



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

D8.8: The THREAT-ARREST dissemination and exploitation report v.2 †

Abstract: This deliverable provides the 2nd and last version of the dissemination and exploitation report for the THREAT-ARREST project.

Contractual Date of Delivery	31/08/2021
Actual Date of Delivery	31/08/2021
Deliverable Security Class	Public
Editors	<i>Spanoudaki Sofia, Smyrlis Michalis, Vasileios Bouras (STS) Vassilis Prevelakis (TUBS)</i>
Contributors	All partners
Quality Assurance	<i>George Hatzivasilis (FORTH), Martin Kunc (CZNIC)</i>

† 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 Hatzivasilis (FORTH)*,
2. *Martin Kunc (CZNIC)*

Revisions

Version	Date	By	Overview
0.6	11/08/2021	LSE	LSE individual exploitation plan
0.5	03/08/2021	STS, TUV	Final Joint Exploitation plan amendments
0.4	27/07/2021	STS	ITML, Final Joint exploitation plan
0.3.1	21/07/2021	Vassilis Prevelakis (TUBS)	Section 2 “Dissemination”
0.3	19/07/2021	STS	AReSS, SIMPLAN, CZ.NIC Contribution
0.2.1	12/07/2021	STS, ATOS	ATOS Contribution
0.2	07/07/2021	Smyrlis Michalis (STS), Ludger Goeke (SEA)	Initial Exploitation Strategy for STS, SEA
0.1	07/06/2021	Vassilis Prevelakis (TUBS)	First Draft

Executive Summary

Deliverable “D8.8 – The THREAT-ARREST dissemination and exploitation report v.2”, is a joint output of the tasks “T8.2 – Sustainability management and Business continuity” and “T8.3 – Dissemination plan and activities”. As such, the main objective of the current document is to deliver the final dissemination and exploitation outcomes of the THREAT-ARREST project.

This second and last version of the deliverable provides the final analysis of the exploitation and dissemination activities of the project in terms of competitiveness and exploitation of the project results for individual project participants and the consortium as a whole. Along with the deliverable “D8.7 – The stakeholders’ engagement & online channels report v.2”, which was delivered at M30, we determine the means to accomplish the milestone “MS8 – 2nd pilot execution and final platform’s evaluation, final business plan, standardisation, dissemination, and exploitation reports”, which forms the final dissemination and exploitation reports (among others), due on M36.

In short, the consortium was quite active during the course of the project and achieved *all dissemination goals*. In total, i) *51 peer-reviewed papers* were published in top-tier conferences/journals and online, ii) *2 special issues* were published with *1 more pending*, iii) a large number of *talks, seminars and presentations* were performed at several established scientific venues, iv) a number of *lectures* were given and *degrees awarded* by the academic partners in their educational programs, v) several *meetings with stakeholders* and other interested parties were held, vi) the project’s *website* and *social media* were maintained regularly and the *brochure* was handed out to all venues where partners attended, vii) a number of *scientific events* (conferences, workshops, demonstrators, summer schools) were organised by the consortium, viii) several *videos* were created and either published online or projected at scientific events.

An *exploitation agreement* was prepared, establishing an *exploitation committee* that will manage any potential business opportunity after the end of the project. The initial lifetime of this committee was set for one year and can be extended afterwards. The joint exploitation strategy is that the consortium will try to *outsource the platform to a business* which will continue the platform support. *STS*, which also led the overall CTPP modelling concept, express its *interest for acting as the company that will continue the commercialization* of the THREAT-ARREST platform. Moreover, *LSE*, which is the smart energy pilot, is very *interested in using the new product as a customer* and purchase a customized programme for a wider range of its employees. These aspects will be the subject of a formal contract between the exploitation committee and the involved parties. Concerning the *contribution to standards*, the consortium had initial conversations and *project presentations with ISACA and ISC²* and a *platform demonstration with CSA*. The goal was to achieve the affiliation of the platform by these organizations and examine the opportunity for future collaboration. CSA requested to examine the potential of establishing training programmes for the top 10 threats for cloud infrastructure. Regarding the *European Competence Network*, THREAT-ARREST supported several of its actions and collaboration initiatives with other cyber-ranges, including surveys, platform demonstrations, joint workshops, summer schools, and other communication/dissemination events. A first *technical federation* was defined between KYPO (supported by CONCORDIA), THREAT-ARREST, and SPIDER, as well as an initial *operation federation* with ECHO’s cyber-ranges marketplace.

Table of Contents

1	INTRODUCTION	8
2	DISSEMINATION	9
2.1	DISSEMINATION OBJECTIVES.....	9
2.1.1	<i>Online dissemination</i>	9
2.1.2	<i>Scientific publications</i>	10
2.1.3	<i>Organization of International Scientific Events</i>	10
2.1.4	<i>System-level demonstrations</i>	11
2.2	PUBLISHED CONFERENCE/JOURNAL PAPERS AND ARTICLES.....	11
2.2.1	<i>Journals</i>	11
2.2.2	<i>Articles</i>	13
2.2.3	<i>Conference/Workshop papers</i>	13
2.2.4	<i>Special Issues in Scientific Journals</i>	16
2.3	TALKS, SEMINARS, AND PRESENTATIONS.....	16
2.4	ACADEMIC DISSEMINATION	19
2.5	OTHER DISSEMINATION ACTIVITIES.....	19
2.6	UPDATES REGARDING THE COMMUNICATION AND ENGAGEMENT OF STAKEHOLDERS' ACTIVITIES.....	21
2.7	EVALUATION OF EFFORTS AGAINST THE INITIALLY SET GOALS.....	22
3	EXPLOITATION	25
3.1	OVERALL AIM	25
3.2	FINAL EXPLOITATION BACKGROUND	25
3.2.1	<i>Analysis of exploitable items</i>	25
3.3	FINAL INDIVIDUAL EXPLOITATION STRATEGIES.....	27
3.3.1	<i>Sphynx Technology Solutions AG</i>	27
3.3.2	<i>ATOS Spain S.A</i>	28
3.3.3	<i>IBM Israel – Science and Technology LTD</i>	28
3.3.4	<i>Social Engineering Academy GmbH</i>	28
3.3.5	<i>Information Technology for Market Leadership</i>	29
3.3.6	<i>Bird & Bird LLP</i>	29
3.3.7	<i>DANAOS Shipping Company LTD</i>	29
3.3.8	<i>TUV HELLAS TUV NORD</i>	30
3.3.9	<i>LIGHTSOURCE LAB LTD</i>	30
3.3.10	<i>CZ.NIC, ZSPO</i>	31
3.3.11	<i>SIMPLAN AG</i>	31
3.3.12	<i>Agenzia Regionale Strategica per la Salute ed il Sociale</i>	32
3.4	FINAL JOINT EXPLOITATION PLAN	32
3.4.1	<i>Final THREAT-ARREST Exploitable assets</i>	32
3.4.2	<i>THREAT-ARREST's Exploitation Agreement & Business Model</i>	37
3.4.3	<i>Final THREAT-ARREST's commercialization life-cycle and Tasks synergies</i>	37
4	CONCLUSIONS	40
5	REFERENCES	41
APPENDIX		42
	THREAT-ARREST BROCHURE.....	42
	NEWSLETTER ISSUE 4 (FEBRUARY 2020).....	43
	NEWSLETTER ISSUE 5 (MAY 2020)	44
	NEWSLETTER ISSUE 6 (SEPTEMBER 2020).....	45
	NEWSLETTER ISSUE 7 (JANUARY 2021)	46
	NEWSLETTER ISSUE 8 (MAY 2021)	47
	NEWSLETTER ISSUE 9 (AUGUST 2021).....	48

List of Abbreviations

AHPS Atos High Performance Security

BDS Big Data & Cybersecurity

ARI Atos Research & Innovation

CTTP Cyber Threat and Training Preparation

DFP Data Fabrication Platform

GKO Global Key Offering

GRC Governance, Risk and Compliance

IH Innovation Hub

IoT Internet of Things

JVT Jasima Visualization Tool

SIEM Security Information and Event Management

List of Figures

Figure 1: Virtual meeting with CSA in search of possible collaboration 17

Figure 2: Marinos Tsantekidis presenting at “Secure Runtime Environments” webinar 18

Figure 3: George Hatzivasilis presenting at “Secure Runtime Environments” webinar..... 18

Figure 4: George Hatzivasilis presenting at CRST workshop 2021 19

Figure 5: Call-for-participation banner for “Secure Runtime Environments” webinar 20

Figure 6: Call-for-Participation banner for CRST 2021 workshop..... 21

Figure 7: Exhibitor booth at COD2020 event 24

Figure 8: Social Engineering Memory card pair by the example of a baiting attack..... 26

Figure 9: THREAT-ARREST Business Model – New Business Entity – Supply Chain context 37

Figure 10: THREAT-ARREST commercialization lifecycle (take from “D8.6 – The THREAT-ARREST market analysis, business, and marketing plan v.2”)..... 38

Figure 11: THREAT-ARREST: Project Task Synergies aiming at Joint Exploitation 38

1 Introduction

The objective of this report is to summarize the dissemination and exploitation activities carried out by the THREAT-ARREST consortium during the second half of the project.

The THREAT-ARREST project disseminated its results and findings intensively to various communities. *Research publications and event presentations* that targeted various groups of academic and industrial researchers, added scientific weight and credibility to our findings. *Press releases and news articles* were used to publish project results to both technical and general audience, as well as public seminars and general articles in both the technical and non-technical press. The project's *website and social media* is used to provide open access to project results, public deliverables, software tools, technical reports, white papers, etc., and serves as a key resource for those wishing to use the project results, whether they are academic researchers, scientific personnel, commercial or independent software developers or private individuals.

Another important goal of the project is to maximize the exploitation of its outcomes and the successful implementation of its findings. Each of the consortium partners has devised an exploitation plan, which was included in the first version of this report (deliverable D8.5) and in this deliverable, they report the progress made based on that plan.

The deliverable is organised as follows: Section 2 deals with the dissemination activities of all partners: Section 2.1 lists the objectives of the project for completeness. Section 2.2 details all papers published in peer-reviewed conferences and journals, since the beginning of the project for completeness. Section 2.3 lists several talks, seminars, and presentations (with accompanying photos) carried out by the project partners, during the second half of the project. In Section 2.4, the academic partners detail in which way they incorporated the project into their programs. In Section 2.5, there is a list of additional dissemination activities. Section 2.6 contains a brief report on the communication and engagement of stakeholders' activities performed in the last six months of the project, after the submission of deliverable D8.7. Finally, in Section 2.7, there is a comparison of the archived efforts concerning the total duration of the project, against the initially set goals.

Following, Section 3 is organized as follows: Section 3.1 provides details regarding the overall aim of THREAT-ARREST's final exploitation strategy. Section 3.2 provides the final exploitation background of THREAT-ARREST by analysing the exploitable items of the THREAT-ARRESTS platform. Section 3.3 lists the final THREAT-ARREST partner's exploitation strategies. Lastly, Section 3.4 describes THREAT-ARREST's final joint exploitation plan.

Closing the deliverable, we offer our conclusions in Section 4.

2 Dissemination

In the following pages, we list the publications presented by the consortium in conferences as well as the presentations made at various events and forums, related to the project. Additional coverage of the project through other dissemination channels is also presented in this document, including releases in the popular press and references to the project. During the second half of THREAT-ARREST, the consortium published a total of **34 peer-reviewed papers** (here listed all 51 published during the whole project for completeness), in addition to organising **3 special issues in scientific journals**, plus **10 presentations, talks, and seminars**.

2.1 Dissemination Objectives

Four categories of dissemination channels have been established, each accompanied by its own content strategy paper. This combined approach ensures efficient dissemination of the technical activities of THREAT-ARREST based on the target audience's needs and involvement.

2.1.1 Online dissemination

The online channel is aimed at primary and secondary targets with diverse information needs and involvement (see section 2.7 for more details).

Project's website: The site¹ is a key instrument for supporting the dissemination of the research results. We regard the website as a “second stop” useful to primary targets who have already been reached via the other channels. Its aim is to provide sound support for those wishing to become champions of the THREAT-ARREST approach within their organizations, providing access to deliverables and presentation materials that support championing THREAT-ARREST adoption. Key results are published on the website, but also added-value services will be offered such as support in using THREAT-ARREST methodology. The project website was set up at a very early stage (M01) and is updated conscientiously and regularly.

Push announcements: The project is present on the major professional social networks, in particular Facebook², LinkedIn³, and Twitter⁴. Contacts already available to project partners were used to kick-start this group, which is a major instrument for recruiting interested parties. THREAT-ARREST social community group is the target for continuous informal communication with members, who can find brief first-hand reports from THREAT-ARREST research and development activities, increasing the timeliness of dissemination.

Regular Newsletter: Starting from M4, a regular quarterly newsletter is being sent out to interested parties outside the project partners including major stakeholders recruited via the other channels. The newsletter relies on a well-balanced mix of dissemination and infotainment content. All partner organisations contribute to the newsletter, which is made available free of charge through electronic means.

Brochure: A THREAT-ARREST folder and brochure was created in M3, distributed in all venues where project partners were involved in, and updated regularly. Distribution also includes a high-quality electronic version in portable document formats (e.g., PDF), which is downloadable from the website (see Appendix 1).

Technical videos: A THREAT-ARREST technical video of around 5 minutes of duration was developed in M04. It has been uploaded in YouTube and is also accessible via the project's website. The video focuses on the technical advancements of the THREAT-ARREST

1 <http://www.threat-arrest.eu/>

2 <http://www.facebook.com/Threat-Arrest-266454357324031/>

3 <http://www.linkedin.com/in/threat-arrest-706485175/>

4 <https://twitter.com/ArrestThreat>

methodology and approach, targeting the technical and business community of the Internet of Things (IoT). Moreover, we considered it to our advantage to create additional videos in order to showcase the specific tools and use-cases that the project developed. Eight more technical videos were created by the partners and were made available to the public. Finally, one professional promotional video was created that shows the project results. The videos are published in the project's YouTube channel⁵.

2.1.2 Scientific publications

THREAT-ARREST partners have been carefully selecting publication venues based on their scientific excellence and impact, privileging where possible open access publishing. Conferences and journals that were targeted for scientific dissemination include:

Journals: International Journal of Internet of Things; Advances in Internet of things (Scientific Research open access); ACM Transactions on Software Engineering and Methodology; ACM Transactions on Information and Systems Security; IEEE Transactions on Secure and Dependable Computing, IEEE Transactions on Information Forensics and Security; Computers and Security; IEEE/ACM Transactions on Networking; Springer International Journal of Information Security; Springer Wireless Personal Communications; Elsevier Network Security;

Magazines: IEEE Security and Privacy; IEEE Cloud Computing; and IEEE Internet Computing.

Conferences: ACM Conference on Computer and Communications Security; ESORICS – European Symposium on Research in Computer Security; ACM/IEEE International Conference on Cyber-Physical Systems; IEEE International Conference on Pervasive Computing and Communications; IFIP International Information Security and Privacy Conference; IEEE Symposium on Security and Privacy; ACM Conference on Computer and Communications Security; ACM Conference on Data and Application Security and Privacy; IEEE International Conference on Internet of Things; and European Conference on Smart Objects, Systems and Technologies.

Special Issues in Scientific Journals: The partners will take the initiative of jointly creating special issues in the area of IoT in scientific journals, and invite top international colleagues to be part of the initiatives.

2.1.3 Organization of International Scientific Events

In order to attract interest to our work and enhance the visibility of our contributions at an international level we have organized several international scientific events (see section 2.7 for more details).

Organization of conferences: THREAT-ARREST organized one significant international conference in the core research areas of the project.

Organization of workshops: THREAT-ARREST organized five international scientific workshops throughout its duration, co-located with top-tier conferences.

Organization of Summer Schools on Cyber Security Training and Simulation: THREAT-ARREST has organized two summer schools. These are aimed at delivering knowledge to researchers, and professionals on cyber security training and simulation platforms. Our plan was to organize these summer schools in M18 and M36. The first summer school “NIS Summer School 2019” was held in M12 (ahead of schedule). However, due to the ongoing COVID-19 pandemic, we had to modify our initial plans for the rest of the summer schools of the series.

