

Expert en cybersécurité

RNCP37649 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31038, 31045, 42881, 13235, 24231
Code(s) ROME	M1802, M1806, M1803, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	31/05/2023
Date d'échéance	31/05/2026

Certificateur(s)

ESGCV · SIRET : 75253547600325

HETIC · SIRET : 49336137200011

PSTB-PARIS SCHOOL OF TECHNOLOGY & BUSINESS EN ABREGE P.S.T.B · SIRET : 81209558600044

Partenaires habilités

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

Organisme	SIRET	Habilitation
ESGCV -75253547600143	75253547600143	Former et organiser l'évaluation
GALILEO FORMATION PROFESSIONNELLE	81212304000063	Former et organiser l'évaluation
GALILEO VAE	90077772300025	Former et organiser l'évaluation
INSTITUT DE MANAGEMENT ECOLE SUP GESTI	39039183700031	Former et organiser l'évaluation
STUDI	91114836900018	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'expert en cybersécurité a un rôle clé dans l'organisation. Il assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de son organisation ou après de plusieurs clients. Il définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction générale.

Mais pourquoi est-ce aujourd'hui un enjeu de taille ? Le marché français de la cybersécurité ne cesse de croître pour répondre aux différents risques et attaques auxquels nous sommes confrontés. Voici quelques chiffres clés :

- Le marché français de la cybersécurité se développe rapidement : 9 Français sur 10 ont déjà été confrontés à un acte de malveillance sur Internet en 2020 et 80% des personnes se disent suffisamment sensibilisées et informées
- Le chiffre d'affaire du secteur de la cybersécurité s'élève à 7.3 milliards d'euro en 2019 en France.

Un plan à 1 milliard d'euros d'ici à 2025 visant à renforcer la cybersécurité du pays a été présenté par le président Emmanuel Macron en février 2021 pour permettre à la filière de réaliser un chiffre d'affaires de 25 milliards d'euros en 2025.

- La France est le 7e pays dans le monde à avoir connu le plus de cyberattaques en 2020, d'après le FBI. De 2018 à 2019, les cyberattaques ont augmenté de 210%, selon cybermalveillance.gouv.fr. Pour 2020, l'augmentation des cyberattaques en France est estimée à 400% depuis la mise en place du télétravail au début de l'année.
 - Les cyberattaques sont de plus en plus intenses : les pertes liées à une cyberattaque ont été multipliées par 6 en un an, en particulier à cause de la recrudescence des ransomwares (+19%).
 - Selon une étude menée sur six pays, les entreprises françaises déclarent les plus faibles pertes liées aux cyber-événements mais 18% d'entre elles indiquent avoir versé une rançon contre 6% des pays du panel (Etats Unis, Royaume Uni, Irlande, Allemagne, Belgique, France, Espagne, Pays Bas)
 - Les dépenses en cybersécurité des entreprises françaises sont passées de 1,9 millions € à 2,8 millions € de 2018 à 2019. En général, ce sont les grandes entreprises ayant déjà subi une faille qui sont les plus dépensières
- Par conséquent, les chiffres le prouvent : la considération de la cybersécurité doit être une priorité dans les stratégies globales des diverses structures de la société, en particulier des entreprises.

ACTIVITÉS VISÉES

L'expert en cybersécurité est amené à réaliser plusieurs activités, décrites en sous-activités secondaires, et communes aux 3 grands domaines d'expertise dans lesquels il peut se spécialiser : le conseil & la recherche, l'audit & la gestion d'incident de sécurité, et la conception & maintien d'un système d'information sécurisé.

