

Sciences et Ingénierie - Sécurité du numérique

RNCP37708 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	326
Formacode(s)	31006, 31032, 31067, 24293
Code(s) ROME	M1804, M1805, M1801, M1802
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2025

Certificateur(s)

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

ECOLE POUR L'INFORMATIQUE ET LES TECHNIQUES AVANCEES (EPITA) · SIRET : 89819207500015

Résumé de la certification

OBJECTIFS ET CONTEXTE

Depuis plusieurs années, le secteur de la sécurité informatique est en très forte croissance et restructuration du fait de l'explosion du nombre des attaques informatiques et de la diversité des formes qu'elles mettent en oeuvre. Les SOC (Security Operation Center) constituent au sein des entreprises les remparts destinés à protéger la sécurité des systèmes d'information. La mission des équipes au sein des SOC a considérablement évolué au cours des dernières années grâce en particulier à l'automatisation de nombreuses fonctions de surveillance. Les ingénieurs en cybersécurité sont ainsi toujours très recherchés mais de nouveaux profils de niveau 6 sont aujourd'hui indispensables au bon fonctionnement des équipes.

La création du Bachelor en Sécurité du Numérique répond à la demande très précise des entreprises de cyber et des entreprises utilisatrices des compétences cyber.

ACTIVITÉS VISÉES

Les titulaires du titre de Bachelor en Sécurité du Numérique de l'EPITA sont préparés à une intégration professionnelle visant les activités suivantes (issues du Panorama des métiers de la cybersécurité produit par l'ANSSI et du référentiel de compétences des métiers de la cybersécurité du groupe de travail « Formation » du Campus Cyber) :

Réaliser des audits techniques sur les Systèmes d'Information de l'entreprise pour évaluer leur robustesse.

Réaliser ou piloter la mise en œuvre de scans de vulnérabilités et de contrôles techniques, en continu et de manière automatisée.

Réaliser une veille permanente vis-à-vis des scénarii d'attaques, des nouvelles menaces, des vulnérabilités associées et sur les techniques de développement sécurisé.

Administrer et paramétrer des solutions de sécurité en assurant leur fonctionnement optimal, le traitement des journaux d'activités et leur conformité aux normes en vigueur, notamment les outils de détection des menaces.

Concevoir et développer des solutions de sécurité : outils d'investigation, d'analyse des journaux d'activité et de détection d'intrusion.

Identifier et analyser les événements de sécurité de l'entreprise ; collecter des informations techniques ou non, des Systèmes d'Information de l'entreprise ou de sources ouvertes permettant la rédaction de rapports d'incidents.

Produire ou contribuer à l'élaboration de plans d'actions suite à la détection d'activités suspectes ou malveillantes.

Intégrer les enjeux et le contexte de la cybermenace afin d'analyser et de pouvoir la qualifier pour produire un rapport

sur le niveau d'exposition d'une organisation.

Contribuer à la définition de l'architecture technique des Systèmes d'Information en lien avec les équipes concernées.
Mettre en œuvre la recette, l'industrialisation et la mise en production d'une solution de sécurité en lien avec le responsable du projet.

COMPÉTENCES ATTESTÉES

Connaître et comprendre les mathématiques, autres sciences de base ainsi que disciplines d'ingénierie et comprendre les équipements, outils applicables, des technologies et processus techniques indispensables à la sécurité informatique

Analyser des produits, processus et systèmes techniques dans le cadre d'un audit technique de sécurité

Sélectionner et appliquer les méthodes analytiques et expérimentales existantes appropriées pour mener à bien la conception, le développement, les tests et le déploiement de solutions informatiques orientées sécurité

Reconnaître l'importance des contraintes non techniques (sociétales, de sécurité, environnementales, économiques et industrielles), notamment dans le cadre de la gestion des risques et de la gestion des crises.

Concevoir et développer des produits, processus et systèmes relevant de la sécurité informatique, en respectant des contraintes imposées en sélectionnant et appliquant les méthodologies de conception appropriées et en tenant compte des aspects non techniques (sociétaux, de sécurité, environnementaux, économiques et industriels).

Mener des recherches bibliographiques, consulter et utiliser avec un œil critique des bases de données scientifiques et d'autres sources d'informations appropriées, réaliser des simulations et analyses afin d'approfondir les études et la recherche sur des sujets techniques dans le domaine de la cybersécurité.

