FORMATIONS EN CYBERSÉCURITÉ,

proposées par IDELUX en partenariat avec Nexova

Nexova

IDELUX DÉVELOPPEMENT


IDELUX
CENTRE CYBERSÉCURITÉ
IDELUX
P

UNE APPROCHE IMMERSIVE ET PRATIQUE POUR RENFORCER VOTRE RÉSILIENCE CYBER

IDELUX, en partenariat avec Nexova, propose un parcours de formations innovant et concret pour sensibiliser et former à la cybersécurité. Le Centre de Cybersécurité comprenant un cyber range et un simulateur de crises, conçus et opérés par Nexova, permet de recréer les conditions d'une crise cyber pour aider les organisations à mieux appréhender la menace et leur capacité à répondre aux attaques.

Les trois modules de formation proposés intègrent des exercices pratiques sur le cyber range. Celui-ci reproduit des répliques virtuelles réalistes des environnements IT/OT, ce qui permet aux participants de se confronter à des scénarios de cyberattaques crédibles, sans compromettre les infrastructures réelles.

Chaque session peut accueillir jusqu'à 20 participants. Un certificat officiel de participation est délivré à l'issue de la formation.

En résumé

Module 1 Introduction à la cybersécurité	**Module 2** Formation à la cybersécurité	**Module 3** Formation des formateurs
Formation basique	Formation avancée	Formation des futurs formateurs et développeurs de scénarios sur cyber range
2 heures	6 heures	2 jours
1 exercice pratique sur cyber range	2 exercices pratiques sur cyber range	Travaux pratiques sur cyber range
Introduction à la cybersécurité	Le cadre général de la cybersécurité	Introduction et approche de la formation
Panorama des menaces actuelles	Les principales contre-mesures et la réponse à incident	Architecture de haut niveau du CITEF
Le cadre législatif	Les bonnes pratiques	Administration, organisation et bibliothèque numérique
Profils des attaquants		Introduction au développement de scénarios
Modèles d'attaque		
Les contre-mesures essentielles		

Module 1 : Introduction à la cybersécurité

Durée : 2 heures

Prérequis : Aucun

Présentation du module

Dans un contexte où les cybermenaces sont de plus en plus nombreuses, sophistiquées et ciblées, cette session de sensibilisation a pour objectif de donner aux participants une compréhension claire des enjeux liés à la cybersécurité. Elle permet d'acquérir les réflexes essentiels à adopter au quotidien pour contribuer efficacement à la protection de l'organisation et de se conformer aux règlementations en vigueur.

Un exercice pratique sur le cyber range, basé sur un scénario d'attaque, vient renforcer l'apprentissage par la mise en situation.

Objectif pédagogique

Permettre à chaque participant de :

- Comprendre les risques et les enjeux de la cybersécurité ;
- Identifier les signaux faibles d'une attaque ;
- Adopter les bons comportements pour renforcer la sécurité globale de l'organisation.

Programme

- Introduction à la cybersécurité : définitions clés, objectifs et rôle dans la protection des actifs numériques
- Panorama des menaces actuelles : typologies des cyberattaques, exemples concrets et récents
- Le cadre législatif : focus sur la directive européenne NIS2
- Profils types des attaquants (hackers, États, cybercriminels, insiders...), motivations et modes opératoires
- Principaux modèles d'attaques : phishing, rançongiciels, compromission de compte, attaques sur la chaîne d'approvisionnement, etc.
- Les contre-mesures essentielles : bonnes pratiques de sécurité à appliquer dans un environnement professionnel, posture individuelle, vigilance collective

Module 2 : Formation à la cybersécurité ou Cybersécurité opérationnelle

Durée : 6 heures

Prérequis : Utilisateur de MS Windows

Présentation du module

Cette formation offre une exploration approfondie des concepts et des menaces cyber pour permettre aux participants de mieux gérer les risques et de renforcer leur résilience cyber. À travers des apports théoriques et deux mises en situation sur cyber range, cette formation permet aux participants de mieux comprendre les vecteurs d'attaque et les méthodes de détection.

