

Ingénieur diplômé du Conservatoire national des arts et métiers, spécialité Informatique et cybersécurité

RNCP39308 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31006, 31094, 24293, 31009, 32062
Code(s) ROME	M1801, M1802, 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

CONSERVATOIRE NATIONAL DES ARTS ET METIERS · SIRET : 19753471200017

Partenaires habilités

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

Organisme	SIRET	Habilitation
CNAM GRAND EST	82304134800017	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Selon l'International Information System Security Certification Consortium (ISC2), la cybersécurité pèserait 4,5 Millions de personnes au niveau mondial sous quelques années. Le marché étant actuellement d'1 Million, c'est 3,5 Millions de spécialistes en cybersécurité? sont qui sont attendus (Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements C. Matt Graham a and Yonggang Lub - FURNELL, Steven. The cybersecurity workforce and skills. Computers & Security, 2021, vol. 100, p. 102080).

En France, en 2021, selon une étude conduite par l'APEC et le Pôle d'Excellence Cyber, ce sont 15% des offres qui sont non couvertes sur les 7 000 offres d'emplois de cadres cybersécurité proposées.

Cette pénurie évolue chaque année de +12%. Un an plus tôt, la filière industrielle de sécurité (CSF) estimait le marché de l'emploi pour les prochaines années à 15 000 offres en cyber. Elle lance dès 2020 un appel à la création de plus de 4 000 formations, favorisant le bac à bac+3, mais également les formations d'experts et d'ingénieurs, ce qui ouvre des perspectives énormes pour l'ensemble des métiers de l'ingénierie en cybersécurité.

Les entreprises recherchent majoritairement des profils à la fois généraliste, pour prendre en charge la cybersécurité dans l'entière de l'organisation, et opérationnels pour entreprendre des activités de confiance au quotidien, comme les fonctions de déploiement des services de sécurité (« build ») ou de leur surveillance (« run »)

Étant donné le tissu industriel et de services du territoire, la formation vise, entre autre, la mise en place d'une cybersécurité adaptée aux besoins des petites et moyennes organisations qui repose sur une approche à la fois système et par composant. Cette question est cruciale, car ces structures n'ont a priori ni les structures ni les moyens ou même la posture pour anticiper, détecter, lever le doute, corriger les cyberattaques. Elles n'ont en outre que peu l'occasion de capitaliser sur ces cyberattaques comme le ferait une structure aguerrie à ces incidents de sécurité.

ACTIVITÉS VISÉES

L'ingénieur disposant de la certification Ingénieur du CNAM dans la spécialité? « Informatique et Cybersécurité? » couvre les différents domaines de la cybersécurité : l'analyse de sécurité et des risques opérationnels cyber, la conception « by design », l'optimisation (« durcissement » ou « hardening »), la supervision (SOC, CERT), il a vocation à assurer les activités suivantes :

- L'analyse de sécurité et du risque cyber de systèmes informatiques ou de systèmes d'informations complexes, incluant l'analyse de la menace, des vulnérabilités et des attaques au profit d'organisations à dimension internationale.
- La conception, la modélisation et l'élaboration de dispositifs informatiques de sécurité? sur l'ensemble des domaines cyber, pour l'optimisation ou « hardening » ou un centre de sécurité opérationnel (SOC).
- Le pilotage du projet d'intégration d'un dispositif informatique de sécurité, dans le contexte d'une organisation complexe, à dimension internationale, sur l'ensemble des domaines cyber.
- L'organisation, l'intégration et la mise en œuvre de mesures de « durcissement » (« hardening ») de dispositifs de sécurité dans des systèmes d'informations complexes, au profit d'organisations à dimension internationale, couvrant les différents domaines cyber.
- L'organisation, les choix, la préparation et le pilotage de grands projets de centres de supervision (SOC, CERT) ainsi que la mise en œuvre du processus de cybersécurité au sein d'organisations à dimension internationales.

