	H2020 projects meetings or EC events
Overall Feedback	Attendees were interested in the training features of the THREAT-ARREST platform, as well as in the modern technical aspects and scalability issues.

Activity #6	
Person in Charge	George Hatzivasilis, Sotiris Ioannidis
Unit	FORTH
Time	November 2020
Place	Online
Event name	Researcher's Night 2020
Event Description	The problem of training and Security in the Cyber-Space was presented to the general public during the annual Researcher's Night, with a focus on THREAT-ARREST approach.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S6: General public
No. attendees	300
Cost of the activity	--
Coverage	City-level
Communication channel	(Online) presentation
Overall Feedback	Attendees were interested in the overall concept of cyber-security training as well as how they can obtain hands-on experience via modern cyber-ranges platforms.

Activity #7	
Person in Charge	Ernesto Damiani
Unit	UMIL
Time	
Place	Sestri Ponente, Genova, Italy
Event name	Meeting with Leonardo company
Event Description	Meeting with the Leonardo company with the “Cyber Trainer” Cyber-Range research group
Type of Audience	S5: Large companies
No. attendees	10
Cost of the activity	--
Coverage	Regional
Communication channel	Meeting
Overall Feedback	The THREAT-ARREST vision has been presented to the Leonardo research center, in particular with team working on the Leonardo cyber range project of the Virginia Cyber-Range project (https://cybersecurity.leonardocompany.com/), getting important feedback on the development of the overall infrastructure, and appreciation on the model-driven approach of THREAT-ARREST.

Activity #8	
Person in Charge	Ernesto Damiani
Unit	UMIL
Time	January 2021
Place	Abu Dhabi (United Arab Emirates)
Event name	Internal meeting with Emirates Nuclear Energy Corporation (ENEC)
Event Description	The THREAT-ARREST concept was presented to a Nuclear Energy corporation seeking a platform to provide specific training for its staff.
Type of Audience	S1: Start-up and SMEs S4: Critical Infrastructure providers S5: Large companies
No. attendees	10
Cost of the activity	--
Coverage	Country-level
Communication channel	Internal meeting
Overall Feedback	Positive feedback from the audience for Project objectives and results. Audience embraced the initiative of enhancing situational awareness and training of a user in a Nuclear Power Plant against cyber threats.

Activity #9	
Person in Charge	Ernesto Damiani
Unit	UMIL
Time	January 2021
Place	Abu Dhabi (United Arab Emirates)
Event name	Internal meeting with Emirates Steels
Event Description	The THREAT-ARREST concept was presented to the Emirates Steels corporation seeking a platform to be used for the evaluation of cyber threats from the IT to OT (operational technology) systems.
Type of Audience	S4: Critical Infrastructure providers S5: Large companies
No. attendees	10
Cost of the activity	--
Coverage	Country-level
Communication channel	Internal meeting
Overall Feedback	Attendees were interested in the overall concept of cyber-security training as well as how they can obtain hands-on experience via modern cyber-ranges platforms.

Activity #10	
Person in Charge	Ernesto Damiani
Unit	UMIL
Time	February, 2021
Place	Abu Dhabi (United Arab Emirates)
Event name	Internal meeting with Abu Dhabi National Oil Company (ADNOC)
Event Description	The THREAT-ARREST concept was presented to an Oil company seeking a way to transfer intellectual capital and human expertise among staff members.
Type of Audience	S1: Start-up and SMEs S4: Critical Infrastructure providers S5: Large companies
No. attendees	10
Cost of the activity	--
Coverage	Country-level
Communication channel	Internal meeting
Overall Feedback	Attendees were interested in the training capabilities of the THREAT-ARREST platform and in the Gamification Tool.

Activity #11	
Person in Charge	Chiara Braghin, Stelvio Cimato, Fulvio Frati
Unit	UMIL
February 2021	October 22, 2020
Place	Online
Event name	Internal meeting with Cyberwiser.eu
Event Description	Presentation of the THREAT-ARREST project and platform to the Cyberwiser.eu team and practical presentation of the Cyberwiser.eu platform and of the SQL injection lab exercise.
Type of Audience	S2: University and R&D organizations
No. attendees	8
Cost of the activity	--
Coverage	Europe
Communication channel	Online
Overall Feedback	The integration issues between the THREAT-ARREST platform and Cyberwiser.eu were investigated. THREAT-ARREST members had the opportunity to use the Cyberwiser.eu platform for a specific use-case scenario on SQL injection.

