Expert en développement de solutions de cybersécurité

RNCP42939 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1802, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/10/2026
Date d'échéance	30/10/2029

Certificateur(s)

ASSOCIATION D'ENSEIGNEMENT TECHNIQUE SUPERIEUR AN21 ACADEMIE NUMERIQUE DU XXIEME SIECLE · SIRET : 85137784600031

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CODA	92219486500031	Former et organiser l'évaluation
CSB EDUCATION GROUP	92991594000019	Former et organiser l'évaluation
DRS SCHOOL	85398915000018	Former et organiser l'évaluation
HECTEN	94943720600020	Former et organiser l'évaluation
IFIR ARL (AIN-RHONE-LOIRE)	38134879600024	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Expert en développement de solutions de cybersécurité conçoit, déploie et pilote la stratégie de sécurité des systèmes d'information d'une organisation, dans un contexte de multiplication et de sophistication croissante des cybermenaces.

Face à l'accélération de la transformation numérique, au renforcement du cadre réglementaire européen — NIS2, DORA, Cyber Resilience Act — et à la généralisation des outils à capacités décisionnelles automatisées, les organisations de toutes tailles doivent se doter de compétences expertes pour protéger leur patrimoine informationnel et assurer leur résilience opérationnelle. Cette demande est particulièrement forte au sein des PME, des ETI et des collectivités territoriales, qui ne disposent pas toujours des ressources internes pour constituer une équipe de sécurité dédiée.

La certification atteste de la capacité à élaborer une stratégie de cybersécurité et à en piloter la mise en conformité réglementaire, à construire et intégrer des solutions de sécurité mobilisant les technologies émergentes, à assurer la supervision et la maintenance des dispositifs déployés — y compris les outils de détection automatisée — et à encadrer une équipe dans un contexte de gestion de projet et de crise.

Le titulaire exerce en autonomie comme responsable de la sécurité des systèmes d'information, architecte sécurité, consultant en cyber-résilience et gouvernance, ingénieur détection et réponse ou responsable de centre opérationnel

de sécurité. Il intervient dans des contextes variés : chez les acteurs dont la cybersécurité est le cœur de métier — éditeurs, sociétés de services numériques, cabinets d'audit et de conseil, SOC mutualisés — comme au sein d'organisations de tous secteurs cherchant à renforcer leur sécurité, y compris celles qui font appel à une expertise externalisée.

ACTIVITÉS VISÉES

L'Expert en développement de solutions de cybersécurité intervient sur l'ensemble du cycle de vie de la sécurité des systèmes d'information, depuis la définition de la stratégie jusqu'à l'exploitation des solutions déployées. Il conjugue une expertise technique de haut niveau — construction de solutions, sécurisation des architectures, tests d'intrusion, supervision des dispositifs de détection — avec une capacité de pilotage stratégique, de mise en conformité réglementaire et d'encadrement d'équipe. Il exerce en autonomie, dans des organisations de toutes tailles et de tous secteurs, en tenant compte de l'évolution permanente des menaces et des environnements technologiques.
Ses activités sont réparties en cinq grands domaines.
Définition de la stratégie de cybersécurité et pilotage des projets associés
Réaliser une veille technologique et réglementaire sur les menaces, les vulnérabilités, les technologies émergentes et le cadre normatif applicable — NIS2, DORA, Cyber Resilience Act, RGPD, systèmes à logique décisionnelle automatisée, IoT/OT et cyber-robotique
Analyser le contexte et les risques de l'organisation, cartographier son système d'information et évaluer sa maturité en cybersécurité
Définir la stratégie et la politique de sécurité de l'information
Piloter les projets de cybersécurité en choisissant et en justifiant les méthodologies les plus adaptées au contexte
Conception et développement de solutions mobilisant les technologies émergentes
Auditer la sécurité des solutions existantes afin d'en identifier les vulnérabilités
Sélectionner les scénarios de développement de solutions au regard des besoins identifiés
Déployer des dispositifs de surveillance automatisée et construire les protocoles d'utilisation et de mise à jour réglementaire associés
Développer des solutions intégrant des outils à capacités décisionnelles automatisées et évaluer leur pertinence au regard du projet
Configurer les équipements de sécurité nécessaires à la mise en œuvre des solutions
Déploiement des solutions de sécurité au sein du système d'information
Intégrer les solutions de cybersécurité développées dans le système d'information de l'organisation
Concevoir et sécuriser les architectures réseau
Mettre en œuvre la gestion des identités et des accès
Déployer des solutions cryptographiques adaptées aux besoins de confidentialité et d'intégrité
Conduire des tests de pénétration afin d'évaluer la robustesse des environnements sécurisés
Exploitation, supervision et maintenance des solutions déployées
Superviser les solutions déployées, y compris les outils de détection automatisée SIEM, XDR et SOAR, en évaluant la pertinence des alertes et des faux positifs et en ajustant les seuils de déclenchement
Gérer les remontées des utilisateurs et le cycle de maintenance corrective et évolutive
Résoudre les incidents complexes et conduire les investigations post-incident
Vérifier l'intégrité des outils de surveillance après un incident
Assurer la traçabilité des modifications et la documentation technique des solutions
Encadrement d'équipe et pilotage de la communication en cybersécurité
Encadrer une équipe au quotidien et dans le cadre de projets de cybersécurité
Conduire les réunions et piloter les activités dans le respect du cadre légal et réglementaire
Communiquer avec les parties prenantes et les instances dirigeantes de l'organisation
Sensibiliser les collaborateurs aux risques de cybersécurité, notamment ceux liés à l'usage non encadré des outils à capacités autonomes

