

Architecte cybersécurité et internet des objets (MS)

RNCP40347 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	110, 326
Formacode(s)	24231, 31006, 31042, 31028
Code(s) ROME	M1805, M1801, M1802, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	28/03/2025
Date d'échéance	28/03/2028

Certificateur(s)

CY CERGY PARIS UNIVERSITE · SIRET : 13002597600015

Résumé de la certification

OBJECTIFS ET CONTEXTE

À l'ère de l'essor des technologies numériques, les entreprises, les organisations et, plus largement, les sociétés, se retrouvent confrontées à une menace croissante de cyberattaques. Au cœur de cette révolution numérique, la cybersécurité se positionne comme un pilier essentiel au bon déroulement des entreprises et des institutions. L'objectif de la certification Architecte cybersécurité et internet des objets (MS) est de former des experts capables de concevoir, déployer et administrer des solutions de cybersécurité efficaces pour assurer la protection des Systèmes Intelligents.

ACTIVITÉS VISÉES

Architecturation d'une solution IoT (Internet des Objets) pour un système intelligent sécurisé, du début à la fin .
Évaluation et renforcement de la sécurité technique d'une organisation, en prenant en compte les spécificités de la cybersécurité et de l'IoT.
Conception et développement de solutions d'intelligence artificielle pour la sécurisation de l'IoT.
Analyse et gestion des données massives issues de l'IoT.
Gestion des identités et des accès (Identity and Access Management).
Mise en œuvre d'une politique de sécurité.
Supervision de la collaboration avec des experts métiers de divers domaines (architectes experts en sécurité, systèmes, réseaux, logiciels, big data, etc.).
Pilotage de l'exécution du projet et animation des équipes intervenantes à chaque étape.
Déploiement et suivi de la solution IoT.
Réalisation d'une investigation approfondie dans le domaine de la cybersécurité et de l'IoT.
Analyse et exploitation des preuves numériques pour établir une chronologie détaillée des incidents de sécurité et identifier les failles exploitées.
Gestion, détection et analyse des incidents de sécurité.
Mise en place de mécanismes de réponse aux incidents et de remédiation pour limiter l'impact des attaques et restaurer la sécurité des systèmes.
Conception et déploiement d'architectures sécurisées
Surveillance des activités réseau et détection des menaces
Analyse des vulnérabilités et gestion des incidents de sécurité
Sensibilisation aux enjeux de sécurité

COMPÉTENCES ATTESTÉES

Évaluer le contexte environnemental et conduire une analyse approfondie du système d'information pour définir une architecture appropriée en se fondant sur le modèle fonctionnel et optimiser la mise en application.

Proposer des architectures techniques de référence conformes pour répondre aux besoins du projet IoT et de cybersécurité.

Organiser et piloter des revues d'architectures et de conceptions pour garantir la prise en compte des exigences initiales et des demandes d'évolutions du cahier des charges

Mettre en œuvre des processus de test robustes en intégrer harmonieusement les composants IoT et de cybersécurité pour garantir la qualité de la solution répondre au cahier des charges

Intégrer les principes de sécurité dès la conception de la solution IoT en adoptant l'approche "Secure by Design," et en respectant les meilleures pratiques et recommandations pour promouvoir la sécurité du système.

Analyser, calibrer et harmoniser l'architecture technique des solutions logicielles à connecter avec la plateforme IoT en validant leurs interopérabilités afin de garantir la robustesse du système.

Assurer la conformité de la solution IoT et de cybersécurité développée aux normes et réglementations en vigueur pour garantir la protection des données personnelles.

Auditer les architectures réseau en documentant les analyses conduites et les résultats des audits de sécurité IoT, pour identifier les points faibles dans l'écosystème IoT.

Planifier des tests d'intrusion éthiques sur les systèmes IoT en utilisant les outils de Kali Linux pour évaluer la robustesse des défenses du système.