⁵ <https://www.youtube.com/channel/UCBUClnDkE6cjYtw7cEgP0vQ>

NIS Summer School 2020 as well as 2021 had to be cancelled in light of the global health crisis. We are, nonetheless, organising a second summer school, right after the end of the project, in September 2021.

2.1.4 System-level demonstrations

THREAT-ARREST has demonstrated the project's platform capabilities (Hatzivasilis *et al.*, 2021; Hatzivasilis *et al.*, 2020; Smyrlis *et al.*, 2021; Smyrlis *et al.*, 2020) to several related venues.

Demonstrations in fairs and exhibitions: THREAT-ARREST demonstrated the project technical results in collaboration with a sister project also dealing with Cyber Ranges, CONCORDIA.

Demonstrations in EU related events: THREAT-ARREST organized two demonstrations of the project technical results in EU related events.

Demonstrations in major international conferences: THREAT-ARREST was demonstrated in IEEE GLOBECOM 2019, as well as the ENISA NIS 2019 summer school and the NATO's 4th NMIOTC Conference on Cyber Security in Maritime Domain.

Demonstrations to critical Stakeholders: The THREAT-ARREST platform and CTPP Programmes were demonstrated, on June 2021, to Cloud Security Alliance (CSA) Executives (Mr. Danielle Catteddu, CTO and Mr. Ryan Bergsma, Training Program Director). The demo was held as a virtual event and was part of THREAT-ARREST "Affiliation efforts" – within Task's "T8.4 – Contribution to Standards" requirements.

2.2 Published conference/journal papers and articles

The THREAT-ARREST Consortium put a lot of effort into disseminating the work carried out throughout the duration of the project to many venues, publishing a large number of academic papers and articles in the popular press. In total, we had **52 publications** on a variety of subjects. For completeness, they are all listed below:

2.2.1 Journals

- 1) G. Hatzivasilis, O. Soutatos, P. Chatziadam, K. Fysarakis, I. Askoxylakis, S. Ioannidis, G. Alexandris, V. Katos, G. Spanoudakis, "**WARDOG: Awareness detection watchdog for Botnet infection on the host device**", IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, vol. 4, pp. 1-15, May 2019 (DOI: 10.1109/TSUSC.2019.2914917)
- 2) E. A. Alkeem, S.-K. Kim, C. Y. Yeun, M. J. Zemerly, K. F. Poon, G. Gianini, P. D. Yoo, "**An Enhanced Electrocardiogram Biometric Authentication System Using Machine Learning**", IEEE Access – Special Section on Artificial Intelligence in Cybersecurity, vol. 7, pp. 123069-123075, August 2019 (DOI: 10.1109/ACCESS.2019.2937357)
- 3) S. Maghool, N. M.-J. Maghoolsaraei, M. Cremonini, "**An Enhanced Electrocardiogram Biometric Authentication System Using Machine Learning**", PLOS ONE, vol. 14, issue 12, article: e0225447, pp. 1-22, December 2019 (DOI:https://doi.org/10.1371/journal.pone.0225447)
- 4) G. Gianini, L. G. Fossi, C. Mio, O. Caelend, L. Brunie, E. Damiani, "**Managing a pool of rules for credit card fraud detection by a Game Theory based approach**", Future Generation Computer Systems, Elsevier, vol. 102, issue 2020, pp. 549-561, January 2020 (DOI: 10.1016/j.future.2019.08.028)

- 5) G. Hatzivasilis, O. Soultatos, S. Ioannidis, G. Spanoudakis, V. Katos, G. Demetriou, **“MobileTrust: Secure Knowledge Integration in VANETs”**, ACM Transactions on Cyber-Physical Systems – Special Issue on User-Centric Security and Safety for Cyber-Physical Systems, ACM, vol. 4, issue 3, Article no. 33, pp. 1-25, March 2020 (DOI: 10.1145/3364181)
- 6) S. Cimato, G. Gianini, M. Sepehri, R. Asal, E. Damiani, **“A cryptographic cloud-based approach for the mitigation of the airline cargo cancellation problem”**, Journal of Information Security and Applications, Elsevier, vol. 51, article 102462, pp. 1-10, April 2020 (DOI:10.1016/j.jisa.2020.102462)
- 7) M. Diamantaris, F. Marcantoni, S. Ioannidis, J. Polakis, **“The Seven Deadly Sins of the HTML5 WebAPI: A Large-scale Study on the Risks of Mobile Sensor-based Attacks”**, ACM Transactions on Privacy and Security (TOPS), ACM, vol. 23, issue 4, article 19, pp. 1-19, July 2020 (DOI: 10.1145/3403947)
- 8) G. Hatzivasilis, N. Papadakis, I. Hatzakis, S. Ioannidis, G. Vardakis, **“AI-driven composition and security validation of an IoT ecosystem”**, Applied Sciences – Special Issue on Smart City and Multi-Agent Systems, MDPI Open Access Journal, vol. 10, issue 14, article 4862, pp. 1-31, August 2020 (DOI: 10.3390/app10144862)
- 9) G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, H. Koshutanski, **“Modern aspects of cyber-security training and continuous adaptation of programmes to trainees”**, Applied Sciences – Special Issue on Cyber Security of Critical Infrastructures, MDPI Open Access Journal, vol. 10, issue 16, article 5702, pp. 1-26, August 2020 (DOI: 10.3390/app10165702)
- 10) M. Hamad, Z. A. H. Hammadeh, S. Saidi, V. Prevelakis, **“Temporal-based intrusion detection for IoV”**, Information Technology, De Gruyter Oldenbourg, vol. 62, issue 5-6, pp. 227-239, December 2020 (DOI: 10.1515/itit-2020-0009)
- 11) G. Hatzivasilis, K. Fysarakis, S. Ioannidis, I. Hatzakis, G. Vardakis, N. Papadakis, G. Spanoudakis, **“SPD-Safe: Secure administration of railway intelligent transportation systems”**, Electronics – Special Issue on Advances in Public Transport Platform for the Development of Sustainability Cities, MDPI Open Access Journal, vol. 10, issue 1, article 92, pp. 1-26, January 2021 (DOI: 10.3390/electronics10010092)
- 12) Pape, S. and Kipker, D-K., **“Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy”**, Datenschutz und Datensicherheit, 45 (5): 310-314, April 2021 (DOI: 10.1007/s11623-021-1440-3)
- 13) M. Smyrlis, I. Somarakis, G. Spanoudakis, G. Hatzivasilis, S. Ioannidis, **“CYRA: A Model-Driven CYber Range Assurance Platform”**, Applied Sciences – Special Issue on Security management of 5G and IoT ecosystems, MDPI Open Access Journal, vol. 11, issue 11, article 5165, pp. 1-28, June 2021 (DOI: 10.3390/app11115165)
- 14) Hatzivasilis, G., Ioannidis, S., Fysarakis, K., Spanoudakis, G., Papadakis, N., **“The Green Blockchains of Circular Economy”**, Electronics – Special Issue on Artificial Intelligence Applications in Next Generation Communication Infrastructures Security, MDPI Open Access Journal, vol. 10, issue 16, pp. 1-16, August 2021 (DOI: 10.3390/electronics10162008)

2.2.2 Articles

- 1) J. Debussche, J. César, S. Mortier, “**Big Data & Issues & Opportunities: Cybersecurity**”, in TwoBirds, the 4th article of the “Big Data & Issues & Opportunities” series, January 2019, also published in Lexology and Digital Business
- 2) J. Debussche, J. César, I. De Moortel, S. Mortier, “**Big Data & Issues & Opportunities: Breach-related obligations**”, in TwoBirds, the 5th article of the “Big Data & Issues & Opportunities” series, February 2019, also published in Lexology and Digital Business
- 3) A. Chieti, G. Maglio, V. Petrarolo, C. Tanzarella, “**Cyber risks in healthcare organizations and the insight of using the THREAT-ARREST platform for training**” (in Italian), Agendadigitale.eu, July 2019
- 4) M. Tsantekidis, “**Cyber Security Threats and Threat Actors Training – Assurance Driven Multi-Layer, end-to-end Simulation and Training**”, Cyberwatching.eu, October 2019
- 5) G. Hatzivasilis, K. Fysarakis, S. Ioannidis, “**Cyber-Ranges as a Mean of Security Culture Establishment**”, ERCIM News – Special Theme: The Climate Action, ERCIM, issue 121, Article no. 36, pp. 36-37, April 2020
- 6) G. Leftheriotis, “**TÜV HELLAS (TÜV NORD) Leading in the Implementation of Cyber-Security Innovations**” (in Greek), TÜV NORD Blog, September 2020
- 7) S. Ioannidis and G. Hatzivasilis, “**Cyber-ranges and security training for the maritime sector**”, 4th NMIOTC Conference on Cyber Security in Maritime Domain, NATO, Souda Bay, Chania, Greece, 30 September – 1 October, 2020
- 8) G. Tsakirakis, “**Security in Human vs Cyber ecosystems**”, ITML Blog, November, 2020
- 9) G. Hatzivasilis, “**Training and Security in the Cyber-Space**” (in Greek), Researcher’s Night, Heraklion, November, 2020
- 10) M. Smyrlis, G. Spanoudakis, K. Fysarakis, “**Teaching Users New IoT Tricks: A Model-driven Cyber Range for IoT Security Training**”, IEEE Internet of Things (IoT) Magazine, March, 2021
- 11) F. Frati, “**THREAT-ARREST**”, UMIL Sesar Lab, July, 2021

2.2.3 Conference/Workshop papers

- 1) J. Najjar and V. Prevelakis, “**A Secure and Efficient File System Access Control Mechanism (FlexFS)**”, International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), RAID Heraklion, Crete, Greece, Springer, LNCS, vol. 11398, pp. 15-26, September 2018 (DOI: 10.1007/978-3-030-12085-6_2)
- 2) C. Mio, G. Gianini and E. Damiani, “**K-Means Clustering in Dual Space for Unsupervised Feature Partitioning in Multi-view Learning**”, 2018 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2018, pp. 1-8, DOI: 10.1109/SITIS.2018.00012
- 3) M. Hamad, M. R. Agha, V. Prevelakis, “**ProSEV: Proxy-Based Secure and Efficient Vehicular Communication**”, IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, pp. 1-8, January 2019 (DOI: 10.1109/VNC.2018.8628360)

- 4) M. Diamantaris; E. P. Papadopoulos, E. P. Markatos, S. Ioannidis, J. Polakis, “**REAPER: Real-time App Analysis for Augmenting the Android Permission System**”, 9th ACM Conference on Data and Application Security and Privacy (CODASPY), Richardson, TX, USA, pp. 3063-3071, March 2019 (DOI: 10.1145/3292006.3300027)
- 5) F. Marcantoni, M. Diamantaris, S. Ioannidis, J. Polakis, “**A Large-scale Study on the Risks of the HTML5 WebAPI for Mobile Sensor-based Attacks**”, The World Wide Web (WWW’18) Conference, San Francisco, CA, USA, pp. 3063-3071, May 2019 (DOI: 10.1145/3308558.3313539)
- 6) G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. I. Tsatsoulis, “**Review of Security and Privacy for the Internet of Medical Things (IoMT)**”, IEEE 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Greece, pp. 457-464, May 2019 (DOI: 10.1109/DCOSS.2019.00091)
- 7) G. Hatzivasilis, N. Christodoulakis, C. Tzagkarakis, S. Ioannidis, K. Fysarakis, G. Demetriou, M. Panayiotou, “**The CE-IoT Framework for Green ICT Organizations**”, IEEE 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Greece, pp. 436-442, May 2019 (DOI: 10.1109/DCOSS.2019.00088)
- 8) G. Hatzivasilis, P. Chatziadam, N. E. Petroulakis, M. Mangini, C. Kloukinas, A. Yautsiukhin, M. Antoniou, D. G. Katehakis, M. Panayiotou, “**Cyber Insurance of Information Systems**”, 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), Cyprus, pp. 1-7, September 2019 (DOI: 10.1109/camad.2019.8858165)
- 9) G. Hatzivasilis, P. Chatziadam, A. Miaoudakis, E. Lakka, A. Alessio, M. Smyrlis, G. Spanoudakis, A. Yautsiukhin, M. Antoniou, N. Stathiakis, “**Towards the Insurance of Healthcare Systems**”, 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, Springer, LNCS, vol. 11981, pp. 185-198, September 2019 (DOI: 10.1007/978-3-030-42051-2_13)
- 10) O. Soultatos, K. Fysarakis, G. Spanoudakis, H. Koshutanski, E. Damiani, K. Beckers, D. Wortmann, G. Bravos, M. Ioannidis, “**The TREAT-ARREST Cyber-Security Training Platform**”, 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, Springer, LNCS, vol. 11981, pp 199-214 September 2019 (DOI: 10.1007/978-3-030-42051-2_14)
- 11) L. Goeke, A. Quintanar, K. Beckers, S. Pape, “**PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks**”, 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, Springer, LNCS, vol. 11981, pp 156-171, September 2019 (DOI: 10.1007/978-3-030-42051-2_11)
- 12) I. Somarakis, M. Smyrlis, K. Fysarakis, G. Spanoudakis, “**Model-driven Cyber Range Training – The Cyber Security Assurance Perspective**”, 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, Springer, LNCS, vol. 11981, pp 172-184, September 2019 (DOI: 10.1007/978-3-030-42051-2_12)
- 13) C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, L. Mauri, “**A model driven approach for cyber security scenarios deployment**”, 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg,

- Springer, LNCS, vol. 11981, pp 107-122, September 2019 (DOI: 10.1007/978-3-030-42051-2_8)
- 14) V. Prevelakis, M., J. Najar, I. Spais, “**Secure Data Exchange for Computationally Constrained Devices**”, International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), ESORICS, Luxembourg, pp. 1-15, September 2019
 - 15) M. Tsantekidis and V. Prevelakis, “**Efficient Monitoring of Library Call Invocation**”, 6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, Granada, Spain, pp. 387-392, October 2019 (DOI: 10.1109/IOTSMS48152.2019.8939203)
 - 16) G. Hatzivasilis, O. Soultatos, E. Lakka, S. Ioannidis, D. Anicic, A. Broring, L. Ciechomski, M. Falchetto, K. Fysarakis, G. Spanoudakis, “**Secure Semantic Interoperability for IoT Applications with Linked Data**”, IEEE Global Communications Conference (GLOBECOM 2019), Waikoloa, HI, USA, pp. 1-7, December 2019 (DOI: 10.1109/globecom38437.2019.9013147)
 - 17) V. Hazilov, S. Pape, “**Systematic Scenario Creation for Serious Security-Awareness Games**”, 2nd Workshop on Security, Privacy, Organizations, and Systems Engineering (SPOSE), ESORICS, Guildford, UK, Springer, LNCS, vol. 12580, pp. 294-311, September 2020 (DOI: 10.1007/978-3-030-66504-3_18)
 - 18) M. Smyrlis, K. Fysarakis, G. Spanoudakis, G. Hatzivasilis, “**Cyber Range Training Programme Specification through Cyber Threat and Training Preparation Models**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 22-37, September 2020 (DOI: 10.1007/978-3-030-62433-0_2)
 - 19) S. Pape, L. Goeke, A. Quintanar, K. Beckers, “**Conceptualization of a CyberSecurity Awareness Quiz**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 61-76, September 2020 (DOI: 10.1007/978-3-030-62433-0_4)
 - 20) C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, S. Astaneh, “**Towards the Monitoring and Evaluation of Trainees’ Activities in Cyber Ranges**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 79-91, September 2020 (DOI: 10.1007/978-3-030-62433-0_5)
 - 21) G. Hatzivasilis and M. Kunc, “**Chasing Botnets: A Real Security Incident Investigation**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 111-124, September 2020 (DOI: 10.1007/978-3-030-62433-0_7)
 - 22) M. Tsantekidis and V. Prevelakis, “**Software System Exploration using Library Call Analysis**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 125-139, September 2020 (DOI: 10.1007/978-3-030-62433-0_8)
 - 23) G. Hatzivasilis, “**Password Management – How Secure Is Your Login Process?**”, 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, Springer, LNCS, vol. 12512, pp. 157-177, September 2020 (DOI: 10.1007/978-3-030-62433-0_10)

- 24) J. T. Hounsou, P. B. C. Niyomukiza, T. Nsabimana, G. Vlavourou, F. Frati, E. Damiani, **“Learning Vector Quantization and Radial Basis Function Performance Comparison Based Intrusion Detection System”**, International Conference on Intelligent Human Systems Integration (IHSI), Palermo, Italy, Springer, AISC, vol. 1322, pp. 561-572, February 2021 (DOI: 10.1007/978-3-030-68017-6_83)
- 25) M. Tsantekidis, V. Prevelakis, **“MMU-based Access Control for Libraries”**, 18th International Conference on Security and Cryptography (SECRYPT 2021), Lisbon, Portugal, Springer, pp. 1-1, July 2021
- 26) G. Hatzivasilis, et al., **“The THREAT-ARREST cyber ranges platform”**, IEEE CSR Workshop on Cyber Ranges and Security Training (CRST), IEEE, Virtual, Greece, pp. 1-6, July 2021
- 27) Pape, S.; Klauer, A. and Rebler, M.: Leech, **“Let's Expose Evidently bad data Collecting Habits - Towards a Serious Game on Understanding Privacy Policies (Poster)”**, 17th Symposium on Usable Privacy and Security (SOUPS), August 2021

2.2.4 Special Issues in Scientific Journals

Furthermore, THREAT-ARREST has issued two Special Issues in open access journals.

