

## Certificat de compétence Analyste en cybersécurité

CC13800A - 24 crédits

**Niveau(x) d'entrée :** Aucun niveau requis  
**Niveau(x) de sortie :** Aucun niveau spécifique  
**Lieu(x) :** Non proposé en présentiel au Cnam HdF, nous contacter



### PRÉSENTATION

#### Public / 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.

### COMPÉTENCES ET DÉBOUCHÉS

#### Compétences

#### 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

### INFORMATIONS PRATIQUES

- Valider les UE du CC avec une moyenne d'au moins 10/20 sans note inférieure à 8/20.

## Contenu de la formation

## Tronc commun

## Parcours Une UE à choisir parmi :

Architectures des systèmes informatiques

NSY104 6 ects

Méthodologies des systèmes d'information

NFE108 6 ects

Conception et administration de bases de données

NFE113 6 ects

Systèmes d'exploitation : principes, programmation et virtualisation

SMB101 6 ects

Linux : principes et programmation

NSY103 6 ects

## Parcours Une UE à choisir parmi :

Sécurité des réseaux

RSX112 6 ects

Contrôle d'accès et Gestion des Identités Numériques

SEC105 6 ects

Cette UE n'est plus proposée, nous contacter

Cybersécurité : référentiel, objectifs et déploiement

SEC101 6 ects

Menaces informatiques et codes malveillants : analyse et lutte

SEC102 6 ects

Méthodes  
pédagogiques:

Pédagogie qui combine des enseignements académiques et des pédagogies actives s'appuyant sur l'expérience en entreprise et le développement des compétences. Equipe pédagogique constituée pour partie de professionnels.

## Modalités d'évaluation:

Chaque unité (UE, UA) fait l'objet d'une évaluation organisée en accord avec l'Etablissement public (certificateur) dans le cadre d'un règlement national des examens.



Un référent Cnam est dédié à l'accompagnement de toute personne en situation de handicap. Contactez : [hdf\\_handicap@lecnam.net](mailto:hdf_handicap@lecnam.net)

## Mentions officielles

**Diplôme** : Certificat de compétence

Analyste en cybersécurité

**Inscrit au RNCP** : non

**Certificateur** : CONSERVATOIRE NATIONAL DES ARTS ET METIERS

**Date d'échéance de l'enregistrement**

:

## Voir nos indicateurs de résultats



<https://www.cnam-hauts-de-france.fr/chiffres-et-indicateurs/>

Document non contractuel.

Le programme et le volume horaire de cette formation sont susceptibles d'être modifiés en fonction des évolutions du référentiel pédagogique national.

**Le Cnam Hauts-de-France vous informe, vous accompagne et vous conseille.**

Contactez nos conseillers formation au  0800 719 720  
ou [hdf\\_contact@lecnam.net](mailto:hdf_contact@lecnam.net)

Tous nos programmes sur [www.cnam-hauts-de-france.fr](http://www.cnam-hauts-de-france.fr)