Simuler des attaques ciblant les objets connectés à l'aide d'outils tels que nmap, metasploit ou armitage, pour identifier et analyser les vulnérabilités des systèmes IoT.

Analyser les configurations des équipements IoT et leurs mécanismes d'authentification en utilisant des outils adaptés pour tester la robustesse du système.

Identifier les risques potentiels pour la sécurité des systèmes IoT en les classant selon leur criticité pour prioriser les actions correctives.

Détecter des activités anormales ou suspectes dans les environnements IoT en interprétant les logs des dispositifs, des communications et des transactions en vue d'identifier des modèles de comportement et d'anticiper des incidents.

Renforcer la sécurité opérationnelle du système IoT en veillant au respect des règles éthiques en matière de traitement des données sensibles pour limiter la survenance des risques d'intrusion.

Créer des modèles prédictifs et de reconnaissance de motifs en exploitant des algorithmes d'apprentissage automatique pour analyser et traiter les données issues des dispositifs IoT.

Collecter, nettoyer et analyser de grandes quantités de données pour améliorer la prise de décision et la sécurité.

Configurer et administrer des solutions d'authentification robustes basées sur les principes Zero trust et Least Privilege, d'authentification multifactorielle et/ou adaptative pour limiter les risques d'intrusion.

Définir et déployer des politiques de gestion des accès et des privilèges liés à la gouvernance des identités (Identity and Access Governance) en conformité avec les normes de sécurité (Numeric Identity, Identity Lifecycle) en élaborant des matrices de rôles et d'accès limités par fonctions pour garantir une répartition des accès adaptée aux besoins métiers.

Intégrer des protocoles d'authentification et d'autorisation tels que Kerberos, WS-Federation, SAML v2, OAuth2.0, OIDC pour protéger les ressources de l'organisation.

Garantir l'interopérabilité du système IAM en s'appuyant sur le principe de fédération des identités (Identity Federation) pour assurer l'intégration fluide des systèmes et faciliter la navigation.

Réaliser une veille permanente sur les évolutions technologiques liées à l'IoT et à la cybersécurité, en anticipant et en accompagnant les changements organisationnels induits, afin d'intégrer les innovations pertinentes dans le projet et d'assurer l'adaptabilité du système.

Appliquer des normes de sécurité techniques spécifiques à la cybersécurité et à l'IoT (ISO 27001, NIST, CIS, etc.) pour interpréter et appliquer les exigences de ces normes dans le contexte des objets connectés.

Garantir le respect des règles éthiques liées à la sécurité, en tenant compte des données sensibles générées par les objets connectés et les informations sensibles découvertes lors des audits IoT pour garantir le respect de la réglementation en matière de traitement des données personnelles.

Planifier de manière détaillée les différentes phases du projet IoT et de cybersécurité, de la conception au déploiement afin d'assurer la réalisation du projet dans les temps impartis

Gérer les ressources, le budget et les délais du projet pour assurer la réalisation efficace des objectifs fixés.

Participer aux instances de pilotage (comité de pilotage) et définir des indicateurs de suivi de projet (KPIs) et des

tableaux de bord pour assurer la coordination des tâches et une gestion efficace du projet.

Coordonner et communiquer de manière efficace et transparente avec les parties prenantes et experts de divers domaines tels que la sécurité, les systèmes, les réseaux, les logiciels, le big data, le cloud... etc afin de comprendre les besoins spécifiques de chaque spécialiste et promouvoir le suivi du projet.

Diriger et motiver les équipes dans une démarche inclusive tout au long du projet pour stimuler leur créativité et leur implication.

Encourager la collaboration, la créativité et l'innovation au sein des équipes de conception, de développement, de tests, d'intégration et de déploiement pour améliorer la cohésion d'équipe.

Recueillir les retours d'expérience utilisateurs et intégrer les remarques dans les demandes d'évolution des solutions IoT et de cybersécurité afin de perfectionner le système IoT et de garantir son accessibilité à tous les publics.