Activités communes en : Conception et pilotage de la politique de sécurité de l'information au sein d'une/plusieurs organisations

- Pilotage d'un système de veille scientifique, technique, technologique, réglementaire, sectorielle et concurrentielle
- Réalisation d'audit périodique de cybersécurité auprès d'une/plusieurs organisations
- Identification des enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation
- Définition de la politique de sécurité et d'organisation de l'information
- Définition des axes et des objectifs stratégiques en matière de cybersécurité
- Planification du déploiement de la politique de sécurité à l'échelle d'une organisation

Activités communes en : Déploiement de la politique de sécurité de l'information de manière à restreindre l'exposition au risque de l'organisation

- Evaluation de la nature et de la criticité des risques
- Organisation des structures de pilotage des plans de traitement des risques en matière de sécurité au sein de l'organisation
- Définition des mesures organisationnelles et techniques nécessaire à l'atteinte des objectifs de sécurité
- Gestion de incidents liés à la sécurité de l'information
- Diffusion d'une culture SSI à destination des utilisateurs et décideurs grâce à de la formation et de la sensibilisation
- Réalisation d'actions de sensibilisation ponctuelles selon les besoins et risques identifiés
- Réalisation d'un reporting régulier auprès de sa hiérarchie sur le niveau de couverture courant des risques de sécurité SI

Activités communes en : Management de projet de transformation et/ou d'innovation SI/cybersécurité

- Evaluation des ressources matérielles, financières, et humaines nécessaires à la réalisation d'un projet
- Pilotage du déploiement du projet
- Sélection de partenaires
- Évaluation du niveau de sécurité au sein de l'organisation, notamment à travers la réalisation d'audits périodiques et de contrôles permanents
- Promotion des chartes de sécurité informatique sur son périmètre
- Sensibilisation des parties intéressées du projet de cybersécurité, ou SI à fort enjeux sécurité

Activités communes en : Management des hommes et des équipes dans un contexte de pilotage de chantiers cyber

- Identification des besoins en compétences nécessaires au déploiement de projet IT / Cyber
- Recrutement des membres d'une direction IT et/ou d'une équipe projet cyber
- Supervision de la réalisation des objectifs individuels et collectifs
- Animation de réunion d'équipe auprès d'une direction IT et/ou d'une équipe projet cyber
- Délégation de tâches, missions et responsabilités aux membres d'une direction IT et/ou d'une équipe projet cyber

Activités de première spécialisation possible correspondant à l'option Conseil & recherche

- Identification d'une problématique de recherche en cybersécurité
- Proposition de solutions innovantes et créatrices de connaissances, de technologies et de valeur, de nouvelles approches, de nouvelles méthodes

- Rédaction d'une réponse à un appel d'offre
- Evaluation des moyens humains, techniques et organisationnels nécessaires à la réalisation de l'appel d'offre
- Conseil stratégique en matière de cybersécurité

Activités de deuxième spécialisation possible correspondant à l'option Audit & gestion d'incidents de sécurité

- Identification des enjeux et du contexte de la cybermenace
- Réaliser une veille sur les menaces émergentes, et les nouvelles évolutions en matière de cybersécurité
- Analyse des techniques d'attaques et les modes opératoires connus
- Amélioration des capacités de détection
- Animation d'une cellule de crise décisionnelle et contribution aux cellules de crise opérationnelles
- Coordination de l'action des différentes parties en présence et la diffusion des informations vers les parties prenantes

Activités de troisième spécialisation possible correspondant à l'option Conception & maintien d'un système d'information sécurisé

- Définition d'une architecture cybersécurisée
- Codage et intégration de solution technique, organisationnel et de contrôle d'accès
- Planification d'actions correctives et préventives

COMPÉTENCES ATTESTÉES

L'expert en cybersécurité doit mobiliser plusieurs compétences pour réaliser les activités communes préalablement décrites. Puis, selon son domaine, il doit maîtriser des compétences complémentaires.

