

Sciences et Ingénierie - Sécurité des Systèmes Numériques

RNCP41285 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	326
Formacode(s)	31006, 24293, 31067, 31032
Code(s) ROME	M1801, M1802, M1804, M1805
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2028

Certificateur(s)

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE · SIRET : 11004401300040
ECOLE POUR L'INFORMATIQUE ET LES TECHNIQUES AVANCEES (EPITA) · SIRET : 89819207500015

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les rapports institutionnels consacrés aux cybermenaces pesant sur les infrastructures numériques des organisations s'accordent sur une augmentation des incidents ainsi qu'une diversification des stratégies d'attaque adoptées (Panorama de la cybermenace 2024 , ENISA Threat Landscape 2024

). Les risques qui en découlent, accentués par des environnements numériques toujours plus complexes et interconnectés, imposent aux entreprises comme aux administrations de renforcer leurs capacités de protection, de détection et de réaction face aux cyberattaques.

Cependant, cette nécessité se heurte à un manque de professionnels qualifiés dans le domaine de la cybersécurité, comme le soulignent l'Eurobaromètre 547

(2023), le rapport de l'ENISA sur l'État de la cybersécurité dans l'Union

(2024) ou, plus récemment, l'Observatoire des métiers 2025

de l'ANSSI.

L'étude nationale menée par l'OPIIEC dans ce cadre (Étude sur les besoins en compétences, emplois et formation en matière de cybersécurité en France

, 2025) décrit la diversité des profils recherchés. Parmi ceux-ci, la proportion d'experts en développement sécurisé ou en sécurité cloud est équivalente à celle des profils plus traditionnels d'ingénieurs spécialisés en cybersécurité.

L'analyse des offres d'emploi réalisée dans cette étude révèle qu'un tiers d'entre elles cible des professions de niveau intermédiaire, parmi lesquelles figurent les rôles d'opérateur analyste SOC, d'expert en intrusion et tests, d'administrateur réseau et infrastructure ou encore de développeur sécurité.

Ces métiers opérationnels constituent le quotidien de la sécurisation des infrastructures des organisations. Les compétences développées par le certifié en Sécurité des systèmes numériques à l'EPITA visent à répondre pleinement aux exigences de ces fonctions.

ACTIVITÉS VISÉES

Les titulaires du titre de Bachelor en Sécurité des Systèmes Numériques de l'EPITA sont préparés à une intégration professionnelle visant les activités suivantes (issues du Panorama des métiers de la cybersécurité produit par l'ANSSI et du référentiel de compétences des métiers de la cybersécurité du groupe de travail « Formation » du Campus

Cyber) :

- Réaliser des audits techniques sur les Systèmes d'Information de l'entreprise pour évaluer leur robustesse.
- Réaliser ou piloter la mise en oeuvre de scans de vulnérabilités et de contrôles techniques, en continu et de manière automatisée.
- Réaliser une veille permanente vis-à-vis des scénarii d'attaques, des nouvelles menaces, des vulnérabilités associées et sur les techniques de développement sécurisé.
- Administrer et paramétrer des solutions de sécurité en assurant leur fonctionnement optimal, le traitement des journaux d'activités et leur conformité aux normes en vigueur, notamment les outils de détection des menaces.
- Concevoir et développer des solutions de sécurité : outils d'investigation, d'analyse des journaux d'activité et de détection d'intrusion.
- Identifier et analyser les événements de sécurité de l'entreprise ; collecter des informations techniques ou non, des Systèmes d'Information de l'entreprise ou de sources ouvertes permettant la rédaction de rapports d'incidents.
- Produire ou contribuer à l'élaboration de plans d'actions suite à la détection d'activités suspectes ou malveillantes.
- Intégrer les enjeux et le contexte de la cybermenace afin d'analyser et de pouvoir la qualifier pour produire un rapport sur le niveau d'exposition d'une organisation.
- Contribuer à la définition de l'architecture technique des Systèmes d'Information en lien avec les équipes concernées.
- Mettre en oeuvre la recette, l'industrialisation et la mise en production d'une solution de sécurité en lien avec le responsable du projet.

COMPÉTENCES ATTESTÉES

Le diplômé du Bachelor Cybersécurité de l'EPITA possède un ensemble de compétences généralistes en informatique et spécialisées en cybersécurité, reposant sur une solide culture technique incluant des compétences en programmation, réseaux et systèmes d'exploitation et une connaissance pratique de l'environnement mathématique, électronique et algorithmique de son domaine.

