Auditer des systèmes sécurisés via une méthodologie offensive Pentest

Soft Skills
Autonomie/ rigueur/ esprit analytique

Profil
Une appétence pour la cybersécurité et une capacite à résoudre des problèmes complexes.

OBJECTIFS / CONTEXTE

Acquérir une expertise en cybersécurité : Développer les compétences nécessaires pour identifier, analyser, et répondre efficacement aux cybermenaces afin de garantir la sécurité des systèmes d'information.

Renforcer la résilience des entreprises : Mettre en œuvre des stratégies de protection et de réaction face aux incidents de cybersécurité, contribuant à la pérennisation des infrastructures numériques.

Se conformer aux exigences légales et réglementaires : Assurer la conformité des entreprises aux cadres juridiques et réglementaires en matière de protection des données personnelles et de cybersécurité.

Cette formation répond aux enjeux actuels auxquels les entreprises doivent faire face, comme la hausse des cyberattaques, se conformer aux réglementations (RGPD), garantir leur résilience face aux crises numériques.

PROGRAMME

En 5 modules pour un parcours complet

1/Identifier et évaluer les risques en cybersécurité
Maîtriser l'évaluation et la gestion des risques en cybersécurité

2/Mettre en œuvre des solutions de sécurisation des systèmes et des connexions
Savoir protéger les systèmes et les données contre les menaces potentielles

3/Configurer et administrer des environnements techniques
Être capable de gérer et de sécuriser les infrastructures

4/Détecter et répondre aux cyberattaques
Savoir identifier, analyser et répondre efficacement aux incidents de sécurité

5/Maîtriser la cryptographie pour protéger les données
Savoir utiliser la cryptographie pour garantir la confidentialité et l'intégrité des données

FINANCEMENT : autofinancement, contactez-nous, nous vous aiderons dans vos démarches

Délai d'accès : 4 semaines (selon le nombre de stagiaires)

Prérequis : aucun

Public : administrateur sécurité / RSSI / gérant de PME-TPE / pentester

Niveau d'expérience : avoir une expérience dans la sécurité informatique d'au moins 1 an

Durée : 3 mois

Modalités d'organisation : en distanciel

Méthodes mobilisées :
Blended learning - Cours sur une plateforme dédiée
Accompagnement individuel par un formateur en visioconférence
Exercices et quiz en ligne - Évaluations pour chaque module - Correction des exercices et évaluations avec le formateur dédié

TARIF : 3 499 €

Modalités d'évaluation :

Une évaluation en fin de chaque module : étude de cas ou mise en situation avec restitution à l'oral

Un examen final : étude de cas sur une machine virtuelle avec rédaction d'un rapport de pentest

Selon la pondération suivante : analyse de l'incident 30 %
: stratégie de pentest 40 %
: rapport 30 %

En cas d'échec : un second passage sera prévu dans les 6 mois au plus tard.

MAJ : 09-24