

Expert en développement de solutions de cybersécurité

RNCP38463 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1802, M1801, M1805, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	21/12/2023
Date d'échéance	21/12/2026

Certificateur(s)

ASSOCIATION D'ENSEIGNEMENT TECHNIQUE SUPERIEUR AN21 ACADEMIE NUMERIQUE DU XXIEME SIECLE · SIRET : 85137784600031

ASSOCIATION D'ENSEIGNEMENT TECHNIQUE SUPERIEUR AN21 ACADEMIE NUMERIQUE DU XXIEME SIECLE · SIRET : 85137784600023

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CODA	92219486500031	Former et organiser l'évaluation
CSB EDUCATION GROUP	92991594000019	Former et organiser l'évaluation
DRS SCHOOL	85398915000018	Former et organiser l'évaluation
HECTEN	94943720600020	Former et organiser l'évaluation
IFIR ARL (AIN-RHONE-LOIRE)	38134879600024	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les attaques informatiques menacent en temps réel le fonctionnement de nos organisations, qu'elles soient du public ou privé. Dans ce contexte agressive, l'ensemble de nos structures prennent progressivement conscience, qu'au-delà de leur fonctionnement au quotidien, leur survie et avenir sont directement lésés. Ces évolutions impactant les métiers liés à la sécurité des systèmes d'information entraînent des besoins en compétences nouveaux, notamment sur le champ de la stratégie, le développement interne et le développement de solutions utilisant les technologies émergentes sous les aspects sécurité.

Les processus de l'innovation et du développement de solutions sécurisées ne sont plus l'affaire exclusive des Directeurs des systèmes d'information (DSI) ou des Directeurs de la Sécurité des Systèmes d'Information (DSSI). La Direction Générale, au même titre que les entités RH, Finance ou Qualité, doit intégrer la Cybersécurité dans la stratégie globale et embarquer chacun de ses collaborateurs dans cette démarche. Pour cela, les entreprises ont besoin de collaborateurs experts dans la mise en place, la gestion et la coordination de solutions de sécurité mais aussi dans l'accompagnement, la gestion d'équipe et l'intégration des solutions dans la stratégie interne d'une entreprise.

Ainsi, le métier d'Expert en développement de solution de cybersécurité évolue dans ses missions et peut être exercé dans tous les secteurs que ce soit industriel, privé, public ou dans les sociétés de services.

Face à ces nouveaux défis de la Cybersécurité, les profils sont depuis quelques années difficiles à trouver, et ce d'autant plus que le champ des missions et des compétences est complexe, hétérogène et difficile à appréhender.

ACTIVITÉS VISÉES

L'expert en développement de solutions de Cybersécurité

joue à la fois un rôle de préventeur, de stratège et de pilote d'actions à mettre en œuvre dans le cadre de solutions et de produits de sécurité? adaptés au contexte des menaces de cybersécurité?.

Il est celui qui encadre l'analyse des menaces et des besoins associés à la cybersécurité qui en découlent afin de pouvoir proposer et orchestrer le développement des logiciels et des applications sûrs. Parallèlement il intègre les évolutions futures, discute et propose des stratégies de défense adaptées aux évolutions de cet univers en fonction des différentes stratégies mises en œuvre.

Ses activités sont réparties en 5 grands domaines :

L'analyse technique et fonctionnelle du contexte dans une démarche de développement de solutions de cybersécurité :

- Analyser et prendre en compte les besoins de cybersécurité et le contexte de menaces
- Imaginer, proposer, argumenter et accompagner une stratégie Cybersécurité
- Contribuer à la définition des spécifications générales de la solution de sécurité
- Valider l'analyse technique et l'étude détaillée de la solution de sécurité
- Piloter la mise en œuvre le projet technique et communiquer sur les actions induites

L'organisation et le pilotage du développement de la solution de cybersécurité :

