Cybersécurité en FAD

Mise à jour : juin 2023

Public

- Demandeurs d'emploi

Prérequis & conditions d'admission

Niveau :

- Être titulaire d'un diplôme ou d'un Titre RNCP de niveau 6 (Bac+3) ou justifier d'une expérience professionnelle de 3 ans minimum dans le domaine du titre visé
- Bonne connaissance de la programmation

Profil :

- Projet professionnel validé dans le domaine de la cybersécurité
- Connaissances générales en maintenance, support, système, réseau
- Notions en sécurité informatique souhaitées
- Être naturellement à l'écoute des autres
- Avoir bon relationnel
- Aimer être tenu informé des nouveautés

Condition d'admission & délais d'accès :

- Validation des prérequis
- Entretien de motivation
- En moyenne entre notre premier contact et votre entrée en formation il se passe 1 mois

Modalités

- Formation continue

Financements

- Région Occitanie

Objectifs

- Concevoir et piloter en mode Agile un projet de sécurisation du système d'information dans l'environnement économique et stratégique propre au client
- Maîtriser l'architecture des systèmes d'information
- Gérer la qualité et la sécurité dans un projet de système d'information
- Mettre en place des exercices de pentesting en entreprise
- Faire face aux principaux problèmes liés à la sécurité dans un réseau informatique, sur un poste de travail ou dans une application et maîtriser des solutions existantes et leurs coûts
- Intervenir, conseiller et dialoguer avec l'ensemble des acteurs du projet
- Rédiger des documents exhaustifs adaptés à différents niveaux de compétences

S'assurer de l'atteinte des objectifs

Débouchés

- Consultant Cybersécurité
- Responsable du SOC
- Analyste Cybersécurité
- Chef de projet Cybersécurité
- Pentester
- Hacker éthique

Programme

Accueil, Onboarding et découverte métier

Accompagnement à la Formation à Distance, savoir chercher sur internet et organiser sa veille

Développement durable

> Le green IT
> La green data
> La fresque du climat

Techniques de recherche d'emploi

> Identifier les enjeux d'une offre d'emploi
> Adapter son CV
> Consolider sa lettre de motivation
> Préparer son pitch
> Mettre en valeur ses réalisations et ses compétences
> Préparer l'entretien d'embauche

- Animer sa page LinkedIn

Citoyenneté, diversité et inclusion

- Les impacts de la data sur la société
- L'égalité Femmes / Hommes
- La diversité dans les métiers tech

Organisation du travail en équipe et soft-skills de groupe

- Travailler en équipe
- S'organiser en équipe
- Communiquer en équipe
- Le souci du travail d'équipe de qualité

Soft-skills individuels

- La communication orale
- L'adaptation aux changements
- L'organisation individuelle (planifier, gérer son temps, ...)
- L'autonomie
- Le souci du travail individuel de qualité

La planification des projets

- Les fondamentaux en gestion de projets
- La planification des projets
- MS Project
- Les fondamentaux de DevOps

Méthodes Agiles

- Définir et identifier les rôles et les responsabilités des acteurs
- Identifier les étapes de SCRUM
- Conduire un projet en appliquant la méthode agile SCRUM
- Maitriser l'aspect technique et fonctionnel DevOps
- Appliquer et mettre en place des méthodes de travail pour Les tests – La livraison – La qualité du code et Le débogage

La Blockchain comme solution de tiers de confiance

- Comprendre la technologie blockchain et les Smart Contract
- Comprendre l'écosystème autour de cette technologie
- Aborder un projet blockchain avec toutes les clés de compréhension
- La cryptographie
- Développer un projet Smart Contract avec les bons réflexes
- Assurer la sécurité d'un projet Smart Contract

Les outils d'audit

- Introduction à l'audit, et plus spécifiquement à l'audit des SI
- Gestion du risque et de la sécurité
- Organisation et management de l'audit : ISO19011
- La méthode COBIT

Sécurité Informatique

- Les fondamentaux de la cybersécurité et de la sécurité informatique
- La cryptographie, l'authentification, les clés et le chiffrement
- La cyberdéfense : les vulnérabilités et les techniques d'attaques
- Déploiement, administration et sécurisation des ressources matérielles et logicielles.
- Mettre en place des techniques afin de sécuriser les applications
- Analyse de la vulnérabilité d'un système d'exploitation
- Mise en place de système de prévention d'intrusions
- Système de détection des attaques et intrusions
- La mise en place d'une stratégie de sécurité
- La maintenance préventive

