

Sciences et ingénierie - Cybersécurité et réseaux

RNCP40745 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	326
Formacode(s)	31045, 13235, 31002, 31097, 24231
Code(s) ROME	M1802, M1810, M1801, M1807, M1806
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2030

Certificateur(s)

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE · SIRET : 11004401300040

EFREI PARIS · SIRET : 39889833800023

Résumé de la certification

OBJECTIFS ET CONTEXTE

La sécurité informatique s'est invitée depuis quelques années dans les médias. Attaques par déni de service (DDoS), ransomwares, di?usions de données sur le Dark Web, autant de types de cyberattaque désormais connues de tous. Pour se protéger de ces attaques, les entreprises investissent de plus en plus dans la cybersécurité même si le niveau de maturité général reste encore faible (49%) d'après une récente étude du cabinet Wavestone.

Pour répondre aux di?érents enjeux de la cybersécurité, les entreprises ont besoin de recruter en masse et ce, alors qu'en 2023, 15000 postes du secteur sont non couverts. Ce chi?re est la conséquence d'une demande toujours plus forte, comme indiqué dans l'enquête 2022

de l'APEC sur le sujet qui a noté, un quasi doublement des o?res cyber sur son site en 5 ans.

Si pendant longtemps, la cybersécurité ne donnait l'impression de ne concerner que des pro?ls de niveau 7, le milieu s'est ouvert progressivement à des pro?ls de niveau 6 pour, notamment, déployer les PSSI (politique de sécurité des systèmes d'information) dé?nies par les DSI et les RSSI. C'est ainsi que dans le dernier répertoire des métiers, publié par l'ANSSI

en 2020, est apparu le métier d'Administrateur de sécurité informatique dénommé aussi Administrateur de solutions de sécurité.

Ses missions sont détaillées par l'ANSSI

et « consistent à installer, mettre en production, administrer et exploiter des solutions de sécurité (antivirus, sondes, ?rewalls, IAM, etc.). Il participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité ».

D'après le site chooseyourboss.com

, il est considéré comme « un expert qui analyse les performances du système d'information de l'entreprise et propose des solutions pour améliorer sa sécurité ».

Si cette fonction spéci?que fut longtemps intégrée aux fonctions des administrateurs systèmes et réseaux, elle s'en dissocie petit à petit pour devenir une fonction à part entière avec des attentes précises de la part des employeurs. Cependant, ce phénomène étant récent, et les o?res couplant encore l'administration de sécurité informatique avec celle des réseaux et/ou des systèmes, les études les associent encore tous les 3, notamment l'OPIIEC qui les regroupe sous le titre généraliste de Spécialiste, systèmes, réseaux et sécurité

Cet ensemble a vu les offres d'emploi croître de plus de 12% sur un an avec plus de 9500 offres pour l'année écoulée, dont près d'un tiers en Ile de France, soulignant que les besoins en cybersécurité se sont étendus au-delà des profils de niveau 7.

Le titulaire de la certification Grade de licence – Cybersécurité et réseaux exerce typiquement ses activités au sein d'une Direction des Systèmes d'Information (DSI) ou d'un Security Operation Center (SOC).

Les candidats à la certification Grade Licence cybersécurité et réseaux, à l'issue du processus de certification doivent être capables d'assurer la sécurité des services numériques à destination des utilisateurs en respectant les normes et standards reconnus par la profession et en suivant l'état et l'art de la sécurité informatique à toutes les étapes, ils doivent prendre en compte la responsabilité numérique et la frugalité dans les processus de sécurisation.

Ils doivent avoir les connaissances mathématiques et techniques de niveaux suffisants pour leurs spécialisations mais aussi la capacité à mener des recherches bibliographiques, à consulter et utiliser avec un œil critique des bases de données scientifiques et d'autres sources d'informations appropriées.

Les détenteurs du Grade Licence en cybersécurité et réseaux doivent avoir une vision claire de leur domaine d'activité, être à la fois opérationnels et aptes à changer d'environnement culturel et technique, à progresser en termes de niveau de responsabilité au sein de leur entreprise ou en rejoignant une autre entreprise en France ou à l'international ; et soucieux de leur équilibre personnel et du bien-être de la société.

