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

D8.4: The Stakeholders' Engagement & Online Channels Report[†]

Abstract: This deliverable provides a report of the communication activities executed by the consortium within the first half of the project and the engagement of stakeholders so far., These activities are performed under the task "T8.1 – Communication and Engagement of Stakeholders".

Contractual Date of Delivery	29/02/2020
Actual Date of Delivery	29/02/2020
Deliverable Security Class	Public
Editor	*Fulvio Frati, Chiara Braghin (UMIL)*
Contributors	All partners
Quality Assurance	*George Bravos (ITML),* *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
Universita 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. *George Bravos (ITML)*
2. *George Leftheriotis (TUV)*

Revisions

Version	Date	By	Overview
1.0	29/02/2020	Editor	Final version after PCC comments
0.7	28/02/2020	Editor	Version for PCC review
0.5	27/02/2020	Editor	Reviewers' comments addressing
0.3	25/02/2020	Editor	Version for internal review
0.2	31/01/2020	Editor	Integration of activities description
0.1	01/01/2020	Editor	First Draft

Executive Summary

Deliverable D8.4 provides a report of the communication activities executed by the consortium as well as the engagement of stakeholders with the project. The deliverable describes the activities included in the task "T8.1 – Communication and Engagement of Stakeholders".

The document includes a first analysis of possible project stakeholders, which can be a target of communication actions, of the activities executed by partners in the first half of the project, and of the result of social media campaign.

Along with the deliverable "D8.5 – THREAT-ARREST dissemination and exploitation report v.1", which is also due at M18, they determine the means to accomplish the milestone "MS3 – Business models, dissemination and exploitation reports", which forms the 1st version of Business Model and market analysis report, due at M18.

The next and final version of this report will be documented for the deliverable "D8.7 – The stakeholders' engagement & online channels report v.2", due at M30.

Table of Contents

List of Figures

1 Introduction

This deliverable reports the communication activities executed by the consortium within the task "T8.1 – Communication and Engagement of Stakeholders". This task aims at addressing and implementing strategies to extend the project's offerings towards key players from industry, with special focus on advanced cyber training and dissemination of the technological and business-related knowledge acquired during the project. 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.

Two main activity flows have been conducted. The first activity flow on advanced and up-to-date cyber training concerns the identification of the stakeholders and their characteristics, expectations and interests. These activities were also required in order to establish a feasible plan for an effective involvement of the identified stakeholders, including their possible engagement, which has to take in consideration the characteristics of each target group, and should, therefore, be continuously adapted to their changing needs.

The second activity flow on technology and knowledge dissemination concerns the way in which the communication strategy, already planned in deliverable D8.1, has been implemented. These activities aim to exploit multiple online channels in order to reach the biggest possible 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 structure of the deliverable is as follows: Section 2 provides an analysis of the stakeholders the project should target, defining stakeholders' categories of interest for the project and analysing the data basing on it. Section 3 reports on the results of the communication activities executed through online channels, i.e., the project website and Twitter, Facebook, LinkedIn project pages. Section 4 presents the activities and synergies the Consortium has initiated with other major projects funded by the European Commission. Finally, Section 5 provides our conclusions and future steps, and in the Appendix I we list and describe the specific communication actions which have been performed so far.

2 Stakeholders' Engagement Strategy

One of the goals of THREAT-ARREST exploitation strategy is to interact with and influence the rapid evolvement 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 most important step is the identification of most relevant stakeholders, whose interaction can maximize the impact of the communication strategy and the diffusion of THREAT-ARREST vision and results. In particular, relevant project stakeholders are defined as any person, group or organization that has interest or concern in the project and can affect or be affected by the project's objectives, actions and policies toward the construction of a rich and structured European network on cybersecurity training.

Engagement activities are aimed at two major goals: the transferring of THREAT-ARREST outcomes to the plateau of interested people / organizations and, in the future, possible customers or users, and the collection of concrete feedback linked to the various activities performed under the project. In particular, the former goal is of paramount importance in the improvement and evolvement of the project framework towards the actual needs of the cybersecurity training market.

In this context, the project Partners have been involved to identify the major stakeholders related to their particular area of interest (academia, public sector, industry, etc.), determine relevant events to engage them, and report the results of their activity.

These steps are analysed in detail in the following subsections.

2.1 Stakeholders Definition

The first step of the selected stakeholder engagement strategy is the identification of 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 refer 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: University 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 risks and vulnerabilities.

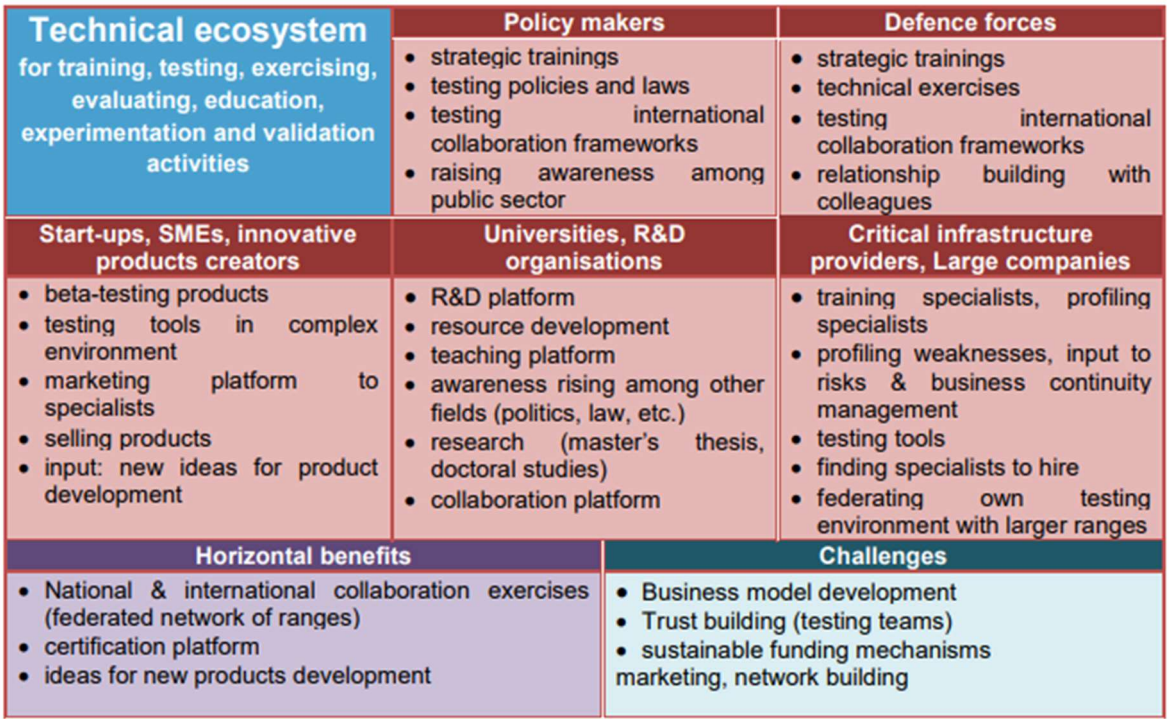

Figure 1: Potentials stakeholders groups and beneficiaries (ECSO, 2016)

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.

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 in the first half of the project, is included in the Appendix I. This list is then analysed in subsection 2.3, and this analysis will be used to support strategic decisions for the upcoming years of the project and to update and improve the communication strategy.

