

Ingénieur diplômé de CentraleSupélec, spécialité Cybersécurité

RNCP41165 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31045, 32062
Code(s) ROME	M1802, M1810, M1805, M1801, 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
CENTRALESUPELEC · SIRET : 13002076100016

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification d'ingénieur CentraleSupélec en Cybersécurité vise à répondre à la forte demande sur les métiers de la cybersécurité, notamment les métiers d'expertise technique identifiés dans le Panorama des métiers de la cybersécurité, élaboré par un groupe de travail composé de représentants de l'enseignement supérieur, du monde industriel et de l'ANSSI (rapport publié en octobre 2020). La plupart des organisations au niveau mondiale sont aujourd'hui touchées par la pénurie des compétences en cybersécurité, alors que le besoin de protection des données et des systèmes face aux attaques informatiques de plus en plus complexes et nombreuses est croissant. Les métiers visés relèvent de la cybersécurité au sens large, notamment la conception et la maintenance de systèmes d'information sécurisés, la gestion des incidents et des crises de sécurité, ainsi que le conseil, les services et la recherche en cybersécurité. La sécurisation d'un composant du système d'information exige souvent une maîtrise approfondie de son fonctionnement, qu'il soit logiciel, matériel, réseau, ou autre. Ainsi, les compétences recherchées reposent sur une solide culture informatique.

Ces ingénieurs allient une connaissance approfondie de leur domaine scientifique et technique avec une ouverture sur les enjeux systémiques dans lesquels celui-ci s'inscrit. Leurs compétences scientifiques et techniques, enrichies par leurs capacités en communication, leur aptitude au travail en équipe dans des milieux culturellement variés et à l'apprentissage continu et autonome, leur permettent d'intégrer de nouvelles problématiques et de prendre des décisions pour des systèmes de plus en plus complexes.

ACTIVITÉS VISÉES

- Analyse et audit de la sécurité d'un système d'information
- Conception et développement de systèmes d'information sécurisés
- Déploiement et administration des solutions de sécurité informatique
- Détection des incidents de sécurité et réponse à ces incidents pour maintenir les conditions de sécurité
- Recherche et innovation en cybersécurité
- Enrichissement, formalisation et transmission des connaissances et savoir-faire de son organisation dans le domaine de la cybersécurité
- Gestion d'un projet et animation d'une équipe technique dans le domaine de la cybersécurité et contribution à l'amélioration de ses pratiques professionnelles

