

Sciences et ingénierie - Cybersécurité des objets connectés

RNCP37931 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	110, 255m, 326
Formacode(s)	31045, 24354, 30812, 31042
Code(s) ROME	M1810, H1209, M1805, M1801
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

ESME SUDRIA · SIRET : 44263925800031

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former.

Organisme	SIRET	Habilitation
ASSOCIATION POUR LA FORMATION DES INFORMATIENS PAR L'APRENTISSAGE	3910872100004 6	Former
ECOLE POUR L'INFORMATIQUE ET LES TECHNIQUES AVANCEES (EPITA)	8981920750001 5	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Internet des objets est désormais partout, aussi bien dans les usages grand public (objets connectés) que dans le monde de l'entreprise (capteurs industriels). Le nombre d'objets connectés croît à grande vitesse (de 8 milliards en 2019, à près de 26 milliards en 2025, selon plusieurs études convergentes menées par ANSSI ou l'OCDE). La prolifération des objets connectés et le volume d'informations généré par ces derniers imposent de repenser la capacité de ces systèmes à résister aux risques cyber : le développement d'un monde ultra-connecté offre pour des groupes malveillants de multiples possibilités d'exploiter les défaillances technologiques.

L'internet des objets se déploie aujourd'hui dans de nombreux secteurs comme le transport, les télécommunications, l'énergie, l'industrie ou encore la santé et fait appel aux concepts qui façonnent nos sociétés de demain : Smart Grids, Smart Industries, Smart Cities, Smart Homes... Si la fuite de données génère des craintes, ce n'est, pour autant, pas le seul risque pressenti par l'utilisation d'objets connectés. En effet, tous ces objets directement connectés à un réseau Internet sont ainsi plus vulnérables aux différentes attaques : vol d'informations, prise en main de l'appareil à distance, modification des données et du contenu, etc.

Au regard des performances escomptées de ces objets connectés, la protection des données et de la vie privée, la sûreté de fonctionnement, tout comme la protection des biens et des personnes dans cet environnement ultra connecté et potentiellement hostile, sont désormais indispensables et incontournables.

Cette certification Cybersécurité des objets connectés garantit l'employabilité de cadres intermédiaires, qui vont

intervenir aux niveaux des fondamentaux des technologies utilisées dans la cybersécurité des objets connectés ainsi que sur la façon de les mobiliser dans le cadre de la conception puis du déploiement de ces dispositifs dans un cadre cyber sécuritaire.

ACTIVITÉS VISÉES

Identification des risques de sécurité numérique pouvant atteindre les objets connectés dans leur environnement :

- Développer une vision « Internet des objets » et cybersécurité permettant de fixer et de respecter les objectifs de l'entreprise en collaboration avec les principaux responsables informatiques.
- Identifier l'objectif IoT de l'entreprise et s'assurer que l'architecture IoT répondra efficacement aux besoins actuels et à venir de l'entreprise.
- Détecter les menaces de sécurité potentielles et répertorier les mesures à prendre pour protéger les systèmes IoT dans le respect des réglementations juridiques en vigueur.

Conception des solutions de sécurisation d'un réseau d'objets connectés en conformité avec la politique de sécurité de l'entreprise :

- Rechercher et/ou exploiter des documents techniques en français et en anglais pour proposer des solutions sécuritaires pertinentes.
- Standardiser le processus de création de solutions IoT.
- Concevoir une sécurité dynamique du réseau des IoT répondant aux normes en vigueur.
- Mesurer les risques encourus par les IoT par une veille active pour mesurer les points sensibles.
- Participer et améliorer la veille sur la réglementation de la cybersécurité en utilisant les informations mises à dispositions (articles, plateforme de partage, revue spécialisée,...).

Implémentation de solutions de sécurité numérique dans le cadre du déploiement d'un parc d'objets connectés :

- Implémenter des solutions de sécurité dans le respect : des spécifications d'un cahier des charges en français et /ou anglais ; des standards de Sécurité en vigueur ; des procédures d'assurance qualité.
- Collaborer avec les différentes équipes technologiques opérationnelles, au sein de l'entreprise afin que les solutions s'intègrent parfaitement aux opérations existantes.
- Documenter les solutions mises en œuvre pour assurer les process de conception.
- Déployer des éléments de sécurité (mise à jour, changement de protocoles, ...).

Élaboration et mise en place d'un plan de formation pour former les usagers à appliquer les principes de sécurité numérique d'un parc d'objets connectés :

- Analyser les écarts de compétences des collaborateurs en matière de sécurité.
- Élaborer un plan de formation adapté aux situations professionnelles des collaborateurs.
- S'assurer que les collaborateurs en situation de handicap auront accès à des aménagements adaptés afin de bien suivre la formation.
- Sélectionner un organisme de formation répondant aux besoins.
- Accompagner les utilisateurs à la détection de faille de cybersécurité sur un parc.

