

Expert en cybersécurité (MS)

RNCP39837 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	28/11/2024
Date d'échéance	28/11/2027

Certificateur(s)

CENTRALESUPELEC · SIRET : 13002076100016

INSTITUT MINES TELECOM - IMT ATLANTIQUE - BRETAGNE - PAYS DE LA LOIRE · SIRET : 18009202500121

Résumé de la certification

OBJECTIFS ET CONTEXTE

Au sein de l'ANSSI, service français créé en 2009 rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN), en charge d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale, le Centre de formation à la sécurité des systèmes d'information (CFSSI), qui intervient dans la définition et la mise en œuvre de la politique de formation à la sécurité des systèmes d'information, a proposé une typologie de métiers visant à guider les entreprises dans leur politique de recrutement, à accompagner les chargés de formation et à encourager les étudiants ou les salariés en reconversion. Cette typologie définit cinq grandes familles de métiers :

- Gestion de la sécurité et pilotage des projets de sécurité
- Conception et maintien d'un SI sécurisé
- Gestion des incidents et des crises de sécurité
- Conseil, services et recherche
- Métiers connexes

L'expert en cybersécurité est un métier qui s'enrichit de plus de besoins liés au contrôle interne, à la maîtrise des risques et la prévention de la cybersécurité

ACTIVITÉS VISÉES

Réalisation d'une analyse de risque

Mise au point d'une stratégie de traitement du risque en accord avec l'analyse de risques

Déploiement d'une architecture de sécurité répondant aux exigences de SSI et assurant la protection des données et services numériques en accord avec la législation

Mise en place des outils de supervision des équipements informatiques et de leur sécurité

Contrôle de l'application des procédures qualité et sécurité des systèmes d'information et télécoms

Veille au respect de la loi Informatique et Libertés, du RGPD dans l'entreprise, gestion de la liste des traitements de données à caractère personnel et interface avec la CNIL

Audit ou supervision d'audit de la sécurité du SI et compte-rendu de l'audit

Veille continue au regard de l'évolution du contexte global (technique, menace, organisationnel, législatif, ...); comptes-rendus et force de proposition.

Détection d'un incident de sécurité et adoption d'une posture adaptée au contexte : gestion de crise
Contrôle de la sécurité de la reprise d'activité.

COMPÉTENCES ATTESTÉES

Identifier les biens essentiels et supports ainsi que procédures d'exploitation de l'organisation en vue de déterminer les risques afférents en recensant les biens au sein du périmètre de l'étude ainsi que leurs relations fonctionnelles.

Analyser des enjeux liés à la sécurité du SI en vue de gérer les risques associés en termes technique, économique et juridique en s'appuyant sur une étude du contexte.

Évaluer la vraisemblance d'un scénario de menace en mettant en regard le potentiel des sources de menaces considérées, l'exposition à ces menaces et la facilité d'exploitation des vulnérabilités identifiées afin d'estimer la plausibilité de celui-ci et déterminer la nature de la réponse à apporter.

Évaluer les coûts liés à la sécurité en mettant en regard les coûts d'un incident de sécurité, d'une mesure préventive et d'une remédiation en vue de déterminer la nature de la réponse à apporter.

Restituer l'analyse de risque et des moyens de remédiation auprès d'un donneur d'ordre (autorité, chef de projet, chef DSI...) dans le domaine de la SSI en réalisant un rapport et une présentation orale adaptés aux parties prenantes concernées (dont les personnes en situations de handicap) afin de sensibiliser les parties prenantes et d'arbitrer les réponses à apporter au regard de l'analyse établie.

Évaluer la pertinence d'une mesure technique de sécurité en mettant en regard le contexte technique, légal et organisationnel afin d'apporter une réponse adaptée au regard des risques identifiés.

Proposer une articulation de moyens techniques et organisationnels répondant aux enjeux de l'analyse de risques en définissant des procédures d'exploitation et d'utilisation des équipements informatiques dans le respect des contraintes SSI en vue de répondre de manière adaptée aux exigences issues de l'analyse de risque

Identifier le contexte légal en s'appuyant sur les référentiels standards (droits, obligations, normes et standards) de la sécurité concernant la protection des données et services numériques afin de mesurer les périmètres de responsabilité en matière de sécurité informatique.