- 1) MDPI Journal “Future Internet”, **Special Issue “Future and Emerging topics in Security for Cyber-Physical Systems”**
- 2) MDPI Journal “Applied Sciences”, **Special Issue “Security management of 5G and IoT ecosystems”**

One additional special issue has already been organised and will be available after the end of the project.

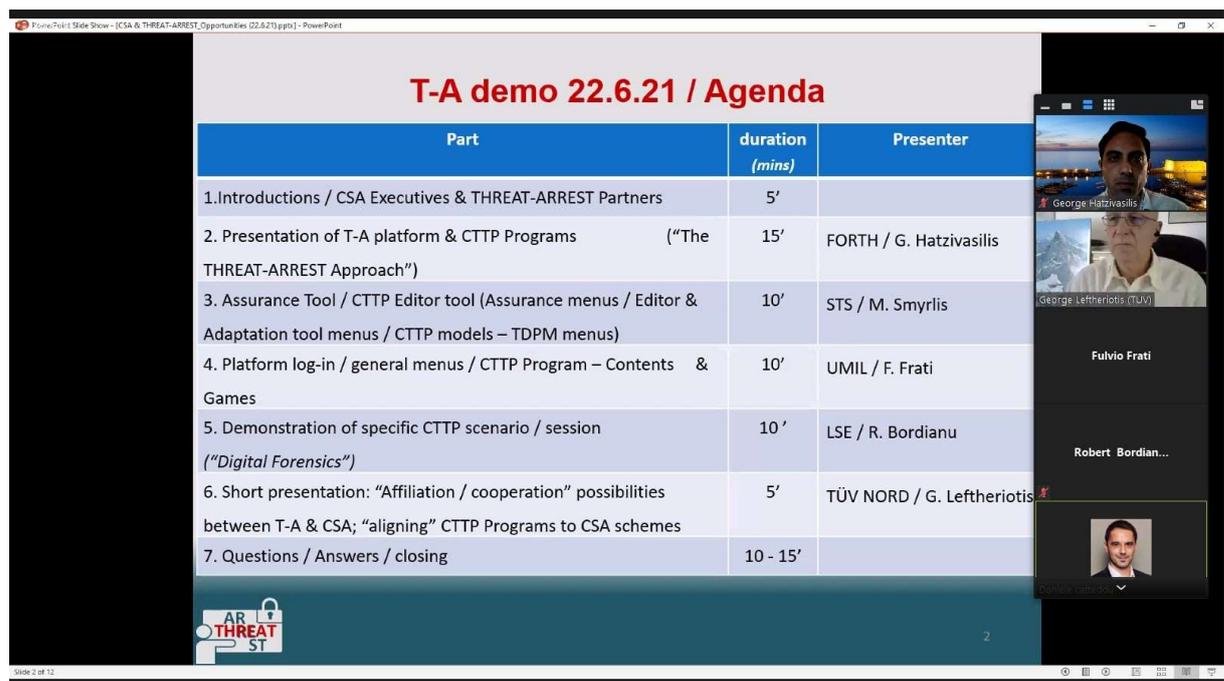
- 3) MDPI Journal “Electronics”, **Special Issue “Artificial Intelligence Applications in Next Generation Communication Infrastructures Security”**

2.3 Talks, seminars, and presentations

As part of the broader dissemination effort for THREAT-ARREST, we presented various aspects of the project at several venues attracting the interest not only of the security training community, but the wider research community as well. Since M18, that was covered in the first version of this deliverable – D8.5, the following actions were taken:

- 1) The THREAT-ARREST project and platform were presented in a joint meeting with CONCORDIA H2020 project
- 2) The THREAT-ARREST project and platform were presented in a joint meeting with SPIDER H2020 project
- 3) The THREAT-ARREST project and platform were presented in the CONCORDIA Open Door 2020 event.
- 4) The THREAT-ARREST project was presented in Researcher's Night 2020 held at FORTH.
- 5) The THREAT-ARREST project was presented in 3rd CypBER Event 2020 held virtually.
- 6) A meeting with the CTO (Chief Technology Officer) of CSA, Daniele Catteddu, at TUV HELLAS Offices in Athens was held in March 2021. THREAT-ARREST was presented and discussions took place about possible routes for a collaboration/affiliation between CSA and the project.

- 7) A second meeting with CSA was organised by TUV HELLAS virtually in June 2021. THREAT-ARREST platform and CTPP Programmes were demonstrated to CSA Executives (Mr. Danielle Catteddu, CTO and Mr. Ryan Bergsma, Training Program Director). The demo also part of THREAT-ARREST’s “Affiliation efforts” – within Task’s T8.4 (“Contribution to Standards”) requirements to further discuss collaboration between the two ventures (Figure 1). The event was promoted through the project’s social media platforms.
- 8) Marinos Tsantekidis from FORTH presented his work in HiPEAC CSW Webinars Spring 2021 “Secure Runtime Environments” session (Figure 2), acknowledging THREAT-ARREST.
- 9) George Hatzivasilis from FORTH presented the THREAT-ARREST cyber ranges platform in HiPEAC CSW Webinars Spring 2021 “Secure Runtime Environments” session (Figure 3), acknowledging THREAT-ARREST.
- 10) George Hatzivasilis from FORTH presented the THREAT-ARREST cyber ranges platform in CRST workshop at IEEE CSR 2021(Figure 4).
- 11) Sebastian Pape from SEA gave a keynote talk on “Serious Games for Security and Privacy Awareness” at the IFIP Summer school on Privacy & Identity Management 2021, acknowledging THREAT-ARREST.



T-A demo 22.6.21 / Agenda

Part	duration (mins)	Presenter
1. Introductions / CSA Executives & THREAT-ARREST Partners	5'	
2. Presentation of T-A platform & CTPP Programs (“The THREAT-ARREST Approach”)	15'	FORTH / G. Hatzivasilis
3. Assurance Tool / CTPP Editor tool (Assurance menus / Editor & Adaptation tool menus / CTPP models – TDPM menus)	10'	STS / M. Smyrlis
4. Platform log-in / general menus / CTPP Program – Contents & Games	10'	UMIL / F. Frati
5. Demonstration of specific CTPP scenario / session (“Digital Forensics”)	10'	LSE / R. Bordianu
6. Short presentation: “Affiliation / cooperation” possibilities between T-A & CSA; “aligning” CTPP Programs to CSA schemes	5'	TÜV NORD / G. Leftheriotis
7. Questions / Answers / closing	10 - 15'	

Slide 2 of 12

Figure 1: Virtual meeting with CSA in search of possible collaboration

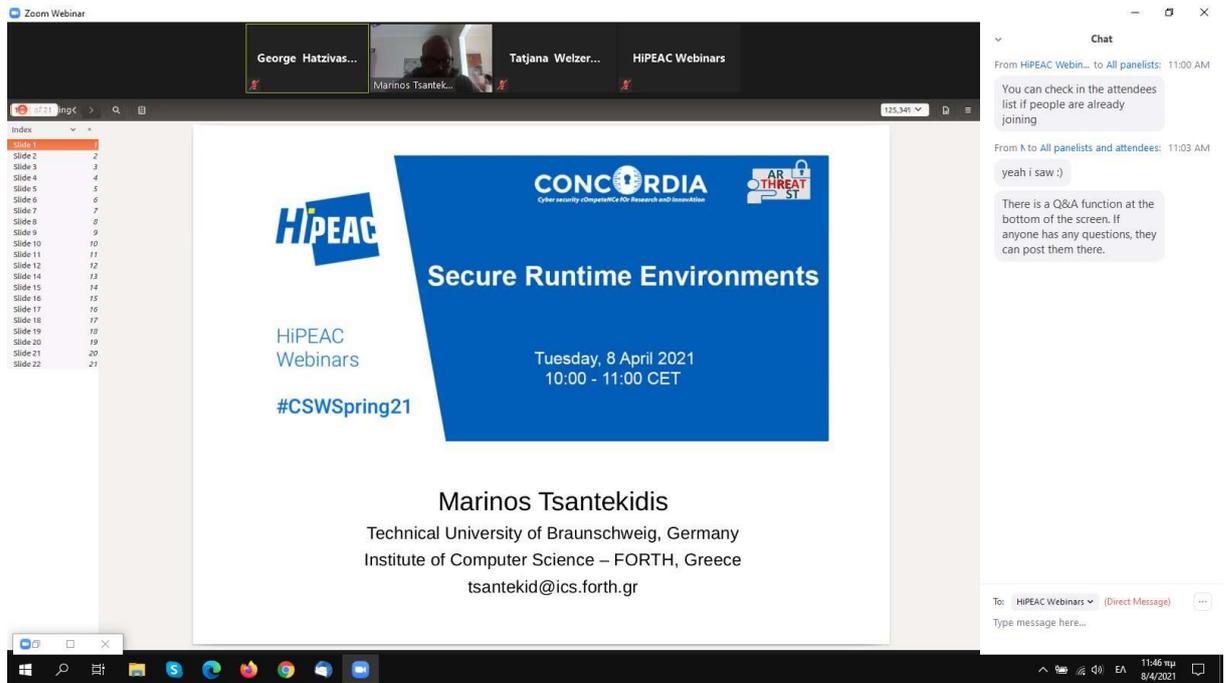


Figure 2: Marinos Tsantekidis presenting at “Secure Runtime Environments” webinar

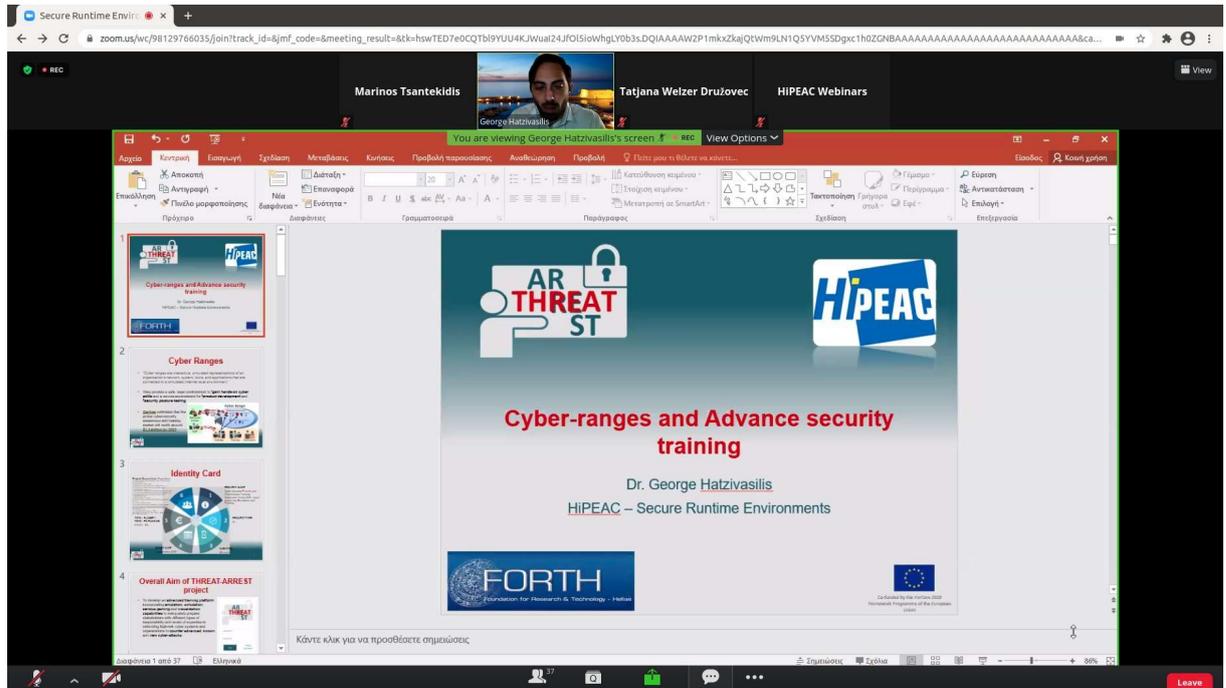


Figure 3: George Hatzivasilis presenting at “Secure Runtime Environments” webinar



Figure 4: George Hatzivasilis presenting at CRST workshop 2021

2.4 Academic Dissemination

There have been three recent graduates that were granted Bachelor/Master degrees at the University of Milan, in the Cybersecurity programme:

- Paolo di Prima, “**Sistema plugin-based per la collezione di eventi nell'utilizzo di cyber range**”, *Master thesis* at University of Milan. Advisor: Elvinia Maria Riccobene, co-advisor: Fulvio Frati.
- Michele Toccagni, “**Approccio model driven per generare cyber ranges**”, *Master thesis* at University of Milan. Advisor: Chiara Braghin.
- Alessandro della Torre, “**Sistema di monitoraggio e valutazione per cyber ranges**”, *Bachelor thesis* at University of Milan. Advisor: Chiara Braghin.

2.5 Other Dissemination Activities

During the second half of the project, the following additional dissemination activities were carried out:

- 1) The THREAT-ARREST project was included in the fourth (Spring)⁶ and fifth (Autumn)⁷ editions of the Cyberwatching.eu project radar.
- 2) THREAT-ARREST co-organised the “Secure Runtime Environments” webinar at HiPEAC CSW Spring 2021 (Figure 5).
- 3) The complete webinar session has been made public and is available on YouTube⁸.
- 4) The project’s newsletters were posted on several online platforms (see Appendix 1). They are also available in electronic form, on the website, as a downloadable file in PDF format.

⁶ <https://radar.cyberwatching.eu/radar/spring-2020>

⁷ <https://radar.cyberwatching.eu/radar/autumn-2020>

⁸ <https://www.youtube.com/watch?v=xyhbW0kKGpE>

- 5) THREAT-ARREST's project page⁹ on Cyberwatching.eu was actively maintained and updated regularly.
- 6) THREAT-ARREST sponsored and supported the 2021 IEEE CSR Workshop on Cyber Ranges and Security Training (CRST) (Figure 6).
- 7) UMIL disseminated their involvement in the THREAT-ARREST project and its progress on their blog¹⁰.
- 8) TUV HELLAS included a news article¹¹ in their July 2021 newsletter (in Greek), with regards to the meeting with CSA.



Figure 5: Call-for-participation banner for “Secure Runtime Environments” webinar

9 <https://www.cyberwatching.eu/projects/996/threat-arrest>

10 <http://sesar.di.unimi.it/threat-arrest/>

11 <https://www.tuv-nord.com/gr/el/nea-enimerosi/nea-eidiseis/news-details/article/threat-arrest-demonstration-for-csa/>



Figure 6: Call-for-Participation banner for CRST 2021 workshop

2.6 Updates regarding the communication and engagement of stakeholders' activities

As promised in D8.7, which is the final output of task “T8.1 – Communication and Engagement of Stakeholders”, in this section we briefly report the communication and engagement of stakeholders' activities performed in the last six months of the project.

Unfortunately, the Covid-19 pandemic restrictions on travel, gatherings, and meetings limited the type and the number of activities we were able to engage in also in the last six months of the project. Nevertheless, physical meetings have been converted into virtual meetings and the Consortium, whenever possible, participated, organized and promoted meetings and events to engage possible stakeholders of the project and continued to build a network of connections with key players from industry and academics and potential business partners, to be used in order to communicate the project's results and to disseminate the technological and business-related knowledge acquired during the project. In particular, we focussed on strengthening the networking built with other European projects and security-concerned industries to foster future dissemination and exploitation activities. Since online channels became even more important in this period, we also produced a professional promotional video.

