

Programme de la formation

Cybersécurité, IA et Protection des Données — Sécurisez les applications, les API et les données de l'entreprise Formation tutorée à distance 120 heures Tout public, Salarié en poste, Demandeur d'emploi, Particulier, Indépendant et dirigeant, Etudiant, Jeune en insertion professionnelle · De 1 à 5 participants À partir de 3 500 € Net de taxe par participant Éligible au CPF (Code : <https://www.francecompetences.fr/recherche/rncp/40792>) Formation certifiante [RNCP40792](#) gérée par France Compétences**Description courte**

Ce parcours opérationnel forme des professionnels capables de protéger les données personnelles, l'identité numérique, les équipements, les usages, les applications et les API, puis de détecter et traiter des incidents de sécurité. Il associe cadre juridique, pratiques techniques, analyse de risques et réponse aux incidents.

Un projet fil rouge SecureFlow met le participant en situation de sécuriser une application SaaS manipulant des données clients. Chaque module produit une preuve professionnelle : registre des risques, politique de protection des données, matrice IAM, audit applicatif, analyse de logs, dossier d'incident et plan de sécurisation.

La formation prépare spécifiquement au bloc RNCP40792BC05 et à son épreuve ponctuelle écrite officielle.

Profil des participants

Développeurs juniors ou confirmés souhaitant intégrer la sécurité dans leurs pratiques.

Cette formation s'adresse en priorité aux :

- **Data Analysts et Data Engineers** souhaitant mieux protéger les données et les pipelines.
- **Techniciens informatiques et profils support** souhaitant évoluer vers des missions cyber.
- **Chefs de projet** technique et professionnels des systèmes d'information.
- **Demandeurs d'emploi et professionnels en reconversion** disposant d'une première culture informatique.

Prérequis

- Maîtrise des usages informatiques courants et capacité à installer des outils.

- Notions de base en systèmes, réseaux, développement ou données ; une consolidation est prévue au début du parcours.
- Capacité à utiliser un terminal et à lire une documentation technique simple en anglais.
- Respect impératif du cadre légal et utilisation des outils de sécurité uniquement sur les environnements autorisés de la formation.

Objectifs

À l'issue du parcours, les participants seront capables de :

- Analyser les risques cyber et prioriser des mesures de traitement.
- Protéger les données personnelles et appliquer les principes essentiels du RGPD.
- Préserver l'identité numérique de l'organisation et sécuriser les accès et privilèges.
- Sécuriser les équipements, les usages, les applications, les API et les bases de données.
- Mettre en œuvre des contrôles alignés sur des référentiels et standards de sécurité.
- Collecter et analyser des logs afin de détecter des actions malveillantes.
- Qualifier un incident, préserver les preuves et proposer des contre-mesures.
- Utiliser l'IA comme assistant défensif sous contrôle humain et dans le respect de la confidentialité.

Aptitudes et compétences visées / attestées

À l'issue de la formation, le candidat sera capable de :

- Protéger les données à caractère personnel : recenser les traitements, identifier les risques, appliquer la réglementation et sensibiliser les utilisateurs.
- Préserver l'identité numérique de l'organisation et déployer des moyens appropriés de preuve électronique.
- Sécuriser les équipements et les usages : informer, identifier les menaces, gérer les accès et vérifier l'efficacité de la protection.
- Garantir la disponibilité, l'intégrité et la confidentialité des services et des données face aux cyberattaques.
- Organiser la collecte et la conservation de preuves numériques et appliquer les procédures liées aux obligations légales.
- Assurer la cybersécurité d'une solution applicative et de son développement, prévenir les attaques et vérifier la conformité à un référentiel.
- Analyser les connexions et les incidents de sécurité, puis proposer et mettre en œuvre des contre-mesures.

Contenu

Siège social 144 rue Paul Bellamy – 44000 NANTES

SAS au capital de 100 000 € - SIRET 452 558 893 00049 – 02 51 84 95 55 – contact@cadresenmission.com
Numéro d'enregistrement de formation : 52 44 06368 44 auprès du Préfet de la Région Pays de la Loire

La formation repose sur un accompagnement individuel et se déroule sur 4 mois. Elle combine **100 heures de formation tutorée à distance et d'activités pédagogiques** avec **20 heures de mentorat**

individuel en visioconférence. Le rythme indicatif est de 7 heures par semaine, adaptable dans le respect du calendrier contractualisé.

