

Ingénieur diplômé de l'école d'ingénieurs Jules Verne de l'université d'Amiens, spécialité cybersécurité

RNCP40947 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31006, 31038, 32062, 15099, 24273
Code(s) ROME	M1801, M1802, M1803, M1806, M1810
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

ECOLE D'INGENIEURS JULES VERNE · SIRET : 19801344300900

Partenaires habilités

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

Organisme	SIRET	Habilitation
FORMASUP NORD-PAS DE CALAIS	42813525500050	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le diplôme d'ingénieur cybersécurité vise des spécialistes des problématiques liées à la sécurité informatique. Depuis plusieurs années le nombre et la diversité des menaces informatiques augmentent de manière drastique, de part l'augmentation des équipements, des failles et des utilisateurs. Toutes les entreprises quels que soient leurs domaines d'activités, sont touchées par ces menaces car les systèmes d'informations sont présents dans tous les secteurs d'activités. Malheureusement les spécialistes n'ont pas été suffisamment formés en nombre, les demandes dans ce domaine croissent de manière significative et les formations et certifications ne sont pas toujours adaptées car elles sont bien souvent incomplètes.

La certification vise donc à répondre à tous les besoins métiers et à toutes les demandes des entreprises dans le domaine de la cybersécurité. Tous les aspects seront abordés, que ce soit au niveau du matériel, des méthodes, des systèmes et des logiciels.

ACTIVITÉS VISÉES

Les activités de l'ingénieur diplômé en cybersécurité sont les suivantes :

- Élaboration d'une politique et d'une stratégie de cybersécurité
- Mise en œuvre d'une organisation cyber sécuritaire dans le cadre légal et réglementaire
- Conception d'une architecture de sécurité efficiente et respectueuse de l'environnement
- Conduite des opérations de maintenance d'un système de cybersécurité durable
- Communication professionnelle et technique en anglais et en français
- Élaboration, présentation et défense du budget alloué à la cybersécurité
- Animation et motivation d'équipes multiculturelles et pluridisciplinaires

- Mise en œuvre de tests de sécurité par attaque simulée
- Réalisation d'un audit de sécurité complet avec préconisations d'amélioration
- Conception et conduite d'un projet informatique en cybersécurité
- Rédaction d'un cahier des charges pour développer et mettre en place un dispositif de cybersécurité
- Développement ou supervision du développement d'applications logicielles pour la sécurité
- Évaluation de l'offre de solutions pour sécuriser les applications ou les systèmes d'exploitation
- Accompagnement des utilisateurs dans l'adoption d'un nouveau logiciel de cyberdéfense
- Gestion des cyberattaques en temps réel et en équipe
- Anticipation et détection en amont des intrusions dans le SI avec l'aide de l'IA
- Adaptation des processus et procédures de défense grâce au retour d'expérience

COMPÉTENCES ATTESTÉES

Elaborer et mettre en œuvre une politique de sécurité des systèmes d'information en mobilisant les outils d'analyse et en utilisant les contraintes juridiques

- Sensibiliser les directeurs et les collaborateurs aux enjeux et aux menaces cyber sécuritaires
- Participer à la définition des principes et des objectifs en termes de sécurité d'un système d'information
- Définir la stratégie cyber sécuritaire d'un Système d'informations (SI)
- Concevoir l'organisation ou la réorganisation de la sécurité d'un SI
- Intégrer les aspects juridiques et réglementaires liés au traitement, au stockage et à la protection des données

Prendre en compte les objectifs de développement durable et la responsabilité sociétale des entreprises pour concevoir et maintenir en opération un dispositif de protection des systèmes d'information efficient en mobilisant les bonnes pratiques environnementales et techniques

- Concevoir des architectures matérielles et logicielles sécurisées et optimisées du point de vue de leur consommation énergétique
- Maintenir un niveau d'équipements et de logiciels en phase avec les nouvelles technologies de cyberdéfense
- Gérer l'obsolescence des équipements et des composants en privilégiant la circularité
- Favoriser au sein des équipes internes et externes, l'adoption de règles de stockage et de traitement durables des données

