

Sciences et ingénierie - Cybersécurité

RNCP40744 · 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, 31009, 24293, 31028
Code(s) ROME	M1805, M1801, M1802, M1806, M1810
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2028

Certificateur(s)

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

YNCREA MEDITERRANEE · SIRET : 38338687700039

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION POUR LA FORMATION DES INFORMATIENS PAR L'APRENTISSAGE	39108721000046	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

À la suite de la prise de conscience grandissante des enjeux de cybersécurité dans l'ensemble des secteurs d'activité publics et privés, la France a annoncé au mois de février 2021 un plan « France 2030 » de lutte dédié à la cybersécurité à hauteur de 1 milliard d'euros. Ce plan a vocation à accélérer la stratégie nationale visant à construire un véritable écosystème cyber français d'ici 2025. L'objectif est de hisser la France au rang des champions mondiaux de la cybersécurité.

Déjà en forte croissance du fait de la multiplication des cyberattaques, le secteur de la cybersécurité est aujourd'hui dopé par cet élan national. Selon certains rapports, le marché lié à la cybersécurité à l'échelle nationale devrait doubler entre 2021 et 2025 à l'image du marché mondial. Par conséquent les entreprises, mais également les organismes publics, sont de plus en plus demandeurs de professionnels opérationnels qualifiés dans le domaine de la cybersécurité. Face à une réelle pénurie, le nombre d'offres d'emploi sur des postes concernant la cybersécurité publiées sur l'APEC a par exemple, doublé entre 2017 et 2021. Les opportunités sont désormais réelles, variées, nombreuses et durables. D'après la société Splunk, multinationale américaine spécialisée dans la cybersécurité, un tiers des entreprises rencontre des difficultés de recrutement.

A la lueur de ce constat, la formation devient un axe stratégique incontournable pour les entreprises et l'Etat Français afin de garantir leurs objectifs stratégiques de sécurité dans le cyberespace.

Sur demande des entreprises locales, régionales et nationales partenaires, l'ISEN Yncréa Méditerranée souhaite s'engager concrètement et avec force dans la certification des professionnels opérationnels en cybersécurité de niveau 6 afin de relever le défi commun qui nous unit.

Pour l'école, l'enjeu est de compléter son offre de certification pour répondre aux besoins en recrutement de toutes les entreprises et organisations au niveau local, régional et national.

Le Grade Licence Cybersécurité de l'ISEN Yncréa Méditerranée s'inscrit dans cette stratégie de former et certifier les jeunes générations aux métiers de la cybersécurité en soutien aux ingénieurs déjà présents dans le tissu industriel. Cette certification apporte des compétences approfondies dans les principaux domaines de la sécurité « hardware » et « software », tels que par exemple, la sécurité des réseaux, la cryptographie, la gestion des identités et des accès, la gestion des risques, la sécurité des objets et applications et la conformité réglementaire.

Les objectifs de cette certification visent ainsi à répondre aux besoins quantitatifs, mais aussi et surtout qualitatifs, en recrutement des entreprises et organisations de toutes tailles confrontées à des risques de plus en plus importants de pertes de données, de fuites d'informations confidentielles, de vols d'identité et de cyberattaques.

ACTIVITÉS VISÉES

Le professionnel en cybersécurité titulaire de cette certification exerce les activités professionnelles suivantes :

- Analyse des risques et des menaces informatiques
- Réalisation d'audits techniques sur des systèmes d'information
- Contribution à la définition d'architectures informatiques sur la base d'exigences en conformité avec les règles de sécurité
- Administration, configuration et exploitation de solutions de sécurité informatique
- Suivi et maintien en condition de sécurité des systèmes d'information
- Développement, test et déploiement de solutions de sécurisation sur les systèmes d'information
- Contribution aux projets liés à la cybersécurité
- Réalisation d'une veille permanente des menaces cybersécurité

