Architecture Cybersécurité

CATEGORIE : C

Vue d'ensemble

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

Spécifique :
- **Support à l'entreprise - Systèmes d'information et de télécommunication**

Code(s) NAF : **62.02A**
Code(s) NSF : **326**
Code(s) ROME : **M1801**, **M1802**, **M1804**, **M1805**, **M1803**
Formacode : **31006**

Date de création de la certification : **01/09/2017**
Mots clés : **Architecture**, **Cybercriminalité**, **Cyber sécurité**, **SECURITE**

Identification

Identifiant : **3115**
Version du : **19/10/2017**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Une composante issue du Mastère Spécialisé labellisé par l'ANSSI au titre du SECNUMEDU**
- **Définition des Opérateurs d'Importance Vitale (OIV) nécessitant la mise en place de systèmes de cybersécurité**
- **BADGE (Brevet d'Aptitude Délivré par les Grandes Ecoles) - Architecte Cybersécurité**

Non formalisé :
- **Estimation ANSSI : seuls 25% des besoins en sécurité numérique sont pourvus**
- **Création d'un pôle cyberdéfense par Orange pour faire face à la pénurie de talents**
- **Les métiers de la cybersécurité ne savent plus comment recruter**
- **Estimation par CISCO du nombre d'emplois à pourvoir en cybersécurité dans le monde**
- **Quand les compétences en cybersécurité se font rares**

Descriptif

Objectifs de l'habilitation/certification

Il s'agit de former les professionnels

exerçant déjà un métier dans le secteur des NTIC et n'ayant aucune expertise dans le domaine de la Sécurité Numérique ;
des métiers de l'intégration sécurisée ;
aux compétences nécessaires à l'exercice de fonctions d'Architecte spécialisé en Cybersécurité. A l'issue de cette formation, il leur sera possible de concevoir des architectures sécurisées et de comprendre de façon transverse les enjeux de la sécurité des structures et organisations. A ce titre, la formation intervient en complément

des métiers existant traditionnellement dans le domaine informatique / télécoms / réseaux, en proposant aux architectes informatiques d'acquérir des compétences en sécurité et ainsi accompagner leur reconversion professionnelle ;
des métiers de l'intégration sécurisée, en proposant aux experts techniques en sécurité une vue globale et transverse sur les architectures et les systèmes de sécurité, ainsi que leur place dans les organisations.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Préventeur(trice) en cybersécurité des systèmes d'informations (CQPM)

Descriptif général des compétences constituant la certification

La formation est construite suivant 2 composantes :

Architecture

1. Auditionner et évaluer le niveau de sécurité des architectures à déployer et existantes
2. Structurer les choix technologiques et méthodologiques d'un ensemble répondant à des exigences de sécurité
3. S'assurer de la déclinaison optimale des exigences fonctionnelles et techniques spécifiques à la sécurité
4. Identifier et valider la cartographie en s'assurant que les hypothèses de sécurité de son architecture sont clairement énoncées et prises en compte dans sa conception
5. Concevoir les nouvelles architectures sécurisées des solutions cibles
6. Vérifier que les exigences de sécurisation sont effectivement déclinées
7. Fournir la connaissance de l'état de l'art des architectures sécurisées
8. Rédiger les dossiers de conception et de justification

Management

1. Bénéficier d'un panorama complet de la sécurité
2. Appréhender la gestion projet : gérer une réponse à appel d'offre dans le cadre d'une architecture sécurisée
3. Identifier les outils nécessaires au bon déroulement d'un projet de sécurité
4. Comprendre les bases juridiques et de la réglementation d'un projet

Public visé par la certification

- Professionnels des NTIC salariés
- Professionnels des NTIC demandeurs d'emploi

de sécurité
5. Appréhender les enjeux d'une communication optimale en cas de gestion de crise de sécurité

Modalités générales

D'une durée de 188 heures, la formation se déroule en alternance (cours les jeudis / vendredis et les vendredis / samedis) sur une durée de 14 mois. Dotée d'une forte composante projets, elle se veut pragmatique et orientée métier d'architecture en sécurité des systèmes d'information, pouvant être exercée en parallèle d'une activité en entreprise.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Formation diplômante en Sécurité Numérique : obtention d'un titre reconnu par le marché (Brevet d'Aptitude Délivré par les Grandes Ecoles) sur un marché en forte expansion (celui de la Cybersécurité)
Offrant d'importantes perspectives en terme d'employabilité et de carrière
Pragmatique, répondant aux besoins du marché (formation conçue avec et pour les professionnels)
Haut degré d'expertise des partenaires & intervenants (notamment via un partenariat avec la société CapGemini / Sogeti)
Favorisant des emplois porteurs & non délocalisables
et ce, via :