Adopter une conduite des opérations de type inclusive efficiente et éthique
Garantir l'accès aux données informatiques pour les collaborateurs en situation de handicap selon le RGAA
Intégrer le fonctionnement et la culture d'une entreprise pour gérer les hommes et les budgets en appliquant les méthodes de communication et de management adaptées

- Communiquer à l'oral et à l'écrit en anglais pour encadrer des équipes multiculturelles
- Exercer son leadership de manière à favoriser la transition numérique et la sécurisation des SI
- Coconstruire les objectifs avec les équipes à l'intérieur du budget alloué pour la cybersécurité
- Fédérer et motiver des équipes pluridisciplinaires : réseau, logiciels, utilisateurs...
- Elaborer et expliciter la partie du budget consacré à la cyber sécurité
- Récompenser l'engagement et l'efficacité dans le travail réalisé par les équipes

Analyser les systèmes et réseaux informatiques pour établir un diagnostic cyber sécuritaire en mobilisant les outils et méthodes de détection et d'audit

- Identifier, caractériser et cartographier les vulnérabilités et les risques inhérents à un SI
- Conduire des audits de sécurité en analysant les procédures et les processus de défense
- Effectuer des tests de pénétration (pentests) pour vérifier la robustesse des dispositifs défensifs
- Etablir un diagnostic global et préconiser des évolutions
- Proposer des solutions innovantes pour déjouer les cyber attaques

Piloter des projets complexes en France ou à l'international pour améliorer la protection des SI contre les cyberattaques en appliquant les méthodes de gestion de projets

- Identifier les parties prenantes d'un projet lié à la cybersécurité : commanditaire, usagers, fournisseurs...
- Définir les contours et les objectifs du projet pour la partie cybersécurité
- Établir un cahier des charges fonctionnel et technique en français et en anglais
- Définir les livrables en spécifiant les coûts, le niveau de qualité attendu, et les délais
- Mobiliser les outils, les méthodes et les indicateurs de performance pour conduire le projet
- Produire des livrables tels qu'attendus par le commanditaire du projet

Développer des solutions logicielles sécurisées en mobilisant les mathématiques et l'algorithmie

- Superviser le développement ou développer des logiciels sécurisés

- Adapter les applications logicielles et systèmes d'exploitation existants face aux nouvelles menaces
- Exécuter le cahier des charges d'un développement logiciel pour la sécurisation du SI
- Tester la sécurité d'une nouvelle application face à des attaques concrètes simulées (Pentests)
- Documenter et accompagner l'utilisateur dans le maniement d'un nouvel outil logiciel de cyber sécurité

Optimiser l'anticipation et la gestion des incidents ou des crises de sécurité en mobilisant les méthodes de gestion des risques et les outils novateurs

- Elaborer des procédures et processus de réponse à des incidents de sécurité
- Gérer en équipe pluridisciplinaire et en temps réel une cyberattaque
- Concevoir et mettre en place des solutions de détection d'incidents à base d'IA
- Exploiter l'IA pour analyser des données massives liés à des incidents de sécurité (Forensic)
- Capitaliser sur l'expérience de crise pour améliorer le système de sécurité du SI

Blocs de compétences

RNCP40947BC01 — Elaborer et mettre en œuvre une politique de sécurité des systèmes d'information en mobilisant les outils d'analyse et en utilisant les contraintes juridiques

LISTE DE COMPÉTENCES

- Sensibiliser les directeurs et les collaborateurs aux enjeux et aux menaces cyber sécuritaires
- Participer à la définition des principes et des objectifs en termes de sécurité d'un système d'information
- Définir la stratégie cyber sécuritaire d'un Système d'informations (SI)
- Concevoir l'organisation ou la réorganisation de la sécurité d'un SI
- Intégrer les aspects juridiques et réglementaires liés au traitement, au stockage et à la protection des données

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale
2. Examens sur table
3. Mises en situations professionnelles reconstituées

