

Spécialiste en cybersécurité

RNCP37987 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	20/09/2023
Date d'échéance	20/09/2026

Certificateur(s)

CSB EDUCATION GROUP · SIRET : 92991594000019

CYBERSECURITY BUSINESS SCHOOL · SIRET : 91090511600026

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION D'ENSEIGNEMENT TECHNIQUE SUPERIEUR AN21 ACADEMIE NUMERIQUE DU XXIEME SIECLE	8513778460 0023	Former et organiser l'évaluation
CSB EDUCATION GROUP	9299159400 0019	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La cybersécurité est un élément essentiel dans la transformation numérique en cours, ce que nous rappellent des cyberattaques qui gagnent en volume, en impact et en sophistication. Elle est essentielle afin de préserver la confidentialité, l'intégrité et la disponibilité des systèmes, des réseaux informatiques et des données. La cybersécurité est omniprésente ; tous les secteurs se dématérialisent et ont l'obligation de mettre en œuvre les technologies et d'attirer et de former les talents indispensables à leur protection.

La cybersécurité représente également un véritable avantage concurrentiel pour des organisations qui doivent la prendre en compte dans l'élaboration de leur stratégie. Avec l'arrivée des nouvelles technologies de l'information et de la communication (NTIC) telles que l'internet, le cloud computing, l'intelligence artificielle, les objets connectés, la cybersécurité s'impose comme un sujet transverse qui englobe la sécurité informatique, la sécurité des systèmes d'information, ainsi que des composantes géopolitiques, géoéconomiques et géostratégiques.

La certification vise à développer les compétences pour le métier de spécialiste en cybersécurité. Le spécialiste en cybersécurité est capable de contribuer à l'amélioration de la posture de cybersécurité des organisations, grâce à sa maîtrise des technologies et des systèmes d'information de gestion ou d'exploitation et à sa compréhension du cadre réglementaire et normatif et de la stratégie des organisations. Il s'agit d'un métier en tension parmi les plus recherchés sur le marché de l'emploi. La pénurie de ressources et de talents formés dans le domaine de la cybersécurité représente un frein à la transformation numérique.

Les titulaires de la certification Spécialiste en Cybersécurité sont aptes à comprendre ces problématiques majeures. La certification leur fournit tout le bagage nécessaire à leur insertion professionnelle sur le marché. Ils seront en

mesure d'exécuter des projets de cybersécurité en cohérence avec la stratégie globale de leur organisation.

ACTIVITÉS VISÉES

Collecte et analyse des informations nécessaires à la conduite d'un test d'intrusion éthique

Test d'intrusion éthique par l'exploitation des informations collectées

Évaluation de l'impact de compromission du périmètre ciblé par un test d'intrusion éthique

Présentation des résultats et des recommandations d'un test d'intrusion éthique

Configuration des éléments de sécurité des réseaux

Configuration des éléments de sécurité des infrastructures informatiques cloud et on premise

Sécurisation des nouvelles technologies de l'information et des communications (objets connectés, intelligence artificielle...)

Maintien de la sécurité des données d'un système d'information

Contrôle des identités et des accès à privilèges au sein d'un système d'information

Elaboration des standards techniques associés aux solutions de sécurité technique mises en oeuvre

Définition et analyse du fonctionnement nominal du système d'information

Définition du processus de collecte des journaux d'événements en fonction des menaces (playbook)

Automatisation et orchestration des règles de corrélation d'événements

COMPÉTENCES ATTESTÉES

Recueillir les données et renseignements relatifs à la cible, à l'aide de pratiques d'investigation légalement autorisées et d'analyse d'information préalablement dissimulée, en récoltant, croisant ou analysant des données numériques disponibles en source ouverte (OSINT), afin d'identifier les faiblesses du système d'information cible et de déterminer la nature du test d'intrusion.

Recueillir les données et renseignements relatifs aux actifs du système d'information de la cible, à l'aide d'outils et de techniques d'investigation légalement autorisés (discovery) afin de cartographier les systèmes les plus critiques et les plus exposés, d'identifier leurs vulnérabilités et de déterminer les chemins d'attaque possibles sur ces systèmes.

Conduire des techniques et tactiques d'attaques de cybersécurité sur base des éléments collectés, en collaboration avec les experts (opérationnels métiers et informatiques) afin de prendre le contrôle du système cible.

Maintenir le contrôle du système cible en déployant des mécanismes techniques (backdoor, webshell...) afin de contrer les mesures de sécurité proactives.

