EduGroupe
Accompagner pour réussir

Certified Incident Responder (Certification comprise)

Référence : **SECCIR** Durée : **5 jours (35 heures)** Certification : **PECB Certified Incident Responder**

Connaissances préalables

- Avoir une une compréhension fondamentale des principes de la cybersécurité
- Avoir les connaissances de base de la réponse aux incidents
- Avoir des connaissances de base en langue anglaise car le support de cours et l'examen sont en langue anglaise

Profil des stagiaires

- Les membres de l'équipe de réponse aux incidents et les analystes en cybersécurité chargés de la gestion des événements de sécurité
- Les professionnels de la sécurité informatique qui cherchent à améliorer leurs compétences techniques et stratégiques en matière de réponse aux incidents
- Les membres du centre des opérations de sécurité (SOC) impliqué dans la détection et la réponse aux menaces
- Les professionnels souhaitant se spécialiser dans les rôles d'intervention en cas d'incident
- Les responsables et les chefs d'équipe chargés de coordonner les stratégies et les protocoles de réponse aux incidents

Objectifs

- Élaborer et mettre en œuvre des stratégies efficaces de réponse aux incidents et gérer les efforts de réponse au sein des équipes et des technologies
- Évaluer les vecteurs d'attaque des ransomwares et les techniques d'atténuation, et mettre en œuvre un plan de réponse robuste afin de minimiser leur impact
- Analyser les comportements des logiciels malveillants, créer des stratégies de remédiation sur mesure et utiliser des techniques d'analyse forensique pour retracer et neutraliser les codes malveillants
- Identifier les menaces externes ciblant les périmètres du réseau et y répondre, et mettre en œuvre des outils et des techniques de détection et de confinement précoces des menaces
- Élaborer des plans de remédiation pour éliminer les menaces récurrentes et identifier les stratégies de persistance avancées

Certification préparée

L'examen « PECB Certified Incident Responder » répond aux exigences du programme d'examen et de certification PECB (ECP).

Pour plus d'informations sur le type d'examen, les langues disponibles et autres détails, veuillez consulter la liste des examens PECB et le règlement des examens.

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

Formateur

- Consultant-formateur expert en Cybersécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. JOUR 1

- Principes fondamentaux de la réponse aux incidents et de la gestion stratégique

2. JOUR 2

- Réponse aux incidents liés aux ransomwares et aux logiciels malveillants

3. JOUR 3

- Détection, analyse et réponse aux menaces périmétriques

4. JOUR 4

- Réponse aux incidents par le biais de mécanismes persistants, d'analyses médico-légales et d'amélioration continue

5. JOUR 5

- Matin : Révision en autonomie. Les moyens pédagogiques nécessaires (support de cours, salles de formations) seront à votre disposition
- Après-midi : Passage de l'examen couvre les domaines de compétences suivants :
- Domaine 1 : Principes fondamentaux de la réponse aux incidents et de la gestion stratégique
- Domaine 2 : Réponse aux incidents liés aux ransomwares
- Domaine 3 : Réponse aux incidents liés aux logiciels malveillants
- Domaine 4 : Détection et réponse aux menaces périmétriques
- Domaine 5 : Réponse aux incidents liés aux mécanismes persistants

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.