COMPÉTENCES ATTESTÉES

L'ingénieur cyber du Conservatoire national des Arts et Métiers a trois types de compétences :

1. L'ingénieur cyber mobilise ses connaissances scientifiques et fondamentaux pour la maîtrise des méthodes et techniques dans les différents domaines cyber de l'analyse de sécurité et des risques cyber, la conception « by design », la supervision (SOC, CERT) et l'optimisation (« durcissement ») de la cybersécurité :

- Analyser le besoin client en matière de conception des mesures et contremesures de cybersécurité et d'investigation des cyberattaques dans les événements de sécurité (SIEM), d'outils en s'appuyant sur les sciences fondamentales : mathématiques (représentation matricielle, théorie des graphes et des treillis, congruence, théorie des ensembles, algorithmie, langages d'automates finis, statistiques et probabilités, etc.), physique, calcul scientifique, etc.
- Piloter le projet de modélisation, conception, mise en œuvre, test et validation d'un modèle, protocole, architecture d'un dispositif de cybersécurité, en s'appuyant sur la méthode scientifique et les ressources des champs scientifiques et techniques de l'informatique et des mathématiques, comprenant le champ de la science des données pour la maîtrise des techniques de recherche, d'évaluation et d'exploitation de l'information.
- Effectuer des activités de recherche, fondamentale ou appliquée du domaine de la cybersécurité à l'aide de méthodes, outils logiciels et services innovants (cryptographie, aléas, graphe d'attaques, arbres de décision, « problème d'atteignabilité », etc.), afin de concevoir « by design », concrétiser, tester (rétroingénierie) et valider des solutions de sécurité informatique.
- Mobiliser les méthodes et outils de l'ingénieur : identification, modélisation et résolution de problèmes complexes et émergents, à l'aide d'une approche systémique et holistique, afin de piloter l'amélioration continue du dispositif de sécurité et coordonner les activités d'analyse des cyber -risques et de la cyber-menace.
- Intégrer diverses disciplines scientifiques (apprentissage des langues, sciences cognitives, sciences de la décision, neurosciences, sciences humaines et sociales), afin de coordonner l'activité d'une équipe pluridisciplinaire et potentiellement à l'international, en anglais et de déléguer diverses responsabilités, en tenant compte des enjeux des relations au travail, la diversité, l'éthique, le professionnalisme, la sécurité et la santé au travail, en situation de crise.

2. L'ingénieur cyber maîtrise les méthodes et technologies afin de mener de grands projets de cybersécurité comme l'évaluation du niveau de sécurité des organisations vulnérables, la gestion d'appels d'offres de solutions cyber et le pilotage de projets de centres de sécurité opérationnels (SOC, CSIRT) :

- Évaluer et modéliser les phénomènes cyber liés aux techniques offensives d'ingénierie sociale, dans le respect total de l'éthique (mécanismes d'« attaque-défense », « threat modeling », « Red team », « blue team », « purple team »), afin de rédiger le cahier des recommandations en prenant en compte les normes techniques (OWASP, calcul CVSS), et les dimensions sociales, géo-politiques, sociétales, organisationnelles et environnementales de l'organisation.
- Concevoir, dimensionner, concrétiser, tester et valider un dispositif de sécurité? informatique complexe et innovants, à partir des normes et standard des modèles, protocoles et architectures dans les différents domaines de la cybersécurité : anticipation, et prévention (risque, CTI), supervision (SOC), remédiation (CSIRT), en choisissant des méthodes de rétroconception (ingénierie inverse) et d'écoconception adaptées, en réponse aux enjeux divers de l'organisation.