COMPÉTENCES ATTESTÉES

- Réaliser une analyse de risque en cybersécurité sur des systèmes complexes et en déduire une politique de sécurité
- Prendre en compte les aspects éthique, législatif et normatif pour l'audit de sécurité et la mise au point de la politique de sécurité
- Analyser de manière critique le code, la configuration, l'architecture d'un système d'information et évaluer de manière objective son niveau de sécurité
- Réaliser un test intrusif en respectant les contraintes clients
- Mobiliser un large spectre de champs scientifiques et techniques de l'informatique pour réaliser un audit de sécurité
- Restituer les résultats de l'audit, à l'oral et à l'écrit, en français et en anglais en s'adaptant à son auditoire
- Recueillir et analyser le besoin client et rédiger un cahier des charges afin de formaliser les exigences fonctionnelles et non fonctionnelles (notamment de sécurité)
- Concevoir des architectures de sécurité répondant au cahier des charges et aux exigences réglementaires
- Intégrer des principes d'éco-conception des systèmes sécurisés
- Modéliser un système complexe en utilisant des approches semi-formelle et formelles pour le spécifier et vérifier sa sécurité
- Développer et mettre au point des systèmes sécurisés complexes comprenant des composants logiciels et matériels
- Gérer un projet de développement en utilisant les outils et méthodologies adaptés
- Recueillir et analyser le besoin client afin d'identifier les flux d'information légitimes
- Identifier les composants logiciels et matériels à déployer à partir de l'analyse des flux légitimes
- Déployer et configurer de manière sécurisée les composants strictement nécessaires d'un système d'information afin de répondre au besoin du client
- Etablir et mettre en œuvre un plan rigoureux de maintien du système en condition de sécurité
- Mener une veille continue sur les vulnérabilités pouvant affecter les composants d'un système d'information
- Concevoir des architectures de supervision de la sécurité pour détecter et réagir aux intrusions
- Déployer et administrer des systèmes de supervision de la sécurité
- Analyser un système compromis pour répondre aux incidents de sécurité et ramener le système dans un état sain
- Analyser un code malveillant par une démarche de rétroconception afin de proposer des méthodes de détection et de remédiation
- Mener une veille permanente sur la menace en cybersécurité afin de mettre à jour les moyens de détection
- Analyser et synthétiser l'état de l'art scientifique et technologique dans un domaine de la cybersécurité
- Concevoir et développer une approche innovante de cybersécurité par rapport à l'état de l'art, en adoptant une démarche scientifique
- Analyser de façon critique et interpréter des résultats d'expérience et de simulation numériques
- Communiquer des résultats de recherche scientifique en cybersécurité auprès d'un public varié
- Mener une veille scientifique, technique et réglementaire permanente sur la menace en cybersécurité et les contre-mesures de l'état de l'art
- Restituer les résultats et formaliser les retours d'expériences par oral et par écrit en utilisant le français ou l'anglais, dans un but de transfert de connaissance ou de formation
- Mener une analyse introspective de ses connaissances et compétences afin de situer ses domaines d'expertises et ses contributions dans son organisation
- Utiliser, avec pédagogie, des médias adaptés afin d'assurer la transmission des connaissances, la formation en cybersécurité en tenant compte des variétés de contexte géographique, social et culturel
- Gérer un projet de cybersécurité en utilisant les méthodes et les outils adaptés à sa spécificité et au contexte
- Animer le travail collaboratif et motiver des équipes multiculturelles en tenant compte des compétences de chacun et des contraintes matérielles et financières
- Prendre en compte la diversité des collaborateurs, les enjeux sociaux (discrimination, VSS, harcèlement, ...) et veiller à l'intégration de tous.
- Assurer une communication efficace en s'adaptant au public visé et en maîtrisant les techniques de base de communication écrite et orale

Blocs de compétences

RNCP41165BC01 — Analyser et auditer la sécurité d'un système d'information

LISTE DE COMPÉTENCES

- Réaliser une analyse de risque en cybersécurité sur des systèmes complexes et en déduire une politique de sécurité
- Prendre en compte les aspects éthique, législatif et normatif pour l'audit de sécurité et la mise au point de la politique de sécurité
- Analyser de manière critique le code, la configuration, l'architecture d'un système d'information et évaluer de manière objective son niveau de sécurité
- Réaliser un test intrusif en respectant les contraintes clients
- Mobiliser un large spectre de champs scientifiques et techniques de l'informatique pour réaliser un audit de sécurité
- Restituer les résultats de l'audit, à l'oral et à l'écrit, en français et en anglais en s'adaptant à son auditoire

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle (études de cas) portant sur une analyse de risque

- L'évaluation porte sur un rapport écrit d'analyse de risque

Mise en situation professionnelle (challenges techniques) portant sur un audit technique

- L'évaluation porte sur un rapport d'audit et une présentation orale des résultats de l'audit

RNCP41165BC02 — Concevoir et développer un système d'information sécurisé

LISTE DE COMPÉTENCES

- Recueillir et analyser le besoin client et rédiger un cahier des charges afin de formaliser les exigences fonctionnelles et non fonctionnelles (notamment de sécurité)
- Concevoir des architectures de sécurité répondant au cahier des charges et aux exigences réglementaires
- Intégrer des principes d'éco-conception des systèmes sécurisés
- Modéliser un système complexe en utilisant des approches semi-formelle et formelles pour le spécifier et vérifier sa sécurité
- Développer et mettre au point des systèmes sécurisés complexes comprenant des composants logiciels et matériels
- Gérer un projet de développement en utilisant les outils et méthodologies adaptés

MODALITÉS D'ÉVALUATION

Projets de développement

- Evaluation de la production écrite (cahier des charges, rapport)
- Evaluation de la qualité de la réalisation technique (code, circuit numérique) et des tests réalisés
- Evaluation de la gestion du projet lors d'une soutenance orale