Activity #12	
Person in Charge	Chiara Braghin
Unit	UMIL
February 2021	October 27, 2020
Place	Online
Event name	Internal meeting with Cyberwiser.eu
Event Description	Presentation of the THREAT-ARREST project and platform to the Cyberwiser.eu team and practical presentation of the Cyberwiser.eu platform and of the Password cracking lab exercise.
Type of Audience	S2: University and R&D organizations
No. attendees	6
Cost of the activity	--
Coverage	Europe
Communication channel	Online
Overall Feedback	The integration issues between the THREAT-ARREST platform and Cyberwiser.eu were investigated. THREAT-ARREST members had the opportunity to use the Cyberwiser.eu platform for a specific use-case scenario on Password cracking.

Activity #13	
Person in Charge	Michael Smyrlis
Unit	STS
February 2021	June 3, 2020
Place	Online
Event name	3rd CyPBER Event 2020 (https://www.cypber.com/)
Event Description	Presentation of the THREAT-ARREST project in the 3rd CyPBER Event 2020
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	100
Cost of the activity	--
Coverage	Worldwide
Communication channel	Conference
Overall Feedback	Attendees have shown interest in the model-based approach of THREAT ARREST.

Activity #14	
Person in Charge	Vito Petrarolo
Unit	ARESS
February 2021	December 15-18, 2020
Place	Arezzo (Italy) and virtual venue
Event name	Forum Risk Management - Health Care (15° Forum Risk Management in Health)
Event Description	Presentation of THREAT ARREST platform in the “Digital Health care and cybersecurity” session of the “15° Forum Risk Management in Health”
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S3: Policy makers S4: Critical Infrastructure providers S5: Large companies S6: General public
No. attendees	100
Cost of the activity	--
Coverage	Country-level
Communication channel	Online
Overall Feedback	Attendees were interested in considering "people" as part of cybersecurity field.

Activity #15	
Person in Charge	George Leftheriotis
Unit	TUV
February 2021	March 3, 2020
Place	TUV HELLAS Offices, Athens
Event name	Meeting with the CTO (Chief Technology Officer) of Cloud Security Alliance (CSA)
Event Description	Meeting with the CTO (Chief Technology Officer) of CSA (Daniele Catteddu), at TUV HELLAS Offices, Athens. Discussion about possible routes for a collaboration/affiliation between CSA and THREAT-ARREST.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	5
Cost of the activity	--
Coverage	Europe
Communication channel	Meeting
Overall Feedback	Promising: CSA proposed several ideas regarding CTTP Programs development and that, when the final platform & programmes are ready, we could arrange for a Workshop.

Appendix II: Pictures from the CONCORDIA Open Doors event

Figure 25: CONCORDIA Open Doors event (webpage)

Figure 26: CONCORDIA Open Doors event – List of participants (Twitter)

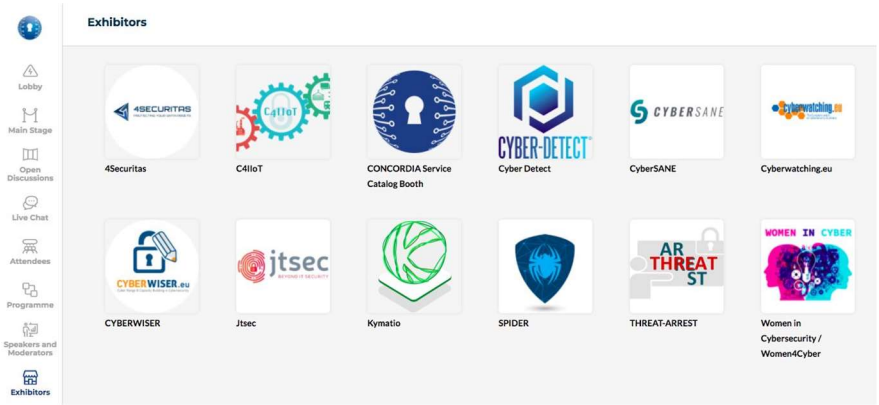

Figure 27: CONCORDIA Open Doors event – List of participants (event webpage)