Il bénéficie grâce à sa formation d'une large exposition aux technologies utilisées en cybersécurité afin de pouvoir s'adapter aux missions qui lui sont demandées. Ainsi, il met en oeuvre un grand nombre de techniques et outils issus notamment des tests d'intrusions, de la rétro-ingénierie, du cloud, des systèmes de gestion des accès, de l'analyse de programmes malveillants, de la recherche de preuves numériques et de l'analyse des menaces. Il maintient les systèmes en état de fonctionnement, procède aux configurations nécessaires, met en place les mesures de protection, prototype et développe des solutions de sécurité en adéquation avec la stratégie de sécurité de son organisation. Fortement acculturé aux problématiques de sécurité opérationnelle, il valorise ses savoir-faire et savoir-être dans la gestion de crise et la réponse à incident ou encore dans l'anticipation des menaces et la gestion des risques. Il met à profit son expérience acquise pendant les périodes de son cursus réalisées en entreprise et, fortement sensibilisé à l'environnement juridique et aux questions éthiques associées à son métier, il évolue en professionnel responsable.

Au sein d'équipes multidisciplinaires, il s'engage dans une collaboration efficace et contribue à la réalisation des objectifs collectifs. Ses compétences en communication, écrite et orale, lui permettent d'adapter son discours en fonction des différents publics et de défendre les choix techniques auprès de l'ensemble des parties prenantes. Sensible aux diversités culturelles, il sait s'intégrer dans des environnements multiculturels, tout en tenant compte des évolutions sociétales.

Enfin, le diplômé du Bachelor Cybersécurité de l'EPITA intègre les enjeux de responsabilité sociale et environnementale dans son approche, en tenant compte de ces aspects dans la conception et le déploiement de solutions de sécurité et en étant attentif à leur impact sur l'entreprise et la société.

Liste des compétences attestées

Appliquer une configuration réseau d'un parc informatique en respectant les protocoles standard et les bonnes pratiques de sécurité.

Configurer les droits d'accès et les habilitations des utilisateurs d'une infrastructure informatique en respectant la politique de sécurité de l'entreprise et les rôles établis pour chacun, en formant les employés aux bonnes pratiques de sécurité.

Mettre en oeuvre des procédures de maintenance sur les composants de l'infrastructure tout en garantissant la continuité d'activité et en contribuant à la documentation de ces procédures.

Mettre en oeuvre des mécanismes de sauvegarde, de restauration et d'archivage des données, en veillant à leur intégrité et à leur disponibilité.

Assurer la traçabilité des événements et des incidents de sécurité à travers une politique de journalisation conforme

aux exigences réglementaires et en spécifiant les seuils d'alertes relatifs aux métriques de bonne santé d'une infrastructure.

Dimensionner une infrastructure au regard des flux réseaux attendus et des volumes de stockage nécessaires, en proposant des solutions techniques permettant de mettre en œuvre une stratégie de sécurité.

Déterminer les conditions d'exécution et l'environnement de production d'un programme et la chaîne de construction des livrables associés.

Sélectionner des structures de données hiérarchiques de manière à répondre efficacement à un problème posé.

Établir une architecture simple et les interactions entre ses composantes.

Construire une base de données adaptée au volume d'information disponible pour répondre efficacement à un problème.

Mettre en place un cycle de développement incluant phases de test et de déploiement.

Produire des programmes documentés et testés qui s'exécutent en prenant en compte l'environnement, les contraintes et les performances de leur système hôte.

Cartographier les acteurs et les composantes de la solution à auditer.

Identifier des points de non-conformité réglementaire sur un système d'information.

Réaliser une campagne de tests d'intrusion qui vise à identifier les vulnérabilités d'une solution, tout en respectant les règles déontologiques et de bonne conduite dans le cadre d'un audit de sécurité.

Rédiger un rapport d'audit présentant un diagnostic des vulnérabilités et des préconisations quant aux corrections à apporter, en adaptant le discours au public cible.

Accompagner le client dans la prise en main du rapport d'audit et le déploiement de correctifs si nécessaire.

Effectuer une recherche documentaire et d'acculturation à un problème donné, en identifiant les ressources et outils pertinents à disposition ou à mobiliser pour une éventuelle résolution.

Valider une modélisation donnée, à l'aide d'outils scientifiques établis (mathématiques, physique, informatique).

Réaliser un prototype à partir d'un besoin spécifié et d'une solution définie, dans l'objectif de tester sa validité, dans un contexte spécifié et contraint.

Suivre des indicateurs de performance et de validité pré-définis, exprimés de la demande client ou du besoin utilisateur.

