Hackers Are Here. Where Are You?...

ECIH – EC-Council Certified Incident Handler

DESCRIPTION DU COURS

Le programme EC-Council Certified Incident Handler-ECIH est conçu pour donner aux stagiaires les compétences fondamentales leur permettant de manipuler et répondre aux incidents de sécurité informatique dans un système d'information. Le cours couvre différents principes et techniques sous-jacentes pour détecter et répondre aux menaces de sécurité actuelles et émergentes. Les participants vont apprendre comment agir face aux différents types d'incidents, les méthodologies d'évaluation des risques et différentes lois et réglementations liées aux traitements des incidents. De plus, les candidats en sauront davantage sur le forensic informatique et son rôle dans la gestion et la réponse aux incidents. Ce cours recouvre également les équipes de réponse aux incidents, les méthodes de rapports d'incidents et les techniques de reprise d'activité en détails.

A l'issue de ce cours, les stagiaires seront capables de créer des politiques de gestion et de réponse aux incidents et seront compétents pour faire face aux différents types d'incidents de sécurité informatique tels que les incidents sur la sécurité du réseau, incidents par codes malveillants et menaces d'attaques internes.

PLAN DE FORMATION

1. Introduction à la réponse aux incidents et à leur gestion
2. Évaluation des risques
3. Étapes de réponses et de gestion des incidents
4. CSIRT
5. Gérer les incidents de sécurité du réseau
6. Gérer les incidents par codes malveillants
7. Gérer les menaces internes
8. Analyse forensique et réponse aux incidents
9. Rapports d'incidents
10. Reprise après incident
11. Lois et réglementations de sécurité

DUREE

3 jours (9h00 – 17h00)

PROFIL DES STAGIAIRES

Ce cours sera particulièrement bénéfique aux gestionnaires d'incidents, administrateurs d'évaluation des risques, pen-testeurs, cyber-enquêteurs judiciaires, consultants en évaluation de vulnérabilité, administrateurs de systèmes, ingénieurs de systèmes, administrateurs de pare-feu, responsables de réseaux, responsables IT, professionnels IT et toutes les personnes intéressées par la gestion et la réponse aux incidents.

CERTIFICATION

L'examen ECIH 212-89 pourra se dérouler le dernier jour de formation. Les étudiants devront réussir l'examen sur la plateforme ECC Exam pour obtenir leur certification.

Titre de l'examen : EC-Council Certified Incident Handler
Code de l'examen : ECIH 212-89
Nombre de questions : 50 QCM
Score requis : 70%
Durée : 2 heures
Disponibilité : ECC exam

EC-Council

i.t. Gnosis