COMPÉTENCES ATTESTÉES

Le professionnel en cybersécurité titulaire de cette certification évolue dans des métiers faisant appel aux compétences suivantes :

- Participer à la conception, le déploiement et configuration de solutions informatiques en appliquant et respectant les normes, les réglementations et les bonnes pratiques en vigueur
- S'intégrer dans une organisation projet en se conformant aux contraintes et aux problématiques induites par le processus de gestion et de conduite d'un projet (gestion du projet, gestion des risques et du changement, gestion du personnel) dans le milieu industriel et des entreprises
- Travailler dans un contexte national et international à travers des présentations orales ou des travaux écrits en langue française ou anglaise afin de communiquer et de collaborer de manière efficace au sein d'une équipe multidisciplinaire.
- Identifier et résoudre une problématique dans le cadre d'une activité ou d'un projet technique dans le domaine de la sécurité informatique
- Analyser des processus et des systèmes informatiques conformément aux méthodes appropriées existantes dans un environnement avec des contraintes techniques et non techniques (humaines, sociétales, environnementales, industrielles et économiques) afin d'identifier et d'évaluer les risques cybernétiques dans le cadre d'un audit technique
- Définir et mener des études expérimentales, interpréter les données et tirer des conclusions dans le cadre d'audit de sécurité et de tests d'intrusion afin de vérifier l'efficacité des politiques de sécurité sous le contrôle de son supérieur hiérarchique.
- Recueillir, interpréter et synthétiser les données et les alertes de sécurité ainsi que les renseignements disponibles afin de réaliser une étude sur les menaces de cybersécurité et d'éclairer les décisions sur les mesures nécessaires à la continuité d'activité d'une entreprise
- Formuler et argumenter des recommandations à sa hiérarchie et/ou aux collaborateurs via des sensibilisations (rapports écrits ou présentations orales) adaptées à tous publics, notamment aux personnes en situation de handicap
- Mener une investigation numérique post incident de sécurité en appliquant rigoureusement les méthodes appropriées et en tenant compte du contexte technique et non technique (judiciaire, économique, industriel, sociétal)
- Communiquer à l'écrit et à l'oral en langue française ou anglaise en s'adaptant au public et à la qualité de ses récepteurs (journalistes, collaborateurs, responsable hiérarchique) dans un environnement de gestion de crise
- Proposer et appliquer des actions de sécurité immédiates sur les aspects vitaux du système informatique pour contenir ou éradiquer rapidement les menaces identifiées afin de permettre la poursuite d'activité de l'entreprise
- Restaurer méthodiquement le système informatique conformément à la politique de sécurité et exploiter le retour d'expérience en appliquant de nouvelles mesures permettant d'améliorer la résilience cybersécurité afin de garantir la reprise de l'activité de l'entreprise
- Appliquer et utiliser les mathématiques, les langages de programmation, les algorithmes, l'intelligence artificielle et les autres sciences de base pour concevoir et développer des outils de sécurité informatique complexes, et accélérer

leur mise au point

- Développer et intégrer des solutions informatiques et organisationnelles adaptées aux critères environnementaux, sociétaux, économiques et industriels
- Contribuer à des réflexions d'innovation dans les projets de l'entreprise et plus généralement dans une approche entrepreneuriale.
- Effectuer une veille technologique et scientifique (sites web spécialisés, publications, forums...) et un état de l'art du domaine de la cybersécurité et des évolutions matérielles informatiques afin d'adapter sa pratique professionnelle et d'approfondir les études et la recherche dans le domaine de la sécurité informatique

Blocs de compétences

RNCP40744BC01 — Participer à la conception et au développement d'une solution de sécurité informatique

