Programme de formation SECUAUDIT

Audit de vulnérabilités et plan de remédiation

Formation axée sur la détection des failles de sécurité (scan réseau, failles applicatives, mauvaises configurations) et sur la création d'un plan d'action priorisé.

Modalité

Formation Ouverte À Distance avec accompagnement par un expert

Durée totale

7 heures (1 jours)

Tarif

500.00€ TTC / pers.

Modalités Pédagogiques

- Méthodes : Expositive, démonstrative et active
- Moyens : Cas pratique, mise en situation
- Ressources : Support de cours et Programme de formation
- Moyens techniques : Teams

Modalités d'assistance technique

L'apprenant est accompagné via une assistance technique disponible par e-mail ou téléphone.
La plateforme utilisée pour le e-learning est Moodle.
En cas de problèmes techniques, le contact référent est : EHRHART Christel - christel@ce-formation.com - 07.68.48.96.63

Prérequis

Connaissances solides des OS, des réseaux et de la cybersécurité

Public cible

Responsables sécurité, RSSI, administrateurs confirmés

Délai et Modalités d'accès

Délai d'accès 15 jours après la signature du contrat. Dates à convenir entre le client et l'organisme de formation.

Objectifs

À l'issue de la formation, le stagiaire doit être capable de maîtriser les compétences suivantes :

- Comprendre les étapes d'un audit technique et analyser une vulnérabilité publique
- Être capable de conduire un scan de sécurité et en tirer une analyse priorisée
- Structurer et planifier efficacement des actions correctives à la suite d'un audit

Déroulé du parcours de formation

Introduction à l'audit de sécurité et au cycle de remédiation

- Définitions : vulnérabilité, menace, risque, exploitabilité
- Typologie des audits : interne, externe, boîte noire, grise, blanche
- Méthodologie d'audit technique : identification, analyse, évaluation, remédiation
- Introduction aux référentiels : CVE, CVSS, OWASP Top 10

Réalisation d'un scan de vulnérabilités (interne/externe)

- Présentation d'outils : OpenVAS, Nessus, Lynis, Nikto
- Préparation de l'environnement : scan ciblé, plage IP, périmètre autorisé
- Analyse des résultats : failles détectées, niveaux de criticité
- Détection de services non sécurisés, ports exposés, patchs manquants

Élaboration d'un plan de remédiation

- Traduction des résultats en actions correctives
- Priorisation : criticité, faisabilité, dépendances
- Suivi des actions : tableau de bord, jalons, responsables
- Exemples de mesures correctives (MAJ, désactivation, segmentation, chiffrement)

Évaluations formatives

Le suivi de la progression pédagogique est assuré par des quiz de validation des connaissances à la fin des modules et des exercices d'application pratiques (mises en situation).

Modalités d'évaluation

Le formateur évalue la progression en cours de formation à l'aide de cas pratiques, mises en situation, QCM…
Un test de positionnement sera complété en amont et en aval afin de valider les compétences acquises.

Formateurs

Tous les formateurs de CE FORMATION sont des professionnels en activité, à leur compte ou salarié, ils conservent ainsi "les mains dans le cambouis".
Ils ont chacun leur spécialité, mais également une vision globale du métier et sont dotés d'un niveau BAC+3 ou supérieur.
Ils sont tous également formateurs dans d'autres centres de formation, depuis au minimum 2 ans, et sont connus et respectés pour leur engagement, leur pédagogie et leur humilité face au métier et à sa constante évolution.

Contacts

CE FORMATION
07.68.48.96.63
contact@ce-formation.com
CE FORMATION

Accessibilité aux PSH

Cette formation est accessible aux personnes en situation de handicap.
Si la situation nécessite des aménagements spécifiques, le candidat peut contacter notre référent handicap :

Christel EHRHART
07.68.48.96.63
christel@ce-formation.com

Indicateurs

Taux de satisfaction : *En cours*

Taux d'accomplissement : *En cours*