TRAINING IN CYBERSECURITY,

offered by IDELUX in partnership with Nexova

Nexova

IDELUX DÉVELOPPEMENT

IDELUX
CENTRE CYBERSÉCURITÉ IDELUX
P

AN IMMERSIVE AND PRACTICAL APPROACH TO STRENGTHEN YOUR CYBER RESILIENCE

IDELUX, in partnership with Nexova, offers an innovative and practical training course to raise awareness and provide training on cybersecurity. The Cybersecurity Centre, including a cyber range and a crisis simulator, created and operated by Nexova, can recreate the conditions of a cyber crisis to help organisations better understand the threat and their ability to respond to attacks.

The three training modules offered include practical exercises on the cyber range. It reproduces realistic virtual situations of IT/OT environments, which allows the participants to confront credible cyberattack scenarios, without compromising real infrastructures.

Each session can hold up to 20 participants. An official participation certificate is issued at the end of the training course.

In summary

Module 1 Introduction to cybersecurity	**Module 2** Cybersecurity training	**Module 3** Training the trainers
Basic training	Advanced training	Training future trainers and developers in cyber range scenarios
2 hours	6 hours	2 days
1 practical exercises on the cyber range	2 practical exercises on the cyber range	Practical work on the cyber range
Introduction to cybersecurity	General framework of cybersecurity	Introduction and approach of the training
Overview or current threats	The main counter measures and the response to an incident	High level architecture of the CITEF
Legislative framework	Best practices	Administration, organisation and digital library
Profile of attackers		Introduction to the development of scenarios
Attack methods		
Essential counter measures		

Module 1: Introduction to cybersecurity

Duration: 2 hours

Prerequisite: None

Module presentation

In a time where cyberthreats are more and more present, sophisticated and targeted, this awareness session aims to give participants a clear understanding of the issues linked to cybersecurity. It provides training in the essential reflexes to adopt on a daily basis to effectively contribute to the protection of the organisation and comply with current regulations.

A practical exercise in the cyber range reinforces learning through role play, based on an attack scenario.

Pedagogical objective

Allow each participant to:

- Understand the risks and issues relating to cybersecurity.
- Identify the early signs of an attack.
- Adopt the right behaviour to reinforce overall security of the organisation.

Programme

- Introduction to cybersecurity: key definitions, objectives and role in the protection of digital assets
- Overview of current threats: typology of cyberattacks, recent and practical examples
- The legislative framework: focus on the NIS2 European directive
- Profile of attackers (hackers, States, cybercriminals, insiders, etc.), motivations and operating methods
- Main types of attacks: phishing, ransomware, account compromise, supply chain attacks, etc.
- Essential counter measures: best security practices to apply in a professional environment, individual posture, collective vigilance

Module 2: Cybersecurity or operational cybersecurity training

Duration: 6 hours

Prerequisite: MS Windows user

Module presentation

This training course offers a profound exploration of cyber concepts and threats for participants to better manage risks and reinforce their cyber resilience. Through theoretical contributions and two role play situations in the cyber range, this training course helps participants to better understand the mediums of an attack and the detection methods.

The course emphasises the role of each employee in upholding cybersecurity and offers practical advice to identify risks, adopt the best practices and respond efficiently to an incident.