LISTE DE COMPÉTENCES

- Participer à la conception au déploiement et à la configuration de solutions informatiques en appliquant et respectant les normes, les réglementations et les bonnes pratiques en vigueur
- S'intégrer dans une organisation projet en se conformant aux contraintes et aux problématiques induites par le processus de gestion et de conduite d'un projet (gestion du projet, gestion des risques et du changement, gestion du personnel) dans le milieu industriel et des entreprises
- Travailler dans un contexte national et international à travers des présentations orales ou des travaux écrits en langue française ou anglaise afin de communiquer et de collaborer de manière efficace au sein d'une équipe multidisciplinaire.
- Identifier et résoudre une problématique dans le cadre d'une activité ou d'un projet technique dans le domaine de la sécurité informatique

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle via des études de cas pratiques avec présentation à l'écrit ou à l'oral :

- du rappel des bonnes pratiques ANSSI, normes réglementation et politique de sécurité adaptées au cas pratique
- de l'architecture retenue avec les éléments de configuration et de paramétrage

Réalisation de projets techniques en groupes basés sur des situations authentiques reprenant le développement d'outils et d'applications répondant à un cahier des charges avec présentation à l'écrit ou à l'oral :

- du cahier des charges
- du rappel des bonnes pratiques ANSSI, normes, réglementation et politique de sécurité adaptées au projet
- un état de l'art des matériels et protocoles pouvant être utilisés
- des équipements informatiques, de l'architecture retenue avec les éléments de configuration et de paramétrage
- de l'organisation projet du groupe

Evaluations individuelles sur les connaissances théoriques portant sur :

- les équipements et architectures réseaux
- normes et réglementations de sécurité
- la gestion de projets

RNCP40744BC02 — Auditer et superviser la sécurité des systèmes

LISTE DE COMPÉTENCES

- Analyser des processus et des systèmes informatiques conformément aux méthodes appropriées existantes dans un environnement avec des contraintes techniques et non techniques (humaines, sociétales, environnementales, industrielles et économiques) afin d'identifier et d'évaluer les risques en cybersécurité dans le cadre d'un audit technique
- Définir et mener des études expérimentales sous le contrôle de son supérieur hiérarchique et tirer des conclusions dans le cadre d'audit de sécurité et de tests d'intrusion afin de vérifier l'efficacité des politiques de sécurité
- Recueillir, interpréter et synthétiser les données et les alertes de sécurité ainsi que les renseignements disponibles afin de réaliser une étude sur les menaces de cybersécurité et d'éclairer les décisions sur les mesures nécessaires à la continuité d'activité d'une entreprise
- Formuler et argumenter des recommandations à sa hiérarchie et/ou aux collaborateurs via des sensibilisations (rapports écrits ou présentations orales) adaptées à tous publics, notamment aux personnes en situation de handicap

MODALITÉS D'ÉVALUATION

Mise en situation individuelle sur un cas concret de sensibilisation d'une équipe aux bonnes pratiques cybersécurité conformément aux recommandations de l'ANSSI sous la forme d'un exposé oral

Mise en situation individuelle sur un cas concret de mise en place et la configuration d'équipements de détection et d'un SIEM sur une architecture réseau virtualisée avec présentation à l'écrit ou à l'oral :

- du choix et de l'emplacement des équipements de détection
- de la configuration des équipements de détection
- de la configuration de la remontée des alertes sur le SIEM
- de la liste des alertes remontées une fois le système configuré
- d'une analyse des alertes obtenues

Mise en situation individuelle sur un cas concret d'analyse de risque sur une infrastructure d'entreprise réaliste avec présentation à l'écrit ou à l'oral :

- des différentes étapes de la méthode EBIOS
- des risques identifiés
- des moyens mis en place pour diminuer ou faire disparaître le risque avec argumentation sur les choix réalisés
- du plan d'actions sur les moyens à mettre en place pour améliorer la sécurité de l'infrastructure

Mise en situation individuelle sur un cas concret d'audit technique de sécurité en utilisant les méthodes OSINT et de pentest avec présentation à l'écrit ou à l'oral :

- des tests d'intrusion utilisés
- du rappel de la réglementation sur le droit du numérique
- des faiblesses de l'infrastructure auditée

