le cnam
Ile-de-France

CERTIFICAT DE COMPÉTENCES ANALYSTE EN CYBERSÉCURITE

Crédit : 30 ECTS Code CC13800A
Niveau d'entrée : Bac + 2

Public concerné 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.

Compétences attestées

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

Description de la formation

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

Un cours au choix parmi :

@ 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	

Un cours au choix parmi :

@ 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	

@ Cours également disponible en ligne (Ile-de-France)

ECTS : Système européen de transfert et d'accumulation de crédits.

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

NSY104 - Architectures des systèmes informatiques
Crédits : 6 ECTS

Public concerné et conditions d'accès
Connaissances générales du fonctionnement d'un ordinateur et de son système d'exploitation, idéalement avoir suivi et/ou validé NFA004
Des connaissances en programmation sont souhaitées.

Objectifs pédagogiques
Etudier l'architecture des systèmes informatiques et de leur parallélisme à différentes échelles, depuis le processeur jusqu'aux systèmes multi-ordinateurs. Cet enseignement permet d'acquérir une vision d'ensemble des moyens disponibles pour augmenter les performances d'un système, tout en assimilant les détails et enjeux de chaque famille de solution étudiée.

Contenu de la formation
- Rappels d'architecture des machines, processeurs, mémoires, cache, OS
- Architecture de processeur pipeline, superscalaire, VLIW
- Architecture des systèmes multiprocesseurs
- Architecture des systèmes multi-ordinateurs
- Architecture des systèmes de stockage
- APIs: OpenMP, CUDA, MPI, OpenCL
- Architecture des systèmes à haute disponibilité
- Introduction aux architectures embarquées

NFE108 - Méthodologies des systèmes d'information
Crédits : 6 ECTS

Objectifs pédagogiques
Fournir les bases méthodologiques nécessaires à la conception et à la réalisation des systèmes d'information d'entreprise. Préparer au métier d'études et développement informatique qui:
- Conçoit, développe et met au point un projet d'application informatique, de la phase d'étude à son intégration, pour un client ou une entreprise selon des besoins fonctionnels et un cahier des charges.
- Peut conduire des projets de développement.

Contenu de la formation
• Introduction aux méthodologies des systèmes d'information
• La méthode MERISE (Rappels)
• L'approche objet
• UML et processus unifié
• De l'analyse à la conception
• Les outils AGL (Projet TP)
• Conclusion sur les méthodes et outils de conception de systèmes d'information

NFE113 - Conception et administration de bases de données
Crédits : 6 ECTS

Objectifs pédagogiques
Préparer des futurs informaticiens orientés vers la conception et l'administration de base de données. L'accent est mis sur l'utilisation d'une méthodologie de conception de base de données centralisée ou répartie, la maîtrise des éléments d'architecture logique et physique d'une base de données relationnelle, les fonctions d'administration d'une base de données, la démarche d'optimisation d'une base de données, les règles d'évaluation du coût des opérations.

Contenu de la formation
• Introduction
• Architecture d'un SGBDR
• Mise en oeuvre d'une base de données relationnelle
• Administration / optimisation d'une base de données
• Approches à la gestion des bases de données réparties ou fédérées
Le cours est concrétisé par des travaux pratiques sur le SGBD ORACLE.

SMB101 - Systèmes d'exploitation : principes, programmation et virtualisation
Crédits : 6 ECTS

Public concerné et conditions d'accès
Elèves ayant des connaissances de base en systèmes informatiques vues en UTC502 au Cnam ou équivalent, ainsi que des connaissances en programmation (de préférence en langage C).

Objectifs pédagogiques
Présenter les concepts des systèmes d'exploitation et leur programmation en étudiant les mécanismes de base des systèmes d'exploitation classiques mais aussi ceux des systèmes temps réel, des systèmes embarqués et des objets connectés. Les principes de virtualisation des systèmes d'exploitation sont aussi abordés dans ce cours.

Contenu de la formation
• *Concepts et paradigmes des systèmes d'exploitation classiques.*
• *Concepts et paradigmes des systèmes temps réel.*
• *Concepts et paradigmes des systèmes embarqués et objets connectés.*
• *Concepts et principes de la virtualisation de systèmes et de la conteneurisation*

RSX112 - Sécurité des réseaux
Crédits : 6 ECTS

Public concerné et conditions d'accès
Ce cours s'appuie sur des connaissances de base en programmation, en systèmes informatiques et en réseaux.