2.3 Communication Activities Results Analysis

The dataset consists of ***18 communication events***, covering a total of ***77 stakeholders***, by the end of month 18. Since some of the stakeholders are consortia or networks, we can potentially reach a greater number of individual stakeholders. As mentioned above, the list of events is reported in the 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.

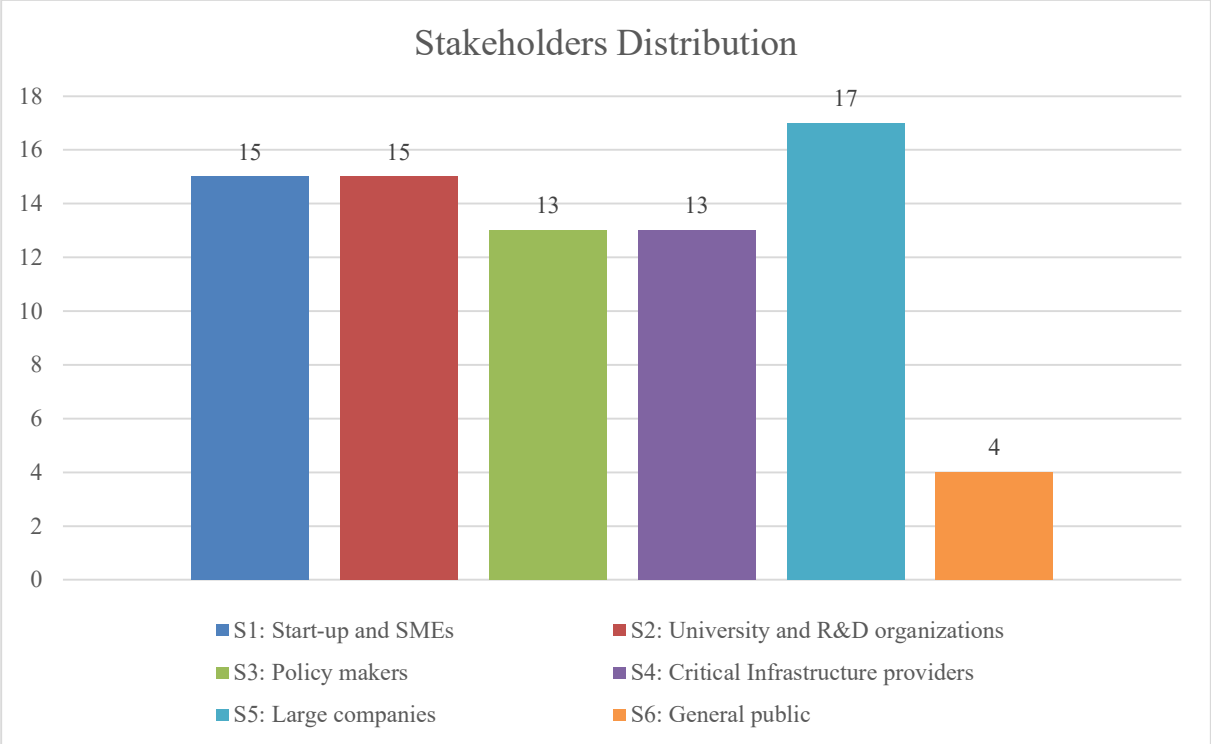

Figure 2: Stakeholders' distribution

However, the actions should be improved in the outreach of the general public, since only in the 5% of the cases the activities were directed to this category of users. On this respect, when the development of the infrastructure will be in a more mature state, the Consortium will take as objective to increase the visibility of the platform on the website via video, short demo, and, if possible, hands-on examples.

3 Online Channels Reports

In the first half of the project, the Communication team exploited multiple online channels trying to reach the biggest audience. The strategy followed was to give visibility to the project-related activities executed by the partners, and to news and events that are 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.

3.1 Website

The THREAT-ARREST website[1] (see Figure 3) is the central access point to find 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 *1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC) workshop*[2] organized within the ESORICS 2019 Conference in Luxembourg (e.g. (Hatzivasilis et al., 2019a)) (Figure 4).

The project has also released and published, under the Publications section of the website, three periodic newsletters, highlighting the achievements and the status of the project at the time. The newsletters are presented in the deliverable D8.5.

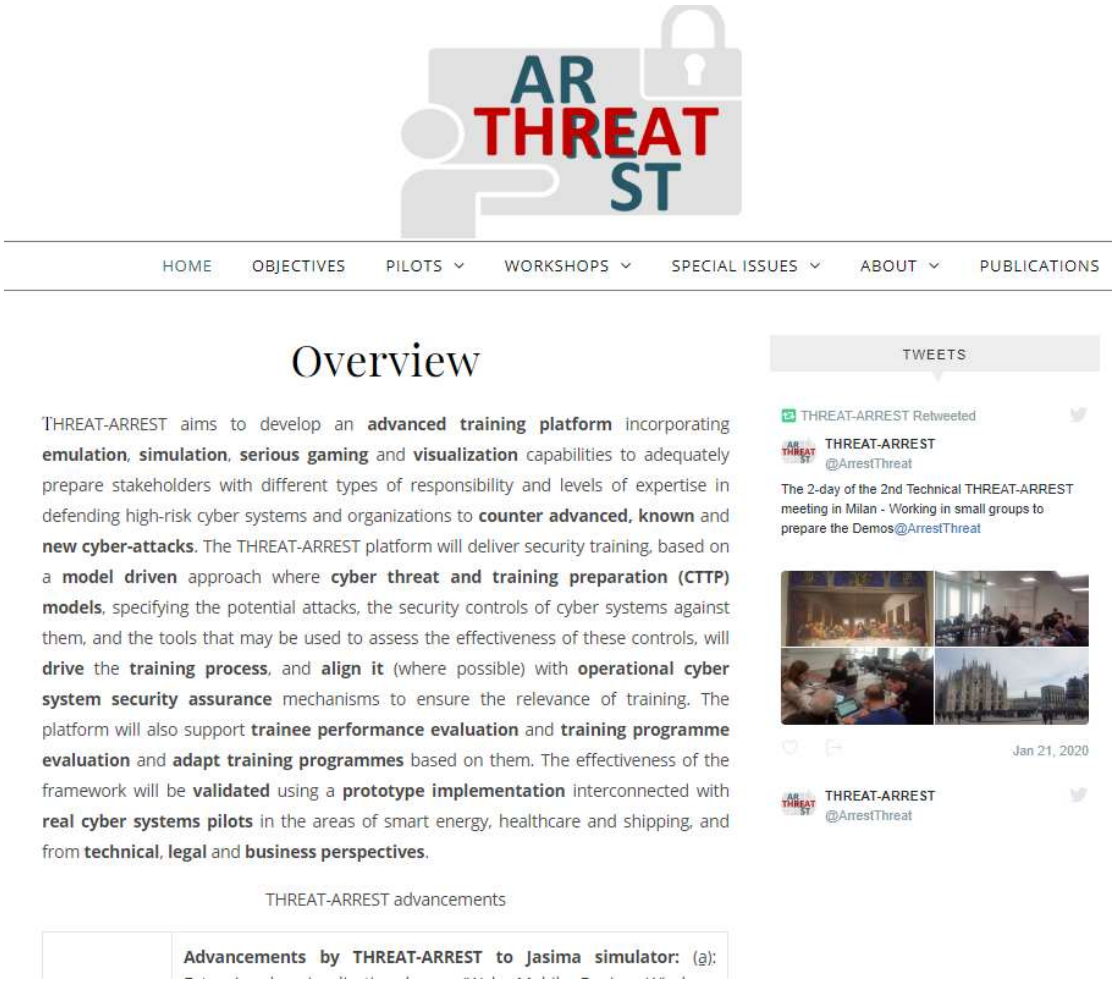

Figure 3: THREAT-ARREST Homepage

[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 15 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 14 – 28 February 2020 of the project show the following trends:

- Total access requests: 17.842
- Unique visitors (see Figure 5): 2.986
- Geographic distribution:
    - Asia: 56.13%
    - Europe: 21.65%
    - North America: 15.70%
    - Africa: 4.87 %
    - South America: 0.43%
    - Oceania: 0.39%
    - Other: 0.83%

Even if it is limited to 15 days, this data shows a good ratio of visits per day, about 1,100, indicating a good interest for the project itself and the topics it is going to explore. 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.