Déployer les différents équipements et protocoles employés dans une architecture sécurisée en vue de garantir le juste niveau de sécurité en s'appuyant sur l'état de l'art.

Rendre compte auprès des équipes techniques (SI, Security Operations center (SOC), Computer Emergency Response Team (CERT)...) des mesures mises en œuvre dans le domaine de la SSI au travers de communications écrites et orales en s'adaptant à l'audience et aux potentiels profils singuliers (situation de handicap, interculturalité, ...) afin de garantir l'appropriation, par les parties prenantes, d'un vocabulaire et d'une connaissance partagée des processus mis en œuvre.

Déployer un juste niveau de supervision en plaçant et configurant de manière adaptée des sondes dans le SI afin de fournir des indicateurs et historiques d'actions utiles à la réponse à incident, à l'investigation numérique et la SSI.

Estimer la criticité d'une alerte de sécurité, en mettant en regard le contexte de celle-ci, le cadre global de l'architecture et son lien aux biens essentiels, en vue de hiérarchiser les alertes pour faciliter le traitement de celles-ci et la recherche de corrélations.

Collecter des preuves d'audits ou des indicateurs de compromission en sécurité en respectant les procédures qualité et sécurité des SI afin de vérifier l'adéquation entre le plan initial et la mise en œuvre effective.

Assurer la conformité des configurations et fonctionnalités des différents composants du SI dans le respect du cadre global de la réglementation en vigueur et des différents référentiels afin d'intervenir en sécurité sur les équipements et les ressources.

Assurer l'adéquation entre les configurations et les évolutions techniques pour garantir un juste niveau de sécurité en mobilisant les principes fondamentaux des outils cryptographiques.

S'assurer du respect du cadre législatif par les opérateurs techniques dans un SI complexe et hétérogène en ayant recours aux procédures qualité et sécurité afin de garantir la conformité aux réglementations en vigueur.

Rendre compte, auprès d'un public à compétences légales et/ou donneur d'ordres ainsi qu'aux autorités compétentes, de l'adéquation ou des éventuels écarts au cadre législatif des traitements relatifs aux données à caractère personnel effectué en réalisant des rapports et présentations orales adaptées aux spécificités du public (dont les personnes en situations de handicap) afin de leur permettre une prise de décision avertie.

Intervenir dans un système complexe et inconnu en rédigeant un programme d'audit comprenant le périmètre, les critères et les objectifs de sorte à collecter des preuves d'audits.

Documenter les procédures permettant la collecte de preuves d'audit en analysant les preuves et en établissant des constatations afin de rejouer ces scénarios de collecte.

Restituer, auprès d'un public technique et/ou de donneur d'ordres, un audit relatif aux procédures effectuées en

collectant les preuves d'audit et les conclusions en termes de SSI, en veillant à ce qu'il soit adapté à tous les lecteurs (dont les personnes en situation de handicap) afin de réaliser des préconisations techniques et/ou organisationnelles. Réaliser une veille continue concernant les dernières évolutions technologiques, des systèmes d'informations et des télécommunications en évaluant leurs impacts et leurs coûts en termes de SSI afin de rendre compte et proposer des évolutions pertinentes en conséquence.

Réaliser une veille continue concernant les dernières vulnérabilités, menaces et produits de sécurité pour les analyser, en évaluant les impacts d'une vulnérabilité ou d'une menace afin de contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet (spécialistes informatiques, les administrateurs, RSSI) et les utilisateurs.

Gérer les risques associés en adaptant l'analyse de risques courante en regard de l'évolution des menaces et des évolutions techniques, structurelles et législatives afin d'opérer une gestion des risques actualisée et optimale.