Identifier rapidement et les problèmes potentiels et mettre en place des processus de maintenance corrective et évolutive pour assurer la pérennité des solutions IoT et de cybersécurité.

Développer des actions de sensibilisation et de formation à la cybersécurité à destination des personnels de l'organisation pour prévenir la survenance du risque cyber.

Identifier, extraire et analyser les traces numériques laissées dans les systèmes, les réseaux et les dispositifs IoT et interpréter les données pour reconstruire des scénarios d'incident.

Considérer la volumétrie des données, le temps disponible, le matériel de copie et d'autres contraintes externes pour définir une stratégie de protection de données efficace.

Rédiger le document de traçabilité des actions effectuées pour assurer le suivi et la mise en application des actions identifiées.

Collecter des preuves de manière sécurisée, en préservant leur intégrité et en garantissant leur fiabilité pour assurer leur admissibilité devant un tribunal.

Interpréter les logs système, les journaux d'événements et les artefacts pour retracer les activités malveillantes et mesurer l'étendue des incidents.

Détecter, isoler et analyser des malwares dans les systèmes et les dispositifs IoT pour intervenir sur les incidents détectés.

Identifier les indicateurs de compromission (IoC) et les méthodes d'intrusion pour optimiser l'analyse de risque.

Extraire et analyser la mémoire volatile et examiner le trafic réseau pour identifier les processus en cours, les connexions réseau et les artefacts liés à des incidents.

Analyser les protocoles spécifiques à l'IoT pour comprendre les communications entre les objets connectés.

Rédiger des rapports techniques et légaux détaillés sur les résultats de l'analyse forensique et présenter clairement les conclusions, les découvertes et les recommandations pour garantir une traçabilité des données transmises.

Collaborer de manière interdisciplinaire, y compris avec des experts en sécurité, des juristes et des forces de l'ordre et assurer une coordination efficace pour une investigation complète.

Détecter les incidents techniques de sécurité en utilisant des algorithmes d'IA (apprentissage automatique et profond) pour identifier des schémas inhabituels et des activités suspectes.

Interpréter les alertes générées par les modèles d'IA et analyser les événements de sécurité pour retracer la chronologie des cyberattaques.

Développer des stratégies automatisées de réponse aux incidents en produisant des correctifs avec des outils tels que Kali Linux et en intégrant des normes telles que ISO 27035 pour remédier aux incidents.

Superviser les infrastructures de l'organisation et les événements de sécurité en utilisant un système de gestion des informations et des événements de sécurité (SIEM) pour détecter les menaces avant qu'elles ne perturbent ses activités.

Mettre en place des systèmes de détection en temps réel pour identifier les sources d'incidents et accroître la réactivité de traitement.

Bloquer proactivement les accès au système informatique pour prévenir les menaces.

Effectuer une analyse statique et/ou dynamique du code malveillant en déployant des méthodes telles que Kill Chain, Diamond Model, et la matrice MITRE ATT&CK pour qualification et catégorisation de l'incident.

Mettre en place un système de veille recensant l'OSINT, SOCMINT, HUMINT, et les informations du Deep et Dark web pour anticiper les évolutions des menaces et limiter l'exposition de l'entreprise et réduire la surface d'attaque.

Développer des stratégies de sécurité réseau et concevoir des architectures sécurisées pour les réseaux et les communications afin d'implémenter des protocoles et des mécanismes de sécurité.

Assurer la conformité aux normes de sécurité en vigueur et suivre les évolutions des réglementations liées à la sécurité des réseaux pour garantir une sécurité des pratiques.

Chiffrer les communications sensibles et mettre en place des réseaux privés virtuels (VPN) sécurisés afin de garantir

l'intégrité et la confidentialité des données transitant à travers les communications.

Mettre en place des outils de surveillance des flux de données et configurer des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) pour assurer une surveillance continue des activités réseau.

