

Ingénieur diplômé de Télécom Nancy de l'université de Lorraine, spécialité cybersécurité

RNCP40421 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31045, 15099, 32062, 31057, 24252
Code(s) ROME	M1802, M1803, M1804, M1805, M1806
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2026

Certificateur(s)

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

UNIVERSITE DE LORRAINE · SIRET : 13001550600012

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation et 1 à former.

Organisme	SIRET	Habilitation
ASS APPRENTISSAGE INDUSTRIEL	34958609900021	Former
INST DES TECH INGENIEUR INDUSTRIEL LORRAINE	38418538500026	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La hausse constante des menaces informatiques (espionnage, sabotage, demande de rançons) auxquelles sont confrontées les entreprises a provoqué une pénurie d'experts dans le secteur de la cybersécurité. D'après une étude menée par l'APEC, les besoins de cadres dans le domaine n'ont jamais été aussi élevés, avec un volume d'offres d'emploi cadre exigeant des compétences dans le champ de la cybersécurité qui a presque doublé en 5 ans, et des entreprises qui peinent à recruter.

Le développement de l'Internet et de ses nouvelles formes (objets connectés, cloud, datacenter, réseaux logiciels...) facilite la conception et le déploiement de systèmes informatiques toujours plus élaborés et interconnectés. Cependant, ces systèmes sont aussi plus difficiles à protéger de par leur complexité, de par leur dynamique, et de par leur exposition croissante à des attaques de plus en plus sophistiquées (par exemple, en s'appuyant sur l'intelligence artificielle pour être davantage furtives).

TELECOM Nancy, école d'ingénieur en informatique et sciences du numérique, forte de son expertise en cybersécurité depuis plus de 10 ans, propose, en partenariat avec l'ITII Lorraine, un diplôme d'ingénieur du numérique de spécialité cybersécurité. Elle dispose, par ailleurs, d'une plateforme d'entraînement à la cybersécurité de tout premier plan, composée de deux cyber-ranges professionnels (Diateam, Airbus), et de trois salles dédiées (salle blue team, salle red team, salle serveurs), qui permettent de placer les apprenants en immersion face à des situations réalistes (gestion de crise cyber).

Les candidats à cette certification à TELECOM Nancy deviendront des ingénieurs rapidement opérationnels, qui

disposent de solides fondamentaux scientifiques, d'une expertise technique poussée en cybersécurité, et de compétences interpersonnelles fortes nécessaires dans un contexte pluridisciplinaire et multiculturel.

ACTIVITÉS VISÉES

Le titre d'ingénieur diplômé, conférant le grade de master, permet au titulaire de ce diplôme d'exercer les activités suivantes :

- Conception et intégration de solutions sécurisées : il contribue au choix et conçoit l'architecture de la solution sécurisée et en assure l'assemblage au sein du système d'informations. Il intègre dans l'environnement de production la solution sécurisée et en assure le déploiement. Il peut également assurer l'exploitation et le maintien en conditions opérationnelles dans la durée à travers la fourniture d'un service de sécurité managé.
- Pilotage de projets de sécurité : il définit, met en œuvre et conduit des projets de déploiement de solutions et d'outils de sécurité, en lien avec les objectifs de sécurité fixés par l'organisation. Il définit des politiques de sécurité et assure la mise en œuvre de celles-ci conformément aux normes et réglementations en vigueur.
- Réalisation d'expertises techniques : il apporte une expertise sur la sécurité d'un domaine technique particulier (système, réseau, composants industriels, IoT, intelligence artificielle). Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte et intervient directement sur tout ou partie d'un projet qui relève de son domaine d'expertise, que ce soit dans les phases d'étude, de mise en œuvre ou de maintien en conditions de sécurité.
- Prestation de services en conseil :

Il propose, à partir d'un diagnostic, des solutions, méthodes, outils qui répondent aux enjeux posés. Il mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne. Il anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché. Il contribue à la définition de la stratégie de cybersécurité de l'organisation et à la mise en œuvre des solutions de cybersécurité. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

- Analyse et réponse aux incidents de sécurité : en cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, il répond aux incidents de sécurité, analyse les symptômes et réalise les analyses techniques sur le système d'information. Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.

