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

FEBRUARY 2020 – ISSUE 4

Newsletter

In this issue:

Progress

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

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

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"**, 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: Elvinia Maria Riccobene, co-advisor: Fulvio Frati

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: Elvinia 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