ADVANCIA TRAINING

EC-Council Incident Handling

Réf. ECIH · EC-Council · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	**Avancé**	**Présentiel · Live · Intra**	**Inclus**

Présentation

EC-Council Certified Incident Handler (ECIH) fournit une approche structurée et normalisée de la gestion des incidents de sécurité. Destinée aux professionnels de la réponse à incident, elle couvre l'ensemble du processus IH&R, du traitement des malwares aux incidents cloud, email et applicatifs.

Objectifs pédagogiques

- Maîtriser le processus de gestion et de réponse aux incidents (IH&R)
- Détecter, trier et prioriser les incidents de sécurité
- Contenir, éradiquer et remédier aux différents types d'incidents
- Traiter les incidents liés aux malwares, au réseau et aux applications web
- Gérer les incidents cloud, email et de menace interne
- Intégrer le forensic et les aspects juridiques à la réponse

Programme détaillé

1. Module 1 — Introduction à la réponse à incident

- Concepts de gestion des incidents
- Vulnérabilités, menaces et attaques
- Cadre et processus IH&R
- Rôles, équipes et conformité

2. Module 2 — Préparation et première réponse

- Préparation à la réponse
- Détection et signalement des incidents
- Triage et confinement initial
- Forensic et collecte de preuves

3. Module 3 — Incidents malwares et réseau

- Traitement des incidents liés aux malwares
- Analyse et éradication
- Réponse aux incidents réseau
- Détection des attaques réseau

4. Module 4 — Applications web et cloud

- Réponse aux incidents d'applications web
- Réponse aux incidents cloud
- Environnements virtualisés
- Bonnes pratiques de remédiation

5. Module 5 — Email et menaces internes

- Incidents de sécurité email
- Menaces internes (insider threats)
- Détection comportementale
- Réponse ciblée

6. Module 6 — Remédiation et amélioration continue

- Éradication et récupération
- Analyse post-incident et leçons apprises
- Reporting et communication
- Amélioration du plan de réponse

Prérequis

Une expérience en administration systèmes/réseaux ou en sécurité, ainsi que des connaissances en gestion des vulnérabilités, sont recommandées.

Public visé

Membres d'équipes CSIRT/CERT, analystes SOC, ingénieurs sécurité, administrateurs, responsables de la réponse à incident et auditeurs.

Ce qui est inclus

- Courseware officiel EC-Council ECIH
- Labs de gestion d'incidents
- Voucher d'examen ECIH inclus
- Attestation de réussite
- Pauses-café, déjeuner et formateur expert en réponse à incident

Certification

Certification ECIH (examen 212-89) : QCM de 100 questions à passer en 3 heures. Advancia Training est centre d'examen agréé Pearson VUE / PSI.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible