LEONARDO CYBER & SECURITY SOLUTIONS

CYBER RANGE

LEONARDO

Cyber Range

The definition and implementation of an optimal cyber security strategy for national ecosystems implies the development of defence capabilities, including training and exercising for security teams and technical staff working in both governmental and critical infrastructure sectors. Institutions and operators of national industries and utilities like telcos, transports, energy providers, defence, must have a deep awareness of the cyber risks that can damage their organizations and they must be able to test and implement promptly, effectively and in a cooperative way the actions needed to face them and minimize their impacts.

Training and testing in highly realistic situations are the two essential human driven processes that can effectively support the overall cyber “protection and response” cycle. The best cyber training and testing environments should theoretically be real production systems, but in practice, such systems cannot be exposed to dangerous situations because of the potential damaging and costly consequences that can be experienced. Advanced digital ecosystems for real-world infrastructure modelling can solve this issue by leveraging state-of-the-art cloud provisioning and virtualisation techniques. Such infrastructures make it possible to create realistic and immersive experiences in highly realistic scenarios, enabling learning, training and exercising for cyber security personnel, and supporting analysis and debriefing on hot cyber security issues.

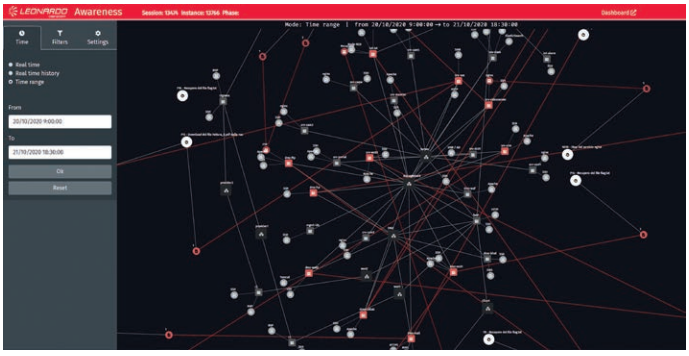
This is essential to ensure service continuity and operative resilience at desired levels. These environments offer the opportunity to conduct deep analysis and testing activities on new software and network components, organisational strategies and procedures to guarantee optimal protection and resilience against malicious cyber activities.

CYBER RANGE

Leonardo Cyber Range is a multi-purpose operational environment, that aims to create realistic operational training scenarios using the best-of-breed technologies for Infrastructure-as-Code (IaC) provisioning, cloud management and software defined networking. Its goal is to adequately train government agencies and critical infrastructures' cyber security teams to ensure they are able to face complex cyber threats and systemic attacks against information (IT) and operational (OT) technologies. It allows them 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 either delivered on premises, or provided in cloud as training-as-a-service. Additionally, in case of exercising and gaming over complex and wide theatres, it can be even accessed into dedicated tenants.

CYBER GAME PHASES

Theatre design – Using the Cyber Range, the creation of the digital twin of a target infrastructure starts from the design of the theatre, i.e. the set of systems, networks, applications combined with documents and any automatic attack/defence platforms. The theatre is built from a library of pre-constituted modules and represents an extremely customizable and reusable model on which multiple gaming scenarios can be built.
Scenario definition – A training 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. Depending on the available resources, hundreds of virtual machines can be allocated to simulate all the target systems - with their applications and network elements.
Gaming session – Once the scenario is deployed and the virtual machines are instantiated, the game session can start. During the practical training sessions, the trainees, generally divided into Red Teams (attackers) and Blue Teams (defenders), can practice cyber-attack and defence techniques over a partially known and dynamic theatre, exploiting the tools they are provided with (such as attack workstation with a collection of tools and defence workstation with SIEM, probes, monitoring tools, etc.).



Visual awareness module interface example

During cyber games, each team acts to achieve pre-assigned goals. To increase their score, participants are required to report their actions and to collaborate through open threat intelligence platforms and team messaging tools.
The Cyber Range provides the White Team (exercise supervisors and trainers) with aggregate visualizations of the attack and defence tactics performed by each team. These interfaces offer a comprehensive and easily interpretable viewpoint of the attack steps, defence actions and participants' behaviours. Finally, the platform also provides administrative/monitoring and reporting tools to support the scoring activities.
All these functionalities are supported by Leonardo skilled professionals who can manage all the complex processes involved in configuration of theatres, scenarios and attack tactics, techniques and procedures.
Evaluation & Debriefing – Automatic and semi-automatic evaluation tools allow participants' performance to be assessed as they progress towards the experiential activities. The Cyber Range supports in depth, ex-post analysis (that can be performed both individually or in team) of the exercise leveraging the tracking of all the actions carried out during the gaming session.

Attack / Defence execution platform interface example

LOGICAL MODEL AND TECHNOLOGIES

Leonardo Cyber Range capabilities are based on environments, applications, tools and connectors implemented on highly scalable and secure software defined architecture. In particular, the entire system in deployed on a software defined datacenter implementing the infrastructure upon which virtual machines and architectural modules (needed to execute the exercises) are instantiated.
The design, implementation and orchestration of the theatres, scenarios and gaming sessions are managed though different modules:

- **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.

- **Attack / Execution Defence Platform**: it provides definition, automatic deployment, configuration, scheduling, 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.
- **Visual Awareness Module**: it provides the portal enabling the White Team to visualize in real time the activities carried out by the teams involved in the exercise, and acquire indications, reports and data regarding their performance helping them in the scoring and evaluation process.
- **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 adoption of Infrastructure-as-Code standard languages, open source cloud management platforms, virtual overlay networking standards and virtual-to-physical gateways, guarantees the system's native interoperability.

CYBER TEST

Leveraging Cyber Range automatic generation and setup of complex theatres and scenarios capabilities, Leonardo Cyber Test is the platform supporting testing activities and vulnerability assessment on virtual twins of software components and network equipments. The system can be also used with external physical-logical real systems that can be integrated into testing scenarios. These activities can be performed either on existing systems (to test their vulnerabilities e.g. against the adoption of new technologies), or on systems under development supporting secure-by-design paradigm.

KEY BENEFITS

- Automatic generation and deployment of reusable and customizable training theatres and scenarios.
- Improvement of post-mortem analysis capabilities to identify main operational errors and best practices to be implemented during cyber defence.
- Provisioning of training sessions simulating complex cyber security incidents to ensure readiness against cyber-attacks.
- Realistic training ecosystem to exchange ideas, improve skills of cyber defence 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 & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM08974 07-23

leonardo.com

LEONARDO