ADMINISTRATEUR CYBERSÉCURITÉ

DIPLÔME « LICENCE GÉNÉRALE SCIENCES TECHNOLOGIES SANTÉ MENTION INFORMATIQUE PARCOURS INFORMATIQUE GÉNÉRALE » DU CNAM

Contact

Christophe DEDOUCHE – Responsable de la Formation Professionnelle
pro@ecam-strasbourg.eu
Cédric BOBENRIETH – Responsable pédagogique de la formation
cedric.bobenrieth@ecam-strasbourg.eu

Accessibilité universelle

Formation accessible aux personnes en situation de handicap
Pour tout renseignement, contacter referenthandicap@ecam-strasbourg.eu

Présentation générale

Permettre aux stagiaires de mettre à niveau leur expérience et leur formation pour se reconvertir vers le métier d'Administrateur Cybersécurité. Les enjeux de Cybersécurité deviennent de plus en plus critiques pour les entreprises, sujettes à des campagnes de malwares et de vol de données de plus en plus fréquentes.
La formation 'Administrateur Cybersécurité' prépare les stagiaires à la Licence 'Informatique Générale' du CNAM, dans une déclinaison adaptée aux métiers de la Cybersécurité. Elle valide les cinq domaines de compétences nécessaires à l'administration sécurisée d'un système d'information, avec validation d'un diplôme de Licence :

-Fondamentaux de l'informatique
-Industrialisation de la cybersécurité
-Cybersécurité, systèmes et réseaux
-Cybersécurité, données et logiciels
-Communication et entreprise

La formation technique est complétée par un module d'accompagnement vers l'emploi 'Technique de Recherche d'Emploi (TRE)'.

Le diplôme offre une formation générale couvrant les principaux domaines de l'informatique : développement, programmation, réseaux, multimédia, systèmes, architecture des machines, génie logiciel, recherche opérationnelle, systèmes d'informations, systèmes industriels.

Il s'adresse plus particulièrement aux salariés du domaine informatique recherchant une valorisation de leur pratique quotidienne en vue d'une promotion ou d'un changement d'employeur, mais il peut accueillir également des salariés d'autres domaines en phase de reconversion.

Suites possibles après cette formation

- **Métiers :** Conception, développement et maintenance en condition opérationnelle d'une architecture de sécurité tenant compte du contexte de l'entreprise, des attentes et besoins des utilisateurs et en veillant aux évolutions technologiques, maintien en sécurité du système d'information de son entreprise : Administrateur de bases de données, Administrateur systèmes et réseaux, Technicien/technicienne en production et exploitation de systèmes d'information
- **Formations :** Cette formation étant une Licence générale Sciences Technologies Santé mention informatique, elle ouvre l'accès à une poursuite d'étude en Master.

Blocs de compétences et capacités professionnelles

- **Bloc de compétence n°1 : Fondamentaux de l'informatique**
  - Capacité C1 : Acquérir des notions d'arithmétique utiles en informatique, notamment pour la cryptographie
  - Capacité C2 : Assimilation de méthodes et d'algorithmes fondamentaux en recherche opérationnelle et aide à la décision

- **Bloc de compétence n°2 : Industrialisation de la cybersécurité**
  - Capacité C3 : Comprendre les enjeux d'une politique et de sécurité informatique cybersécurité et appliquer des méthodologies efficaces d'aguerrissement
  - Capacité C4 : Savoir auditer, conseiller, accompagner le changement
  - Capacité C5 : Savoir mener et intégrer des solutions de sécurité suite à l'analyse de risque
  - Capacité C6 : Savoir gérer un projet

- **Bloc de compétence n°3 : Cybersécurité, systèmes et réseaux**
  - Capacité C7 : Appréhender les mécanismes fondamentaux des systèmes d'exploitation.
  - Capacité C8 : évaluer les principales contraintes réseaux et leur impact sur une application client/serveur ou distribuée
  - Capacité C9 : participer à la définition des principaux éléments d'un cahier des charges fonctionnels à destination d'une maîtrise d'ouvrage
  - Capacité C10 : Conception et programmation de tout type de système d'exploitation
  - Capacité C11 : Maîtrise des principes sous-jacents à la virtualisation de systèmes afin de faciliter l'intégration et l'administration de ce type de service dans un système informatique
  - Capacité C12 : Pouvoir mettre en oeuvre des solutions de sécurités dans l'architecture Internet.

- **Bloc de compétence n°4 : Cybersécurité, données et logiciels**
  - Capacité C13 : Recueillir et analyser les besoins Connaître le cycle de développement des logiciels
  - Capacité C14 : Concevoir les MCD et MLD
  - Capacité C15 : Concevoir les applications
  - Capacité C16 : Pouvoir aborder un nouveau langage de programmation ou une nouvelle bibliothèque en reconnaissant les usages dans ceux-ci des principaux paradigmes de programmation
  - Capacité C17 : Être capable de faire de la remédiation adaptée aux contextes de menace.

