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

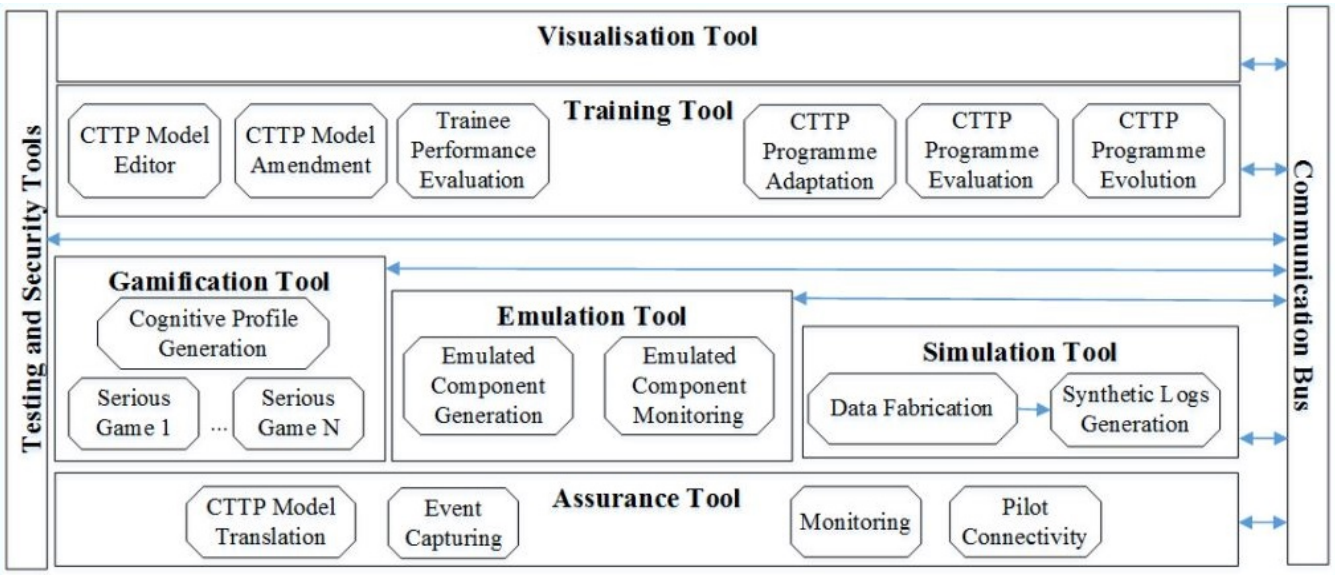
OBJECTIVES

- 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 CTTP 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 CTTP programs and adapting them depending on it; and assessing the overall effectiveness of a CTTP 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 these 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.

Supported by the European Union Horizon 2020 Programme under grant number 786890

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 and levels of expertise in defending high-risk cyber systems and organizations to **counter advanced, known** and **new cyber-attacks**. The THREAT-ARREST platform will deliver security training, based on a **model driven** approach where **cyber threat and training preparation (CTTP) models**, specifying the potential attacks, the security controls 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



Visualisation

Visualisation tool of Jasima simulator: The visualisation platform enables the visualisation of simulations and the effect of training actions on simulated systems. It, also, facilitates the creation, parameterization and interaction with the simulation and training platforms. Moreover, it enables users to parameterize scenarios, trigger simulations and view their outcomes.
Advancements by THREAT-ARREST: (a): Extension by visualization layers (Web, Mobile Device, Windows 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 Gaming

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 in CTTP models (security assurance).
Advancements by THREAT-ARREST: Enhancement of the various serious games with (i) advanced scenarios of cyber threats' mitigation and (ii) new visualisation components.

Simulation

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

Training

Data Fabrication Platform: The DFP supports the definition of CTTP models and programmes, the presentation of learning materials/exercises of CTTP programmes, enables trainee actions in response to cyber threats, interactions with simulated and/or emulated cyber system components, trainee performance evaluation, CTTP programme evaluation and adaptation. The platform is extendible 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 CTTP models and statistical profiles into DFP rules to enable synthetic event generation for the purposes of THREAT-ARREST.

