LEONARDO CYBER & SECURITY SOLUTIONS

# CYBER TRAINER

LEONARDO

In recent years, there has been an extremely significant growth in cyber-attacks which became one of the most critical threats for companies and institutions.
Cyber-attacks determine the impairment of business continuity, the theft of intellectual property, the loss or dissemination of sensitive and financial data, money fraud, damage to corporate image and reputation, together with a heavy repercussion on the financial statements of the organizations that are victims.

Cyber threats are constantly evolving. They can originate from various sources, using multiples vectors and shaping into different forms. For these reasons, in the past few years the demand for Cyber Security experts has significantly increased, due as well to the growing digitalization and the consequent escalation of cybersecurity incidents.
This scenario entails the necessity of constantly updating the skills of operators, who are dedicated to the protection of IT infrastructures, as well as taking into account the continuous evolution of the legislation and the progress of ICT technology providing at the same time the opportunity to experiment, in situations as close to reality as possible, the most appropriate defence techniques.
Furthermore, considering that each infrastructure of security is as effective as its weakest link, attackers tend to exploit more and more frequently the human factor combined with technological vulnerabilities.
The effectiveness of the most sophisticated protection systems can be cancelled if the user, willingly or not, makes its credentials of access to the corporate infrastructures public.
Thereafter training became of vital importance. In order to reduce cyber threats exposure of institutions and companies, it is very important that every resource within the organization receive adequate behavioral training in order to minimize cyber risks.

## THE CYBER TRAINER

To meet these needs, Leonardo has developed the **Cyber Trainer**. A platform dedicated to cyber security and IT, designed with the purpose to train and keep up to date both security professionals and non-expert users.
The Cyber Trainer aims to support users throughout the whole training process: from the identification of training needs, to formal learning, from the practical application of acquired knowledge, to the certification of skills, offering social tools that allow each user to keep up to date on the topics of greatest interest in a continuous and autonomous way.

## THE PROPOSED APPROACH

To achieve these goals, the Cyber Trainer consists of the following modules:



LEARNING Module → TRAINING Module → SOCIAL Module

REPORTING Module
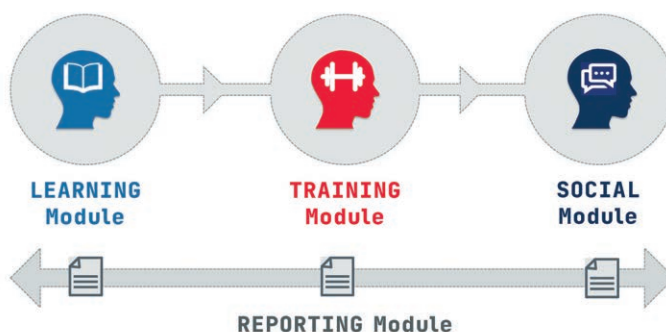
→ **Learning module:** it allows to take advantage of educational content, offering users the opportunity to monitor their progress in terms of skills acquired.

→ **Training module:** it allows to put into practice what has been learned in the Learning module throughout training sessions.

→ **Social module:** it supports the continuous training by sharing posts on topics of major interests in the general field of Cyber Security.

The platform organizes the training material based on a three level scheme:
1. Learning Path: an educational path organised in didactic modules.
2. Educational module: macro theme within the educational path that includes more learning contents.
3. Learning content: video, pdf, SCORM and linked content, Individual Virtual Lab.

A **Reporting module**, transversal to the other ones, allows teachers and students to keep track of their progress related to the learning activities. Each student can visualize its own state of progress in terms of path, completed modules and contents.

Furthermore, it helps to keep track of the Virtual Labs executed and of the badges acquired, to visualize the results of tests carried out and monitor the skills enhanced during the learning process. The teacher has the possibility to view the after mentioned information in an aggregate format by selecting the students of interest.

## THE LEARNING MODULE

Starting from a preliminary assessment, the **LEARNING** module offers synchronous and asynchronous learning functionalities and supports the evaluation of the results obtained by students.