The pages viewed by the visitors of the website can be seen in Figure 6 and Figure 7. Naturally enough, the front page of the website dominates the page views. Additionally, Figure 8 shows the geographic origin of visitors. Also, Figure 9 and Figure 10 show the age groups and the gender of these visitors, respectively.

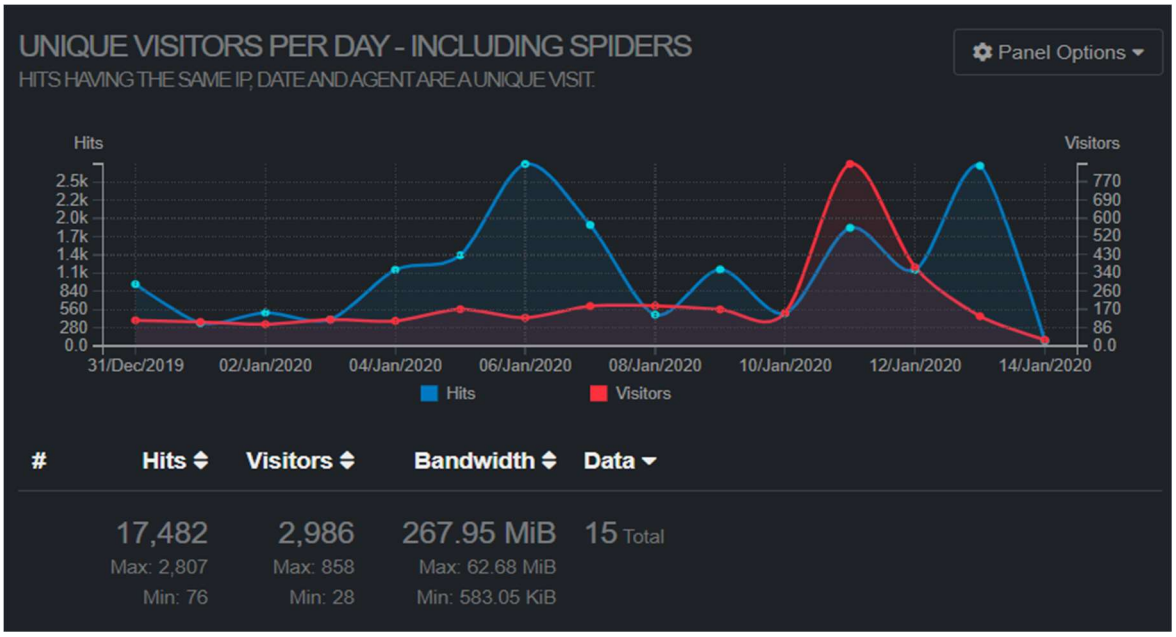

Figure 5: Website unique visitors per day

1	5,033 (32.58%)	222 (4.11%)	3.68 MiB (5.06%)	POST	HTTP/1.1	/xmlrpc.php
2	2,712 (17.56%)	16 (0.30%)	8.88 MiB (12.20%)	GET	HTTP/1.1	/xmlrpc.php
3	1,521 (9.85%)	763 (14.11%)	16.35 MiB (22.48%)	GET	HTTP/1.1	/
4	792 (5.13%)	438 (8.10%)	2.99 MiB (4.11%)	GET	HTTP/1.1	/wp-login.php
5	316 (2.05%)	238 (4.40%)	1.41 MiB (1.94%)	POST	HTTP/1.1	/wp-login.php

Figure 6: Pages mostly viewed – Part I

6	155 (1.00%)	131 (2.42%)	1.48 MiB (2.04%)	GET	HTTP/1.1	/html/eurosec-2019/
7	115 (0.74%)	99 (1.83%)	1.5 MiB (2.06%)	GET	HTTP/1.1	/html/mstec/
8	90 (0.58%)	41 (0.76%)	1.21 MiB (1.66%)	GET	HTTP/1.1	/downloads/
9	78 (0.50%)	72 (1.33%)	121.69 KiB (0.16%)	GET	HTTP/1.1	/wp-includes/js/wp-embed.min.js?ver=
10	78 (0.50%)	68 (1.26%)	557.6 KiB (0.75%)	GET	HTTP/1.1	/wp-includes/css/dist/block-library/styl

