

Spécialiste en cybersécurité (MS)

RNCP38434 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	24293, 31045, 24237, 31008
Code(s) ROME	M1801, M1802, M1810, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	21/12/2023
Date d'échéance	21/12/2028

Certificateur(s)

INSTITUT NATIONAL SCIENCES APPLIQUEES LYON · SIRET : 19690192000013

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le spécialiste en cybersécurité intervient dans la construction ou l'amélioration des fonctions de sécurité d'un système d'information, afin de protéger des malveillances les actifs informationnels d'une organisation.

Il définit, met en œuvre et veille à l'application de la stratégie de gouvernance de la sécurité de l'information. C'est un interlocuteur privilégié de la DSI (Direction des Systèmes d'Information), de la DG (Direction Générale) et des métiers. Il garantit la protection des données et le niveau de sécurité des systèmes d'information.

Il s'assure de l'alignement de la sécurité de l'information avec les objectifs business, réglementaires et organisationnels de l'organisation. Il conçoit l'architecture matérielle et logicielle, support des fonctions de sécurité, adaptées aux besoins des métiers et aux contraintes du système cible (réseaux, systèmes, applications), en tenant compte des règles de l'art, du niveau de sécurité de l'existant et des solutions de sécurité du marché. Il assure la continuité de service dans un but préventif et curatif sur les malveillances et dysfonctionnements.

ACTIVITÉS VISÉES

Élaboration du Système de Management de la Sécurité du Système d'Information (SMSI)

Gouvernance et gestion des accès et des identités

Analyse et cartographie des risques en sécurité de l'information selon la méthodologie EBIOS RM (Risk manager)

Conception et mise en œuvre de la sécurisation d'une Infrastructure IT (réseaux, systèmes, applications)

Étude et Intégration de la sécurité dans le processus de développement d'un produit industriel complexe (Train, Avion, etc.)

Réalisation de tests d'intrusion

Mise en place du plan de continuité et de Reprise d'activité (PCA/PRA)

COMPÉTENCES ATTESTÉES

Définir le périmètre d'application et la politique de sécurité, afin de recenser les actifs informationnels et supports sur lesquels doit porter une démarche d'appréciation des risques et les principes d'action de la politique de sécurité de l'information, grâce au contexte de l'organisation établi et validé par la direction générale

Identifier, apprécier et définir les seuils d'acceptabilité des risques sur le périmètre, afin d'établir un plan de traitement des risques grâce à une méthodologie d'appréciation du risque en concordance avec les objectifs de la politique de sécurité de l'information de l'organisme mais aussi du cadre normatif

Choisir et piloter la mise en place des mesures de sécurité techniques et organisationnelles, afin de réduire ou supprimer des risques, en allouant les moyens budgétaires et humains qui permettront la mise en œuvre effective des

fonctions adéquates de sécurité

Contrôler le SMSI dans une boucle d'amélioration continue, technique, financière et organisationnelle, afin d'éclairer les choix stratégiques à opérer en matière de sécurité, par la mise en place d'indicateurs pertinents sur le périmètre d'analyse

Piloter les différents projets liés à la définition et mise en œuvre du SMSI, afin que le niveau de maturité en cybersécurité de l'organisation soit en phase avec ses choix stratégiques et orientations business, par la mise en œuvre de capacités comportementales tel que leadership, rigueur, sens relationnel, travail en équipe inclusive, gestion du stress, communication orale et écrite, analyse et synthèse, respect des délais et des budgets

Identifier tous les accès internes et externes existants aux actifs (réseaux, systèmes, applications, données), afin de prendre en compte les différents environnements d'utilisateurs Interne, cloud et fédérés par la mise en œuvre d'un audit préalable auprès des responsables d'application

Implémenter et gérer les mécanismes d'autorisation afin de prendre en compte l'évolution des accès par la mise en œuvre de modèles de contrôle des accès, dans une matrice des rôles du ressort des managers des directions métier

Gérer le cycle de vie des identités et du provisionnement des accès, afin de réaliser des revues des accès des utilisateurs, comptes d'accès système, provisionnement et dé-provisionnement

Choisir des solutions de gestion des accès et des identités adaptées au contexte et besoins, afin de mettre en place des architectures IAM (Identity Access Management) , techniques et fonctionnelles, par la mise en œuvre et le déploiement sur les systèmes de fonctions tel que fédération des identités, Single Sign on, gestion des comptes privilégiés etc.