Emulation

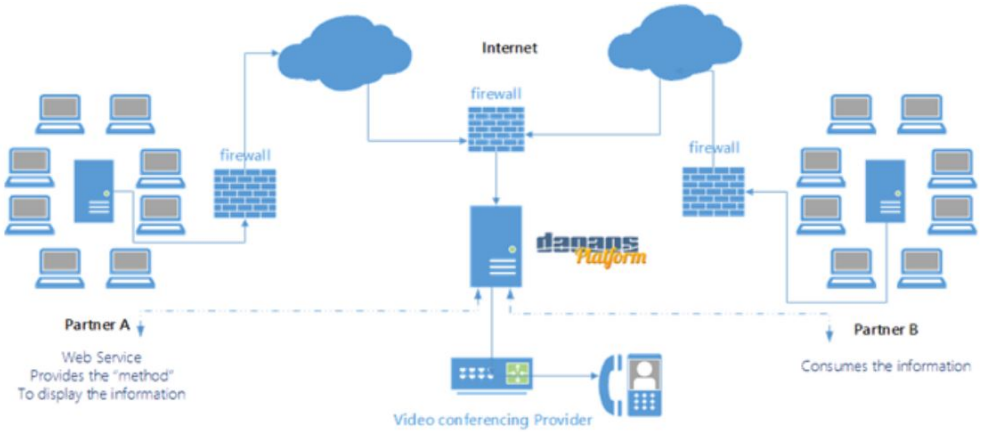
Emulation tools: The emulation platform provides the automated generation of emulated cyber-system components, in the form of interconnected virtual machines equipped with the appropriate software stack, as well as their interconnections in Physical and/or Software Architecture Layers (PAL/SAL) of a 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 CTTP models.

Assurance

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 CTTP models, APIs for monitoring/testing evidence and checks reporting etc.

THREAT-ARREST APPLICATIONS

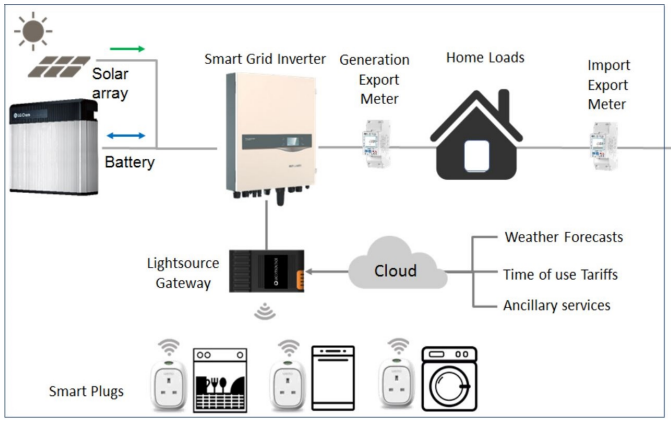
Smart Shipping Management



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

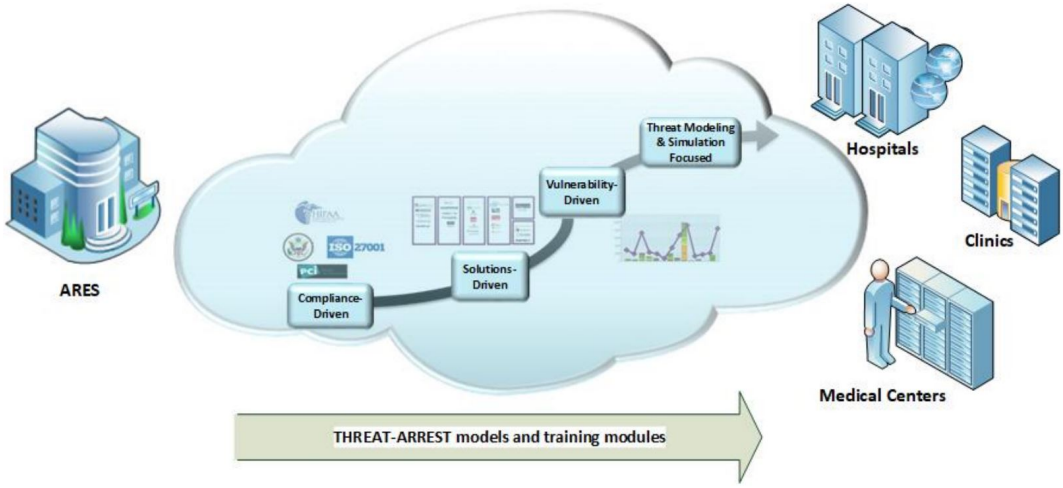
jeopardizing the operations of ICT systems in the Shipping Management industry and (ii) engaging multiple stakeholders from the shipping industry in the exploitation of the THREAT-ARREST training platform.

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 CTTP 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
Start Date: 2018-09-01
Duration: 36 months
Project Cost: €6,431,125
Project Coordinator: FORTH

MORE INFORMATION
Web: https://www.threat-arrest.eu/
Twitter: @ArrestThreat
Facebook: @Threat-Arrest-266454357324031
LinkedIn: @/in/threat-arrest-706485175/