Figure 7: Pages mostly viewed – Part II

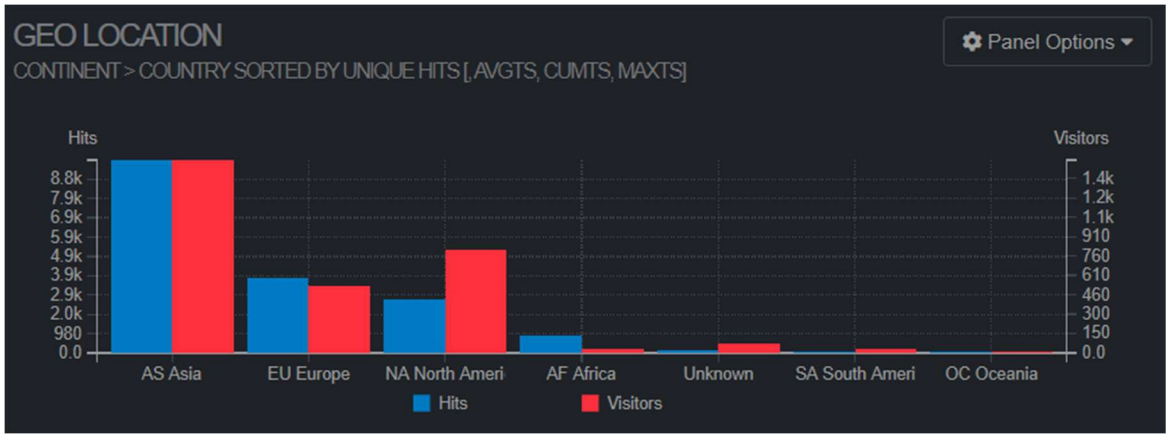

Figure 8: Geographic origin of requests

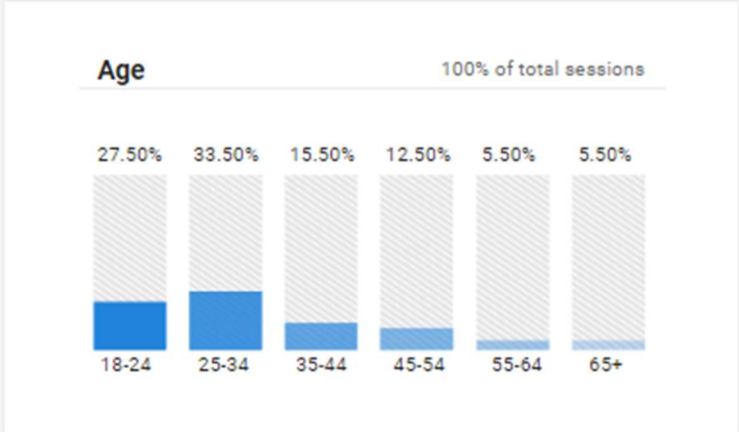

Figure 9: Age groups of visitors

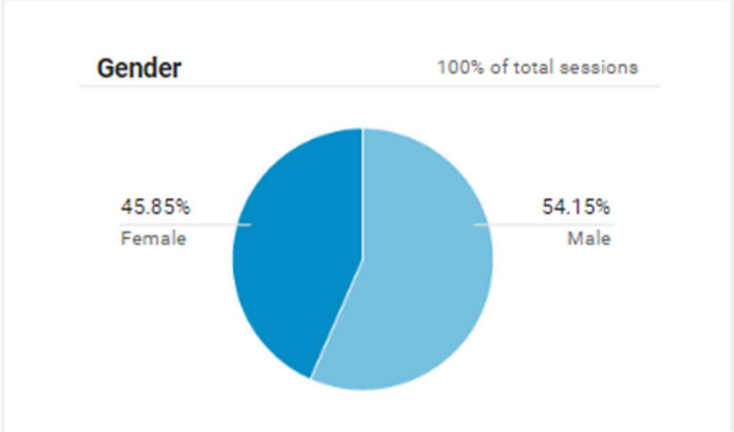

Figure 10: Gender of visitors

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 11.

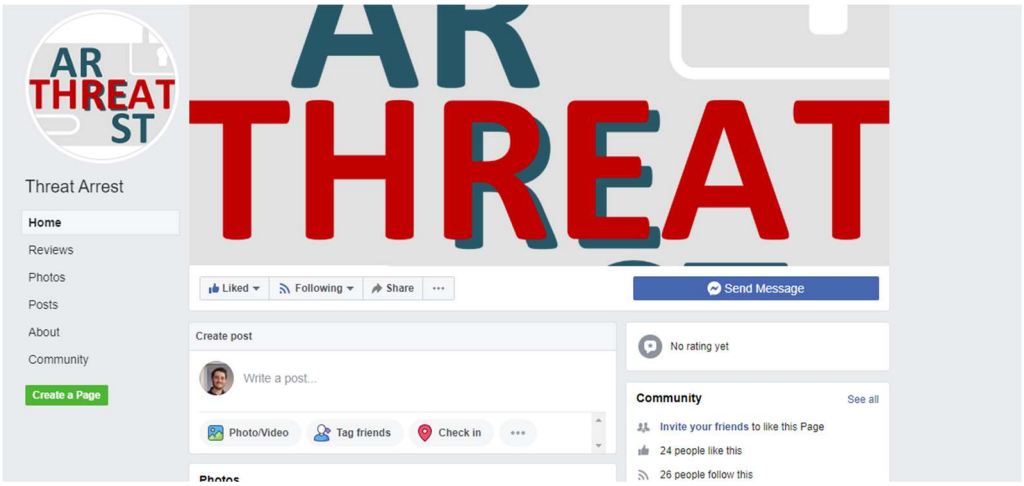

Figure 11: THREAT-ARREST Facebook page

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

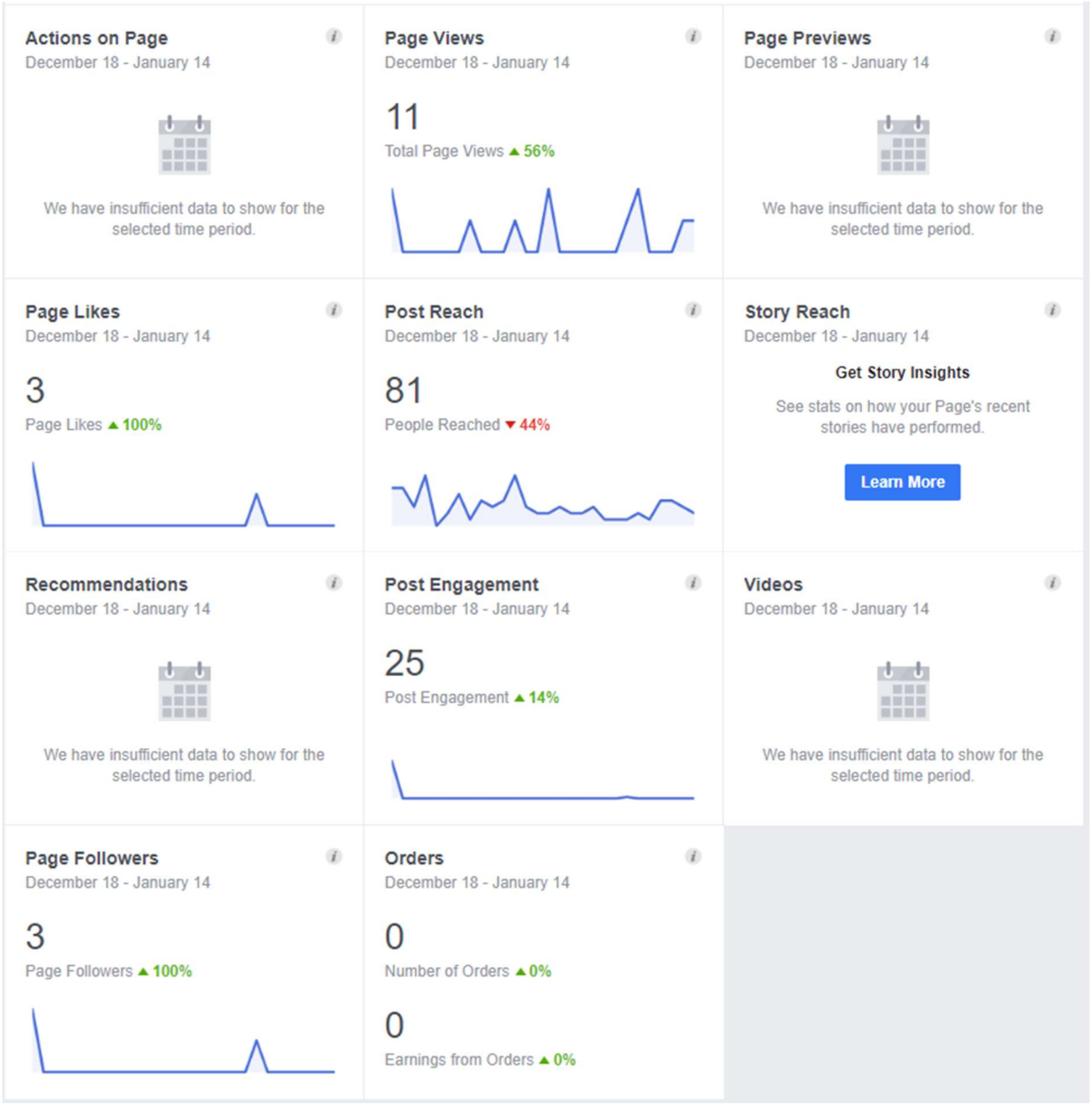

Figure 12: THREAT-ARREST Facebook page data

Figure 12 shows the monitoring panel of Facebook depicting the data relative to the last 30 days (from December 18, 2019, to January 14, 2020). Even if the number of followers is not high (*50*), 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 13.