Analyser les données liées aux identités, aux comptes et leurs habilitations applicatives afin de les faire évoluer par la mise en œuvre d'un outillage logiciel

Piloter les différents projets sur la gestion des accès et des identités, afin de permettre à l'organisation de contrôler de manière stricte qui accède à quel actif informationnel et dans quel but ? Par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.

Concevoir une architecture qui prend en compte les enjeux et contraintes techniques, organisationnelles, réglementaires et financières de l'organisation/entreprise, afin de construire une architecture durable, performante et évolutive

Intégrer au mieux les différents équipements et solutions de sécurité du marché (veille technologique approfondie), afin de prendre en compte le contexte propre à l'organisation par la mise en œuvre de techniques de déploiement et de migration compatibles avec le contexte et le cadre réglementaire

Conseiller et/ou convaincre un donneur d'ordre (autorité, chef de projet, chef DSI...), afin de mobiliser les ressources budgétaires et humaines pour réaliser le projet de sécurisation

Piloter les différents projets sur la conception et mise en œuvre des fonctions de sécurité, afin de permettre à l'organisation de protéger son infrastructure par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets

Réaliser les études de sécurité dans le cadre d'un développement de produit industriel afin d'identifier les fonctions de sécurité qui permettront à l'utilisateur d'opérer ce produit en sécurité, en intégrant les étapes classiques de la sécurité (analyse de risque, réduction des risques par intégration des mesures de sécurité, évaluation) au cycle de développement du produit.

Identifier, adapter et intégrer les activités de gestion des risques dans le processus de développement d'un produit industriel complexe (avion, train, etc. ...) par la mise en œuvre de méthodologies adaptées (analyse de code) afin de mettre en conformité son niveau de sécurité

Évaluer les informations de sécurité attendues et le niveau de maturité à chaque étape du processus de développement afin d'établir le niveau de sécurité du produits et les risques résiduels à l'issue de la phase d'intégration finale du produit

Identifier et adapter le processus de gestion du changement du produit afin de maintenir le niveau de sécurité du produit à travers son évolution

Définir et mettre en œuvre un système d'assurance sécurité pour garantir l'atteinte des objectifs de sécurité dans la supply chain

Définir et analyser le périmètre d'intervention afin d'y rechercher des vulnérabilités par une recherche directe ou indirecte d'informations sur l'organisation cible (services accessibles, infrastructure..)

Réaliser des audits de type tests d'intrusion, audit de code, audit de configuration etc. afin d'identifier et qualifier les vecteurs de risques (défauts de configuration, ports ouverts, code non sécurisé etc.), par l'élaboration, et la

planification de scénarios d'attaques

Rédiger pour les métiers, un rapport d'analyse des vulnérabilités découvertes afin de préconiser des mesures correctives, fournir des preuves, rendre compte et documenter

Réaliser des analyses post-mortem (Forensic) afin d'adapter la campagne de tests par l'intégration dans ses propositions des exigences des différents types d'investigation (administratives, criminelles, civiles, réglementaires)

Piloter les différents projets sur la conception et mise en œuvre des tests d'intrusion, afin de permettre à l'organisation de protéger son infrastructure, par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets

Procéder à une classification des applications et serveurs afin d'identifier ceux qui sont critiques, et prévoir leur continuité de fonctionnement, par un questionnement structuré avec les métiers, des visites sur site, des réunions, des tests d'intrusion, un examen des documents existants (politiques, chartes etc.)

Définir avec les métiers et la direction des systèmes d'information la continuité de service, pour les applications et serveurs critiques, afin de garantir un fonctionnement normal, par l'estimation des critères de continuité de service (durée d'interruption maximal du service, perte de données maximum admissible etc.)