The most relevant activities are summarized below:

- The Consortium carried on the promotion of THREAT-ARREST platform's functionalities with *Emirates Nuclear Energy Corporation* (ENEC) in order to extend the platform to build an NPP-Cyber Range Framework for specific high-risk organizations, Nuclear Power Plants, to provide cyber-tests, training, and hardening its architecture. NPP-Cyber Range will provide a mechanism to automatically prepare and manage the OT cyber ranges based on Security Experts' specifications in the Nuclear Power plants.
- According to the Communication strategy, also in the last six months 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 YouTube account has been used to upload videos showing the first prototypes of the platform and the promotional video.

- The Consortium continued 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: we were able to present THREAT-ARREST platform and have feedback from people working in the same field, we have been introduced to other tool owners or to use-cases different from smart energy, healthcare, and shipping, being involved into the building of a cyber ranges federation. We also organized meetings with CSA and discussed with them possible dissemination and exploitation activities.

2.7 Evaluation of efforts against the initially set goals

In this chapter, we compare the THREAT-ARREST dissemination activities for the whole project against the key performance indicators (KPIs) defined in the project proposal (below in parentheses). In this way, we can verify whether the project dissemination objectives have been met.

Push announcements (Success Indicator: ≥ 50 announcements): Regular announcements and posts have been pushed through social media (Facebook, LinkedIn, Twitter) (see the deliverable “D8.7 – The stakeholders’ engagement & online channels report v.2” for more detailed information). On each of the platforms, continuous posts have been made, totalling to more than 1000 since the start of the project.

Regular Newsletter (Success Indicator: ≥ 9 newsletters): Ninth newsletters have already circulated through social media and are available for download from the website (see Appendix for the last five, since the previous deliverable D8.5).

Brochure (Success Indicators: ≥ 2.000 hard copies distribution in ≥ 10 events): 2000 hard copies have been printed and distributed at all the events where one or more of the consortium partners attended (see Appendix).

Technical video (Success Indicators: ≥ 1000 views, ≥ 10 event presentations): Eight technical videos were created^{12 13 14 15 16 17 18 19} totalling to around 780 views so far. Moreover, one more video²⁰ was created by a professional company that presents the whole project and its results. The videos have been presented on more than 10 events where one or more of the consortium partners have attended.

Journal publications (Success Indicator: ≥ 10 publications): Fourteen journal papers have been published (see Section 2.2)

12 <https://www.youtube.com/watch?v=Nr6wejCKKsI>

13 <https://www.youtube.com/watch?v=7sObSkQSVqc>

14 https://www.youtube.com/watch?v=0vGNXkne_wM

15 <https://www.youtube.com/watch?v=TR2jeRVLSIY>

16 <https://www.youtube.com/watch?v=iFmFTBVWeio>

17 <https://www.youtube.com/watch?v=vs8T1oZoha0>

18 <https://www.youtube.com/watch?v=K0UiFgfWoHk>

19 <https://www.youtube.com/watch?v=DGOg1sEENCY>

20 https://www.youtube.com/watch?v=1RItDlps_Ds

Magazine publications (Success Indicator: ≥ 10 publications): Eleven publications have been released (see Section 2.2)

Conference publications (Success Indicator: ≥ 12 publications): 27 conference papers have been published (see Section 2.2)

Special issues (Success Indicators: ≥ 2 issues, ≥ 10 selected papers/issue): Two special issues have been released. One more is scheduled for release after the end of the project (see Section 2.2).

Conference organization (Success Indicators: ≥ 1 event, ≥ 100 attendees/event): We co-organised IEEE CAMAD 2019²¹ in Cyprus (focusing on Computer Aided Modelling and on communication and experimentation aspects of 5G networking), as well as the 3rd CypBER Event in 2020.

Workshops organization (Success Indicators: ≥ 2 events, ≥ 30 attendees/event): The MSTEC²² workshop was organized in conjunction with ESORICS 2019, where 30 persons attended. Additionally, we organised EuroSec 2019²³ (co-located with EuroSys). Moreover, DANAOS hosted the “2nd Workshop of EU Research & Innovation Maritime Projects” in November 2019. Also, we co-organize a Special Session in the IEEE CAMAD 2019, where more than 30 persons attended. Furthermore, the second workshop of the series, MSTEC 2020²⁴ (also co-located with ESORICS) was organised, attracting numerous attendees. Finally, we organized the CRST workshop at IEEE CSR 2021.

Summer schools (Success Indicators: ≥ 2 events, ≥ 30 attendees/event): The first ENISA summer school “NIS Summer School 2019”²⁵ was co-organised by FORTH in M13 (ahead of schedule, , where more than 100 persons attended. However, due to the ongoing COVID19 pandemic, we had to modify our initial plans for the rest of the summer schools of the series. NIS Summer School 2020 as well as 2021 had to be cancelled in light of the global health situation. We are, nonetheless, organising a second summer school “Cybersecurity Hands-On-Training – CyberHOT” under the auspices of NMIOTC²⁶, right after the end of the project, in September 2021.

Exhibition demonstrations (Success Indicator: ≥ 1 demo): The CONCORDIA Open Door (COD) 2020 event was held virtually in October, attracting stakeholders of all backgrounds to discuss societal and technological needs in the cybersecurity field and to discover others’ competences for potential collaborations. THREAT-ARREST held an Exhibitor booth at the event among other relevant projects.²⁷ (Figure 7).

EU demonstrations (Success Indicator: ≥ 2 demos): The Serious Games training session at the ENISA summer school was held in September 2019. Additionally, there was a demonstration of the project at the 3rd CypBER Event 2020, where attendees showed particular interest in the model-based approach of THREAT ARREST.

Conference demonstrations (Success Indicator: ≥ 2 demos): The Emulation Tool and the overall THREAT-ARREST approach was demonstrated during the interactive sessions at the

21 <https://camad2019.ieee-camad.org>

22 <https://www.threat-arrest.eu/html/mstec-2019/>

23 <https://www.threat-arrest.eu/html/eurosec-2019/>

24 <https://www.threat-arrest.eu/html/mstec/>

25 <https://nis-summer-school.enisa.europa.eu/2019/index.html>

26 <https://nmiotc.nato.int/transformation/conferences/cyber-security-conference/>

27 <https://www.facebook.com/266454357324031/posts/register-and-come-visit-our-virtual-exhibitor-booth-in-the-concordia-open-door-e/645222259447237/>

IEEE GLOBECOM 2019, as well as at ESORICS 2019, IEEE CSR 2021, and HiPEAC CSW Webinars 2021. The project’s video was also demonstrated during the NIS 2019 summer school to all participants. Furthermore, in October 2020 the project’s Smart Shipping scenario was demonstrated at the 4th NMIOTC Conference on Cyber Security in Maritime Domain.

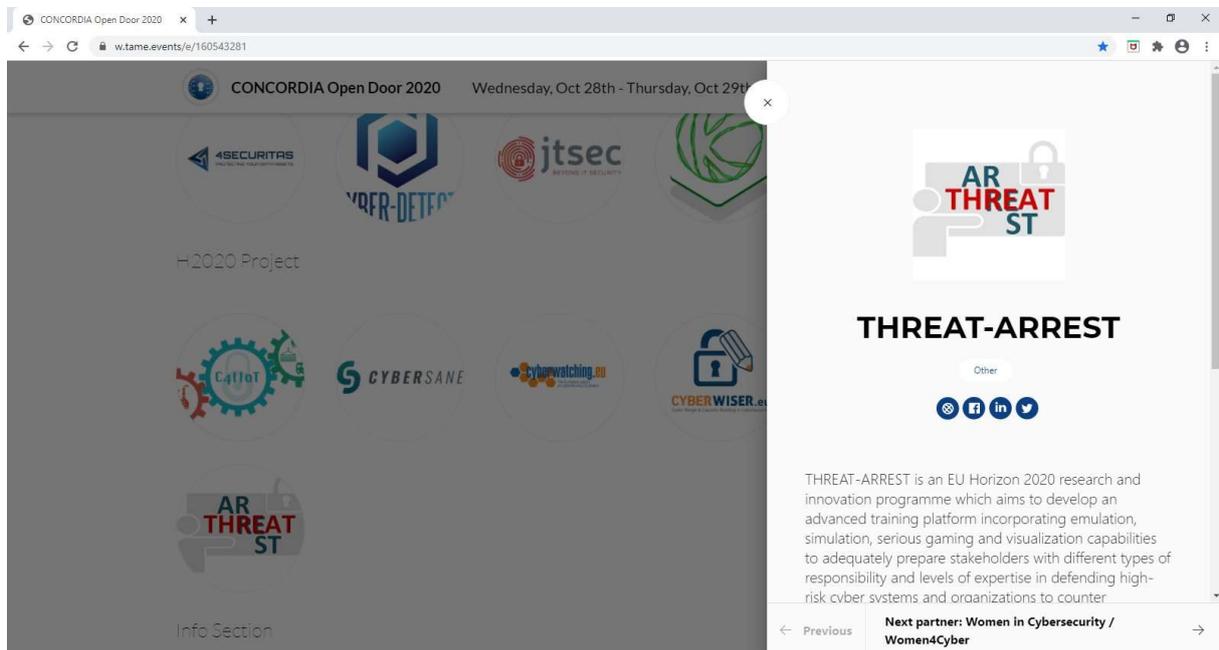


Figure 7: Exhibitor booth at COD2020 event

3 Exploitation

3.1 Overall Aim

The main goal of the exploitation plan is the continuation of the THREAT-ARREST project beyond the end of the project funding. For that, different elements will be described: exploitable items, individual exploitation strategies, and joint exploitation plans.

3.2 Final Exploitation Background

The THREAT-ARREST platform will consist of several individual tools from the industrial partners. This section includes the exploitation plans of these tools.

3.2.1 Analysis of exploitable items

3.2.1.1 Sphinx's Assurance Tool

STS aims to exploit THREAT-ARREST's Assurance Tool, a tool that incorporates (a) the Cyber Threat and Training Preparation (CTTP) Models and Programmes editor, (b) STS' Assurance Platform, and (c) the CTTP Models and Programmes adaptation tool, as a basis for allowing its Cyber Range platform to be used as a tool that generates Training and Awareness Programmes for users of all levels of expertise (e.g., end-users, system administrators, etc.), focusing on cyber systems of private and public organizations in the healthcare and telecoms sectors, which are the focus markets of the company.

The above-mentioned, will not only allow the generation of said scenarios and programmes, but also the incorporation of these within the Cyber Range platform in a twofold manner: i) as input for assessing the probability that human-caused security & privacy incidents (stemming from the lack of user training and awareness) will occur, and ii) as a means of mitigating the risks associated with said incidents. The latter will be achieved, (a) by observing the real-time operational evidence as provided by STS' Assurance Platform and creating CTTP Models and Programmes based on the specific organizations' needs and (b) by adapting existing Training Programmes and models or creating new ones in response to upcoming cyber threats and/or changes of the assessed cyber systems through the use of the CTTP Model and Programmes adaptation tool.

3.2.1.2 Social Engineering Academy Gamification GmbH

In the following, the exploitation plans for the different serious games of SEA are described.

HATCH

SEA created a new game scenario for HATCH in the field of smart shipping. Additionally, SEA was able to improve the design of the cards of the tabletop game HATCH in the context of the THREAT-ARREST project. In relation to the persona cards of the basic office scenario of HATCH, SEA has created gender-inclusive versions of these cards, representing a female and male persona on each card. The new scenario allows SEA to serve an additional industrial sector. With the improved design and gender-inclusive office persona cards, SEA expects a greater acceptance in the business area and thus an increase in training with HATCH.

PROTECT

SEA refactored their serious online game PROTECT resulting among others in an improved graphical user interface and usability. Furthermore, the configurability of the learning content and the game itself was enhanced. Besides the creation of at least one specific PROTECT game for each THREAT-ARREST pilot (smart energy, healthcare, and smart shipping), the enhanced configuration allows SEA to faster adapt the game to new industry sectors and company-

specific requirements. Altogether, this allows SEA to offer training with PROTECT to new industry sectors, and therefore increase the set of potential customers.

AWARENESS QUIZ

Through the development of the new online game AWARENESS QUIZ, SEA expands its online training offering with another game in the form of a quiz. Similar to PROTECT, the learning content of the AWARENESS QUIZ is adaptable and the game itself configurable. With the AWARENESS QUIZ, SEA plans to maintain a constantly growing database of quiz questions that are based on current real-world cybersecurity attack scenarios. Based on this set of questions, quizzes can be created to sensitize employees to cybersecurity threats in general and to keep their knowledge of present cybersecurity threats up to date. This allows SEA a lightweight adoption of game content to new threats or new customers.

SOCIAL ENGINEERING MEMORY

Based on attack scenarios which have been created for the PROTECT game, SEA has created an additional game within the THREAT-ARREST project in the form of a physical memory/concentration card game named “Social Engineering Memory”. In this game, a single player or a group of players must identify from the set of covered cards individual card pairs which represent social engineering attacks and the corresponding correct defense behaviors (see Figure 8). Copies of the Social Engineering Memory can be purchased by companies as an extremely affordable initial training measure for their employees.

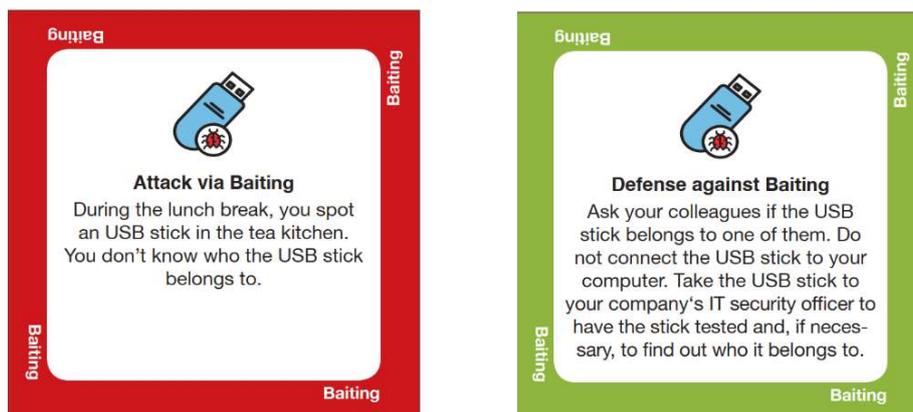


Figure 8: Social Engineering Memory card pair by the example of a baiting attack

3.2.1.3 Information Technology for Market Leadership Training Tool

ITML will exploit the outcomes of THREAT-ARREST, to enhance its market position with respect to intelligent management of advanced security threats, as well as on providing training services in multiple domains. Having already an Event – Management Software that provides Cybersecurity related services to a wide range of sectors, ITML’s vision through THREAT-ARREST is to exploit the advanced visualization, gamification, and training tools on the basis of the project’s findings, which will be used to further enhance the services already provided by its product.

Last, ITML will exploit the project’s findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in THREAT-ARREST. In more detail, ITML aims to form strategic cooperation with stakeholders from the maritime field, the healthcare domain, and the smart buildings domain, so that it can provide tailor-made services related to cybersecurity-based training.

3.2.1.4 IBM's data fabrication tool

IBM aims to exploit the extended and enhanced version of its Data Fabrication Platform (DFP) technology. The new technology version will be capable to fabricate synthetic realistic cybersecurity events for the THREAT-ARREST training and simulation framework. The extended tool is used to fabricating off-line synthetic data to support all the project use cases and fabrication of the security events logs of the simulated scenarios. The extended version of the DFP tool automatically extracts the simulated network topology and scenario properties from the project CTTP model. DFP then simulates the scenario, calling in application functions, declared by the scenario actions, propagating events from one network node to another, and stores the resulting event messages down to some persistent storage, producing event log files.

3.2.1.5 SIMPLAN AG

Exploitable items for SIMPLAN consist of the extended and enhanced version of SIMPLAN's discrete event simulation library "Jasima". The work conducted in THREAT-ARREST resulted in a library of simulation components to support the training scenarios of the pilots. This library is a foundation for developing training simulations in the field of cybersecurity. Developing these new components required a set of new features for the core simulation library (like enabling the process-oriented modelling style, integration into a message-broker-based platform architecture). These new features are also of interest for SIMPLAN's future activities not only in the cybersecurity domain.

