PROGRAMME DE FORMATION

Formation à la cybersécurité - 30h de cours particuliers en ligne - Tout niveau

OBJECTIFS DE LA FORMATION :

Le stagiaire souhaitant développer ses compétences sur la cybersécurité , l'objectif est de lui permettre d'acquérir les savoirs suivants :

- Introduction à la cybersécurité.
- Les fondamentaux de la cybersécurité.
- Les outils et les techniques de cybersécurité.
- La sécurité des réseaux.
- La gestion des identités et des accès.
- La sécurité des données.

PUBLIC :

Formation tout public, tous métiers.

PRÉREQUIS :

- Maîtrise de la navigation et recherche sur les sites web.
- Maîtrise de la messagerie électronique.
- Équipement technique adapté : ligne téléphonique fixe, ordinateur (PC ou MAC) doté d'une carte son, d'une connexion Internet et d'une caméra ou webcam.

MODALITÉS DE SUIVI ET D'ÉVALUATION :

Le séquençage de la formation diffère en fonction du niveau initial de l'apprenant et du nombre d'heures de la formation.
Les contenus sont également orientés en fonction des objectifs professionnels du stagiaire.

Formation en ligne composée d'une partie en cours individuels et d'une autre basée sur des supports fournis au stagiaire.
Une fois votre inscription réalisée, votre formateur vous contactera dans les 15 jours précédant la date de début de votre formation, date à laquelle le test de niveau d'entrée en formation vous sera transmis..

Des évaluations sont réalisées au cours de votre formation, elles permettront à votre formateur d'adapter les cours et exercices à votre profil. Le professeur vous guide et vous assignera des exercices tout au long de votre période de formation.

DATES :

Les dates de formation sont renseignées dans le corps de l'email de convocation.

HORAIRES :

E-learning : Les supports e-learning sont accessibles 7j/7 et 24h/24.

Assistance pédagogique : Disponible du lundi au vendredi de 10h à 18h au 01 84 60 51 77.

RÉFÉRENTS PÉDAGOGIQUE ET FORMATEURS :

Chaque formation est sous la responsabilité du directeur pédagogique de l'organisme de formation. Le bon déroulement est assuré par les formateurs désignés par l'organisme de formation.
Tous nos formateurs sont sélectionnés pour leur excellence et leurs méthodes pédagogiques.

Les personnes chargées d'assister le bénéficiaire de la formation sont sous la supervision de Christophe Sorel, titulaire d'un Master 2 Entrepreneuriat, Directeur des consultants pédagogiques dédiés aux parcours de formation au sein de Clic Compétences.

DURÉE :

La durée minimale de l'action de formation est renseignée en page 1 au début du programme.

Elle comprend :

- Des cours particuliers (cours par visioconférence).
- Un parcours e-learning pendant 12 mois.

L'accès au parcours e-learning est transmis une fois les cours particuliers totalement réalisés.

LIEU :

Formation ouverte à distance réalisée par visioconférence ou en présentiel dans les locaux de l'entreprise ou dans un espace dédié.
Pour les personnes en situation de handicap, nous mettrons tout en œuvre pour vous accueillir ou pour vous réorienter. Vous pouvez nous contacter au 01 84 60 51 77.

COACHING ET ACCOMPAGNEMENT :

Le stagiaire dispose à tout moment d'un coach pour l'accompagner, tout au long de sa formation :

Tout au long de la formation, le coach dispense des conseils pédagogiques au stagiaire et se tient au courant de sa progression par téléphone, e-mail ou SMS.

Le stagiaire dispose à tout moment d'une hotline téléphonique au 01 84 60 51 77 pour toute question, problème technique ou conseils, il peut également programmer un rendez-vous via notre calendrier de réservation disponible sur www.clic-competences.fr/rdv, ou réaliser une demande d'assistance par email à cpf@clic-competences.fr.

Une fois le test de positionnement validé par le stagiaire au début de sa formation, il peut solliciter son coach pour avoir une démonstration de prise en main par téléphone. Cette démonstration a pour but de le familiariser avec notre outil d'apprentissage et de lui donner des conseils pédagogiques.