La formation met l'accent sur le rôle de chaque employé dans le maintien de la cybersécurité et offre des conseils pratiques pour identifier les risques, adopter les bons réflexes et réagir efficacement face à un incident.

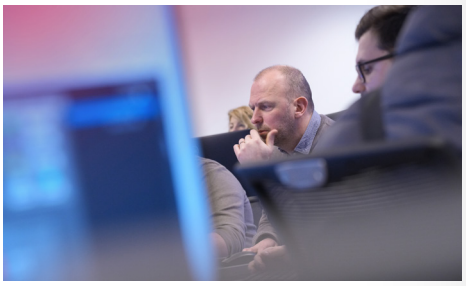
Objectif pédagogique

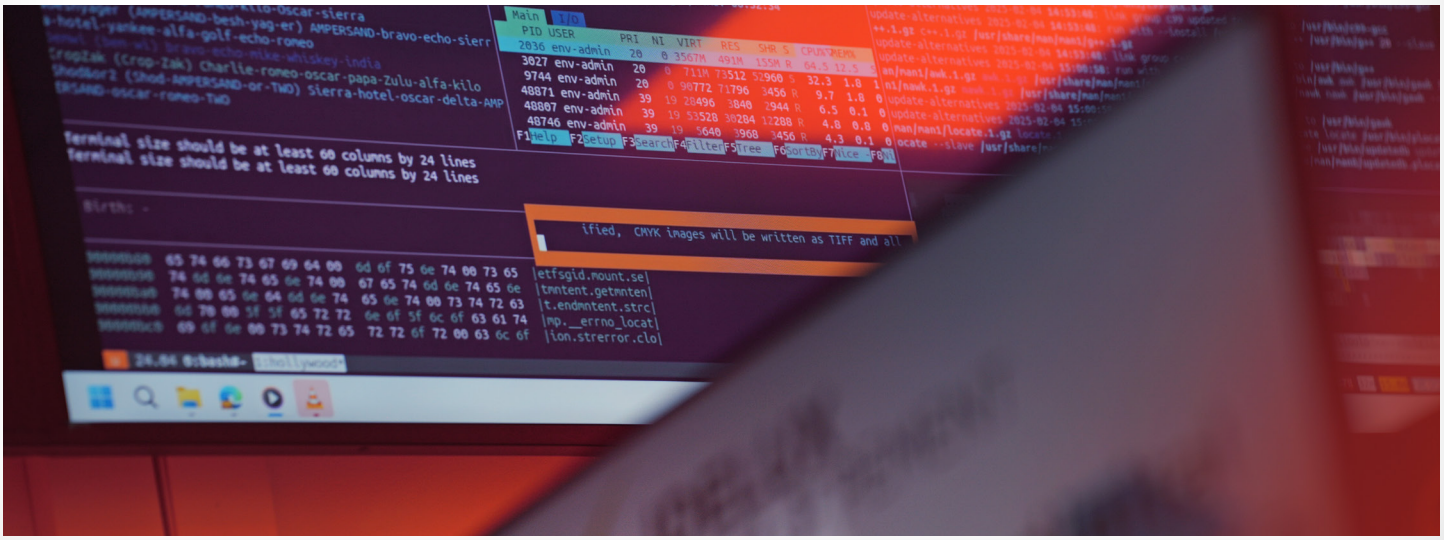
Permettre à chaque participant de :

- Comprendre les typologies d'attaques modernes et leurs impacts ;
- Identifier les vulnérabilités exploitées par les attaquants ;
- Se familiariser avec les méthodes de détection et de réponse.