Définir une organisation afin de gérer le plus efficacement possible un sinistre par la mise en œuvre d'une équipe dédiée PCA/PRA

Identifier les évolutions à apporter au PCA/PRA, afin d'anticiper de futures cyber-crisis, en inscrivant le PCA/PRA dans une boucle d'amélioration continue avec la mise en œuvre d'un plan de maintien en condition opérationnelle

Piloter le projet de PCA/PRA afin de permettre à l'organisation d'augmenter sa résilience, par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets

Blocs de compétences

RNCP38434BC01 — Elaborer la stratégie et gouvernance de la sécurité de l'information

LISTE DE COMPÉTENCES

Définir le périmètre d'application et la politique de sécurité, afin de recenser les actifs informationnels et supports sur lesquels doit porter une démarche d'appréciation des risques et les principes d'action de la politique de sécurité de l'information, grâce au contexte de l'organisation établi et validé par la direction générale

Identifier, apprécier et définir les seuils d'acceptabilité des risques sur le périmètre, afin d'établir un plan de traitement des risques grâce à une méthodologie d'appréciation du risque en concordance avec les objectifs de la politique de sécurité de l'information de l'organisme mais aussi du cadre normatif

Choisir et piloter la mise en place des mesures de sécurité techniques et organisationnelles, afin de réduire ou supprimer des risques, en allouant les moyens budgétaires et humains qui permettront la mise en œuvre effective des fonctions adéquates de sécurité

Contrôler le SMSI dans une boucle d'amélioration continue, technique, financière et organisationnelle, afin d'éclairer les choix stratégiques à opérer en matière de sécurité, par la mise en place d'indicateurs pertinents sur le périmètre d'analyse

Piloter les différents projets liés à la définition et mise en œuvre du SMSI, afin que le niveau de maturité en cybersécurité de l'organisation soit en phase avec ses choix stratégiques et orientations business, par la mise en œuvre de capacités comportementales tel que leadership, rigueur, sens relationnel, travail en équipe inclusive, gestion du stress, communication orale et écrite, analyse et synthèse, respect des délais et des budgets

Identifier tous les accès internes et externes existants aux actifs (réseaux, systèmes, applications, données), afin de prendre en compte les différents environnements d'utilisateurs Interne, cloud et fédérés par la mise en œuvre d'un audit préalable auprès des responsables d'application

Implémenter et gérer les mécanismes d'autorisation afin de prendre en compte l'évolution des accès par la mise en œuvre de modèles de contrôle des accès, dans une matrice des rôles du ressort des managers des directions métier

Gérer le cycle de vie des identités et du provisionnement des accès, afin de réaliser des revues des accès des utilisateurs, comptes d'accès système, provisionnement et dé-provisionnement

Choisir des solutions de gestion des accès et des identités adaptées au contexte et besoins, afin de mettre en place des architectures IAM (Identity Access Management) , techniques et fonctionnelles, par la mise en œuvre et le déploiement sur les systèmes de fonctions tel que fédération des identités, Single Sign on, gestion des comptes privilégiés etc.

Analyser les données liées aux identités, aux comptes et leurs habilitations applicatives afin de les faire évoluer par la mise en œuvre d'un outillage logiciel

Piloter les différents projets sur la gestion des accès et des identités, afin de permettre à l'organisation de contrôler de manière stricte qui accède à quel actif informationnel et dans quel but ? Par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.

