

Architecte réseaux et cybersécurité (MS)

RNCP32121 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	14297, 24273
Code(s) ROME	M1801, M1802, M1803, M1804, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	04/01/2024

Certificateur(s)

INSTITUT MINES TELECOM - TELECOM PARIS · SIRET : 18009202500162

Résumé de la certification

OBJECTIFS ET CONTEXTE

A compléter (Reprise)

ACTIVITÉS VISÉES

L'architecte réseaux et cybersécurité est un métier essentiel dans les organisations modernes. Son expertise lui permet de piloter la conception d'une architecture réseau (la partie matérielle du réseau), de définir l'architecture d'un système d'information (la partie logicielle) et de créer une architecture de cybersécurité, prenant en compte les choix fait au niveau du réseau et du système d'information.

Activités visées par le titre :

- Réalisation de l'architecture d'un réseau télécom de transport de données
- Réalisation de l'architecture d'un système d'information ou d'un service applicatif
- Réalisation de l'architecture cybersécurisée d'un réseau ou d'un système d'information
- Pilotage et réalisation d'un projet du domaine de la cybersécurité

COMPÉTENCES ATTESTÉES

- Réaliser l'architecture d'un réseau télécom de transport de données sur la base des besoins du client interne ou externe et des enjeux de sécurité et d'évolution future
- Réaliser l'architecture d'un système d'information ou d'un service applicatif de manière à assurer son fonctionnement pérenne et ses évolutions selon les besoins du client
- Réaliser l'architecture cybersécurisée d'un réseau ou d'un SI en mettant en œuvre des méthodes et techniques préventives et palliatives, répondant aux enjeux de sécurité et aux obligations légales du client
- Piloter et réaliser un projet de développement de la cybersécurité d'un réseau ou d'un SI, en s'appuyant sur des équipes techniques internes et des sous-traitants

Blocs de compétences

RNCP32121BC01 — Réaliser l'architecture d'un système d'information ou d'un service applicatif de manière à assurer son fonctionnement pérenne et ses évolutions à venir, selon les besoins du client

LISTE DE COMPÉTENCES

Compétences évaluées :

- Décrire le modèle de représentation du SI le plus conforme aux besoins, en soumettant des solutions pour adapter le réseau de l'entreprise en conséquence

- Définir une organisation pour assurer le maintien en bon fonctionnement du SI et son évolution, en respectant la structure existante et les contraintes qui lui sont liées
- Définir les performances applicatives relatives à l'évolution du SI, de façon à adapter l'écosystème du Cloud selon le contrat de service, et faire valoir les arguments auprès de la direction

Modalités d'évaluation :

- Tests d'acquisition des connaissances, ou QCM (questions à choix multiples)
- Projets pédagogiques : projet d'une conception technique et sécurisée d'un service, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement
- Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : mise en place d'une solution SI sécurisée

RNCP32121BC02 — Réaliser l'architecture cybersécurisée d'un réseau ou d'un SI en mettant en œuvre des méthodes et techniques préventives et palliatives, répondant aux enjeux de sécurité et aux obligations légales

LISTE DE COMPÉTENCES

Compétences évaluées :

- Mettre en œuvre une méthode adaptée, en fonction du SI, de restitution des failles de sécurité, en signalant des recommandations plausibles, selon le contexte de l'entreprise
- Mettre en œuvre des solutions techniques et organisationnelles pour pallier les risques élémentaires, en élaborant les solutions de contrôle des accès, et en protégeant le réseau de la corruption des données
- Mettre en place une architecture cybersécurisée qui puisse détecter et filtrer les programmes malveillants, afin de lutter contre les menaces persistantes avancées

Modalités d'évaluation

- Tests d'acquisition des connaissances, ou QCM (questions à choix multiples)
- Projets pédagogiques : projet d'une conception technique et sécurisée d'un service, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement
- Cas pratique : conception d'une architecture de sécurité, mise en place d'un audit de sécurité
- Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : mise en place d'une solution SI sécurisée

