

Expert de la sécurité des données, des réseaux et des systèmes

RNCP42335 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 344t
Formacode(s)	31045
Code(s) ROME	M1801, M1802, M1805, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/05/2026
Date d'échéance	29/05/2029

Certificateur(s)

2600 · SIRET : 89344030500025

Résumé de la certification

OBJECTIFS ET CONTEXTE

Face à la croissance et à la sophistication des menaces cyber, amplifiées par la transformation numérique et l'essor des technologies connectées, les organisations doivent s'appuyer sur des professionnels qualifiés pour protéger leurs systèmes d'information et leurs données.

L'expert en cybersécurité joue un rôle central dans l'analyse des risques, la réalisation d'audits techniques et organisationnels, et la définition de stratégies de sécurité adaptées aux enjeux métiers et réglementaires. Il structure une démarche de sécurité proactive, intégrant la conformité légale, la gouvernance de la sécurité de l'information et la prise en compte des facteurs humains, en coordination avec la direction et le DPO.

Il contribue également au développement de solutions sécurisées et à l'amélioration continue de la résilience de l'organisation, notamment par des approches offensives maîtrisées (tests d'intrusion, Red Team). Enfin, il intervient dans la gestion des incidents et la préparation des plans de continuité et de reprise d'activité.

ACTIVITÉS VISÉES

- Gouvernance et gestion des risques SSI
- Conformité et audit réglementaire
- Résilience opérationnelle et gestion de crise
- Conseil en matière de sécurité des SI
- Supervision et analyse des événements de sécurité
- Ingénierie de la détection
- Investigation numérique et analyse forensique
- Réponse aux incidents (DFIR)
- Audit d'architecture et de configuration
- Audit applicatif et IA/ML
- Tests d'intrusion et simulation avancée
- Communication et cadre légal des audits
- Collecte et analyse du renseignement cyber
- Caractérisation et analyse des menaces
- Détection des campagnes malveillantes
- Production de renseignement et conformité

Management de projet en sécurité
Conception et mise en œuvre de solutions sécurisées
Justification et évaluation du projet
Retour d'expérience et amélioration continue

COMPÉTENCES ATTESTÉES

Piloter la gouvernance de la cybersécurité en élaborant et maintenant la PSSI (Politique de Sécurité des Systèmes d'Information), en assurant son adéquation avec les objectifs stratégiques et les politiques internes, notamment RSE, et en y intégrant les exigences d'accessibilité et d'inclusion (gestion des risques spécifiques, adaptation des mesures) pour tous les profils, pour garantir une protection cohérente et durable du SI de l'organisation.

Piloter la démarche de gestion des risques de cybersécurité (identification, analyse, traitement), en tenant compte des vulnérabilités techniques, organisationnelles et humaines ainsi que de l'équilibre entre performance, efficacité et sobriété des mesures envisagées, pour définir et arbitrer les mesures de sécurité nécessaires au renforcement de la résilience de l'organisation.

Garantir la conformité de l'organisation aux cadres juridiques (ex: RGPD, NIS 2, CRA, DORA, ...) et normatifs (ex: ISO 2700x) en supervisant les audits et en évaluant l'application des standards, pour limiter les risques juridiques et financiers et renforcer la confiance des parties prenantes.

Définir et superviser les stratégies de résilience opérationnelle, incluant l'élaboration et le test des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA), pour garantir la disponibilité des services critiques et limiter les interruptions d'activité en cas d'incident de sécurité ou de crise cyber.

Organiser et piloter la gestion de crise cyber, de la détection à la coordination des équipes, et superviser les plans de remédiation post-incident, pour contenir les impacts des attaques et rétablir un niveau de sécurité opérationnelle optimal dans les meilleurs délais.

Conseiller la direction sur la définition et le pilotage de la stratégie de sécurité de ses systèmes d'information, en s'appuyant sur les résultats de sa veille stratégique, réglementaire et technologique et sur ses analyses, pour orienter les choix de solutions et d'accompagnement face aux menaces identifiées et ajuster de manière proactive la posture de sécurité de l'organisation et des équipes.

Exploiter et interpréter les outils de détection et de protection (tels que SIEM, EDR/XDR, IDS/IPS, pare-feu) pour assurer la supervision continue de la sécurité du système d'information.

Analyser et qualifier les alertes de sécurité issues des plateformes de supervision (SOC) en corrélant les journaux d'événements et les indicateurs de compromission (IoCs), en veillant à la clarté, l'interprétabilité et l'accessibilité des informations à traiter, pour identifier les incidents avérés et permettre leur prise en charge.