Travaux pratiques de conception et modélisation semi-formelle et formelle

- Evaluation de la qualité et la complétude de la modélisation

Travaux pratiques (mini-projets) de développement sécurisé, de conception de circuits matériels, de systèmes d'exploitation et de compilateurs

- Evaluation de la qualité et la complétude des développements sécurisés

RNCP41165BC03 — Déployer et administrer un système d'information sécurisé

LISTE DE COMPÉTENCES

- Recueillir et analyser le besoin client afin d'identifier les flux d'information légitimes
- Identifier les composants logiciels et matériels à déployer à partir de l'analyse des flux légitimes
- Déployer et configurer de manière sécurisée les composants strictement nécessaires d'un système d'information afin de répondre au besoin du client
- Etablir et mettre en œuvre un plan rigoureux de maintien du système en condition de sécurité
- Mener une veille continue sur les vulnérabilités pouvant affecter les composants d'un système d'information

MODALITÉS D'ÉVALUATION

Travaux pratique de sécurisation des OS et des réseaux et des environnements cloud :

- Évaluation des rapports ou des restitutions orales

RNCP41165BC04 — Détecter les incidents de sécurité et réagir pour maintenir les conditions de sécurité

LISTE DE COMPÉTENCES

- Concevoir des architectures de supervision de la sécurité pour détecter et réagir aux intrusions
- Déployer et administrer des systèmes de supervision de la sécurité
- Analyser un système compromis pour répondre aux incidents de sécurité et ramener le système dans un état sain
- Analyser un code malveillant par une démarche de rétroconception afin de proposer des méthodes de détection et de remédiation
- Mener une veille permanente sur la menace en cybersécurité afin de mettre à jour les moyens de détection

MODALITÉS D'ÉVALUATION

Travaux pratique de supervision de sécurité et d'attaques en mémoire :

- Evaluation des rapports ou des restitutions orales

Mise en situation professionnelle (challenges) de rétroconception :

- Evaluation des rapports ou des restitutions orales

RNCP41165BC05 — Mener une activité de recherche et de développement de solutions innovantes en cybersécurité

LISTE DE COMPÉTENCES

- Analyser et synthétiser l'état de l'art scientifique et technologique dans un domaine de la cybersécurité
- Concevoir et développer une approche innovante de cybersécurité par rapport à l'état de l'art, en adoptant une démarche scientifique
- Analyser de façon critique et interpréter des résultats d'expérience et de simulation numériques
- Communiquer des résultats de recherche scientifique en cybersécurité auprès d'un public varié

MODALITÉS D'ÉVALUATION

Projet de recherche ou d'innovation

- Evaluation de la soutenance orale et du rapport
- Evaluation de la qualité et de la complétude du rapport bibliographique

Travaux pratique des ECUE orientées recherche (sécurité matérielle et de protection des contenus)

- Evaluation de la qualité de la présentation de la soutenance des TP
- Evaluation de la qualité de l'analyse critique des résultats et de leur interprétation lors de la restitution orale et écrite

RNCP41165BC06 — Enrichir, formaliser et transmettre les connaissances et savoir-faire de son organisation dans le domaine de la cybersécurité

LISTE DE COMPÉTENCES

- Mener une veille scientifique, technique et réglementaire permanente sur la menace en cybersécurité et les contre-mesures de l'état de l'art
- Restituer les résultats et formaliser les retours d'expériences par oral et par écrit en utilisant le français ou l'anglais, dans un but de transfert de connaissance ou de formation
- Mener une analyse introspective de ses connaissances et compétences afin de situer ses domaines d'expertises et ses contributions dans son organisation
- Utiliser, avec pédagogie, des médias adaptés afin d'assurer la transmission des connaissances, la formation en cybersécurité en tenant compte des variétés de contexte géographique, social et culturel

MODALITÉS D'ÉVALUATION

Exposés de compléments de cours réalisés par groupes d'élèves

- Evaluation de la qualité de la présentation (pédagogie, qualité du support de présentation)
- Evaluation de la complétude et de la pertinence de l'étude et des éléments présentés

Stage de fin d'étude

Missions en entreprises dans le cadre d'un contrat de professionnalisation, projets de recherche ou d'entrepreneuriat

