Cyber Security & ICT Solutions

CYBER TRAINER

In a country ecosystem, the ability to execute today, and address in the future, the best cyber security strategy includes the development of national defense capabilities, in order to enhance training, exercises and the continuous update of Governments' and Critical Infrastructures' cyber defense staff. The operators of national defense and critical industries such as utilities, posts, airports and hospitals must know the main cyber threats that can damage their organizations and being able to implement promptly, quickly and in a cooperative way the needed actions to stop a threat or to minimize the effects of an attack.

An advanced cyber training environment takes advantage of fully-developed simulation and virtualization technologies to build realistic and immersive experiences to allow the education and the training of cyber security personnel and to support debriefings on "hot" themes relevant to national resilience.

An interaction scenario is also useful to develop analysis and test activities on new ideas and strategies related to the cyber warfare.

CYBER TRAINER SOLUTIONS

Leonardo Cyber Trainer, designed on advanced virtualization technologies, artificial intelligence and simulation, is a unique and integrated environment for training. Its goal is to block complex cyber threats and attacks against information and operational systems, continuously training cyber resilience staff of Federal Agencies and Critical Infrastructures.
The Cyber Trainer platform, usable through on premises or hybrid models, allows the generation of multiple training scenarios with variable complexity, where practical cyber warfare exercise sessions can be executed.

CYBER TRAINER

The platform also enables the management of education and the interaction between students into the classroom. The platform offers tools for the automatic evaluation of performances, both in the training and in the gaming phases, and for management of “in action” briefing and post training debriefings.
Leonardo Cyber Trainer also leverages our cyber resilience, intelligence and cyber security specialists to help the customer in the design of physical on premises infrastructures dedicated to cyber training and in the supply of professional services supporting the education and the training.

CYBER TRAINING PROCESS AND SKILLS

The solution is based on training process that starts with the design of the education path for students and gaming sessions to train them. The participants, divided into teams, compete in launching simulated cyber attacks and in defending assigned structures and borders. The detailed evaluation and analysis of learning performances and practical training complete the overall training process, with the goal of having cyber resilience teams constantly skilled and trained in the cyber warfare.

Design: planning of paths for education in classroom and gaming practical sessions through automatic tools both to support teachers and to set up, design and configure training scenarios in terms of theaters, attack tactics and defense techniques.

Gaming set up and execution: set up of the simulation and training operational scenario. Execution, tracking and awareness of the gaming activities in progress or addressed by students, with the chance to visualize their performance, also in the form of a simplified metaphor, to support the debriefing immediately following the action (hot wash debriefing).

Evaluation: automatic and semi-automatic evaluation of the overall student training.

Cold Debriefing: analysis that can be performed both individually and in team of the post portem exercise; it allows the tracking of all the actions carried out during the execution phase and the use of visual analytics and gamification techniques for the simplified reading of the exercise operating scenario.

Leonardo Cyber Trainer solutions take advantage of skilled professionals, particularly in complex processes of set up of theaters, scenarios and attack tactics. Scenario researchers know in detail the platform and are skilled in the most critical international issues of Cyber Security, Intelligence and Digital Resilience domains. They are able to build realistic and successful training operative scenarios for learning, training and testing purposes.

FUNCTIONALITIES AND LOGIC MODEL

Leonardo Cyber Trainer provides four families of functionalities based on environments, applications, tools and connectors implemented on scalable and secure hardware architecture and virtualized software infrastructure. They allow to have physical and digital solutions profiled by user typology and potentially provided in multi-tenancy mode in case of cloud delivery.

Functionalities:

- **Configuration:** configuration of training scenarios, attack tactics and operational scenarios.
- **Learning:** support tools dedicated to teachers and apprentices aimed at the definition of training paths and for evaluation and collaboration purposes.
- **Range:** execution, tracking, automatic and semi-automatic evaluation of the training sessions, ex post debriefing.
- **Test:** cyber security tests on physical and virtual devices and cyber weapons experimentation.

