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

D8.1: The stakeholders' engagement plan & online channels development [†]

Abstract: The objective of this document is to present the stakeholders' engagement and online channels plan and approach followed by the consortium communication teams during the whole duration of the project.

Contractual Date of Delivery	30/11/2018
Actual Date of Delivery	30/11/2018
Deliverable Security Class	Public
Editor	*Michael Vinov (IBM)*
Contributors	All partners
Quality Assurance	*George Hatzivasilis (FORTH),* *Dirk Wortmann (SIMPLAN)*

[†] *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
Socal 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 Sanitaria Pugliese (ARES)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Hatzivasilis (FORTH)*
2. *Dirk Wortmann (SIMPLAN)*

Revisions

Version	Date	By	Overview
1.0	28/11/2018	Editor	Final version
0.3	28/11/2018	Editor	Changes based on the internal review comments
0.2	22/11/2018	Editor	Updated draft
0.1	05/11/2018	Editor	First draft

Table of Contents

1 Introduction

The objective of this document, as part of the Work Package 8 initial set of deliverables for M3, is to present the plan and approach followed by the consortium communication teams during the whole duration of the project. D8.1 is the first deliverable of Task 8.1 – Communication and Engagement of stakeholders. This task aims at addressing the strategic objective of extending the project's offerings to key players from industry with special focus on training towards dealing with advanced cyber threats, at disseminating the technological and business-related knowledge acquired through the project. In particular, this task aims to raise awareness about the project concept, developments and findings to all key actors (large industry, SMEs, academics, policy makers) and ensure the success of the project dissemination strategy and social media presence to provide the maximum visibility and public awareness of the project results.

TREAT-ARREST started with an initial survey of the stakeholders, results and channels through which information is to be disseminated. Then, dissemination activities were split into two streams: awareness and knowledge transfer. The strategy applied to the former is based on first recruiting audiences through the website and social media channels, ready to be exploited during the project as the results mature and take shape. In parallel, knowledge transfer should be achieved through the standard publishing of results in conferences and in journals.

2 Stakeholders Engagement Plan & Online Communication Channels Development

One of the major goals of the THREAT-ARREST project is to extend the project's offerings towards industrial key players with special focus on advanced cyber threats training, at disseminating the technological and business-related knowledge acquired through the project.

The aim of the communication strategy is to take up of THREAT-ARREST results for the creation and support of a dynamic innovation ecosystem (Ferrera et al., 2018; Cesena et al., 2017) around THREAT-ARREST results, targeting to achieve maximum market visibility for the technologies and services developed. Moreover, THREAT-ARREST will ensure that the research activities – both the action and, when available, its results – are made known to society at large in such a way that they can be understood by non-specialists, thereby improving the public's understanding of science.

We plan to achieve this goal by the following means:

- **Knowledge transfer and awareness**
  - Establish communication channel to effectively and efficiently reach the target audience of cyber systems platform owners, application developers and entrepreneurs so that they engage in learning, providing feedback about, and experimenting with THREAT-ARREST framework.
  - Define and implement promotional campaigns, notably towards cyber systems platform owners, application developers and entrepreneurs.
  - Organize the necessary physical workshops and gatherings, at least one being linked to and visible within a large-scale event in Europe, as well as online events/tools such as webinars.
  - Organize a cyber security threats mitigation contest, targeted to reward the most innovative cyber threat responses based on the THREAT-ARREST framework. Our plan is to organize this contest in a summer schools organized by THREAT-ARREST.
  - Develop an approach to reach relevant stakeholders and partners, who may contribute to further enhance the scope of the THREAT-ARREST framework targeting to bring cyber security solution providers after the end of the project.
  - Develop a scalable online platform, capable of growing up to large number of users enabling networking activities across all the stakeholders of the wider ecosystem of cyber systems and cyber security around THREAT-ARREST. These would, for example, include: web entrepreneurs, investors, mentors, serial entrepreneurs, accelerators, crowd-funding platform providers, large corporations, media, research. The platform should allow advanced functionalities on training and simulation to support the communities' needs.
  - Combine expertise of the key players coming from different application and business domains and ensure their collaboration.
- **Public information**
  - Define and manage activities facilitating successful and effective knowledge and project results dissemination to the general public.
  - Establish information portal as a communication channel, reflecting the project's progress and outcomes. This portal should be easy to use and available to key players as well as to the general audience.

