Implémenter la cybersécurité en entreprise

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**

Cette certification peut être utilisée dans tout secteur d'activité.

Code(s) NAF : **—**
Code(s) NSF : **326**
Code(s) ROME : **M1801**, **M1805**
Formacode : **31006**

Date de création de la certification : **25/01/2016**
Mots clés : **AUDIT**, **Cybersécurité**, **protection**, **SECURITE**

Identification

Identifiant : **3068**
Version du : **19/10/2017**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **L'ANSSI répertorie les compétences en sécurité des SI et des réseaux et en fait une priorité**
- **Les entreprises classées OIV (Organisme d'Importance Vitales) sont poussées par l'Etat pour mettre en place des systèmes de cybersécurité ce qui induit naturellement l'émergence de nouveaux besoins en formation et en compétences**

Non formalisé :
- **La cyberdéfense : un enjeu mondial, une priorité nationale**
- **Des informaticiens prêts à développer leurs compétences pour investir le domaine de la cybersécurité**

Descriptif

Objectifs de l'habilitation/certification

Les objectifs de la certification visent à permettre au candidat de :

• Réaliser des diagnostics des systèmes d'information pour chercher les points faibles du système
• Trouver des solutions pour lutter contre les failles du système pour protéger et sécuriser les données de l'entreprise

- Mettre en place des processus de sécurité
- Actualiser les processus de sécurité en fonction des nouvelles technologies

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- aucun

Descriptif général des compétences constituant la certification

La certification couvre les principales compétences permettant à un consultant en cybersécurité d'auditer en amont comme en aval les systèmes d'information intranet et extranet pour déceler d'éventuelles failles de sécurité et autres vulnérabilités. Ces compétences sont rares, ne serait-ce que par l'évolution exponentielle des méthodes et outils de protection mis en œuvre.
Les compétences visées par cette certification sont :

- Maîtriser une séquence d'audit du système d'information.
- Maîtriser l'ensemble des assets à surveiller.
- Ordonnancer, piloter et coordonner le projet un projet de sécurisation d'un système.
- Fédérer et animer une équipe projet.
- Sécuriser des données de l'entreprise.
- Actualiser les processus de sécurité en fonction des nouvelles technologies et maîtriser les tests d'intrusion.
- Vérifier le système protégé.

Public visé par la certification

- Tout public, salariés comme demandeurs d'emploi
- Les demandeurs d'emploi sont les principales cibles de cette certification, elle leur assure un taux d'employabilité à la sortie de formation de 97%.

Modalités générales

2 sessions de formation sont organisées par an. Une session de formation est composée de différents modules répartis sur 196 heures de formation. Les formations mêlent théorie et pratique au travers de cas concret afin de préparer au mieux les candidats à la réalité de terrain. Pour ce faire, Fitec fait intervenir des formateurs experts dans le domaine. La certification permet l'accès aux activités suivantes :

Réalisation de diagnostics des systèmes d'information pour chercher les points faibles du système.
Conduite de projet.
Animation de réunions.
Mise en place de solutions pour lutter contre les failles du sytème afin de protéger et sécuriser les données de l'entreprise.
Utilisation d'outils de surveillance.
Mise en place de processus de sécurité.
Vérification du système.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Actualisation des processus de sécurité en fonction

Pour l'entité utilisatrice

Obtention d'un gage de professionnalisme dans ce

des nouvelles technologies.
Contribution à l'employabilité dans un domaine en tension.
Valorisation de son parcours et de ses compétences dans le secteur de la cybersécurité.
Maîtrise des processus et des technologies liés à des enjeux stratégiques.
Mise en œuvre d'une politique de protection décidée par le/la DSI de l'entreprise.

domaine, vis-à-vis des clients finaux.
Mise en place d'un système de protection des données.
Sécurisation des données internes à l'entreprise.

Evaluation / certification

Pré-requis

Titulaire d'un Bac +4/5 en informatique, ou issue d'une filière Juriste ou détenteur d'un bac +2 avec une expérience professionnelle dans le domaine.

Compétences évaluées

L'ensemble des compétences sont évaluées.

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

aucun niveau

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Document Fitec « Certificat de Compétences », spécifiant l'intitulé de la certification, les compétences acquises, la date d'examen, le visa du directeur du Centre et la mention obtenue.

Centre(s) de passage/certification

- FITEC, 6 bd de Pesaro, 92000 Nanterre

Plus d'informations

Statistiques

En 2016, 36 personnes ont suivi la formation.

A ce jour, 16 candidats ont suivi la formation.

Autres sources d'information

https://www.fitec.fr/

https://www.devenez.fr

https://www.fitec-formation.fr/