- Valider le résultat d'un audit et analyser le contexte pour imaginer les solutions de développement
- Orchestrer les différents projets de développement de solutions de cybersécurité
- Contrôler le développement de solutions de cybersécurité sélectionnées et les résultats obtenus
- Encadrer le développement des logiciels adaptés aux systèmes embarqués et Machine Learning

La qualification de la solution de cybersécurité :

- Superviser le prototypage et les tests nécessaires pour s'assurer que les solutions de sécurité répondent bien aux exigences de protection ou de détection
- Faciliter et accompagner l'implémentation de la solution ou du produit dans une architecture logicielle et le tester
- S'assurer du bon accompagnement par les équipes projet auprès de l'ensemble des opérateurs lors de la mise en œuvre et de l'appropriation des solutions proposées

La maintenance de la solution de cybersécurité :

- Organiser la maintenance corrective et la maintenance adaptative évolutive des solutions de sécurité
- Mettre en place et faire respecter un processus regroupant l'ensemble des actions à vocation corrective et d'amélioration continue

L'animation d'un collectif au service de la sécurité :

- Participer aux échanges avec les Directions et les décideurs
- Piloter et dynamiser l'équipe en charge des développements et améliorations
- Recruter, encadrer et gérer une équipe au quotidien
- Vulgariser et faciliter l'appropriation des solutions par l'ensemble des personnes impactés

COMPÉTENCES ATTESTÉES

- Proposer une stratégie globale de protection en termes de cybersécurité en tenant compte des enjeux, du développement et de l'environnement de l'entreprise
- Définir une stratégie de sécurisation en tenant compte du contexte technique, organisationnel et légal de l'entreprise afin d'apporter une réponse adaptée au regard des risques identifiés
- Mettre en œuvre une veille sur les dernières innovations technologiques applicables à l'entreprise afin de comprendre les technologies en évolution et envisager des solutions pour le futur (Cybersécurité, Cyber-robotique, intelligence artificielle, ML, etc.)
- Analyser les besoins de sécurité et le contexte des menaces propres à chacune des technologies afin d'élaborer des solutions en cohérence avec les priorités stratégiques et les besoins du client et formuler le tableau des exigences techniques
- Appliquer une méthodologie de gestion de projet et une organisation adaptée afin de garantir un résultat respectant les exigences techniques et fonctionnelles du cahier des charges
- Communiquer auprès de l'équipe et le commanditaire en organisant des réunions de travail et des comités de suivi

afin de garantir des prises de décision et faciliter le déroulement du projet

- Réaliser un audit de sécurité sur les solutions existantes en listant leurs forces et leurs vulnérabilités afin de définir un plan de remise en conformité des équipements sensibles et vulnérables
- Sélectionner des scénarii de développement de solutions potentielles en s'appuyant sur une étude de faisabilité et selon des critères bien définis afin de retenir la solution la plus adaptée par rapport aux exigences exprimées par le client
- Développer une solution sécurité en appliquant les bonnes pratiques de cybersécurité afin de garantir un résultat respectant les normes et réglementation en vigueur
- Mettre en place un modèle de Machine Learning en s'appuyant sur un jeu de données pertinent afin d'augmenter la performance de la solution de sécurité
- Développer le logiciel permettant de mettre en place l'algorithme d'intelligence artificielle en s'appuyant sur une analyse des fonctionnalités afin d'évaluer sa pertinence par rapport au projet
- Sélectionner et configurer les différents équipements en appliquant les bonnes pratiques Cybersécurité afin de renforcer la sécurité des systèmes embarqués
- Valider la solution sur les aspects de sécurité en construisant un prototype afin de garantir la faisabilité de l'architecture dans les systèmes réseaux avant sa mise en œuvre
- Conduire un plan de tests techniques en déployant des méthodologies de tests afin de contrôler la qualité du code, la performance et la sécurité de la solution
- Orchestrer le déploiement de la solution en communiquant tous les protocoles nécessaires aux équipes d'exploitation et de maintenance afin de garantir la réalisation des bénéfices attendus de la solution
- Superviser l'assistance auprès des parties prenantes en charge de l'installation de la solution en production afin de résoudre les dysfonctionnements de la solution
- Élaborer des scénarii d'évolution de la solution en tenant compte des retours des équipes d'exploitation et du client afin de garantir la cohérence globale de la solution
- Mettre en exploitation la solution en veillant à son adaptation au regard des besoins utilisateurs afin de faciliter son appropriation et son utilisation
- Résoudre des opérations de maintenance complexes en effectuant une analyse des causes afin d'évaluer les vulnérabilités et les menaces et les corriger
- Rendre compte des incidents et dysfonctionnements de la solution dans le logiciel de suivi à disposition afin de contribuer à l'amélioration continue de la solution tout au long de son cycle de vie
- Encadrer et animer une équipe projet en mettant en œuvre des méthodes et des outils efficaces afin de faciliter la réalisation du projet et travailler efficacement au quotidien avec l'ensemble des parties prenantes
- Conduire des réunions de projet en structurant sa présentation orale et écrite afin de faciliter l'avancement du projet et le partage d'informations
- Mettre en place une communication adaptée en démocratisant le processus technique cybersécurité afin de faciliter l'adhésion de l'ensemble des parties prenantes
- Piloter une équipe dans le respect du cadre légal, des droits et devoirs de chacun