Ainsi le référentiel de certification vise les compétences communes suivantes :

- Elaborer un dispositif de veille scientifique, technique, technologique, réglementaire, sectorielle et concurrentielle portant sur les évolutions en matière de cybersécurité
 - Piloter la réalisation et/ou réaliser un audit de cybersécurité au sein d'une organisation sur un périmètre préalablement établi avec le commanditaire
 - Elaborer la politique de sécurité de l'information d'une/plusieurs organisations en tenant compte des actifs/biens de l'organisation et de son activité
 - Planifier les plans d'actions annuels et/ou pluriannuels permettant le déploiement de la politique de sécurité de l'information
 - Établir un plan de traitement des risques
 - Déployer des mesures de sécurité opérationnelle sur l'ensemble du parc informatique et des SI
 - Diagnostiquer un incident de sécurité
 - Former et sensibiliser les collaborateurs
 - Elaborer des tableaux de bords mesurant l'efficacité des mesures et la conformité du système, à destination de la direction de l'organisation
 - Concevoir un projet de transformation et/ou d'innovation SI/cyber sur la base d'une étude d'opportunité et de faisabilité
 - Définir l'organisation et les étapes d'un projet de transformation et/ou d'innovation, les principaux livrables, les besoins en ressources humaines, matérielles et financières, ainsi que les contraintes spécifiées
 - Identifier et sélectionner des partenaires (prestataires, fournisseurs, experts...)
 - Piloter l'accompagnement au changement suite au déploiement d'un projet SI/Cybersécurité
 - Evaluer l'adéquation entre les compétences des collaborateurs d'une DSI et/ou d'une équipe projet cyber et le besoin en compétences nécessaires au soutien des besoins fonctionnels et stratégiques IT
 - Organiser des entretiens de recrutement (interne et externe) adaptés aux postes à pourvoir, en collaboration avec la direction des ressources humaines
 - Accompagner les collaborateurs dans la définition et la réalisation de leurs objectifs individuels et collectifs dans le respect des obligations légales et contractuelles
 - Mettre en œuvre un management de délégation en définissant des objectifs SMART, les méthodes et les modalités de mise en œuvre ainsi que les indicateurs de performance
- Il adjoint les compétences de l'option conseil & recherche
- Concevoir et piloter un projet de recherche scientifique en matière de cybersécurité, en autonomie et/ou en partenariat avec des pairs au sein de son organisation ou d'un laboratoire
 - Répondre à des appels d'offre de marché public, et auprès d'entreprises privés
 - Emettre des recommandations et préconisations portant sur la définition et le déploiement d'une stratégie de cybersécurité et de conformité (à une réglementation, à des référentiels d'exigences) auprès de clients externes

Les compétences de l'option audit & gestion d'incidents de sécurité

- Piloter les activités de renseignement en matière de cybersécurité d'une organisation
- Piloter le système d'amélioration continue des moyens de détection
- Piloter une cellule de crise décisionnelle et contribuer aux cellules de crise opérationnelles

Ou enfin les compétences de l'option conception & maintien d'un système d'information sécurisé

- Elaborer une architecture cybersécurisée
- Développer des solutions techniques, organisationnelles et de contrôle des accès, et les intégrer au sein d'un SI
- Planifier des actions de développement correctives et préventives suite à l'identification d'un incident cybersécurité

Blocs de compétences

RNCP37649BC01 — Concevoir et piloter le déploiement d'une politique de sécurité de l'information au sein d'une/plusieurs organisations

LISTE DE COMPÉTENCES

Elaborer un dispositif de veille scientifique, technique, technologique, réglementaire, sectorielle et concurrentielle portant sur les évolutions en matière de cybersécurité en : - définissant les objectifs de veille, - mobilisant des méthodologies de recherche, traitement et exploitation de données, - évaluant la fiabilité du protocole, afin d'anticiper les enjeux de cybersécurité des organisations.

Piloter la réalisation et/ou réaliser un audit de cybersécurité au sein d'une organisation sur un périmètre préalablement établi avec le commanditaire en :- définissant les objectifs visés par l'audit, - réalisant des interviews auprès des audités (administrateurs système, développeurs, commanditaire, collaborateurs ...) - réalisant des analyses techniques sur des points de contrôles précisés, afin de réaliser un état des lieux exhaustif des risques menaçant l'organisation et de la maturité des système SI en matière de cybersécurité.