As a second exploitable item, the Jasima Visualization Tool (JVT) was developed as part of THREAT-ARREST. It runs in a web browser and allows the flexible creation of visualization scenarios based on state-of-the-art web technologies. It will be used as the basis for visualizations of Jasima simulations in the future. As demonstrated in the THREAT-ARREST platform (integration with the eMon-Component of the Emulation Tool) the JVT also allows integrating data from other data sources. Therefore, it can serve as a flexible basis for creating dashboard-like, web-based visualizations for future SIMPLAN projects, whether they are related to cyber-security or other application domains.

3.3 Final Individual Exploitation Strategies

This section describes the individual exploitation strategies of the THREAT-ARREST industrial partners.

3.3.1 Sphynx Technology Solutions AG

As a final exploitation strategy, STS will use the outcomes of THREAT-ARREST for strengthening its service and product portfolio. STS' plan is to augment the capabilities of its Cyber Range platform in ways that will enable it to support the delivery of model-driven Cyber Range Programmes. The model-driven approach will also make use of STS' Security Assurance Platform to provide organization-tailored Cyber Range Programmes (based on the findings of the platform).

From a technical perspective, STS' strategy for achieving this exploitation route will be to develop a tool supporting (a) the creation of model-driven CTTP Models and Programmes, (ii) the continuous security assurance of the actual operating system, and (iii) the dynamic adaptation of the training procedures in the virtual cyber range's environment. As of today, STS designed and implemented the Assurance Tool, a tool that incorporates: (a) STS' Security Assurance Platform, (b) the CTTP Models and Programmes editor, and (c) the CTTP Models and Programmes adaptation tool. These components work together to provide Cyber Range Training Programmes that (a) can train users to understand the ever-increasing threat landscape, (b) are tailored to an organization's needs (based on the use of the Security Assurance Platform), and (c) can be adopted to upcoming cyber threats and/or changes of the assessed cyber systems.

3.3.2 ATOS Spain S.A

ATOS's exploitation activities in THREAT-ARREST will be performed by the Innovation Hub (IH) unit in ATOS Research & Innovation (ARI), the R&D hub for emerging technologies and a key reference for the whole Atos group. The IH, created in 2018 within ARI, is fostering the incubation of assets coming from R&D projects to build commercial solutions based on innovation results. Through the creation of "shuttles", we mature these assets and create for them all marketing and business material needed to put them into the market.

The general strategy of exploitation is to evaluate the THREAT-ARREST results for added value to the ATOS portfolio of security solutions, particularly offering advanced training capabilities for professionals of relevant sectors, such as critical infrastructures, to gather specialized skills on cybersecurity. The expected result of exploitation is to enrich ATOS's training offerings through cyber range platforms such as THREAT-ARREST.

ATOS foresees different lines of exploitation for THREAT-ARREST:

- Horizontal exploitation: Positioning THREAT-ARREST outcomes within ATOS technology services offering. This has a two-fold approach: i) the improvement of existing products in the Global Key Offering (GKO) portfolio by incorporating partial results from THREAT-ARREST to existing solutions, or ii) by offering THREAT-ARREST as a stand-alone product based on the final platform version.

It is worth mentioning the following two:

- Big Data & Cybersecurity (BDS) is in charge of solutions addressed to the protection of Critical Infrastructures and Homeland Security.
- ATOS High-Performance Security (AHPS) service that is managed by the Security Information and Event Management (SIEM) service provided of ATOS, is targeting customers with more than 3000 monitored devices (event sources), and billions of collected events per month.

Atos results may be presented to relevant managers to analyse how to provide added value to the divisions' portfolio.

- Vertical exploitation: Positioning specific THREAT-ARREST advances in the field of cybersecurity training and preparedness to the following lines: i) the GKO on cybersecurity, ii) the Cyber Threat Management Services within the Managed Services portfolio, and iii) the Governance, Risk and Compliance (GRC) offering.

3.3.3 IBM Israel – Science and Technology LTD

IBM's role in this project is to fabricate synthetic realistic security attacks. IBM research lab in Haifa is working closely with the IBM Security business unit brands and incorporates innovations into their products, for example, the security products of Guardium, Trusteer, and Xforce. IBM has been named by Gartner as a leader in several security fields. Participation in the THREAT-ARREST project, including close collaboration with the use case partners will help guide the next generation of IBM security products. We will ensure that relevant IBM business units which are involved with developing the company's relevant products and services are aware of the technologies developed in the THREAT-ARREST project and will consider them for inclusion in products, as well as in factoring the project innovation into the overall IBM product strategy.

3.3.4 Social Engineering Academy GmbH

Through the further development of their serious games HATCH and PROTECT, SEA plans to increase its orders for training measures in enterprises with these games. SEA sees this

potential particularly for PROTECT, whose learning content can now be adapted more easily to the specific requirements of companies. Based on the new PROTECT card decks which have been developed during the THREAT-ARREST project for the different project pilots (smart energy, smart shipping, healthcare), SEA plans to exploit new industry sectors.

With the completely newly developed online quiz game AWARENESS QUIZ, SEA plans to expand its online training portfolio and address further training scenarios. Because the AWARENESS QUIZ allows fast creation of new questions and the compilation of quizzes by thematic aspects, training on real-world attacks can be provided in a fast manner. This allows to enhance SEA's training offers and allows to provide continuous service with repetitive training targeting real cybersecurity attacks.

Copies of the Social Engineering Memory can be purchased by companies as an extremely affordable initial training measure for their employees. The game is intended to make companies aware of the fact that serious games enable the mediation of cybersecurity aspects in an interesting and sustainable way. On the other hand, SEA is expecting that the game generates more contacts to companies which increases the chance of generating follow-up orders for their premium training offers, like PROTECT, AWARENESS QUIZ, and HATCH.

3.3.5 Information Technology for Market Leadership

ITML will exploit the outcomes of THREAT-ARREST, to enhance its market position with respect to intelligent management of advanced security threats, as well as on providing training services in multiple domains. Having already an Event – Management Software that provides Cybersecurity related services to a wide range of sectors, ITML's vision through THREAT-ARREST is to exploit the advanced visualization, gamification, and training tools on the basis of the project's findings, which will be used to further enhance the services already provided by its product.

Last, ITML will exploit the project's findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in THREAT-ARREST. In more detail, ITML aims to form strategic cooperation with stakeholders from the maritime field, the healthcare domain, and the smart buildings domain, so that it can provide tailor-made services related to cybersecurity-based training.

3.3.6 Bird & Bird LLP

Bird & Bird will, as a legal partner, in principle does not exploit the THREAT-ARREST training platform for its account.

However, Bird & Bird may have the opportunity to present the Project as well as its outcomes to third parties, such for example, during know-how sessions aiming at introducing new IT tools and solutions to clients, to academics, and/or policy makers' audience.

The exploitation of the THREAT-ARREST Platform for Bird & Bird may in such a case take the form of showcasing the THREAT-ARREST Project while affirming the B&B position as an expert IT-law firm.

3.3.7 DANAOS Shipping Company LTD

DANAOS as a leading operator in container sea transportation, chartering out ships to major shipping liners will exploit the innovative solution of the THREAT-ARREST platform to: (i) train and familiarize the company's crew and offshore personnel to potential cyber-threats in shipping operation thus boosting up situational awareness on cyber risks; (ii) strengthen DANAOS security plan against these threats and assist company for the adoption of the ideal

and most effective framework for efficient protection, while at the same time (iii) enhance DANAOS leading position and reputation in maritime trade by ensuring that charterers interests, vessel integrity against cyber vulnerabilities and data protection remains a priority. In this context, DANAOS will exploit the THREAT-ARREST environment so to incorporate cybersecurity training framework and relevant CTTP Programmes to the overall company's training plan and strategy, capitalizing mostly on the company's existing technology infrastructure and training curriculums. In particular, DANAOS aims to explore the possibility to integrate the THREAT-ARREST platform with bridge and incident command simulators, part of the company's training equipment, thus structuring and offering multi-scale combined training scenarios performed in a similar to the ship environment.

3.3.8 TUV HELLAS TUV NORD

TÜV HELLAS / TÜV NORD's exploitation strategy will be implemented under the coordination of the Group's Innovation Corporate Center. Exploitation strategy focuses on utilizing the Project's outcomes to explore synergies and opportunities to be able to participate in offering innovative, "certifiable", cyber range-based Cybersecurity Training services. Such specialized Training & Certification services are anticipated to be in high demand in the immediate & near future, as they will satisfy the needs both of specialized, hands-on technical training as well as of covering/satisfying the changing European Legislation landscape requirements (e.g., NIS Directive, GDPR Regulation, etc.).

The Group's exploitation potential is significant, as it is a Global Services Group, with core activities in Industrial Services, Mobility, Training, Natural Resources, Aerospace, and IT, covering more than 70 Countries, with more than 14,000 Employees and thousands of Clients. Furthermore. Training services are a very significant part of the Group's overall services portfolio and cyber range-based training sessions/Programmes can fit within the training services portfolio (both horizontal & vertical exploitation).

Regarding the "Standardization" Tasks of the Project (T.3.4), TÜV has already been involved in aligning / mapping CTTP Programmes to International Cybersecurity Training & Certification Bodies' schemes (ISC2, ISACA, CSA, etc) and in related affiliation activities. The Group aims to further exploit the overall opportunity here and gain upon such collaborations.

Regarding the "Certification of CTTP Programmes" Tasks (T.8.4) of the Project, the experience gained via searching for, consolidating, comparing, and mapping CTTP Programmes to many Cybersecurity-related technical Standards & Frameworks (ISO, NIST, CIS, CSA as well as MITRE ATT@CK) as well as to Cybersecurity Skills & Competencies Frameworks (NIST NICE, e-CF) will also be a potential part of the overall exploitation, as such mappings/alignments can be a valuable "addition" to any focused cybersecurity training Programme.

3.3.9 LIGHTSOURCE LAB LTD

Lightsource Labs (LSE) develops and commercialises technology which unlocks flexibility and value in energy assets at the grid edge. LSE's solutions combine the power of advanced Internet of Energy technologies with cutting-edge artificial intelligence and big data analytics, in order to help customers, optimise asset utilisation, balance energy demand and unlock financial opportunities. From residential solar, storage and EV charging management, to commercial & industrial building optimisation, our technology helps accelerate the transition to net zero.

LSE will look to exploit the THREAT-ARREST project as a training platform on which its employees, partners and stakeholders can be educated on cyber security concerns regarding LSE infrastructure as well as within the energy specific sector. LSE hope to utilise the

THREAT-ARREST platform as the main training platform for all employees who require cyber security risk awareness and incident handling training. The training scenarios will help improve cyber security risk awareness for device installers and homeowners as well as prepare them on how to deal with potential cyber-threats. Use of the platform to run advanced simulated threats will guide the company towards defining an effective security response plan in order to efficiently and effectively deal with potential security treats. LSE is looking to exploit the ability to run advanced simulated training scenarios in order to train our system administrators, solidify our procedures and protect our cyber physical systems.

When and where appropriate, LSE will focus on our existing network of SME associations via participation at industry events, which aims to expand communication of THREAT-ARREST results to a wider number of value chain participants.

3.3.10 CZ.NIC, ZSPO

CZ.NIC will exploit the THREAT-ARREST platform (TAp) in two general directions: a) internally in relation to our employees and members of the CZ.NIC association; b) externally for the dissemination of modern teaching tools within the cybersecurity community in the Czech Republic.

3.3.10.1 Internal level

We plan to use TAp to train new employees as well as to increase the qualifications of existing ones who are not directly part of the national CERT/CSIRT.CZ team, but knowledge of cybersecurity issues is appropriate for them regarding the activities of the CZ.NIC association. Thanks to TAp, we will expand the existing online courses offered within the CZ.NIC Academy and provide our staff with modern tools such as "playing a scenario", "emulation or simulation gameplay", etc. At the same time, they will profit from modern PaaS service (and environment), supplemented by advanced tools for visualization and evaluation.

CZ.NIC plans to disseminate TAp through the existing communication tools/channels, PR department, blog, or via our contributions to technically oriented media.

3.3.10.2 External level

At the external level, we plan to share the outputs of the project with a professional cybersecurity community in the Czech Republic. In doing so, we will use our position as a respected national CERT/CSIRT.CZ team, and therefore the already existing ties to all major players in the field of cybersecurity in the country. At the same time, we expect the interest of some stakeholders to prepare/deliver their content, which could enrich TAp.

Finally, appropriate communication of information on the existence and benefits of TAp to all relevant partners and the professional community will take place.

3.3.11 SIMPLAN AG

The exploitation strategy for SimPlan is based on services offered around jasima as well as licensing the software itself. Jasima is the discrete-event simulation library used as the core of THREAT-ARREST's Simulation Tool and the new jasima Visualization Tool (JVT) is used within THREAT-ARREST to visualize the state of simulated and emulated cyber-system components.

SimPlan has the full copyright on the simulation library jasima and the JVT, meaning we can license it under any commercial license we like. The core of the discrete-event simulation library is offered under the AGPL (GNU Affero General Public License) license. SimPlan plans to release the components developed within THREAT-ARREST to support cyber-security

training also under this license after the project has finished. Using the AGPL license anyone can use the simulation component as he wants to but would have to open-source it if a derived work is created and distributed. In addition to that, the software is also available using a commercial license not requiring to release of the source code of derived work (dual licensing). We are currently also discussing implementing a freemium model, offering an extended set of components with a commercial license, while the basic functionality is offered free of charge using AGPL licensing.

Services around cyber-security training will likely be the main exploitation strategy for SimPlan, fitting SimPlan's business model very well. Such services would include creating/extending simulation components as required to implement specific training scenarios as well as the creation of customized visualization scenarios. Given SimPlan's large customer base in manufacturing and logistics, we also envision that they are interested in cyber-security training for, e.g., industrial IoT scenarios.

3.3.12 Agenzia Regionale Strategica per la Salute ed il Sociale

ARESS is a technical-operational and instrumental body of the Apulia Region in support of the definition and management of social and health policies, at the service of the Apulia Region in particular and of the public administration in general and operates as an agency for study, research, analysis, verification, consultancy, and technical-scientific support. ARESS aims to organize and improve, through the continuous monitoring and verification of results, the readiness of the regional health system to respond to the needs and expectations of the health demand of the citizens of Puglia (about 4 million people). As a strategic Agency, it acquires and develops new strategic and organizational knowledge. Therefore, it experiments with paths of innovation and improvement, analyses, and disseminates the best existing social-healthcare protocols both nationally and internationally, promotes and verifies innovative management models of clinical governance in compliance with the need to rationalize and optimize expenditure from the regional budget, particularly in the issues related to the use of ICT tools. Since cyberattacks are exponentially growing in the health sector, and Covid -19 Pandemic has stressed the sector, raising awareness in human operators (medical, administrative, and technical staff) about these dangerous risks is vital. Some cybersecurity threats are caused by human errors or ignorance. The ARESS target is to organize and improve, the readiness of the regional health information system to respond to the threats of malicious persons attacking the healthcare sector. For this reason, it identifies, plans, and promotes lines of development in the field of cybersecurity so that health and social welfare are not compromised by the essential use of new technologies. Moreover, it can foster and increase virtuous relations in the health and social-health field between the world of research, the business sector, and the community, through the exploitation of the project results, to standardize best practices in the field of cybersecurity for the health sector, to be used over the whole Apulian region or at a wider level, even in other Research Projects.

3.4 Final Joint Exploitation Plan

3.4.1 Final THREAT-ARREST Exploitable assets

As presented in Table 1 (taken from "D8.6 – The THREAT-ARREST market analysis, business, and marketing plan v.2"), THREAT-ARREST managed to develop several exploitable results/assets both as unique entities and as integrated components within the final THREAT-ARREST platform.

