

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

RNCP42803 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31045, 32062, 32154, 73054
Code(s) ROME	M1802, M1803, M1804, M1805, M1806
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
UNIVERSITE DE LORRAINE · SIRET : 13001550600012

Partenaires habilités

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

Organisme	SIRET	Habilitation
INST DES TECH INGENIEUR INDUSTR LORRAINE	38418538500026	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La multiplication et la sophistication des attaques informatiques (espionnage, sabotage, rançongiciels) placent les organisations devant un besoin durable de compétences en cybersécurité que le marché du travail ne parvient pas à satisfaire. L'Observatoire des métiers de la cybersécurité (ANSSI, DGEFP, Afpa), dans son enquête 2025, a recensé plus de 23 000 offres d'emploi publiées en France dans ce domaine entre juin 2023 et juin 2024, dans un contexte de difficultés persistantes de recrutement sur les profils qualifiés. Ce besoin est renforcé par l'extension du cadre réglementaire européen (directive NIS 2, règlement DORA, règlement sur la cyberrésilience) qui soumet des milliers d'entités à des obligations de gouvernance de la sécurité, de gestion des risques et de notification des incidents. Ces besoins portent sur des systèmes d'information dont la sécurisation est rendue plus difficile par leur complexité et leur exposition croissantes : informatique en nuage, objets connectés, réseaux logiciels, chaînes d'approvisionnement logicielles, systèmes industriels. Les attaques y sont elles-mêmes plus élaborées, notamment par le recours à l'intelligence artificielle pour en accroître la furtivité. Les organisations recherchent en conséquence des ingénieurs capables d'intervenir sur l'ensemble du cycle de vie de la sécurité d'un système d'information, et non sur un seul de ses volets : concevoir et intégrer des solutions sécurisées, piloter des projets de sécurité, produire des composants logiciels et des services résilients, conduire des expertises techniques, évaluer et maintenir la sécurité en conditions opérationnelles, analyser et traiter les incidents de sécurité. Ces activités s'exercent dans des environnements pluridisciplinaires et internationaux, sous contrainte réglementaire et budgétaire ; elles supposent donc, outre l'expertise technique, la maîtrise du management opérationnel de la sécurité, de la conduite de projet et de la communication auprès d'interlocuteurs non spécialistes. La certification atteste la maîtrise de ces compétences. Elle correspond au titre d'ingénieur diplômé de Télécom

Nancy de l'université de Lorraine, spécialité cybersécurité, délivré sous accréditation de la Commission des titres d'ingénieur. Elle est structurée en quatre blocs (management opérationnel de la sécurité des systèmes d'information, conduite de projets complexes de cybersécurité, production de composants logiciels et de services informatiques résilients, évaluation et maintien de la sécurité des systèmes d'information) dont la validation intégrale est requise pour son obtention.

ACTIVITÉS VISÉES

Le titulaire de la présente certification, titre d'ingénieur diplômé conférant le grade de master, exerce les activités suivantes :

- Management opérationnel de la sécurité des systèmes d'information : il manage des ressources et des équipes pluridisciplinaires et internationales, dans leurs dimensions humaine, matérielle, budgétaire et contractuelle, et négocie avec les partenaires et fournisseurs en garantissant la chaîne d'approvisionnement. Il met en œuvre la gouvernance, les normes et les standards de la cybersécurité, spécifie la politique de sécurité de l'organisation et assure sa mise en œuvre. Il anticipe et gère les risques en intégrant les aspects législatif, juridique, réglementaire et normatif (protection des données, propriété intellectuelle, souveraineté numérique, cybercriminalité) et conduit la gestion de la crise cyber. Il diffuse la culture de cybersécurité au sein de l'organisation et communique l'information selon son niveau de confidentialité.
- 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'information. Il intègre la solution sécurisée dans l'environnement de production et en assure le déploiement. Il peut également assurer son exploitation et son 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 leur mise en œuvre 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, objets connectés, intelligence artificielle). Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, et intervient sur tout ou partie d'un projet relevant de son domaine d'expertise, dans les phases d'étude, de mise en œuvre ou de maintien en conditions de sécurité.
- Conseil en cybersécurité : il propose, à partir d'un diagnostic, des solutions, méthodes et outils répondant aux enjeux posés, en mobilisant son expertise ainsi que des outils développés en interne. Il anticipe les évolutions du contexte de cybersécurité et 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 correspondantes, sur des sujets tant méthodologiques que techniques.
- Analyse et réponse aux incidents de sécurité : il répond aux incidents de sécurité en cas de soupçon d'activité malveillante ou d'attaque au sein du système d'information. Il analyse les symptômes et réalise les analyses techniques sur le système d'information, identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation en vue de l'assainissement et du durcissement des systèmes attaqués.