  - Establish ways of cooperation with social media to inform general audience about project's goals, progress and outcomes.
  - Participate in relevant European Commission's events as well as in large public events.
- **Individual dissemination**
  - Allow each project participant to participate in their own dissemination efforts.

Stakeholders Engagement Plan & Communication Channels Development will follow a cyclic approach of *plan – act – observe.* That is to say, actions are planned (targeting a specific audience, with a specific objective), carried out by the assigned partner, and monitored regarding achieving the objective. The data collected is used to modify the engagement and communication strategy to ensure that the Task 8.1 goals are reached and all the above topics and means are covered. This re-planning, if needed, will occur on-the-fly and will be formally described in the following Task deliverables – D8.4 and D8.7.

3 Communication Channels

We realize that target audience for THREAT-ARREST Engagement and Communication plan should be separated into two major parts – the project consortium members and the general public. The first audience includes the project industrial and academic partners. We plan to encourage and ensure efficient knowledge transfer between all the project participants and keep them aware of the on-going project outcomes and results. The general public and cybersecurity-related communities outside the project consortium will be updated about the project progress through the project web page, social media channels, conferences and workshops.

The following channels are considered for dissemination and sharing the project results. For completeness of the project communication activities, we define and list here both on- and off-line communication channels.

Community conferences

This refers to events organised by the European Commission or Support Action projects for the good of the Horizon 2020 project community.

Industry events

This category refers equally to tradeshows and commercial conferences. In the case of the former, having an exhibition stand could be a strong way to get feedback from innovative start-ups and potential collaborators. In the case of the latter, a well-placed conference presentation could recruit influential or well positioned individuals who could advise the project and utilize its results. Analyst events could also be useful to get widespread dissemination to market actors, but requires a strong message and tangible results.

Project Conferences, Workshops and Meetings

In this category we refer to conferences, workshops and meetings hosted by the project participants in which a series of presentations, technical sessions and discussions about the project are given. These should include hand-on demos and could be interspersed with invited talks on related subjects. We believe that project conferences and meetings is the most efficient communication channel to encourage and ensure efficient knowledge transfer between all the project participants and keep them aware of the on-going project outcomes and results.

Scientific conferences

Scientific conferences are those which cater to a largely academic audience and which present a series of papers on a given topic. This is an ideal way to explain some of the more innovative and detailed aspects of the project. They provide a forum for the discussion and adoption of the research output. Commonly after delivering a presentation at a conference, the conference proceedings will include a full-length paper from the speaker. The principle ones are: ACM/IEEE International Conference on Cyber-Physical Systems, IEEE Symposium on Security and Privacy, etc.

Newsletter

This is a periodical report about the project. Typically, 3 or 6 monthly newsletters will inform subscribers of developments in the project. It can be a format to maintain a large group of observers and other stakeholders up to date and to invite participation at key points. It can be used for announcements, such as the availability of results or software. Newsletters have been largely superseded by social media and require the recruitment of subscribers prior to launch.

Posters

Posters in this context refer to detailed, typically A2, posters used to display at the posters sessions of conferences. They are designed to be read by conference participants who can then be further assisted by a project participant on site.

Press releases

Press releases continue to be a strong format for announcing achievements in a project and for reaching the mass media. Their use is standardised thus they can reach broad coverage quickly.

Videos

Companies and projects are increasingly using the combination of animated graphics and voiceovers to relay complex messages in an easy-to-understand format. They can be hosted on the website, shown at events and shared via social media.