Le titulaire de la certification Grade Licence en sciences de l'ingénierie Cybersécurité et réseaux exerce typiquement ses activités au sein d'une direction des systèmes d'information (DSI), sous la responsabilité d'un ingénieur ou d'un Security Operation Center (SOC).

ACTIVITÉS VISÉES

Concevoir des algorithmes faisant appel à des connaissances et des logiques mathématiques tout en intégrant l'innovation frugale et l'obsolescence numérique :

- Application des langages de programmation et algorithmique, variables, structures de contrôle, fonctions et passage de paramètres.
- Assimilation des principes généraux du traitement de données par des machines binaires et des mécanismes et concepts fondamentaux propres aux traitements informatiques.
- Manipulation d'expressions algébriques
- Prise en compte de l'obsolescence numérique

Mettre en œuvre des systèmes de défense contre les attaques informatiques en mobilisant des connaissances en informatique et réseaux :

- Configuration d'une infrastructure réseau et système existante
- Administration des systèmes d'exploitation, des réseaux informatiques et des bases de données
- Développement de composants ou de solutions de sécurité
- Sécurisation du système d'information d'une entreprise

Analyser et tester les outils de détection d'anomalies d'un système d'information en tenant compte des réglementations nationales et internationales et des bonnes pratiques en usage en matière de sécurité :

- Analyse des besoins en matière de sécurité d'un système d'information
- Identification et sélection des outils de protection adaptés au système d'information (type EDR, Pare-feu...) et conformes aux réglementations en vigueur
- Configuration et déploiement des outils de protection sélectionnés
- Application des méthodes de test d'intrusion (Pentest) et détection de failles de sécurité
- Sensibilisation de l'ensemble des équipes et des clients dans la sécurisation du SI

Mettre en œuvre un système de réponses à incidents performant suite à un diagnostic afin de mettre en place des actions correctrices optimales :

- Analyse du risque et gestion d'incidents
- Mise en œuvre d'un plan de continuité et de restauration d'activité
- Recherche de preuves sur des supports numériques
- Propositions de mesures d'amélioration via une documentation de l'incident
- Mise en place de nouvelles mesures de protection

Résoudre les situations techniques complexes pour entreprendre et innover :

- Application d'outils et de méthodes de modélisation et de simulation afin d'optimiser des systèmes complexes sous contraintes multiples
- Intégration de la connaissance des systèmes complexes (interdisciplinarité et approche systémique) afin de concevoir, développer, améliorer et innover dans l'ingénierie des systèmes complexes

- Contribution à la recherche, l'innovation et la prospective commerciale
- Identification des avancées technologiques et déployer des solutions créatives

Mettre en place une veille technique et des recherches bibliographiques pour recueillir et exploiter des données pertinentes :

- Organisation et animation d'un système de veille active pour se tenir à jour sur les offres et solutions d'architecture des SI
- Analyse des indicateurs d'activité des solutions choisies pour identifier les besoins de mises à jour ou d'évolutions du SI
- Organisation et animation d'un système de veille active pour se tenir à jour sur les menaces en cyber sécurité et solutions de sécurisation