Concevoir et mener des études expérimentales, interpréter les données et tirer des conclusions dans le domaine de la cybersécurité dans le cadre d'audit de sécurité et de tests d'intrusion.

Identifier, formuler et résoudre des problèmes complexes, gérer des activités ou projets techniques ou professionnels dans le domaine de la sécurité informatique.

Identifier les aspects non techniques (humains, sociétaux, de sécurité, environnementaux, économiques et industriels) de la pratique de l'ingénierie informatique et la gestion d'une infrastructure informatique logicielle ou physique.

Prendre en compte les problèmes économiques, organisationnels et de gestion (gestion de projet, gestion des risques et du changement...) dans le milieu industriel, des entreprises et des acteurs gouvernementaux de la cybersécurité.

Consulter et appliquer les normes, codes de bonne pratique et les réglementations de sécurité? de la cybersécurité dans le cadre de la conception de solutions informatiques orientées sécurité.

Recueillir et interpréter des données pertinentes et appréhender la complexité? dans la sécurité du numérique, afin d'éclairer les décisions nécessitant une réflexion sur des problèmes sociaux et éthiques importants.

Communiquer des informations, idées, problèmes et solutions de manière efficace avec la communauté? des ingénieurs et la société? en général.

Travailler de manière efficace dans un contexte national et international, en tant qu'individu et membre d'une équipe, et collaborer de manière efficace avec des ingénieurs et non-ingénieurs, gérer des activités ou projets techniques ou professionnels complexes dans la sécurité des systèmes d'information, en assumant la responsabilité de ses décisions.

Entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux

Suivre les évolutions scientifiques et technologiques dans le domaine de l'ingénierie informatique et dans le domaine de la sécurité informatique et s'engager dans un apprentissage tout au long de la vie.

Blocs de compétences

RNCP37708BC01 — Analyser et développer une solution informatique dans le domaine des réseaux et de la cybersécurité

LISTE DE COMPÉTENCES

Appliquer les mathématiques, autres sciences de base ainsi que les disciplines d'ingénierie et compréhension des équipements, outils applicables, des technologies et processus techniques indispensables à la sécurité informatique, à un niveau suffisant pour atteindre les autres acquis de formation.

Analyser des produits, processus et systèmes techniques dans le cadre d'un audit technique de sécurité en appliquant :

- les méthodes analytiques et expérimentales existantes appropriée pour mener à bien la conception, le développement, les tests et le déploiement de solutions informatiques orientées sécurité ;
- en identifiant les contraintes non techniques (sociétales, de sécurité, environnementales, économiques et industrielles), notamment dans le cadre de la gestion des risques et de la gestion des crises.

Concevoir et développer des produits, processus et systèmes relevant de la sécurité informatique :

- en respectant des contraintes imposées
- en sélectionnant et en appliquant les méthodologies de conception appropriées
- en tenant compte des aspects non techniques (sociétaux, d'hygiène et de sécurité, environnementaux, économiques et industriels).

Mener des recherches bibliographiques, à consulter et utiliser avec un œil critique des bases de données scientifiques et d'autres sources d'informations appropriées, à réaliser des simulations et analyses afin d'approfondir les études et la recherche sur des sujets techniques dans le domaine de la cybersécurité.

Concevoir et mener des études expérimentales, interpréter les données et tirer des conclusions dans le domaine de la cybersécurité dans le cadre d'audit de sécurité et de tests d'intrusion.

Identifier, formuler et résoudre des problèmes complexes, à gérer des activités ou projets techniques ou professionnels dans le domaine de la sécurité informatique.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle via des études de cas pratiques nécessitant l'élaboration et la rédaction d'un état de l'art et d'un état des lieux d'un domaine d'application de la cybersécurité (réseaux, télécom, ...) sur une thématique inspirée de celles d'entreprises.

Réalisation de projets informatiques concrets basés sur des situations authentiques et sur le développement d'outils et d'applications répondant à un cahier des charges, certains projets seront construits ex nihilo tandis que d'autres partiront d'une base existante.