- Evaluation de la qualité de la présentation (pédagogie, qualité du support de présentation)
- Evaluation de la qualité du rapport

RNCP41165BC07 — Gérer un projet de cybersécurité, animer une équipe, contribuer à l'amélioration de ses pratiques professionnelles en gardant un comportement éthique et responsable

LISTE DE COMPÉTENCES

- Gérer un projet de cybersécurité en utilisant les méthodes et les outils adaptés à sa spécificité et au contexte
- Animer le travail collaboratif et motiver des équipes multiculturelles en tenant compte des compétences de chacun et des contraintes matérielles et financières
- Prendre en compte la diversité des collaborateurs, les enjeux sociaux (discrimination, VSS, harcèlement, ...) et veiller à l'intégration de tous.
- Assurer une communication efficace en s'adaptant au public visé et en maîtrisant les techniques de base de communication écrite et orale

MODALITÉS D'ÉVALUATION

Les savoir-faire et savoir-être associés aux compétences sont évalués lors des mises en situation par observation des activités demandées à un élève ou un groupe d'élève?dans différents contextes :

- Projets longs.
- Stage de fin d'étude.
- Missions en entreprises dans le cadre d'un contrat de professionnalisation, projets de recherche ou d'entrepreneuriat

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Activités informatiques et services d'information
- Fabrication d'équipements électriques, électroniques, informatiques
- Activités scientifiques et techniques
- Administration publique, enseignement,
- Recherche-développement scientifique
- Autres activités spécialisées, scientifiques et techniques
- Tous secteurs d'activités nécessitant des experts en cybersécurité, en particulier
 - o Télécommunications
 - o Activités industrielles
 - o Activités financières et d'assurance

TYPE D'EMPLOIS ACCESSIBLES

Expert technique d'un domaine de la cybersécurité

- Cryptologue
- Administrateur de solutions de sécurité
- Auditeur de sécurité technique (intrusion, code, configuration)
- Analyste réponse incident
- Consultant en cybersécurité
- Formateur en cybersécurité
- Évaluateur de la sécurité des technologies de l'information (sécurité des produits)
- Développeur de solution de sécurité
- Intégrateur de solutions de sécurité
- Chercheur en cybersécurité

Après 3 à 5 ans d'expérience :

- Architecte sécurité
- Chef de projet cybersécurité
- Responsable de la Sécurité des Systèmes d'Information

Après obtention d'un Doctorat :

Enseignant-chercheur

Chercheur en cybersécurité

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, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Concours CPGE

Niveau 6 de formation scientifique ou technologique

PRÉREQUIS À LA VALIDATION

Niveau C1 (CECRL) en anglais validé par un test d'un organisme extérieur reconnu par CentraleSupélec

Pour les non anglophones, niveau B2 (CECRL) en FLE validé par un test d'un organisme extérieur reconnu par CentraleSupélec

39 semaines de stages ou expérience professionnelle dont au moins 14 semaines en entreprise

Expérience internationale de 18 semaines minimum

COMPOSITION DU JURY — FORMATION INITIALE, CONTRAT DE PROFESSIONNALISATION

Le jury de diplomation est présidé par le Directeur de CentraleSupélec. Il est composé du directeur des formations, de deux industriels du conseil des études ou du conseil d'administration, des responsables académiques des cursus de spécialité et du directeur des études du cursus généraliste. Il statue à partir des informations élaborées par la commission de diplomation du cursus qui est constituée du directeur des formations, du responsable académique, du

responsable de la scolarité et de quatre enseignants ayant contribué à la formation.

COMPOSITION DU JURY — VAE

Le jury de diplomation est présidé par le Directeur de CentraleSupélec. Il est composé du directeur des formations, de deux industriels du conseil des études ou du conseil d'administration, des responsables académiques des cursus de spécialité et du directeur des études du cursus généraliste. Il statue à partir des informations élaborées par le jury de validation des acquis de l'expérience du cursus composé de représentants académiques et professionnels du domaine de spécialité :

- le responsable académique VAE
- un enseignant chercheur du domaine
- 2 professionnels du domaine

Base légale

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

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

www.centralesupelec.fr

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41165/>