Vérifier la conformité d'une solution numérique vis-à-vis des réglementations RSE, et la prise en compte des enjeux éthiques et déontologiques classiques.

Identifier le niveau de risque auquel est confrontée l'entreprise et son système d'information, en cartographiant la structure organisationnelle de l'entreprise ou du service, les parties prenantes et ressources associées.

Intégrer la stratégie de sécurité dans les phases de conception et de développement d'une solution numérique (security by design).

Proposer des solutions techniques permettant de mettre en œuvre une stratégie de sécurité.

Expliciter la façon dont les normes réglementaires s'inscrivent dans cette stratégie.

Planifier une campagne de déploiement d'une stratégie de sécurité en tenant compte des besoins des différents acteurs impactés et en identifiant les blocages humains et organisationnels à sa mise en place.

Mesurer l'adoption d'une politique de sécurité par les employés.

Blocs de compétences

RNCP41285BC01 — Maintenir tout ou partie d'une infrastructure informatique en état de fonctionnement opérationnel, en respectant les schémas organisationnels et les modes de travail de l'entreprise ou du service.

LISTE DE COMPÉTENCES

1. Appliquer une configuration réseau d'un parc informatique en respectant les protocoles standard et les bonnes pratiques de sécurité.
2. Configurer les droits d'accès et les habilitations des utilisateurs d'une infrastructure informatique en respectant la politique de sécurité de l'entreprise et les rôles établis pour chacun, en formant les employés aux bonnes pratiques de sécurité.
3. Mettre en œuvre des procédures de maintenance sur les composants de l'infrastructure tout en garantissant la continuité d'activité et en contribuant à la documentation de ces procédures.
4. Mettre en œuvre des mécanismes de sauvegarde, de restauration et d'archivage des données, en veillant à leur intégrité et à leur disponibilité.

5. Assurer la traçabilité des événements et des incidents de sécurité à travers une politique de journalisation conforme aux exigences réglementaires et en spécifiant les seuils d'alertes relatifs aux métriques de bonne santé d'une infrastructure.
6. Dimensionner une infrastructure au regard des flux réseaux attendus et des volumes de stockage nécessaires, en proposant des solutions techniques permettant de mettre en œuvre une stratégie de sécurité.
7. Recueillir et documenter les évolutions des besoins des utilisateurs de l'infrastructure.

MODALITÉS D'ÉVALUATION

Dans le cadre de la confrontation à des situations professionnelles authentiques, incluant des échanges réguliers avec des tuteurs adoptant des postures professionnelles dépendant de la situation :

- Installer et configurer un parc de machines
- Réagir en temps réel à une cyberattaque dans une équipe aux rôles variés
- Tirer les leçons d'une attaque passée et apporter des solutions pour rendre un système plus résilient
- Développer une solution de monitoring

Évaluation des livrables techniques (configuration, journalisation, sauvegarde et restauration) pour la conformité de l'infrastructure à la politique de sécurité spécifiée et la réponse aux besoins.

Évaluation in situ de la posture et de la réaction lors d'une situation de crise.

Évaluation de la démarche itérative lors d'échanges oraux avec un tuteur projet, prenant en compte des jalons de validation.

RNCP41285BC02 — Développer des solutions logicielles qui visent à assurer la sécurité des systèmes d'information et des infrastructures numériques en s'appuyant sur des standards et des normes établis.

LISTE DE COMPÉTENCES

1. Déterminer les conditions d'exécution et l'environnement de production d'un programme et la chaîne de construction des livrables associés.
2. Sélectionner des structures de données hiérarchiques de manière à répondre efficacement à un problème posé.
3. Établir une architecture simple et les interactions entre ses composantes.
4. Construire une base de données adaptée au volume d'information disponible pour répondre efficacement à un problème.
5. Mettre en place un cycle de développement incluant phases de test et de déploiement.
6. Produire des programmes documentés et testés qui s'exécutent en prenant en compte l'environnement, les contraintes et les performances de leur système hôte.
7. Appliquer les bonnes pratiques en matière de développement collaboratif : utilisation des outils de versionnage, analyse de code par les pairs et retours sur cahier des charges fonctionnel.

MODALITÉS D'ÉVALUATION

Dans le cadre de la confrontation à des situations professionnelles authentiques, incluant des échanges réguliers avec des tuteurs adoptant des postures professionnelles dépendant de la situation :

- Développer un jeu ou un outil
- Initiation à la démarche de la recherche
- Développer une solution de monitoring

Analyse de la qualité des solutions logicielles.