- Développer une méthodologie de R&D et effectuer une veille continue, une analyse comparative à l'état de l'art, adaptée au contexte fortement dynamique de la cybersécurité (CI/CC, DevOps et SecDevOps), le test de solutions (« Threat modeling »), la preuve de concept (PoC), le prototype (MVP-TRL),
 - Intégrer les enjeux environnementaux et sociétaux dans le cadre du déploiement de projets de cybersécurité et accompagner l'organisation dans toutes les transitions, en mettant en œuvre des choix technologiques adaptés aux grands enjeux sociétaux actuels, naturellement en matière de protection des systèmes d'information (LPM, NIS, ISO 27x, homologation, ANSSI), de vie privée (RGPD), mais également par une démarche vertueuse et respectueuse de l'éthique et la RSE de l'organisation vis-à-vis des exigences commerciales, économiques, de compétitivité et de productivité de l'entreprise.
 - Évaluer et élever le niveau de sécurité globale cyber de l'organisation, à partir d'outils d'audits, de cartographie des actifs (ebios, EGERIE), de détection de vulnérabilités et d'anomalies (IDS, TENABLE) ou d'analyse postmortem (SIEM)), afin d'intégrer les propres contraintes, besoins, exigences de sécurité de l'organisation, les traduire en termes techniques, par l'élaboration d'une politique de sécurité (PSSI), la, planification et la mise en œuvre de recommandations concrètes (CWPP, Cloud Workload Protection Platform, DMZ, gestion des identités, MFA, etc.), puis de les rédiger, les présenter et les défendre, en langue anglaise, dans un environnement multiculturel.
 - Piloter l'amélioration continue du dispositif de sécurité? ou de la sécurité du SI de l'organisation, coordonner les activités de tests de robustesse (« White » », « Gray », « black » box mode), à partir d'analyses cyber risques et des méthodes et outils de l'ingénieur pour l'identification, la modélisation et la résolution de problèmes complexes, prendre des responsabilités d'animation en intelligence collective en situation de crise cyber, tout en assurant le respect des relations de travail, de la diversité, l'éthique, la sécurité et la santé au travail.
 - Définir des indicateurs de performance de la sécurité d'un système informatique (IoC, CVSS, etc.) afin d'organiser et mettre en place le reporting technique, administratif et financier en intégrant par une approche holistique les impératifs environnementaux (énergétiques, écologiques et climatiques).
 - Capitaliser sur les expériences des experts cybersécurité à l'aide d'une démarche scientifique (Datascience), afin d'organiser et enrichir les bases de connaissances de nouvelles techniques d'attaques et de transmettre les principes de cyberdéfense.
 - Travailler en contexte international et multiculturel avec la maîtrise d'une ou plusieurs langues étrangères et ouverture culturelle associée, capacité d'adaptation aux contextes internationaux.
 - Communiquer et gérer au sein d'équipes pluridisciplinaires (clients, architectes, fournisseurs, sous-traitant), les appels d'offre de projets de transformation cyber, et, les mettre en œuvre à partir de méthodes et outils de conception, d'optimisation (« hardening ») et de supervision de la cybersécurité de systèmes d'information complexes et émergents (« Cloud computing », « fog » et « edge computing »).
3. L'ingénieur cyber maîtrise les techniques de l'ingénieur des domaines cyber pour atteindre une expertise cyber et intégrer des entreprises de services numériques, spécialisées dans la gestion des risques opérationnels cyber et/ou l'optimisation (« durcissement ») de la cybersécurité dans une organisation et/ou dans un centre de sécurité opérationnel (CSIRT, CERT, SOC) :
- Concevoir, dimensionner (« hardening ») et déployer le dispositif de sécurité? (parefeu, DMZ, IDS, Scanner, Proxy, etc.), réaliser une représentation fonctionnelle du dispositif et les schémas d'architecture (Merise, UML, SysML), rédiger les documents formalisant l'architecture, les spécifications détaillées et les notifications de changements d'architecture.
 - Maintenir la sécurité du dispositif informatique en condition opérationnel, mettre en œuvre un outil de suivi des incidents de sécurité, suivre les demandes d'évolution, corriger les incidents techniques, proposer des solutions alternatives avant la correction (fenêtre de vulnérabilité, "zero day"), rédiger, partager et publier un bulletin d'alerte de sécurité,
 - Conduire des analyses SOC « hunting », élaborer la détection précoce des incidents de sécurité (CTI), dans les événements de sécurité? (SIEM), mettre en place des outils DevOps (Ansible Playbooks, Puppet, etc.).
 - Conduire des analyses SOC "red team", dans le respect total de l'éthique, pénétrer un système informatique à l'aide de tests d'intrusion (KALI), après avoir identifié et utilisé une faille de sécurité applicative, réseau ou système, réaliser le fuzzing d'un logiciel afin de tester la robustesse à l'injection de code malveillants, analyser les indicateurs de compromission (IoC), calculer un indicateur de vulnérabilité (CVSS), produire un arbre d'attaque, proposer des solutions de remédiation.
 - Conduire des analyses SOC "postmortem", dans le respect total des règles de l'investigation numérique légale (ISO 27042 et suite), conserver les preuves de la cyber attaque afin de pouvoir les produire lors d'une expertise judiciaire, expliquer l'attaque (timeline, causalité), la publier dans des conférences techniques internationales (par exemple blackhat), expliquer et entraîner l'équipe SOC à ces principes d'analyse forensique légale, évaluer financièrement le