Blocs de compétences

RNCP39837BC01 — Concevoir la sécurité d'un système d'information

LISTE DE COMPÉTENCES

Identifier les biens essentiels et supports ainsi que procédures d'exploitation de l'organisation en vue de déterminer les risques afférents en recensant les biens au sein du périmètre de l'étude ainsi que leurs relations fonctionnelles.

Analyser des enjeux liés à la sécurité du SI en vue de gérer les risques associés en termes technique, économique et juridique en s'appuyant sur une étude du contexte.

Évaluer la vraisemblance d'un scénario de menace en mettant en regard le potentiel des sources de menaces considérées, l'exposition à ces menaces et la facilité d'exploitation des vulnérabilités identifiées afin d'estimer la plausibilité de celui-ci et déterminer la nature de la réponse à apporter.

Évaluer les coûts liés à la sécurité en mettant en regard les coûts d'un incident de sécurité, d'une mesure préventive et d'une remédiation en vue de déterminer la nature de la réponse à apporter.

Restituer l'analyse de risque et des moyens de remédiation auprès d'un donneur d'ordre (autorité, chef de projet, chef DSI...) dans le domaine de la SSI en réalisant un rapport et une présentation orale adaptés aux parties prenantes concernées (dont les personnes en situations de handicap) afin de sensibiliser les parties prenantes et d'arbitrer les réponses à apporter au regard de l'analyse établie.

Évaluer la pertinence d'une mesure technique de sécurité en mettant en regard le contexte technique, légal et organisationnel afin d'apporter une réponse adaptée au regard des risques identifiés.

Proposer une articulation de moyens techniques et organisationnels répondant aux enjeux de l'analyse de risques en définissant des procédures d'exploitation et d'utilisation des équipements informatiques dans le respect des contraintes SSI en vue de répondre de manière adaptée aux exigences issues de l'analyse de risque.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur une analyse de risques - Le candidat est évalué sur l'étude d'un cas pratique représentatif de cas réels en suivant la méthodologie EBIOS Risk Manager. L'étude donne lieu à un rapport écrit devant mettre en évidence : Une cartographie des biens essentiels et supports, une cartographie des risques associés, des scénarios de menace opérationnels vraisemblables, des mesures de sécurité complémentaires, la priorité des remédiations et un budget estimatif.

Mise en situation professionnelle portant sur la sécurisation d'un service fourni - Le candidat est évalué sur sa stratégie de sécurisation mise en œuvre qui donne lieu à la rédaction d'un rapport d'architecture et d'une restitution orale devant un jury de professionnels de la SSI. Le rapport doit comprendre les choix fonctionnels effectués et une architecture SI avec son analyse de risques

RNCP39837BC02 — Déployer les mesures techniques et organisationnelles répondant aux exigences de sécurité du SI

LISTE DE COMPÉTENCES

Identifier le contexte légal en s'appuyant sur les référentiels standards (droits, obligations, normes et standards) de la sécurité concernant la protection des données et services numériques afin de mesurer les périmètres de responsabilité en matière de sécurité informatique.

Déployer les différents équipements et protocoles employés dans une architecture sécurisée en vue de garantir le juste niveau de sécurité en s'appuyant sur l'état de l'art.

Rendre compte auprès des équipes techniques (SI, Security Operations center (SOC), Computer Emergency

Response Team (CERT)... des mesures mises en œuvre dans le domaine de la SSI au travers de communications écrites et orales en s'adaptant à l'audience et aux potentiels profils singuliers (situation de handicap, interculturalité, ...) afin de garantir l'appropriation, par les parties prenantes, d'un vocabulaire et d'une connaissance partagée des processus mis en œuvre.

Déployer un juste niveau de supervision en plaçant et configurant de manière adaptée des sondes dans le SI afin de fournir des indicateurs et historiques d'actions utiles à la réponse à incident, à l'investigation numérique et la SSI.

Estimer la criticité d'une alerte de sécurité, en mettant en regard le contexte de celle-ci, le cadre global de l'architecture et son lien aux biens essentiels, en vue de hiérarchiser les alertes pour faciliter le traitement de celles-ci et la recherche de corrélations.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur la mise en place d'une architecture physique - Le candidat conçoit l'architecture, met en place des procédures répondant aux exigences de sécurité et réalise les tests inhérents. Les solutions proposées sont évaluées par des professionnels de la SSI.