COMPÉTENCES ATTESTÉES

- Appliquer des concepts mathématiques en utilisant des outils de calcul afin de résoudre des problématiques complexes.
- Résoudre des problèmes en mobilisant des outils mathématiques, afin de proposer des solutions adaptées à des situations dans un cadre prédéfini.
- Concevoir des algorithmes en mobilisant des connaissances scientifiques afin de résoudre des problèmes complexes.
- Choisir l'outil le plus adapté, en s'appuyant sur une analyse des besoins, pour répondre à une problématique bien identifiée.
- Savoir utiliser une large variété d'outils numériques complexes, en s'appuyant sur une compréhension approfondie de leurs fonctionnalités et de leurs contextes d'usage, afin de répondre à différents besoins.
- Employer des langages de programmation de référence, en respectant les bonnes pratiques de développement, afin de permettre la maintenance des logiciels développées par le plus grand nombre.
- Intégrer la programmation frugale et les problèmes d'obsolescence numérique en utilisant des outils adaptés pour mettre en place une approche éco numérique.
- Analyser l'architecture d'un système d'information en identifiant l'ensemble de ses composants afin de garantir son bon fonctionnement
- Administrer un environnement système, réseaux et cloud computing en mettant en place des infrastructures aux besoins métiers afin d'en garantir la performance des services
- Administrer des bases de données en en gérant l'intégrité, la disponibilité et la sécurité pour garantir leur exploitation efficace par le plus grand nombre
- Optimiser le fonctionnement des bases de données d'un système en analysant la structure et les performances des requêtes afin d'améliorer l'efficacité du traitement des données
- Concevoir, sécuriser et actualiser des infrastructures et réseaux en respectant les normes et réglementation en vigueur pour prévenir les vulnérabilités
- Développer une solution logicielle sécurisée en tenant compte des bonnes pratiques afin de réduire les surfaces d'attaque
- Intégrer la solution logicielle sécurisée à un système d'information existant pour garantir son interopérabilité et renforcer sa sécurité
- Diagnostiquer les besoins en matière de sécurité en utilisant les méthodologies d'analyse appropriées afin de contribuer à la stratégie de sécurisation
- Sélectionner des outils de protection identifiés en se basant sur le diagnostic réalisé afin de rendre le système d'information plus résilient
- Installer et mettre à jour les outils de protection de base (pare-feu, antivirus) en assurant leur mise à jour pour garantir une sécurité opérationnelle
- Effectuer des tests d'intrusion de manière éthique afin d'identifier les failles de sécurité d'un système d'information
- Communiquer les résultats aux parties prenantes en utilisant des outils adaptés afin de sensibiliser les parties prenantes
- Détecter et analyser les cybermenaces sur un système d'information en exploitant des outils de surveillance afin d'identifier les vecteurs d'attaques
- Évaluer l'impact d'un incident de sécurité en identifiant les ressources et systèmes non compromis afin d'assurer la continuité des services
- Mettre en place des mesures d'atténuations de l'incident en appliquant les protocoles de confinement afin de limiter la propagation de l'incident et protéger l'intégrité du système d'information

- Identifier la source et le mode opératoire d'un incident de cybersécurité, en analysant les indicateurs de compromission, afin de mettre en œuvre des mesures correctives adaptées
- Déployer un plan de reprise d'activité (PRA) en restaurant les systèmes compromis, afin de contribuer au rétablissement progressif des services.
- Proposer des mesures d'amélioration à sa hiérarchie, en contribuant à l'élaboration d'un document de retour d'expérience, afin de renforcer la résilience du système d'information.
- Implémenter les mesures d'amélioration retenues, en respectant les bonnes pratiques en vigueur, afin d'anticiper les nouvelles menaces
- Mettre en œuvre une démarche de recherche scientifique afin de résoudre un problème complexe en le reformulant en différents sous-problème plus simple à résoudre techniquement.
- Réaliser un état de l'art sur un sujet dans un cadre défini, en se basant sur des productions scientifiques afin d'identifier les apports, limites et perspectives des travaux existants.
- Faire un bilan objectif et critique des avancées de ses propres travaux, en mobilisant des outils d'autoévaluation, afin d'identifier la valeur ajoutée par rapport aux travaux antérieurs.
- Décrire le processus d'exploitation commerciale de résultats de recherche pour être à même d'identifier les occasions de contribuer à la coopération entre la recherche universitaire, la recherche industrielle et l'ensemble des secteurs de production dans un objectif d'innovation.
- Mettre en place des actions efficaces facilitant les interactions au sein d'une équipe multiculturelle, en mobilisant des compétences en communication interculturelle, afin de favoriser la compréhension mutuelle et la réussite collective dans des environnements professionnels internationaux.
- Déterminer les axes de la veille technologique notamment au niveau éco numérique, en analysant les tendances émergentes, afin de pérenniser une approche durable.
- Sélectionner les outils adéquats (logiciels, moteurs de recherche...) et les paramétrer, en s'appuyant sur une analyse des besoins et une connaissance des fonctionnalités techniques, afin de faciliter la collecte et l'archivage des données pertinentes.
- Sélectionner des services de banques de données adaptés à la recherche, en s'appuyant sur une analyse des sources, des critères de fiabilité et des outils de requêtage, afin d'accéder à une information adaptée aux besoins d'un projet.
- Utiliser les critères booléens en s'appuyant sur une compréhension logique des expressions conditionnelles, afin d'extraire, trier ou croiser efficacement des informations pertinentes dans le cadre d'analyses en cybersécurité.
- Pratiquer les techniques de recherche d'informations dans des bases de données scientifiques, en utilisant des stratégies de requêtage efficaces (mots-clés, opérateurs booléens, filtres, thésaurus), afin de sélectionner et d'exploiter des sources fiables et pertinentes pour alimenter une démarche de recherche.
- Exploiter les bilans de veille, en analysant les informations collectées, afin d'orienter la prise de décision, l'innovation ou l'adaptation stratégique.
- Constituer une revue de littérature académique et/ou professionnelle sur un sujet défini, en appliquant des méthodes de recherche documentaire rigoureuses, afin de poser les bases d'une réflexion critique.
- Maintenir et développer continuellement ses connaissances et compétences afin de rester à jour face aux évolutions rapides du secteur numérique.