Développer et maintenir des règles de détection (Detection Engineering), notamment au format YARA et SIGMA, pertinentes et proactives, basées sur les TTPs (Techniques, Tactiques et Procédures) des menaces, en corrélation avec le référentiel MITRE ATT&CK, tout en optimisant l'usage des ressources (arbitrage entre performance de détection, efficacité opérationnelle et sobriété des ressources de la plateforme) pour affiner les capacités du SIEM.

Mener une investigation numérique (Forensic), en reconstituant la chronologie détaillée d'un incident (timeline forensics), en examinant les artefacts système, la mémoire vive et les traces réseau, pour collecter et préserver les preuves numériques d'une intrusion tout au long de son déroulement.

Analyser la charge utile des logiciels malveillants (Reverse Engineering) pour comprendre leur fonctionnement, identifier leurs signatures et en extraire des indicateurs de compromission exploitables.

Piloter le processus de réponse aux incidents (DFIR) en appliquant les procédures de traitement et de reporting employés en CERT/CSIRT et en veillant à la coordination des actions ainsi qu'à la production des livrables documentaires selon les principes de la conception universelle, y compris dans un contexte de charge ou de tension élevée, pour contenir, éradiquer la menace, permettre la remédiation des systèmes affectés et en garantir la lecture par l'ensemble des profils types de destinataires.

Cadrer et conduire un audit d'architecture de sécurité (revue de conception, analyse des flux, positionnement des défenses) pour identifier les failles conceptuelles et les risques de contournement, en fonction du périmètre et des contraintes, notamment environnementales.

Mener un audit de configuration (boîte blanche/grise) des composants d'un SI (serveurs, postes, équipements réseau, cloud), pour vérifier leur conformité aux standards de durcissement et aux politiques de sécurité.

Auditer le code source d'une application pour identifier les failles de sécurité et les non-conformités aux bonnes pratiques de développement sécurisé.

Auditer la sécurité des systèmes d'Intelligence Artificielle et des modèles de Machine Learning (IA/ML) pour identifier les vulnérabilités spécifiques (ex: évasion, empoisonnement des données, extraction de modèle).

Conduire un test d'intrusion (pentest) sur un périmètre technique défini (systèmes, réseaux, applications web/mobiles) pour identifier et exploiter les vulnérabilités.

Piloter une simulation d'intrusion avancée (Red Team) en élaborant des scénarios d'attaque visant la persistance (infiltration, collecte, surveillance) par des techniques furtives (évasion, obfuscation), sans compromettre la sécurité réelle de l'organisation et des collaborateurs, afin d'évaluer la chaîne de détection et de réponse face à une menace non-bruyante.

Rédiger et restituer les résultats d'un audit selon les principes de la conception universelle (structure, lisibilité, accessibilité numérique des livrables) en adaptant la communication des vulnérabilités et des plans de remédiation à la maturité, au métier et aux besoins spécifiques du public cible, notamment en situation de handicap, pour en garantir la compréhension par tous les profils de lectorat et favoriser la mise en œuvre effective des mesures correctives.

Cadrer et conduire un audit technique en garantissant sa conformité au cadre légal (législation en vigueur), aux principes éthiques et au périmètre contractuel défini avec les parties prenantes, pour en assurer la fiabilité.

Collecter du renseignement d'origine multiple (OSINT, SOCMINT, GEOINT, HUMINT, etc.) en menant des investigations sur des cibles (entités, individus, infrastructures) dans le respect des mesures de prévention des risques psychosociaux liés à l'exposition à du contenu sensible (dark web, cybercriminalité, contenus traumatisants), pour identifier des signaux faibles et des traces numériques.

Appliquer le cycle du renseignement (orientation, collecte, traitement, analyse, diffusion) pour transformer des données numériques hétérogènes en renseignement exploitable (Cyber Threat Intelligence).

Caractériser les menaces (profils d'acteurs, motivations, TTPs, IoCs) en analysant les modes opératoires et les infrastructures (C2, domaines malveillants) pour anticiper les attaques futures.

Corréler les éléments techniques (IoCs, TTPs) avec le contexte stratégique et sociétal (géopolitique, financier, environnemental) pour identifier les groupes d'attaquants, comprendre leurs motivations et leurs méthodes d'action hybrides (ex: manipulation de l'information, ingérence).