Etude de cas - Cet examen porte sur la maîtrise des fondamentaux nécessaires au déploiement d'une architecture de sécurité, à travers un audit d'architecture de sécurité sur la base du rapport produit. Il est attendu du candidat l'emploi du vocabulaire adapté aux comptes-rendus à réaliser auprès des équipes techniques.

RNCP39837BC03 — Exploiter en sécurité un SI

LISTE DE COMPÉTENCES

Collecter des preuves d'audits ou des indicateurs de compromission en sécurité en respectant les procédures qualité et sécurité des SI afin de vérifier l'adéquation entre le plan initial et la mise en œuvre effective.

Assurer la conformité des configurations et fonctionnalités des différents composants du SI dans le respect du cadre global de la réglementation en vigueur et des différents référentiels afin d'intervenir en sécurité sur les équipements et les ressources.

Assurer l'adéquation entre les configurations et les évolutions techniques pour garantir un juste niveau de sécurité en mobilisant les principes fondamentaux des outils cryptographiques.

S'assurer du respect du cadre législatif par les opérateurs techniques dans un SI complexe et hétérogène en ayant recours aux procédures qualité et sécurité afin de garantir la conformité aux réglementations en vigueur.

Rendre compte, auprès d'un public à compétences légales et/ou donneur d'ordres ainsi qu'aux autorités compétentes, de l'adéquation ou des éventuels écarts au cadre législatif des traitements relatifs aux données à caractère personnel effectué en réalisant des rapports et présentations orales adaptées aux spécificités du public (dont les personnes en situations de handicap) afin de leur permettre une prise de décision averties orales, de l'adéquation au cadre législatif des traitements effectués auprès d'un public à compétences légales et/ou donneur d'ordres ainsi qu'aux autorités compétentes afin de protéger l'entreprise.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée portant sur l'exploitation d'un SI proposé au candidat - Restitution orale individuelle

- Le candidat doit exploiter l'architecture, mettre en place des procédures répondant aux exigences de sécurité et réaliser les tests inhérents. Les solutions proposées sont évaluées par des professionnels de la SSI. Le candidat présente le résultat de ses travaux lors d'un entretien oral.

RNCP39837BC04 — Maintenir de manière continue la sécurité d'un SI

LISTE DE COMPÉTENCES

Intervenir dans un système complexe et inconnu en rédigeant un programme d'audit comprenant le périmètre, les critères et les objectifs de sorte à collecter des preuves d'audits.

Documenter les procédures permettant la collecte de preuves d'audit en analysant les preuves et en établissant des constatations afin de rejouer ces scénarios de collecte.

Restituer, auprès d'un public technique et/ou de donneur d'ordres, un audit relatif aux procédures effectuées en collectant les preuves d'audit et les conclusions en termes de SSI, en veillant à ce qu'il soit adapté à tous les lecteurs (dont les personnes en situation de handicap) afin de réaliser des préconisations techniques et/ou organisationnelles.

Réaliser une veille continue concernant les dernières évolutions technologiques, des systèmes d'informations et des télécommunications en évaluant leurs impacts et leurs coûts en termes de SSI afin de rendre compte et proposer des évolutions pertinentes en conséquence.

Réaliser une veille continue concernant les dernières vulnérabilités, menaces et produits de sécurité pour les

analyser, en évaluant les impacts d'une vulnérabilité ou d'une menace afin de contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet (spécialistes informatiques, les administrateurs, RSSI) et les utilisateurs.

Gérer les risques associés en adaptant l'analyse de risques courante en regard de l'évolution des menaces et des évolutions techniques, structurelles et législatives afin d'opérer une gestion des risques actualisée et optimale.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée portant sur l'audit d'un système d'information - A partir d'un programme d'audit, le candidat collecte les informations dans le but d'établir les preuves d'audit, les analyser afin d'établir des constats recensés dans un rapport.