Elaborer la politique de sécurité de l'information d'une/plusieurs organisations en définissant : - le périmètre du système de management de la sécurité de l'information, - les objectifs en matière de niveau de sécurité attendu (intégrité, confidentialité et disponibilité de l'information) et en tenant compte des actifs/biens de l'organisation et de son activité.

Planifier les plans d'actions annuels et/ou pluriannuels permettant le déploiement de la politique de sécurité de l'information en déterminant les objectifs et les mesures de sécurité, ainsi qu'un calendrier d'audit interne de manière à permettre le suivi des risques initialement identifiés, les mesures prises et les nouvelles menaces associées.

MODALITÉS D'ÉVALUATION

- Mémoire professionnel
- Mises en situation professionnelles

RNCP37649BC02 — Déployer la politique de sécurité de l'information de manière à restreindre l'exposition au risque de l'organisation

LISTE DE COMPÉTENCES

Établir un plan de traitement des risques à partir d'une définition du niveau de sécurité selon divers scénarii, la nature et la criticité des risques rencontrés et les exigences légales, réglementaires et contractuelle, dans le but d'adresser l'ensemble des risques d'une organisation.

Déployer des mesures de sécurité opérationnelle sur l'ensemble du parc informatique et des SI, grâce à : - des mesures organisationnelles (politique d'habilitation, cartographie de la donnée, sensibilisation, politique de confidentialité...) - des mesures techniques (outils d'anonymisation de la donnée, protection des serveur, process d'identification et d'authentification, techniques de cryptographie ...) de manière à limiter les risques en matière de cybersécurité.

Diagnostiquer un incident de sécurité en recherchant et analysant les informations liées à l'incident (traces informatiques, journaux d'évènements, diagrammes de topologie réseau ...) à l'aide d'outils afin d'évaluer l'ampleur de l'incident et de proposer des actions correctrices.

Former et sensibiliser les collaborateurs au travers de : - la rédaction d'une charte informatique, - la réalisation de campagne d'information (communication, sensibilisation et formation), - l'animation de campagne de live-hacking, - en partageant les risques en matière de cybersécurité et les impacts RSE associés, afin de diminuer les risques de cybersécurité liée aux comportements humains.

Elaborer des tableaux de bord mesurant l'efficacité des mesures et la conformité du système, à destination de la direction de l'organisation, de manière à superviser le déploiement de la politique de sécurité de l'information.

MODALITÉS D'ÉVALUATION

- Mises en situation professionnelles
- Etude de cas

RNCP37649BC03 — Manager des projets de transformation et/ou d'innovation intégrant des enjeux de cybersécurité

LISTE DE COMPÉTENCES

Concevoir un projet de transformation et/ou d'innovation SI/cyber sur la base d'une étude d'opportunité et de faisabilité, évaluant le retour sur investissement, en mobilisant des outils d'idéation et innovation technologique afin de soutenir les objectifs stratégiques SI et cybersécurité de l'organisation.

Définir l'organisation et les étapes d'un projet de transformation et/ou d'innovation, les principaux livrables, les besoins en ressources humaines, matérielles et financières, ainsi que les contraintes spécifiées par la maîtrise d'ouvrage afin de prioriser les différents chantiers SI.

Identifier et sélectionner des partenaires (prestataires, fournisseurs, experts...) sur la base d'une grille de critères spécifiques base, dans le respect de la politique et des règles de sécurité des SI de manière à lancer un projet de transformation et/ou d'innovation SI/Cybersécurité.

Piloter l'accompagnement au changement suite au déploiement d'un projet SI/Cybersécurité en mobilisant des outils (charte de sécurité, procédure...) et méthodes de conduite du changement adaptés à la singularité des personnes (handicap, intergénérationnel...) et du projet de cybersécurité de manière à permettre l'acculturation des collaborateurs et la gestion des résistances.