Objectifs pédagogiques
Ce cours présente les principaux aspects de la sécurité des réseaux. Il présente les problèmes généraux de sécurité (confidentialité, intégrité, disponibilité, authentification et contrôle d'accès, non-répudiation), les solutions-types connues pour ces problèmes et leur mise en œuvre dans l'architecture Internet.

Contenu de la formation
Introduction à la sécurité et à la gestion des risques informatiques (normes ISO 27000)
1) Primitives cryptographiques :
2) Contrôle d'accès et sécurité de l'information :
3) Disponibilité et sûreté de fonctionnement :
4) Protocoles de sécurité

SEC101 - Cybersécurité : référentiel, objectifs et déploiement
Crédits : 6 ECTS

Public concerné et conditions d'accès
Niveau Bac + 2 en informatique, il est conseillé de suivre ou d'avoir suivi l'unité d'enseignement SEC001.

Objectifs pédagogiques
Savoir mener, argumenter et déployer une politique de sécurité informatique dans une entreprise en lien avec une analyse de risque.

Contenu de la formation
1- Principaux enjeux de la sécurité pour la société numérique[VL2]
2- La continuité d'activité :[VL3]
3- Organisation de la sécurité et de ses métiers dans l'entreprise :
4- Implémentation de la sécurité

SEC102 - Menaces informatiques et codes malveillants : analyse et lutte
Crédits : 6 ECTS

Public concerné et conditions d'accès
Informaticiens en poste dans les entreprises mais aussi publics en recherche de double compétence ou en reconversion.

Objectifs pédagogiques
Etre capable de faire de la remédiation adaptée aux contextes de menace.

Contenu de la formation
Typologies des codes et des effets : Virus, worm, botnet, etc.
Etudes des modes d'action des codes malveillants : analyse intrinsèque des codes malveillants, anatomies d'attaques type, à partir d'exemples réels.
Lutte contre le code malveillant- veille, alertes, détection des effets des codes, identification de la menace.
Caractérisation des effets, Impacts techniques, économiques, fonctionnels.
Réduction des effets, limitation des impacts techniques et fonctionnels.
Analyse postmortem (forensic)
Méthodologies de réponses à incidents
Audits

SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications
Crédits : 6 ECTS

Public concerné et conditions d'accès
Informaticiens en poste dans les entreprises mais aussi publics en recherche de double compétence ou en reconversion.

Objectifs pédagogiques
Comprendre les objectifs, exigences et contraintes spécifiques à l'application des bonnes pratiques de la sécurité informatique
• Comprendre les mécanismes informatiques réseau, système, data et applicatifs de base,
• Apprendre les architectures techniques, protocoles et configuration en lien avec les bonnes pratiques de base à déployer sur un SI en vue de garantir une hygiène informatique de base,
• Apprendre les différents outils et techniques pour valider l'adéquation et la mise en place des bonnes pratiques, les tester.
• Apprendre à garantir des conditions opérationnelles de sécurité d'un système conformément aux politiques de sécurité organisationnelles, opérationnelles et techniques,
• Apprendre à intégrer la composante technique dans les procédures accompagnant la mise en place des bonnes pratiques,
• Être en mesure de prendre les décisions pour que l'entreprise mette en œuvre des mesures techniques en réponse aux bonnes pratiques,

Contenu de la formation
- Introduction aux architectures, leur sécurisation et l'application des principes de défense en profondeur
- Architectures et protocoles de sécurité pour les accès au SI (AAA : authentification, Autorisations, Accounting)
- Sécurité de base des matériels et des systèmes d'exploitation
- Architectures et protocoles de sécurité pour la virtualisation
- Architectures et protocoles de sécurité pour les réseaux locaux, les mobiles et Internet
- Architectures et protocoles de sécurité pour la messagerie
- Architectures et protocoles de sécurité pour la sauvegarde des données, des applications, des bases de données
- Architectures et protocoles de sécurité pour les architectures applicatives
- Architectures et protocoles pour la protection des données : travail, domicile & mobilité