Maintenance des outils de sécurité des objets connectés :

- Élaborer et planifier un programme de maintenance avec les parties prenantes.
- Maintenir le niveau de sécurité à l'aide des tests réguliers et une surveillance soutenue.
- Assurer le support client dans le cadre d'un service de maintenance.
- Rédiger des rapports en conformité avec la réglementation.
- Suivre les plans de maintenance curative et préventive.

Encadrement d'une équipe dans l'environnement professionnel de la cybersécurité des objets connectés :

- Définir et suivre les objectifs de projet (méthodes et outils) en prenant en compte l'environnement professionnel.
- Planifier les activités et les ressources du projet en s'assurant que les collaborateurs en situation de handicap aient accès à des outils de travail adaptés afin de mener à bien leurs missions.
- Veiller à la sécurité personnelle.
- Organiser, coordonner et animer une équipe projet pour assurer le suivi des objectifs en tenant compte de sa diversité (culturelle, situation de handicap, etc) afin de mobiliser tous les membres.

COMPÉTENCES ATTESTÉES

- Identifier la nature de l'objet connecté en analysant l'environnement
- Identifier les risques d'intrusions dans un système connecté
- Détecter, classer et caractériser les risques de sécurité
- Répertorier les mesures à prendre pour protéger les systèmes
- Effectuer une veille et appliquer les différents standards de sécurité

- Sécuriser un objet en sélectionnant des solutions
- Concevoir et appliquer une sécurité de manière dynamique
- Exploiter les documents techniques en version française et anglaise
- Implémenter les solutions
- Analyser un cahier des charges en français et /ou anglais
- Gérer à distance le dispositif en s'appuyant sur des standards
- Appliquer les procédures d'assurance qualité
- Rédiger la documentation fonctionnelle et technique
- Elaborer les process des solutions de sécurité implémentées
- Définir un plan de formation pour les usagers et sélectionner les organismes
- Planifier les mises à jour logicielle et gérer des solutions logicielles correctives
- Évaluer la progression et la nature des risques sur un réseau en exploitation
- Proposer un plan de maintenance
- Définir des objectifs de projet, apporter des corrections de trajectoire
- Travailler avec les équipes en prenant en compte leur diversité (culturelle, situation de handicap, etc)
- Animer des réunions d'équipe en utilisant des outils de communication en langue française ou anglaise

Blocs de compétences

RNCP37931BC01 — Identification des risques de sécurité numérique pouvant atteindre les objets connectés dans leur environnement

LISTE DE COMPÉTENCES

1. Identifier la nature de l'objet connecté en analysant l'environnement dans lequel il évolue afin de déterminer un mécanisme de sécurisation adapté.
2. Identifier les risques d'intrusions dans un système connecté en appliquant les méthodes d'analyse de risques afin de protéger l'environnement opérationnel et d'adapter les logiciels en conséquence.
3. Détecter les alertes de sécurité en les analysant afin d'apporter la réponse aux incidents de sécurité.
4. Classifier les risques de sécurité en les analysant afin d'identifier les niveaux de vulnérabilité des objets connectés.
5. Caractériser les failles de sécurité en analysant les problèmes de cybersécurité des objets connectés mis en service afin de proposer des solutions en conformité avec les services informatiques internes et/ou externes à l'entreprise.
6. Répertoire les mesures à prendre pour protéger les systèmes des attaques potentielles en appliquant les méthodes de l'analyse de risque.
7. Effectuer une veille juridique afin d'être en capacité de respecter les réglementations en vigueur dans le but de répondre à toutes obligations légales.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise
- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise
- L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :
- Identifier l'environnement et les risques associés,
 - Classifier, répertoire les risques
 - S'appuyer sur des procédures de références et prendre en compte le cadre légal.

RNCP37931BC02 — Conception des solutions de sécurisation d'un réseau d'objets connectés en conformité avec la politique de sécurité de l'entreprise

LISTE DE COMPÉTENCES

1. Appliquer les différents standards relatifs à la sécurité des systèmes connectés afin de répondre aux obligations imposées en examinant les différents textes juridiques en vigueur.
2. Sécuriser un objet en sélectionnant des solutions existantes tant au niveau de leurs performances techniques

- (contraintes en termes de puissance de calcul, de mémoire, de disponibilité énergétique et d'occupation de la bande passante réseau, etc.) que de leur impact économique et social afin de répondre aux normes et standard en vigueur.
3. Concevoir une sécurité de manière dynamique en intégrant des mises à jour ou des changements de clés de chiffrement afin que ceux-ci puissent s'effectuer à distance (autoconfigurations automatiques et/ou reconfigurations de certains paramètres, configurations et clés de sécurité de manière dynamique au premier démarrage de l'appareil).
 4. Appliquer une sécurité dynamique de l'objet connecté en s'appuyant sur des logiques permettant de changer les clés de sécurité de l'appareil si celles-ci ont été compromises et de révoquer un appareil si celui a été volé, etc.
 5. Exploiter les documents techniques en version française et anglaise afin de proposer la solution la plus adaptée.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise
- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise

L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :

- Analyser des textes juridiques
- Concevoir et sélectionner des solutions de sécurité
- Exploiter des documents techniques

RNCP37931BC03 — Implémentation de solutions de sécurité numérique dans le cadre du déploiement d'un parc d'objets connectés

LISTE DE COMPÉTENCES

1. Implémenter les solutions, essentielles au déploiement d'objets connectés en adoptant des standards ouverts de Sécurité qui permettent d'assurer la sécurité des objets connectés notamment en termes d'authentification et de chiffrement des communications.
2. Analyser un cahier des charges en français et /ou anglais afin d'exploiter les spécifications associées à sa réalisation dans une situation de bureau d'études.
3. Gérer à distance le dispositif en s'appuyant sur des standards édictés par des consortiums de standardisation internationaux afin de sécuriser les systèmes et objets connectés.
4. Appliquer les procédures d'assurance qualité en implémentant une sécurité aux objets connectés afin d'intégrer des fonctionnalités de gestion standardisées telles que le Bootstrap ou le provisioning de paramètres.
5. Rédiger la documentation fonctionnelle et technique en suivant les nouvelles directives afin de les appliquer et/ou de les faire appliquer.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise
- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise

L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :

- Implémenter des solutions
- Analyser le cahier des charges
- Gérer à distance un dispositif avec son environnement sécurisé
- Prendre en compte les nouvelles directives

RNCP37931BC04 — Élaboration et mise en place d'un plan de formation pour former les usagers à appliquer les principes de sécurité numérique d'un parc d'objets connectés

LISTE DE COMPÉTENCES

1. Elaborer les process des solutions de sécurité implémentées afin de former les usagers aux nouveaux standards ou mises à jour déployées pour répondre aux différents niveaux de crise.

2. Analyser les écarts de compétences en observant l'application des procédures et des protocoles en matière de sécurité afin d'évaluer les besoins en formation du personnel et définir un plan de formation.
3. Définir un objectif pédagogique afin de sélectionner un organisme de formation pour adapter les compétences des usagers à leur poste de travail en prenant en compte les situations de handicap.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise
- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise

L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :

- Analyser les besoins des utilisateurs, avec la prise en compte et adaptation aux situations de handicap.
- Définir un plan de formation.

RNCP37931BC05 — Maintenance des outils de sécurité des objets connectés

LISTE DE COMPÉTENCES

1. Planifier les mécanismes de mise à jour logicielle dans le but d'intégrer l'obsolescence des produits en appliquant des correctifs de sécurité.
2. Gérer des solutions logicielles correctives en adoptant des technologies adaptées aux objets connectés, afin d'assurer la pérennité et la viabilité économique du parc d'objets connectés.
3. Évaluer la progression et la nature des risques sur un réseau en exploitation en contrôlant le développement des endroits susceptibles d'être attaqués sur chaque parc d'appareils connectés à Internet afin de mettre en place une solution de sécurité (Pare-feu, etc).
4. Proposer un plan de maintenance en élaborant un projet tenant compte de l'obsolescence des équipements matériels et informatiques afin de répondre à la demande des parties prenantes.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise
- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise

L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :

- Fournir un plan de maintenance tenant compte de l'obsolescence des différents matériels
- Proposer des solutions d'ajustement pour garantir la sécurité

RNCP37931BC06 — Encadrement d'une équipe dans l'environnement professionnel de la cybersécurité des objets connectés

LISTE DE COMPÉTENCES

1. Définir des objectifs en utilisant les méthodes et outils de l'environnement professionnel (Sécurité personnelle, poste de travail adapté aux situations de handicap) afin de garantir le bon déroulement du projet.
2. Apporter des corrections de trajectoire (durée, moyens matériels et humains) en fonction des résultats obtenus afin d'atteindre les objectifs du projet.
3. Travailler avec les équipes en prenant en compte leur diversité (culturelle, situation de handicap, etc) en mode collaboratif sur le choix de différents scénarios afin qu'ils s'approprient les solutions retenues.
4. Animer des réunions d'équipe en utilisant des outils de communication en langue française ou anglaise ainsi que des supports numériques adaptés (tableau de bord, illustrations graphiques, etc) afin de faciliter les échanges constructifs.

MODALITÉS D'ÉVALUATION

Projet d'entreprise. Travail individuel.