MODALITÉS D'ÉVALUATION

- Dossier de consulting

RNCP37649BC04 — Manager des hommes et des équipes dans un contexte de pilotage de chantiers cyber

LISTE DE COMPÉTENCES

Evaluer l'adéquation entre les compétences des collaborateurs d'une DSI et/ou d'une équipe projet cyber et le besoin en compétences nécessaires au soutien des besoins fonctionnels et stratégiques IT de manière à déployer un plan de développement de compétences, de formation, et/ou de recrutement.

Organiser des entretiens de recrutement (interne et externe) adaptés aux postes à pourvoir, en collaboration avec la direction des ressources humaines, en veillant à la non-discrimination des candidats (notamment liée au handicap), afin de renforcer une direction IT et/ou une équipe projet cyber.

Accompagner les collaborateurs dans la définition et la réalisation de leurs objectifs individuels et collectifs dans le respect des obligations légales et contractuelles en : - évaluant le niveau de compétences et de motivation, - capitalisant sur les résultats des entretiens individuels d'évaluation et entretiens professionnels, - organisant des réunions d'équipe rappelant les actions, les objectifs et les moyens nécessaires, - résolvant les problèmes d'organisation et les conflits éventuels, - en veillant à l'adaptation de leur poste de travail notamment pour les publics en situation de handicap.

Mettre en œuvre un management de délégation en définissant des objectifs SMART, les méthodes et les modalités de mise en œuvre ainsi que les indicateurs de performance afin de renforcer l'efficacité collective dans le cadre du déploiement de projet IT / cyber.

MODALITÉS D'ÉVALUATION

- Etudes de cas

RNCP37649BC05 — Spécialisation 1 - Développer une activité de conseil et de recherche approfondie dans le secteur de la cybersécurité

LISTE DE COMPÉTENCES

Concevoir et piloter un projet de recherche scientifique en matière de cybersécurité, en autonomie et/ou en partenariat avec des pairs au sein de son organisation ou d'un laboratoire, de manière à renforcer les échanges entre les laboratoires de recherche et les milieux socio-économiques et contribuer au processus d'innovation.

Répondre à des appels d'offre de marché public, et auprès d'entreprises privés, en :- présentant l'organisation et démontrant son expertise sur la problématique de travail, son éthique et sa dimension RSE, - précisant le mémoire technique (analyse, méthodologie...) , - évaluant l'offre de prix en partenariat avec les équipes commerciales, de manière à développer le CA de l'organisation et de décrocher de nouveaux marchés.

Emettre des recommandations et préconisations portant sur la définition et le déploiement d'une stratégie de

cybersécurité et de conformité (à une réglementation, à des référentiels d'exigences) auprès de clients externes, en veillant à l'évaluation du budget nécessaire à la réalisation de la prestation.

MODALITÉS D'ÉVALUATION

- Mémoire
- Mise en situation professionnelle
- Dossier de consulting

RNCP37649BC06 — Spécialisation 2 - Auditer et piloter la gestion des incidents de sécurité informatique

LISTE DE COMPÉTENCES

Piloter les activités de renseignement en matière de cybersécurité d'une organisation en collectant, qualifiant, organisant, recoupant et analysant diverses sources de données (dark web, renseignements open source, média sociaux, CERT, etc.) de manière à anticiper les risques et attaques cybersécurité.

Piloter le système d'amélioration continue des moyens de détection, en : - capitalisant sur les activités de renseignement préalablement mené, - en produisant des documents d'analyse permettant l'alimentation des outils de détection, - en capitalisant sur les apprentissages générés lors de précédents incidents ou de crises de cybersécurité. Piloter une cellule de crise décisionnelle et contribuer aux cellules de crise opérationnelles en :- organisant et d'articulant un dispositif global de gestion de crise, - analysant la situation et évaluant les conséquences pour l'entreprise,- délimitant les périmètres de chaque cellule et le rôle de chaque interlocuteur, de manière à solutionner la crise en limitant ses impacts.