Détecter des campagnes d'ingénierie sociale (phishing, spear phishing, vishing, etc.) en analysant les vecteurs d'attaque et les artefacts associés, pour identifier les tentatives de manipulation visant les individus, les processus organisationnels et/ou les systèmes d'information.

Conduire les activités de collecte et d'investigation dans le respect des cadres éthiques et légaux (Code pénal, RGPD) relatifs à la lutte contre la cybercriminalité, pour produire des éléments de preuve recevables et documenter les menaces et incidents dans un cadre sécurisé.

Produire des rapports de CTI (stratégiques, tactiques, opérationnels) selon les principes de la conception universelle : trois strates de lecture explicitées (executive summary, synthèse tactique, annexes techniques), accessibilité numérique des livrables, alternatives textuelles pour les visualisations (heatmaps, graphes d'attribution, matrices MITRE ATT&CK) pour orienter les décisions de l'organisation et sa posture de défense.

Cadrer et piloter un projet en sécurité des systèmes d'information (définition de la gouvernance/instances de décision et des objectifs, allocation des ressources) en appliquant une méthodologie de gestion de projet adaptée au contexte et en documentant ses actions, pour assurer le bon déroulement du projet en alignement avec les objectifs.

Animer les équipes mobilisées dans un projet en sécurité des systèmes d'information, en veillant à la coordination de leurs interventions et en adaptant l'organisation du travail aux risques et aux besoins spécifiques, notamment en cas de situation de handicap, pour maintenir leur engagement tout au long du projet.

Concevoir une solution (à dominance technique, organisationnelle ou procédurale) en appliquant les principes "Secure by Design" notamment la définition des politiques de gestion des identités et des accès (IAM, moindre privilège), et en arbitrant les choix de conception entre performance, efficacité opérationnelle et sobriété des ressources mobilisées, pour répondre aux objectifs de résilience identifiés dans les environnements on-premise ou cloud.

Mettre en œuvre la solution conçue (à dominance technique, organisationnelle ou procédurale) et définir les processus de son maintien en condition opérationnelle ou de son pilotage (administration, revue, mise à jour), pour en garantir le déploiement maîtrisé et l'intégration durable dans l'environnement cible.

Argumenter et défendre la pertinence des choix techniques, méthodologiques et d'analyse pour démontrer l'atteinte des objectifs du projet.

Évaluer l'impact environnemental et de souveraineté du projet en analysant les ressources mobilisées (matérielles, logicielles, énergétiques) pour justifier les choix au regard des enjeux de l'informatique durable (green IT) et contribuer à une démarche plus globale de responsabilité.

Conduire le retour d'expérience du projet en évaluant l'atteinte des objectifs du projet et en documentant les leçons apprises (difficultés, succès) selon les principes de la conception universelle, pour alimenter la démarche

d'amélioration continue à destination de l'ensemble des profils types impliqués (équipe projet, futurs porteurs, direction, audit qualité).

Blocs de compétences

RNCP42335BC01 — Piloter la stratégie de sécurité des systèmes d'information d'une organisation

LISTE DE COMPÉTENCES

Piloter la gouvernance de la cybersécurité en élaborant et maintenant la PSSI (Politique de Sécurité des Systèmes d'Information), en assurant son adéquation avec les objectifs stratégiques et les politiques internes, notamment RSE, et en y intégrant les exigences d'accessibilité et d'inclusion (gestion des risques spécifiques, adaptation des mesures) pour tous les profils, pour garantir une protection cohérente et durable du SI de l'organisation.

Piloter la démarche de gestion des risques de cybersécurité (identification, analyse, traitement), en tenant compte des vulnérabilités techniques, organisationnelles et humaines ainsi que de l'équilibre entre performance, efficacité et sobriété des mesures envisagées, pour définir et arbitrer les mesures de sécurité nécessaires au renforcement de la résilience de l'organisation.

Garantir la conformité de l'organisation aux cadres juridiques (ex: RGPD, NIS 2, CRA, DORA, ...) et normatifs (ex: ISO 2700x) en supervisant les audits et en évaluant l'application des standards, pour limiter les risques juridiques et financiers et renforcer la confiance des parties prenantes.

Définir et superviser les stratégies de résilience opérationnelle, incluant l'élaboration et le test des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA), pour garantir la disponibilité des services critiques et limiter les interruptions d'activité en cas d'incident de sécurité ou de crise cyber.