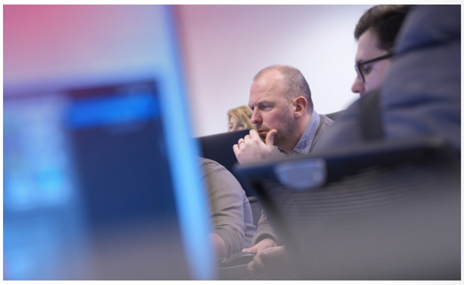
Pedagogical objective

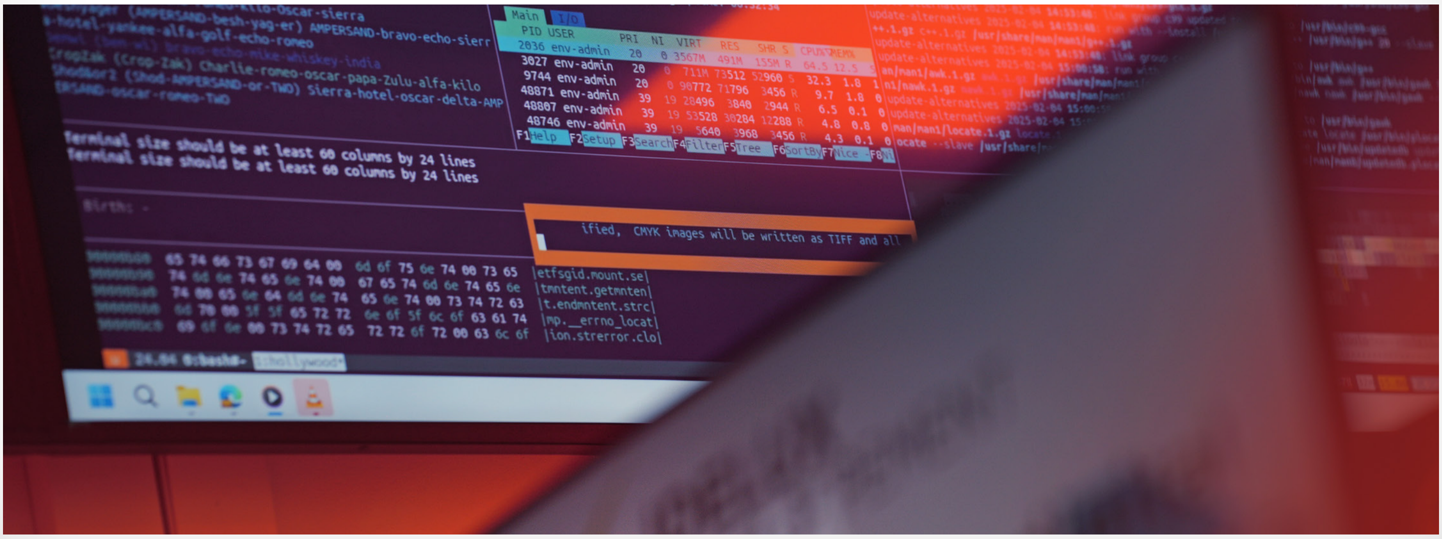
Allow each participant to:

- Understand the typology of modern attacks and their impacts.
- Identify the vulnerabilities exploited by the attackers.
- Be familiar with the methods of detection and response.

Programme

- Overview of the main threats and players in cyber risk
- Introduction to the regulatory framework
- Practical exercise 1 - Cyber range: targeted phishing scenario (30 min)
- The main counter measures and the response to an incident
- Practical exercise 2 - Cyber range: privilege escalation attack (30 min)
- The best security practices, individual posture and collective vigilance





```
-Kilo-Oscar-sierra
(AMPERSAND-besh-yag-er) AMPERSAND-bravo-echo-sierr
-hotel-yankee-alfa-golf-echo-romeo
bravo-echo-mike-whiskey-india
CropZak (Crop-Zak) Charlie-romeo-oscar-papa-Zulu-alfa-kilo
ShodWor2 (Shod-AMPERSAND-or-TWO) Sierra-hotel-oscar-delta-AMP
RSAND-oscar-romeo-TWO

Main  I/O
  PID USER       PRI  NI  VIRT   RES   SHR S  CPU% MEM%
 2036 env-admin   20   0 3567M  491M  155M R  64.5 12.5
 3027 env-admin   20   0  711M 73512 52960 S  32.3  1.8
 9744 env-admin   20   0 90772 71796  3456 R   9.7  1.8
48871 env-admin   39  19 28496  3840  2944 R   6.5  0.1
48807 env-admin   39  19 53528 30284 12288 R   4.8  0.8
48746 env-admin   39  19  5640  3968  3456 R   4.3  0.1
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Ni

Terminal size should be at least 60 columns by 24 lines
Terminal size should be at least 60 columns by 24 lines

Birth: -

      ified,  CMYK images will be written as TIFF and all

65 74 66 73 67 69 64 00  6d 6f 75 6e 74 00 73 65  |etfsgid.mount.se|
74 6d 6e 74 65 6e 74 00  67 65 74 6d 6e 74 65 6e  |tmntent.getmnten|
74 00 65 6e 64 6d 6e 74  65 6e 74 00 73 74 72 63  |t.endmntent.strc|
6d 70 00 5f 5f 65 72 72  6e 6f 5f 6c 6f 63 61 74  |mp.__errno_locat|
69 6f 6e 00 73 74 72 65  72 72 6f 72 00 63 6c 6f  |ion.strerror.clo|
```