MODALITÉS D'ÉVALUATION

- Mise en situation professionnelle
- Dossier de consulting

RNCP37649BC07 — Spécialisation 3 - Concevoir et maintenir un système d'information sécurisé

LISTE DE COMPÉTENCES

Elaborer une architecture cybersécurisée en intégrant des solutions d'acquisition, de traitement et de stockage de données, de détection de programmes malveillants et de menaces de manière à détecter en temps réel des incidents en cybersécurité.

Développer des solutions techniques, organisationnelles et de contrôle des accès, et les intégrer au sein d'un SI de manière à protéger le réseau de la corruption des données.

Planifier des actions correctives et préventives suite à l'identification d'un incident cybersécurité en adoptant une approche DevSecOps de manière à remédier à la situation et de limiter le risque de reproduction de cette faille.

MODALITÉS D'ÉVALUATION

- Mise en situation professionnelle
- Mise en situation professionnelles dans la salle de Simulation Cyber du Groupe Galileo Education au sein du Cybercampus

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La cybersécurité concerne aujourd'hui l'ensemble des secteurs d'activités. Néanmoins, certains secteurs sont davantage la cible des cyberattaques. Parmi eux figurent les secteurs ci-dessous, sans en être toutefois restrictif :

- Le secteur bancaire,
- L'administration publiques & les collectivités,
- L'informatique et les télécommunications,
- L'enseignement et la recherche,
- Le secteur énergétique,
- La santé,
- Le service aux entreprises,
- L'industrie Chimique / Parachimique / Agroalimentaire...
- Le transport et la logistique.

TYPE D'EMPLOIS ACCESSIBLES

L'expert en cybersécurité peut se spécialiser dans 3 grands domaines d'expertise : le conseil & la recherche, l'audit &

la gestion d'incident de sécurité, et la conception & maintien d'un système d'information sécurisé.
Les intitulés de postes peuvent donc varier selon le domaine d'expertise dans lequel l'expert en cybersécurité évolue.

- 1. Centre d'expertise : Conseil et recherche en cybersécurité
 - Consultant en cybersécurité
 - Chercheur en sécurité des systèmes d'information
 - Formateur en cybersécurité
 - Evalueur de la sécurité des technologies de l'information
 - Directeur de la cybersécurité
 - Responsable de projet de sécurité
- 2. Centre d'expertise audit et gestion d'incident de sécurité
 - Responsable de la sécurité des systèmes d'information (rssi)
 - Déclinaison pour le responsable de sécurité des si au sein d'une pme / tpe
 - Coordinateur sécurité
 - Auditeur de sécurité organisationnelle
 - Auditeur de sécurité technique
 - Gestion des incidents et des crises de sécurité
 - Responsable du soc
 - Opérateur analyste soc
 - Responsable du csirt
 - Analyste réponse aux incidents de sécurité
 - Gestionnaire de crise de cybersécurité
 - Analyste de la menace cybersécurité
- 3. Conception et maintien d'un SI sécurisé
 - Administrateur de solutions de sécurité
 - Chef sécurité de projet
 - Architecte sécurité
 - Spécialiste sécurité d'un domaine technique
 - Spécialiste en développement sécurisé
 - Cryptologue

RÈGLEMENTATIONS D'ACTIVITÉ
A ce jour, la profession d'expert en cybersécurité n'est pas règlementée dans le sens où il n'est pas nécessaire que le candidat détienne un titre ou qualité particulière, ni ne dispose d'une habilitation ou d'une certification complémentaire.
En revanche, il y a un durcissement de la réglementation en matière de droit du numérique (RGPD, droit des contrats ou encore questions de propriété intellectuelle...). Les titulaires de la certification sont donc formés et évalués sur leur capacité à mobiliser des savoirs pluridisciplinaires, à maintenir leurs connaissances en matière de lois, de réglementations, de normes, référentiels, et recommandations délivrés par les organes compétents.