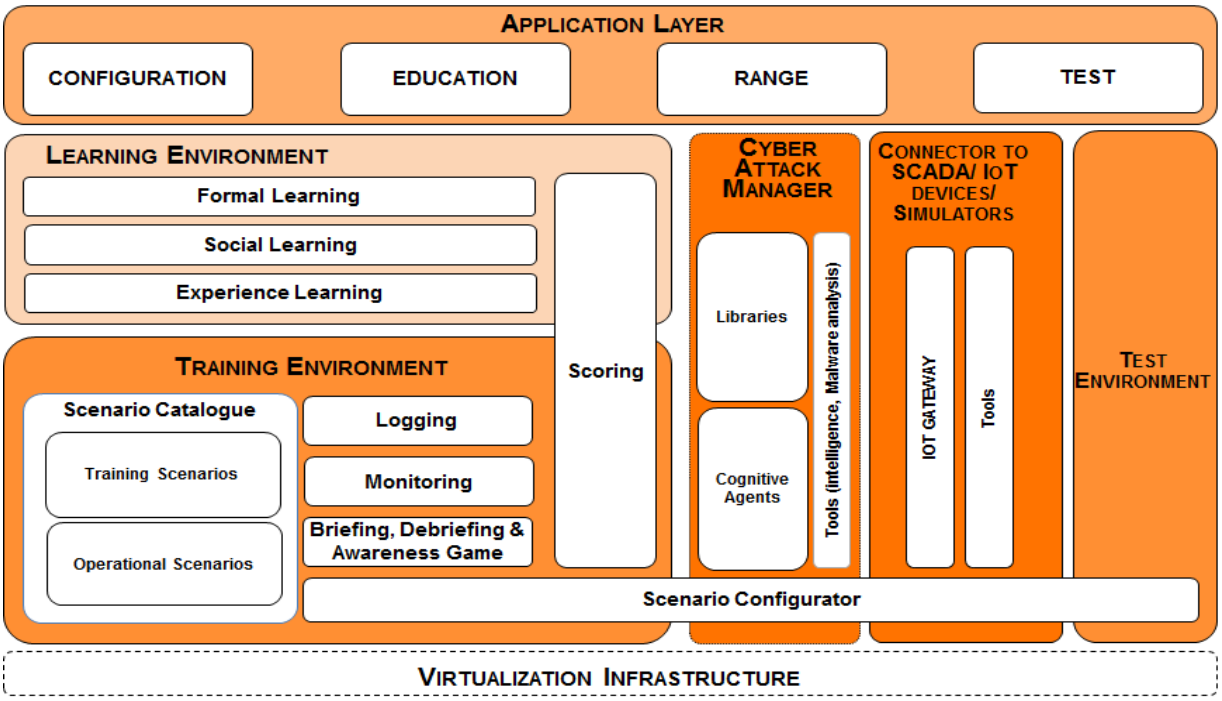
Environments:

- **Cyber Attack Manager:** provides tools, based on predefined libraries and cognitive systems, for the definition, the automatic & intelligent generation and the execution of attack tactics.
- **Connector to SCADA, IoT devices and Simulators:** allows the integration of physical systems in the virtualized scenarios, includes traffic generators, anti-virus/ anti malware tools and software probes used to define the operating context of the simulations.
- **Learning Environment:** integrates tools to support formal, social, experiential and collaborative learning.
- **Training Environment:** addresses complex training scenario modeling, manages the practical exercise sessions and their tracking also to enable debriefings.
- **Test environment:** allows the testing of physical and virtual devices; it is based on multi standard interfaces (physical communication networks and protocols) for the integration of heterogeneous devices dynamically programmable using the Connector module.
- **Virtualization Infrastructure:** permits to abstract the variety of computers contained in the hardware infrastructure and to manage them accordingly to the specific configurations required to reproduce a training scenario, in terms of information systems, hostile activities, defense architectures. The virtualization infrastructure allows to reproduce training scenarios with the highest level of automation, also with an on-demand mode and a multi-tenancy approach.

GAMING, AWARENESS GAME AND ARTIFICIAL INTELLIGENCE

The practical training sessions allow the students, divided into the Red Team and Blue Team, to practice the cyber attack and defense. This happens after the configuration of the specific training scenario and the implementation of the simulation, in terms of roles, traffic network, systems to be protected or attacked, scoring mechanisms. During the session, each team can use the suggestions of a Purple Team, made up of experts and process leaders.

Gamification features (awareness game) present at a glance and in an intuitive way the real development of the exercise. In practice, the session is turned into an electronic game for an easy understanding and interpretation and can be used both in the hot wash debriefing phase and in the cold debriefing.



CYBER TRAINER

In this context artificial intelligence has the key function for automatically generating attack tactics, continuously updated in line with the new threats detected in the real cyber-space by the Threat Intelligence systems. Threats are selected and configured within the training scenarios also on the basis of the learners' specific training needs.

