Mise en œuvre de la sécurité numérique (DU)

CATEGORIE : C

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse :
- **Informatique**
- **Sécurité des systèmes d'informations**

Code(s) NAF : **—**
Code(s) NSF : **326**
Code(s) ROME : **M1810**, **M1806**, **M1805**, **M1802**, **M1801**
Formacode : **—**

Date de création de la certification : **01/03/2018**
Mots clés : **Systèmes**, **Réseaux**, **Informatique**, **Sécurité**

Identification

Identifiant : **3733**
Version du : **11/07/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **N/A**

Non formalisé :
- **Cybersécurité : les entreprises françaises à la traîne, mais plus pour longtemps**
- **La cybersécurité, ou sécurité des systèmes informatiques face aux attaques**
- **Cybersécurité : les peurs des entreprises françaises en 2018**

Descriptif

Objectifs de l'habilitation/certification

A travers cette formation, le candidat développe les compétences techniques et organisationnelles lui permettant d'appréhender ses futures missions en lien avec cette thématique.

Ainsi les principaux objectifs de la certification Mise en œuvre de la sécurité numérique (MSN) délivrée par l'UTT sont :

Tronc commun :

Compréhension des aspects juridiques des problèmes suscités par le développement des technologies de l'information et de l'internet (droit à la protection des données, droit du commerce électronique, droit de la propriété intellectuelle, droit de l'informatique sur le lieu de travail).
Connaissance des dispositions nouvelles du règlement européen sur la protection des données, et les conséquences opérationnelles pour les professionnels.
Connaissance des droits et obligations dans l'usage des technologies de l'information et de la communication.
Maîtrise des risques juridiques encourus par le représentant légal d'un organisme, l'employeur et les salariés.
Appréhension des moyens de protection des ressources et des données informatiques de l'entreprise.
Compréhension des enjeux de la SSI.
Connaissance des spécificités de l'analyse de risque et définition du périmètre de la donnée.
Sécurité Développement :

Conception sécurisée d'applications.
Implémentations des fonctions de sécurité.
Développement logiciel sans vulnérabilité.
Réalisation de tests de robustesse dans les logiciels développés.
Déploiement et intégration sécurisés d'applications.
Intégration de la sécurité dans les projets.

Sécurité des réseaux :

Conception et mise en place d'architectures sécurisées.
Durcissement de la configuration des équipements réseaux.
Mise en place de réseaux privés virtuels.
Compréhension des protocoles sécurisés et du protocole TLS.

Sécurité dans les projets :

Intégration de la sécurité informatique dans le projet.
Analyse du risque informatique et juridique.
Intégration de la sécurité dans la rédaction des documents.
Contrôle de la sécurité pendant la vie du projet et vérification de la sécurité à l'issue du projet.

Sécurité des systèmes industriels :

Déploiement sécurisé de réseaux industriels.
Compréhension des grands principes de sécurité et de la sécurité des équipements industriels.
Sensibilisation aux risques liés aux réseaux industriels.
Intégration de la sécurité dans les projets.
Développement de programmes automates simples.
Méthodologie et développement d'outils pour la réalisation de tests d'intrusion et d'audit en milieu industriel.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Absence de lien

Descriptif général des compétences constituant la certification

Les compétences constituant la certification du D.U Mise en œuvre de la sécurité numérique (MSN) sont les suivantes :

Tronc commun :

Module 1 :

Appliquer quotidiennement les normes inhérentes à l'informatique.
Assurer la protection des données et des ressources informatiques de l'entreprise en utilisant les normes réglementaires.
Module 2 :

Intégrer le risque cyber dans la Sécurité des Systèmes d'Information (SSI).

Option sécurité développement :

Module 1 :

Intégrer l'analyse des risques et la sécurité au sein de sa gestion de projet.
Module 2 :

Concevoir les spécifications fonctionnelles et techniques de l'application.
Implémenter les fonctions de sécurité de l'application.
Module 3 :

Public visé par la certification

- Salariés
- Demandeurs d'emploi

Programmer en sécurité en faisant face aux éventuels problèmes sur les applications web, les langages spécifiques et ceux liés aux systèmes.
Réaliser des tests de sécurité au sein des projets.
Module 4 :

Installer et intégrer la sécurité au sein des logiciels.
Option Sécurité des réseaux :

Module 1 :

Concevoir et mettre en place la sécurité dans les infrastructures réseau.
Configurer les équipements réseaux en durcissant les pratiques de sécurité.
Module 2 :

Mettre en place les protocoles sécurisés et TLS au sein des réseaux privés virtuels.
Module 3 :

Mettre en œuvre et déployer la sécurité au sein des infrastructures réseaux.
Option Sécurité dans les projets :

Module 1 :

Intégrer le respect des clauses de sécurité dans les contrats inhérents au projet.
Module 2 :

Intégrer la sécurité dans toutes les phases du projet en mettant en place des indicateurs sécurité.
Module 3 :

Assurer le contrôle régulier de la sécurité tout au long du projet.
Option sécurité des systèmes industriels :

Module 1 :

Réaliser le déploiement des protocoles de sécurité informatique dans les réseaux industriels.
Module 2 :

Intégrer une sécurité respectant les grands principes liés aux réseaux industriels.
Développer des programmes automates simples.
Module 3 :

Développer des outils pour la réalisation de tests d'intrusion et d'audits en milieu industriel.