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

Figure 13: THREAT-ARREST Twitter Homepage

The profile has *104 followers* and, as indicated the graph in Figure 14, in the last 91 days earned a total of about 15,000 impressions. This metric describes how many times the posts has been seen by users, indicating a good reach in the cybersecurity community.

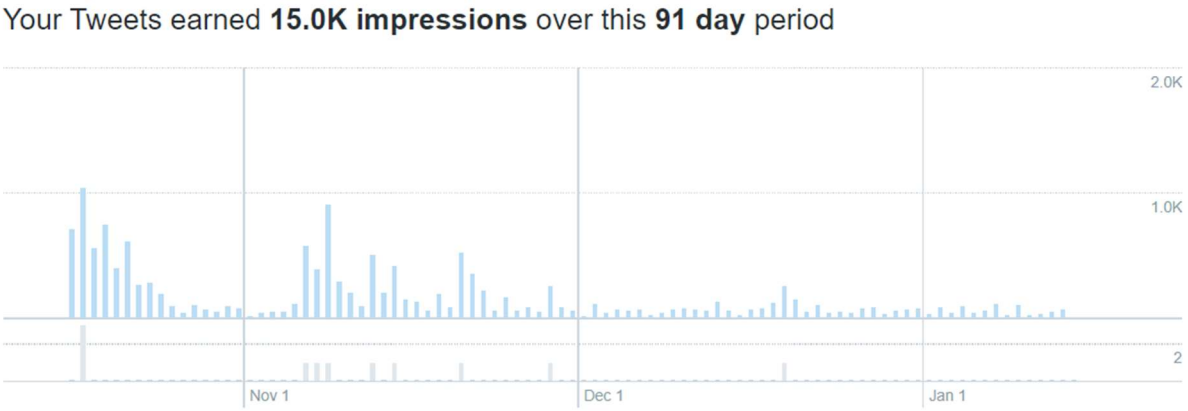

Figure 14: THREAT-ARREST Twitter data

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 *59 connections* and posted *more than 100 articles* in the last 18 months of activities.

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

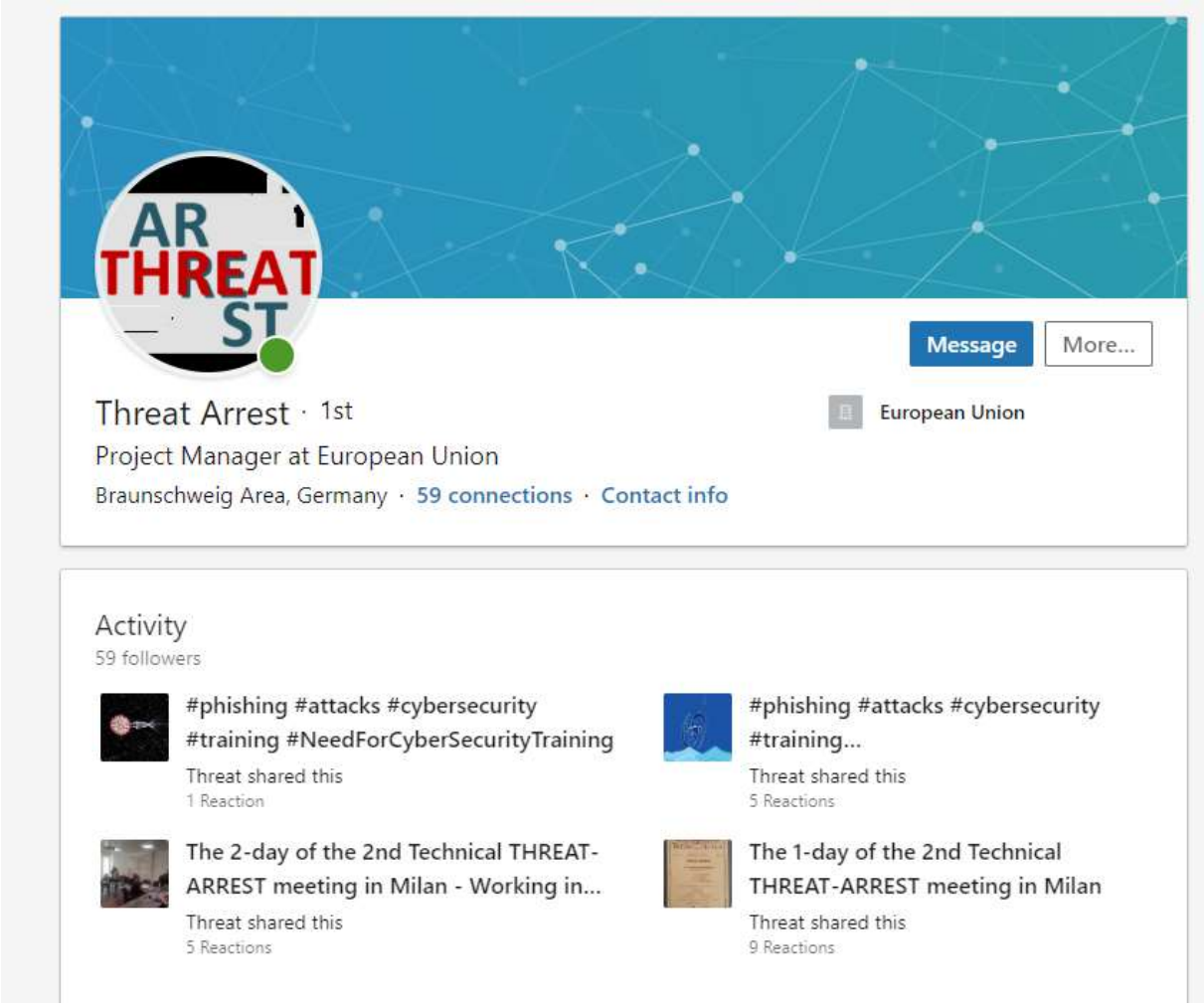

Figure 15 : THREAT-ARREST LinkedIn page

4 Liaisons with running H2020 Projects

Part of the activities addressed in task T8.1 include the active participation to events and activities funded by the H2020 Framework Programme or other European Commission's instruments. The Consortium started an active cooperation with the H2020 projects *CONCORDIA, Cyberwatching.eu*, *Spider*, *SmartShip*, *SEMIoTICS*, *Ideal-Cities*, and *CE-IoT*.

4.1 CONCORDIA

The CONCORDIA project[6] 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 16: 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;

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

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.

4.1.1 Interactions with THREAT-ARREST

CONCORDIA and THREAT-ARREST are 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 are examined, 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[7] to discuss the cooperation between the two projects.

4.2 Cyberwatching.eu

Cyberwatching.eu[8] is the European observatory of research and innovation in the field of cybersecurity and privacy.

