Architecture en cybersécurité

CATEGORIE : B

Vue d'ensemble

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

Transverse : ■ **Support à l'entreprise — Systèmes d'information et de télécommunication**

La certification concerne la sécurité des systèmes d'information et des réseaux de télécommunication des entreprises, elle est donc transverse à tous les secteurs économiques

Code(s) NAF : —

Code(s) NSF : **326n**

Code(s) ROME : **M1806**, **M1804**, **M1803**, **M1801**

Formacode : **31006**

Date de création de la certification : **01/01/2014**

Mots clés : **Sécurité des réseaux**, **Contrôle d'accès**, **Cybersécurité**, **Cyberdéfense**

Identification

Identifiant : **1753**

Version du : **08/02/2016**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Les entreprises classées OIV \(Organisme d'Importance Vitales\) sont poussées par l'Etat à mettre en place des systèmes de cybersécurité ce qui induit naturellement l'émergence de nouveaux besoins en formation et en compétence](#)
- [L'ANSSI répertorie les compétences en sécurité des SI et des réseaux et en fait une priorité](#)

Non formalisé :

- [La cyberdéfense : un enjeu mondial, une priorité nationale](#)
- [Recrutement, Formation, Compétences : 3 priorités pour disposer des compétences en cybersécurité nécessaires dans la durée](#)

Norme(s) associée(s) :

—

Descriptif

Objectifs de l'habilitation/certification

Vérifier l'acquisition et la maîtrise des connaissances et **compétences théoriques, techniques et**

organisationnelles nécessaires à la définition, au déploiement et à la **gestion d'une architecture de sécurité**, pour des professionnels susceptibles d'exercer des responsabilités en lien avec la **sécurité des systèmes d'information et des réseaux**.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification vérifie la capacité à :

- C1. Concevoir une architecture de cybersécurité
- C2. Définir une politique de gestion des identités et des autorisations
- C3. Piloter un audit de la politique de cybersécurité et de vulnérabilité
- C4. Prendre en compte les résultats d'un audit de sécurité et de vulnérabilité
- C5. Définir la politique de cybersécurité liée à l'externalisation des données du Cloud

Public visé par la certification

- salariés
- demandeurs d'emplois
- jeunes diplômés

Modalités générales

La certification est accessible à la suite d'une formation de **25 jours soit 150 heures**. Elle se déroule sur une période de **6 mois** et est organisée pour permettre la **poursuite de l'activité professionnelle**.

Démarche pédagogique :

Une formation en réponse aux nouveaux besoins des acteurs du domaine, validée par un comité de veille et assurée par des experts reconnus. La formation alterne :

- Enseignements académiques
- Acquisition de savoir-faire au travers de retours d'expérience
- Travaux pratiques
- Projet personnel d'application concrétisé par la rédaction et la soutenance d'un mémoire professionnel

Liens avec le développement durable

niveau 1 : Certifications et métiers qui internalisent le développement durable. Les activités et compétences mobilisées mettent en oeuvre des matériaux et produits moins polluants

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Perspectives de carrière attrayantes dans de multiples branches professionnelles
Volet de travaux pratiques garantissant le caractère opérationnel de la certification
Caractère scientifique pointu permettant aux certifiés de développer des capacités de compréhension des outils nécessaires pour s'adapter à leurs évolutions dans le temps
Réseau des anciens diplômés

Pour l'entité utilisatrice

Emploi de professionnels opérationnels et capables de s'adapter aux évolutions d'un secteur hyperconcurrentiel
Légitimité, professionnalisme et partenariats d'une école d'ingénieurs de renom membre de l'institut Mines Télécom

Evaluation / certification

Pré-requis

Techniciens et ingénieurs avec expérience professionnelle en sécurité des systèmes et des réseaux ou master 2 réseaux avec formation de base en sécurité ou formation en sécurité équivalente au CES
Consultant Sécurité Systèmes et Réseaux délivré par Télécom SudParis

Compétences évaluées

CE1a **Concevoir une architecture de cybersécurité** en tenant compte des contraintes (organisationnelles, financières, humaines, juridiques) afin d'élaborer des solutions adaptées aux besoins du système cible

CE1b **Déployer une architecture globale de cybersécurité** en communiquant les informations techniques adéquates aux acteurs clés du déploiement afin de mettre en place des solutions adaptées au système cible

CE2. **Définir une politique de gestion des identités et des autorisations** en tenant compte des besoins et des contraintes spécifiques du système

CE3. **Piloter un audit de la politique de cybersécurité et de vulnérabilité** afin d'évaluer le degré de sécurité d'un système cible

CE4. **Prendre en compte les résultats d'un audit de sécurité et de vulnérabilité** en préconisant des mesures correctives afin d'améliorer le degré de sécurité d'un système cible

C5. **Définir la politique de cybersécurité liée à l'externalisation des données** du Cloud en fonction des avantages et des contraintes identifiés afin de répondre aux besoins du système cible

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

Absence de niveau

La validité est Permanente

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Certificat d'Etudes Spécialisées de Télécom Bretagne

Centre(s) de passage/certification

- L'institut certificateur est Telecom Bretagne :
<http://www.telecom-bretagne.eu/>

Plus d'informations

Statistiques

Absence de statistiques

Autres sources d'information

<http://ces.telecom-evolution.fr/cybersecurite/> ;

<http://ces.telecom-evolution.fr/architecte-cybersecurite/programme-du-ces-architecte-cybersecurite/>

<http://ces.telecom-evolution.fr/wp-content/uploads/2014/04/Plaque-CES-Cybers--curit--.pdf>