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) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 892 €
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) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
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 M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les prérequis d'entrée en formation dépendent de la voie d'accès et du cadre de la formation.

- En initial ou en alternance : le candidat doit avoir obtenu un niveau 6, et/ou avoir validé 180 crédits ECTS, et/ou être titulaire d'un diplôme étranger équivalent à un niveau 6, dans le domaine de l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.
- En formation continue : le candidat doit être diplômé d'un niveau 6 et exercer une fonction dans le domaine de la cybersécurité ou dans un domaine annexe(*), et souhaiter se reconverter dans le domaine de la cybersécurité (*) pour exemples (non limitatifs): cadre du secteur des Stratégies Informatiques (DSI), de la Sécurité Globale et des Stratégies Sécurité, anciens fonctionnaires du Ministère de la Défense ou de l'Intérieur en reconversion vers le secteur privé
- Dérogation - cas spécifique : dans le cadre d'une VAPP (Validation des Acquis Professionnels et Personnels), le candidat doit avoir interrompu ses études depuis au moins 2 ans (3 ans en cas d'échec) et être âgé d'au moins 20 ans pour les non titulaires du baccalauréat.
- Classe dédiée toute voie confondue : dans le cadre d'une classe dédiée - que ce soit en partenariat avec une entreprise, une collectivité locale ou territoriale, une branche professionnelle - les prérequis pourraient être en deçà de ceux prévus initialement. Et dans ce cas, la formation sera adaptée à ce public pour permettre d'assurer les mêmes chances de réussite.

PRÉREQUIS À LA VALIDATION

Avec effet cumulatif :

- Avoir respecté les prérequis d'accès d'entrée en formation,
- Avoir validé les blocs de compétences 1,2, 3 et 4, ainsi que le bloc 5, 6 ou 7 au choix.
- Avoir obtenu la certification "Handimanagement"

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

Le jury est composé de 4 membre dont 50% de professionnels :

- Le représentant du certificateur ou son représentant :
- Un enseignant, formateur ou responsable pédagogique exerçant pour le compte d'une formation en cybersécurité
- Deux professionnels externes exerçant dans le métier visé

La parité employeur salarié est contrôlée.

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 € – 11 564 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 166 branches
11 564 €	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
9 000 €	CPNE Banque, CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire, CPNEFP de la branche des prestataires de services du secteur tertiaire
11 500 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des métiers du géomètre, CPNEFP de la profession d'économiste de la construction
10 000 €	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
10 164 €	CPNE Casinos, CPNE de la branche de la Distribution Directe
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
8 740 €	CNPEFP des sociétés d'assistance, CPNFPE des sociétés d'assurances
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
10 163 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
10 100 €	CNPE des sociétés financières
9 842 €	CPNEFP Grands Magasins/ Magasins Populaires
9 800 €	CPNEF de l'audiovisuel
9 231 €	CPNEFP Commerce à distance
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	31/05/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	31/05/2026
Date de dernière délivrance possible	31/05/2030

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42868

CORRESPONDANCES (PAR BLOCS)
RNCP35588, RNCP36072, RNCP36122, RNCP36595

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
HETIC : <https://www.hetic.net/formations/mastere-cybersecurite>
MBA ESG : <https://www.mba-esg.com/master-cybersecurite-risques>
PSTB : <https://www.pstb.fr/mastere-cybersecurite>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37649/>

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Formations à distance	1
Sessions	de 09/2026 à 08/2027

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

Entrées et sorties de formation

Entrées en formation	156
Parcours menés à terme	87
Taux d'achèvement	56 %
Période	11/2023 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	169
Montant total engagé	570 387 €
Coût moyen par dossier	3 375 €
Durée moyenne	168 h
Période	09/2023 – 05/2026
France compétences	82 %
France Travail	6 %
OPCO	4 %
Entreprise	4 %
Reste à charge titulaire	3 %
Compte d'engagement citoyen	0 %

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