Les approches Red, Blue et Purple Teaming et les outils Red Teaming

- Mesurer les impacts des menaces de sécurité sur une organisation
- Comprendre les modes opératoires suivis
- Utiliser des Framework de modélisation des différentes tactiques, techniques et procédures d'attaque
- Maitriser la méthodologie, les objectifs et priorités d'un exercice Red Team
- Développer une méthodologie adéquate à l'organisation concernée en se basant sur de la méthodologie Red Team
- Identifier les faiblesses et vulnérabilités de l'organisation dans laquelle se déroule l'exercice Red Team.
- Evaluer les solutions de sécurité mise en place dans un organisation (SIEM, EDR et Anti-Virus) à travers l'application des techniques de furtivités
- Durcir les postures défensives de l'organisation à partir des vulnérabilités et faiblesses remontées
- Formaliser des rapports et des présentations de synthèse d'exercice Red Team
- Mettre en place un plan de communication et d'amélioration de la sécurité de l'organisation entre les équipes Red et Blue Team.

Projet personnel

Travail personnel

Stage en entreprise

Préparation a la présentation du Dossier – Mémoire, révisions et valorisation des acquis

> Accompagnement à la rédaction des 5 fiches du Dossier – Mémoire
> Valorisation des projets réalisés
> Actualisation des outils de recherche d'emploi (linkedin, CV, ...)

Epreuves

> Passage devant un jury de 3 personnes autour d'une mise en situation professionnelle autour d'un cahier des charges issu de données d'entreprises

Bilan

Durée

- Durée totale de la formation : 1070 heures dont 560 heures de formation + 210 heures de travail personnel + 300 heures de stage en entreprise

Modalités d'évaluation

Formation sanctionnée par le passage du bloc de compétence Cybersécurité du titre Développeur Full Stack BIG DATA de niveau 7 délivré par Cegefos et comportant 6 blocs de compétences.

Titre de **Développeur Full Stack BIG DATA**

Titre de **niveau 7**, inscrit au RNCP (RNCP 32123), délivré par un jury de professionnels.

Modalités d'évaluation pour chaque bloc

Evaluation par un jury (formation en alternance et continue) :

- Mise en situation professionnelle ou présentation d'un projet réalisé en amont de la session, éventuellement complétée par d'autres modalités d'évaluation : entretien technique, questionnaire professionnel, questionnement à partir de production(s)
- Jury composé de 3 professionnels :
- 1 président du jury, le directeur de l'école
- 1 représentant des employeurs ; formateur
- 1 représentant des salariés ; salarié

Compétences évaluées

Bloc 7 – Sécurité Informatique

RNCP3123BC07

Compétences évaluées :

- La maîtrise des textes de loi et des procédures liés à la sécurité informatique
- L'utilisation de l'authentification, du chiffrement et des clés pour sécuriser les bases de données et les applications
- La maîtrise des normes de sécurité d'un réseau et la mise en place des outils de sécurité réseau
- Le développement des modules spécifiques afin de sécuriser par le code les applications pour lutter contre les attaques
- L'optimisation du code pour contrer les fraudes, les attaques de piratages
- Etudier es différents types de solutions pour contrecarrer les différentes menaces

Méthodes et Moyens pédagogiques

Modalités de formations possibles

Présentiel	E-learning	Classe virtuelle	Blended-Learning
En continu	En alternance	Formation collective	Formation individuelle

Moyens pédagogiques

- Présentiel :
  - Salle de formation équipée : Paper-Board, Télé connectée
  - Un ordinateur par apprenant avec connexion internet
- E-learning :
  - Accès plateforme LMS
- Classe virtuelle :
  - Compte sur un outil de visio
- Supports de cours et d'exercices
- Équipe pédagogique composée de professionnels métier

Méthodes et techniques pédagogiques

- Présentiel :
  - Apports théoriques en salle
  - Mises en situation pratiques en plateau technique
  - Jeux de rôles et cas pratiques
  - Exercices individuels et en sous-groupes
  - Application réelle lors des périodes de stage

- Distanciel :
  - Autoformation accompagnée
  - Etudes de cas corrigées
  - Exercices / quiz à la fin de chaque cours
  - Forum d'échanges
  - Cours en live possibles
  - Suivi personnalisé

Accessibilité aux personnes en situation de handicap

Vous êtes en situation de handicap ?
Nous pouvons mettre en place des adaptations pour vous permettre de suivre la formation.
Rendez-vous sur notre page dédiée pour plus d'informations : **https://unlearn-school.fr/informations-pratiques/**