Identifier les métiers, rôles et trajectoires en cybersécurité

Décrypter l'écosystème et sélectionner les opportunités clés en cybersécurité

DESCRIPTION
Face à l'augmentation des cybermenaces et à la forte demande en compétences en cybersécurité, ce module d'une journée propose une immersion structurée au cœur de l'écosystème cyber. Les participants y découvrent le panorama des activités, les principaux rôles et responsabilités, ainsi que les compétences clés attendues sur le marché. Le module met également en lumière les trajectoires professionnelles possibles (formations, certifications, évolutions et tendances). À l'issue de la formation, les participants disposent d'un socle de compréhension commun leur permettant de mieux se projeter dans les métiers de la cybersécurité et de contribuer plus efficacement aux enjeux de sécurité de leur organisation

OBJECTIFS PEDAGOGIQUES

- Décrire les fondamentaux et les composantes de l'écosystème de la cybersécurité
- Identifier les principaux métiers, rôles et responsabilités associés
- Expliquer les compétences clés attendues pour les différents métiers de la cybersécurité
- Identifier les trajectoires professionnelles possibles (formations, certifications, évolutions) en cybersécurité

PUBLIC CIBLE

- Collaborateurs en situation de reconversion
- Collaborateurs IT ou SSI (Débutant)

PRE-REQUIS
Aucun prérequis technique nécessaire

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus

Séminaire en présentiel
Sécurité

Code :
IMRTC

Durée :
1 jour(s) (7,00 heures)

Exposés : **70 %**
Cas pratiques : **0 %**
Echanges d'expérience : **30 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 1 500,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

1) PRÉSENTATION GLOBALE DE LA CYBERSÉCURITÉ

- Définition et enjeux actuels et des menaces (cybercriminalité, espionnage, hacktivisme...)
- La place de la cybersécurité dans les organisations
- Les acteurs clés (entreprises, institutions, autorités, éditeurs...)
- Les spécificités et contraintes de la cybersécurité (Travail en équipe et en crise, transversalité, astreintes...)

2) PANORAMA DES ACTIVITÉS DE LA CYBERSÉCURITÉ

- Découverte des grandes familles d'activités (GRC, technique, opérationnel, audit...)
- Activités émergentes (cloud security, IA dans la cybersécurité...)

3) MÉTIERS, RÔLES ET PRINCIPALES COMPÉTENCES EN CYBER

- Présentation des principaux métiers : des rôles transverses (RSSI, chef de projet cyber...) aux rôles techniques (analyste SOC, pentesteur...)
- Métiers émergents (cloud security, IA & cyber, conformité...)
- Les responsabilités associées (individuelle et collective)
- Compétences techniques vs transverses
- Soft skills indispensables (communication, esprit critique...)
- Référentiels métiers (ANSSI, NIST, NICE...)

4) LES DIFFÉRENTS CADRES ASSOCIÉS : ÉTHIQUE, PROFESSIONNALISME ET RÉGLEMENTAIRE

- La responsabilité professionnelle et éthique des métiers de la cybersécurité
- Vision globale des réglementations clé (RGPD, CRA, NIS2, Data Act, IA Act...) et des cadres normatifs et réglementaires (ISO 27001, NIST) et leur impact sur les métiers.

- Sensibilité des métiers cybersécurité (accès, confiance, confidentialité, intégrité)

4) PARCOURS PROFESSIONNNELS ET ÉVOLUTIONS DE CARRIÈRE EN CYBER

- Parcours types selon les Profils (junior / confirmé / expert) dans la cybersécurité
- Mobilité et passerelles depuis d'autres domaines (IT, juridique, management) et passerelles entre métiers
- Les grandes orientations : Spécialisation ou polyvalence ? Fonctionnel ou technique…
- Les possibilités d'évolution vers des postes à responsabilité dans la cyber
- Témoignages / retours d'expérience

4) LES FORMATIONS ET CERTIFICATIONS CYBER

- Diplômes et formations initiales
- Certifications reconnues (CEH, CISSP, OSCP...)
- Stratégies de montée en compétences

4) TENDANCES ET ÉVOLUTIONS TECHNOLOGIQUES

- Menaces émergentes et futurs défis (IA et Cyber, Automatisation...)
- Impact des nouvelles menaces et des technologies émergentes sur les organisations

4) SYNTHÈSE ET PERSPECTIVES

- Récapitulatif des points clés
- Opportunités dans le secteur
- Conseils pour se lancer ou évoluer

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com