Déterminer les risques et dommages pour le système d'information cible en évaluant l'impact fonctionnel d'une attaque en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données, afin de rédiger un rapport de test d'intrusion dans un format prenant en compte les éventuelles situations de handicap.

Communiquer l'ensemble des résultats d'un test d'intrusion à travers un rapport de synthèse, dans un format prenant en compte les éventuelles situations de handicap, afin de présenter à l'organisation sa surface d'exposition, ses vulnérabilités, leur criticité et leur impact.

Déterminer les mesures de sécurité permettant de traiter les risques et dommages présents dans le rapport de test d'intrusion, en collaboration avec les opérationnels métiers et informatiques, afin d'établir un plan de remédiation adapté.

Etablir les mesures de sécurité applicables en concevant une infrastructure réseau sécurisée afin de protéger les réseaux WAN, LAN et sans fil.

Configurer les éléments de sécurité des réseaux (firewall, WAF, reverse proxy, NDR...) afin de mettre en place un réseau sécurisé répondant aux exigences de sécurité applicables à l'organisation

Configurer les éléments de sécurité des infrastructures internalisées dites "on-premise" (EDR, PAM...), en s'appuyant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux, afin de détecter et prévenir les comportements déviants des utilisateurs du système d'information.

Configurer les éléments de sécurité des infrastructures Cloud (CASB, CSPM, SWG, etc.) en reposant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de sécuriser l'environnement Cloud de l'organisation

Déployer des mesures de sécurité opérationnelles (chiffrement, contrôle d'accès, etc.) en s'appuyant sur les politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de prévenir les risques de fuite de données.

Configurer les éléments de sécurité des objets connectés industriels (IIoT) et non industriels (IoT), en intégrant les contraintes et spécificités de l'environnement de déploiement (industriel ou tertiaire), afin de garantir l'intégrité et la disponibilité des systèmes.

Déployer des mesures de sécurité s'appuyant sur l'intelligence artificielle en collaboration avec les experts

cybersécurité et les opérationnels métiers, afin de contenir les risques liés au déploiement de l'Intelligence Artificielle au sein d'un Système d'Information.

Mettre en oeuvre les mesures de sécurité des données, en fonction des contraintes et besoins fonctionnels de l'organisation, afin de garantir le niveau de confidentialité, d'intégrité et de disponibilité des données.

Traiter les vulnérabilités d'un projet à déployer sur un système d'information existant, via des solutions automatisées de patch management, afin de limiter les impacts et les risques inhérents à la sécurité des données.

Déployer des solutions de sécurité permettant de prévenir les risques de fuite de données d'un système d'information existant, afin d'être conforme au système de management de la sécurité de l'information (SMSI).

Mettre en oeuvre les mesures de sécurité et les solutions techniques associées (contrôle d'accès, authentification...) adéquates pour assurer la sécurité des identités humaines, machines et services.

Déployer un bastion de sécurité en gérant, contrôlant et enregistrant l'accès aux ressources du système d'information, afin de contrôler les accès à privilèges.

Elaborer les standards techniques de sécurité et la documentation technique, applicables et accessibles aux personnes en situation de handicap, en fonction des solutions techniques mises en oeuvre, afin de répondre aux exigences du système de management de la sécurité de l'information (SMSI).

Définir les comportements attendus du système d'information, en collaboration avec les différents experts (experts métier, DSI, fonctions support), afin de formaliser le comportement nominal attendu du système d'information.

Qualifier un événement de cybersécurité en fonction du comportement nominal du système d'information et des scénarios de gestion d'événements cyber (playbook), afin de le documenter, de déterminer son niveau de criticité et d'appliquer le traitement associé

Définir la collecte, la conservation et l'archivage des journaux d'événements (logs) nécessaires, en fonction des scénarios de gestion d'événements cyber (playbooks) et en accord avec les contraintes et exigences de l'organisation (conformité, budget...), pour analyser le fonctionnement du système d'information

Adapter les scénarios de gestion d'événements cyber (playbook) en fonction de l'état la menace afin d'optimiser les détections des événements de sécurité dans une optique d'amélioration continue

Programmer des règles de corrélation d'événements associées aux scénarios de gestion d'événements cyber (playbook) en vue de détecter des événements de sécurité de façon automatisée à travers un système de gestion des événements et des informations de sécurité (SIEM).

Développer des réponses automatisées, en programmant des règles de corrélation (algorithmes) d'événements et en les intégrant dans un outil d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR), afin d'optimiser le traitement des incidents de sécurité détectés.