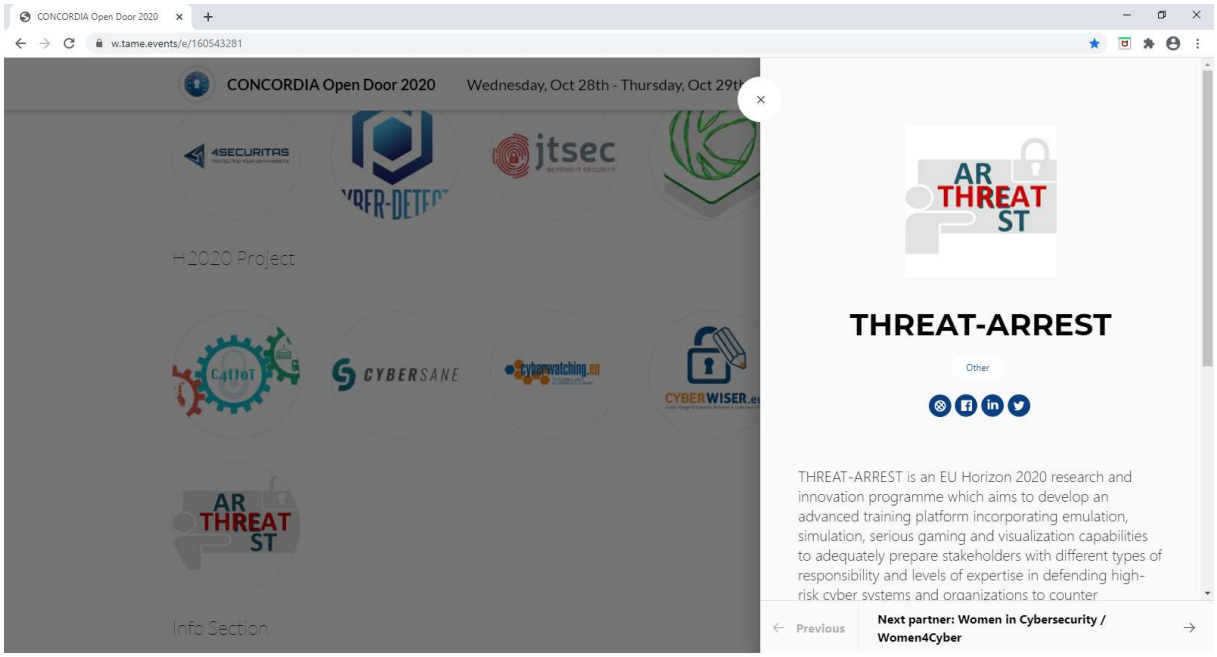

Figure 28: CONCORDIA Open Doors event – THREAT-ARREST description (1)

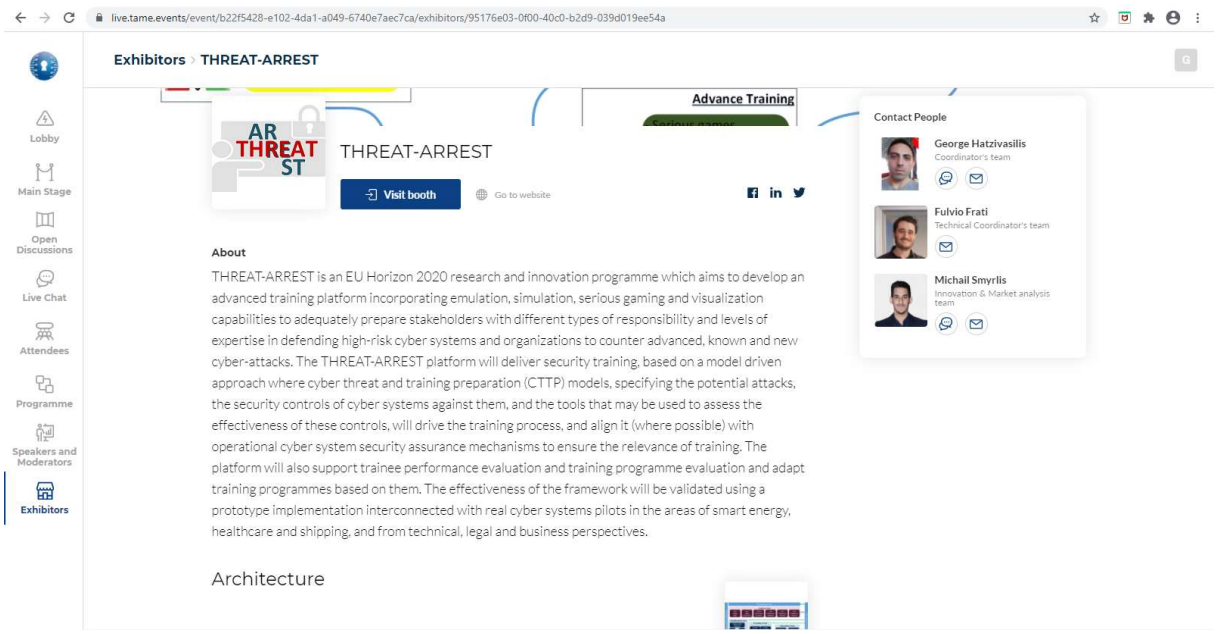

Figure 29: CONCORDIA Open Doors event – THREAT-ARREST description (2)