La maîtrise de tous le processus de conception d'une architecture sécurisée d'une solution SI : architectures systèmes, réseaux et applicatives
La connaissance d'une culture transverse de la sécurité numérique, des enjeux de la cyberdéfense et de la sybercrimminalité sur un ensemble de secteurs d'activité varié : banques/assurances, industrie, institutionnels
La connaissance des stratégies, objectifs, processus et du management de la sécurité

Pour l'entité utilisatrice

Très forts besoins pour requalifier / recycler des profils issus des technologies de l'information et de la communication devenus obsolètes, vers des métiers de la sécurité numérique en plein essor

Evaluation / certification

Pré-requis

Bénéficier de connaissances dans le domaine informatique, des télécommunication ou des réseaux
Détenir un diplôme de type Master 2 (BAC+5) ou équivalent
Détenir un diplôme de type Master 1 (BAC+4) ou équivalent et justifier d'une expérience professionnelle de 3 ans minimum

Centre(s) de passage/certification

- http://formation-continue.isep.fr/

Détenir un diplôme de type Master 1 (BAC+4) ou équivalent sans justifier d'une expérience professionnelle ou détenir un diplôme de type Licence (BAC+3) et justifier d'une expérience professionnelle de 3 ans minimum, via régime dérogatoire (30% des effectifs maximum)
Autres cas : via un entretien pour valider les acquis professionnels (10% des effectifs)

Compétences évaluées

L'ensemble des compétences précitées sont évaluées au moyen de contrôles de connaissances proposés par les intervenants :

Architecture

1. Auditionner et évaluer le niveau de sécurité des architectures à déployer et existantes :

Cohérence de la démarche, respect de la méthodologie, exhaustivité de l'analyse, identification des points à risques, validation lors de mises en situation

2. Structurer les choix technologiques et méthodologiques d'un ensemble répondant à des exigences de sécurité :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, pertinence des choix d'équipements, validation lors de mises en situation

3. S'assurer de la déclinaison optimale des exigences fonctionnelles et techniques spécifiques à la sécurité :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, justification de la pertinence des choix effectués, validation lors de mises en situation

4. Identifier et valider la cartographie en s'assurant que les hypothèses de sécurité de son architecture sont clairement énoncées et prises en compte dans sa conception :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, exhaustivité de l'analyse, validation lors de mises en situation

5. Concevoir les nouvelles architectures sécurisées des solutions cibles :

Démonstration de la viabilité technicoéconomique des architectures, du niveau d'adéquation avec le besoin exprimé, justification de la pertinence des choix effectués, validation lors de mises en situation

6. Vérifier que les exigences de sécurisation sont effectivement déclinées :

Définition des priorités, exhaustivité de l'analyse, cohérence de la démarche, respect de la méthodologie

7. Fournir la connaissance de l'état de l'art des architectures sécurisées :

Vérification de connaissances

8. Rédiger les dossiers de conception et de justification :

Validation de la structure documentaire, exhaustivité, validation fond et forme lors de mises en situation

Management

1. Gérer un projet de sécurité complexe :

Validation de la démarche projet lors de mises en situation

2. Anticiper, identifier et gérer les risques :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

3. Appréhender les enjeux humains, organisationnels et juridiques :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

4. Les outils du Manager pour communiquer et faire adopter ses idées :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

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

Obtention d'un BADGE® (Brevet d'Aptitude Délivré par les Grandes Ecoles), diplôme délivré par la Confédération des Gandes Ecoles.

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Remise du Brevet d'Aptitude Délivré par les Grandes Ecoles : BADGE Architecte Cybersécurité

Plus d'informations

Statistiques

Entre 5 et 10 personnes certifiées par an.

Autres sources d'information

Pour en savoir plus : http://formation-continue.isep.fr/architecture-cyber-securite-et-integration (focus ARCHITECTURE)