Ref. formation 202312209735

Cybersécurité | Cryptographie

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 de base de la cryptographie. • Identifier les concepts tels que clés, algorithmes et chiffrement. • Mettre en œuvre des techniques de chiffrement symétrique. • Appliquer des algorithmes de chiffrement asymétrique. • Mettre en place une infrastructure à clé publique (PKI). • Utiliser des certificats pour sécuriser les communications. • Appliquer des fonctions de hachage pour l'intégrité des données. • Utiliser des protocoles de signature numérique pour l'authentification. • Comprendre le concept de preuve de connaissance nulle. • Mettre en place des procédures de gestion des clés et assurer leur mise à jour régulière.

Contenu et modalités d'organisation

Module 1: Comprendre les Fondamentaux Cryptographiques Acquérir une compréhension des principes de base de la cryptographie. Identifier les concepts tels que clés, algorithmes, et chiffrement. Module 2: Appliquer Chiffrement Symétrique Mettre en œuvre des techniques de chiffrement symétrique. Comprendre les modes d'opération pour la confidentialité des données. Module 3: Utiliser Chiffrement Asymétrique Appliquer des algorithmes de chiffrement asymétrique. Comprendre le concept de clés publique et privée. Module 4: Protéger Communications avec Certificats et PKI Mettre en place une infrastructure à clé publique (PKI). Utiliser des certificats pour sécuriser les communications. Module 5: Comprendre Mécanismes de Hachage Appliquer des fonctions de hachage pour l'intégrité des données. Comprendre les applications des fonctions de hachage. Module 6: Mettre en Place Protocoles de Signature Numérique Utiliser des protocoles de signature numérique pour l'authentification. Comprendre le processus de création et de vérification des signatures. Module 7: Garantir Confidentialité des Données avec Zero Knowledge Proof Comprendre le concept de preuve de connaissance nulle. Appliquer des techniques pour garantir la confidentialité sans révéler l'information. Module 8: Assurer Confidentialité des Communications avec Perfect Forward Secrecy Mettre en œuvre des mécanismes de Perfect Forward Secrecy. Comprendre comment assurer la confidentialité des communications à long terme. Module 9: Sécuriser Échanges de Clés avec Protocoles Diffie-Hellman Appliquer les protocoles de l'échange de clés Diffie-Hellman. Comprendre les mécanismes pour l'établissement sécurisé de clés secrètes. Module 10: Gérer et Mettre à Jour Clés Cryptographiques Mettre en place des procédures de gestion des clés. Assurer la mise à jour régulière des clés pour garantir la sécurité à long terme. 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 !

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
00425138	du 01/01/2024 au 31/12/2024	Mérignac (33)	EVOLUTION5		Non éligible	FPC
00532274	du 01/01/2025 au 31/12/2025	Mérignac (33)	EVOLUTION5		Non éligible	FPC