Module 3: Training the trainers

Duration: 2 days

Prerequisite: The participants must:

- have a personal work station for practical sessions.
- be able to install software, including Visual Studio Code and MobaXterm on their device.
- have a good command of Unix/Windows systems.
- know how to debug logs and understand the basics of networks.

Module presentation

This training the trainers programme has been created to transfer the skills and knowledge required for the pedagogical use of the CITEF cyber range.

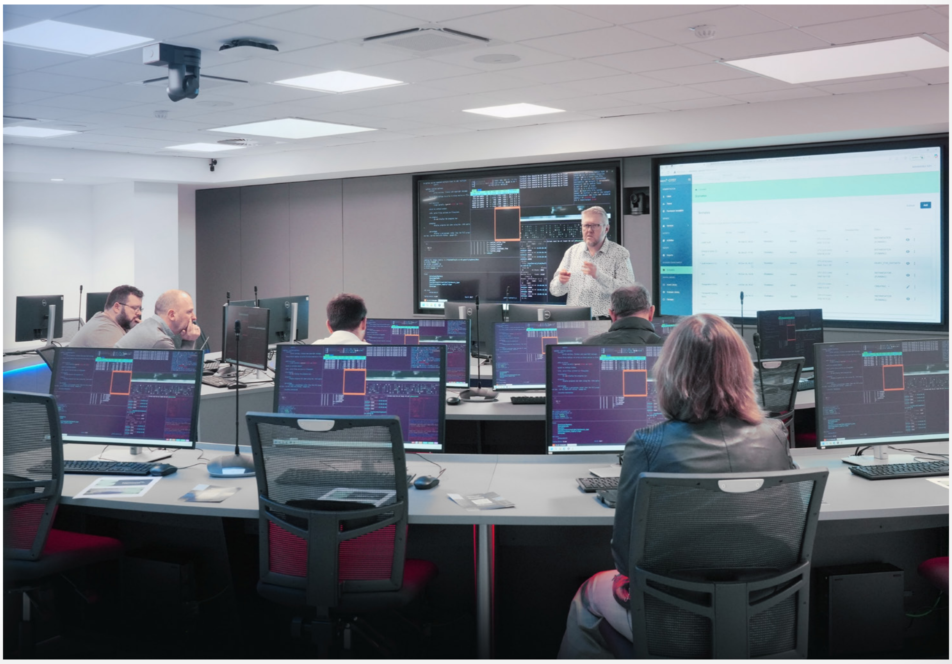
This training alternates between theory and role play to explore the architecture of the platform, its administration and the management of pedagogical contents. The participants will learn how to create, construct and deploy realistic cyber scenarios using tools such as Ansible and IaaS technologies. The training ends with a laboratory session where each participant will develop and execute their own scenario, ready to be used in future training sessions.

Pedagogical objective

Train future trainers and scenario developers on the professional use of the CITEF IDELUX platform.

Programme

- Introduction and methodology of the training
- High level architecture of the CITEF cyber range
- Administration, organisation and digital library
- Practical work: introduction to the development of scenarios



Contact

PIerre-Yves DEFOSSE
Business Developer

Tel. +32 476 34 93 40

@ pierre-yves.defosse@idelux.be

www.investinluxembourg.be

Address

IDELUX Cybersecurity Centre
Galaxia Business Park
Allée de la Comète 80
B-6890 Libin

Publisher in charge: Fabian COLLARD - Drève de l'Arc-en-Ciel, 98 - B - 6700 ARLON

Nexova

IDELUX DÉVELOPPEMENT

digital wallonia .be

Wallonie Relance

Avec le soutien de la Wallonie