RNCP32121BC03 — Piloter un projet de développement de la cybersécurité d'un réseau et / ou d'un SI, en s'appuyant sur des équipes techniques internes et des sous-traitants

LISTE DE COMPÉTENCES

Compétences évaluées :

- Elaborer un plan de recrutement de l'équipe projet, en s'appuyant sur les enjeux, les produits à livrer, les contraintes de coût, délai et qualité identifiés, afin d'obtenir l'accord de la hiérarchie
- Etablir les critères de sélection des fournisseurs en prenant en compte les objectifs de réalisation du projet, les besoins exprimés, et en analysant les transcrits des soutenances
- Réaliser le plan de gestion du projet, en ordonnant les tâches, en dressant une cartographie réaliste des risques et des palliatifs, en déterminant les éléments de coût-délai-qualité, et en communiquant sur les actions mises en œuvre

Modalités d'évaluation :

- Tests d'acquisition des connaissances, ou QCM (questions à choix multiples)
- Projet pédagogique : réponse à l'appel d'offres d'un client
- Cas pratique : conception d'une architecture de sécurité
- Travaux de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : élaboration d'une architecture télécom, fixe ou mobile, mise en place d'une solution SI sécurisée, définition du calendrier des processus du projet, organisationnels et techniques, description des livrables d'un projet

RNCP32121BC04 — Réaliser l'architecture d'un réseau télécom de transport de données, sur la base des besoins du client interne ou externe, des enjeux de sécurité et des évolutions à venir

LISTE DE COMPÉTENCES

Compétences évaluées :

- Analyser et élaborer une architecture de réseau d'entreprise, de réseau d'accès fixe, et de réseau cœur de transport, cuivre, optique ou hertzien, en considérant les évolutions de trafic, du matériel, et de la technologie.

- Analyser et élaborer une architecture de réseau radiomobile de type 4G, en prenant en compte le développement de la capacité des trafics, et en anticipant les évolutions vers la 5G, notamment celles liées aux services des objets connectés.
- Définir les solutions vraisemblables aux dysfonctionnements courants de la qualité de service, notamment ceux liés aux flux du trafic et à la garantie de l'accès au service.

Modalités d'évaluation :

- Tests d'acquisition des connaissances, ou QCM (questions à choix multiples)
- Projets pédagogiques : réponse à l'appel d'offres d'un client, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement.
- Cas pratique : atelier de sécurisation d'un réseau mobile
- Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : élaboration d'une architecture télécom, fixe ou mobile.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'architecte réseaux et cybersécurité est amené à travailler dans les grandes entreprises, les opérateurs télécoms, les constructeurs ou équipementiers télécoms, les sociétés de services numériques (ESN). De façon générale, il peut exercer ses activités dans les DSI (direction du service d'information) de n'importe quelle entreprise de taille suffisante.

TYPE D'EMPLOIS ACCESSIBLES

Architecte réseaux, Architecte cybersécurité et blockchain, Responsable sécurité informatique, Chef de projet SI, Analystes et experts réseaux et SI

RÈGLEMENTATIONS D'ACTIVITÉ

A compléter (Reprise)

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 962 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	34 624
Jugés difficiles à recruter	52 %

Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

A compléter (Reprise)

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, CONTRAT DE PROFESSIONNALISATION

6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés

COMPOSITION DU JURY — VAE

Par VAE, 6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés

Base légale

Date d'échéance de l'enregistrement	04/01/2024
-------------------------------------	------------

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RNCP38140

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

« Les formations et les compétences en France sur la cybersécurité », étude FAFIEC, mai 2017 - www.fafiec.fr
Site de Télécom ParisTech pour le MS

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/32121/>

Entrées et sorties de formation

Entrées en formation	22
Parcours menés à terme	24
Taux d'achèvement	109 %
Période	12/2022 – 06/2024

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	26
Montant total engagé	247 165 €

Coût moyen par dossier	9 506 €
Durée moyenne	596 h
Période	09/2020 – 12/2023
Entreprise	56 %
France compétences	36 %
Reste à charge titulaire	4 %
France Travail	3 %

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