Piloter une démarche de cybersécurité

CATEGORIE : C

Vue d'ensemble

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

Transverse :
- **Domaines concernés : ingénierie, grands projets internes, conseil (tous secteurs d'activité), informatique, gestion des risques**

Tous les domaines d'activité impliquant des systèmes informatiques sont concernés notamment ceux impliquant des systèmes complexes.

Code(s) NAF : **—**
Code(s) NSF : **—**
Code(s) ROME : **M1806**, **M1805**, **M1803**, **M1802**, **M1801**
Formacode : **31006**

Date de création de la certification : **01/08/2016**
Mots clés : **sécurité informatique**, **DIGITAL**, **Cryptologie**, **Cybersécurité**

Identification

Identifiant : **2341**
Version du : **05/01/2017**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Pas de consensus formalisé**

Non formalisé :
- **Développer la cybersécurité est devenue indispensable pour toutes les entreprises qui opèrent leur transformation numérique. Le niveau des menaces ne cesse de s'accroître au fur et à mesure du développement technologique. Elle permet de protéger, les machines, les personnes, les opérations,... la compétence concerne la capacité à concevoir et à mettre en œuvre des dispositifs sécurisants et à piloter des spécialistes amenés à les réaliser.**

Descriptif

Objectifs de l'habilitation/certification

Validation des capacités à identifier de potentielles menaces et proposer des solutions

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- NS

Descriptif général des compétences constituant la certification

Etre capable de :

Avoir une connaissance permanente de l'état de l'art (menaces et solutions de sécurité)
Présenter, cartographier les voies d'attaques du logiciel au matériel et les différentes techniques de sécurisation
Appréhender les questions techniques relatives à l'emploi de la cryptographie dans les infrastructures modernes de traitement de l'information
Proposer des choix de conception et de dimensionnement des principaux algorithmes utilisés
Savoir choisir des outils adaptés en fonction des types de menace
Savoir piloter et superviser les acteurs chargés de mettre en œuvre la sécurisation des systèmes.

Public visé par la certification

- Ingénieurs de développement, chefs de produit, managers technique, consultants, informaticiens, responsables informatiques

Modalités générales

Production d'un mémoire sur une ou des réalisations en situation réelle présenté à un jury de professionnels et/ou recueil de preuves. C'est en effet la preuve de leur mise en application qui permet de vérifier la réalité des compétences requises.

Un parcours de formation, hors de l'entreprise ou dans l'entreprise, est mis à disposition de ceux et celles qui souhaiteront renforcer leurs compétences. Il cible les principales compétences certifiables, par modules de 2 à 3 jours, principalement sous forme de partage et d'analyse d'expériences. Ce parcours peut servir à faciliter la mise en place de solution de cybersécurité et à l'élaboration du mémoire.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Cette certification est une reconnaissance que la personne a acquis les compétences nécessaires pour identifier des menaces et proposer des solutions adaptées. C'est un champ en plein essor qui permet de sécuriser notre environnement quotidien tant la gestion des données, les objets connectés font partie intégrante de ce dernier.

Pour l'entité utilisatrice

Cette certification garantit l'entité utilisatrice que les compétences de la personne la rendent apte à anticiper, cartographier les menaces potentielles et aussi à mettre en œuvre les solutions sécurisantes adaptées.

Elle permet de ce fait de favoriser une diffusion des solutions dans de nombreux domaines, ce qui favorise sa capacité d'innovation en lui permettant d'y trouver un relais de croissance.

Evaluation / certification

Pré-requis

Diplôme d'ingénieur (ou équivalent) ou expérience professionnelle dans l'industrie équivalente

Compétences évaluées

Avoir une connaissance de l'Etat de l'art (menaces et solutions de sécurité)
Présenter, cartographier les voies d'attaques du logiciel au matériel et les différentes techniques de sécurisation

Centre(s) de passage/certification

- Ecole Polytechnique Executive Education

Appréhender les questions techniques relatives à l'emploi de la cryptographie dans les infrastructures modernes de traitement de l'information
Proposer des choix de conception et de dimensionnement des principaux algorithmes utilisés en pratique
Savoir choisir des outils adaptés en fonction de menace
Savoir piloter et superviser des acteurs chargés de mettre en œuvre des systèmes sécurisés

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

NS

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Certificat de compétence délivré par l'Ecole Polytechnique Executive Education

Plus d'informations

Statistiques

Entre 20 et 40 personnes par an

Autres sources d'information

Brochure papier et électronique détaillant : les objectifs, les conditions d'accès, le référentiel de compétences, le programme de formation, les conditions de certification
Site Web : Ecole Polytechnique Executive Education (http://exed.polytechnique.edu/fr)