Organiser et piloter la gestion de crise cyber, de la détection à la coordination des équipes, et superviser les plans de remédiation post-incident, pour contenir les impacts des attaques et rétablir un niveau de sécurité opérationnelle optimal dans les meilleurs délais.

Conseiller la direction sur la définition et le pilotage de la stratégie de sécurité de ses systèmes d'information, en s'appuyant sur les résultats de sa veille stratégique, réglementaire et technologique et sur ses analyses, pour orienter les choix de solutions et d'accompagnement face aux menaces identifiées et ajuster de manière proactive la posture de sécurité de l'organisation et des équipes.

MODALITÉS D'ÉVALUATION

Étude de cas d'une entreprise qui souhaite renforcer sa posture de sécurité face aux menaces de cyberattaques. Production d'un rapport et soutenance devant un jury d'experts.

Mise en situation au travers d'un scénario de crise suivie de l'écriture d'une présentation contenant un compte-rendu technique et situationnel.

RNCP42335BC02 — Détecter les intrusions et traiter les incidents numériques

LISTE DE COMPÉTENCES

Exploiter et interpréter les outils de détection et de protection (tels que SIEM, EDR/XDR, IDS/IPS, pare-feu) pour assurer la supervision continue de la sécurité du système d'information.

Analyser et qualifier les alertes de sécurité issues des plateformes de supervision (SOC) en corrélant les journaux d'événements et les indicateurs de compromission (IoCs), en veillant à la clarté, l'interprétabilité et l'accessibilité des informations à traiter, pour identifier les incidents avérés et permettre leur prise en charge.

Développer et maintenir des règles de détection (Detection Engineering), notamment au format YARA et SIGMA, pertinentes et proactives, basées sur les TTPs (Techniques, Tactiques et Procédures) des menaces, en corrélation avec le référentiel MITRE ATT&CK, tout en optimisant l'usage des ressources (arbitrage entre performance de détection, efficacité opérationnelle et sobriété des ressources de la plateforme) pour affiner les capacités du SIEM.

Mener une investigation numérique (Forensic), en reconstituant la chronologie détaillée d'un incident (timeline forensics), en examinant les artefacts système, la mémoire vive et les traces réseau, pour collecter et préserver les preuves numériques d'une intrusion tout au long de son déroulement.

Analyser la charge utile des logiciels malveillants (Reverse Engineering) pour comprendre leur fonctionnement, identifier leurs signatures et en extraire des indicateurs de compromission exploitables.

Piloter le processus de réponse aux incidents (DFIR) en appliquant les procédures de traitement et de reporting employés en CERT/CSIRT et en veillant à la coordination des actions ainsi qu'à la production des livrables documentaires selon les principes de la conception universelle, y compris dans un contexte de charge ou de tension élevée, pour contenir, éradiquer la menace, permettre la remédiation des systèmes affectés et en garantir la lecture

par l'ensemble des profils types de destinataires.

MODALITÉS D'ÉVALUATION

Mise en situation : le candidat est chargé de la protection des systèmes d'information d'une entreprise ciblée par des cyberattaques. Le candidat doit mettre en place une stratégie de protection. Production d'un rapport et soutenance devant un jury d'experts.

RNCP42335BC03 — Mener des audits techniques et des simulations d'intrusion

LISTE DE COMPÉTENCES

Cadrer et conduire un audit d'architecture de sécurité (revue de conception, analyse des flux, positionnement des défenses) pour identifier les failles conceptuelles et les risques de contournement, en fonction du périmètre et des contraintes, notamment environnementales.

Mener un audit de configuration (boîte blanche/grise) des composants d'un SI (serveurs, postes, équipements réseau, cloud), pour vérifier leur conformité aux standards de durcissement et aux politiques de sécurité.

Auditer le code source d'une application pour identifier les failles de sécurité et les non-conformités aux bonnes pratiques de développement sécurisé.

Auditer la sécurité des systèmes d'Intelligence Artificielle et des modèles de Machine Learning (IA/ML) pour identifier les vulnérabilités spécifiques (ex: évasion, empoisonnement des données, extraction de modèle).

Conduire un test d'intrusion (pentest) sur un périmètre technique défini (systèmes, réseaux, applications web/mobiles) pour identifier et exploiter les vulnérabilités.

Piloter une simulation d'intrusion avancée (Red Team) en élaborant des scénarios d'attaque visant la persistance (infiltration, collecte, surveillance) par des techniques furtives (évasion, obfuscation), sans compromettre la sécurité réelle de l'organisation et des collaborateurs, afin d'évaluer la chaîne de détection et de réponse face à une menace non-bruyante.