Website

The project website should cover a wide range of functions, from a mere information page, to a hub of activity where the project participants and third parties can interact. We plan to make the website interactive and participative to enable a larger number of stakeholders to discover the project. The website will provide free, open and publicly searchable access to all the public deliverables, to technical reports, data and results (if data subjects have given permission for this), to software tools and libraries, to white papers and also to all the other non-confidential documents that will be generated in the course of THREAT-ARREST.

Whitepapers

Unlike Scientific Conferences proceedings, whitepapers refer to self-published papers. These are convenient because of their speed to publish and the full control of their copyright and distribution. They are ideal for descriptions of the technical approach and results, predictions and visions, and exploitation material, where the research over the state of the art is not the primary focus of the article.

4 Social Media

Blog

Blogs are frequent and short articles posted on the project website or to ‘open blogs’ and can be focused on a specific topic or on a broader subject.

Forums

Forums are a useful mean, particularly where there are many users, such as in very large projects, those with many use cases or those with open calls or public access. They can be used as internal tools.

News/ RSS feed

The project can publish news on its website, to announce progress, milestones, events, the publishing of papers, or future plans. An RSS feed can be set up for subscribers.

Wikipedia / content seeding

Although Wikipedia is not the only outlet for content seeding, it is one of the better ones. The concept is to implant references to the project in relevant articles. This can then draw readers to the website or cited material. It is important to act responsibly and not spam the outlet, contributions should be fair and relevant, and abide by the rules of Wikipedia.

The following table defines the expected impact of the above communication activities and channels:

Planned Means	Success Indicators	Coverage
THREAT-ARREST website	>5000 accesses annually >500 downloads	Worldwide
Press releases	≥10	Europe
Newspapers (business and normal)	≥10	Europe
Newsletter	≥9	Worldwide
Social Media (Twitter, LinkedIn, ResearchGate)	≥500 Followers	Worldwide
Public lecture and/or networking event for end users & general public	≥2,>50 attendees (each)	Europe
Public lecture and/or networking event for policy makers	≥2, >20 attendees (each)	Europe
Policy events targeting policy makers of EU, National, Regional and Local Authorities	≥4, >50 attendees (each)	Europe
Information days	≥3, 100 attendees (each)	Europe

5 Conclusions

The THREAT-ARREST project aims to communicate itself and its findings intensively to various communities. Research publications and presentations will aim to target various groups of academic and industrial researchers and will add scientific weight and credibility to our findings. Press releases and news articles will be used to communicate project results and major project life events (start, finish, key milestones) to both technical and general audience. We will also take advantage of opportunities as they arise for radio/TV interviews, public seminars and general articles in both the technical and non-technical press. The project website will be used to provide open access to project results, public deliverables, software tools, technical reports, white papers, (video) tutorials, podcasts etc., and will serve as a key resource for those wishing to use the project results, whether they are acting as an academic researcher, scientific, commercial or independent software developer, public sector worker, educator or private individual. By making research results public in this way, we especially aim to engage with the software developers and cyber communities, who may not normally have access to academic papers and reports. We will disseminate information about our tools and standards directly to customers, aiming to increase engagement with an already motivated group of cyber developers/scientists/users.

We will run open technical workshops that will showcase our work to interested parties. These will generally be co-located with major networking events. We will also engage with relevant cyber industrial/science/developer conferences, workshops etc., producing poster and demonstrations as necessary to communicate with the broader user community and especially with project managers and decision makers. Finally, we will communicate our results through established networks of excellence and other organisations.

The results of the above communication plan will be reported in the future THREAT-ARREST project deliveries D8.4 and D8.7.

References

[1] Cesena, M., et al. 2017. SHIELD Technology Demonstrators. CRC Press, Book for Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems, pp. 381-434.

[2] Ferrera, E., et al., 2018. IoT European Security and Privacy Projects: Integration, Architectures and Interoperability. CRIStin – SINTEF, Next Generation Internet of Things. Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation. Book Chapter 7, pp. 207-292.