Projet de recherche suivant plusieurs phases : consultation et analyse de papiers scientifiques de recherche sur l'existant, élaboration d'un cahier des charges répondant au problème avec un chercheur du domaine, conception de la solution selon les méthodes scientifiques de la recherche et possible conception d'une affiche de recherche ou d'un papier de recherche sur le sujet soutenu devant le chercheur concerné.

RNCP37708BC02 — Auditer et analyser le contexte et les exigences de l'entreprise en matière de cybersécurité

LISTE DE COMPÉTENCES

Identifier les aspects non techniques (humains, sociétaux, de sécurité, environnementaux, économiques et industriels) de la pratique de l'ingénierie informatique et la gestion d'une infrastructure informatique logicielle ou physique.

Identifier les problèmes économiques, organisationnels et de gestion (gestion de projet, gestion des risques et du changement...) dans le milieu industriel, des entreprises et des acteurs gouvernementaux de la cybersécurité.

Consulter, appliquer et respecter les normes, codes de bonnes pratiques et les réglementations de sécurité de la cybersécurité dans le cadre de la conception de solutions informatiques orientées sécurité.

Interpréter des données pertinentes et à appréhender la complexité dans la sécurité du numérique, afin d'éclairer les décisions nécessitant une réflexion sur des problèmes sociaux et éthiques importants.

Formuler des recommandations aux utilisateurs, développeurs et aux décideurs suite à l'analyse du contexte de cybersécurité de l'entreprise.

MODALITÉS D'ÉVALUATION

Exercices individuels et en groupes de mises en situation en prenant en compte les enjeux du développement durable, les réglementations en vigueur et les bonnes pratiques du développement pour s'assurer de la sécurité des utilisateurs et de leurs données. Ces exercices prendront la forme d'études de cas réels (ou authentiques) sur des projets techniques ayant un fort impact humain, sociétal ou environnemental et comportant une problématique à résoudre.

Évaluations sur les connaissances théoriques des normes et réglementations sous forme de soutenance, d'exposés ou de devoirs papiers.

Réalisation d'un audit de la gestion d'une entreprise et des projets techniques liés à la sécurité, notamment sous la forme d'un rapport.

RNCP37708BC03 — Réaliser une veille dans le domaine de la sécurité du numérique, sur les évolutions scientifiques et techniques et adaptation de sa pratique professionnelle

LISTE DE COMPÉTENCES

Communiquer des informations, idées, problèmes et solutions de manière efficace avec la communauté des ingénieurs et la société en général.

Travailler de manière efficace dans un contexte national et international, en tant qu'individu et membre d'une équipe, et à collaborer de manière efficace avec des ingénieurs et non-ingénieurs, aptitude à gérer des activités ou projets techniques ou professionnels complexes dans la sécurité des systèmes d'information, en assumant la responsabilité de ses décisions.

Entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux.

Suivre les évolutions scientifiques et technologiques dans le domaine de l'ingénierie informatique et dans le domaine de la sécurité informatique et à s'engager dans un apprentissage tout au long de la vie.

MODALITÉS D'ÉVALUATION

Exercices individuels et en groupes sous forme de jeux de rôle et d'improvisation dans un contexte technique ou non, dans un contexte national ou international.

Réalisation de projets techniques et théoriques dans un environnement international piloté et proposé par des entités internationales.

RNCP37708BC04 — Concevoir et développer des solutions informatiques et de sécurité informatique

LISTE DE COMPÉTENCES

Concevoir, développer, tester et déployer des solutions informatiques orientées sécurité.

Planifier et gérer des projets en prenant en compte la gestion des risques et la gestion de crises afin de garantir la réalisation et la pérennité du projet.

Formuler des recommandations aux développeurs de solutions informatiques et former les utilisateurs et clients pour une prise en main efficace et efficiente de la solution.

MODALITÉS D'ÉVALUATION

Réalisation d'un projet informatique en plusieurs phases : création d'un site web sécurisé prenant en compte les bonnes pratiques techniques préconisées, déploiement manuel puis automatique du site "on premise" ou sur une infrastructure cloud, mise en place de la remontée des logs du site pour automatiser les actions de sécurité et scénarii blue/red team selon des temporalités prévues et inattendues pour garantir la résilience du produit. Ce projet sera défendu lors d'une soutenance.

Conception d'outils d'intrusion individuellement et par équipe sur différents systèmes d'exploitation et sur différentes applications en mode blue/red team.