Un **projet fil rouge** relie les apprentissages et constitue le support des exercices, audits et incidents simulés.

MODULE 1 — Fondamentaux de la Cybersécurité et Analyse des Risques

MODULE 2 — Protection des Données, RGPD et Preuve Numérique

MODULE 3 — Identités, Accès, Postes et Usages Sécurisés

MODULE 4 — Sécurité des Applications, API et Bases de Données

MODULE 5 — Logs, Détection, Incidents et IA Défensive

MODULE 6 — Projet Final et Préparation au Bloc RNCP40792BC05

Pédagogie et organisation

Ce dispositif garantit une montée en compétences progressive, structurée et directement applicable aux enjeux des entreprises.

La formation repose sur une **pédagogie par la pratique**. Le projet fil rouge relie les apprentissages. Elle est proposée **100 % à distance** et comprend **100 heures de formation tutorée à distance et d'activités pédagogiques** : ressources structurées, démonstrations, exercices, études de cas, travaux pratiques, évaluations et réalisation des projets. Elle comprend également **20 heures de mentorat individuel** en visioconférence avec un expert cyber, réparties sur les 4 mois.

Positionnement et Modalités d'évaluation des acquis

- **Positionnement** : Entretien de positionnement obligatoire avant l'entrée en formation pour vérifier les attentes et les prérequis, valider le profil et définir le parcours individualisé.
- **Évaluations formatives** : QCM et auto-évaluations par module, exercices corrigés avec feedback personnalisé du mentor.
- **Évaluations sommatives** : Mini-projets avec soutenance orale à l'issue de chaque module.
- **Certification** : La formation prépare au bloc de compétences RNCP40792BC05 — Cybersécurité des services informatiques, option B « Solutions logicielles et applications métiers ». L'évaluation du bloc est organisée par l'organisme certificateur. Le candidat peut se présenter en candidat libre, selon les modalités définies par le certificateur. Une procédure détaillée est fournie en fin de formation pour accompagner l'apprenant dans son inscription.

Mode de validation

- **Attestation de fin de formation** délivrée par MyDataMentor à l'issue du parcours.
- **Projet final** présenté en soutenance devant le formateur.
- La formation prépare au bloc de compétences RNCP40792BC05 — Cybersécurité des services informatiques, option B « Solutions logicielles et applications métiers ».
- L'évaluation du bloc est organisée par l'organisme certificateur (Ministère de l'enseignement supérieur et de la recherche).
- Le candidat peut se présenter à la certification en tant que **candidat libre**. Une procédure détaillée est transmise en fin de formation.
- Seul le Ministère de l'enseignement supérieur et de la recherche est habilité à délivrer le bloc de compétences.

Financements possibles

Cette formation est éligible à plusieurs dispositifs de financement, sous réserve des critères propres à chaque organisme :

- **Financement public** : CPF (Mon Compte Formation), OPCO (selon branche professionnelle — particulièrement adapté au financement via plan de développement des compétences entreprise), AGEFICE (TNS du commerce), FIF-PL (professions libérales), France Travail (demandeurs d'emploi).
- **Financement entreprise** : Prise en charge possible dans le cadre du plan de développement des compétences de l'employeur — devis sur demande pour les entreprises souhaitant former plusieurs collaborateurs.
- **Financement personnel** : Possibilité d'échelonnement et de facilités de paiement pour les apprenants finançant la formation à titre individuel..

Modalités et délai d'accès

- **Inscriptions** : Ouvertes en continu tout au long de l'année.
- **Durée & Rythme** : 120 heures en distanciel sur 4 mois, soit un rythme indicatif de 7 heures par semaine.
- **Délais d'accès** : Démarrage possible sous 14 jours après validation administrative et entretien de positionnement. Planning adaptable et individualisé dès l'entrée en formation.

Référent handicap

PERSONNES EN SITUATION DE HANDICAP : (*mise en place de compensation...*)

Contact : Référent handicap 02 51 84 95 55 / 06 28 70 45 28 / nadiahadjeri@cadresenmission.com

Accessibilité aux personnes en situation de handicap

Personnes en situation de handicap : On s'engage pour l'inclusion de tous les apprenants. Un protocole d'adaptation aux modalités pédagogiques et de passation à la certification est mis en place pour chaque situation individuelle (aménagement du temps, supports adaptés, accompagnement renforcé).

Contactez notre référent handicap pour toute demande d'aménagement avant l'entrée en formation.