Certificat de compétence Analyste en cybersécurité

Mis à jour le 21-01-2022

Code : CC13800A

24 crédits

Certificat de compétence

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Responsabilité opérationnelle : Isabelle GUÉE

Niveau CEC d'entrée requis : Sans niveau spécifique

Niveau CEC de sortie : Sans niveau spécifique

Mode d'accès à la certification :

- Validation des Acquis de l'Expérience
- Formation continue

NSF : Informatique, traitement de l'information, réseaux de transmission (326)

Métiers (ROME) : Responsable sécurité informatique (M1802)

Contact national :

EPN05 - Informatique

2 rue Conté
accès 33.1.11B
75003 Paris
01 40 27 28 21
Mmadi Hamida
hamida.mmadi@lecnam.net

Présentation

Publics / 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.

Modalités de validation

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

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

Enseignements

24 ECTS

Une UE à choisir parmi : 6 ECTS

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

Une UE à choisir parmi : 6 ECTS

Sécurité des réseaux	RSX112 6 ECTS
Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	SEC105 6 ECTS

Cybersécurité : référentiel, objectifs et déploiement	SEC101 6 ECTS
Menaces informatiques et codes malveillants : analyse et lutte	SEC102 6 ECTS