Mise en situation professionnelle simulée portant sur l'audit de systèmes reposant sur les technologies du web - Le candidat mesure

la sécurité d'une application web réaliste à travers un test d'intrusion (pentest). Il identifie les vulnérabilités présentes dans l'application, évalue leur exploitabilité par un attaquant, leur criticité et propose des contremesures. Ses résultats sont synthétisés dans un rapport de pentest similaires aux rapports attendus en milieu professionnel, évalué par des professionnels en activité dans ce domaine. Ce rapport couvre ou comprend : Résumé exécutif (Une vue d'ensemble des principales découvertes et recommandations) ; Méthodologie (Description des méthodes et des outils utilisés) ; Découvertes (Liste des vulnérabilités identifiées. Chaque vulnérabilité est accompagnée des implications pour la sécurité, et des preuves de son existence) ; Recommandations (Conseils sur la manière de corriger les vulnérabilités identifiées) ; Plan de remédiation (Un plan détaillé pour la mise en œuvre des recommandations)

Mise en situation professionnelle simulée portant sur une analyse de risques - Le candidat établit une étude bibliographique et constitue un rapport d'analyses de risques

Mise en situation professionnelle simulée portant sur l'analyse de sécurité d'un produit de sécurité - Le candidat rédige un rapport technique détaillant les vulnérabilités d'un produit de sécurité identifiées avec une cotation de celles-ci.

RNCP39837BC05 — Réagir à un incident de sécurité du SI

LISTE DE COMPÉTENCES

Identifier la portée temporelle et fonctionnelle d'un incident de sécurité en ayant recours aux différentes sources d'informations à disposition (documents d'architecture, alertes de sécurité et analyse de risque courante...) afin de caractériser la menace.

Collecter des indicateurs de compromission en mesurant les coûts associés à l'incident afin d'agir en accord avec la posture[1] adaptée.

Coordonner la gestion de crise et la réponse à incident en prenant en compte les contextes techniques et organisationnels en vue de limiter la portée temporelle et fonctionnelle de l'incident.

Diagnostiquer, en sécurité, la nature et l'origine des incidents en vue d'exhiber le scénario d'attaque effectif et d'ainsi faire évoluer l'analyse de risque en conséquence.

Établir un rapport d'incident détaillant le scénario d'attaque effectif en préconisant des actions curatives et formatives en vue de déterminer des contre-mesures adéquates.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée portant sur un incident de sécurité - Le candidat propose une architecture de détection d'intrusion : il propose les phases de tests ; il doit collecter et analyser les informations de l'incident ; il collecte des indicateurs de compromissions et coordonne la gestion de crise ; il rédige le diagnostic et émet des préconisations

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en cybersécurité évolue au sein de tous types d'entreprises (industrielles, de services et de conseil, organismes publics, associations, sociétés de services informatiques). Il travaille en relations avec différents services (DSI, production/exploitation, études et développement, maintenance, ...), en contact avec de multiples intervenants (chef de projet MOA, utilisateurs, ...).

TYPE D'EMPLOIS ACCESSIBLES

Expert cybersécurité - Ingénieur cybersécurité - Architecte cybersécurité - Analyste en cybersécurité - Consultant cybersécurité - Auditeur SSI - Ingénieur projet cybersécurité - Officier SSI - Ingénieur sécurité système et réseau -

RÈGLEMENTATIONS D'ACTIVITÉ

L'expert en cybersécurité doit maîtriser le cadre légal et réglementaire propre à la sécurité des données dont, en particulier, la loi de programmation militaire (LPM) de 2013, la loi renseignement de 2015, la directive NIS, les responsabilités des intermédiaires techniques (LCEN), le règlement général sur la protection des données européen (RGPD), et les principes généraux autour de la recherche et divulgation de vulnérabilités et la propriété intellectuelle (Hadopi, jurisprudence VideoLan). Il doit également connaître et appliquer les référentiels de sécurité internationaux (ISO / IEC 27001 / 27002, série ISA-99 / IEC 62443, guides NIST, etc.) et nationaux (RGS, II901, guides ANSSI, guides CNIL...) ainsi que les principaux référentiels en gestion de risques (ISO / IEC 27005, EBIOS, EIVP/PIA, BIA...).