RNCP40947BC02 — Prendre en compte les objectifs de développement durable et la responsabilité sociétale des entreprises pour concevoir et maintenir en opération un dispositif de protection des systèmes d'information efficient en mobilisant les bonnes pratiques environnementales et techniques

LISTE DE COMPÉTENCES

- Concevoir des architectures matérielles et logicielles sécurisées et optimisées du point de vue de leur consommation énergétique
- Maintenir un niveau d'équipements et de logiciels en phase avec les nouvelles technologies de cyberdéfense
- Gérer l'obsolescence des équipements et des composants en privilégiant la circularité
- Favoriser au sein des équipes internes et externes, l'adoption de règles de stockage et de traitement durables des données
- Adopter une conduite des opérations de type inclusive efficiente et éthique
- Garantir l'accès aux données informatiques pour les collaborateurs en situation de handicap selon le RGAA

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale
2. Élaboration d'une monographie écrite
3. Mises en situations professionnelles reconstituées.

RNCP40947BC03 — Intégrer le fonctionnement et la culture d'une entreprise pour gérer les hommes et les budgets en appliquant les méthodes de communication et de management adaptées

LISTE DE COMPÉTENCES

- Communiquer à l'oral et à l'écrit en anglais pour encadrer des équipes multiculturelles
- Exercer son leadership de manière à favoriser la transition numérique et la sécurisation des SI
- Coconstruire les objectifs avec les équipes à l'intérieur du budget alloué pour la cybersécurité
- Fédérer et motiver des équipes

pluridisciplinaires : réseau, logiciels, utilisateurs...

- Elaborer et expliciter la partie du budget consacré à la cyber sécurité
- Récompenser l'engagement et l'efficience dans le travail réalisé par les équipes

MODALITÉS D'ÉVALUATION

1. Conduite de Projets
2. Mises en situations professionnelles reconstituées.
3. Projet de fin d'études

RNCP40947BC04 — Analyser les systèmes et réseaux informatiques pour établir un diagnostic cyber sécuritaire en mobilisant les outils et méthodes de détection et d'audit

LISTE DE COMPÉTENCES

- Identifier, caractériser et cartographier les vulnérabilités et les risques inhérents à un SI
- Conduire des audits de sécurité en analysant les procédures et les processus de défense
- Effectuer des tests de pénétration (pentests) pour vérifier la robustesse des dispositifs défensifs
- Établir un diagnostic global et préconiser des évolutions
- Proposer des solutions innovantes pour déjouer les cyber attaques

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale
2. Conduite de Projets
3. Mises en situations professionnelles reconstituées

RNCP40947BC05 — Piloter des projets complexes en France ou à l'international pour améliorer la protection des SI contre les cyberattaques en appliquant les méthodes de gestion de projets

LISTE DE COMPÉTENCES

- Identifier les parties prenantes d'un projet lié à la cybersécurité : commanditaire, usagers, fournisseurs...
- Définir les contours et les objectifs du projet pour la partie cybersécurité
- Établir un cahier des charges fonctionnel et technique en français et en anglais
- Définir les livrables en spécifiant les coûts, le niveau de qualité attendu, et les délais
- Mobiliser les outils, les méthodes et les indicateurs de performance pour conduire le projet
- Produire des livrables tels qu'attendus par le commanditaire du projet

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale
2. Conduite de projets
3. Mises en situations professionnelles reconstituées

RNCP40947BC06 — Développer des solutions logicielles sécurisées en mobilisant les mathématiques et l'algorithmie

LISTE DE COMPÉTENCES

- Superviser le développement ou développer des logiciels sécurisés
- Adapter les applications logicielles et systèmes d'exploitation existants face aux nouvelles menaces
- Exécuter le cahier des charges d'un développement logiciel pour la sécurisation du SI
- Tester la sécurité d'une nouvelle application face à des attaques concrètes simulées (Pentests)
- Documenter et accompagner l'utilisateur dans le maniement d'un nouvel outil logiciel de cyber sécurité

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale
2. Conduite de Projets
3. Mises en situations professionnelles reconstituées

RNCP40947BC07 — Optimiser l'anticipation et la gestion des incidents ou des crises de sécurité en mobilisant les méthodes de gestion des risques et les outils novateurs