RNCP37708BC05 — Auditer la sécurité et définir la politique de sécurité informatique de l'entreprise

LISTE DE COMPÉTENCES

Évaluer le niveau de sécurité d'un système d'information.

Définir des politiques de sécurité afin de les mettre en œuvre dans l'entreprise.

MODALITÉS D'ÉVALUATION

Réalisation d'un projet informatique en plusieurs phases : création d'un site web sécurisé prenant en compte les bonnes pratiques techniques préconisées, déploiement manuel puis automatique du site "on premise" ou sur une infrastructure cloud, mise en place de la remontée des logs du site pour automatiser les actions de sécurité et scénarii blue/red team selon des temporalités prévues et inattendues pour garantir la résilience du produit. Ce projet sera défendu lors d'une soutenance.

Conception d'outils d'intrusion individuellement et par équipe sur différents systèmes d'exploitation et sur différentes applications en mode blue/red team.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Entreprise de services du numérique (ESN)

Editeurs de logiciel

Cabinets de conseil
 Industrie
 Secteur « Banque, Finances et Assurance »
 E-business
 Secteur des télécommunications
 Défense
 Sécurité informatique
 Autres : Formation, Négoce/Distribution, Administration, Audiovisuel & Média, Jeux vidéo, Santé

TYPE D'EMPLOIS ACCESSIBLES

Développeur informatique
 Administrateur système / sécurité informatique
 Administrateur réseaux
 Assistant Ingénieur support
 Assistant Architecte télécoms
 Assistant Architecte en Systèmes d'information
 Architecte sécurité informatique junior
 Spécialiste en développement sécurité informatique
 Opérateur analyste SOC (Security Operation Center)
 Consultant en cybersécurité
 Coordinateur sécurité informatique
 Analyste de Malware
 Auditeur de sécurité informatique technique

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, Contrat de professionnalisation, 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.
Le recrutement en deuxième ou troisième année se fait après obtention d'une certification de niveau 5 dans un même domaine d'activité ou à l'issue de l'obtention d'un nombre équivalent de crédit européen de transfert et d'accumulation (ECTS).

PRÉREQUIS À LA VALIDATION

La certification s'obtient par la validation de chacun des blocs qui la compose, complétée d'une soutenance finale organisée à la fin du parcours et permettant de revalider l'ensemble des compétences du référentiel.
La validation du niveau B2 (norme CECRL, équivalent d'un score d'au moins 785 au TOEIC), une expérience multiculturelle comportant un séjour d'au moins 4 semaines à l'international et une immersion en entreprise d'au moins 14 semaines (hors apprentissage) sont nécessaires à l'obtention de la certification ; ces conditions peuvent être adaptées pour les étudiants (ou apprentis) en situation de handicap.

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

Le jury d'attribution du Titre est présidé par une personnalité extérieure à l'Ecole appartenant au monde économique ou universitaire. Il comprend en plus du Président, le Directeur de l'EPITA, le Directeur des études du Bachelor, le Directeur des Relations Entreprises, 2 enseignants et 4 personnalités extérieures représentant des entreprises significatives du secteur d'activité des diplômés.

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	9 475 €
Selon la branche	7 000 € – 12 000 €

Prise en charge	Branches concernées
9 475 €	Valeur par défaut · 176 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Branche des organismes de formation, CPNEF de la Publicité
9 480 €	CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films, CPNEF de l'audiovisuel
7 200 €	CPNE Banque, CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
11 055 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
8 990 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité

7 923 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 000 €	CPNE chimie, CPNEFP de la métallurgie
11 845 €	CPNE des Télécoms
11 844 €	CPNE Travail Temporaire
10 500 €	CPNEFP des industries des tuiles et briques
10 400 €	CPNEFP de la Mutualité Sociale Agricole
10 000 €	CPNE des exploitations frigorifiques
9 500 €	CPNE de l'ingénierie, des services informatiques et du conseil
9 000 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 842 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 500 €	CPNE des industries de santé (CPNEIS)
8 057 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 036 €	CPNE FP Branche des magasins du Bricolage
8 029 €	CPNEFP des jardineries et graineteries

Base légale

Date d'échéance de l'enregistrement 31/08/2025

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP41285

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://epita.fr/bachelor-cybersecurite-rncp>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37708/>