

# Certified Lead Ethical Hacker (formation et examen de certification)



## Objectifs

La formation Certified Lead Ethical Hacker vous permettra d'acquérir l'expertise nécessaire pour maîtriser le hacking éthique. Le cours fournit des informations sur les dernières méthodes de piratage éthique et outils. Il fournit également une méthodologie pour effectuer des tests d'intrusion conformément aux normes et aux meilleures pratiques. Le cours est basé sur le concept de mise en pratique de ce que vous avez appris. Il comprend le laboratoire des séances et des exemples pratiques pour vous aider à mettre la théorie en pratique. La formation se conclut par un examen donnant lieu à une certification Lead Ethical Hacker.

## A qui s'adresse ce cours

Ce stage s'adresse aux professionnels informatiques et aux personnes en charge de la cybersécurité et qui cherchent à maîtriser les techniques de piratage éthique et de test d'intrusion.

## Cours de 5 jours – 2 950 € HT

<u>Paris</u>	<u>Lyon</u>
28 fév. 2022	28 fév. 2022
25 avril	27 juin
27 juin	
28 nov.	

### Intra entreprise

Sur demande

\*Examen de certification inclus

Formation à distance possible (hors examen)



Certification enregistrée RS3716  
<https://www.francecompetences.fr>

## Pour vous inscrire

Téléphone : 01 40 33 76 88

E-mail : [contact@beresilientgroup.com](mailto:contact@beresilientgroup.com)

### Courrier

BRG – 10, rue Emile Landrin – 75020 Paris

Centre de formation agréé préfecture : 11754161975

SAS au Capital de 150 000 Euros - Siret Paris B 441 951 845

## Contenu du module 921

### Jour 1 Introduction au piratage éthique

- Objectifs et structure de la formation
- Normes, méthodologies et cadres réglementaires relatifs aux tests d'intrusion
- Présentation du laboratoire
- Concepts fondamentaux du piratage éthique
- Concepts fondamentaux des réseaux
- Comprendre le chiffrement
- Tendances et technologies pertinentes
- Principes fondamentaux de Kali Linux
- Lancement du test d'intrusion
- Analyse du périmètre du test d'intrusion
- Implications juridiques et accord contractuel

### Jour 2 Lancement de la phase reconnaissance

- Reconnaissance passive
- Reconnaissance active
- Identification des vulnérabilités

### Jour 3 Lancement de la phase exploitation

- Modèle de menace et plan d'attaque
- Eviter les systèmes de détection d'intrusion
- Attaque côté serveur
- Attaque côté client
- Attaques des applications web
- Attaques Wi-Fi
- Escalades des privilèges
- Pivotement
- Transfert de fichier
- Maintien des accès

### Jour 4 Post-exploitation et rapports

- Nettoyage et destruction des artefacts
- Atténuation des vulnérabilités identifiées
- Génération d'un rapport de conclusions
- Clôture de la formation

### Jour 5 Examen de certification

# Certified Lead Ethical Hacker (formation et examen de certification)

## Prérequis

Le candidat doit avoir des connaissances fondamentales de la sécurité de l'information, il doit posséder de solides compétences sur les systèmes d'exploitations (Microsoft, Linux). La certification est accessible aux personnes disposant d'au moins cinq années d'expérience

## Modalités et délais d'accès

1. Contacter nous par mail ou téléphone pour qualifier votre besoin de formation
  2. Renvoyez le bon de réservation complété (disponible à la fin du catalogue)
  2. Validation de votre inscription (éligibilité du stagiaire)
  3. Etablissement et signature de la convention de formation
  4. Envoi de votre convocation à la session de formation avec les détails (horaires, lieu...)
- Durée estimée entre la demande du bénéficiaire et le début de la prestation: de 1 à 3 mois

## Méthodes mobilisées

Cours magistral basé sur les meilleures pratiques liées à la mise en œuvre de tests d'intrusion  
Exercices pratiques panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.  
Support de cours au format papier et numérique, version française

## Modalités d'évaluation – Validation des compétences - Certification

Examen de certification 3 heures - Organisme certificateur PECB

Evaluation de la totalité des cinq compétences constitutives de la certification :

- Simuler l'attaque d'un système d'information d'entreprise par un utilisateur malintentionné ou un logiciel malveillant, afin de détecter les fragilités de celui-ci.
- Concevoir et mettre en œuvre une série de tests d'intrusion à même de situer le degré de risque représenté par chacune des fragilités identifiées.
- Rédiger un rapport de pentest présentant l'ensemble des vulnérabilités exploitables dans les configurations ou la programmation, en vue de la conception par les responsables d'un plan d'amélioration de la sécurité du système d'information cohérent avec l'échelle des risques.
- Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
- Conseiller une entreprise sur les bonnes pratiques en matière de détection et de lutte contre le piratage, afin de faciliter la mise en place des mesures et procédures adéquates.

## Equivalences, passerelles, suite de parcours et débouchés

Pas de certification partielle – Remise d'un certificat de compétences PECB valable 3 ans

La certification permet aux individus de disposer des compétences nécessaires à la conception et à la mise en œuvre de tests d'intrusion sur différents types de systèmes d'information. Répondre aux exigences de postes correspondants à ces caractéristiques : RSSI, chefs de projet/consultant en sécurité des systèmes d'information. La certification permet aux entités utilisatrices de faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue. Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs. Garantir aux parties prenantes de l'organisation un certain standard de qualité. Le maintien dans le temps de la certification garantit la transférabilité des compétences d'une entité utilisatrice à une autre. Suite de parcours: ISO 27001 Lead Implementer/Auditor, Cyber-résilience

## Accessibilité aux personnes handicapées

Procédure Accueil Handicap: En cas d'accueil d'un stagiaire handicapé, l'office manager de BRG est le référent handicap, qui pourra si besoin mobiliser notre réseau de partenaires du champ du handicap.

Accessibilité aux personnes à mobilité réduite: Nos locaux sont Etablissement Recevant du Public (ERP)

Attestation de vérification de l'accessibilité aux personnes handicapées – Dossier accessibilité