Blocs de compétences

RNCP37987BC01 — Conduire des tests d'intrusion éthiques

LISTE DE COMPÉTENCES

Recueillir les données et renseignements relatifs à la cible, à l'aide de pratiques d'investigation légalement autorisées et d'analyse d'information préalablement dissimulée, en récoltant, croisant ou analysant des données numériques disponibles en source ouverte (OSINT), afin d'identifier les faiblesses du système d'information cible et de déterminer la nature du test d'intrusion.

Recueillir les données et renseignements relatifs aux actifs du système d'information de la cible, à l'aide d'outils et de techniques d'investigation légalement autorisés (discovery) afin de cartographier les systèmes les plus critiques et les plus exposés, d'identifier leurs vulnérabilités et de déterminer les chemins d'attaque possibles sur ces systèmes. Conduire des techniques et tactiques d'attaques de cybersécurité sur base des éléments collectés, en collaboration avec les experts (opérationnels métiers et informatiques) afin de prendre le contrôle du système cible.

Maintenir le contrôle du système cible en déployant des mécanismes techniques (backdoor, webshell...) afin de contrer les mesures de sécurité proactives.

Déterminer les risques et dommages pour le système d'information cible en évaluant l'impact fonctionnel d'une attaque en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données, afin de rédiger un rapport de test d'intrusion dans un format prenant en compte les éventuelles situations de handicap.

Communiquer l'ensemble des résultats d'un test d'intrusion à travers un rapport de synthèse, dans un format prenant en compte les éventuelles situations de handicap, afin de présenter à l'organisation sa surface d'exposition, ses vulnérabilités, leur criticité et leur impact.

Déterminer les mesures de sécurité permettant de traiter les risques et dommages présents dans le rapport de test

d'intrusion, en collaboration avec les opérationnels métiers et informatiques, afin d'établir un plan de remédiation adapté.

MODALITÉS D'ÉVALUATION

Le candidat devra collecter les informations permettant de déterminer et de déployer une ou plusieurs techniques de tests d'intrusion éthiques. Il sera demandé au candidat d'explicitier sa démarche et de présenter les impacts et les résultats du test d'intrusion conduit.

Cette mise en situation s'appuie sur la simulation d'une entreprise fictive et de son Système d'Information déployé et connecté à l'infrastructure physique implémentée dans les locaux du certificateur, avec une liste d'utilisateurs possédant une existence numérique, une gouvernance (organigramme, politiques de sécurité...) et une activité internationale multi-sites.

Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.

RNCP37987BC02 — Configurer les éléments de sécurité des infrastructures et des réseaux

LISTE DE COMPÉTENCES

Etablir les mesures de sécurité applicables en concevant une infrastructure réseau sécurisée afin de protéger les réseaux WAN, LAN et sans fil.

Configurer les éléments de sécurité des réseaux (firewall, WAF, reverse proxy, NDR...) afin de mettre en place un réseau sécurisé répondant aux exigences de sécurité applicables à l'organisation

Configurer les éléments de sécurité des infrastructures internalisées dites "on-premise" (EDR, PAM...), en s'appuyant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux, afin de détecter et prévenir les comportements déviants des utilisateurs du système d'information.

Configurer les éléments de sécurité des infrastructures Cloud (CASB, CSPM, SWG, etc.) en reposant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de sécuriser l'environnement Cloud de l'organisation

Déployer des mesures de sécurité opérationnelles (chiffrement, contrôle d'accès, etc.) en s'appuyant sur les politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de prévenir les risques de fuite de données.

Configurer les éléments de sécurité des objets connectés industriels (IIoT) et non industriels (IoT), en intégrant les contraintes et spécificités de l'environnement de déploiement (industriel ou tertiaire), afin de garantir l'intégrité et la disponibilité des systèmes.

Déployer des mesures de sécurité s'appuyant sur l'intelligence artificielle en collaboration avec les experts cybersécurité et les opérationnels métiers, afin de contenir les risques liés au déploiement de l'Intelligence Artificielle au sein d'un Système d'Information.

MODALITÉS D'ÉVALUATION

Simulation sur plateforme

Il sera demandé au candidat, dans le cadre d'une mise en situation simulée, de sélectionner et configurer les solutions techniques appropriées pour sécuriser une architecture réseaux.

Cette simulation repose sur la simulation d'une entreprise fictive et la réplique de son Système d'Information déployé et connecté à l'infrastructure physique implémentée dans les locaux du certificateur simulé.