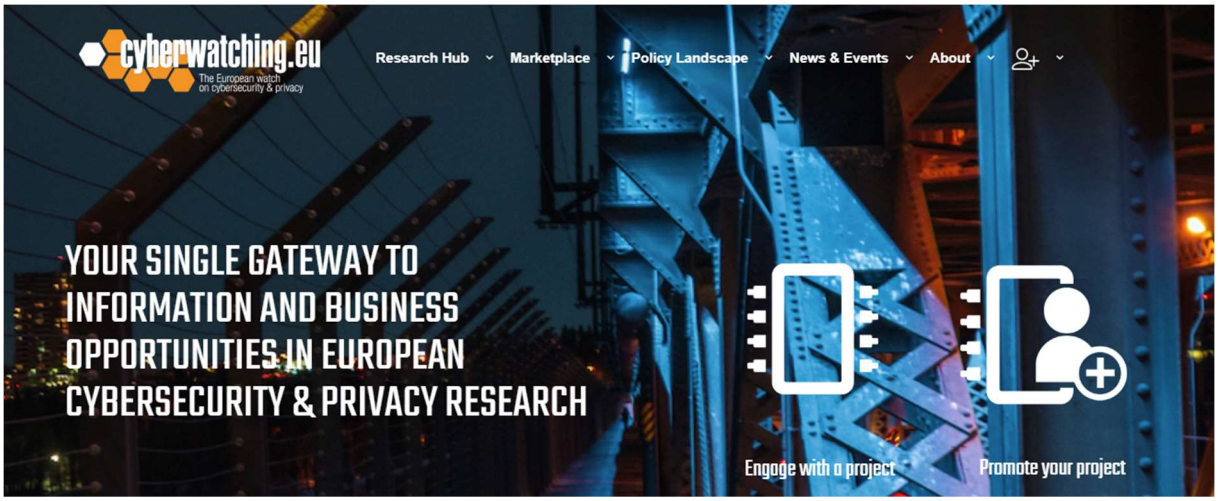

Figure 17: CyberWatching.eu homepage

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 who will have unlimited access to project information, and also to a Marketplace of services to help improve their cybersecurity offering.

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

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.

4.2.1 Interactions with THREAT-ARREST

THREAT-ARREST has been included in the Cyberwatching.eu Radar Data[9] in the Secure System section, in the ASSESS category (see Figure 18), since the project is still under development. The Radar depicts the state of the art of the EU-funded projects active in the context 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.

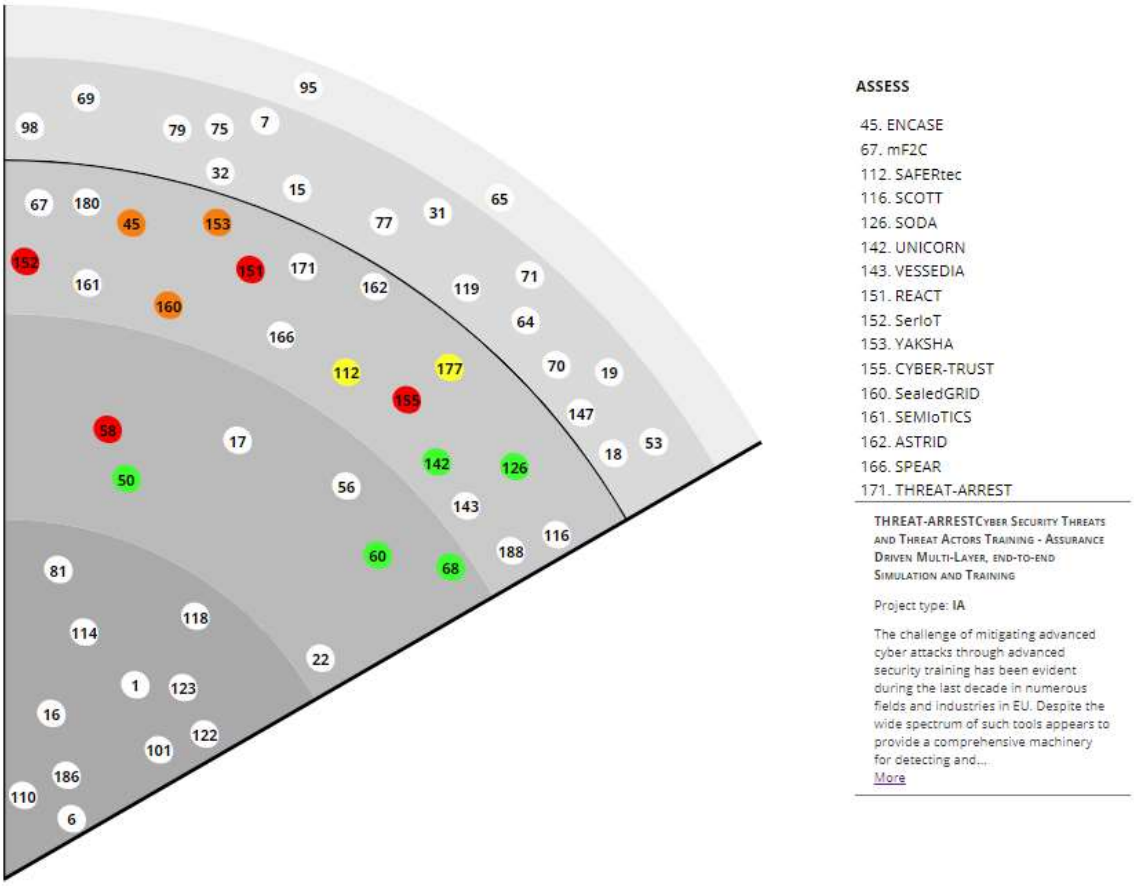

Figure 18: THREAT-ARREST in the Cyberwatching.eu Radar Data

4.3 SPIDER

SPIDER[10] (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.

[9] Cyberwatching.eu Radar: https://radar.cyberwatching.eu/
[10] SPIDER EU project: https://spider-h2020.eu

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.

4.3.1 Interactions with THREAT-ARREST

Some of THREAT ARREST partners 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.

4.4 SmartShip

SmartShip[11] 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.

4.4.1 Interactions with THREAT-ARREST

Also in this case, some of THREAT ARREST partners are part of SmartShip consortium. We believe that the two projects may collaborate in the definition and the testing of THREAT ARREST's pilot on smart shipping management.

4.5 SEMIoTICS, Ideal-Cities, and CE-IoT

The three collaborating EU projects, namely the SEMIoTICS[12], Ideal-Cities[13], and CE-IoT[14], deal with security and privacy issues in smart environments and IoT settings (e.g. (Alexandris et al., 2018; Hatzivasilis et al., 2019b; Hatzivasilis et al., 2019c; Hatzivasilis et al., 2019d; 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.

4.5.1 Interactions with THREAT-ARREST

Also in this case, some of THREAT ARREST partners are part of the related consortiums. We are in close collaboration with all these members in order to co-organize workshops and conferences with higher impact to the targeted audience. At the moment, we successfully co-organize the *"Special Session on Security & Privacy for Intelligent, 5G-Enabled IoT Ecosystems"*[15], in conjunction with the IEEE CAMAD 2019 conference (Soultatos et al., 2019; Hatzivasilis et al., 2019e), in Limassol, Cyprus (see Figure 19). Now, we have just started planning the potential upcoming workshops/conferences for 2020.