MODALITÉS D'ÉVALUATION

Cas pratiques - rendu de livrables - soutenance orale

RNCP38434BC02 — Concevoir et mettre en service d'infrastructures de cybersécurité

LISTE DE COMPÉTENCES

Concevoir une architecture qui prend en compte les enjeux et contraintes techniques, organisationnelles, réglementaires et financières de l'organisation/entreprise, afin de construire une architecture durable, performante et évolutive

Intégrer au mieux les différents équipements et solutions de sécurité du marché (veille technologique approfondie), afin de prendre en compte le contexte propre à l'organisation par la mise en œuvre de techniques de déploiement et de migration compatibles avec le contexte et le cadre réglementaire

Conseiller et/ou convaincre un donneur d'ordre (autorité, chef de projet, chef DSI...), afin de mobiliser les ressources budgétaires et humaines pour réaliser le projet de sécurisation

Piloter les différents projets sur la conception et mise en œuvre des fonctions de sécurité, afin de permettre à l'organisation de protéger son infrastructure par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets

Réaliser les études de sécurité dans le cadre d'un développement de produit industriel afin d'identifier les fonctions de sécurité qui permettront à l'utilisateur d'opérer ce produit en sécurité, en intégrant les étapes classiques de la sécurité (analyse de risque, réduction des risques par intégration des mesures de sécurité, évaluation) au cycle de développement du produit.

Identifier, adapter et intégrer les activités de gestion des risques dans le processus de développement d'un produit industriel complexe (avion, train, etc. ...) par la mise en œuvre de méthodologies adaptées (analyse de code) afin de mettre en conformité son niveau de sécurité

Évaluer les informations de sécurité attendues et le niveau de maturité à chaque étape du processus de développement afin d'établir le niveau de sécurité du produits et les risques résiduels à l'issue de la phase d'intégration finale du produit

Identifier et adapter le processus de gestion du changement du produit afin de maintenir le niveau de sécurité du produit à travers son évolution

Définir et mettre en œuvre un système d'assurance sécurité pour garantir l'atteinte des objectifs de sécurité dans la supply chain

MODALITÉS D'ÉVALUATION

Cas pratiques - rendu de livrables - soutenance orale

RNCP38434BC03 — Maintenir en continuité de service

LISTE DE COMPÉTENCES

Définir et analyser le périmètre d'intervention afin d'y rechercher des vulnérabilités par une recherche directe ou indirecte d'informations sur l'organisation cible (services accessibles, infrastructure..)

Réaliser des audits de type tests d'intrusion, audit de code, audit de configuration etc. afin d'identifier et qualifier les vecteurs de risques (défauts de configuration, ports ouverts, code non sécurisé etc.), par l'élaboration, et la planification de scénarios d'attaques

Rédiger pour les métiers, un rapport d'analyse des vulnérabilités découvertes afin de préconiser des mesures correctives, fournir des preuves, rendre compte et documenter

Réaliser des analyses post-mortem (Forensic) afin d'adapter la campagne de tests par l'intégration dans ses propositions des exigences des différents types d'investigation (administratives, criminelles, civiles, réglementaires)

Piloter les différents projets sur la conception et mise en œuvre des tests d'intrusion, afin de permettre à l'organisation de protéger son infrastructure, par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et

écrite, respect des délais et des budgets

Procéder à une classification des applications et serveurs afin d'identifier ceux qui sont critiques, et prévoir leur continuité de fonctionnement, par un questionnement structuré avec les métiers, des visites sur site, des réunions, des tests d'intrusion, un examen des documents existants (politiques, chartes etc.

Définir avec les métiers et la direction des systèmes d'information la continuité de service, pour les applications et serveurs critiques, afin de garantir un fonctionnement normal, par l'estimation des critères de continuité de service (durée d'interruption maximal du service, perte de données maximum admissible etc.)

Définir une organisation afin de gérer le plus efficacement possible un sinistre par la mise en œuvre d'une équipe dédiée PCA/PRA

Identifier les évolutions à apporter au PCA/PRA, afin d'anticiper de futures cyber-crises, en inscrivant le PCA/PRA dans une boucle d'amélioration continue avec la mise en œuvre d'un plan de maintien en condition opérationnelle

Piloter le projet de PCA/PRA afin de permettre à l'organisation d'augmenter sa résilience, par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets

MODALITÉS D'ÉVALUATION

Cas pratiques - rendu de livrables - soutenance orale

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le spécialiste en cybersécurité peut exercer dans des entreprises de toute taille : de la TPE à la grande entreprise, en passant par les entreprises publiques, les opérateurs en télécommunication et les ESN

TYPE D'EMPLOIS ACCESSIBLES

RSSI

Consultant organisationnel en cybersécurité

Auditeur organisationnel en cybersécurité

Consultant technique en cybersécurité

Ingénieur-Intégrateur de solutions en cybersécurité

Analyste cybersécurité

Chef de projet cybersécurité

Auditeur technique d'infrastructures de cybersécurité

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les conditions d'accès sont définies dans le règlement intérieur de la Conférence des Grandes Ecoles (CGE).