Interpréter les journaux et les données de surveillance pour repérer les anomalies et mettre en œuvre des technologies de détection des menaces et réagir rapidement à des activités suspectes ou malveillantes.

Effectuer des analyses de vulnérabilité sur les infrastructures réseau et mettre en place des correctifs de sécurité en appliquant des pratiques de gestion des risques pour remédier aux vulnérabilités identifiées et sécuriser le système.

Élaborer des plans d'intervention et coordonner les actions collaboratives nécessaires lors de la détection d'une activité malveillante pour une résolution efficace.

Documenter les configurations de sécurité mises en place en rédigeant des rapports d'incidents et d'analyses de sécurité et maintenir une documentation à jour sur les politiques de sécurité réseau pour garantir une traçabilité efficace.

Communiquer efficacement sur les enjeux de sécurité aux parties prenantes et sensibiliser les utilisateurs aux bonnes pratiques de sécurité des réseaux afin de minimiser les risques.

Blocs de compétences

RNCP40347BC01 — Concevoir et Mettre en œuvre de Systèmes intelligents Sécurisés

LISTE DE COMPÉTENCES

Évaluer le contexte environnemental et conduire une analyse approfondie du système d'information pour définir une architecture appropriée en se fondant sur le modèle fonctionnel et optimiser la mise en application.

Proposer des architectures techniques de référence conformes pour répondre aux besoins du projet IoT et de cybersécurité.

Organiser et piloter des revues d'architectures et de conceptions pour garantir la prise en compte des exigences initiales et des demandes d'évolutions du cahier des charges

Mettre en œuvre des processus de test robustes en intégrant harmonieusement les composants IoT et de cybersécurité pour garantir la qualité de la solution répondre au cahier des charges

Intégrer les principes de sécurité dès la conception de la solution IoT en adoptant l'approche "Secure by Design," et en respectant les meilleures pratiques et recommandations pour promouvoir la sécurité du système.

Analyser, calibrer et harmoniser l'architecture technique des solutions logicielles à connecter avec la plateforme IoT en validant leurs interopérabilités afin de garantir la robustesse du système.

Assurer la conformité de la solution IoT et de cybersécurité développée aux normes et réglementations en vigueur pour garantir la protection des données personnelles.

Auditer les architectures réseau en documentant les analyses conduites et les résultats des audits de sécurité IoT, pour identifier les points faibles dans l'écosystème IoT.

Planifier des tests d'intrusion éthiques sur les systèmes IoT en utilisant les outils de Kali Linux pour évaluer la robustesse des défenses du système.

Simuler des attaques ciblant les objets connectés à l'aide d'outils tels que nmap, metasploit ou armitage, pour identifier et analyser les vulnérabilités des systèmes IoT.

Analyser les configurations des équipements IoT et leurs mécanismes d'authentification en utilisant des outils adaptés pour tester la robustesse du système.

Identifier les risques potentiels pour la sécurité des systèmes IoT en les classant selon leur criticité pour prioriser les actions correctives.

Détecter des activités anormales ou suspectes dans les environnements IoT en interprétant les logs des dispositifs, des communications et des transactions en vue d'identifier des modèles de comportement et d'anticiper des incidents.

Renforcer la sécurité opérationnelle du système IoT en veillant au respect des règles éthiques en matière de traitement des données sensibles pour limiter la survenance des risques d'intrusion.

MODALITÉS D'ÉVALUATION

Projet pratique - Conception de l'architecture d'une solution IoT .

Mise en situation professionnelle - Rapport d'Audit IoT

Mise en situation professionnelle - Analyse des Configurations IoT .

RNCP40347BC02 — Elaborer un système d'intelligence artificielle et gérer des données, des identités et d'accès (IAM)

LISTE DE COMPÉTENCES

Créer des modèles prédictifs et de reconnaissance de motifs en exploitant des algorithmes d'apprentissage automatique pour analyser et traiter les données issues des dispositifs IoT.

Collecter, nettoyer et analyser de grandes quantités de données pour améliorer la prise de décision et la sécurité.

