Intégration 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**

Elle concerne plus particulièrement les ESN (Entreprises de Service Numérique), intervenant sur l'ensemble des secteurs d'activité.

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

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

Identification

Identifiant : **3116**
Version du : **20/11/2017**

Références

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

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'architecture sécurisée ;
aux compétences nécessaires à l'exercice de fonctions d'Intégrateur spécialisé en Cybersécurité. A l'issue de cette formation, il leur sera possible de connaître les systèmes, sous-systèmes et composants de sécurité à la fois physiques et virtuels, appréhender les enjeux et méthodologies des projets d'intégration sécurisée ainsi que de bénéficier d'une dimension juridique et managériale. A ce titre, la formation intervient en complément

des métiers existant traditionnellement dans le domaine informatique / télécoms / réseaux, en proposant aux intégrateurs informatiques d'acquérir des compétences en sécurité et ainsi accompagner leur reconversion professionnelle ;
des métiers de l'architecture sécurisée, en proposant aux experts fonctionnels en sécurité une vue technique sur les systèmes de sécurité, ainsi que leur principaux processus et composants.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Non

Descriptif général des compétences constituant la certification

La formation est construite suivant 2 composantes :

Intégration

1. Mettre en oeuvre des solutions de sécurité (services, fonctionnalité de sécurité, plateforme d'intégration) dans les nouvelles architectures et celles existantes
2. Planifier et coordonner les actions issues des exigences d'intégration exprimées
3. Installer des composants matériels, des composants logiciels ou des soussystèmes supplémentaires de sécurité dans un système existant ou en cours de développement
4. Respecter les processus et procédures afin de garantir intégrité et interopérabilité des solutions sécurisées
5. Qualifier et intégrer les solutions sécurisées dans l'environnement de production
6. Documenter les processus de mise en oeuvre, de mise à jour et d'exploitation des composants de sécurité
7. Organiser les conditions de mise en oeuvre du maintien en condition de sécurité

Management

1. Appréhender les enjeux du management d'équipe
2. Appréhender la méthodologie et les enjeux de la gestion de projets de sécurité
3. Identifier les outils nécessaires au bon déroulement d'un projet
4. Etre initié aux bases juridiques et de la règlementation

Public visé par la certification

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

Modalités générales

D'une durée de 164 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'intégration 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 d'intégration sécurisée d'une solution SI : infrastructures sécurisées, serveurs, terminaux et techniques pour l'intégration
La connaissance d'une composante gestion de projets d'intégration en sécurité informatique
La connaissance d'une composante gestion d'équipe en environnement projets de sécurité informatique
La connaissance des mécanismes de communication en période de crise de 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
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

Centre(s) de passage/certification

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

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

Architecture

1. Mettre en oeuvre des solutions de sécurité (services, fonctionnalité de sécurité, plateforme d'intégration) dans les nouvelles architectures et celles existantes :

Cohérence de la démarche, respect de la méthodologie, vérification de connaissances, analyse de l'existant

2. Planifier et coordonner les actions issues des exigences d'intégration exprimées :

Vérification du niveau de priorité accordé aux actions, respect de la démarche projet, validation de l'avancée projet en situation

3. Installer des composants matériels, des composants logiciels ou des soussystèmes supplémentaires de sécurité dans un système existant ou en cours de développement :

Respect de la méthodologie, vérification de connaissances, analyse de l'existant, anticipation des risques, validation lors de mises en situation

4. Respecter les processus et procédures afin de garantir intégrité et interopérabilité des solutions sécurisées :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

5. Qualifier et intégrer les solutions sécurisées dans l'environnement de production :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

6. Documenter les processus de mise en oeuvre, de mise à jour et d'exploitation des composants de sécurité :

Structure documentaire, exhaustivité, validation fond et forme lors de mises en situation

7. Organiser les conditions de mise en oeuvre du maintien en condition de sécurité :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

Management

1. Gérer un projet de sécurité complexe :

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

2. Appréhender les enjeux humains en temps de crise :

Contrôle de connaissances, validation de la démarche projet

lors de mises en situation

3. Appréhender les enjeux juridiques :

Contrôle de connaissances

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 Intégration 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 INTEGRATION)