Les éléments suivants seront mis à la disposition du candidat :

- un réseau d'entreprise comprenant une zone entreprise, une zone industrielle et une zone démilitarisée ;
- un ensemble de pare-feux (Fortinet, Stormshield, Palo Alto, etc.) ;
- un ensemble d'EDR (Tethris, HarFangLab, etc.) ; - un ensemble de Cloud Security Posture Management (Palo Alto, Netskope, etc.) ;
- un ensemble de solutions de chiffrement (BitLocker, BitDefender, etc.) ;
- une PKI (infrastructure de clé publique) avec les politiques associées ;
- une intelligence artificielle de type apprentissage automatique ;
- des équipements industriels (Schneider, Weidmueller, Siemens, Codra, Hirschmann,...)

Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.

RNCP37987BC03 — Sécuriser les données et les identités d'un système d'information existant

LISTE DE COMPÉTENCES

Mettre en oeuvre les mesures de sécurité des données, en fonction des contraintes et besoins fonctionnels de l'organisation, afin de garantir le niveau de confidentialité, d'intégrité et de disponibilité des données.

Traiter les vulnérabilités d'un projet à déployer sur un système d'information existant, via des solutions automatisées de patch management, afin de limiter les impacts et les risques inhérents à la sécurité des données.

Déployer des solutions de sécurité permettant de prévenir les risques de fuite de données d'un système d'information existant, afin d'être conforme au système de management de la sécurité de l'information (SMSI).

Mettre en oeuvre les mesures de sécurité et les solutions techniques associées (contrôle d'accès, authentification...) adéquates pour assurer la sécurité des identités humaines, machines et services.

Déployer un bastion de sécurité en gérant, contrôlant et enregistrant l'accès aux ressources du système d'information, afin de contrôler les accès à privilèges.

Elaborer les standards techniques de sécurité et la documentation technique, applicables et accessibles aux personnes en situation de handicap, en fonction des solutions techniques mises en oeuvre, afin de répondre aux exigences du système de management de la sécurité de l'information (SMSI).

MODALITÉS D'ÉVALUATION

Etude de cas pratique

Il sera demandé au candidat, dans le cadre d'un cas pratique, de rédiger un standard technique de sécurité et d'implémenter des mesures techniques de sécurité afin de sécuriser les données et les identités d'un Système d'Information existant.

Ce cas pratique sera conduit dans le contexte de sécurisation d'un Système d'Information.

Afin de mener à bien ce pratique, le candidat recevra les éléments suivants :

- un jeu des identités
- les politiques de sécurité incluant les exigences réglementaires et normatives applicables à l'organisation
- un jeu de données simulées de l'organisation
- une solution de prévention de fuite de données (DLP)
- un outil de gestion des correctifs ("patch management")
- une solution technique de type "bastion"
- un outil d'authentification multi-facteur (MFA)
- un ensemble de solutions de chiffrement (BitLocker, BitDefender, etc.) ;
- une PKI (infrastructure de clé publique) avec les politiques associées ;

Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'un cas pratique en salle et sur outils informatiques.

RNCP37987BC04 — Détecter et analyser les événements de cybersécurité

LISTE DE COMPÉTENCES

Définir les comportements attendus du système d'information, en collaboration avec les différents experts (experts métier, DSI, fonctions support), afin de formaliser le comportement nominal attendu du système d'information.

Qualifier un événement de cybersécurité en fonction du comportement nominal du système d'information et des scénarios de gestion d'événements cyber (playbook), afin de le documenter, de déterminer son niveau de criticité et d'appliquer le traitement associé

Définir la collecte, la conservation et l'archivage des journaux d'événements (logs) nécessaires, en fonction des scénarios de gestion d'événements cyber (playbooks) et en accord avec les contraintes et exigences de l'organisation (conformité, budget...), pour analyser le fonctionnement du système d'information

Adapter les scénarios de gestion d'événements cyber (playbook) en fonction de l'état la menace afin d'optimiser les détections des évènements de sécurité dans une optique d'amélioration continue

Programmer des règles de corrélation d'événements associées aux scénarios de gestion d'événements cyber (playbook) en vue de détecter des événements de sécurité de façon automatisée à travers un système de gestion des événements et des informations de sécurité (SIEM).

Développer des réponses automatisées, en programmant des règles de corrélation (algorithmes) d'événements et en les intégrant dans un outil d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR), afin d'optimiser le traitement des incidents de sécurité détectés.