[11] SmartShip EU project: https://smartship2020.eu
[12] SEMIoTICS EU project: https://www.semiotics-project.eu/
[13] Ideal-Cities EU project: https://www.ideal-cities.eu/
[14] CE-IoT EU project: https://www.ce-iot.eu/
[15] Special Session in IEEE CAMAD 2019: http://camad2019.ieee-camad.org/wp-content/uploads/sites/51/2019/04/SS05.pdf

IEEE CAMAD 2019 (11-13 Sept. 2019, Limassol, Cyprus)

SPECIAL SESSION ON SECURITY & PRIVACY FOR INTELLIGENT, 5G-ENABLED IOT ECOSYSTEMS

CALL FOR PAPERS

Europe is faced with economic and societal challenges such as ageing of population, ensuring societal cohesion, and sustainable development. The introduction of digital technologies in economic and societal processes is key to address these challenges and, while the fifth generation (5G) mobile communications are already upon us, the next steps in their evolution will be key in supporting this societal transformation, while also leading to a fourth industrial revolution that will impact multiple sectors. 5G is expected to transform our lives and unleash enormous economic potential. There is now the opportunity to define and develop 5G networks technologies with the long term and sustainable support of new and diverse connected devices and services, towards the realization of the pervasive computing vision. Nevertheless, some important challenges and complexities will have to be addressed in the way towards the provision of pervasive mobile 5G services, such as: sustaining massively generated network traffic with heterogeneous requirements; providing networking infrastructures featuring end-to-end connectivity, security and resource self-configuration; enabling trusted information sharing between tenants and hosts systems, and, ultimately; enabling new services and applications (e.g., communications with smart vehicles, high-speed trains, drones, industrial robots). These present diverse and often-conflicting needs for high bandwidth, lower latency, better reliability, massive connection density and improved energy efficiency. Moreover, this increasing complexity of the smart environments and the unprecedented levels of data sharing and cyber systems interoperability, have also led to increasingly sophisticated, stealthy, targeted, and multi-faceted cyber-attacks. In light of the latter, the provision of effective management of the associated cyber security risks in organizations and enterprises is becoming even more important, due to the sheer complexity of cyber systems that need to be secured and the ever-increasing number and level of sophistication of cyber-attacks.

Figure 19: THREAT-ARREST's Special Session in IEEE CAMAD 2019

5 Conclusions and Future Steps

Deliverable 8.4 presented the work conducted during the first year of the THREAT-ARREST project regarding the liaison with stakeholders. We described the stakeholder engagement strategy that we put in place to this aim, in particular, how we defined and identified the stakeholders and the results of concrete actions to get engaged with them.

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 next and final version of this report will be documented at M30, under the deliverable "D8.7 – The stakeholders' engagement & online channels 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. Towards the Insurance of Healthcare Systems. 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol. 11981, Luxembourg, 27 September 2019, pp. 1-14.

[4] Hatzivasilis, G., et al., 2019b. Secure Semantic Interoperability for IoT Applications with Linked Data. IEEE Global Communications Conference (GLOBECOM 2019), IEEE, Waikoloa, HI, USA, 9-13 December 2019, pp. 1-7

[5] Hatzivasilis, G., et al., 2019c. 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.

[6] Hatzivasilis, G., et al., 2019d. 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.

[7] Hatzivasilis, G., et al., 2019e. 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.

[8] 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.

[9] 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

Activity #1	
Person in Charge	Lara Mauri
Unit	UMIL
Time	June 2019
Place	Carovigno, Italy
Event name	IDE'19: Industry Digital Evolution
Event Description	Summer School organized by the University of Salento open to researchers from European Academy and Industry (small and medium enterprises of South Italy)
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S5: Large companies
No. attendees	100
Cost of the activity	€ 600.00
Coverage	Country-level
Communication channel	Conference
Overall Feedback	Attendees have shown interest in the model-based approach of THREAT-ARREST and its approach to cybersecurity training

Activity #2	
Person in Charge	Marinos Tsantekidis, Othonas Soultatos, Sotiris Ioannidis, Michalis Smyrlis, Sebastian Pape, Kristian Beckers, Ludger Goeke
Unit	TUBS, FORTH, STS, SEA
Time	September 2019
Place	Heraklion, Greece
Event name	6th Network and Information Security (NIS'19) Summer School
Event Description	"Summer school jointly organised by the European Union Agency for cybersecurity (ENISA) and the Foundation for Research and Technology - Hellas (FORTH). The theme for this year was "Security Challenges of Emerging Technologies". SEA provided sessions of their card game PROTECT with a shipping scenario to the attendees.
Type of Audience	S1: Start-up and SMEs S2: University and R&D organizations S3: Policy makers S5: Large companies
No. attendees	100
Cost of the activity	€ 600.00
Coverage	Worldwide
Communication channel	Poster presentation
Overall Feedback	Attendees have shown interest in the simulation/emulation aspect in conjunction with the gamification aspect of THREAT ARREST and its approach to cybersecurity training

Activity #3	
Person in Charge	Ludger Goeke
Unit	SEA
Time	January 2020
Place	Munchen, Germany
Event name	IT-Risikofaktor Mensch (IT risk factor human)
Event Description	Information and networking event regarding security awareness organized by the Zentrum Digitaisierung Bayern (Center Digitalisation Bavaria). Short presentation of the project after the regular talks. Conversation with participants and distribution of project-flyer during networking part of the 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	60
Cost of the activity	€ 277.80
Coverage	Country-level
Communication channel	Knowledge exchange programme
Overall Feedback	Attendees have shown interest in the overall project, especially in Serious Gaming.

Activity #4	
Person in Charge	George Hatzivasilis, Othonas Soultatos
Unit	FORTH
Time	September 2019
Place	Limassol, Cyprus
Event name	24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019)
Event Description	THREAT-ARREST co-organized with other EU projects (SEMIoTICS, IdealCities, and CE-IoT) a special session in the conference. During this event, there was a poster presentation of the project. Flyers were distributed as well.
Type of Audience	S2: University and R&D organizations S5: Large companies
No. attendees	200
Cost of the activity	€ 500.00
Coverage	Worldwide
Communication channel	Conference
Overall Feedback	Attendees were interested about the modelling of the training process and its overall integration with the REST platform modules

Activity #5	
Person in Charge	George Hatzivasilis, Othonas Soultatos, Sotiris Ioannidis, Marinos Tsandekidis, Michalis Smyrlis, Chiara Braghin, Ludger Goeke, Sebastian Pape
Unit	FORTH, TUBS, STS, UMIL, SEA
Time	September 2019
Place	Luxembourg
Event name	The European Symposium on Research in Computer Security (ESORICS)
Event Description	THREAT-ARREST organized the workshop MSTEC. Except from the research papers, the overall project was presented via a poster in the main conference event. Flyers were also distributed.
Type of Audience	S2: University and R&D organizations S5: Large companies
No. attendees	300
Cost of the activity	€ 700.00
Coverage	Worldwide
Communication channel	Conference
Overall Feedback	Except from the poster and flyers, papers were presented during the MSTEC workshop, detailing the CTTP modelling, system assurance technologies, emulated components, and serious gaming. The attendees were interested in all these topics. The presentations were made by FORTH, UMIL, STS, and SEA.

Activity #6	
Person in Charge	George Hatzivasilis
Unit	FORTH
Time	August - September 2019
Place	Heraklion, Greece
Event name	Marie Curie Secondment programme - CyberSure
Event Description	Personnel exchange between FORTH and the Cypriot Internet provider CABLENET. This project examines the insurance of cyber-systems. During these knowledge exchange and training sessions, THREAT-ARREST was considered as a mean to train the organization's personnel in an attempt to mitigate the risk for the insurer, and thus, reducing the amount of the insurance contract that must be paid by CABLENET. The event included detailed description of the THREAT-ARREST platform, poster presentation, and flyer distribution.
Type of Audience	S1: Start-up and SMEs S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	20
Cost of the activity	--
Coverage	Organization-level
Communication channel	Knowledge exchange programme
Overall Feedback	The organization's administration personnel were interested in the economic part and how training can decrease the overall costs for security certification and insurance. The technical and security personnel were interested in the security awareness features and the subsequent enhancement of the protection level.

