Apprendre au cnam change votre vie

le cnam

Certificat de compétence - CC13800A

Analyste en cybersécurité

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, prérequis de l'UE RSX112 ;
- Il est recommandé de suivre les UE SEC101 et SEC102 en fin de parcours.

Compétences visées

A – Administrer le réseau ou les réseaux et des télécommunications de l'entreprise

1 - 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.

2 - 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 provisionnement et 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, etc.) ;
- Assurer des fonctions de support technique IT et Réseaux (bureau d'aide).

B – Assurer la sécurité du système

1 - 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, etc.) 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.

2 - 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) ;
- Écrire 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 vidéotransmission ;
- Mettre à jour les systèmes ;
- Savoir contrer les attaques, prendre les bonnes décisions dans la réduction de l'impact de ces attaques.

Modalités d'évaluation

Deux sessions de contrôle sont associées aux unités d'enseignements de cours/ED. Le certificat de compétence est délivré à tout auditeur remplissant les conditions suivantes dans un délai maximum de 4 ans :

- valider les UE du certificat avec une moyenne d'au moins 10/20 sans note inférieure à 8/20 ;
- valider un rapport d'expérience ;
- aucune expérience professionnelle n'est exigée pour l'obtention du certificat. La rédaction du rapport nécessitant cependant une mise en pratique des savoirs enseignés, la réalisation d'un stage de 3 mois est vivement recommandée afin de rédiger un rapport conforme aux attentes.

Le thème du rapport d'expérience doit être soumis à l'enseignant responsable et validé par lui. Le rapport, d'une quinzaine de pages, sera structuré en 3 parties :

- ***Introduction***
  - Description du projet et du cadre général de l'activité (présentation de l'entreprise, durée du stage, poste occupé, etc.) ; quel objectif pédagogique vous étiez-vous fixé (approfondissement ou découverte d'une compétence, d'un outil, etc.) ?
- ***Développement***
  - Missions réalisées : contexte (périmètre, enjeux) et objectif de la mission, quel problème a été traité (description) et quelles méthodologies, procédures, outils, etc. ont été utilisés ?
  - Analyse réflexive sur les missions réalisées (analyse des outils et des méthodes utilisés pour pratiquer ces tâches, actions correctives à mettre en place, etc.) ;
  - Synthèse des compétences acquises (les classer par domaine et nature : techniques, organisationnelles, management).
- ***Conclusion***
  - Bilan (de la mission pour l'entreprise, personnel, etc.) ;
  - Des références au cours, un sommaire et l'utilisation d'une bibliographie sont les bienvenues ;
  - Le rapport d'expérience professionnel exigé dans le cadre de la licence Informatique générale, s'il traite principalement de travaux en cybersécurité, peut être proposé dans le cadre de la validation de cette UA.

Tarifs

- 180 € pour une UE à 6 crédits

Reponsables de la formation

Véronique Legrand et Isabelle Guée

Coordonnées

EPN05 Informatique
2 rue conté
75003 Paris
Bureau 31.1.79

Programme du certificat		
Code UE	Intitulé de l'UE	Crédits
SEC101	Cybersécurité : référentiel, objectifs et déploiement	6
SEC102	Menaces informatiques et codes malveillants : analyse et lutte	6
UARS0C	Projet	6
Une UE à choisir parmi :		
NSY104	Architectures des systèmes informatiques	6
NFE108	Méthodologies des systèmes d'information	6
NFE113	Conception et administration de bases de données	6
SMB101	Systèmes d'exploitation : principes, programmation et virtualisation	6
Une UE à choisir parmi :		
RSX112	Sécurité des réseaux	6
SEC105	Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	6

deptinfo.cnam.fr

Contact
Swathi Rajaselvam,
gestionnaire pédagogique
01 40 27 22 58
swathi.ranganadin@cnam.fr