COMPÉTENCES ATTESTÉES

Le titulaire de la présente certification dispose des compétences attestées suivantes, organisées selon les quatre blocs de compétences dont la validation intégrale est requise pour l'obtention de la certification.

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

- manager des ressources et des équipes pluridisciplinaires et internationales : procédures, données, moyens humains et matériels, dimensions commerciale, budgétaire et comptable
- mettre en œuvre 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 œuvre une démarche qualité (plan, assurance qualité, sûreté, sécurité)
- spécifier une politique de sécurité et assurer sa mise en œuvre au sein d'une organisation
- modéliser, concevoir et optimiser des systèmes d'information 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

Conduire des projets complexes en matière de cybersécurité de manière agile

- 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 œuvre la sécurité de systèmes dans le cadre d'un projet
- mettre en œuvre la sécurité de réseaux et protocoles dans le cadre d'un projet

Produire des composants logiciels et des services informatiques résilients

- 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 œuvre 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)

Évaluer et maintenir la sécurité des systèmes d'information

- 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 réseau 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

Blocs de compétences

RNCP42803BC01 — 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 œuvre 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 œuvre une démarche qualité (plan, assurance qualité, sûreté, sécurité)

spécifier une politique de sécurité et assurer sa mise en œuvre au sein d'une organisation

modéliser, concevoir et optimiser des systèmes d'information 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

Étude de cas

Présentation orale devant le jury

Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP42803BC02 — 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 œuvre la sécurité de systèmes dans le cadre d'un projet

mettre en œuvre la sécurité de réseaux et protocoles dans le cadre d'un projet

MODALITÉS D'ÉVALUATION

Travaux écrits

Étude de cas

Présentation orale devant le jury

Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP42803BC03 — 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 œuvre 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

Étude de cas

Présentation orale devant le jury

Mise en situation professionnelle dans le cadre des périodes en entreprise

RNCP42803BC04 — Évaluer 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 réseau 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

Étude de cas

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, agrégés 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, Formation continue, Apprentissage, Contrat de professionnalisation, 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.

PRÉREQUIS À LA VALIDATION

Quelle que soit la voie d'accès, la validation de la certification requiert un niveau B2 du Cadre européen commun de référence pour les langues (CECRL) en langue anglaise, attesté par une certification indépendante.

L'exigence d'expérience internationale est différenciée selon la voie d'accès :

- après un parcours de formation sous statut d'élève ou d'étudiant, en contrat d'apprentissage ou en contrat de professionnalisation : justifier d'une mobilité internationale d'une durée supérieure ou égale à 12 semaines, effectuée à l'étranger dans un cadre académique ou professionnel (mission professionnelle, stage ou échange académique) ;
- après un parcours de formation continue ou par expérience (validation des acquis de l'expérience) : justifier d'une expérience professionnelle à dimension internationale, dont le jury apprécie la nature et la durée au regard des compétences visées.

COMPOSITION DU JURY — FORMATION INITIALE

Les membres du jury de diplôme sont nommés par la Présidence de l'Université de Lorraine après validation par le Conseil de la Formation de l'Université de Lorraine. Le jury est composé a minima de 2 enseignants-chercheurs (dont la Direction de l'École qui préside le jury, la Direction des études), et est complété par a minima par 5 des enseignants et enseignants-chercheurs de l'école.

COMPOSITION DU JURY — FORMATION CONTINUE, CONTRAT DE PROFESSIONNALISATION

Les membres du jury de diplôme sont nommés par la Présidence de l'Université de Lorraine après validation par le Conseil de la Formation de l'Université de Lorraine.

Le jury est composé a minima de 2 enseignants-chercheurs (dont la Direction de l'École qui préside le jury, la Direction des études), et est complété par a minima par 5 des enseignants et enseignants-chercheurs de l'école.

COMPOSITION DU JURY — APPRENTISSAGE

Les membres du jury de diplôme sont nommés par la Présidence de l'Université de Lorraine après validation par le Conseil de la Formation de l'Université de Lorraine.

Le jury est composé a minima de 3 enseignants-chercheurs (dont la Direction de l'École qui préside le jury, la Direction des études et le responsable de l'alternance à Télécom Nancy), d'un représentant du CFA partenaire.

COMPOSITION DU JURY — VAE

Le jury VAE est désigné par la Présidence de l'Université de Lorraine sur proposition de la Direction de l'École.

La composition du jury est définie par le Code de l'éducation : article L613-4 modifié par la loi n°2016-1088 du 8 août 2016 - art. 78.

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

Base légale

Date d'échéance de l'enregistrement	31/08/2028
Date de dernière délivrance possible	31/08/2028

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP40421

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

TELECOM Nancy ()

Université de Lorraine ()

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42803/>