Ingénieur cybersécurité, Bootcamp (6 mois) (Titre RNCP)

by DataScientest

Formation pratique - 32j - 224h00 - Réf. 3CU

Prix : 11990 € H.T.

NEW

Devenez expert en cybersécurité afin de protéger et sécuriser les infrastructures et les données. Un ingénieur en cybersécurité est un spécialiste jouant un rôle vital dans la protection des infrastructures et des données sensibles des entreprises contre les cyberattaques. Cette formation certifiante se déroule à distance dans un format hybride mêlant temps d'échanges synchrones avec un formateur expert, exercices pratiques et modules E-learning. Basée sur la pédagogie Learning By Doing, vous réaliserez un projet fil rouge en équipe afin de mettre en pratique vos connaissances. Lors de votre inscription, vous serez rattaché à l'une des promotions Datascientest. A l'issue de cette formation, vous obtiendrez un certificat « Gestionnaire de la sécurité des données, des réseaux et des systèmes » certification RNCP de niveau 7 délivrée par HEXAGONE et enregistrée au RNCP sous le n°RNCP37796. Contactez-nous dès maintenant pour connaître les prochaines dates !

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Formuler et formaliser la politique de la sécurité des systèmes d'information d'une organisation
- Mettre en place les outils techniques nécessaires à la sécurisation du système d'information
- Suivre l'évolution du niveau de sécurité d'un système d'information d'une organisation
- Organiser une réponse adaptée en cas de crise

Public concerné

Toutes les personnes ayant une appétence pour la cybersécurité souhaitant se reconvertir ou faire évoluer ses compétences.

Prérequis

Un diplôme ou un titre de niveau bac+3 dans le domaine de l'informatique.

PARTICIPANTS

Toutes les personnes ayant une appétence pour la cybersécurité souhaitant se reconvertir ou faire évoluer ses compétences.

PRÉREQUIS

Un diplôme ou un titre de niveau bac+3 dans le domaine de l'informatique.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Certification

Pour clôturer la formation, l'équipe pédagogique évaluera le projet fil rouge de l'apprenant à l'aide d'un rapport écrit et d'une soutenance à distance. La validation des compétences développées au cours de la formation Ingénieur cybersécurité vous permettra d'obtenir : Un certificat « Gestionnaire de la sécurité des données, des réseaux et des systèmes » certification RNCP de niveau 7 délivrée par HEXAGONE et enregistrée au RNCP sous le n°RNCP37796.

Méthodes et moyens pédagogiques

Activités digitales

Cours et exercices en ligne, masterclass collective, séances de questions/réponses, classes de soutien, accompagnement par mail, projet fil rouge, coaching carrière individualisé, social learning.

Tutorat

Un formateur expert accompagne l'apprenant tout au long de sa formation. Il échange régulièrement avec lui sur son projet fil rouge et l'accompagne lors de points de mentorat (individuel). Plusieurs formateurs animent également les différentes masterclass (classes collectives) et répondent aux questions des apprenants à tout moment depuis un forum dédié. En complément, de nombreuses séances de questions-réponses peuvent être organisées pour aider les apprenants.

Pédagogie et pratique

Lors de l'inscription, l'apprenant est affecté à une promotion (dates à définir lors de l'inscription) et reçoit son calendrier de formation. Le parcours de formation est découpé en « Sprint » de plusieurs semaines sur une thématique dédiée. Chaque semaine l'apprenant est convié à un temps d'échange avec le formateur qui se présente sous la forme de masterclass (classe collective) ou de points de mentorat (individuel). Pendant 80% du temps, l'apprenant travaille en autonomie sur la plateforme d'enseignement. Tous les modules intègrent des exercices pratiques permettant de mettre en œuvre les concepts développés en cours. L'apprenant doit également travailler en binôme ou trinôme sur un projet fil rouge tout au long de la formation. Cela lui permettra de développer et faire reconnaître ses compétences. En complément, des événements et ateliers thématiques sont régulièrement proposés pour permettre aux apprenants de découvrir les dernières innovations en matière de cybersécurité. Afin de suivre efficacement la formation, nous estimons le temps travail nécessaire entre 30 et 35 heures par semaine.

Programme de la formation

1 Prochaines dates de session

- Avril 2026 : Début au 07/03/26
- Juin 2026 : Début au 02/06/2026
- Septembre 2026 : Début au 08/09/2026

2 Fondamentaux des systèmes et réseaux

- Les bases du réseau.
- Administration Windows et Linux & scripting

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

3 Les fondamentaux de la cybersécurité et du SOC

- Introduction à la cybersécurité et aux menaces
- Cadre juridique et fonctionnement d'un SOC

4 Sécurité des réseaux

- Sécurité des réseaux et protection des infrastructures
- Architecture réseau sécurisée et Zero Trust

5 Cryptographie & Durcissement des systèmes

- Cryptographie et IGC.
- VPN et durcissement des systèmes

6 SIEM Splunk

- Introduction Splunk.
- Analyse, requêtes SPL et visualisation

7 SIEM Splunk avancé

- Requêtes avancées et exploitation des données
- Reporting avancé et visualisation

8 Ethical Hacking

- Méthodologie des tests d'intrusion et reconnaissance
- Exploitation des failles et reporting

9 APT & Mitre ATT&CK

- Analyse de cyberattaques avancées et groupes APT
- MITRE ATT&CK et adversary emulation

10 Détection d'intrusion

- Détection des intrusions et analyse des événements
- Cyber Threat Intelligence et qualification des incidents
- Préparation et gestion de Cybercrise

11 Forensique et réponses aux incidents

- Réponse aux incidents et investigation numérique
- Computer Forensics et gestion de cybercrises

12 Sécurité du cloud et le métier de consultant

- Fondamentaux du cloud et sécurité associée
- Posture, compétences et pratiques du consultant cybersécurité

13 Les indicateurs et suivi de projet

- Rôle de l'auditeur et conduite de l'audit
- Pilotage du SMSI et indicateurs de sécurité

14 L'implémentation des normes liées à la SSI

- Gouvernance, Risques et Conformité (GRC)
- Mise en œuvre des référentiels et du SMSI

15 Les analyses de risque

- Fondements de la gestion des risques
- Méthode d'analyse des risques et mise en pratique

16 Gestion des incidents et gestion de crise cyber

- Préparation et réponse aux incidents de sécurité
- Gestion de crise cyber et continuité d'activité