- **Bloc de compétence n°5 : Communication et entreprise**
  - Capacité C18 : Communiquer en anglais à l'oral et à l'écrit dans des situations professionnelles.
  - Capacité C19 : Définir son projet professionnel à court terme, actualiser et marqueter son CV et sa LM pour être en cohérence avec sa cible de poste recherché.

Objectifs pédagogiques de la formation

- Permettre une reconversion vers les métiers de l'administration système dans des environnements fortement exposés aux risques de cybersécurité
- Permettre aux stagiaires de maîtriser les référentiels cybersécurité et leur application aux systèmes et réseaux, données et logiciels.
- Donner aux stagiaires les compétences leur permettant d'être opérationnels dans le suivi opérationnel des systèmes d'informations et de leur protection

Modalités pratiques

- **Public** : Demandeurs d'emplois ayant une formation technique en informatique (au minimum niveau Bac +2 avec de bonnes connaissances en gestion des systèmes d'information) et de l'expérience (min. 1 an).

- **Prérequis** : être titulaire d'un diplôme de niveau III en informatique (DUT informatique, DPCT informatique, BTS informatique de gestion, diplôme analyste programmeur du Cnam, DUT GEII, certains titres Afpa homologués au niveau III) ou d'un diplôme qui dispense des niveaux L1 et L2
- **Conditions d'accès** : Recrutement en 3 étapes :
  - test d'évaluation des compétences
  - entretien de motivation professionnel
  - entretien de recrutement par l'entreprise accueillant le stagiaire durant la période en entreprise
- **Conditions de démarrage** : Nombre de participants de 8 personnes (minimum) à 15 personnes (maximum) pour l'ensemble de la formation

- **Lieu** : ECAM Strasbourg Europe, 2 Rue de Madrid, 67300 SCHILTIGHEIM
- **Nombre d'heures** : 1200 heures réparties de la manière suivante :
  - 450 heures en centre de formation
  - 750 heures en Entreprise
- **Horaires** : 9h–12h30 et 13h30–17h00 (accueil à partir de 8h30)
- **Type de formation** : Formation en présentiel
- **Date début de formation** : 11 octobre 2021
- **Examen de validation des compétences** : Chaque unité d'enseignement de la formation ne peut être validée que si la présence du stagiaire est attestée sur l'ensemble des sessions de formation.
  Deux sessions de contrôle sont associées aux unités d'enseignements. Dans ce cadre l'unité d'enseignement est acquise lorsque l'élève a obtenu la note de 10/20 à l'une des deux sessions. La licence est délivrée à tout auditeur remplissant les conditions suivantes : obtenir la moyenne générale à l'ensemble des unités d'enseignements composant la licence et avoir validé 17 crédits au titre de l'expérience professionnelle.
- **Validation** : L'atteinte des compétences de la formation est validée par le CNAM.

Moyens pédagogiques

- **Alternance de théorie, travaux dirigés :** cours en présentiel, cours à distance, travaux pratiques, travaux dirigés, selon une organisation (horaires, lieu de formation, enseignants,..) mise en oeuvre par l'ECAM, sous la tutelle pédagogique du Cnam en grand Est dans le cadre des règlements du Conservatoire National des Arts et Métiers.
- **Accompagnement :** Un module 'Techniques de Recherche d'Emploi' (TRE) vous permet de développer vos capacités professionnelles et de vous préparer à valoriser les compétences acquises durant la formation. Un accompagnement personnalisé vous est proposé, dont les modalités seront précisées par le formateur lors de la première séance du module. Une demi-journée optionnelle d'Aide à la Recherche de Stage (ARS) sera également proposée aux stagiaires qui désireraient avoir des conseils d'un professionnel dans leur démarche de recherche de stage.

Programme détaillé

- **Fondamentaux de l'informatique (68 heures)**
  - **Outils Mathématiques pour l'informatique (FOAD, 30,5 heures)**
    - Éléments de logique : proposition, prédicats, validité, satisfiabilité.
    - Les techniques de raisonnement : direct, par cas, par contraposition, par récurrence, par l'absurde.
    - Eléments d'arithmétique : divisibilité, nombres premiers, propriétés du PGCD, algorithme d'Euclide, décomposition en produit de facteurs premiers, arithmétique modulaire, algorithme RSA.
    - Relations et ordres : relations binaires, d'équivalence, ordres partiels et totaux.

        - Calcul matriciel et analyse : résolution de systèmes linéaires, méthode de Gauss, Gauss Jordan et manipulation de séries de Fourier avec l'aide d'un logiciel.
        - Systèmes de transition : traces, exécutions, états accessibles, états récurrents, transitions récurrentes, systèmes de transitions étiquetées, propriétés générales (de sûreté, de vivacité), introduction aux réseaux de Pétri.
        - Processus stochastiques et modélisation : chaînes de Markov à temps discret ; distribution stationnaire, processus de Markov continus ; processus de Poisson ; processus de naissance et de mort ; application aux files d'attente simples.
    - **Recherche opérationnelle et aide à la décision (37,5 heures)**
        - Graphes et ordonnancements en gestion de projets
        - Programmation linéaire et applications
        - Analyse multicritère
        - Eléments de théorie des files d'attente et de sûreté de fonctionnement

