

AUDITEUR EN CYBERSÉCURITÉ



Devenez auditeur en cybersécurité :
développez les compétences techniques
essentielles pour la protection
des infrastructures informatiques

AUDITEUR EN CYBERSÉCURITÉ

Le volume et l'impact des cyberattaques sont en constante augmentation partout dans le monde. Ceci est lié aux changements des systèmes d'Informations (SI), à la digitalisation de nombreuses activités et aux nouvelles modalités d'organisation du travail définies par les entreprises tel que le télétravail.

Ces cyberattaques affectent directement ou indirectement les particuliers, les administrations et les entreprises.

La cyber sécurité est ainsi un marché en pénurie de talents, où ces derniers et leurs compétences techniques sont très sollicités par les recruteurs. En tension, à la recherche de talents aux compétences techniques pointues reconnues.

OBJECTIFS DE LA FORMATION

- Maîtriser les fondamentaux de la cybersécurité, l'ensemble des technologies les plus populaires et les plus utilisées, protéger des infrastructures informatiques et remédier à leurs éventuelles vulnérabilités.

PROGRAMME

a) Modules en cyber sécurité

- Module 1 : Welcome to the cyber world
- Module 2 : Networking : les systèmes réseaux
- Module 3 : Reconnaissance
- Module 4 : Let's dive into web penetration
- Module 5 : Exploitation des vulnérabilités
- Module 6 : Windows exploitation : active directory
- Module 7 : Post exploitation
- Module 8 : Wireless
- Module 9 : Red team
- Module 10 : Coaching carrière
- Module 11 : Demoday

b) Modules assuranciers

Module 1 : Protection de la clientèle et conformité en assurance

- Protection de la clientèle
- DDA : maîtriser les impacts pour les différents acteurs de l'assurance
- Devoir d'information et de conseil dans la cadre de la DDA
- Contrôle des pratiques commerciales en assurance
- RGPD appliqué à l'assurance
- Ethique, déontologie et anticorruption
- Rôle et fonctionnement de l'ACPR

Module 2 : Management des risques

- Transformation digitale et assurance
- Big data et assurance
- Objets connectés et assurance
- Environnement juridique du risque cyber
- Les nouveaux risques
- Le risque cyber et entreprise
- Management des risques industriels et commerciaux
- Le financement du risque
- Cartographie et gestion des risques
- Solvabilité 2 : Maîtrise des risques et des processus
- Identifier et connaître les cyber-risques et les solutions d'assurance
- Audit sécurité et cartographie des risques opérationnels
- Sensibilisation des équipes au risque cyber
- Elaborer un plan de continuité d'activité en cas d'attaque informatique
- Gérer une crise cyber

c) Anglais TOIEC

- Module 1 : Anglais professionnel
- Module 2 : Préparation au TOIEC
-

DURÉE DE LA FORMATION

- 900 heures sur 24 mois

BLOCS DE COMPÉTENCES

- Pilotage des projets cybersécurité
- Gestion des réseaux et systèmes informatiques
- Analyse des vulnérabilités et contrôles techniques
- Conception des mesures de défense cybersécurité

PUBLIC

- Cette formation est destinée à des diplômés scientifiques ou techniques, ayant ou non une expérience professionnelle, désirant acquérir des compétences en cybersécurité.

MÉTIER VISÉS

- Auditeur en cybersécurité
- Analyste en cybersécurité
- Opérateur, analyste SOC
- IT Security specialist

PRÉREQUIS

- Être titulaire d'un diplôme bac +3 dans un domaine scientifique et/ou économique. À l'international, un niveau équivalent est requis (ce niveau sera justifié par le CV de l'apprenant).
- Ou expérience professionnelle équivalente.
- Les compétences de base en cybersécurité.

CONDITIONS D'ADMISSION

- La réussite d'un test d'admission "coding challenge", validant les compétences nécessaires scientifiques en mathématiques appliquées.
- La réussite d'un entretien préalable qui jugera : De la plus-value de l'acquisition des compétences décrites dans le référentiel « Auditeur en cyber sécurité
-

MODALITÉS PÉDAGOGIQUES

- La réalisation de projets est au cœur de la pédagogie, elle s'accompagne d'une excellence théorique pour comprendre l'environnement global de la cybersécurité.
- La formation est en format hybride en distanciel et en présentiel.
- Il est mis à disposition des apprenants une plateforme d'apprentissage de la tech avec des cours en ligne et d'autres ressources facilitant l'acquisition des compétences visées

MODALITÉS D'ÉVALUATION

- Les candidats sont évalués par des tests et des mises en situation professionnelle permettant l'Elaboration d'un plan d'Audit cybersécurité, la Conception d'architectures sécurisées, la résolution d'un « Test d'intrusion » et l'établissement d'un Rapport d'audit expliquant la reproductibilité de la CVE.

TARIFS

- **Formation en alternance** : les frais de formation sont pris en charge par l'entreprise.

LIEUX DE FORMATION

Puteaux, Bordeaux, Lyon, Marseille, Niort, Strasbourg et à distance /Campus JEDHA Paris



AU PLUS PRÈS DE VOUS

proche Paris...

CFA DE L'ASSURANCE > 01 47 76 58 52
172-174 rue de la République - 92800 Puteaux
informations@ifpass.fr



Nos formations sont accessibles aux candidats en situation de handicap :
L'IFPASS met en place des aménagements techniques ainsi qu'un accompagnement humain
adapté en fonction du besoin du candidat.