MODALITÉS D'ÉVALUATION

Simulation sur plateforme

Il sera demandé au candidat de collecter et d'analyser les éléments techniques permettant de détecter et qualifier des événements de cybersécurité. Pour ce faire, le candidat sera immergé dans la simulation d'une entreprise fictive et de son Système d'Information. Cette simulation s'appuie sur une plateforme technologique répliquant un Centre Opérationnel de Sécurité (SOC) à taille réelle, déployé et connecté à l'infrastructure physique implémentée dans les

locaux du certificateur.

Le candidat recevra les éléments suivants :

- un système de gestion d'événements de sécurité (SIEM)
- un outil d'automatisation et d'orchestration des événements de sécurité (SOAR)
- un puits de logs
- un playbook
- des rapports de CERT
- une équipe d'experts métiers pour les jeux de rôles

Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'un cas pratique en salle et sur outils informatiques.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le métier de spécialiste en cybersécurité ne se limite pas au secteur d'activité des entreprises spécialisées en cybersécurité. Celui-ci est présent au sein de tous types de structures (publiques, privées, petites, moyennes et grandes organisations) et dans les secteurs du conseil, de l'industrie ou du tertiaire. Le contexte de travail varie selon l'organisation dans laquelle l'emploi est effectué (déplacement sur sites, contexte international, travail à distance, taille de l'équipe, etc.).

TYPE D'EMPLOIS ACCESSIBLES

Spécialiste en Cybersécurité
Pentester (conduite de tests d'intrusion)
Architecte sécurité
Opérateur Analyste SOC

RÈGLEMENTATIONS D'ACTIVITÉ

Bien que le métier ne soit pas réglementé en tant que tel, le spécialiste en cybersécurité veille, dans ses activités, à respecter les réglementations, normes et recommandations liées à son domaine d'intervention

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)	Très élevée (5/5)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Peuvent accéder à l'entrée en formation préparant à la certification, des candidats disposant :

- d'une certification professionnelle / diplôme de niveau 5 ou équivalent, ayant une spécialité informatique ou cybersécurité ; ou d'une expérience significative dans un emploi ayant permis l'acquisition de compétences en informatique ou cybersécurité.
- d'un niveau d'anglais permettant d'avoir une conversation professionnelle et de lire de la documentation technique

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

Le jury de certification est constitué de trois membres :

- un membre représentant du champ professionnel de la cybersécurité encadrant une ou plusieurs personnes exerçant le métier visé par la certification
- un membre représentant du champ professionnel de la cybersécurité exerçant le métier visé par la certification
- un membre de l'organisme certificateur

COMPOSITION DU JURY — APPRENTISSAGE

Le jury de certification est constitué de trois membres :

- un membre représentant du champ professionnel de la cybersécurité encadrant une ou plusieurs personnes exerçant le métier visé par la certification
- un membre représentant du champ professionnel de la cybersécurité exerçant le métier visé par la certification
- un membre de l'organisme certificateur

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 475 €
Selon la branche	7 000 € – 12 000 €
Prise en charge	Branches concernées
9 475 €	Valeur par défaut · 174 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Publicité, CPNEF de la presse et des agences de presse
9 480 €	CPNE Casinos, CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films, CPNEF de l'audiovisuel
8 500 €	CPNE des industries de santé (CPNEIS), CPNE des métiers du géomètre, CPNEFP de la profession d'économiste de la construction, Commission Paritaire Activités de Marchés Financiers
11 055 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
8 990 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
7 923 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 000 €	CPNE chimie, CPNEFP de la métallurgie
11 845 €	CPNE des Télécoms
11 844 €	CPNE Travail Temporaire
11 200 €	CPNEFP de la Mutualité Sociale Agricole
10 500 €	CPNEFP des industries des tuiles et briques
10 000 €	CPNE des exploitations frigorifiques
9 500 €	CPNE de l'ingénierie, des services informatiques et du conseil

9 000 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 942 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 285 €	CPNEFP Commerce à distance
8 057 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 036 €	CPNE FP Branche des magasins du Bricolage
8 029 €	CPNEFP des jardineries et graineteries
7 720 €	CPNE de la branche des experts comptables et commissaires aux comptes

Base légale

Date de décision	20/09/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	20/09/2026
Date de dernière délivrance possible	20/09/2030

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42503

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37987/>

Se former en apprentissage

Formations en apprentissage	2
Organismes gestionnaires (CFA)	2
Organismes formateurs	2
Régions couvertes	2
Départements couverts	2
Organismes certifiés Qualiopi	2
Sessions	de 09/2026 à 09/2027

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).