Table 1: THREAT-ARREST key exploitable assets

#	Innovation / Key Exploitable Result (KER)	Supported by	Related WP	Innovation macro type*	Foreseen KER Exploitability* *
1	Complete <i>Integration</i> of Cyber Range Training Platform and Training Environment	<ul style="list-style-type: none"> ✓ CTPP Models-driven approach (core Model and sub-models for the various platform-tools) ✓ Full integration of all individual tools to the Platform ✓ Training Tool / Dashboard as the single User web-based interface ✓ Training Tool interlinking to all platform tools. Training Tool initializes all training sessions and all platform tools. ✓ State-of-the-Art Platform Orchestration / Management architecture. Utilization of Cloud / Open Stack and Containerization capabilities ✓ Robust Messaging processes 	WP3 WP6 WP2 WP4 WP5	IP SW TS	
2	Innovative Content / Scenario / Model <i>Generation & Deployment</i>	<ul style="list-style-type: none"> ✓ Highly innovative platform / CTPP Models-driven / multi-layer modelling ✓ Automated Scenario generation / Dynamic Scenarios ✓ Models-driven process ensures the rapid development / availability of "attacks library" (one scenario model can "build" on existing ones) ✓ Trainer is assisted in choosing individual Contents (or build new ones) in order to build-up a new / customized Training Programme. ✓ CTPP Models-driven deployment & execution (core Model and sub-models for the platform tools) 	WP3 WP4	SW TS	
3	Advanced Content /	<ul style="list-style-type: none"> ✓ Strong Customization / Adaptation features (can be tailored to Organizational needs / 	WP3 WP4	SW TS	

#	Innovation / Key Exploitable Result (KER)	Supported by	Related WP	Innovation macro type*	Foreseen KER Exploitability* *
	Scenario / Model <i>Adaptability</i>	<ul style="list-style-type: none"> Trainee type - customized Learning path and content development) ✓ State-of-the-Art Programme Adaptation capabilities. Advanced & user-friendly CTTT Models Adaptation Tool / GUI ✓ CTTT Model Adaptation based on the Assurance Tool findings. ✓ Varying difficulty levels / Runtime difficulty level adaptability 			
4	Advanced <i>Emulation</i> capabilities	<ul style="list-style-type: none"> ✓ Trainee evaluation agent in each deployed VM, configured at deployment time by the Emulation Compiler. ✓ Scoring of the trainee's activity inside the VM, monitored by the Evaluation Agent, based on graph similarity technique 	WP2	SW	
5	Advanced <i>Simulation</i> capabilities	<ul style="list-style-type: none"> ✓ Models-driven, Realistic Simulation of Cyber Systems ✓ Advanced Simulation Tool "components" structure 	WP5	SW	
6	Advanced <i>Virtual Lab</i> capabilities	<ul style="list-style-type: none"> ✓ Full Integration between Emulation – Simulation ✓ Capability to simulate / emulate numerous cases - scenarios (CTTT Models-driven Virtual Labs, utilizing Emulation + Simulation modalities 	WP2 WP3	SW TS	
7	Advanced <i>Serious Games</i> capabilities	<ul style="list-style-type: none"> ✓ Integration of Gaming tool to the Platform and Training sessions ✓ Online, single Games (could be played as a “mobile” game) ✓ Social Engineering scenarios ✓ Extendable and adjustable learning content for specific scenario 	WP4	SW TS	

#	Innovation / Key Exploitable Result (KER)	Supported by	Related WP	Innovation macro type*	Foreseen KER Exploitability* *
		<ul style="list-style-type: none"> ✓ Advanced playing mode / Game Difficulty Attribute - two playing modes ("on-demand" or "pre-defined") 			
8	Advanced <i>Data Fabrication</i> capabilities	<ul style="list-style-type: none"> ✓ Data Fabrication tool integrated to Platform. ✓ Customizable synthetic data fabrication capability ✓ Synergy with Statistical Logs Analysis Tool 	WP5	SW	
9	Advanced <i>Security Assessment / Security Posture / Testing</i> capabilities	<ul style="list-style-type: none"> ✓ Advanced & automated Security Posture Assessment ✓ Vulnerabilities Analysis / Risks-based - all layers of the implementation stack - Continuous Security Assurance ✓ Creation of customized/tailored Training Programs based on the findings of the Assurance Tool security posture assessment. ✓ CTPP Models Adaptation based on the Assurance Tool findings 	WP3	SW TS CS	
10	Advanced <i>Actionable Intelligence</i> capabilities	<ul style="list-style-type: none"> ✓ Training & Adaptation based on known and/or new advanced cyber-attack Scenarios. ✓ Continuous monitoring for new Threats / Continuous "adaptation" to new Threats - Risks (Assurance Tool-based adaptation process) 	WP3	SW TS CS	
11	Integrated <i>Learning path / capability to offer both Integrated and Customizable training programs</i>	<ul style="list-style-type: none"> ✓ Development of <i>Integrated Training Programs (Courses)</i> ✓ Customizable Learning Path (Assurance Tool findings + specific Threats modelling via the STRIDE process "drive" a customizable Scenario / Model/ Content / Learning Path creation) ✓ Integrated Learning path / capability (Training objectives as per Bloom scale, Threats) 	WP3 WP4	TS CS	

#	Innovation / Key Exploitable Result (KER)	Supported by	Related WP	Innovation macro type*	Foreseen KER Exploitability* *
		Landscapes and Cybersecurity Professionals roles training needs drive the Scenario / Model/ Content / Learning Path / overall Training Program - Course creation)			
12	<i>Trainee Evaluation and After-Action Analysis - Review (AAR)</i>	<ul style="list-style-type: none"> ✓ Trainee and Training process overall Evaluation based on Programme "Life-Cycle" (Pre-Training / On-Training / Post-Training) ✓ Post-Training Auditing & Security posting evaluation (Overall Competency evaluation based, among others, on the improvement of the Trainees Organizations' "overall security posture improvement" as assessed by the Assurance Tool) 	WP3 WP4	SW TS	
13	<i>Standardization & Certification of CTTT Training Programs</i>	<ul style="list-style-type: none"> ✓ Standardization of CTTT Programs following ISO 17024 requirements and implementing dedicated developed Taxonomy. ✓ Clear mapping against International Workforce / Role Frameworks (NICE, e-CF) / Training – Certifications schemes (ISACA, ISC², CSA, SANS) / CyberSec Standards (ISO & NIST Standards). ✓ Trainee overall Evaluation based on the Programme "Life-Cycle" (Pre-Training / On-Training / Post-Training scoring & evaluation) ✓ Trainee overall Competency evaluation is based, among others, on the improvement of the Trainees' Organizational "security posture improvement" as assessed by the Assurance Tool before and after the Training 	WP3 WP4	TS	

* **Innovation “Macro type”**: (IP) = Integrated "Product", (SW) = SW App-tool-operational system, (TS) = Training Service, (CS) = Consulting Service

****KER Exploitability** (column colour): GREEN = High, YELLOW = Moderate, ORANGE = Weak, RED = Not exploitable

3.4.2 THREAT-ARREST’s Exploitation Agreement & Business Model

In view of the project completion, THREAT-ARREST Consortium Partners decided to:

- Draft a joint “Exploitation Agreement”, which sets the framework for the “after-project” continuing joint exploitation and seeking/exploiting specific Business Opportunities. The final exploitation agreement will be created by Bird & Bird and will be signed by the THREAT-ARREST consortium.
- Discuss/draft a potential “after-project” Business Model for THREAT-ARREST (presented in Figure 9).

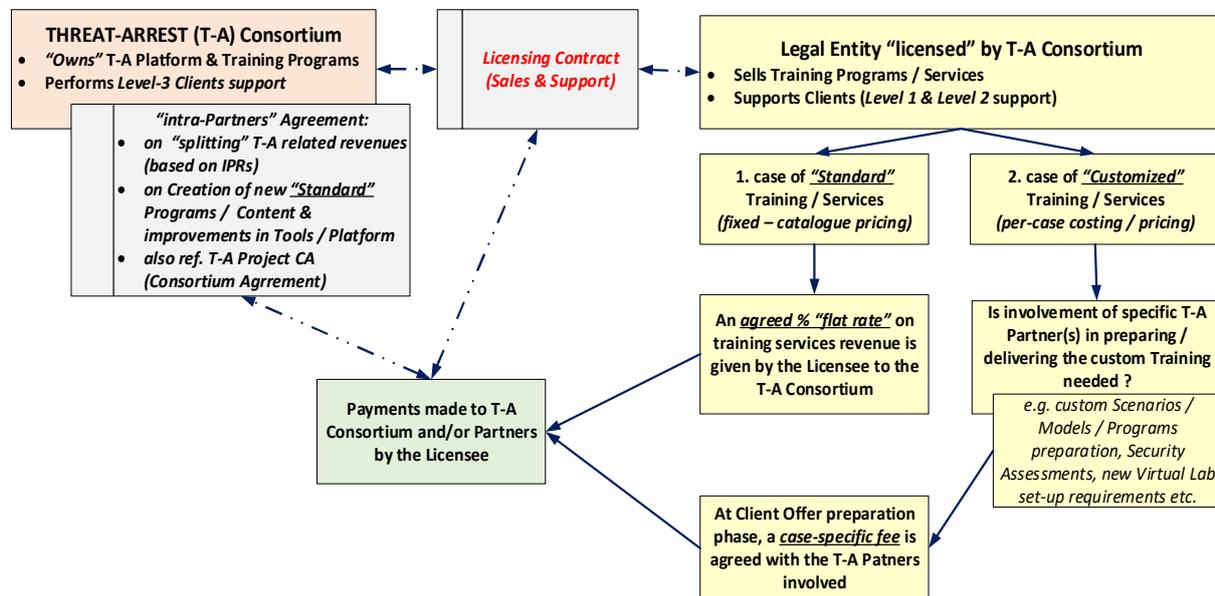


Figure 9: THREAT-ARREST Business Model – New Business Entity – Supply Chain context

3.4.3 Final THREAT-ARREST’s commercialization life-cycle and Tasks synergies

A foreseen commercialization “life-cycle” for THREAT-ARREST is presented in Figure 10.

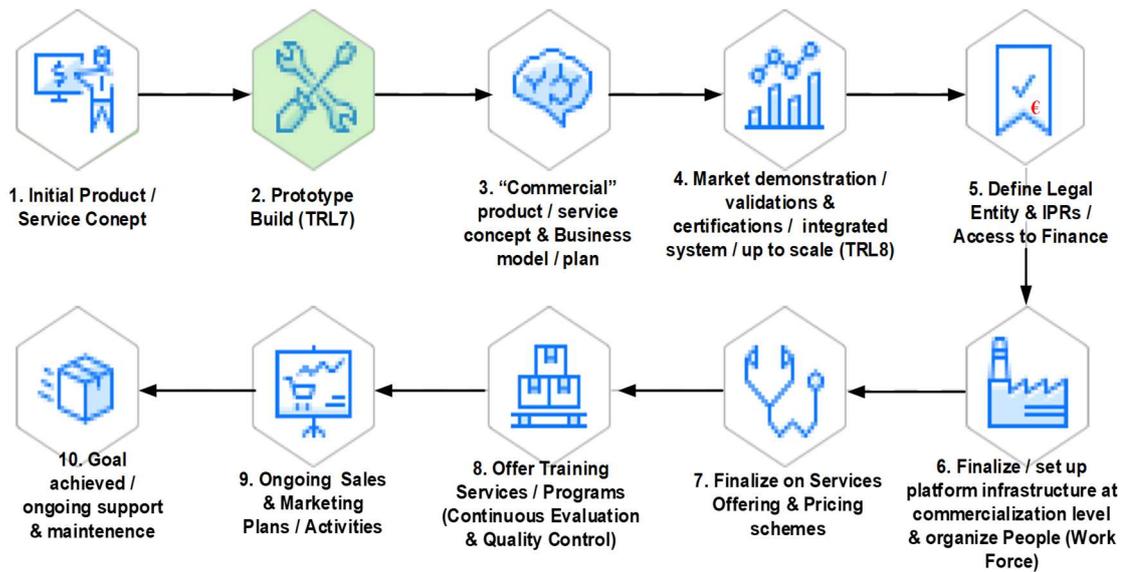


Figure 10: THREAT-ARREST commercialization lifecycle (take from “D8.6 – The THREAT-ARREST market analysis, business, and marketing plan v.2”)

Moreover, synergies among the various project Tasks, aiming at Joint Exploitation, are presented in Figure 11.

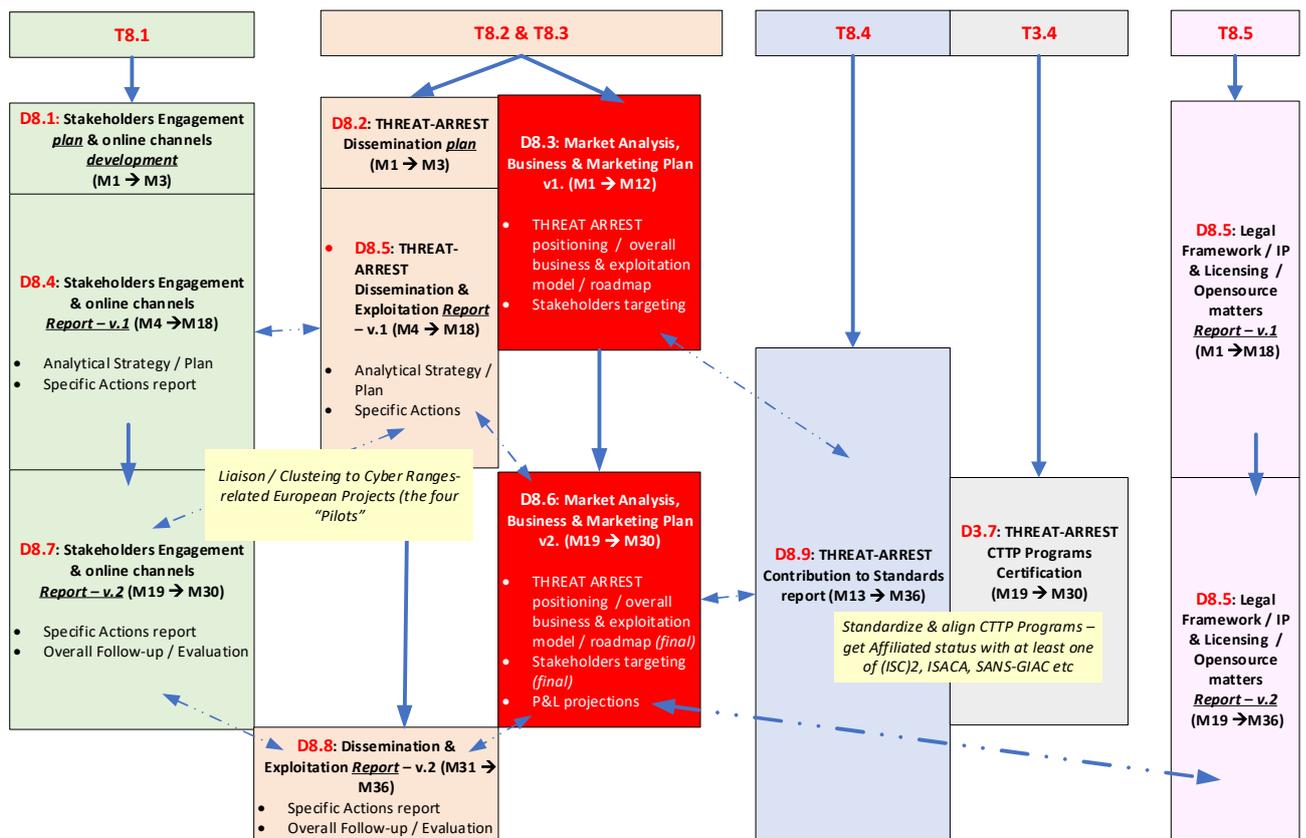


Figure 11: THREAT-ARREST: Project Task Synergies aiming at Joint Exploitation

THREAT-ARREST, within the context of its final joint exploitation plan, managed to present its work to international cybersecurity professional Training & Certifications Vendors (such as CSA) and cooperate with different European Cyber Ranges and Professional certification-related projects. More details on the above will be presented in “*D8.9 – Contribution to Standards Report*”.

4 Conclusions

This report presents the second update about the dissemination and exploitation plans by the partners of the THREAT-ARREST consortium. Every partner involved in the project had their own exploitation and dissemination plans to carry out and contributed during the whole project.