A la fin de la formation, le coach fait un bilan pédagogique avec le stagiaire sur ses connexions et progrès réalisés. Nos coachs ont reçu une formation initiale dispensée par le responsable pédagogique. Chaque coach est formé régulièrement sur les nouveautés et mises à jour de l'offre de formation.

Délai de réponse : une assistance sera apportée au stagiaire dans un délai maximum de 48 heures jours ouvrés après l'envoi d'un e-mail à l'adresse suivante : cpf@clic-compétences.fr.
Notre hotline téléphonique est disponible du lundi au vendredi de 10h à 18h.

COURS PARTICULIERS EN LIGNE :

❖ **Introduction à la cybersécurité :**

- Les enjeux de la cybersécurité pour les entreprises et les particuliers.
- Les menaces et les risques liés à la sécurité informatique, tels que les attaques par force brute, les exploits, les virus, les chevaux de Troie, les rootkits, les ransomwares, etc.
- Les types de cyberattaques les plus courants et leurs conséquences, avec les attaques de phishing, les attaques par déni de service distribué (DDoS) et les attaques de l'homme du milieu (MitM).

❖ **Les Fondamentaux de la cybersécurité :**

- Les principes de base de la sécurité informatique comme l'authentification, l'autorisation, la confidentialité, l'intégrité et la disponibilité (AICID).
- Les méthodes de cryptage et de déchiffrement, tels que les algorithmes de chiffrement symétrique et asymétrique, les fonctions de hachage, etc.
- Les protocoles de sécurité courants, tels que SSL/TLS, VPN, IPsec, SSH, etc. Les techniques de gestion des identités et des accès, tels que l'annuaire LDAP, la fédération d'identités, etc.

❖ **Les outils et les techniques de cybersécurité :**

- Les outils de protection contre les malwares et les virus, avec les antivirus, les anti-malwares et les pare-feu.
- Les techniques de prévention de l'usurpation d'identité, ainsi que l'authentification multifactorielle, la biométrie, etc.
- Les outils de surveillance et de détection d'intrusions, tels que les sondes de détection d'intrusion (IDS), les systèmes de détection et de prévention d'intrusion (IDPS).
- Les méthodes d'analyse de vulnérabilité : les scanners de vulnérabilités, les audits de sécurité, les tests de pénétration, etc.

❖ **La sécurité des réseaux :**

- Les architectures et les technologies de réseau sécurisées, comme les réseaux privés virtuels (VPN), les réseaux définis par logiciel (SDN), les réseaux de confiance zéro, etc.
- Les méthodes de configuration de pare-feu et de filtrage de paquets : les règles de pare-feu, les politiques de sécurité.
- Les techniques de protection des réseaux sans fil, équivalentes aux protocoles WPA2, WPA3 et les cloisonnements de réseau.
- Les mesures de prévention des attaques par déni de service, avec les systèmes de prévention de déni de service (DPS), les filtres anti-DDoS, etc.

❖ **La gestion des identités et des accès :**

- Les méthodes de gestion des identités et des accès, telles que la gestion des comptes utilisateurs, la gestion des privilèges et la gestion des rôles.
- Les protocoles d'authentification : Kerberos, SAML, OAuth, etc.
- Les techniques d'attaque sur les identités et les accès, de la même nature que les attaques par détournement de session, les attaques de type «homme du milieu», les attaques par force brute, etc.

❖ **La sécurité des données :**

- Les techniques de cryptage des données, et le chiffrement symétrique et asymétrique, la gestion des clés, etc.
- Les mesures de protection contre les fuites de données, telles que la classification des données, la protection contre les pertes de données et la protection des données en transit.
- La vulnérabilité des données, et les différents types d'attaques comme les fuites de données, les attaques de type « phishing », les attaques par déni de service distribué, etc.

Le support de formation sera remis au stagiaire en fin de formation.

E-LEARNING FACULTATIF :

Un support de cours (plateforme e-learning) facultatif sera proposé à l'apprenant pour lui permettre de travailler en autonomie sur des manipulations de tout niveau. Les accès à la plateforme e-learning sont transmis à la fin de la formation une fois que toutes les heures de cours sont réalisées. Les différents thèmes abordés sont listés ci-dessous :

- **Cybersécurité (sécurité sur internet) 1- module tout niveau :**

- Un monde numérique hyper connecté.
- Un monde à hauts risques.
- Les acteurs de la cybersécurité.
- Protéger le cyberespace.
- Mon rôle dans la sécurité numérique.