Mise en situation professionnelle en groupes avec un scénario Red/Blue team dont l'objectif est de construire une infrastructure de bout en bout à défendre/attaquer

RNCP40744BC03 — Gérer les incidents de sécurité et contribuer à réaliser les actions de remédiation

LISTE DE COMPÉTENCES

- Mener une investigation numérique post incident de sécurité en appliquant rigoureusement les méthodes appropriées et en tenant compte du contexte technique et non technique (judiciaire, économique, industriel, sociétal)
- Communiquer à l'écrit et à l'oral en langue française ou anglaise en s'adaptant au public et à la qualité de ses récepteurs (journalistes, collaborateurs, responsable hiérarchique) dans un environnement de gestion de crise
- Proposer et appliquer des actions de sécurité immédiates sur les aspects vitaux du système informatique pour contenir ou éradiquer rapidement les menaces identifiées afin de permettre la poursuite d'activité de l'entreprise
- Restaurer méthodiquement le système informatique conformément à la politique de sécurité et exploiter le retour d'expérience en appliquant de nouvelles mesures permettant d'améliorer la résilience cybersécurité afin de garantir la reprise de l'activité de l'entreprise

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle via des études de cas pratiques d'investigation numérique avec présentation à l'écrit ou à l'oral :

- de la procédure d'investigation et des protocoles mis en oeuvre
- les traces et preuves relevées

Mise en situation professionnelle en groupes via des études de cas pratiques de gestion d'incidents avec présentation à l'écrit ou à l'oral :

- du plan d'actions immédiates pour contenir l'incident
- des éléments de communication à destination des parties prenantes (état du système, délai, conséquences...)
- du plan de remédiation avec planification des opérations pour recouvrir la totalité des services

RNCP40744BC04 — Mobiliser des connaissances scientifiques pour développer des solutions de cybersécurité

LISTE DE COMPÉTENCES

- Appliquer et utiliser les mathématiques, les langages de programmation, les algorithmes, l'intelligence artificielle et les autres sciences de base pour concevoir et développer des outils de sécurité informatique complexes, et accélérer leur mise au point
- Développer et intégrer des solutions informatiques et organisationnelles adaptées aux critères environnementaux, sociétaux, économiques et industriels
- Entreprendre et innover tant dans des projets personnels que par l'engagement entrepreneurial au sein de l'entreprise

- Effectuer une veille technologique et scientifique (sites web spécialisés, publications, forums...) et un état de l'art du domaine de la cybersécurité et des évolutions matérielles informatiques afin d'adapter sa pratique professionnelle et d'approfondir les études et la recherche dans le domaine de la sécurité informatique

MODALITÉS D'ÉVALUATION

Exercices individuels ou en groupes de mise en situation avec des cas concrets permettant d'évaluer :

- les connaissances en programmation et algorithmie
- les connaissances des technologies émergentes (IA, blockchain...)
- la prise en compte des enjeux du développement durable et les bonnes pratiques de développement

Réalisation de projets techniques ou de recherche en groupes basés sur des situations authentiques reprenant le développement d'outils et d'applications répondant à un cahier des charges avec présentation à l'écrit ou à l'oral :

- de l'état de l'art des technologies (IA, Blockchain, Crypto...) et matériels pouvant être utilisés
- des connaissances scientifiques mobilisées
- du cahier des charges avec les spécifications fonctionnelles et techniques
- de la solution permettant de répondre au cahier des charges
- de l'aspect innovant ou créatif de la solution retenue
- de la prise en compte des contraintes DDRSE

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le professionnel en cybersécurité titulaire de cette certification exerce son activité au sein des organisations suivantes. Aujourd'hui, toutes les organisations ont besoin d'experts techniques en cybersécurité pour la protection de leurs données et de leur système d'information.

