Ref. formation 202312209781

Cybersécurité | Référent Cybersécurité

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

EVOLUTION5
Jean-Denis Coindre
06.29.78.66.25
contact@evolution5.fr

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Dossier

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Aucune

Prérequis pédagogiques :

• Etre sensibilisé à la Cybersécurité • Savoir naviguer sous Windows • Savoir installer un logiciel

Contrat de professionnalisation possible ?

Non

Objectif de la formation

• Comprendre les principes fondamentaux de la cybersécurité. • Analyser les enjeux actuels liés à la sécurité informatique. • Reconnaître les différentes menaces sur les systèmes d'information. • Évaluer les risques associés et leurs implications. • Élaborer une stratégie globale de sécurité adaptée à l'entreprise. • Définir des protocoles et des procédures de sécurité. • Mettre en œuvre des bonnes pratiques d'hygiène informatique. • Sensibiliser les utilisateurs aux risques et aux comportements sécurisés. • Établir un plan de réponse aux incidents. • Sélectionner et configurer des outils de surveillance efficaces.

Contenu et modalités d'organisation

Module 1: Définir les Fondamentaux de la Cybersécurité Comprendre les principes fondamentaux de la cybersécurité. Analyser les enjeux actuels liés à la sécurité informatique. Module 2: Identifier les Menaces et les Risques en Cybersécurité Reconnaître les différentes menaces qui pèsent sur les systèmes d'information. Évaluer les risques associés et leurs implications. Module 3: Mettre en Place une Stratégie de Sécurité Élaborer une stratégie globale de sécurité adaptée à l'entreprise. Définir des protocoles et des procédures de sécurité. Module 4: Assurer l'Hygiène Informatique et Sensibiliser les Utilisateurs Mettre en œuvre des bonnes pratiques d'hygiène informatique. Sensibiliser les utilisateurs aux risques et aux comportements sécurisés. Module 5: Gérer les Incidents de Sécurité Établir un plan de réponse aux incidents. Maîtriser les procédures de gestion des crises en cas d'attaques. Module 6: Mettre en Place des Outils de Surveillance et de Détection Sélectionner et configurer des outils de surveillance efficaces. Développer des compétences de détection des activités suspectes. Module 7: Sécuriser les Infrastructures Réseaux Concevoir des architectures réseau sécurisées. Configurer et administrer des pare-feu et des dispositifs de sécurité réseau. Module 8: Protéger les Données et les Systèmes Mettre en œuvre des mécanismes de chiffrement des données. Appliquer des solutions de sauvegarde et de restauration. Module 9: Gérer la Sécurité des Applications Évaluer la sécurité des applications existantes. Intégrer des mesures de sécurité dans le développement d'applications. Module 10: Conduire des Audits de Sécurité Planifier et réaliser des audits de sécurité. Analyser les résultats des audits et proposer des améliorations. Nous pouvons adapter et personnaliser le programme en fonction de vos besoins par des compléments. N'hésitez pas à nous contacter pour ajuster le programme de votre formation !

Durées de la formation ***30h en FOAD**
Parcours de formation personnalisable ? **Oui** Type de parcours ***Non renseigné***

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00425386	du 01/01/2024 au 31/12/2024	(33)	EVOLUTION5		Non éligible	FPC
00532272	du 01/01/2025 au 31/12/2025	(33)	EVOLUTION5		Non éligible	FPC