Ref. formation 202309172156

Certificat de compétence Analyste en cybersécurité

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

CNAM NOUVELLE AQUITAINE
Accueil
05.57.59.23.00
contact@cnam-nouvelle-aquitaine.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 :

Entretien

Niveau d'entrée requis :

Niveau 5 : DEUG, BTS, DUT, DEUST (Niveau 5 européen)

Conditions d'accès :

Bac+ 2 informatique ou bac+2 scientifique/technique avec une expérience professionnelle significative dans les métiers de l'informatique. + Avoir le niveau de l'UE RSX101, pré-requis de l'UE RSX112. Il est recommandé de suivre les UE SEC101 et SEC102 en fin de parcours.

Prérequis pédagogiques :

Bac+ 2 informatique ou bac+2 scientifique/technique avec une expérience professionnelle significative dans les métiers de l'informatique. + Avoir le niveau de l'UE RSX101, pré-requis de l'UE RSX112. Il est recommandé de suivre les UE SEC101 et SEC102 en fin de parcours.

Contrat de professionnalisation possible ?

Non

Objectif de la formation

Administrer le réseau ou les réseaux et des télécommunications de l'entreprise a) Process institutionnels Participer aux évolutions de l'architecture IT de l'entreprise Participer à la définition de l'architecture réseau Participer à l'organisation de la mise en place de l'architecture (câblage, débogage technique). Définir une ligne de conduite pour la gestion du parc. Diagnostiquer, anticiper les besoins et préconiser des plans d'évolution b) Process techniques Installer et gérer le parc informatique et télécommunications Installer et tester la connectique, le matériel informatique et les logiciels réseaux Installer de nouvelles extensions (configuration et gestion des droits d'accès). Paramétrer l'équipement LAN Suivre les performances du réseau (réalisation de tests réguliers, simulation d'incidents). Mettre en place et configurer de nouveaux logiciels. Adapter les configurations de systèmes applicatifs et réseaux Intervenir pour la création et la gestion de comptes utilisateurs, pour assurer le provisioning et pour régler des incidents ou des anomalies Administrer les composants informatiques d'un système d'information d'entreprise en prenant en compte les contraintes de sécurité Dépanner des serveurs de messagerie Opérer techniquement les fonctions d'entreprise situées le cloud (PAAS, SAAS ...) Assurer des fonctions de support technique IT et Réseaux (helpdesk) Assurer la sécurité du système a) Process gestion des risques du système d'information de l'entreprise Participer à la définition de la politique générale de sécurité du système d'information de l'entreprise Connaître les grands standards de la sécurité dont l'environnement ISO Comprendre les mécanismes de continuité d'activité (business) dans l'entreprise Analyser et identifier les risques (sécurité, confidentialité, fiabilité, ...) et connaitre les méthodes de base associées. Mettre en place l'organisation nécessaire au déploiement de la politique de sécurité des équipements et des données Anticiper les besoins et préconiser des plans d'évolution Apporter son expertise dans la gestion opérationnelle des incidents de sécurité b) Process techniques Effectuer un relevé des outils et identifier chaque risque (réaliser un

...

Contenu et modalités d'organisation

Total de 24 ECTS Une UE à choisir parmi : (6 ECTS) NSY104 - Architectures des systèmes informatiques / 6 ECTS NFE108 - Méthodologies des systèmes d'information / 6 ECTS NFE113 - Conception et administration de bases de données / 6 ECTS SMB101 - Systèmes d'exploitation : principes, programmation et virtualisation / 6 ECTS NSY103 - Linux : principes et programmation / 6 ECTS Une UE à choisir parmi : (6 ECTS) RSX112 - Sécurité des réseaux / 6 ECTS SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications / 6 ECTS SEC101 - Cybersécurité : référentiel, objectifs et déploiement / 6 ECTS SEC102 - Menaces informatiques et codes malveillants : analyse et lutte / 6 ECTS

Parcours de formation personnalisable ? **Oui** Type de parcours ***Non renseigné***

Validation(s) Visée(s)

Certificat de compétence analyste en cybersécurité - *Sans niveau spécifique*

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00376970	du 01/09/2023 au 30/06/2025	Bègles (33)	CNAM NOUVELLE AQUITAINE		Non éligible	FPC
00510027	du 14/10/2024 au 30/06/2027	Bègles (33)	CNAM NOUVELLE AQUITAINE		Non éligible	FPC