Activity #7	
Person in Charge	Sotiris Ioannidis, Manos Athanatos
Unit	FORTH
Time	September 2019
Place	Athens, Greece
Event name	Researcher's Night 2019
Event Description	The THREAT-ARREST concept was presented to the general public
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	Poster presentation
Overall Feedback	Attendees were interested in the overall concept of cyber-ranges and the opportunity of obtaining hands-on experience on cyber-security

Activity #8	
Person in Charge	Takis Varelas, George Bravos, Sotiris Ioannidis
Unit	DANAOS, ITML, FORTH
Time	November 2019
Place	Piraeus, Greece
Event name	2nd Workshop of EU Research & Innovation Maritime Projects, The Hellenic contribution
Event Description	The THREAT-ARREST concept applied in shipping sector was presented by Dr. George Bravos from ITML to an audience with maritime background (Shipping companies, Associations, Universities, Class societies, etc.)
Type of Audience	S1: Start-up and SMEs S4: Critical Infrastructure providers S5: Large companies
No. attendees	120
Cost of the activity	--
Coverage	Country-level
Communication channel	Conference
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 shipping company against cyber threats in ship operation

Activity #9	
Person in Charge	Lucia Bisceglia
Unit	ARESS
Time	September 2019
Place	Bari, Italy
Event name	Mediterranean Forum on Health
Event Description	The project THREAT-ARREST was presented during the speech in a panel about Cancer Registries (pilot)
Type of Audience	S2: University and R&D organizations S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	500+
Cost of the activity	--
Coverage	Regional
Communication channel	Conference
Overall Feedback	Attendees were interested about the training in cybersecurity for work force in health sector

Activity #10	
Person in Charge	Vito Petrarolo
Unit	ARESS
Time	October 2019
Place	Milano, Italy
Event name	Legal Privacy & Cyber Security
Event Description	The project THREAT-ARREST was presented during the speech in morning session "Protection of epidemiological databases and European cooperation: the THREAT-ARREST Project"
Type of Audience	S1: Start-up and SMEs S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	200
Cost of the activity	--
Coverage	Country-level
Communication channel	Conference
Overall Feedback	The conference was about GDPR and cyber security in health care sector. ARESS showed the threat arrest project and platform related to the security of epidemiological databases. The intervention has received the keen interest of the audience

Activity #11	
Person in Charge	Bird & Bird team
Unit	B&B
Time	September 2018
Place	
Event name	Publication of a press release
Event Description	Bird & Bird website: Press release on the THREAT-ARREST Project and the specific role of B&B
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	252 (General audience of the B&B website, interested in legal issues or in need of legal assistance)
Cost of the activity	--
Coverage	Worldwide
Communication channel	Web site
Overall Feedback	

Activity #12	
Person in Charge	Bird & Bird team
Unit	B&B
Time	10-14 September 2019
Place	Trier, Germany
Event name	ERA Summer Course on EU Data Protection Law
Event Description	Workshop on the successful implementation of the EU General Data Protection Regulation in their daily practice.
Type of Audience	S1: Start-up and SMEs S3: Policy makers S4: Critical Infrastructure providers S5: Large companies
No. attendees	60
Cost of the activity	--
Coverage	Europe
Communication channel	Conference
Overall Feedback	The team discussed the THREAT-ARREST GDPR compliance with the participants

Activity #13	
Person in Charge	Bird & Bird team
Unit	B&B
Time	5 March 2019
Place	
Event name	Data Law Camp: Construire un droit des données, Designing Data Law
Event Description	Working sessions dedicated to the shaping of European Data Law. Discussion themes: • Data and Intellectual Property • Data and Competition • Data and Trade Secrets • Data as a Legal Object • Data and Public Authorities • Personal Data and Business • Data and Automated Processing • Data, Science and Education
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	150
Cost of the activity	--
Coverage	European
Communication channel	Conference
Overall Feedback	Representing THREAT-ARREST and giving a presentation on “Data Breaches at the Crossroads of Privacy, Fintech and Corporate Law”. A book compiling the series of articles has been produced and distributed (50 copies)

Activity #14	
Person in Charge	Bird & Bird Team
Unit	B&B
Time	28 January 2019 - 4 February 2019
Place	
Event name	Big Data & Issues & Opportunities: Cybersecurity – Articles series
Event Description	Publication of a series of articles on Bird & Bird website, Lexology, Digital Business law https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-breach-related-obligations
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	
Cost of the activity	
Coverage	Worldwide
Communication channel	Website
Overall Feedback	The THREAT-ARREST project has been cited in the article.

Activity #15	
Person in Charge	Bird & Bird Team
Unit	B&B
Time	4 April 2019
Place	Brussels, Belgium
Event name	Towards assessing the risk in personal data breaches
Event Description	EDPS-ENISA Conference on the current state of play in personal data breach notification
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	200
Cost of the activity	--
Coverage	European
Communication channel	Conference
Overall Feedback	B&B represented THREAT-ARREST in the context of the workshop

Activity #16	
Person in Charge	Bird & Bird Team
Unit	B&B
Time	24 April 2019
Place	Brussels, Belgium
Event name	Data Law – Why It Matters to Business
Event Description	Evening Lecture at the Vesalius College
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	60
Cost of the activity	--
Coverage	Regional
Communication channel	Conference
Overall Feedback	Presentation on the EU Data Economy: legal aspects of Data Law and related topics such as free flow of data, data sharing, data ownership, privacy, cybersecurity, data breach and more. B&B discussed how topics can related in the cybersecurity training context.

Activity #17	
Person in Charge	Bird & Bird Team
Unit	B&B
Time	June 2019
Place	Brussels, Belgium
Event name	Seminar on Data Breaches
Event Description	Seminar organized by Bird & Bird on handling risk of data breaches
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	60
Cost of the activity	--
Coverage	Regional
Communication channel	Conference
Overall Feedback	THREAT-ARREST training approach has been presented among best practices on how to prepare for, handle, and follow up on a data breach and how to mitigate the risk of a breach through strong information governance

Activity #18	
Person in Charge	TUV HELLAS Team
Unit	TUV HELLAS
Time	26 September 2019
Place	Athens, Greece
Event name	(ISC)² Hellenic Chapter Fall19 Event
Event Description	Chapter business seasonal meeting
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	60
Cost of the activity	--
Coverage	Regional
Communication channel	Industry event
Overall Feedback	Presentation of the THREAT-ARREST project to the (ISC)² Greek Chamber (Cybersecurity Professionals "jobs gap" / need for hands-on training / importance of Cyber-Ranges as Training tools / presentation of THREAT-ARREST and explanation of the Platform's advantages)

Activity #18	
Person in Charge	Ernesto Damiani
Unit	UMIL
Time	
Place	Boston, MA, USA
Event name	Virginia Tech Meeting
Event Description	Meeting with the Virginia Tech with the Virginia Cyber-Range research group
Type of Audience	S2: University and R&D organizations S3: Policy makers
No. attendees	20
Cost of the activity	--
Coverage	Regional
Communication channel	Meeting
Overall Feedback	The THREAT-ARREST vision has been presented to the VT research center and senior faculty, in particular with the steering committee of the Virginia Cyber-Range project (https://www.virginiacyberrange.org/), getting important feedback on the development of the overall infrastructure, and appreciation on the model-driven approach of THREAT-ARREST.