risque d'une cyber attaque.

- Conduire des activités de réponse à incident cyber, mettre en place le plan de continuité d'activité et de reprise d'activité dans le respect de la norme ISO 22301, réaliser des analyses de contenu (DLP : Data Loss Prevention), calculer les indicateurs clé (RTO : Recovery Time Objective, RPO (Recovery Point Objective), avec des équipes internationales.
- S'insérer dans la vie professionnelle, collaborer, communiquer, animer et faire évoluer l'organisation en s'intégrant au sein d'équipes multiculturelles et pluridisciplinaires en exerçant la responsabilité?, l'engagement, le management, la position de référent technique, de chef ou directeur de projets.

Blocs de compétences

RNCP39308BC01 — Conduire une analyse de sécurité et des risques cyber des systèmes d'information d'une organisation complexe, à dimension internationale

LISTE DE COMPÉTENCES

- Identifier les risques techniques les évaluer, les traiter par réduction, transfert ou confinement, afin de concevoir un dispositif informatique pour protéger et/ou maintenir la sécurité de tout ou partie du système d'information d'une organisation à dimension internationale et multiculturelle.
- Analyser les besoins du Système de management des Informations de Sécurité (SMSI) en identifiant les informations de sécurité et la structure du fond documentaire cyber relatif à la sécurité du SI et à l'aide d'une méthodologie de gestion du risque cyber (EBIOS; etc.), afin d'élaborer et conduire les démarches pour l'audit ou l'homologation.
- Évaluer la surface d'attaque à partir du repérage des points d'entrée potentiels dans le système d'information ou l'un des composants d'une organisation à dimension internationale et multiculturelle, ou de l'une de ses entités afin de mener une analyse d'ingénierie inverse.
- Évaluer la surface d'exposition à partir d'une analyse de vulnérabilités afin de rechercher les vulnérabilités potentielles du système d'information ou de l'un des composants d'une organisation à dimension internationale et multiculturelle, ou de l'une de ses entités.
- Réaliser et présenter à la direction un diagnostic, une cartographie des risques et/ou un plan de remédiation, de recommandations et d'actions prioritaires incluant les moyens humains et financiers nécessaires à l'amélioration continue de la sécurité d'une organisation à dimension internationale et multiculturelle.

MODALITÉS D'ÉVALUATION

- Examens sur table.
- Contrôle continu.
- Travaux Pratiques
- Mises en situation
- Exercices dirigés
- Projets tuteurés conduits en groupe et en entreprise mettant en œuvre les concepts et acquisitions enseignées lors des séquences à l'école.
- Rédaction de rapports et soutenance devant un jury afin d'argumenter les choix réalisés sur divers aspects technologiques, sociétaux ou organisationnels et normatifs.