In these 1.5 past years, many dissemination activities have been conducted, through different channels, such as events participation and sponsorships, scientific publications, website and social network activities, formal and informal meetings with several potential stakeholders of the project. Moreover, each partner of the consortium led several exploitation activities, which range from commercial uses to consulting services and insurance products.

Moreover, this deliverable fulfils part of the requirements of the milestone “MS8 – 2nd pilot execution and final platform’s evaluation, final business plan, standardisation, dissemination, and exploitation reports”, due at M36.

5 References

- [1] Hatzivasilis, G.; et al.: *The THREAT-ARREST cyber ranges platform*. IEEE CSR Workshop on Cyber Ranges and Security Training (CRST), IEEE, Virtual, Greece, 26 July 2021, pp. 1-6.
- [2] Hatzivasilis, G.; et al.: *Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees*. Applied Sciences – Special Issue on Cyber Security of Critical Infrastructures, MDPI Open Access Journal, vol. 10, issue 16, article 5702, pp. 1-26, August 2020.
- [3] Smyrlis, M.; et al.: *CYRA: A Model-Driven Cyber Range Assurance Platform*. Applied Sciences – Special Issue on Security Management of 5G and IoT Ecosystems, MDPI Open Access Journal, vol. 11, issue 11, article 5165, pp. 1-28, June 2021.
- [4] Smyrlis, M.; et al.: *Cyber Range Training Programme Specification through Cyber Threat and Training Preparation Models*. 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol. 12512, Guildford, UK, 17 September 2020, pp. 22-37.

Appendix

THREAT-ARREST Brochure



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

OBJECTIVES

- Develop the means for specifying cyber security threat training and preparation models and programs to drive the realization of the training process
- Develop emulation capabilities enabling the creation of virtual cyber system components, subjecting them to cyber-attacks for training purposes, and enabling trainees to take appropriate response actions and hands-on experience against these cyber-attacks
- Develop multi-layer simulation capabilities enabling the realistic simulation of cyber systems, their usage and security attacks launched on them, through synthetic events at all layers in the implementation stack of these systems and their components reflecting realistic system conditions
- Develop cyber security training based on serious games and enable trainees to get engaged in cyber-defence, elicit threats and learn about attacks
- Develop key capabilities for the effective delivery of CTPP programs, i.e. the visualization of the operation and state of cyber systems and the emergence and effects of attacks against them; assessing trainee performance in CTPP programs and adapting them depending on it; and assessing the overall effectiveness of a CTPP program and evolving it accordingly
- Align training and simulation with the continuous security assurance of real operational cyber systems, by integrating the developed capabilities into a common platform together with security assurance assessment capabilities
- Demonstrate the use of the THREAT-ARREST framework for effective training against cyber-attacks in the domains of smart energy, healthcare and transport (shipping), using real operational cyber systems within the domains as pilots and, through them, evaluate and validate the framework
- Ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework.



Data Fabrication Platform: The DFP supports the definition of CTPP models and programmes, the presentation of learning materials/exercises of CTPP programmes, enables trainee actions in response to cyber threats, interactions with simulated and/or emulated cyber system components, trainee performance evaluation, CTPP programme evaluation and adaptation. The platform is extensible allowing new rule types to be added by users and automatically integrated in the platform. It is, also, capable of generating data from scratch, inflating existing databases or files, moving existing data and transforming data from previously existing resources. **Advancements by THREAT-ARREST:** Translation of simulation specifications in CTPP models and statistical profiles into DFP rules to enable synthetic event generation for the purposes of THREAT-ASSERT.

Emulation tools: The emulation platform provides the automated generation of emulated cyber-system components, in the form of interconnected virtual machines equipped with the appropriate software stack, as well as their interconnections in Physical and/or Software Architecture Layers (PAL/SAL) of a cyber system. It also enables interaction with the trainees. **Advancements by THREAT-ARREST:** Combination and expansion of the capabilities of the emulation and penetration testing software frameworks in order to achieve the automated generation and interconnection of emulated cyber system components. Enabling of trainees to perform security mitigation tasks. Selection of cyber-system components and attacks based on CTPP models.

Security assurance platform: This platform supports the continuous assessment of the security of the cyber system through the combination of runtime monitoring and dynamic testing in order to provide information about the status of the actual cyber system. It also collects runtime system events and generates alerts that provide the basis for setting up realistic simulations. Furthermore, it enables the configuration of security assessment, reporting and certification to the needs of different stakeholders ranging from senior management to external auditors and regulators. **Advancements by THREAT-ARREST:** (a) Offering customizable security data analytics applied to data-at-rest and live, streaming data. Off-the-shelf hardware components coupled with a custom software engine to provide a clear upgrade path, without vendor-specific lock-in. (b) Development of mechanisms to support the connectivity and use of the platform as part of a cyber threat training framework. Mechanisms supporting the implementation of continuous assurance by executing the assurance sub model of CTPP models, APIs for monitoring/testing evidence and checks reporting etc.

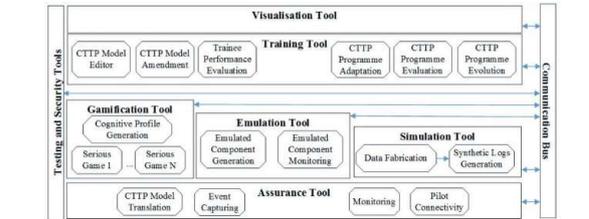
THREAT-ARREST APPLICATIONS

Smart Shipping Management

This pilot envisions to validate the THREAT-ARREST platform and provide feedback in regards to its effectiveness in the shipping industry. A system of this kind involves (i) multiple types of data and (ii) numerous stakeholders, which results in it being considered as a significantly high-risk ICT system. To that end, within this pilot, scenarios will be built and training will be designed towards advanced cyber threats and security attacks related to (a) machine failure, (b) sensors' failure and (c) performance monitoring sub-system failure. Existing security procedures will be incorporated into the THREAT-ARREST training platform, and at the same time advanced threats will also be identified and considered in the envisioned scenarios. This THREAT-ARREST application will increase security awareness in shipping ICT systems' operators and, security attacks related to the aforementioned failures are expected to be minimized. Moreover, this pilot will help towards (i) identifying specific threats

THREAT-ARREST aims to develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility & levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and a cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model driven approach where cyber threat and training preparation (CTPP) models, specifying the potential attacks, the security control of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training. The platform will also support trainee performance evaluation and training programme evaluation and adapt training programmes based on them. The effectiveness of the framework will be validated using a prototype implementation interconnected with real cyber systems pilots in the areas of smart energy, healthcare and shipping, and from technical, legal and business perspectives.

ENVISAGED PLATFORM AND PROJECT ENHANCEMENTS



Visualization tool of Jasima simulator: The visualization platform enables the visualization of simulations & the effect of training actions on simulated systems. It also, facilitates the creation, parameterization & interaction with the simulation and training platforms. Moreover, it enables users to parameterize scenario trigger simulations and view their outcomes. **Advancements by THREAT-ARREST:** (a) Extension by visualization layers (Web, Mobile Device, Window Client) based on existing technology, as required for presenting the outcomes of simulation/emulation of cyber system components in the project. (b) Leveraging serious gaming elements in order to increase learning motivation for small and medium groups.

Serious Games tools: These tools host various serious games, scenarios and training evaluation mechanisms which enable trainees to develop skills in being resilient to and preventing social engineering attacks (e.g. phishing, impersonation attacks etc.). The provided games are driven by the threats and assumptions specified CTPP models (security assurance). **Advancements by THREAT-ARREST:** Enhancement of the various serious games with (i) advanced scenario of cyber threats' mitigation and (ii) new visualization components.

Jasima-Java Simulator for Manufacturing and Logistics: Jasima generates synthetic system logs & simulates individual cyber system components and networks of such components to enable the simulation entire training scenarios defined in CTPP programmes. **Advancements by THREAT-ARREST:** Configuration and adoption of the simulator in order to meet the need of the THREAT-ARREST training platform (i.e., simulation of different layers in the cyber system implementation stack).

jeopardizing the operations of ICT systems in the Shipping Management industry and (ii) engaging multiple stakeholders from the shipping industry in the exploitation of the THREAT-ARREST training platform.

Smart Energy System

This pilot focuses on the generation of electricity from solar array installations on domestic household roofs based on a family of products and services. The end-to-end security of the Smart Energy System (SES) is a key requirement. This applies to several general types of security requirements e.g., energy consumption/production data anonymity/integrity, privacy controls over accessibility, high dependability, availability and security of all the smart objects and components involved, etc. All these components will feature in the CTPP scenarios and programmes providing a comprehensive basis for evaluating the THREAT-ARREST approach. In particular, our expectation is that the SES pilot security requirements will cover test, monitoring and hybrid-based certification as well as provide scenarios and requirements for incremental and compositional certification.

Healthcare Cyber-Security Training

This is a scenario showcasing model-based generation and delivery of training tailored to healthcare organizations of different sizes. This scenario will radically move away from current compliance-driven and technology-driven training programs, which are designed with the suppliers' interests and capabilities in mind. Instead, it will develop on threat-focused models, prioritizing the threats relevant to the specific organization's size, IT infrastructure and competence level. This way, the THREAT-ARREST model-based design technique will support customization of cyber-security training for the healthcare domain, focusing only on what is actually relevant for each specific healthcare user. The Healthcare Cyber-Security Training scenario includes the following stages: (1) Set up of a features/threats matrix for healthcare organizations, (2) Identification and prioritization of organization-specific threats, (3) Design of THREAT-ARREST models for high priority threats, (4) Generation and delivery of model-based simulations and training in selected healthcare institutions. In the end, this pilot will: (a) provide actionable information on cyber-security threats/proper responses and on medical device vulnerabilities, (b) establish an operational framework for alleviating healthcare data breaches, (c) spread best practices in public health, safety science and cyber-physical systems security to address the challenges associated with healthcare cyber-security risks and (d) develop a training framework to assess patient safety and public health risks associated with cybersecurity vulnerabilities and mitigate the risks.

PROJECT DETAILS	MORE INFORMATION
Start Date: 2018-09-01	Web: https://www.threat-arrest.eu/
Duration: 36 months	Twitter: @ArrestThreat
Project Cost: €6,431,125	Facebook: @Threat-Arrest-266454357324031
Project Coordinator: FORTH	LinkedIn: @m/threat-arrest-706485175/

Newsletter Issue 4 (February 2020)



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

FEBRUARY 2020 - ISSUE 4

Newsletter

Progress

CTTP models/programmes creation: Finalizing of Use Case scenarios. Creation and finalizing of CTPP models for the three pilots. Finalizing of Assurance Tool VM. Training Tool APIs. Development of JSON and XML versions of the CTPP models.

Emulation tool: Installation and configuration of the Emulation Tool in the final project environment. Interconnection with the Training Tool. Preparation of virtual machines needed for the three Use Case scenarios. Implementation of an algorithm for the management of VMs packet filtering, exploiting the Security Group resource of Heat. Implementation and installation of the Monitoring Tool in the final platform, in order to monitor and visualize the status of each deployed VM (e.g. CPU usage, RAM consumption, Hard Disk operation, etc.).

Training and Visualization tools: Delivery of the first draft version of the Training Tool and the relevant Dashboard. Update of training assessment methods. Integration of emulation and serious gaming components in the Training Tool. Deployment of the the Training Tool in the project's dedicated VMs. Establishment of communication between the training platform and the THREAT-ARREST training models module. Fine-tuning of technical details on how to incorporate the Jasmina Visualization Tool (JVT) in the integrated platform. Integration with the central message broker of the platform. Amendments of the visualizations for the training scenarios. Provision of the PROTECT game in the THREAT-ARREST platform and first interaction with the Training Tool. Further improvement of the user interface of the PROTECT game. Creation of the content and corresponding JSON files for the card deck regarding the healthcare pilot. Further development of the communications and data flow between the Training and Visualisation Tools and the rest of the platform's tools focusing on the training models.

Simulation Environment: Refined development/deployment process for simulating components and scenarios. Implementation of process-oriented simulation capabilities in the Jasmina simulation kernel. Finalizing of the details of the integration of the Simulation Tool with the other platform components. Presentation of an extended version of the Simulation Tool running on the THREAT-ARREST platform.

Platform Integration and Validation: Acquisition of the physical hosting server of the platform. OpenStack setup (including networking) and VMs for each tool completed and available. All platform tools' latest versions deployed in the corresponding VMs. REST APIs of tools agreed upon and available. RabbitMQ message broker installed and configured. Advances in the integration of cyber system simulation with cyber system emulation environment.

In this issue:

Progress	1
Publicity	1
Physical meetings	2
Publications	2
Academic Dissemination	2
Follow us	2



Publicity

- ✓ DANAOS hosted at their premises the "2nd Workshop of EU Research & Innovation Maritime Projects" (November 2019, more than 100 attendees), where THREAT-ARREST was presented among other projects
- ✓ FORTH and STS presented the project and demonstrated the preliminary versions for some of the platform tools in the interactive sessions of the IEEE GLOBECOM 2019 conference

Physical meetings

The 4th and 5th THREAT-ARREST plenary meetings, as well as a series of technical meetings, were successfully held



4th Plenary meeting on October 16th – 17th 2019 at SIMPLAN premises in Hanau, Germany



5th Plenary and External Advisory Board meetings on February 17th – 18th – 19th 2020 at ATOS premises in Madrid, Spain





Publications

M. Tsantekidis and V. Prevelakis, **"Efficient Monitoring of Library Call Invocation"**, at the Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), October 2019

S. Maghool, N. Maleki-Jirarajei, M. Cremonini, **"The coevolution of contagion and behavior with increasing and decreasing awareness"**, PLOS ONE open access publication, December 2019

G. Hatzivasilis, O. Soulatos, E. Lakka, S. Ioannidis, D. Anicic, A. Broring, L. Clechomski, M. Falchetto, K. Fysarakis, G. Spanoudakis, **"Secure Semantic Interoperability for IoT Applications with Linked Data"**, at the IEEE Global Communications Conference (GLOBECOM), December 2019

Academic Dissemination

Francesco Gallese, **"Feasibility study of a cyber range on OCCP platform"**, Bachelor thesis, University of Milan, Cybersecurity programme. Advisor: Elyvinia Maria Riccobene, co-advisor: Fulvio Frai

Andrea Sorrentino, **"Model-driven design of a language for the specification of attack scenarios in a cyber range"**, Bachelor thesis, University of Milan, Cybersecurity programme. Advisor: Elyvinia Maria Riccobene, co-advisor: Chiara Braghin

Alberto Porchera, **"Definition of attack scenarios for training systems"**, Bachelor thesis, University of Milan, Cybersecurity programme. Advisor: Chiara Braghin

Follow us



Newsletter Issue 5 (May 2020)



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



May 2020 – ISSUE 5

Newsletter

Progress

CTTP model/programmes creation: Preparation of all the different Training programmes needed for the mid-term review. Update of the web-based model editor. Creation of sub-models for each of the three use-cases. Updates to the CTTP Model editor, including the activation of the TLS certificate. Internal security assessments towards identifying vulnerabilities.

Emulation tool: Finalization of the first release of the integrated platform. Development of three complete use cases. Definition of the model and preparation of the virtual machine images containing software required in the training scenarios. Implementation and installation of the Monitoring tool. Added support for multi-user and multi-scenario testing. Integration of the security level of the Emulation and Monitoring tools with all the other tools. Integration of the Emulation and Monitoring tools in the overall THREAT-ARREST platform.

Training and Visualization tools: Further development of the Training Tool. Integration and communication with all the other platform tools. Deployment of the main security mechanisms. Further development of the Visualization Tool and the Dashboard. Implementation of the interaction of the Gamification Tool with the Training Tool. Deployment of the Message Broker level communications. Integration of support of TLS.

Simulation Environment: Testing and refining platform integration and security of the Simulation Tool. Integration of the Data Fabrication Platform (DFP) to the THREAT-ARREST environment. Integration of the security aspects of the DFP and its internal communications.

Platform Integration and Validation: Delivery and demonstration of the first version of the THREAT-ARREST platform. Integration of three full-fledged training scenarios. Release of video tutorials of the different platform demonstrations. Preparation of the platform's operational state for the first phase of pilots' evaluations (training).