Blocs de compétences

RNCP38463BC01 — Mettre en place une stratégie de cybersécurité dans une démarche de développement de solutions

LISTE DE COMPÉTENCES

Proposer une stratégie globale de protection en termes de cybersécurité en tenant compte des enjeux, du développement et de l'environnement de l'entreprise

Définir une stratégie de sécurisation en tenant compte du contexte technique, organisationnel et légal de l'entreprise afin d'apporter une réponse adaptée au regard des risques identifiés

Mettre en œuvre une veille sur les dernières innovations technologiques applicables à l'entreprise afin de comprendre les technologies en évolution et envisager des solutions pour le futur (cybersécurité, cyber-robotique, intelligence artificielle, ML, etc.)

Proposer une stratégie globale de protection en termes de cybersécurité en tenant compte des enjeux, du développement et de l'environnement de l'entreprise

Appliquer une méthodologie de gestion de projet et une organisation adaptée afin de garantir un résultat respectant les exigences techniques et fonctionnelles du cahier des charges

Communication auprès de l'équipe et le commanditaire en organisant des réunions de travail et des comités de suivi afin de garantir des prises de décision et faciliter le déroulement du projet

MODALITÉS D'ÉVALUATION

L'ensemble des évaluations se font sous la forme de mise en situation au travers d'étude cas d'entreprise (réels et/ou fictifs).

RNCP38463BC02 — Construire des solutions de cybersécurité en utilisant les technologies émergentes

LISTE DE COMPÉTENCES

Réaliser un audit de sécurité sur les solutions existantes en listant leurs forces et leurs vulnérabilités afin de définir un plan de remise en conformité des équipements sensibles et vulnérables

Sélectionner des scénarii de développement de solutions potentielles en s'appuyant sur une étude de faisabilité et selon les critères bien définis afin de retenir la solution la plus adaptée par rapport aux exigences exprimées par le client

Développer une solution sécurité en appliquant les bonnes pratiques de cybersécurité afin de garantir un résultat respectant les normes et réglementations en vigueur

Mettre en place un modèle de Machine Learning en s'appuyant sur un jeu de données pertinent afin d'augmenter la performance de la solution de sécurité

Développer le logiciel permettant de mettre en place l'algorithme d'intelligence artificielle en s'appuyant sur une analyse des fonctionnalités afin d'évaluer sa pertinence par rapport au projet

Sélectionner et configurer les différents équipements en appliquant les bonnes pratiques cybersécurité afin de renforcer la sécurité des systèmes embarqués

MODALITÉS D'ÉVALUATION

L'ensemble des évaluations se font sous la forme de mise en situation professionnelle, d'étude cas d'entreprise (réels et/ou fictifs) et sous la forme d'une questionnaire à visée professionnelle.