RNCP39308BC02 — Concevoir, modéliser, élaborer un dispositif informatique ou de sécurité informatique destiné à la protection, l'analyse, la supervision, la correction ou l'optimisation des fonctions de cybersécurité d'un système d'information ou de l'un de ses composants

LISTE DE COMPÉTENCES

- Identifier et traduire les besoins d'un dispositif informatique ou plus spécifiquement de sécurité informatique, en mesures techniques et organisationnelles, à partir des plans de remédiation, en priorisant les mesures à concevoir.
- Concevoir un dispositif informatique ou plus spécifiquement de sécurité informatique pour la protection, l'audit, la supervision, la remédiation et/ou l'optimisation du système d'information ou de l'un de ses composants.
- Modéliser les exigences d'un dispositif informatique, et plus spécifiquement de sécurité informatique, dont la menace, les protections et opérations de sécurité que le dispositif devra satisfaire.
- Élaborer et valider une maquette du dispositif informatique de sécurité pour analyser, superviser, corriger et/ou optimiser les opérations de cybersécurité d'un système d'information ou de l'un de ses composants. .

MODALITÉS D'ÉVALUATION

- Examens sur table.
- Contrôle continu.
- Travaux Pratiques
- Mises en situation
- Exercices dirigés
- Projets tuteurés conduits en groupe et en entreprise mettant en œuvre les concepts et acquisitions enseignées lors des séquences à l'école.
- Rédaction de rapports et soutenance devant un jury afin d'argumenter les choix réalisés sur divers aspects technologiques, sociétaux ou organisationnels et normatifs.
- PFE soutenu face à un jury d'enseignants et de professionnels.

RNCP39308BC03 — Piloter un projet d'intégration d'un dispositif informatique de sécurité, dans le contexte d'une organisation complexe, à dimension internationale

LISTE DE COMPÉTENCES

- Identifier les vulnérabilités en termes organisationnels, technologiques, humaines et économiques mettant en jeu l'atteinte des objectifs stratégiques du projet de sécurité du fait de la prise en compte de la taille de l'organisation, de sa complexité, de sa dimension internationale et multiculturelle, éloignée de la culture cyber, en mettant des mesures en place le cas échéant.
- Rédiger un appel d'offres pour un projet de sécurité informatique en organisant le phasage, les critères de choix en s'appuyant sur des référentiels d'activité, afin de consulter les fournisseurs potentiels et de restreindre la liste des candidats ("short list").
- Évaluer les solutions et candidats retenus en utilisant une grille critérielle démontrant que le dispositif informatique de sécurité proposé est adapté au système d'information de l'organisation complexe, à dimension internationale, éloignée de la culture cyber.
- Établir et superviser la réalisation d'un plan de communication interne et organiser la concertation autour du projet de sécurité, y compris en situation de crise.

MODALITÉS D'ÉVALUATION

- Examens sur table.
- Contrôle continu.
- Travaux Pratiques
- Mises en situation
- Exercices dirigés
- Projets tuteurés conduits en groupe et en entreprise mettant en œuvre les concepts et acquisitions enseignées lors des séquences à l'école.
- Rédaction de rapports et soutenance devant un jury afin d'argumenter les choix réalisés sur divers aspects technologiques, sociétaux ou organisationnels et normatifs.
- PFE soutenu face à un jury d'enseignants et de professionnels.

RNCP39308BC04 — Organiser, mettre en œuvre et renforcer la robustesse d'un ou plusieurs dispositifs informatiques ou de sécurité d'une organisation complexe, à dimension internationale

LISTE DE COMPÉTENCES

- Planifier, structurer, piloter, installer et configurer les systèmes de management des informations ou de systèmes d'ordonnancement des opérations de sécurité, en respectant les priorités à priori, afin de permettre une application et un suivi rigoureux du plan de remédiation.
- Appliquer, coder, installer, configurer les mesures de sécurité de base, au regard des principes essentiels de maintien de la confidentialité (chiffrement, authentification, autorisations, etc.), de l'intégrité, la disponibilité (sauvegardes, etc.) et traçabilité (journaux, logs), afin de réduire, transférer ou confiner les risques selon les moyens et la maturité cyber de l'organisation complexe, à dimension internationale et multiculturelle.
- Durcir un système, coder, installer, configurer des mesures de sécurité avancées, offensives ou défensives, ou mettre en place des sondes ou points de contrôles de conformité, afin de réduire, confiner et traiter le risque cyber.
- Évaluer, contrôler et optimiser la robustesse du dispositif informatique de sécurité vis à vis des cyberattaques par le biais de tests unitaires ou d'un jumeau de type cyberrange.
- Conduire les démarches d'homologation du Système de management des Informations de Sécurité (SMSI)