Devant le jury de certification :

- Soutenance individuelle d'un projet d'entreprise

- Temps de questions/réponses en français et en anglais portant sur le projet d'entreprise

Le candidat doit fournir un livrable sous format d'un rapport écrit attendu en amont de la session du jury de certification :

- Dossier professionnel mettant en œuvre les compétences acquises lors de la réalisation du projet d'entreprise

L'apprenant devra démontrer ses compétences développées dans son projet d'entreprise :

- Comprendre les enjeux globaux d'un projet

- Définir des objectifs de travail

- Utiliser des outils de communication en anglais

- Animer une réunion avec son groupe de travail en tenant compte des diversités de chacun (culturelle, situation de handicap, etc)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Informatique
- BTP
- Énergie
- Armement, Aéronautique
- Santé (Secteur hospitalier, Recherche)
- Production (Robotique, Industrie 4.0, etc)
- Qualité/Sécurité/Environnement
- Entretien/Maintenance

TYPE D'EMPLOIS ACCESSIBLES

- Administrateur/trice Systèmes et Sécurité
- Développeur IoT
- Intégrateur/trice de Systèmes sécuritaires pour l'IoT
- Gestionnaire d'un parc IoT

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 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 792 €
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) N0X70 — Techniciens d'étude, recherche et développement · tension 5/5 (Très élevée) N1X90 — Ingénieurs et cadres d'étude, recherche et développement (industrie) · tension 5/5 (Très élevée)

Projets de recrutement (BMO 2026)	52 304
Jugés difficiles à recruter	49 %
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 N0X70 — Techniciens d'étude, recherche et développement N1X90 — Ingénieurs et cadres d'étude, recherche et développement (industrie)

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le parcours de formation est accessible :

1. en 1ère année (S1) :

Pour prétendre à l'admissibilité, les candidats doivent être issus :

- d'un parcours de formation certifié de niveau 4 dans les domaines d'activités en lien avec la certification visée (énergie, informatique, électronique)
- de terminales générales (validation définitive de l'intégration sur attestation de réussite au BAC)
- de terminales technologiques sciences et technologies de l'industrie et du développement durable – STI2D
- d'une première année d'enseignement supérieur (BUT, BTS, L1...)

2. en 2ème année (S3) :

L'entrée en 2ème année (S3) est accessible :

- aux titulaires d'un titre certifié de niveau 5 dans les domaines d'activités en lien avec la certification visée (énergie, informatique, électronique)
- aux étudiants de 2ème année de classes préparatoires scientifiques
- aux élèves en cours d'études pour les BUT, L1 sous réserve qu'ils aient validé leur première année ou leurs 2 premiers semestres

3. en 3ème année (S5)

L'entrée en 3ème année (S5) est accessible :

- aux titulaires d'un titre certifié de niveau 5 dans les domaines d'activités en lien avec la certification visée (énergie, informatique, électronique)
- aux titulaires d'un diplôme français de niveau BAC + 2 (BUT, BTS, L2, etc.)
- aux titulaires d'un titre français, titre ou diplôme étranger reconnu équivalent aux titres et diplômes cités ci-dessus par une commission ad hoc *
- aux candidats détenteurs d'une évaluation d'acquis professionnels et personnels sanctionnée par une commission ad hoc *.

(*) : Une commission ad hoc est chargée d'apprécier l'équivalence des diplômes, des formations ou des acquis de l'expérience.

Pour tout candidat, l'accès au parcours de formation se fait sur la base :

- Concernant les publics de formation initiale : des épreuves d'admissibilité sur dossier et d'admission sur tests et entretien en cas de succès à l'admissibilité.
- Concernant les publics adultes en reprise d'études : étude du projet professionnel et évaluation des compétences et acquis d'expériences antérieures pour l'identification du parcours de formation adaptée.

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE, VAE

Le jury de certification est composé de 5 membres ayant les compétences professionnelles visées par le titre, dont à minima 3 professionnels extérieurs à l'école.

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 € – 11 787 €
Prise en charge	Branches concernées
9 475 €	Valeur par défaut · 187 branches
11 787 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE Travail Temporaire, CPNE des Télécoms, CPNEF de la Publicité, CPNEF de la presse et des agences de presse
10 500 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des métiers du géomètre, CPNEFP de la profession d'économiste de la construction, CPNEFP des industries des tuiles et briques
9 000 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
8 467 €	CPNE Casinos, CPNE de la branche de la Distribution Directe
8 500 €	Commission Paritaire Activités de Marchés Financiers
8 466 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
8 400 €	CPNEF de l'audiovisuel
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
8 000 €	CPNE chimie
7 923 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
7 808 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 720 €	CPNE de la branche des experts comptables et commissaires aux comptes
7 000 €	CPNEFP de la métallurgie

Base légale

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

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP41278

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www.esme.fr/titres-rncp/cybersecurite-des-objets-connectes/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37931/>