Configurer et administrer des solutions d'authentification robustes basées sur les principes Zero trust et Least Privilege, d'authentification multifactorielle et/ou adaptative pour limiter les risques d'intrusion.

Définir et déployer des politiques de gestion des accès et des privilèges liés à la gouvernance des identités (Identity and Access Governance) en conformité avec les normes de sécurité (Numeric Identity, Identity Lifecycle) en élaborant des matrices de rôles et d'accès limités par fonctions pour garantir une répartition des accès adaptée aux besoins métiers.

Intégrer des protocoles d'authentification et d'autorisation tels que Kerberos, WS-Federation, SAML v2, OAuth2.0, OIDC pour protéger les ressources de l'organisation.

Garantir l'interopérabilité du système IAM en s'appuyant sur le principe de fédération des identités (Identity Federation) pour assurer l'intégration fluide des systèmes et faciliter la navigation.

MODALITÉS D'ÉVALUATION

Projet pratique et soutenance orale - Conception d'une solution intelligente.

Projet, rapport et soutenance orale - Analyse et gestion de données.

Simulations pratiques – IAM

RNCP40347BC03 — Gérer et piloter un projet de mise en œuvre d'une solution IoT sécurisée by design

LISTE DE COMPÉTENCES

Réaliser une veille permanente sur les évolutions technologiques liées à l'IoT et à la cybersécurité, en anticipant et en accompagnant les changements organisationnels induits, afin d'intégrer les innovations pertinentes dans le projet et d'assurer l'adaptabilité du système.

Appliquer des normes de sécurité techniques spécifiques à la cybersécurité et à l'IoT (ISO 27001, NIST, CIS, etc.) pour interpréter et appliquer les exigences de ces normes dans le contexte des objets connectés.

Garantir le respect des règles éthiques liées à la sécurité, en tenant compte des données sensibles générées par les objets connectés et les informations sensibles découvertes lors des audits IoT pour garantir le respect de la réglementation en matière de traitement des données personnelles.

Planifier de manière détaillée les différentes phases du projet IoT et de cybersécurité, de la conception au déploiement afin d'assurer la réalisation du projet dans les temps impartis

Gérer les ressources, le budget et les délais du projet pour assurer la réalisation efficace des objectifs fixés.

Participer aux instances de pilotage (comité de pilotage) et définir des indicateurs de suivi de projet (KPIs) et des tableaux de bord pour assurer la coordination des tâches et une gestion efficace du projet.

Coordonner et communiquer de manière efficace et transparente avec les parties prenantes et experts de divers domaines tels que la sécurité, les systèmes, les réseaux, les logiciels, le big data, le cloud... etc afin de comprendre les besoins spécifiques de chaque spécialiste et promouvoir le suivi du projet.

Diriger et motiver les équipes dans une démarche inclusive tout au long du projet pour stimuler leur créativité et leur implication.

Encourager la collaboration, la créativité et l'innovation au sein des équipes de conception, de développement, de tests, d'intégration et de déploiement pour améliorer la cohésion d'équipe.

Recueillir les retours d'expérience utilisateurs et intégrer les remarques dans les demandes d'évolution des solutions IoT et de cybersécurité afin de perfectionner le système IoT et de garantir son accessibilité à tous les publics.

Identifier rapidement et les problèmes potentiels et mettre en place des processus de maintenance corrective et évolutive pour assurer la pérennité des solutions IoT et de cybersécurité.

Développer des actions de sensibilisation et de formation à la cybersécurité à destination des personnels de l'organisation pour prévenir la survenance du risque cyber.

MODALITÉS D'ÉVALUATION

Etudes de cas – Mise en place d'une politique de sécurité.

Mise en simulation – Gestion de Projet IoT en Cybersécurité .