LISTE DE COMPÉTENCES

- Elaborer des procédures et processus de réponse à des incidents de sécurité
- Gérer en équipe pluridisciplinaire et en temps réel une cyberattaque
- Concevoir et mettre en place des solutions de détection d'incidents à base d'IA
- Exploiter l'IA pour analyser des données massives liés à des incidents de sécurité (Forensic)
- Capitaliser sur l'expérience de crise pour améliorer le système de sécurité du SI

MODALITÉS D'ÉVALUATION

1. Etude de cas avec présentation orale

2. Examens sur table
3. Mises en situations professionnelles reconstituées

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les ingénieurs diplômés de l'Ecole d'ingénieurs de l'université spécialité Cybersécurité exercent leur activité dans le cadre d'entreprises issues des secteurs suivants :

- Les sociétés de service Informatique (ESN),
- Les sociétés de conseil en organisation et en management
- Les entreprises industrielles quel que soit le secteur
- Les grandes administrations et services de l'Etat
- Les collectivités territoriales
- Les entreprises spécialisées e-commerce et e-services

TYPE D'EMPLOIS ACCESSIBLES

POG : pilotage, organisation et gestion des risques

- Responsable de la sécurité des systèmes d'information (RSSI)
- Correspondant sécurité
- Spécialiste en gestion de crise Cyber
- Responsable du plan de continuité d'activité (RPCA)

MPC : management de projets et cycle de vie

- Chef de projet sécurité
- Développeur de sécurité
- Architecte de sécurité
- Intégrateur de sécurité

OMCO : opération et maintien en condition opérationnelle

- Administrateur sécurité

SGL : support et gestion des incidents

- Analyste SOC
- Expert réponse à incident (CERT)

CAE : conseil, audit, expertise

- Consultant sécurité « organisationnel »
- Consultant sécurité « technique »
- Cryptologue
- Juriste spécialisé en cybersécurité
- Évaluateur sécurité
- Analyste de la menace
- Délégué à la Protection des Données (DPD)

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)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % 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) M2X91 — Chefs de projet et directeurs de service 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)	16 497
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 M2X91 — Chefs de projet et directeurs de service 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

Prérequis pour l'accès en 1ère année du cycle ingénieur :

- Admission sur concours nationaux des grandes écoles avec un niveau 5 ou niveau supérieur
- Admission sur dossier en justifiant d'un titre de niveau 5 ou niveau supérieur

Prérequis pour l'accès en 2ème année du cycle ingénieur :

Admission sur dossier en justifiant d'un titre de niveau 6 ou niveau supérieur

PRÉREQUIS À LA VALIDATION

- Validation d'un niveau B2 en Anglais, attesté par un organisme tiers
- Réalisation d'une mobilité à l'international d'une période d'au moins 9 semaines

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE

La direction, des représentants de l'équipe pédagogique et des représentants du milieu professionnel.

COMPOSITION DU JURY — VAE

Deux rapporteurs nommés par l'école et instruction du dossier menée par le jury VAE de l'établissement.

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	10 134 €
Selon la branche	7 500 € – 10 952 €
Prise en charge	Branches concernées
10 134 €	Valeur par défaut · 189 branches
10 952 €	CPNE Casinos, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEF de la Publicité

10 000 €	CPNE des industries de santé (CPNEIS), CPNEFP de l'enseignement privé indépendant, CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 500 €	CPNEFP de la Mutualité Sociale Agricole, CPNEFP de la métallurgie
10 514 €	CPNE Travail Temporaire
10 268 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
9 992 €	CPNEFP Mutualité
9 800 €	CPNEFP des industries électriques et gazières
9 000 €	CNPE des sociétés financières
8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 000 €	CPNE chimie
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
7 500 €	CPNE de l'ingénierie, des services informatiques et du conseil

Base légale

Date d'échéance de l'enregistrement 31/08/2030

Date de dernière délivrance possible 31/08/2034

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP39312

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://eijv.u-picardie.fr>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40947/>