en évaluant en amont la menace, les surfaces d'attaques et d'exposition de façon adaptée à une organisation à dimension internationale et multiculturelle.

MODALITÉS D'ÉVALUATION

- Examens sur table.
- Contrôle continu.
- Travaux Pratiques
- Mises en situation
- Exercices dirigés
- Projets tuteurés conduits en groupe et en entreprise mettant en œuvre les concepts et acquisitions enseignées lors des séquences à l'école.
- Rédaction de rapports et soutenance devant un jury afin d'argumenter les choix réalisés sur divers aspects technologiques, sociétaux ou organisationnels et normatifs.
- PFE soutenu face à un jury d'enseignants et de professionnels.

RNCP39308BC05 — Organiser et superviser un centre de sécurité opérationnelle (SOC) d'un ou plusieurs systèmes d'information au sein d'une entreprise de cyber sécurité

LISTE DE COMPÉTENCES

- Superviser les équipes d'un centre de sécurité opérationnelle (SOC) dans l'organisation et la réalisation des opérations de sécurité de l'analyse de la menace, de détection d'attaques et de vulnérabilités, d'investigation et de remédiation.
- Former les équipes à l'utilisation des outils de sécurité défensifs (règles de pare feu, mise en place de sondes, SNORT, UEBA, ..) et offensifs (MALTEGO, KALI,..) adaptés au système d'information de l'organisation à dimension internationale et multiculturelle afin de détecter, analyser, lever le doute.
- Organiser et piloter la réponse à un incident de sécurité afin de neutraliser et bloquer les cyberattaques, en s'appuyant sur des outils de réponse à incident (SOAR,EDR, XDR,..) , adaptés au système d'information de l'organisation à dimension internationale et multiculturelle.
- Analyser, caractériser les modes opératoires des cyberattaquants et constituer un fond documentaire cyber relatif à la sécurité du SI et une méthodologie de gestion du risque cyber (EBIOS) afin de capitaliser l'expérience dans le cadre d'une démarche d'amélioration continue de la protection de l'organisation à partir d'une analyse des modes opératoires des cyberattaquants.

MODALITÉS D'ÉVALUATION

- Examens sur table.
- Contrôle continu.
- Travaux Pratiques
- Mises en situation
- Exercices dirigés
- Projets tuteurés conduits en groupe et en entreprise mettant en œuvre les concepts et acquisitions enseignées lors des séquences à l'école.
- Rédaction de rapports et soutenance devant un jury afin d'argumenter les choix réalisés sur divers aspects technologiques, sociétaux ou organisationnels et normatifs.
- PFE soutenu face à un jury d'enseignants et de professionnels.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Tous secteurs.

TYPE D'EMPLOIS ACCESSIBLES

Métiers de la conception et de l'urbanisation du SI : traduire les besoins fonctionnels d'un système d'information en fonction d'objectifs et d'exigences métier en vue d'élaborer une urbanisation du système d'information et mettre en œuvre un SI évolutif, ou définir et mettre en œuvre une gestion globale des risques en termes de SI :

- Conseil et maîtrise d'ouvrage en systèmes d'information
- Conduite projet informatique

- Architecture système information

Métiers des infrastructures réseaux et systèmes : garantir l'accès et la performance de l'infrastructure informatique d'une organisation en vue de sécuriser l'ensemble des interconnexions :