Blocs de compétences

RNCP40745BC01 — Concevoir des algorithmes faisant appel à des connaissances et des logiques mathématiques tout en intégrant l'innovation frugale et l'obsolescence numérique

LISTE DE COMPÉTENCES

- Appliquer des concepts mathématiques en utilisant des outils de calcul afin de résoudre des problématiques complexes.
- Résoudre des problèmes en mobilisant des outils mathématiques, afin de proposer des solutions adaptées à des situations dans un cadre prédéfini.
- Concevoir des algorithmes en mobilisant des connaissances scientifiques afin de résoudre des problèmes complexes.
- Choisir l'outil le plus adapté, en s'appuyant sur une analyse des besoins, pour répondre à une problématique bien identifiée.
- Savoir utiliser une large variété d'outils numériques complexes, en s'appuyant sur une compréhension approfondie

de leurs fonctionnalités et de leurs contextes d'usage, afin de répondre à différents besoins.

- Employer des langages de programmation de référence, en respectant les bonnes pratiques de développement, afin de permettre la maintenance des logiciels développées par le plus grand nombre.
- Intégrer la programmation frugale et les problèmes d'obsolescence numérique en utilisant des outils adaptés pour mettre en place une approche éco numérique

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre de :

- travaux écrits individuels
- mise en situation professionnelle avec un projet à réaliser dans le cadre de travaux pratiques

RNCP40745BC02 — Mettre en œuvre des systèmes de défense contre les attaques informatiques en mobilisant des connaissances en informatique et réseaux

LISTE DE COMPÉTENCES

- Analyser l'architecture d'un système d'information en identifiant l'ensemble de ses composants afin de garantir son bon fonctionnement
- Administrer un environnement système, réseaux et cloud computing en mettant en place des infrastructures aux besoins métiers afin d'en garantir la performance des services
- Administrer des bases de données en en gérant l'intégrité, la disponibilité et la sécurité pour garantir leur exploitation efficace par le plus grand nombre
- Optimiser le fonctionnement des bases de données d'un système en analysant la structure et les performances des requêtes afin d'améliorer l'efficacité du traitement des données
- Concevoir, sécuriser et actualiser des infrastructures et réseaux en respectant les normes et réglementation en vigueur pour prévenir les vulnérabilités
- Développer une solution logicielle sécurisée en tenant compte des bonnes pratiques afin de réduire les surfaces d'attaque
- Intégrer la solution logicielle sécurisée à un système d'information existant pour garantir son interopérabilité et renforcer sa sécurité

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un projet visant à sécuriser un système existant.

Mise en situation professionnelle

Présentation orale devant jury

RNCP40745BC03 — Analyser et tester les outils de détection d'anomalies d'un système d'information en tenant compte des réglementations nationales et internationales et des bonnes pratiques en usage en matière de sécurité

LISTE DE COMPÉTENCES

- Diagnostiquer les besoins en matière de sécurité en utilisant les méthodologies d'analyse appropriées afin de contribuer à la stratégie de sécurisation
- Sélectionner des outils de protection identifiés en se basant sur le diagnostic réalisé afin de rendre le système d'information plus résilient
- Installer et mettre à jour les outils de protection de base (pare-feu, antivirus) en assurant leur mise à jour pour garantir une sécurité opérationnelle
- Effectuer des tests d'intrusion de manière éthique afin d'identifier les failles de sécurité d'un système d'information
- Communiquer les résultats aux parties prenantes en utilisant des outils adaptés afin de sensibiliser les parties prenantes