Rédiger et restituer les résultats d'un audit selon les principes de la conception universelle (structure, lisibilité, accessibilité numérique des livrables) en adaptant la communication des vulnérabilités et des plans de remédiation à la maturité, au métier et aux besoins spécifiques du public cible, notamment en situation de handicap, pour en garantir la compréhension par tous les profils de lectorat et favoriser la mise en œuvre effective des mesures correctives.

Cadrer et conduire un audit technique en garantissant sa conformité au cadre légal (législation en vigueur), aux principes éthiques et au périmètre contractuel défini avec les parties prenantes, pour en assurer la fiabilité.

MODALITÉS D'ÉVALUATION

Mise en situation : audit technique d'une organisation. Production d'un rapport technique détaillé et présentation devant un jury d'experts.

RNCP42335BC04 — Analyser et anticiper les menaces numériques pesant sur une organisation

LISTE DE COMPÉTENCES

Collecter du renseignement d'origine multiple (OSINT, SOCMINT, GEOINT, HUMINT, etc.) en menant des investigations sur des cibles (entités, individus, infrastructures) dans le respect des mesures de prévention des risques psychosociaux liés à l'exposition à du contenu sensible (dark web, cybercriminalité, contenus traumatisants), pour identifier des signaux faibles et des traces numériques.

Appliquer le cycle du renseignement (orientation, collecte, traitement, analyse, diffusion) pour transformer des données numériques hétérogènes en renseignement exploitable (Cyber Threat Intelligence).

Caractériser les menaces (profils d'acteurs, motivations, TTPs, IoCs) en analysant les modes opératoires et les infrastructures (C2, domaines malveillants) pour anticiper les attaques futures.

Corréler les éléments techniques (IoCs, TTPs) avec le contexte stratégique et sociétal (géopolitique, financier, environnemental) pour identifier les groupes d'attaquants, comprendre leurs motivations et leurs méthodes d'action hybrides (ex: manipulation de l'information, ingénierie).

Détecter des campagnes d'ingénierie sociale (phishing, spear phishing, vishing, etc.) en analysant les vecteurs d'attaque et les artefacts associés, pour identifier les tentatives de manipulation visant les individus, les processus organisationnels et/ou les systèmes d'information.

Conduire les activités de collecte et d'investigation dans le respect des cadres éthiques et légaux (Code pénal, RGPD) relatifs à la lutte contre la cybercriminalité, pour produire des éléments de preuve recevables et documenter les menaces et incidents dans un cadre sécurisé.

Produire des rapports de CTI (stratégiques, tactiques, opérationnels) selon les principes de la conception universelle :

trois strates de lecture explicitées (executive summary, synthèse tactique, annexes techniques), accessibilité numérique des livrables, alternatives textuelles pour les visualisations (heatmaps, graphes d'attribution, matrices MITRE ATT&CK) pour orienter les décisions de l'organisation et sa posture de défense.

MODALITÉS D'ÉVALUATION

Mise en situation : le candidat doit mener une enquête d'investigation complète en sources ouvertes (OSINT) et analyser des traces numériques pour caractériser une menace. Le candidat doit remettre un rapport de Cyber Threat Intelligence (CTI).

RNCP42335BC05 — Piloter un projet visant le renforcement de la résilience des systèmes d'information

LISTE DE COMPÉTENCES

Cadrer et piloter un projet en sécurité des systèmes d'information (définition de la gouvernance/instances de décision et des objectifs, allocation des ressources) en appliquant une méthodologie de gestion de projet adaptée au contexte et en documentant ses actions, pour assurer le bon déroulement du projet en alignement avec les objectifs.

Animer les équipes mobilisées dans un projet en sécurité des systèmes d'information, en veillant à la coordination de leurs interventions et en adaptant l'organisation du travail aux risques et aux besoins spécifiques, notamment en cas de situation de handicap, pour maintenir leur engagement tout au long du projet.

Concevoir une solution (à dominance technique, organisationnelle ou procédurale) en appliquant les principes "Secure by Design" notamment la définition des politiques de gestion des identités et des accès (IAM, moindre privilège), et en arbitrant les choix de conception entre performance, efficacité opérationnelle et sobriété des ressources mobilisées, pour répondre aux objectifs de résilience identifiés dans les environnements on-premise ou cloud.

