Cyber Range and Training Solutions

CYBER SECURITY DIVISION

LEONARDO

The execution and development of an optimized cyber security strategy for national ecosystems imply the construction of defence capabilities, including training and exercising for technical staff working in both governmental and critical infrastructures sectors.

The operators of national industries and utilities like telcos, transports, energy providers, posts and many others, must have a deep awareness of the main cyber threats that can damage their organizations, and must be able to test and 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 ecosystem for modelling real life infrastructures, cyber training and cyber pen testing must takes advantage of state-of-the-art cloud provisioning and virtualization technologies to build realistic and immersive experiences, enabling learning, training, tool testing and exercising for cyber security personnel, supporting analysis and debriefings on “hot” themes relevant to how keep service and functional resilience at the desired levels.

The same environment should be used for the development of analysis and testing activities on new software components and network equipment, to optimize organizational strategies and procedures to protect against internet cyber warfare malicious activities.

CYBER RANGE

Leonardo Cyber Range, designed upon best-of-breed technologies for Infrastructure-as-a-Code provisioning, cloud management, network function virtualization, is a complete, added value ecosystem of integrated tools and applications.
Its goal is to adequately keep personnel able to face complex cyber threats and attacks against information (IT) and operational (OT) systems, supporting testing, continuous training and managing complex, highly realistic exercises for staffs and teams belonging to Government Agencies and Critical Infrastructures Operators.
The Cyber Range allows the generation of multiple training scenarios characterized by different levels of complexity and the execution of practical cyber warfare exercise sessions based upon the designed scenarios.
The Cyber Range can be delivered on premises, provided in the cloud as “live lab” based training-as-a-

service, or even accessed into dedicated tenants, in case of exercising and gaming over complex, wide theatres (as the “digital twin” representations of enterprises and infrastructures are indeed).
The system allows the development of a complete e-learning contents including support for class based sessions, tools for the automatic evaluation of performances and for handling “live” monitoring of exercises and post gaming debriefing analysis.
Leonardo Cyber Range 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 supports a training process that starts with the design of the learning path for students and related training sessions to train them.
The participants, organized in competing teams, launch cyber-attacks and defend assigned infrastructures and borders. The process, aiming at the development of a continuously skilled and trained team, is completed by the detailed evaluation and analysis of learning performances related to the training session.

- **Design:** planning of practical sessions through automatic tools both to support teachers and to set up, design and configure training scenarios in terms of learning paths, theatres, attack tactics and defence techniques.
- **Set up and execution:** set up of the simulation and training operational scenario. Execution, tracking and awareness of the training activities, possibility to visualize trainees’ performance to support the hot wash debriefing analysis.
- **Evaluation:** automatic and semi-automatic evaluation of the overall student training.
- **Cold Debriefing:** in depth, ex-post analysis (that can be performed both individually or in team) of the exercise; it allows the tracking of all the actions carried out during the execution phase.

Leonardo Cyber Range & Training solutions take advantage of skilled professionals managing complex processes involved in configuration of theatres, scenarios and attack tactics.
Scenario researchers have a deep knowledge of the system are able to build realistic and successful training operative scenarios for learning, training and testing purposes.

CAPABILITIES AND LOGIC MODEL

Leonardo Cyber Range capabilities are based on environments, applications, tools and connectors implemented on highly scalable, secure software defined architecture.

CAPABILITIES

- **Theatre composition and configuration:** visual and textual configuration of training labs, gaming theatres, digital twins and attack tactics, with multiple replication capability of theatre instances, concurrent exercise management and multi game session capability.
- **Dynamic deployment of theatres:** engine for structured deployment of team access networks, external theatre monitoring and scoring subsystems, management networks, internet and/or complex network environments, attack tools, target digital twins.
- **Learning & educational services:** support tools dedicated to teachers and apprentices aimed at the definition of learning paths, access to goal oriented, course-dedicated cyber labs, evaluation and collaboration tools, automatic and semiautomatic evaluation of the learning tests.
- **Gaming & exercise manager:** management of remote access to the theaters for attack and defence activities, tracking of actions, team reports acquisition, advanced, multidimensional scoring based on availability, usability, automated attack exits, team report quality.
- **Red team automation:** attack campaigns’ configuration over multiple theaters replicas, automatic and semiautomatic execution, support for scoring and awareness.
- **Interoperability:** adoption of Infrastructure-as-a-code standard languages, open source cloud management platforms, virtual overlay networking standards and virtual-to-physical gateways to guarantee the system’s native interoperability.

MAIN COMPONENTS

- **Attack execution platform:** it provides definition, automatic deployment, configuration and execution of attack tactics. It includes FOSS and/or COTS red tools covering the full attack chain, from recognition to final command and control.
- **Exercise Management & Orchestration platform:** it enables theatre composition, exercise configuration, theatre deployment & management, game monitoring, theatre event data capturing, team scoring metrics evaluation and scoring, gaming awareness
- **Educational platform:** it supports the course execution and includes formal, experience-based and social learning allowing students to share fluid information with other apprentices.

The cyber range permits to realistically reproduce the communication and processing of any technological node as part of the infrastructure to be modelled in order to support a full exercise or cyber pen test scenario. The system enables the reproduction of attack testing and multi team training scenarios with the highest level of automation and tracking support.

EXERCISE MANAGEMENT AND AWARENESS

The practical training sessions allow the students trainees, generally divided into Red Teams (attackers) and or Blue Teams (defenders), to practice cyber-attack and defense techniques over a partially known, dynamic theatre.
During the session, each team is required to issue attack execution or threat, incident or action reports and cooperate using an open source threat intelligence platform and team messaging tools. Red and Blue Teams take advantage of the suggestions of a White Team, composed by exercise supervisor and/or cyber experts and process leaders.
The range provides a series of awareness canvas fulfilling "at a glance" visualizations of the attack and defence actions for each theatre instance. Awareness offers an easy understanding and interpretation of the attack steps, defence actions and behaviours and can be used both in the hot wash debriefing phase, as in later cold debriefings.
Artificial intelligence is used by the system to support trainees during their learning path through a virtual assistant and to automatically generate attack tactics, providing continuously hints to configure tactics in order to face the exercise objectives.

BENEFITS

- Design, development and improvement of cyber defence capabilities for Operators of Governments and Critical Infrastructure.
- Improvement of ex-post analysis capabilities of main operational errors and best practices during cyber defence.
- Provision of training sessions simulating on-the-job experience and solution of complex problems related to cyber security incidents.
- Dedicated training ecosystem to exchange ideas, improve skills of cyber defense teams, propose and test new approaches and collect new requirements in the field of cyber protection.
- Interoperability with remote orchestrators, scenarios and native capabilities to share cyber gaming fields and be federated with other Cyber Ranges services.

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 Range & Training 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 Defence 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.

For more information please email:
ict-cyber@leonardocompany.com

Leonardo S.p.a.
Via Puccini, 2 - 16154 Genoa - Italy
Tel. +39 010 65821
Fax +39 010 6582898

leonardocompany.com

MM08974 09-19

LEONARDO