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

L'évaluation des acquis s'effectue dans le cadre d'un projet d'Ethical Hacking comprenant :

- des tests d'intrusion
- la rédaction d'un rapport d'audit technique

RNCP40745BC04 — Mettre en œuvre un système performant de réponses à incidents suite à un diagnostic afin de mettre en place des actions correctrices optimales

LISTE DE COMPÉTENCES

- Détecter et analyser les cybermenaces sur un système d'information en exploitant des outils de surveillance afin

d'identifier les vecteurs d'attaques

- Évaluer l'impact d'un incident de sécurité en identifiant les ressources et systèmes non compromis afin d'assurer la continuité des services
- Mettre en place des mesures d'atténuations de l'incident en appliquant les protocoles de confinement afin de limiter la propagation de l'incident et protéger l'intégrité du système d'information
- Identifier la source et le mode opératoire d'un incident de cybersécurité, en analysant les indicateurs de compromission, afin de mettre en œuvre des mesures correctives adaptées
- Déployer un plan de reprise d'activité (PRA) en restaurant les systèmes compromis, afin de contribuer au rétablissement progressif des services.
- Proposer des mesures d'amélioration à sa hiérarchie, en contribuant à l'élaboration d'un document de retour d'expérience, afin de renforcer la résilience du système d'information.
- Implémenter les mesures d'amélioration retenues, en respectant les bonnes pratiques en vigueur, afin d'anticiper les nouvelles menaces

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Cas d'étude à partir d'une situation de crise simulée sous forme de challenge.

A l'issue du challenge, les candidats soumettent un rapport écrit documentant les étapes suivantes :

- Gestion de l'incident
- Mise en œuvre du Mise en œuvre d'un plan de continuité et de restauration d'activité (PCA/PRA)
- Préconisations et mesures correctives

RNCP40745BC05 — Résoudre les situations techniques complexes pour entreprendre et innover

LISTE DE COMPÉTENCES

- Mettre en oeuvre une démarche de recherche scientifique afin de résoudre un problème complexe en le reformulant en différents sous-problème plus simple à résoudre techniquement.
- Réaliser un état de l'art sur un sujet dans un cadre défini, en se basant sur des productions scientifiques afin d'identifier les apports, limites et perspectives des travaux existants.
- Faire un bilan objectif et critique des avancées de ses propres travaux, en mobilisant des outils d'autoévaluation, afin d'identifier la valeur ajoutée par rapport aux travaux antérieurs.
- Décrire le processus d'exploitation commerciale de résultats de recherche pour être à même d'identifier les occasions de contribuer à la coopération entre la recherche universitaire, la recherche industrielle et l'ensemble des secteurs de production dans un objectif d'innovation.
- Mettre en place des actions efficaces facilitant les interactions au sein d'une équipe multiculturelle, en mobilisant des compétences en communication interculturelle, afin de favoriser la compréhension mutuelle et la réussite collective dans des environnements professionnels internationaux.

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un mémoire professionnel.

Le candidat travaillera sur un sujet co-validé avec le maître de mémoire.

L'élaboration du mémoire professionnel fera l'objet d'étapes intermédiaires :

- présentation de la problématique
- présentation et critique de la bibliographie / webographie prenant en compte la dimension multiculturelle
- présentation de l'introduction, d'un plan détaillé et d'un premier jet rédigé
- rendu du mémoire

Soutenance orale individuelle devant un jury composé à minima de 50% de professionnels

RNCP40745BC06 — Mettre en place une veille technique et des recherches bibliographiques pour recueillir et exploiter des données pertinentes

LISTE DE COMPÉTENCES

- Déterminer les axes de la veille technologique notamment au niveau éco numérique, en analysant les tendances émergentes, afin de pérenniser une approche durable.
- Sélectionner les outils adéquats (logiciels, moteurs de recherche...) et les paramétrer, en s'appuyant sur une analyse des besoins et une connaissance des fonctionnalités techniques, afin de faciliter la collecte et l'archivage des données pertinentes.
- Sélectionner des services de banques de données adaptés à la recherche, en s'appuyant sur une analyse des sources, des critères de fiabilité et des outils de requêtage, afin d'accéder à une information adaptée aux besoins

d'un projet.