Mettre en œuvre la solution conçue (à dominance technique, organisationnelle ou procédurale) et définir les processus de son maintien en condition opérationnelle ou de son pilotage (administration, revue, mise à jour), pour en garantir le déploiement maîtrisé et l'intégration durable dans l'environnement cible.

Argumenter et défendre la pertinence des choix techniques, méthodologiques et d'analyse pour démontrer l'atteinte des objectifs du projet.

Évaluer l'impact environnemental et de souveraineté du projet en analysant les ressources mobilisées (matérielles, logicielles, énergétiques) pour justifier les choix au regard des enjeux de l'informatique durable (green IT) et contribuer à une démarche plus globale de responsabilité.

Conduire le retour d'expérience du projet en évaluant l'atteinte des objectifs du projet et en documentant les leçons apprises (difficultés, succès) selon les principes de la conception universelle, pour alimenter la démarche d'amélioration continue à destination de l'ensemble des profils types impliqués (équipe projet, futurs porteurs, direction, audit qualité).

MODALITÉS D'ÉVALUATION

Soutenance de projet en sécurité des systèmes d'information : le candidat doit soutenir un projet professionnel. Ce projet doit démontrer la capacité du candidat à renforcer la résilience des systèmes d'information, que ce soit par des actions à dominance technique ou organisationnelle.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert de la sécurité des données, des réseaux et des systèmes exerce principalement au sein d'entreprises de services du numérique (ESN), de cabinets de conseil spécialisés en cybersécurité, ou directement dans les directions des systèmes d'information (DSI) d'organisations de toute taille et de tout secteur. Il intervient également au sein de structures dédiées telles que les centres opérationnels de sécurité (SOC), les équipes de réponse aux incidents (CERT/CSIRT) ou les cellules de renseignement sur les menaces (CTI).

Les secteurs d'activités concernés sont variés : banque, assurance et services financiers, industries de défense et aérospatiale, énergie et infrastructures critiques, santé, télécommunications, administrations publiques, e-commerce et grande distribution. L'expert peut exercer en tant que salarié, consultant ou prestataire, en mode projet ou en exploitation, dans des environnements allant de la PME aux grands groupes internationaux.

TYPE D'EMPLOIS ACCESSIBLES

Analyste cybersécurité - Architecte cybersécurité - Auditeur technique / Pentester - Consultant en sécurité informatique - DevSecOps - Expert cybersécurité - Ingénieur R&D en sécurité - Responsable de la réponse à incident (DFIR) - Responsable de la sécurité des systèmes d'information (RSSI) - Responsable / analyse SOC (Security

RÉGLEMENTATIONS D'ACTIVITÉ

Un expert en cybersécurité ne relève pas d'une activité réglementée. En revanche, le domaine de la cybersécurité présente un certain nombre de réglementations que cet expert doit maîtriser et faire respecter, dont :

- Règlement Général sur la Protection des Données (RGPD)
- Directives NIS et NIS 2
- Cyber Resilience Act (CRA)
- Digital Operational Resilience Act (DORA)
- Loi de Programmation Militaire (LPM)
- Normes internationales et sectorielles :
 - o La suite ISO/CEI 2700x (notamment ISO 27000, 27001, 27002 et 27005)
 - o Payment Card Industry Data Security Standard (PCI DSS)
 - o IEC 62443
- Instructions Interministérielles (ex: II901 et IGI1300) et la réglementation concernant les articles contrôlés de la sécurité des systèmes d'information (ACSSI)
- Référentiels d'exigences spécifiques de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) :
 - o Prestataire d'Audit de la Cybersécurité (PACS)
 - o Prestataire de Détection des Incidents de Sécurité (PDIS)
 - o Prestataire de Réponse aux Incidents de Sécurité (PRIS)
 - o Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI)

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, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'un titre ou diplôme de niveau 6 minimum (en mathématiques, informatique, numérique ou sur un domaine connexe à la cybersécurité) ou équivalent (diplôme étranger...) ou d'une expérience professionnelle équivalente. Cette équivalence sera appréciée par une commission d'admission sur la base d'une étude complète du profil du candidat.

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

Le jury est composé de 4 membres dont 2 membres externes, professionnels de la cybersécurité

Base légale

Date de décision	29/05/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	29/05/2029
Date de dernière délivrance possible	29/05/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	73	2	96 %	—
2024	66	4	100 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP38951

CORRESPONDANCES (PAR BLOCS)

RNCP37989, RNCP38951, RNCP39999, RNCP40640

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42335/>