RNCP38463BC03 — Intégrer des solutions de cybersécurité dans le système d'information

LISTE DE COMPÉTENCES

Valider la solution sur les aspects de sécurité en construisant un prototype afin de garantir la faisabilité de l'architecture dans les systèmes réseaux avant sa mise en oeuvre

Conduire un plan de tests techniques en déployant des méthodologies de tests afin de contrôler la qualité du code, la performance et la sécurité de la solution

Orchestrer le déploiement de la solution en communiquant tous les protocoles nécessaires aux équipes d'exploitation et de maintenance afin de garantir la réalisation des bénéfices attendus de la solution

Superviser l'assistance auprès des parties prenantes en charge de l'installation de la solution en production afin de résoudre les dysfonctionnements de la solution

Élaborer des scénarii d'évolution de la solution en tenant compte des retours des équipes d'exploitation et du client afin de garantir la cohérence globale de la solution

MODALITÉS D'ÉVALUATION

L'ensemble des évaluations se font sous la forme de mise en situation professionnelle et d'étude cas d'entreprise (réels et/ou fictifs).

RNCP38463BC04 — Assurer la mise en exploitation et la maintenance de solutions de cybersécurité développées

LISTE DE COMPÉTENCES

Mettre en exploitation la solution veillant à son adaptation au regard des besoins utilisateurs afin de faciliter son appropriation et son utilisation

Résoudre des opérations de maintenance complexes en effectuant une analyse des causes afin d'évaluer les vulnérabilités et les menaces et les corriger

Rendre compte des incidents et dysfonctionnements de la solution dans le logiciel de suivi à disposition afin de contribuer à l'amélioration continue de la solution tout au long de son cycle de vie

MODALITÉS D'ÉVALUATION

L'ensemble des évaluations se font sous la forme de mise en situation professionnelle (réelle et/ou fictive)

RNCP38463BC05 — Animer et encadrer une équipe au quotidien et en mode projet

LISTE DE COMPÉTENCES

Encadrer et animer une équipe projet en mettant en oeuvre des méthodes et des outils efficaces afin de faciliter la réalisation du projet et travailler efficacement au quotidien avec l'ensemble des parties prenantes

Conduire des réunions de projet en structurant sa présentation orale et écrite afin de faciliter l'avancement du projet et le partage d'informations

Mettre en place une communication adaptée en démocratisant le processus technique cybersécurité afin de faciliter l'adhésion de l'ensemble des parties prenantes

Piloter une équipe dans le respect du cadre légal, des droits et devoirs de chacun

MODALITÉS D'ÉVALUATION

L'ensemble des évaluations se font sous la forme de mise en situation au travers d'étude cas d'entreprise (réels et/ou fictifs).

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert en développement de solutions de sécurité peut travailler dans tous les secteurs d'activités publics et privés ayant un système d'information.

Il peut exercer dans :

- Tous les secteurs industriels au sein de structures privées ou publiques ;
- Des sociétés de services telles que des éditeurs de logiciels, des entreprises, informatiques, ou encore des sociétés de conseil en hautes technologies ;
- Dans le secteur public, corps d'état ou collectivités territoriales.

Pour rester autonome dans le choix de ses missions et de ses clients, il peut également exercer son métier en tant qu'indépendant, sous le statut d'auto-entrepreneur ou d'une société individuelle en travaillant pour le compte de clients faisant appel à ses compétences.