- Administrations publiques du type ministère des Armées, ANSSI, ministère de l'intérieur,
- Grands groupes du secteur industriel, banques, commerces, assurances,
- Entreprises de taille intermédiaire (ETI),
- Petites et moyennes entreprises (PME),
- Organisations spécialisées en conseil en sécurité des systèmes d'information,
- Associations,
- Entreprise de Services Numériques (ESN).

Le titulaire de cette certification peut également devenir créateur d'entreprise dans le domaine du numérique et/ou de la cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

Le marché de l'emploi dans le secteur de la cybersécurité connaît une forte tension et une dynamique croissante. Le titulaire de cette certification peut prétendre aux métiers et activités suivantes (cf. panorama des métiers de la cybersécurité ANSSI – édition 2020) :

- Développeur de solutions de sécurité,
- Intégrateur de solutions de sécurité
- Opérateur analyste SOC,
- Analyste réponse aux incidents de sécurité,
- Analyste de la menace cybersécurité,
- Administrateur de solutions de sécurité,
- Responsable de projet de sécurité,
- Responsable de la sécurité des SI au sein d'une PME/TPE.

Après une première expérience, le titulaire de cette certification peut évoluer vers les métiers et activités suivantes (cf. panorama des métiers de la cybersécurité ANSSI – édition 2020) :

- Responsable de CSIRT,
- Responsable de SOC,
- Auditeur de sécurité,
- Formateur en cybersécurité
- Consultant cybersécurité,
- Responsable de la Sécurité des Systèmes d'Information (RSSI),
- Chef sécurité projet.

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

MODALITÉS D'ACCÈS
Formation initiale, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION
Le recrutement en première année se fait après obtention d'une certification de niveau 4 général ou technologique.
Des admissions parallèles sont possibles en deuxième année si le candidat a validé 60 crédits (ECTS) dans une formation d'enseignement supérieur en informatique, réseaux, numérique ou cybersécurité.

PRÉREQUIS À LA VALIDATION
Pour les candidats inscrits dans le parcours de formation, outre la validation des compétences détaillées ci-dessus, l'obtention du Grade Licence - Sciences et ingénierie – Cybersécurité nécessite la validation :

- d'un niveau B1 du cadre européen commun de référence pour les langues (CECRL) en anglais,
- d'une mobilité à l'international de 4 semaines minimum,
- d'un engagement responsable (ER)

Les candidats inscrits dans un processus de VAE, devront apporter les preuves de l'acquisition des compétences au travers de leur expérience professionnelle permettant de valider les 4 blocs de compétences et un niveau B1 du cadre européen commun de référence pour les langues (CECRL) en anglais.

COMPOSITION DU JURY — FORMATION INITIALE

Le jury d'attribution du Titre est présidé par le Directeur / la Directrice de l'ISEN Méditerranée. Il comprend en plus du Président, le Directeur des études du Bachelor, le Responsable de la Vie Etudiante, deux enseignants du programme et deux personnalités extérieures représentant des entreprises significatives du secteur d'activité des diplômés.

COMPOSITION DU JURY — APPRENTISSAGE

Le jury d'attribution du Titre est présidé par le Directeur / la Directrice de l'ISEN Méditerranée. Il comprend en plus du Président, le Directeur des études du Bachelor, le Directeur du CFA ou son représentant, le Responsable de la Vie Etudiante, deux enseignants du programme et deux personnalités extérieures représentant des entreprises significatives du secteur d'activité des diplômés.

COMPOSITION DU JURY — VAE

Le jury d'attribution du Titre est présidé par le Directeur / la Directrice de l'ISEN Méditerranée. Il comprend en plus du Président, le Directeur des études du Bachelor, le Responsable de la VAE, deux enseignants du programme et deux personnalités extérieures représentant des entreprises significatives du secteur d'activité des diplômés.

Base légale

Date d'échéance de l'enregistrement	31/08/2028
-------------------------------------	------------

Date de dernière délivrance possible	31/08/2030
--------------------------------------	------------

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40744/>