Leonardo Cyber Trainer uses Artificial Intelligence also to create a virtual assistant, a Cyber Assistant, allowing learners to access the information gathered by intelligence and cyber security simulated knowledge base. In practice, the Cyber Assistant effectively supports the Blue Team with operative suggestions while playing the game.

BENEFITS

- Design, development and improvement of the defense and attack abilities of Governments and Critical Infrastructures in national and international cyber-warfare strategic contexts.aving
- Improvement of ex-post capabilities analysis of main errors and best practices during training.
- Provision of training sessions based on simulation of the on-the-job experience and on solving complex problems related to cyber security issues.
- Having a dedicated environment in order to exchange ideas, improve the teamwork of cyber defense teams, propose and test new ideas and finally collect new needs in the field.

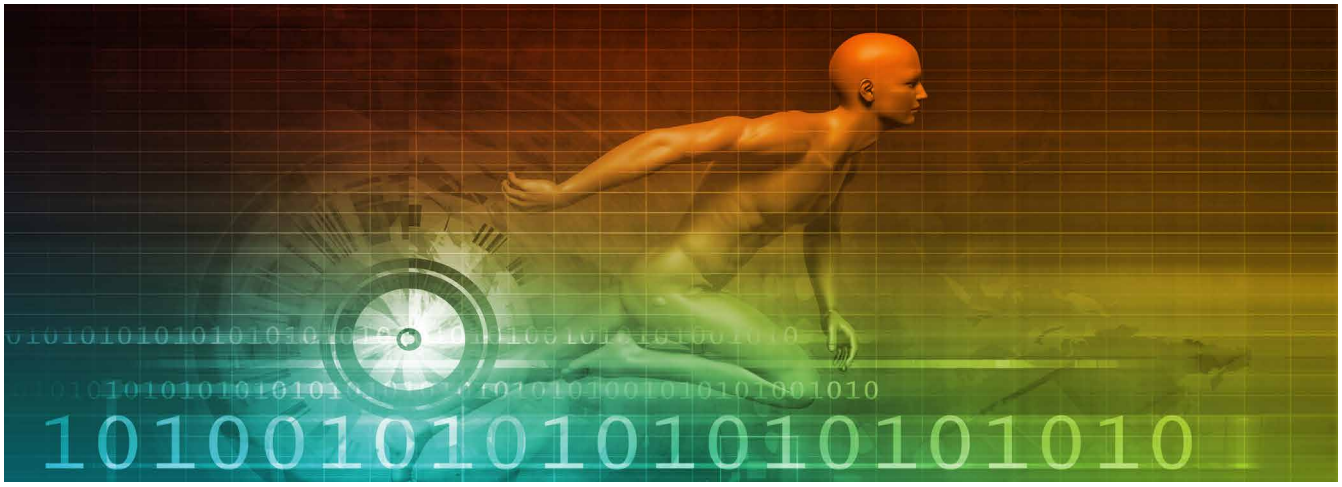
LEONARDO'S OFFER PORTFOLIO

Leonardo protects Governments, National Critical Infrastructures and National Strategic Industries against cyber threats and attacks using its technology and experience in cutting-edge cyber security and critical IT systems, all crucial for the operation and service continuity for citizens and countries.

Organized into two different lines **Business-driven Cyber Security and Critical Information Systems**, Leonardo's Portfolio leverages the main emerging technologies and the most up to date technological paradigms to offer solutions, platforms and services able to support customers' secure digital transformation.

The Cyber Trainer Solutions are part of the Business-driven cyber security offer, including:

- **Cyber Protection & Resilience** for governments and critical infrastructures through services, tools and methodologies for the management of the entire threat life cycle and for the resilience of systems and services against cyber-attacks.
- **Intelligence & Investigation** in order to support Law Enforcement Agencies, Blue Lights e and Defense in the research, the collection and the analysis of relevant information for investigation activities, strategic intelligence and preventing crime.
- **Cyber Training**: for the creation and simulation of complex cyber-warfare scenarios with the aim of training operators in charge of IT/OT system security, both in the civil and military sector.



LEONARDO
SISTEMI PER LA SICUREZZA E LE INFORMAZIONI

For more information please email: ICT-Cyber@leonardocompany.com
Leonardo S.p.a.
Via Laurentina, 760 - 00143 Roma - Italy - Tel: +39 06 50275738 - Tel +39 06 50275685