- **Cybersécurité (sécurité de l'authentification) 2- module tout niveau :**

- Principes de l'authentification.
- Attaques sur les mots de passe.
- Sécuriser ses mots de passe.
- Gérer ses mots de passe.
- Notions de cryptographie

- **Cybersécurité (sécurité sur internet) 3- module tout niveau :**

- Internet : de quoi s'agit-il ?
- Les fichiers en provenance d'internet.
- La navigation web.
- La messagerie.
- L'envers du décor d'une connexion internet.

- **Cybersécurité (sécurité du poste de travail) 3- module tout niveau :**

- Applications et mises à jour.
- Options de configuration de base.
- Configurations supplémentaires
- Sécurité des périphériques amovibles
- Séparations des usages.

RESSOURCES PÉDAGOGIQUES :

Il est conseillé au stagiaire de fournir un travail personnel régulier entre les séances de formation.
Le stagiaire dispose de ressources pédagogiques, documents et exercices fournis par le formateur.

À la fin de chaque cours téléphonique, le professeur indiquera les tâches à effectuer par le stagiaire, au travers de liens postés sur l'espace cours du stagiaire.

Au début de chaque cours, le professeur vérifie avec le stagiaire que ces tâches ont bien été effectuées.

ENCADREMENT :

Les professeurs qui dispensent les cours par téléphone sont des professionnels confirmés dans la formation à but professionnel pour un public d'adultes.

Tous nos formateurs comptabilisent au moins 2 ans d'expérience en milieu professionnel et sont diplômés.
Ils ont été individuellement sélectionnés pour leur qualité de pédagogue et font l'objet d'une évaluation permanente.

CALENDRIER DES COURS :

Les professeurs contacteront les élèves afin de connaître leurs créneaux et réserver avec eux les plages de cours. En cas d'annulation, le professeur devra être prévenu en amont selon ses modalités.

Le stagiaire organise son travail en ligne en fonction de ses besoins, mais également en fonction des impératifs et créneaux de connexion imposés par son employeur.

SUIVI ET ÉVALUATION DE TRAVAUX ACCOMPLIS PAR LE STAGIAIRE :

La première session de formation fait l'objet d'un test initial de niveau. Puis, les connaissances du stagiaire sont contrôlées grâce à des tests qui jalonnent la formation de l'apprenant tout au long de son processus d'apprentissage (contrôle continu). Ces tests ont lieu à la fin de chaque session.

Le niveau du stagiaire ainsi que ses progrès et son niveau d'assiduité sont ainsi réévalués lors de chaque session.

Ces données sont accessibles, à tout moment, au stagiaire comme au formateur et au coach qui suivent le stagiaire. Ils permettent d'apprécier le niveau obtenu par le stagiaire en comparaison avec son niveau initial.

Les ressources étudiées lors des sessions de travail sont enregistrées et consultables par le stagiaire et le formateur, et ce via des interfaces spécifiques. Les données relatives à ces sessions (durée de connexion, résultats) sont mises à jour quotidiennement.
Ces données sont exportables.

SUIVI DE L'EXÉCUTION :

- Attestation d'assiduité mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation.
- Relevé des connexions, signé par un représentant de l'organisme de formation indiquant :
- La date de l'action et les heures de début et de fin d'utilisation du programme.
- La dénomination du ou des modules suivis.
- Attestation de réalisation des unités, signée par un représentant de l'organisme de formation, détaillant les travaux finalisés en cohérence avec le programme de formation.

APPRÉCIATION DES RÉSULTATS EN FIN DE FORMATION :

- Recueil individuel des attentes du stagiaire.
- Questionnaire d'auto-évaluation des acquis en début et en fin de formation.
- Évaluation continue durant la session.
- Remise d'une attestation de fin de formation.
- Questionnaire d'évaluation de la satisfaction en fin de formation.