LEONARDO CYBER & SECURITY SOLUTIONS

CYBER RANGE

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, 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 ways the needed actions to stop a threat and to minimize the cyber attacks' impacts.

Training and testing are the two essential, human driven processes that can effectively support the overall cyber "protection" cycle only and only if they can cope with real threats in highly realistic situations.
The best cyber training and testing environments should theoretically be real production systems, but in practice, such systems cannot be exposed to critical situations because of potential consequences and the high price of learning only by mistakes.
This issue is solved by using advanced ecosystems for real-world infrastructure modelling that leverage state-of-the-art cloud provisioning and virtualisation technologies. Such infrastructures allow to build realistic and immersive experiences, enabling learning, training and exercising for cyber security personnel, supporting analysis and debriefing on hot cyber security issues, that are essential to maintain service and operative resilience at desired levels.
These environments should also be used to develop analysis and testing activities on new software components and network equipments, as well as to optimise organisational strategies and procedures to protect against malicious cyber warfare activities on the Internet.

CYBER RANGE

Leonardo **Cyber Range** is a multi-purpose operational environment, that aims to create realistic operational training scenarios using best-of-breed technologies for Infrastructure-as-Code provisioning, cloud management, software defined networking.
Its goal is to adequately keep Government Agencies and Critical Infrastructures' cyber security teams able to face complex cyber threats and attacks against information (IT) and operational (OT) technologies, to test new attacks and defence techniques, to verify infrastructures management procedures as well as actions and methods used to protect technological systems and to manage security incidents.
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 such as "digital twin" representations of enterprises and infrastructures.

PROCESS AND SKILLS

The Cyber Range allows the generation of multiple training scenarios characterized by different levels of complexity and the execution of practical cyber game sessions based upon the designed scenarios.
The practical training sessions allow the trainees, generally divided into Red Teams (attackers) and Blue Teams (defenders), to practice cyber-attack and defence techniques over a partially known, dynamic theatre.
During the cyber game session each team behaves according to assigned targets and can log each action (with evidences) in order to earn score. The teams are required to issue attack execution or threat, incident or action reports and cooperating through open threat intelligence platforms and team messaging tools. Red and Blue Teams take advantage of the suggestions of a White Team, composed by exercise supervisors and/or cyber experts and process leaders.

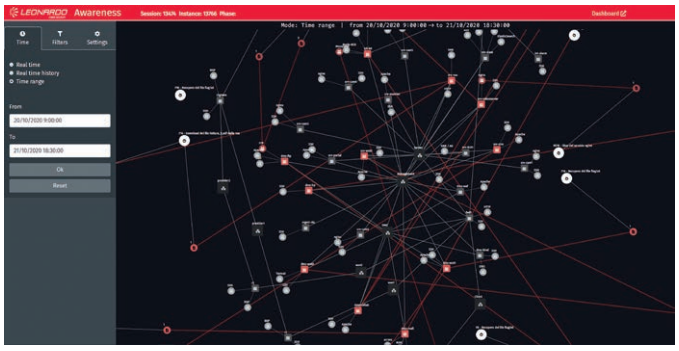
Each team has suitable tools deployed in theatre (attack workstation with a collection of tools and defence workstation with SIEM, probes, monitoring tools, etc.) in addition to an automated attack/defence platform. The Cyber Range provides also a series of awareness canvas fulfilling "at a glance" visualizations 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. The platform portal provides administrative/monitoring and reporting tools; automated actions recorded and scored as well.

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

CAPABILITIES

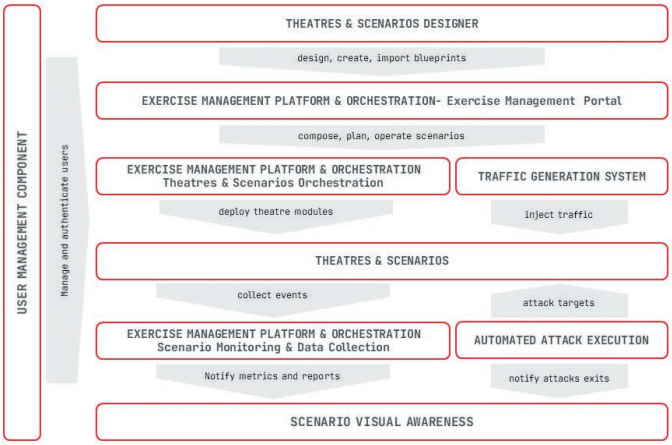
Leonardo Cyber Range capabilities are based on environments, applications, tools and connectors implemented on highly scalable and secure software defined architecture. The instantiated systems, networks and applications together with contextualized information and any automatic attack and defence tool constitute the exercise theatre. The theatre represents a model that can be reused and specialised. A scenario is built on a theatre by defining the type of exercise, the objectives, the rules for scheduling events, the composition and type of teams that will compete during the cyber game.

- **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.
- **Cyber Gaming & Exercise Manager:** management of remote access to the theatres 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 and Blue Team Automation:** attack campaigns and defence tactics' configuration over multiple theatres replicas, automatic and semiautomatic execution, support for scoring and awareness.
- **Interoperability:** adoption of Infrastructure-as-Code standard languages, open source cloud management platforms, virtual overlay networking standards and virtual-to-physical gateways to guarantee the system's native interoperability.



Visual awareness module interface example

Attack (defence) execution platform interface example



Logic model scheme

LOGIC MODEL

Cyber Range is based upon a software defined datacenter implementing the infrastructure upon which virtual machines and architectural modules needed to execute the exercises are instantiated.

- **Attack Execution (defence) Platform:** it provides definition, automatic deployment, configuration, scheduling and orchestration and execution of attack and defence tactics. It may include FOSS (Free and Open Source Software) and COTS (Commercial Off-The-Shelf) 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 & orchestration, game monitoring, theatre event data capturing, team scoring metrics evaluation and scoring, gaming awareness.

- **Theatre Module Design:** graphic tool that provides library management, visual design, blueprint generation and publication. It is designed to set up a theatre which is the simulation environment where the teams will compete.

- **Visual Awareness Module:** this portal allows to acquire the indications and evaluations of the White Team regarding the performance of the participants during the cyber game to track the activities carried out by the teams involved in the exercise.

- **Traffic Generator:** subsystem to simulate users' activities and related network traffic within the simulated environment.

- **Identity and Access Management:** it allows remote access to the virtualised environment via VPN (Virtual Private Network).

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 cyber game scenario. The system enables the reproduction multi team training scenarios with the highest level of automation and tracking support.

KEY BENEFITS

- Automatic generation and setup of training theatres and reusable scenarios.
- Improvement of defence and 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.
- Cooperative, **competitive and technology evaluation processes** based on the integration with external **virtual and physical environments.**
- Interoperability with remote orchestrators, scenarios and native capabilities to share cyber gaming fields and be federated with other **cyber ranges** services.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber and Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy
T. +39 010 658 7003 - Fax +39 010 10013290

MM08974 04-22

leonardo.com

LEONARDO