Programme

- Panorama des principales menaces et acteurs du risque cyber
- Introduction au cadre réglementaire
- Exercice pratique #1 – Cyber range : scénario de phishing ciblé (30 min)
- Les principales contre-mesures et la réponse à incident
- Exercice pratique #2 – Cyber range : attaque de type « élévation de privilèges » (30 min)
- Les bonnes pratiques de sécurité, posture individuelle et vigilance collective





Module 3 : Formation des formateurs

Durée : 2 jours

Prérequis : Les participants doivent :

- disposer d'un poste de travail personnel pour les travaux pratiques ;
- pouvoir installer des logiciels, y compris Visual Studio Code et MobaXterm sur leur appareil ;
- avoir une bonne maîtrise des systèmes Unix/Windows ;
- savoir déboguer des logs et comprendre les bases des réseaux.

Présentation du module

Ce programme de formation des formateurs est conçu pour transmettre les compétences et connaissances nécessaires à l'utilisation pédagogique de la plateforme de cyber range CITEF.

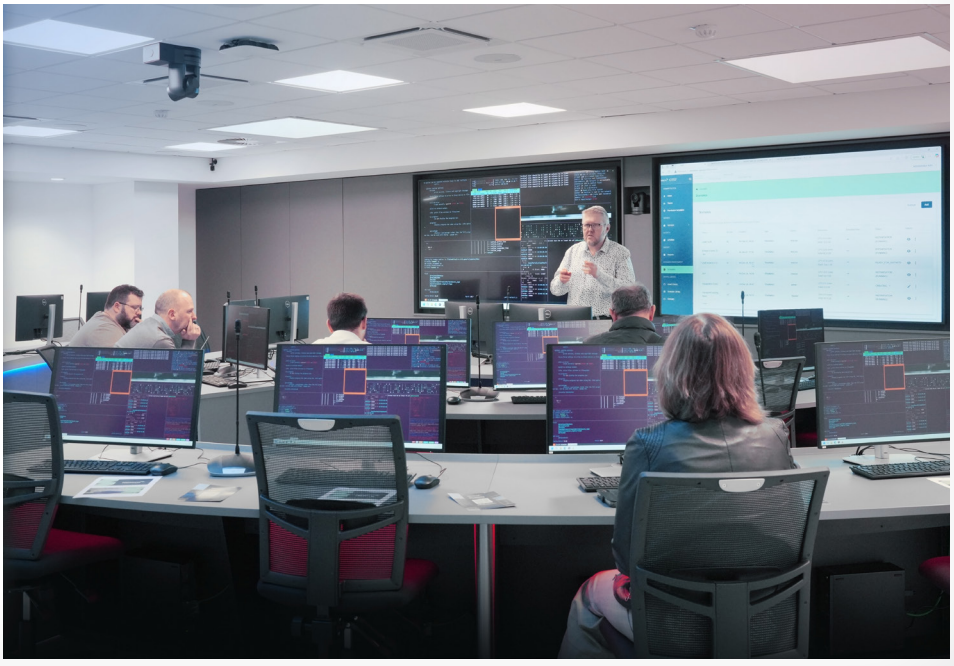
Cette formation alterne théorie et mise en pratique pour explorer l'architecture de la plateforme, son administration et la gestion des contenus pédagogiques. Les participants apprendront à concevoir, construire et déployer des scénarios cyber réalistes à l'aide d'outils tels qu'Ansible et les technologies IaaS. La formation se termine par un laboratoire où chaque participant développe et exécute son propre scénario, prêt à être utilisé lors de futures sessions de formation.

Objectif pédagogique

Former les futurs formateurs et développeurs de scénarios à l'utilisation professionnelle de la plateforme CITEF IDELUX.

Programme

- Introduction et méthodologie de formation
- Architecture de haut niveau du cyber range CITEF
- Administration, organisation et bibliothèque numérique
- Travaux pratiques : introduction au développement de scénarios



Contact

Pierre-Yves DEFOSSE
Business Developer

Tel. +32 476 34 93 40

pierre-yves.defosse@idelux.be

www.investinluxembourg.be

Adresse

Centre de Cybersécurité IDELUX
Parc d'activités Galaxia
Allée de la Comète 80
B-6890 Libin

Éditeur responsable : 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