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

Justifier de l'une des conditions suivantes :

- Diplôme d'ingénieur habilité par la Commission des Titres d'Ingénieur (CTI)
- Diplôme des instituts d'Etudes Politiques (IEP)
- Diplôme de médecine (6e année validée)
- Diplôme de pharmacie (5e année validée)
- Diplôme des écoles nationales vétérinaires
- Diplômes des écoles nationales supérieures d'architecture
- Diplôme d'une école de management habilitée à délivrer le Grade de Master (CEFDG)
- Master 2 universitaire de toutes spécialités
- Master international de toutes spécialités
- Titre inscrit au RNCP niveau 7 du Cadre européen des certifications
- Master 1 universitaire de toutes spécialités et trois ans d'expérience professionnelle post-diplôme
- Bachelor en 4 ans (français ou international) de toutes spécialités et trois ans d'expérience professionnelle post-diplôme

Sont également examinées à titre dérogatoire (30% maximum de l'effectif admis) les candidatures présentant un cursus original ou un parcours de très grande qualité suivantes :

- Master 1 universitaire de toutes spécialités, sans ou avec moins de 3 ans d'expérience professionnelle post diplôme

en lien avec la formation visée

- Bachelor en 4 ans (français ou international) de toutes spécialités, sans ou avec moins de 3 ans d'expérience professionnelle post-diplôme en lien avec la formation visée
- Licence 3 universitaire de toutes spécialités, plus 3 ans d'expérience professionnelle post-diplôme en lien avec la formation visée
- Bachelor en 3 ans (français ou international) de toutes spécialités, plus 3 ans d'expérience professionnelle post-diplôme en lien avec la formation visée
- La VAPP est également possible avec 5 ans d'expérience professionnelle ayant un lien avéré avec les compétences professionnelles visées par la certification (40% maximum de l'effectif admis)

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

Le jury est composé de 3 personnes : deux professionnels extérieurs à l'autorité de certification dont le président et un membre interne.

COMPOSITION DU JURY — VAE

Le jury est composé de 4 personnes : deux professionnels extérieurs à l'autorité de certification dont le président et deux membres internes.

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	9 350 €
Selon la branche	7 700 € – 10 000 €

Prise en charge	Branches concernées
9 350 €	Valeur par défaut · 180 branches
10 000 €	CPNE Casinos, CPNE Travail Temporaire, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNE des industries de santé (CPNEIS)
8 500 €	CPNE des MFR, CPNE des Métiers de la Transformation des Grains, CPNE des Vins et Spiritueux, CPNE des centres de gestion agréés et habilités agricoles, CPNEFP Transformation Laitière
9 992 €	CPNEFP branche retraite complémentaire et prévoyance, CPNEFP Mutualité
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP du Négoce de l'ameublement
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
9 055 €	CPNEFP Habillement succursaliste
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 750 €	CPNEFP Commerce à distance
8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 000 €	CPNE chimie
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date de décision	28/11/2024
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	28/11/2027

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	18	0	95 %	—
2021	20	0	95 %	90 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP28224

CORRESPONDANCES (PAR BLOCS)

RNCP28224

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://exed.centralesupelec.fr/formation/mastere-specialise-cybersecurite/>

<https://www.imt-atlantique.fr/fr/formation/masteres-specialises/cybersecurite>

Formation continue et valorisation des acquis de l'expérience | IMT Atlantique

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39837/>

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	1
Prix indicatif	18 500 €

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Entrées et sorties de formation

Entrées en formation	3
Parcours menés à terme	2
Taux d'achèvement	67 %
Période	09/2025 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	3
Montant total engagé	45 000 €
Coût moyen par dossier	15 000 €
Durée moyenne	521 h

Période	05/2025 – 06/2026
Reste à charge titulaire	83 %
France compétences	17 %

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