

Architecture en cybersécurité

RS1753 · RS · Publiée

L'essentiel

Code(s) NSF	326n
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

INSTITUT MINES TELECOM - TELECOM BRETAGNE · SIRET : 18009202500030

Résumé de la certification

OBJECTIFS ET CONTEXTE

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

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.

COMPÉTENCES ATTESTÉES

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
- 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 clefs 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

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

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

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<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/Plaquette-CES-Cybers--curit--.pdf>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/1753/>

Demande CPF — formations engagées

Dossiers CPF engagés	8
Montant total engagé	30 906 €
Coût moyen par dossier	3 863 €
Durée moyenne	346 h
Période	05/2020 – 04/2021
France compétences	75 %
Reste à charge titulaire	25 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.