COMPÉTENCES ATTESTÉES

L'ingénieur diplômé de Télécom Nancy spécialisé en cybersécurité dispose des compétences attestées suivantes :

- concevoir, développer et gérer des infrastructures réseau et leurs services,
- planifier et opérer des architectures et systèmes connectés de grande taille dans le cyberespace,
- développer et / ou intégrer des ressources fournies sur le cyberespace pour construire de nouveaux services,
- anticiper et analyser les principales menaces, vulnérabilités et attaques liées au cyberespace,
- assurer la sécurité et la résilience des services, des informations et des échanges,
- spécifier une politique de sécurité et contribuer à sa mise en œuvre dans des architectures nouvelles ou existantes,
- prévenir et détecter les attaques relatives aux services et à leurs ressources,
- déployer et configurer les mécanismes et outils de protection usuels et d'analyse post-mortem,
- mener des activités de veille technologique au regard des nouvelles menaces,
- mobiliser les ressources d'un large champ de sciences fondamentales,
- exploiter le champ scientifique et technique de disciplines du numérique,
- concevoir, réaliser et piloter un projet informatique d'envergure en maîtrise d'ouvrage et en maîtrise d'œuvre,
- mettre en œuvre les méthodes et les outils de l'ingénieur,
- s'intégrer dans une organisation, l'animer et la faire évoluer,
- prendre en compte des enjeux industriels, économiques et professionnels,
- travailler en équipe et dans un contexte international,
- respecter les valeurs humaines et sociétales.

Blocs de compétences

RNCP40421BC01 — Assurer le management opérationnel pour la sécurité des systèmes d'information dans un contexte pluridisciplinaire et international

LISTE DE COMPÉTENCES

- manager des ressources et des équipes pluridisciplinaires et internationales : procédures, données, moyens humains et matériels, dimensions commerciale, budgétaire et comptable
- mettre en oeuvre la gouvernance, les normes, et les standards spécifiques au domaine de la cybersécurité et du numérique
- anticiper et gérer les risques en intégrant les aspects législatif, juridique, réglementaire et normatif (propriété intellectuelle, protection des données, souveraineté numérique, crise cyber, cybercriminalité, ...)
- mettre en oeuvre une démarche qualité (plan, assurance qualité, sûreté, sécurité)
- spécifier une politique de sécurité et assurer sa mise en oeuvre au sein d'une organisation
- modéliser, concevoir et optimiser des systèmes d'informations résilients
- animer des réunions : utiliser, produire et communiquer l'information (recherche, technique d'expression, de présentation...) selon son niveau de confidentialité
- intégrer la dimension humaine, sociale et éthique de l'entreprise dans son activité
- négocier avec des partenaires et fournisseurs, et garantir la chaîne d'approvisionnement
- s'intégrer dans une organisation ou une équipe, l'animer, la faire évoluer et gérer les conflits
- exploiter les fondamentaux des principaux domaines de la cybersécurité et du numérique, diffuser une culture cybersécurité au sein de l'organisation

MODALITÉS D'ÉVALUATION

- Travaux écrits
- Etude de cas
- Présentation orale devant le jury
- Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP40421BC02 — Conduire des projets complexes en matière de cybersécurité de manière agile

LISTE DE COMPÉTENCES

- concevoir, réaliser et piloter un projet cyber d'envergure en maîtrise d'ouvrage
- concevoir, réaliser et piloter un projet cyber d'envergure en maîtrise d'œuvre
- utiliser les méthodes et outils de l'ingénieur pour un projet cyber
- évaluer le panorama des offres de cybersécurité du marché et formuler des solutions
- prendre en compte la sécurité pour des architectures nouvelles ou existantes
- intégrer des technologies de sécurité et les outils associés au sein d'un projet
- mettre en oeuvre la sécurité de systèmes dans le cadre d'un projet
- mettre en oeuvre la sécurité de réseaux et protocoles dans le cadre d'un projet

MODALITÉS D'ÉVALUATION

- Travaux écrits
- Etude de cas
- Présentation orale devant le jury
- Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP40421BC03 — Produire des composants logiciels et des services informatiques résilients

LISTE DE COMPÉTENCES

- analyser et formaliser les besoins en traitement de l'information et évaluer les ressources requises
- concevoir et développer un produit ou service informatique résilient en utilisant les méthodes, techniques et bonnes pratiques de développement
- spécifier formellement et vérifier des propriétés d'un protocole, produit ou service informatique
- assurer le déploiement et la maintenance d'un produit ou service informatique
- mettre en oeuvre les normes et procédures de développement sécurisé
- utiliser les architectures, protocoles, et technologies des systèmes et réseaux (cloud, internet des objets, ...)
- assurer la configuration et la supervision d'un système informatique (système d'exploitation, services et objets connectés, ...)
- mesurer les performances d'un produit ou service informatique (indicateurs, outils, méthodes)