Évaluation de la démarche itérative lors d'échanges avec un tuteur projet, prenant en compte des jalons de validation.

Évaluation en soutenance de la prise de recul sur la solution livrée et son dimensionnement, ainsi que la conformité aux normes et standards de sécurité.

RNCP41285BC03 — Auditer un système d'information ou une solution numérique, et en tester les vulnérabilités, tout en respectant les contraintes de confidentialité.

LISTE DE COMPÉTENCES

1. Cartographier les acteurs et les composantes de la solution à auditer.
2. Identifier des points de non-conformité réglementaire sur un système d'information.
3. Réaliser une campagne de tests d'intrusion qui vise à identifier les vulnérabilités d'une solution, tout en respectant les règles déontologiques et de bonne conduite dans le cadre d'un audit de sécurité.
4. Rédiger un rapport d'audit présentant un diagnostic des vulnérabilités et des préconisations quant aux corrections à apporter, en adaptant le discours au public cible.
5. Présenter les conclusions d'un rapport d'audit dans le cadre d'une livraison à un client, en veillant à la clarté du propos et en adoptant un ton adapté aux risques encourus et constatés.

6. Accompagner le client dans la prise en main du rapport d'audit par une aide à l'analyse et au déploiement de correctifs si nécessaire.

MODALITÉS D'ÉVALUATION

Dans le cadre de la confrontation à des situations professionnelles authentiques, incluant des échanges réguliers avec des tuteurs adoptant des postures professionnelles dépendant de la situation :

- Introduction aux tests d'intrusions : atelier tests d'intrusions web
- Analyser un fichier potentiellement malveillant pour en comprendre l'intention et le niveau de dangerosité
- Tirer les leçons d'une attaque passée et apporter des solutions pour rendre un système plus résilient
- Offensif : auditer une solution numérique et rédiger un rapport d'audit

Évaluation du plan de déploiement de la phase de tests, et de sa mise en oeuvre.

Évaluation du listing des vulnérabilités identifiées.

Évaluation de l'analyse de risque présentée dans l'audit.

Évaluation de la pertinence des remédiations proposées.

Évaluation de la capacité à défendre l'analyse portée par l'audit lors d'une présentation orale dédiée.

RNCP41285BC04 — Prototyper une solution numérique et tester sa validité, la qualité de sa réponse au besoin et mesurer son impact.

LISTE DE COMPÉTENCES

1. Effectuer une recherche documentaire et d'acculturation à un problème donné, en identifiant les ressources et outils pertinents à disposition ou à mobiliser pour une éventuelle résolution.
2. Valider une modélisation donnée, à l'aide d'outils scientifiques établis (mathématiques, physique, informatique).
3. Réaliser un prototype à partir d'un besoin spécifié et d'une solution définie, dans l'objectif de tester sa validité, dans un contexte spécifié et contraint.
4. Animer efficacement les temps d'échanges avec l'ensemble des parties prenantes de façon à prendre en compte les retours utilisateurs et répondre aux contraintes clients.
5. Suivre des indicateurs de performance et de validité pré-définis, exprimés de la demande client ou du besoin utilisateur.
6. Vérifier la conformité d'une solution numérique vis-à-vis des réglementations RSE, et la prise en compte des enjeux éthiques et déontologiques classiques.

MODALITÉS D'ÉVALUATION

Dans le cadre de la confrontation à des situations professionnelles authentiques, incluant des échanges réguliers avec des tuteurs adoptant des postures professionnelles dépendant de la situation :

- Développer un jeu ou un outil
- Initiation à la démarche de la recherche
- Développer une solution de monitoring

Évaluation des livrables au regard de leur pertinence et la démarche de spécification des fonctionnalités, tests inclus.

Évaluation de la démarche itérative et la qualité des interactions et de pris en compte des parties prenantes, lors d'échanges avec un tuteur « client » du projet, prenant en compte des jalons de validation et les retours utilisateurs.

RNCP41285BC05 — Mettre en place une stratégie de sécurité numérique au sein d'une entreprise ou d'un service.

LISTE DE COMPÉTENCES

1. Identifier le niveau de risque auquel est confrontée l'entreprise et son système d'information, en cartographiant la structure organisationnelle de l'entreprise ou du service, les parties prenantes et ressources associées.
2. Intégrer la stratégie de sécurité dans les phases de conception et de développement d'une solution numérique (security by design).
3. Proposer des solutions techniques permettant de mettre en œuvre une stratégie de sécurité.
4. Expliciter la façon dont les normes réglementaires s'inscrivent dans cette stratégie.
5. Planifier une campagne de déploiement d'une stratégie de sécurité en tenant compte des besoins des différents acteurs impactés et en identifiant les blocages humains et organisationnels à sa mise en place.
6. Expliquer les enjeux d'une politique de sécurité aux salariés d'une entreprise en adoptant un langage adapté au public.
7. Mesurer l'adoption d'une politique de sécurité par les employés.