Jeu de rôle – Animation d'équipe et gestion des conflits

Etude de cas – Suivi de projet

RNCP40347BC04 — Réaliser une analyse forensique

LISTE DE COMPÉTENCES

Identifier, extraire et analyser les traces numériques laissées dans les systèmes, les réseaux et les dispositifs IoT et interpréter les données pour reconstruire des scénarios d'incident.

Considérer la volumétrie des données, le temps disponible, le matériel de copie et d'autres contraintes externes pour définir une stratégie de protection de données efficace.

Rédiger le document de traçabilité des actions effectuées pour assurer le suivi et la mise en application des actions identifiées.

Collecter des preuves de manière sécurisée, en préservant leur intégrité et en garantissant leur fiabilité pour assurer leur admissibilité devant un tribunal.

Interpréter les logs système, les journaux d'événements et les artefacts pour retracer les activités malveillantes et mesurer l'étendue des incidents.

Détecter, isoler et analyser des malwares dans les systèmes et les dispositifs IoT pour intervenir sur les incidents détectés.

Identifier les indicateurs de compromission (IoC) et les méthodes d'intrusion pour optimiser l'analyse de risque.

Extraire et analyser la mémoire volatile et examiner le trafic réseau pour identifier les processus en cours, les connexions réseau et les artefacts liés à des incidents.

Analyser les protocoles spécifiques à l'IoT pour comprendre les communications entre les objets connectés.

Rédiger des rapports techniques et légaux détaillés sur les résultats de l'analyse forensique et présenter clairement les conclusions, les découvertes et les recommandations pour garantir une traçabilité des données transmises.

Collaborer de manière interdisciplinaire, y compris avec des experts en sécurité, des juristes et des forces de l'ordre et assurer une coordination efficace pour une investigation complète.

MODALITÉS D'ÉVALUATION

Mise en situation - Simulation d'Investigation Forensique

Rapport d'Analyse Forensique

Mise en situation Simulation de Témoignage Expert

Examen - Éthique et Confidentialité

RNCP40347BC05 — Détecter et traiter les incidents techniques

LISTE DE COMPÉTENCES

Détecter les incidents techniques de sécurité en utilisant des algorithmes d'IA (apprentissage automatique et profond) pour identifier des schémas inhabituels et des activités suspectes.

Interpréter les alertes générées par les modèles d'IA et analyser les événements de sécurité pour retracer la chronologie des cyberattaques.

Développer des stratégies automatisées de réponse aux incidents en produisant des correctifs avec des outils tels que Kali Linux et en intégrant des normes telles que ISO 27035 pour remédier aux incidents.

Superviser les infrastructures de l'organisation et les événements de sécurité en utilisant un système de gestion des informations et des événements de sécurité (SIEM) pour détecter les menaces avant qu'elles ne perturbent ses activités.

Mettre en place des systèmes de détection en temps réel pour identifier les sources d'incidents et accroître la réactivité de traitement.

Bloquer proactivement les accès au système informatique pour prévenir les menaces.

Effectuer une analyse statique et/ou dynamique du code malveillant en déployant des méthodes telles que Kill Chain, Diamond Model, et la matrice MITRE ATT&CK pour qualification et catégorisation de l'incident.

Mettre en place un système de veille recensant l'OSINT, SOCMINT, HUMINT, et les informations du Deep et Dark web pour anticiper les évolutions des menaces et limiter l'exposition de l'entreprise et réduire la surface d'attaque.

MODALITÉS D'ÉVALUATION

Mise en situation réelle – Gestion des Incidents de Sécurité avec l'Intelligence Artificielle

RNCP40347BC06 — Sécuriser les Réseaux et les Communications

LISTE DE COMPÉTENCES

Développer des stratégies de sécurité réseau et concevoir des architectures sécurisées pour les réseaux et les communications afin d'implémenter des protocoles et des mécanismes de sécurité.

Assurer la conformité aux normes de sécurité en vigueur et suivre les évolutions des réglementations liées à la sécurité des réseaux pour garantir une sécurité des pratiques.