- Ingénieur en cybersécurité.
- Architecte sécurité Cloud.
- Architecte réseaux et sécurité.
- Ingénieur/ingénieure sécurité télécom.
- Administrateur/administratrice de la sécurité des réseaux et des systèmes.
- Administration de systèmes d'information.
- Expertise et support en systèmes d'information.
- Direction des systèmes d'information.
- Études et développement de réseaux de télécoms.
- Conseil et maîtrise d'ouvrage en systèmes d'information

Métiers de l'intégration logicielle, : garantir que les programmes sont bien conçus et fonctionnent correctement :

- Chef de projet de sécurité numérique.
- Intégrateur chef de la sécurité d'un projet web.
- Architecte de la sécurité logicielle.
- Expertise et support en systèmes d'information

Métiers des sciences des données, de leur organisation base de données et des systèmes décisionnels qui les exploitent :

- Ingénieur en Business Intelligence.
- Directeur de la sécurité des systèmes d'information. Administrateur/administratrice de la sécurité des bases de données.
- Administration de systèmes d'information
- Maintenance informatique et bureautique
- Études et développement informatique

Métiers de l'optimisation logicielle, à partir d'une connaissance approfondie de l'algorithmie, souvent requise dans les départements recherche et développement des entreprises.

- Data Scientists dans un Centre de Sécurité Opérationnel
- Ingénieur simulations en industrie pour la sécurité de systèmes embarqués.
- Chercheur en cybersécurité.

Métiers de la sécurité de ces briques : mise en service de ces différentes briques informatiques.

- Responsable, auditeur Sécurité Informatique.
- Responsable d'un SOC (Security Operation Center).
- Responsable d'un centre de réponse à incident de sécurité (CSIRT). M1802, Expertise et support en 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)	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

Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Certification scientifique et technique de niveau 5 minimum.

COMPOSITION DU JURY — APPRENTISSAGE

Le jury est présidé par le Directeur de l'EICnam ou son représentant.

En plus du président, le jury est composé paritativement de personnalités du milieu professionnel et du milieu académique avec un quorum de huit personnes. Il comprend a minima :

- le directeur du Centre Cnam en région Grand-Est ou son représentant,
- le responsable national du diplôme concerné ou son représentant,
- le responsable opérationnel du diplôme concerné ou son représentant,
- le Directeur du CFA ou son représentant,
- le représentant du partenaire institutionnel de la formation (association de partenariat et/ou établissement d'enseignement supérieur) le cas échéant
- de représentants des entreprises partenaires.

La composition du jury est arrêtée chaque année par le Directeur de l'EICnam sur proposition du responsable national du diplôme ou de son représentant et portée à la signature de l'administrateur général du Cnam par la Direction nationale des formations.

La composition du jury est arrêtée chaque année par le Directeur de l'EICnam sur proposition du responsable national du diplôme ou de son représentant et portée à la signature de l'administrateur général du Cnam par la Direction nationale des formations.

COMPOSITION DU JURY — VAE

Le jury de validation des acquis de l'expérience (VAE) pour le diplôme d'ingénieur diplômé par le Cnam est composé de 3 enseignants-chercheurs et 2 professionnels choisis dans une liste validée annuellement par l'administrateur générale du Cnam.

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	10 268 €
Selon la branche	7 700 € – 10 952 €
Prise en charge	Branches concernées
10 268 €	Valeur par défaut · 191 branches
10 952 €	CPNE Casinos, CPNE chimie, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel
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
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
8 500 €	CPNEFP de la Mutualité Sociale Agricole, CPNEFP de la métallurgie
10 514 €	CPNE Travail Temporaire
9 200 €	CPNEFP des industries électriques et gazières
8 750 €	CPNEFP Commerce à distance
8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
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	31/08/2030

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42432

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Cette formation par la voie de l'apprentissage est préparée par le
Centre Cnam en Grand Est,
Centre de formation Saint-Dié-des-Vosges
7 rue Maurice Jeandon
88100 Saint-Dié-des-Vosges
site web : <https://www.cnam-grandest.fr/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39308/>