L'admission des étudiants et l'organisation des études sont de la responsabilité de l'établissement délivrant le Mastère Spécialisé®. Sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :

Diplôme d'ingénieur habilité par la Commission des Titres d'Ingénieur (liste CTI)

Diplôme d'une école de management habilitée à délivrer le grade national de Master (liste CEFDG)

Diplôme de 3ème cycle habilité par les autorités universitaires (DEA, DESS, Master...) ou diplôme professionnel de niveau BAC + 5

Diplôme de M1 ou équivalent, pour des auditeurs justifiant d'au moins trois années d'expérience professionnelle.

Titre inscrit au RNCP niveau 7 (ancienne nomenclature niveau I)

Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Pour des diplômes anciens, qui ne sont plus actuellement délivrés, on se rapprochera de ceux qui s'y sont éventuellement substitués.

Conditions d'accès dérogatoires :

a) Dans la limite de 40 % maximum de l'effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des acquis personnels et professionnels (VAPP), les candidatures de personnes justifiant a minima de 5 années d'expérience professionnelle (hors stage, césure, cursus initial en alternance).

b) Par dérogation pour 30 % maximum du nombre d'étudiants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :

Niveau M1 validé ou équivalent sans expérience professionnelle

Diplôme de L3 justifiant d'une expérience adaptée de 3 ans minimum

Le pourcentage total des dérogations prévues au a) et au b) ci-dessus ne doit pas excéder 40%.

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

Le jury est composé de 4 membres dont 2 professionnels externes

COMPOSITION DU JURY — VAE

Le jury est composé de 6 membres dont 3 professionnels externes

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	9 157 €
Selon la branche	8 000 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 173 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE Services de l'eau, 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
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de la branche Banque Populaire, CPNE des métiers du géomètre, CPNEFP de la profession d'économiste de la construction
10 000 €	CPNE des exploitations frigorifiques, CPNE des industries de santé (CPNEIS), Commission Paritaire Activités de Marchés Financiers
8 696 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP des jardineries et graineteries, CPNEFP du Négoce de l'ameublement
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 200 €	CPNEFP de la Mutualité Sociale Agricole
10 500 €	CPNEFP des industries des tuiles et briques
10 164 €	CPNE de la branche de la Distribution Directe
10 163 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
9 992 €	CPNEFP Mutualité
9 800 €	CPNEF de l'audiovisuel
9 231 €	CPNEFP Commerce à distance
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
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 701 €	CPNE FP Branche des magasins du Bricolage
8 520 €	CPNE de la branche des experts comptables et commissaires aux comptes
8 500 €	CPNEFP de la métallurgie
8 000 €	CPNE chimie

Base légale

Date de décision	21/12/2023
Durée de l'enregistrement	5 ans

Date d'échéance de l'enregistrement	21/12/2028
Date de dernière délivrance possible	21/12/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	20	0	100 %	—
2021	19	0	100 %	100 %
2020	16	0	100 %	100 %
2019	15	0	100 %	100 %

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.insa-lyon.fr/fr/mastere-cybersecurite-numerique>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38434/>

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	1
Prix indicatif	15 000 €
Durée	1549 h

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

Entrées et sorties de formation

Entrées en formation	23
Parcours menés à terme	15
Taux d'achèvement	65 %
Période	02/2024 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	23
Montant total engagé	168 145 €
Coût moyen par dossier	7 311 €
Durée moyenne	1363 h
Période	01/2024 – 09/2026
Reste à charge titulaire	45 %

France compétences	35 %
Entreprise	13 %
France Travail	7 %

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