Chiffrer les communications sensibles et mettre en place des réseaux privés virtuels (VPN) sécurisés afin de garantir l'intégrité et la confidentialité des données transitant à travers les communications.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La certification permet de travailler dans de nombreux secteurs d'activités, la cybersécurité et les technologies IoT étant omniprésents. Ci-après les types d'entreprises et secteurs d'activité les plus fréquents où les professionnels peuvent exercer :

- Technologies de l'Information et de la Communication (TIC)
- Industrie Manufacturière
- Santé et Secteur Pharmaceutique
- Énergie
- Transports
- Sécurité Nationale et Défense
- Entreprises de Cybersécurité
- Consulting en Sécurité Informatique
- Fournisseurs de Services IoT
- Services Financiers et Bancaires
- Startups Technologiques et Innovantes

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur IoT sécurisé
- Analyste en sécurité des données IoT
- Architecte IoT et cybersécurité
- Consultant en cybersécurité IoT
- Développeur sécuritaire IoT
- Ingénieur en cybersécurité et système intelligent
- Gestionnaire de projets en cybersécurité et smart system
- Chef de projet en IoT sécurisé
- Formateur et Responsable de la sécurité IoT
- Ingénieur en R&D en IoT sécurisé
- Directeur de la sécurité des systèmes 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)	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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Sont recevables les candidatures des titulaires d'un des diplômes suivants :

- Titre d'ingénieur diplômé conférant le grade de master (formations évaluées par la Commission des titres d'ingénieur, liste publiée au journal officiel) ;
- Diplôme de 3ème cycle habilité par les autorités universitaires (Diplôme national de master, DEA, DESS, ...) ou diplôme professionnel de niveau BAC + 5;
- Diplôme ou attestation de validation d'un niveau équivalent M1 pour des candidats ayant au moins trois ans d'expérience professionnelle en lien avec la formation visée.
- Titre inscrit au Répertoire national des certifications professionnelles (RNCP) niveau 7
- Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Conditions d'accès dérogatoires

a) Dans la limite de 40 % maximum de l'effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des acquis personnels et professionnels (VAPP), les candidatures de personnes, justifiant a minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation.

b) Par dérogation pour 30 % maximum du nombre d'apprenants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures de titulaires d'un des diplômes suivants :

- Diplôme ou attestation de validation d'un niveau équivalent M1 sans expérience professionnelle ou ayant moins de trois ans d'expérience professionnelle en lien avec la formation visée.
- Diplôme de licence (L3) ou grade de Licence ou titre inscrit au RNCP niveau 6 justifiant d'une expérience professionnelle de 3 ans minimum, en lien avec la formation visée

Le pourcentage total des dérogations prévues au a) et au b) ci-dessus ne doit pas excéder 40%.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

La composition de jury est de quatre membres :

- Un président de jury avec un statut d'enseignant
- Directeur des programmes de la formation continue CY Tech ou un responsable de formation des mastères

spécialisés

- Deux membres de jury issu du monde professionnel.

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	10 000 €
Selon la branche	7 700 € – 11 574 €

Prise en charge	Branches concernées
10 000 €	Valeur par défaut · 196 branches
11 574 €	CPNE Travail Temporaire, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEFP des commerces de gros
11 290 €	CPNEF de la Publicité, CPNEF de la presse et des agences de presse, CPNEF des Espaces de Loisirs, d'Attractions et Culturels (ELAC)
9 992 €	CPNEFP Mutualité
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires
9 055 €	CPNEFP Habillement succursaliste
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 750 €	CPNEFP Commerce à distance
8 700 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 647 €	CPNE Casinos
8 500 €	CPNEFP de la métallurgie
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date de décision	28/03/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	28/03/2028
Date de dernière délivrance possible	28/03/2032

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)
RNCP36072, RNCP37048, RNCP38140

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
Mastère Spécialisé ® Cybersecurité & Smart Systems à CY Tech

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40347/>