The initial assessment aims to identify the training needs in order to: define different learning profiles, to associate said profiles to users and to create learning paths, organised in educational modules which includes frontal lectures delivered in a physical or virtual class.
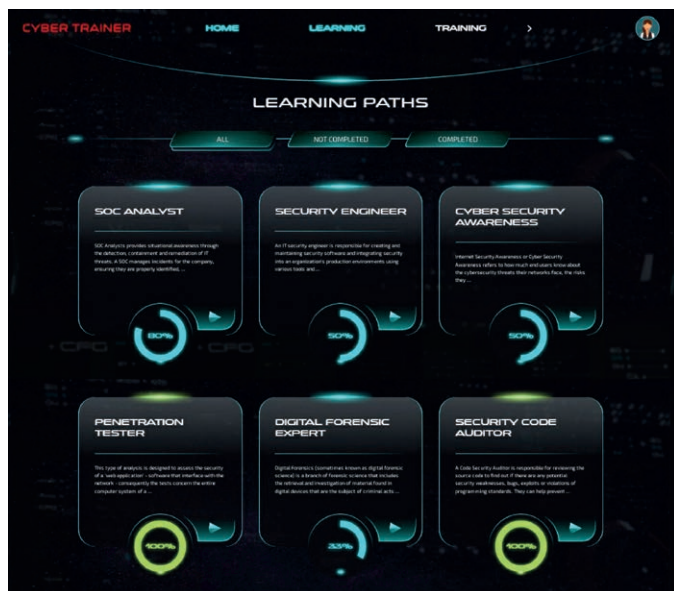


Learning module interface example

The different learning paths include:

→ Heterogeneous contents sorted by typology (such as pdf, video) and origin, including third parties' contents compatible with SCORM standard.

→ Individual Virtual Lab, which are individual exercise sessions aiming at experiential learning, enabled by the training module, in order to consolidate the acquired skills.

The assessment of the obtained results and the identification of new training needs take place through a process defined as **Continuous Assessment**, based on multiple choice tests and it is designed on the basis of specific needs of the Customer.
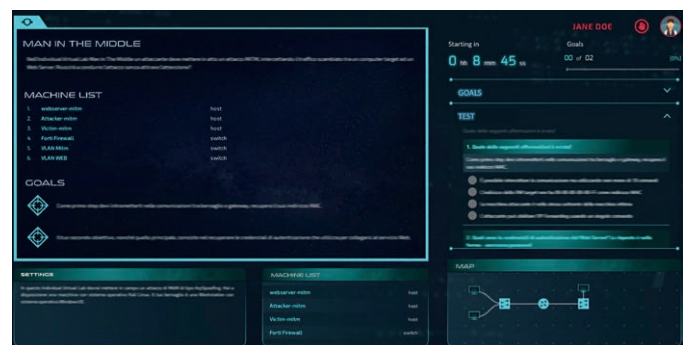
## TRAINING MODULE

The **TRAINING** module allows students to put into practice their own knowledge and skills acquired in the Learning Module by means of training sessions. These sessions, called Virtual Labs, not only allow to acquire or strengthen technical knowledge, but also allow to develop decision-making and diagnostic skills in an environment which is really close to real operational situations.

The **Virtual Labs**, supported by the platform, can be both individual (Individual Virtual Lab) or they can involve the participation of multiple users organised in groups (Red vs Blue Virtual Lab).

**Individual Virtual Labs** can be immediately enjoyed by the student, to whom specific roles and objectives are assigned.

**Virtual Labs Red vs Blue** foresee a challenge between teams: a defence team, the Blue Team, must defend the infrastructure from cyber threats generated by a team of attackers: the Red Team. The main purpose of these Labs is to train student by experiencing a simulated, yet realistic attack scenario, proposing situations that typically are faced by analysts in a Security Operation Center while defending their own infrastructure form external threats.

Virtual labs execution determines the issue of badges: certificates which allows to formalize the skills acquired by the student and that can be used to indicate the level of education reached. Badges include both Custom Badge, which can be neither exported nor recognised externally, and Open Badge standardized and exportable.



Training module interface example

## THE SOCIAL MODULE

The **SOCIAL** module offers to students the opportunity to share and visualize heterogeneous posts (sorted by origin and typology) on the main themes of interest in the field of Cyber Security and IT, in order to guarantee a continuous update on the most innovative discussion in these fields.

Furthermore, the social module offers the chance to participate to webinars taking advantage of links contained in particular posts issued by a class of "super editors" who always have the maximum visibility regardless the profile of interest of the user.

## SERVICE DELIVERY MODELS

The Cyber Trainer provides students with a Student Portal
to be accessed for the fruition of the learning contents.
The definition and organisation of contents which have to
be uploaded on the platform and the management of the
Administrator Portal, are managed by a dedicated Leonardo
staff once agreed Customer needs and related learning plan.

## KEY BENEFITS

→ Customer support from the identification of the training needs up to the
certification and updating of skills by means of a platform dedicated to
theoretical and experiential learning.

→ Access to training sessions in individual mode and in teams, which allow to
put into practice, in simulated but realistic operating contexts, the acquired
knowledge.

→ Platform with "gamified" interface designed to be attractive and easy to use by
both non-expert personnel in the field of information security and specialized
technical profiles already operating in the sector.

→ Social module for sharing information and news of interest on cybersecurity, to
allow a continuous update on the most current topics in the sector.

For more information please email: cyberandsecurity@leonardo.com

leonardo.com

## ⚹ LEONARDO