MODALITÉS D'ÉVALUATION

- Travaux écrits
- Etude de cas
- Présentation orale devant le jury
- Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP40421BC04 — Evaluer et maintenir la sécurité des systèmes d'information

LISTE DE COMPÉTENCES

- identifier et contrer les menaces de cybersécurité
- détecter et corriger les vulnérabilités des environnements informatiques
- exploiter les techniques d'attaques et d'intrusions de manière éthique
- analyser des flux réseaux à des fins de sécurité
- utiliser les outils d'analyse et procédures légales d'analyse post-mortem
- réaliser une veille technologique cybersécurité avec étude des tendances
- configurer les outils et les environnements de cybersécurité
- formuler des propositions innovantes pour répondre à des menaces cyber

MODALITÉS D'ÉVALUATION

- Travaux écrits
- Etude de cas
- Présentation orale devant le jury
- Mise en situation professionnelle dans le cadre des périodes en entreprise

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Services aux entreprises (conseil-projet-développement), Informatique (éditeurs de logiciels, constructeurs, systèmes et réseaux, opérateurs de réseaux, d'infrastructures numériques et de services), Industrie, Banques, Assurances, Administrations, Enseignement/Recherche.

TYPE D'EMPLOIS ACCESSIBLES

Spécialiste sécurité d'un domaine technique, Intégrateur de solutions de sécurité, Responsable de projet de sécurité, Consultant en cybersécurité, Analyste réponse aux incidents de sécurité, Architecte sécurité, Responsable sécurité des systèmes d'information, Chef de projet TIC, Ingénieur logiciel, Maître d'ouvrage, Ingénieur développement, Ingénieur R&D, Architecte infrastructures informatiques, Architecte logiciel, Administrateur systèmes, réseaux et services, Ingénieur de production (datacenter, cloud, ...).

Le titre d'ingénieur diplômé, conférant le grade de master, permet au titulaire de ce diplôme d'exercer les activités (ou fonctions) suivantes :

- Spécialiste sécurité d'un domaine technique,
- Intégrateur de solutions de sécurité,
- Responsable de projet de sécurité,
- Consultant en cybersécurité,
- Analyste réponse aux incidents de sécurité,
- Expert en tests d'intrusion,
- Responsable de la sécurité des systèmes d'information.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agréés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 892 €

Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'un titre ou diplôme de niveau 5 ou 6 (informatique, mathématiques, sciences du numérique, cybersécurité ou domaine connexe) ou équivalent (diplôme étranger) ou d'une expérience professionnelle équivalente.

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE

Les membres du jury de diplôme sont nommés par la Présidence de l'Université de Lorraine

Les jurys de semestre (validation des UE), d'année (passage en année supérieure) et de diplôme sont composés à 50% d'enseignants de l'école et à 50% de professionnels extérieurs en activité dont la liste est validée par le Conseil de la Formation de l'Université de Lorraine et le Centre de Formation des Apprentis de l'Industrie.

Les jurys de semestre et d'année sont composés a minima de 3 enseignants dont la/le responsable TELECOM Nancy de l'alternance et d'1 représentant du CFA partenaire (ITII).

Le jury de diplôme est

composé a minima de 3 enseignants-chercheurs (la Direction de l'Ecole qui préside le jury, la Direction des Etudes, la/le responsable TELECOM Nancy de l'alternance) et d'1 représentant du CFA partenaire (ITII).

COMPOSITION DU JURY — VAE

Le jury VAE est désigné par la Présidence de l'Université de Lorraine sur proposition de la Direction de l'Ecole. Il est composé a minima de 3 enseignants-chercheurs (parmi lesquels est désigné la Présidence du jury) et de personnes (à raison d'au moins un quart) ayant une activité principale autre que l'enseignement et compétentes pour apprécier la nature des acquis, notamment professionnels. Il est complété par des membres consultatifs : référent VAE et accompagnateur VAE (si celui-ci n'est pas membre du jury).

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	10 257 €
Selon la branche	7 700 € – 10 952 €
Prise en charge	Branches concernées
10 257 €	Valeur par défaut · 191 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
9 992 €	CPNEFP Mutualité
9 800 €	CPNEFP des industries électriques et gazières
9 556 €	CPNEFP du Négoce de l'ameublement
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

Base légale

Date d'échéance de l'enregistrement	31/08/2026
Date de dernière délivrance possible	31/08/2026

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42803

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Contact :

contact@telecomnancy.eu

etudes@telecomnancy.eu

Université de Lorraine ()

TELECOM Nancy ()

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40421/>