Modalités générales

Durée de la certification : entre 56 heures à (soit 8 jours à raison de 7 heures par jour) et 70 heures (soit 10 jours à raison de 7 heures par jour), selon le suivi ou non du tronc commun

Organisation pédagogique : Le nombre d'heures d'enseignement est fixé à 70 heures en présentiel, soit 10 jours de formation, répartis comme suit :

Tronc commun : 14 heures, soit 2 jours
Option : 56 heures, soit 8 jours
La certification est dispensée en temps partagé (part time), à raison de 5 séquences de formation de 2

jours (1 pour le tronc commun, 4 pour les options), à raison d'une séquence toutes les 3 ou 4 semaines.

Le rythme d'enseignement pourra être modifié selon les demandes et besoins d'entreprises qui souhaiteraient organiser une session du DU au bénéfice de leurs seuls salariés.

Prérequis : Etre titulaire d'un diplôme de L3 ou équivalent, justifiant d'au moins 3 années d'expérience professionnelle.

Avoir répondu aux tests de positionnement / évaluation préalables des compétences pour permettre le positionnement du candidat sur la spécialisation du DU « Mise en œuvre de la sécurité numérique (MSN) », en relation avec son profil et son projet professionnel.

En fonction des résultats obtenus aux tests d'évaluation des compétences, les candidats pourront, soit intégrer les 10 jours de la certification (tronc commun + spécialisation), soit seront autorisés à intégrer directement les 8 jours correspondant à l'une des quatre options.

Conditions d'admission : L'admission au DU « Mise en œuvre de la sécurité numérique (MSN) » sera prononcée par un jury qui se déterminera sur la base d'un dossier de candidature, comprenant les éléments suivants :

Lettre de motivation
Curriculum vitae
Copie du diplôme le plus élevé
Dossier de candidature (cf. modèle joint au dossier)
Public cible selon chaque spécialisation :

Sécurité Développement : Développeurs, développeurs intégrateurs (DevOps), chefs de projets.

Sécurité des réseaux : Administrateurs réseau, Architectes réseaux, Chefs de projets.

Sécurité dans les projets :

Managers, décideurs, chefs de projets et rédacteurs de cahiers des charges ou toute personne concernée par l'intégration de sécurité dans les projets IT

Sécurité des systèmes industriels : Automaticiens, Responsables techniques, Responsables supervision, intégrateurs, Consultants et auditeurs en sécurité informatique

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Développer ses compétences dans la sécurité informatique dans la conception, le développement et la mise en production.
Développer ses compétences dans la sécurité des réseaux et des infrastructures.
Développer ses compétences dans la sécurité informatique appliquée à la gestion de projet.
Développer ses compétences dans la sécurité des systèmes rencontrés en milieu industriel.

Pour l'entité utilisatrice

Intégrer les composantes de la sécurité numérique face aux risques d'attaques.
Se protéger des attaques informatiques.
Préserver leur compétitivité.
Développer les compétences de leurs collaborateurs en matière de sécurité numérique.

Evaluation / certification

Pré-requis

Etre titulaire d'un diplôme de L3 ou équivalent, justifier d'au moins 3 années d'expérience professionnelle.

Compétences évaluées

Tronc commun :

C.1 Appliquer quotidiennement les normes inhérentes à l'informatique.
C.2 Assurer la protection des données et des ressources informatiques de l'entreprise en utilisant les normes réglementaires.
C.3 Intégrer le risque cyber dans la Sécurité des Systèmes d'Information (SSI).

Option 1 :

C.4 Intégrer l'analyse des risques et la sécurité au sein de sa gestion de projet.
C.5 Concevoir les spécifications fonctionnelles et techniques de l'application.
C.6 Implémenter les fonctions de sécurité de l'application.
C.7 Programmer en sécurité en faisant face aux éventuels problèmes sur les applications web, les langages spécifiques et ceux liés aux systèmes.
C.8 Réaliser des tests de sécurité au sein des projets.
C.9 Installer et intégrer la sécurité au sein des logiciels.

Option 2 :

C.4 Concevoir et mettre en place la sécurité dans les infrastructures réseau.
C.5Configurer les équipements réseaux en durcissant les pratiques de sécurité.
C.6 Mettre en place les protocoles sécurisés et TLS au sein des réseaux privés virtuels.
C.7 Mettre en œuvre et déployer la sécurité au sein des infrastructures réseaux.

Option 3 :

C.4 Intégrer le respect des clauses de sécurité dans les contrats inhérents au projet.
C.5 Intégrer la sécurité dans toutes les phases du projet en mettant en place des indicateurs sécurité.
C.6 Assurer le contrôle régulier de la sécurité tout au long du projet.

Option 4 :

C.4 Réaliser le déploiement des protocoles de sécurité informatique dans les réseaux industriels.
C.5 Intégrer une sécurité respectant les grands principes liés aux réseaux industriels.
C.6 Développer des programmes automates simples.
C.7 Développer des outils pour la réalisation de tests d'intrusion et d'audits en milieu industriel.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Absence de niveaux

Centre(s) de passage/certification

- Dans les locaux de l'EPITA : 24 Rue Marie Pasteur, Kremlin Bicêtre 94 270

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
La certification est matérialisée sous forme papier où il est inscrit : « Diplôme d'Université Mise en œuvre de la sécurité numérique »

Plus d'informations

Statistiques

Pour le tronc commun, le nombre d'inscrits est fixé à 8 participants mini et à 16 participants maxi par session.

Pour chacune des 4 spécialisations, le nombre d'inscrits est fixé à 5 participants mini et à 10 participants maxi par session.

Il y aura 2 sessions du tronc commun pour 1 session de chacune des 4 spécialisations.

Une première session de formation sera organisée à partir du mois d'octobre 2018.

A partir de 2019-2020 l'organisation de sessions supplémentaires sera réalisée.

Autres sources d'information

http://www-forum.utt.fr/