- Utiliser les critères booléens en s'appuyant sur une compréhension logique des expressions conditionnelles, afin d'extraire, trier ou croiser efficacement des informations pertinentes dans le cadre d'analyses en cybersécurité.
- Pratiquer les techniques de recherche d'informations dans des bases de données scientifiques, en utilisant des stratégies de requêtage efficaces (mots-clés, opérateurs booléens, filtres, thésaurus), afin de sélectionner et d'exploiter des sources fiables et pertinentes pour alimenter une démarche de recherche.
- Exploiter les bilans de veille, en analysant les informations collectées, afin d'orienter la prise de décision, l'innovation ou l'adaptation stratégique.
- Constituer une revue de littérature académique et/ou professionnelle sur un sujet défini, en appliquant des méthodes de recherche documentaire rigoureuses, afin de poser les bases d'une réflexion critique.
- Maintenir et développer continuellement ses connaissances et compétences afin de rester à jour face aux évolutions rapides du secteur numérique.

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'une étude de cas sur la veille autour d'un sujet donné par le formateur.

Le candidat présentera un rapport de veille technique et de recherches bibliographiques contenant :

- le périmètre de la veille technologique
- un outil de curation pour sa veille et sa recherche
- les éléments retenus et leur analyse
- la bibliographie / webographie
- un système d'alertes permettant de maintenir les connaissances et compétences

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les titulaires de la certification Cybersécurité et réseaux pourront exercer majoritairement leurs activités au sein de cinq types d'employeurs :

- Les grands groupes, banques, assurances, industrie
- Les ETI qui ont emboîté rapidement le pas aux grands groupes
- Les PME toujours plus conscientes des pertes d'exploitation liées aux cybers attaques
- Les entreprises spécialisées en conseil en sécurité des SI
- Les éditeurs de logiciels et les Entreprises de Services Numériques ou ESN

Il peut également être créateur d'entreprise innovante dans un des secteurs le plus en demande du domaine numérique.

TYPE D'EMPLOIS ACCESSIBLES

Le marché de l'emploi dans le secteur de la sécurité informatique est en tension et en fort développement. Les métiers et fonctions visés par la certification Cybersécurité et réseaux se présentent comme suit

Les emplois visés par la formation en début de carrière :

- Analyste sécurité systèmes et réseaux
- Assistant-ingénieur sécurité des systèmes d'information
- Assistant-ingénieur intégration
- Administrateur des systèmes d'information
- Analyste SOC

Après 2 à 3 ans d'expérience :

- Pentester
- Ingénieur Cybersécurité
- Consultant cybersécurité
- Responsable de la sécurité des systèmes d'information (RSSI)

RÈGLEMENTATIONS D'ACTIVITÉ

Il n'y a pas de réglementation d'activité à proprement parler. Cependant des références juridiques sont recommandées dans le cadre de l'exercice des activités :

ISO2001, ISO 27005, RGPD, NIS2.

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (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)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique 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

MODALITÉS D'ACCÈS

Formation initiale, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le cas échéant, prérequis à l'entrée en formation :

Accès en B1 (1ère année) : L'admission au Bachelor en sciences et Ingénierie spécialité Cybersécurité et réseaux se fait après le Baccalauréat ou un diplôme étranger de fin d'études secondaires reconnu comme équivalent par le Ministère Français de l'Éducation Nationale.

Entrées en B1 : Les candidat(e)s postbac seront recruté(e)s via la procédure Parcours Sup et sous réserve de passer le concours Alpha. La réforme du lycée implique aujourd'hui des choix d'options, c'est donc à partir du profil d'options choisies par le candidat qu'il faut aujourd'hui déterminer la stratégie et les objectifs de recrutement. Du fait de l'importance de l'enseignement scientifique, une spécialisation parmi les mathématiques, les sciences physiques ou l'informatique est indispensable.

Accès en B3 (3ème année) : L'admission au Bachelor en sciences et Ingénierie spécialité Cybersécurité et réseaux est possible pour les titulaires d'un diplôme de niveau 5 minimum. Le recrutement est ouvert typiquement à des étudiants ayant validé une deuxième année dans le secteur informatique.