- **Industrialisation de la cybersécurité (75 heures)**
    - **Cybersécurité : référentiel, objectifs et déploiement (44,5 heures)**
        - Comprendre les enjeux d'une politique et de sécurité informatique cybersécurité et appliquer des méthodologies efficaces d'aguerrissement
        - Comprendre les différentes situations d'incident
        - Savoir mettre en place une gouvernance efficace dans le domaine de la cybersécurité
        - Savoir auditer, conseiller, accompagner le changement
        - Savoir mener et intégrer des solutions de sécurité suite à l'analyse de risque
    - **Management de projet (30,5 heures)**
        - Les projets : définition et enjeux pour l'entreprise
        - Les grands modèles d'organisation des projets
        - Le management des équipes projet
        - Les outils de pilotage des projets (gestion du temps et des coûts)
        - L'intégration des partenaires dans les projets
        - Introduction au management multi-projets : portefeuille, plateforme, lignées
        - Perspectives du management de projet

- **Cybersécurité, systèmes et réseaux (143 heures)**
    - **Système (FOAD, 30,5 heures)**
        - Notions de base sur les systèmes d'exploitation, mise en oeuvre de la protection/isolation : notion d'espace d'adressage, de modes d'exécution user/superviseur, introduction des appels système.
        - Gestion des exécutions programmes, processus, ordonnancement, threads
        - Synchronisation
        - Gestion de la mémorisation, mémoire centrale pagination, problèmes de gestion mémoire et d'allocation de blocs de tailles variables
        - Notion de base en administration système, comptes, droits, etc… Gestion des I/O asynchrones et des Ginterruptions.
    - **Introduction à la cyberstructure de l'internet : réseaux et sécurité (30,5 heures)**
        - Diviser pour régner (modèle OSI) : Découverte de l'architecture de communication en couches
        - Les autoroutes de l'information
        - Concepts et problèmes de la transmission de données.
        - Collectivisme ou Libre entreprise… à la recherche d'un modèle équitable (sous-couche MAC). Grandes familles de protocoles à compétition et à

coopération, détail sur CSMA/CD et CSMA/CA en mode infrastructure. Ponts et commutation.
    - Croisements et Destination (couche réseau). Adressage, tables de routage et l'expédition de données dans le réseau IP. Evolution de IPv4 à IPv6.
    - Transport de données entre un client et un serveur à travers UDP et TCP avec le modèle datagramme, et les approches connecté et non connecté. Gestion et utilisation de l'API socket.
    - Aspects sécurité de base pour la confidentialité, l'intégrité, l'authentification et la notarisation : principes de cryptographie symétrique et asymétrique, fonctions de hachage cryptographique.
  - **Systèmes d'exploitation : principes, programmation et virtualisation (37,5 heures)**
    - Conception et programmation de tout type de système d'exploitation (système classique comme Linux, système temps réel, système embarqué pour objets connectés).
    - Architecture et fonctionnement des systèmes d'exploitation tels que Unix et Linux mais aussi des systèmes embarqués (comme par exemple Raspberry pi, Arduino, STM32, ou Android) et des systèmes temps réel (dans le domaine de l'avionique, des automobiles, etc.) pour maîtriser leur administration et le développement d'applications.
    - Maîtrise des principes sous-jacents à la virtualisation de systèmes afin de faciliter l'intégration et l'administration de ce type de service dans un système informatique (Cloud Computing, Haute Disponibilité, Tolérance aux pannes, etc.).
  - **Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications (44,5 heures)**
    - Protection de l'accès aux données et protection des interfaces dans les systèmes
    - Protection dans les réseaux
    - Cryptographie
    - Protocoles de sécurité dans les réseaux
    - Mise en oeuvre des protocoles de sécurité

- **Cybersécurité, données et logiciels (105,5 heures)**
  - **Systèmes d'informations et bases de données (30,5 heures)**
    - Recueillir et analyser les besoins Connaître le cycle de développement des logiciels
    - Concevoir les MCD et MLD
    - Concevoir les applications (spécification de la solution et de la structure de la base de données)
  - **Paradigmes de programmation (FOAD , 30,5 heures)**
    - Paradigme objet, généricité, héritage et polymorphisme, introspection
    - Paradigme fonctionnel, lambda expressions, clôtures, objets persistants, promesses ; paradigme logique.
    - Divers langages de programmation : Java ou C# pour le paradigme objet, Javascript, Scala,Haskell ou Kotlin pour la programmation fonctionnelle, Prolog pour la programmation logique.
  - **Menaces informatiques et codes malveillants : analyse et lutte (44,5 heures)**
    - Phase de veille : comprendre les modes d'action pour prévoir les effets
    - Phase d'alerte : Détecter les effets des codes malveillants
    - Phase de réponse : minimiser, stopper ou réduire l'impact du code malveillant

- **Communication et entreprise (44,5 heures)**
  - **Anglais (37,5 heures)**
  - **Soutenance de stage (7 heures)**

- **Techniques de Recherche d'Emploi (14 heures)**

- **Stage en Entreprise (750 heures)**