TYPE D'EMPLOIS ACCESSIBLES

- Lead-concepteur Cybersécurité
- Expert développeur en produits de sécurité
- Consultant(e) Expert DevOps
- Intégrateur Expert de solutions de sécurité.
- Security Product Developer Manager
- Consultant expert en Cybersécurité

RÈGLEMENTATIONS D'ACTIVITÉ

Le cadre législatif et réglementaire de la cybersécurité constitue un enjeu, car son évolution et adaptation pour faire face à la montée de la cybercriminalité sont permanentes. La prise en compte de ces contraintes est exprimée et évaluée

au fil des référentiels.

A date les réglementations en vigueur sont :

- Loi Godfrain du 5 Janvier 1988 réglementant les systèmes de traitements automatisés de données, la falsification de documents informatisés et toutes tentatives de délits informatiques en groupes organisés.
- Loi informatique et libertés, créée en 1978 et modifiée en 2004, concernant l'ensemble des traitements automatisés de données personnelles
- RGPD ou "Règlement Général sur la Protection des Données" renforçant l'obligation d'information et de transparence à l'égard de toutes les personnes par rapport au traitement de leurs données
- Loi "Cybersecurity Act" entrée en vigueur le 27 Juin 2019, elle s'applique à l'ensemble de l'Union Européenne et oblige tout organisme économique (public ou privé) à sécuriser tout le cycle de vie d'un produit ou d'un service, protéger ses données et veiller à ce que seuls les ayants droits puissent accéder aux données personnelles.
- Loi "CyberScore" du 3 Mars 2022, mettant en place une certification de cybersécurité à destination des plateformes numériques afin que les internautes qui fréquentent ces sites et/ou ces réseaux sociaux puissent identifier le niveau de sécurité des plateformes concernées et connaître la sécurisation de leurs données.

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

L'entrée en formation est accessible pour des titulaires d'un Niveau 6 en informatique ou équivalent.

La certification s'adresse à des candidats titulaires d'un niveau 6 dans le domaine de l'informatique, les sciences de l'ingénieur et/ou qui apportent la preuve d'une expérience professionnelle de trois années au moins dans le champ de la certification visée.

A titre dérogatoire, pourront être considérées comme recevables les candidatures qui, tout en ne répondant pas aux critères formels ci-dessus, apparaîtraient exceptionnelles au vu du dossier. Ces dérogations visent en particulier à autoriser l'admission de personnes ayant exercé pendant plusieurs années des fonctions en lien avec des activités informatiques de haut niveau et dont l'employeur propose un changement d'activité?, et/ou des personnes en reconversion professionnelle, ou une validation des acquis de l'expérience.

Les candidats présentant un dossier satisfaisant aux critères énoncés ci-dessus seront convoqués pour un entretien, en présentiel ou distanciel selon la situation, par le Responsable pédagogique en charge de la certification. L'épreuve de l'entretien individuel a pour but de comprendre la motivation du candidat et valider l'intérêt de la certification dans son projet professionnel. Elle complète le dossier de candidature et valide les objectifs du candidat.

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

Le jury d'évaluation est composé au minimum de deux membres externes à l'organisme. Les évaluateurs sont des

professionnels avec une expérience de terrain ayant la capacité à évaluer de manière objective les candidats.

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	7 500 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 180 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 Publicité
9 500 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des métiers du géomètre, CPNEFP de la profession d'économiste de la construction
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
9 000 €	CPNE chimie, CPNEFP de la branche des prestataires de services du secteur tertiaire
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 258 €	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
10 000 €	Commission Paritaire Activités de Marchés Financiers
9 992 €	CPNEFP Mutualité
9 800 €	CPNEF de l'audiovisuel
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
8 696 €	CPNEFP des jardineries et graineteries
8 520 €	CPNE de la branche des experts comptables et commissaires aux comptes
8 500 €	CPNEFP de la métallurgie
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	21/12/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	21/12/2026

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38463/>

Se former en apprentissage

Formations en apprentissage	4
Organismes gestionnaires (CFA)	4
Organismes formateurs	4
Régions couvertes	3
Départements couverts	4
Organismes certifiés Qualiopi	4
Sessions	de 09/2025 à 09/2028

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