In this issue:

Progress	1
Publicity	1
Virtual meetings	1
Publications	1
Follow us	1

Publicity

- ✓ Organization of the second MSTEC workshop in the upcoming ESORCS 2020 conference.
- ✓ Continuous updates of the social media accounts



Virtual Meetings

Because of the COVID-19 pandemic, all the meetings were held virtually

- ✓ Virtual technical meeting
- ✓ Virtual review rehearsal meeting
- ✓ Virtual review meeting

Publications

G. Hatzivasilis, K. Fysarakis, S. Ioannidis, "Cyber-Ranges as a Mean of Security Culture Establishment", ERCIM News – Special Theme: The Climate Action, ERCIM, issue 121, Article no. 36, pp. 35-37, April 2020 (Accepted)



Newsletter Issue 6 (September 2020)



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



SEPTEMBER 2020 – ISSUE 6

Newsletter

Progress

CTTP models/programmes creation: TLS renewed, updates in the CTPP Model editor (modified hardware components, new REST APIs). New/updated training programmes.

Emulation tool: Definition and design of the second phase of the development. Multiple instances of the same scenario, thanks to the use of the Jasima Visualization Tool (JVT) including information about the session, scenario, and user id. Active monitoring of the trainees' activities by the emulated components. Trainee's runtime activities evaluation based on expected traces and graph modeling of actual trainee's traces. All connections converted to HTTPS.

Training and Visualization tools: Improvement of the Training Tool (bug fixes, development in the trainees' scoring method, efficient integration and communication with all other tools). Roadmap of the new features to implement in the Jasima Visualization Tool. "Quiz Manager" and "Quiz Game" components for "Awareness Quest" quiz game. Design of the CTPP models evaluation mechanisms. Updates to the Message Broker (RabbitMQ) level communications (exchanges and queues).

Simulation Environment: Improvement of the security of the Simulation tool. Implementation, test and support of the Smart Energy pilot. Full integration of the Data Fabrication Platform in the overall platform.

Platform Integration and Validation: Second-phase hardening procedures on access protocols to the platform's services. Access of tools and services through HTTPS, TLS and SSH. Enhanced JVT-based authentication of trainees' access to the platform. Two new CTPP models/programmes integrated in the platform for the Smart Health and Shipping pilots. Preparations underway for the Smart Energy pilot. First successful results on the use of Selenium framework for comprehensive platform-level integration and quality assurance testing.

Pilots Implementation and Evaluation: 1st pilot implementation/evaluation phase and training sessions.

In this issue:

Progress	1
Plenary meeting	1
Publicity	2
Publications	2
Follow us	2

Plenary meeting

The 6th THREAT-ARREST plenary meeting was successfully held on June 29th-30th, 2020 online, because of COVID19 restrictions





Publicity

- ✓ Organization of the 2nd MSTEC workshop in conjunction with the ESORICS 2020 online conference
- ✓ Establishment of an Innovation Working Group (IWG) to facilitate the overall innovation aspects of the project
- ✓ Continuous updates of the social media accounts
- ✓ STS participated in the 3rd International Conference on CyberSecurity4 Maritime – Oil & Gas – Energy (CyBER 2020) and presented the THREAT-ARREST project and the overall CTPP modelling concept.
- ✓ The THREAT-ARREST partners were involved in several discussions and presentations for the collaboration between relevant EU projects under the umbrella of CONCORDIA and SPIDER.



Publications

G. Hatzivasilis, N. Papadakis, I. Hatzakis, S. Ioannidis, G. Vardakis, "AI-driven composition and security validation of an IoT ecosystem" at Applied Sciences – Special Issue on Smart City and Multi-Agent Systems, MDPI Open Access Journal, August 2020

G. Hatzivasilis, S. Ioannidis, M. Smytli, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, H. Koschulanski, "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees" at Applied Sciences – Special Issue on Cyber Security of Critical Infrastructures, MDPI Open Access Journal, August 2020

G. Leftheriotis, "TUV HELLAS (TUV NORD) Leading in the Implementation of Cyber-Security Innovations" article at TÜV NORD Blog, September 2020

S. Ioannidis and G. Hatzivasilis, "Cyber-ranges and security training for the maritime sector" at 4th NMIOTC Conference on Cyber Security in Maritime Domain, NATO, Souda Bay, Chania, Greece, October 2020

G. Hatzivasilis, "Password Management – How Secure Is Your Login Process" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

M. Smytli, K. Fysarakis, G. Spanoudakis, G. Hatzivasilis, "Cyber Range Training Programme Specification through Cyber Threat and Training Preparation Models" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

G. Hatzivasilis and M. Kunc, "Chasing Botnets: A Real Security Incident Investigation" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

M. Tsantekidis and V. Prevelakis, "Software System Exploration using Library Call Analysis" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, S. Astaneh, "Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

S. Pape, L. Goeke, A. Quintanar, K. Beckers, "Conceptualization of a CyberSecurity Awareness Quiz" at 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol., Guildford, UK, September 2020

Follow us



Newsletter Issue 7 (January 2021)



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



JANUARY 2021 – ISSUE 7

Newsletter

Progress

CTTP models/programmes creation: Update and finalization of the CTTP Model Editor and structure of CTTP Training Programmes. Modified hardware components. New REST APIs. New Training Parameter / Educational Model. Presentation of the Assurance Tool. New Training Programmes.

Emulation tool: Design and development of advancements and new features expected in the second phase. Integration and testing of the multi-session support, for deploying the same scenario more than once at the same time. Use of the Message Broker for initializing of the emulation environment and releasing of Guacamole credentials to access the Vms. Integration of a new Guacamole ad-hoc client to strengthen the connection security. Implementation of the final version of the tool modules. Design and development of the Evaluation agent, to monitor trainees' activities inside the VM and return the results as actual traces to the Training Tool through the Message broker. New VMs for the full CTTP Programmes.

Training and Visualization tools: Improvement of the Training Tool (efficient integration and communication with all the other tools). Split functionality of the Visualization and the Simulation tools. New simulation scenarios (red/blue team). Finalization of the Visualization Tool. Documentation of the final version of the Gamification Tool. Finalization of PROTECT and AWARENESS QUEST serious games. Design and development of the CTTP models and Programmes evaluation mechanisms. Implementation of training adaptation mechanisms with Machine Learning procedures. Further development of Message-Broker-level communications for interconnecting the tools.

Simulation Environment: Extension of the Simulation Tool and new simulated components. Full integration of the Data Fabrication Platform (DFP). Analysis of input log files to the DFP for creating realistic training scenarios.

Platform Integration and Validation: Revised integration for tools' initialisation sequence and communications through the message broker component. Final version of THREAT-ARREST components and interconnections. Simulation Tool environment initialised as part of the Virtual Lab (VL) emulation initialisation. Integration of the DFP as part of the VL initialisation process. Continued progress of Training Tool integration. Current platform state at a satisfactory level of readiness.

Pilots Implementation and Evaluation: Complete training sessions for all three pilot sectors. Conclusion of the 1st phase of THREAT-ARREST pilots implementation. Refinement of scenarios and CTTP modelling for all pilot domains (2nd phase).

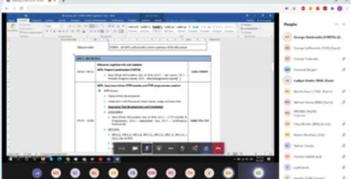
In this issue:

Progress	1
Plenary meeting	2
Publicity	2
Publications	2
Follow us	2



Plenary meeting

The 8th THREAT-ARREST plenary meeting was successfully held on February 9th 2021 online, because of COVID19 travel restrictions



Publicity

- ✓ [Article](#) and [project video](#) presentation published in Researcher's Night, November 2020, Crete – Greece.
- ✓ [Blog post](#) concerning 'Security in Human vs Cyber ecosystems'.
- ✓ Presentation of the THREAT-ARREST project in the 3rd CypBER Event 2020
- ✓ Continuous updates of the social media accounts
- ✓ Presentation and demonstration of project results in the event 'CONCORDIA – Open Doors'.
- ✓ Paper and project presentation in NATO's 4th NMIOTC Conference on Cyber Security in Maritime Domain.
- ✓ Preparation of the second special issue of the project on 'Security management of 5G and IoT ecosystems' and the open access journal MDPI Applied Sciences.
- ✓ Article posted in the TUV Nord portal concerning the THREAT-ARREST cyber-ranges approach.
- ✓ Joint workshop with other EU cyber security projects: 'Cyber Ranges and Security Training (CRST)' in IEEE International Conference on Cyber Security and Resilience (IEEE CSR).
- ✓ Presentation of the THREAT-ARREST cyber-range solution Leonardo Mechatronica company, Emirates Nuclear Energy Corporation (ENEC), Emirates Steels and Abu Dhabi National Oil Company (ADNOC).
- ✓ Evaluation of the CTTP editor and the overall THREAT-ARREST platform by external stakeholders.
- ✓ THREAT-ARREST presentation in the "Forum Risk Management – Health Care: Digital Health care and cybersecurity" session

Publications

G. Tsakirakis, "Security in Human vs Cyber ecosystems" ITML Blog post, November 2020

G. Hatzivasilis, "Training and Security in the Cyber-Space" at Researcher's Night 2020, Heraklion, November 2020

M. Hamad, Z. A. H. Hammadeh, S. Saadi, V. Prevelakis, "Temporal-based intrusion detection for IoT" at Information Technology Journal, De Gruyter Oldenbourg, vol. 62, issue 5-6, pp. 227-239, December 2020

G. Hatzivasilis, K. Fysarakis, S. Ioannidis, I. Hatzakis, G. Vardakis, N. Papadakis, G. Spanoudakis, "SPD-Safe: Secure administration of railway intelligent transportation systems" at Electronics – Special Issue on Advances in Public Transport Platform for the Development of Sustainability Cities, MDPI Open Access Journal, vol. 10, issue 1, article 92, pp. 1-26, January 2021

Mohammad Hamad, Emanuel Regnath, Jan Lauringer, Vasilis Prevelakis, Sebastian Steinhorst, "SPPS: Secure Policy-based Publish/Subscribe System for V2C Communication" at the Conference on Design, Automation and Test in Europe (DATE 2021), February 2021

Follow us



Newsletter Issue 8 (May 2021)



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

MAY 2021 – ISSUE 8

Newsletter

Progress

Platform Integration and Validation: Release of the second version of the integrated THREAT-ARREST platform. Several full-fledged training programmes and scenarios for the different project use cases included. Ongoing testing activities of pilot scenarios' implementation readiness level. TRL 7 "System prototype demonstration in operational environment" successfully reached. All platform requirements addressed in the second version of the platform. Platform quality and technical testing to ensure platform readiness for the second pilot evaluation phase, to follow. In-depth revision of selected training scenarios particularly their implementation across emulation, simulation, and gamification modalities. Further integration of AWARENESS QUIZ game into the platform. Extension of the content of the COVID-19 Quiz. Further improvements of the Botnet Quiz of the Smart Home scenario.

Pilots Implementation and Evaluation: User stories (requirements) as stemmed from the first pilot evaluation, concluded and fully addressed. Detailed timeline for the 2nd pilot implementation stage prepared and shared with partners. All CTPP programs for all pilot domains identified and under development/configuration. Preparations for the arrangements and scheduling of training sessions for the 2nd pilots' deployment. Deployment of event captors for monitoring vulnerabilities in pilots' real networks in progress.

In this issue:

Progress	1
Communication	1
Innovation/Legal	2
Publications	2
Follow us	2

Communication / Standardization

- ✓ Initial discussions for the participation of THREAT-ARREST in the [ECHO Federated Cyber Range Marketplace](#)
- ✓ Discussions for the creation of a meta-model and the technical federation with KYPO (CONCORDIA H2020 project)
- ✓ Registration process with (ISC)² "PDI" (Professional Development Institute), regarding THREAT-ARREST & CTPP Programs evaluation and potential "authoring" for (ISC)² in progress.
- ✓ Communication with (ISC)² PDI Key Executives
- ✓ Communication with ISACA Athens Chamber in order to organize THREAT-ARREST demonstration/workshop
- ✓ Communication with ISACA Key Executives regarding potential evaluation of THREAT-ARREST & CTPP Programs
- ✓ Communication with Cyber Security Alliance (CSA) Key Executives in order to organize THREAT-ARREST demonstration/workshop
- ✓ Supporting of [Cyber Ranges and Security Training \(CRST\)](#) workshop in the IEEE International Conference on Cyber Security and Resilience (IEEE CSR)
- ✓ Special Issue on 'Artificial Intelligence Applications in Next Generation Communication Infrastructures Security' on the MDPI Journal Electronics



Innovation / Legal Framework

- ✓ Innovation aspects of the project facilitated by the Innovation Working Group (IWG)
- ✓ Further analysis of the basic legal and security requirements of the platform
- ✓ Interim legal audit regarding free and open source software used in the platform
- ✓ Identification of other key legal action points
- ✓ Legal guidance and recommendations in the context of the discussion on the exploitation of the THREAT-ARREST platform

Publications

J. T. Hounsou, P. B. C. Niyomukiza, T. Nsabimana, G. Vlavonou, F. Frati, E. Damiani, "Learning Vector Quantization and Radial Basis Function Performance Comparison Based Intrusion Detection System", International Conference on Intelligent Human Systems Integration (IHSI), Palermo, Italy, Springer, AISC, vol. 1322, pp. 561-572, February 2021. (DOI: 10.1007/978-3-030-68017-6_83)

M. Smyrli, G. Spanoudakis, K. Fysarakis, "Teaching Users New IoT Tricks: A Model-driven Cyber Range for IoT Security Training", IEEE Internet of Things (IoT) Magazine, March, 2021

M. Smyrli, I. Somarakis, G. Spanoudakis, G. Hatzivassilis, S. Ioannidis, "CYRA: A Model-Driven Cyber Range Assurance Platform", Applied Sciences – Special Issue on Security management of 5G and IoT ecosystems, MDPI Open Access Journal, vol. 11, Issue 11, article 5165, pp. 1-28, June 2021 (DOI: 10.3390/app11115165)

Follow us







Newsletter Issue 9 (August 2021)



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



AUGUST 2021 – ISSUE 9

Newsletter

Progress

Pilots Implementation and Evaluation

All evaluation tests performed:

- 3 distinct pilots (Smart Health, Smart Energy, Smart Transportation)
- Around 20 participants/employees evaluated in each Pilot
- 3 CTTTP programs (General Awareness, Edge System Security, Backend Security Manager)

"The THREAT-ARREST EU project is coming to an end after a wondrous three-year journey. We had our good times and our bad times, but we faced everything together. Thank you all for your great work and devotion to the project. I am looking forward our future collaborations!"

Coordinator: Sotiris Ioannidis

In this issue:

Progress	1
Commercialisation	1
Innovation/Legal	2
Publications	2
Follow us	2

Publications

M. Tsantekidis, V. Prevelakis, "MMU-based Access Control for Libraries", 18th International Conference on Security and Cryptography (SECRYPT 2021), Lisbon, Portugal, Springer, pp. 1-1, July 2021

G. Hatzivasilis, et al., "The THREAT-ARREST cyber ranges platform", IEEE CSR Workshop on Cyber Ranges and Security Training (CRST), IEEE, Virtual, Greece, pp. 1-6, July 2021

Pape, S.; Klauer, A. and Rebler, M.; Leach, "Let's Expose Evidently bad data Collecting Habits - Towards a Serious Game on Understanding Privacy Policies (Poster)", 17th Symposium on Usable Privacy and Security (SOUPS), August 2021

Hatzivasilis, G., Ioannidis, S., Pysarakis, K., Spanoudakis, G., Papadakis, N., "The Green Blockchains of Circular Economy", Electronics – Special Issue on Artificial Intelligence Applications in Next Generation Communication Infrastructures Security, MDPI, Open Access Journal, vol. 10, Issue 16, pp. 1-16, August 2021. (DOI: 10.3390/electronics10162005)



Academic achievements

Paolo di Prima, "Sistema plugin-based per la collezione di eventi nell'utilizzo di cyber range", Master thesis at University of Milan. Advisor: Evinia Maria Roccobene, co-advisor: Fulvio Fusi.

Michele Toccafani, "Approccio model driven per generare cyber ranges", Master thesis at University of Milan. Advisor: Chiara Braghin.

Alessandro della Torre, "Sistema di monitoraggio e valutazione per cyber ranges", Bachelor thesis at University of Milan. Advisor: Chiara Braghin.