



DIPLÔME
Certificat de compétence Analyste en cybersécurité

Code : CC13800A



Niveau d'entrée : Aucun
Niveau de sortie : Aucun
ECTS : 24
Diplôme national
Oui

Déployabilité

A la carte : Formation pouvant s'effectuer au rythme de l'élève, en s'inscrivant aux unités du cursus
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)
Contrat de professionnalisation : Formation pouvant se suivre en contrat de professionnalisation

Compétences et débouchés

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 connaître 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 état des lieux, détecter les menaces)
- Superviser les activités réseaux et systèmes et mettre en place les outils nécessaires
- Auditer un système (opérer des tests)
- Ecrire et mettre en place des procédures de protection et de réaction à incident
- Administrer la sécurité : mise en place d'outils de sécurité et de sauvegarde, administration de la messagerie, du réseau téléphonique, de la messagerie vocale, de la vidéo transmission
- Mettre à jour les systèmes
- Savoir contrer les attaques, prendre les bonnes décisions dans la réduction de l'impact de ces attaques

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

Prérequis et 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.

MENTIONS OFFICIELLES

Mots-clés

[Cybersécurité](#)

Informations complémentaires

Type de diplôme

[Certificat de compétence](#)

Code NSF

326 - Informatique, traitement de l'information, réseaux de transmission

Codes ROME

Responsable sécurité informatique[M1802]

Formacode

Sécurité informatique [31006]

Code du parcours

CC13800A

Modules d'enseignement

- [Architectures des systèmes informatiques](#)
- [Conception et administration de bases de données](#)
- [Contrôle d'accès et Gestion des Identités Numériques](#)
- [Cybersécurité : référentiel, objectifs et déploiement](#)
- [Linux : principes et programmation](#)
- [Menaces informatiques et codes malveillants : analyse et lutte](#)
- [Méthodologies des systèmes d'information](#)
- [Sécurité des réseaux](#)
- [Systèmes d'exploitation : principes, programmation et virtualisation](#)

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.

Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.

Chaque bloc de compétences peut être validé séparément.

Information non disponible, pour plus d'information veuillez [contacter le Cnam](#)