MODALITÉS D'ÉVALUATION

Dans le cadre de la confrontation à des situations professionnelles authentiques, incluant des échanges réguliers

avec des tuteurs adoptant des postures professionnelles dépendant de la situation :

- Concevoir une campagne de sensibilisation aux enjeux de sécurité
- Réagir en temps réel à une cyberattaque dans une équipe aux rôles variés
- Tirer les leçons d'une attaque passée et apporter des solutions pour rendre un système plus résilient
- Développer une solution de monitoring

Évaluation de l'analyse d'une situation d'incident de sécurité.

Évaluation de proposition de campagne de sensibilisation.

Évaluation de la conformité de la mise en place d'une stratégie de sécurité compte tenu du document cadre fourni.

Évaluation du prototype d'un outil de sécurité en vérifiant que la stratégie de sécurité est respectée.

Évaluation de la capacité à présenter les enjeux d'une politique de sécurité à un profil non initié, dans le cadre d'une présentation orale.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Entreprise de services du numérique (ESN)
- Éditeurs de logiciel
- Cabinets de conseil
- Industrie
- Secteur « Banque, Finances et Assurance »
- E-business
- Secteur des télécommunications
- Défense
- Sécurité informatique
- Autres : Formation, Négoce/Distribution, Administration, Audiovisuel & Média, Jeux vidéo, Santé

TYPE D'EMPLOIS ACCESSIBLES

- Développeur informatique
- Administrateur système / sécurité informatique
- Administrateur réseaux
- Assistant Ingénieur support
- Assistant Architecte télécoms
- Assistant Architecte en Systèmes d'information
- Architecte sécurité informatique junior
- Spécialiste en développement sécurité informatique
- Opérateur analyste SOC (Security Operation Center)
- Consultant en cybersécurité
- Coordinateur sécurité informatique
- Analyste de Malware
- Auditeur de sécurité informatique technique

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)	2 781 €
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)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) 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) 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)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique 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 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, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Voie d'accès via Concours Advance Bachelors pour une entrée en première année de Bachelor : titulaires d'une certification niveau 4 (Baccalauréat Général avec deux options scientifiques recommandées ou Baccalauréat Technologique filière STI2D).
- Voie d'accès sur dossier via Concours Advance Parallèle pour une entrée en première, deuxième ou troisième année : titulaires de certifications de niveaux 5 et 6 (BTS CIEL, BTS SIO, BUT orientés numérique, Licences universitaires en mathématiques et informatique).

PRÉREQUIS À LA VALIDATION

Outre la validation des compétences détaillées ci-dessus, pour viser le grade licence le candidat doit valider les critères suivants :

- Validation d'un niveau B2 en anglais (cadre européen commun de référence pour les langues), via une certification extérieure.
- Validation d'une expérience multiculturelle comportant un séjour d'au moins 4 semaines à l'international.
- Une immersion en entreprise d'au moins 12 semaines (hors apprentissage).

Ces conditions peuvent être adaptées pour les étudiants (ou apprentis) en situation de handicap.

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE, VAE

Le jury d'attribution du Titre est présidé par une personnalité extérieure à l'Ecole appartenant au monde économique ou universitaire. Il comprend en plus du Président, le Directeur de l'EPITA, le Directeur des études du Bachelor, le Directeur des Relations Entreprises, 2 enseignants et 4 personnalités extérieures représentant des entreprises significatives du secteur d'activité des diplômés.

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 · 176 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 Branche des organismes de formation, CPNEF de la Publicité
9 480 €	CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films, CPNEF de l'audiovisuel
7 200 €	CPNE Banque, CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
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
10 500 €	CPNEFP des industries des tuiles et briques
10 400 €	CPNEFP de la Mutualité Sociale Agricole
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
8 842 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 500 €	CPNE des industries de santé (CPNEIS)
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

Base légale

Date d'échéance de l'enregistrement 31/08/2028

Date de dernière délivrance possible 31/08/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	21	0	0 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP37708

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

BACHELOR CYBERSÉCURITÉ (RNCP NIVEAU 6) - EPITA

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41285/>