PRÉREQUIS À LA VALIDATION

La certification Cybersécurité et réseaux donne lieu à un titre de grade de licence, il faut à ce titre avoir validé les critères suivants en plus des blocs de compétences afin d'obtenir la certification :

- Un niveau minimum en anglais : le candidat doit avoir validé un niveau B1 (CECRL : Cadre Européen Commun de Référence pour les Langues) en anglais à l'issue du processus menant à la certification
- Une période professionnelle : le candidat doit avoir réalisé une période en entreprise de 8 semaines par année (stage ou alternance)

- Une mobilité internationale : le candidat doit avoir effectué une période à l'international telle que mentionnée sur le site de l'Efrei

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE

Le jury de certification est composé de :

3 personnes, dont 2 membres externes respectant les critères suivants :

Salarié(e)s et/ou indépendant(e)s exerçant les métiers visés au minimum depuis 2 ans et n'ayant pas quitté le champ professionnel d'exercice des métiers visés depuis plus de 5 ans,

- À minima titulaire d'un diplôme ou d'un titre/certification à finalité professionnelle de même niveau que la certification visée, et ce, quel que soit la voie d'acquisition du diplôme ou du titre,
- À titre dérogatoire : la capitalisation d'une expérience professionnelle justifiée d'au moins 5 années dans les secteurs d'activités et les métiers visés de la certification, peut donner lieu à habilitation de membre de jury par la réalisation d'un entretien d'appréciation avec un expert métier de l'Efrei ;

et 1 membre interne employé d'Efrei Paris :

à minima titulaire d'un diplôme ou d'un titre/certification à finalité professionnelle de même niveau que la certification visée, et ce, quel que soit la voie d'acquisition du diplôme ou du titre.

Le cas échéant, son expérience dans les secteurs d'activités et les métiers visés de la certification est justifiée par 5 années minimum et par leur participation obligatoire à la construction du projet de certification.

Le président du jury sera désigné par le directeur général de l'Efrei.

COMPOSITION DU JURY — VAE

Le jury de certification est composé de :

3 personnes, dont 2 membres externes respectant les critères suivants :

Salarié(e)s et/ou indépendant(e)s exerçant les métiers visés au minimum depuis 2 ans et n'ayant pas quitté le champ professionnel d'exercice des métiers visés depuis plus de 5 ans,

- À minima titulaire d'un diplôme ou d'un titre/certification à finalité professionnelle de même niveau que la certification visée, et ce, quel que soit la voie d'acquisition du diplôme ou du titre,
- À titre dérogatoire : la capitalisation d'une expérience professionnelle justifiée d'au moins 5 années dans les secteurs d'activités et les métiers visés de la certification, peut donner lieu à habilitation de membre de jury par la réalisation d'un entretien d'appréciation avec un expert métier de l'Efrei ;

et 1 membre interne employé d'Efrei Paris :

à minima titulaire d'un diplôme ou d'un titre/certification à finalité professionnelle de même niveau que la certification visée, et ce, quel que soit la voie d'acquisition du diplôme ou du titre.

Le cas échéant, son expérience dans les secteurs d'activités et les métiers visés de la certification est justifiée par 5 années minimum et par leur participation obligatoire à la construction du projet de certification.

Le président du jury sera désigné par le directeur général de l'Efrei.

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	7 923 €
Selon la branche	7 000 € – 9 210 €
Prise en charge	Branches concernées
7 923 €	Valeur par défaut · 199 branches
9 210 €	CPNE Casinos, CPNE autoroutes, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEF des Espaces de Loisirs, d'Attractions et Culturels (ELAC)
8 400 €	CPNEFP de l'habillement, mercerie, chaussure et jouet

8 255 €	CPNEFP Professions de la Photographie
8 134 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie
7 967 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
7 700 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 500 €	CPNE des industries de santé (CPNEIS)
7 124 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie
7 000 €	CPNEFP de la métallurgie

Base légale

Date d'échéance de l'enregistrement	31/08/2030
Date de dernière délivrance possible	01/10/2032

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP36806

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
Bachelor Ingénierie et Cybersécurité - Efrei

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40745/>