COMPÉTENCES ATTESTÉES

Définir une stratégie de sécurisation et de contrôle afin d'apporter une réponse adaptée au regard des risques identifiés et des évolutions du domaine
Mettre en œuvre une veille efficiente sur les dernières innovations technologiques applicables et impactantes à l’entreprise afin de comprendre les technologies en évolution et envisager des solutions adaptées pour le futur
Analyser les besoins de sécurité et le contexte des menaces propres à chacune des technologies afin d’élaborer des solutions en cohérence avec les priorités stratégiques, les besoins du client et ses performances

Définir les spécifications générales afin de formuler un tableau des exigences techniques détaillées
Choisir une méthodologie de gestion de projet adaptée et l'appliquer au pilotage des projets de cybersécurité afin de garantir un résultat respectant les exigences du cahier des charges
Communiquer auprès de l'équipe et du commanditaire afin de garantir des prises de décision argumentées facilitant le déroulement et le déploiement du projet
Réaliser un audit de sécurité sur les solutions existantes et outils utilisés afin de définir un plan de remise en conformité des équipements sensibles et vulnérables
Sélectionner des scénarii de développement de solutions potentielles afin de retenir la solution la plus adaptée aux exigences internes et externes
Développer une solution de sécurité afin de garantir un résultat respectant les normes et réglementations en vigueur
Construire un plan d'automatisation afin d'élargir au maximum le périmètre d'action de l'outil de surveillance cyber
Développer une solution intégrant des outils à capacités décisionnelles automatisées et évaluer sa pertinence au regard du projet
Sélectionner et configurer les différents équipements afin de renforcer la sécurité des systèmes embarqués
Valider la solution sur les aspects de sécurité afin de garantir la faisabilité de l'architecture dans les systèmes réseaux avant sa mise en œuvre
Conduire un plan de tests techniques afin de contrôler la qualité du code, la performance et la sécurité de la solution
Déployer la solution en communiquant tous les protocoles nécessaires aux équipes d'exploitation et de maintenance afin de garantir la réalisation des bénéfices attendus de la solution
Superviser l'assistance auprès des parties prenantes en charge de l'installation de la solution en production afin de résoudre les dysfonctionnements de la solution
Élaborer des scénarii d'évolution de la solution afin de garantir la cohérence globale de la solution
Mettre en exploitation la solution en veillant à son adaptation au regard des besoins utilisateurs afin de faciliter son appropriation et garantir la fiabilité de la détection.
Résoudre des opérations de maintenance complexes afin d'évaluer les vulnérabilités, les menaces et de les corriger
Rendre compte des incidents et dysfonctionnements de la solution afin de contribuer à l'amélioration continue de la solution ainsi qu'à sa bonne diffusion auprès des utilisateurs
Constituer, gérer et animer une équipe projet en mettant en œuvre des méthodes et des outils efficients pour faciliter la réalisation du projet et travailler efficacement avec les parties prenantes et décisionnaires
Conduire des réunions de projet afin de faciliter l'avancement du projet, partager les informations, prendre des décisions sur des sujets critiques et assumer les responsabilités associées
Mettre en place une communication adaptée afin de faciliter l'adhésion de l'ensemble des parties prenantes

Blocs de compétences

RNCP42939BC01 — Mettre en place une stratégie de cybersécurité dans une démarche de développement de solutions

LISTE DE COMPÉTENCES

Définir une stratégie de sécurisation et de contrôle en tenant compte du contexte technique, organisationnel et légal de l'entreprise afin d'apporter une réponse adaptée au regard des risques identifiés et des évolutions du domaine
Mettre en œuvre une veille efficiente sur les dernières innovations technologiques applicables et impactantes à l'entreprise afin de comprendre les technologies en évolution et envisager des solutions adaptées pour le futur (cybersécurité IT, IoT et OT, cyber-robotique, intelligence artificielle, LLMs, …)
Analyser les besoins de sécurité et le contexte des menaces propres à chacune des technologies afin d'élaborer des solutions en cohérence avec les priorités stratégiques, les besoins du client et ses performances
Définir les spécifications générales (techniques, risques, délais, qualité, budget…) en s'appuyant sur les résultats de l'analyse des besoins du client afin de formuler un tableau des exigences techniques détaillées
Choisir une méthodologie de gestion de projet adaptée à une organisation et l'appliquer afin de garantir un résultat respectant les exigences techniques, fonctionnelles et normatives du cahier des charges.
Communiquer auprès de l'équipe et du commanditaire en organisant et animant des réunions de travail et des comités de suivi afin de garantir des prises de décision argumentées facilitant le déroulement du projet et le déploiement du projet

MODALITÉS D'ÉVALUATION

Étude de cas présentant le profil d'une entreprise : le candidat choisit et applique les outils de veille les plus adaptés.

Il conduit une analyse stratégique afin d'identifier les forces-faiblesses-opportunités-menaces de l'écosystème de la cybersécurité de l'entreprise dans le but d'établir un diagnostic macro-environnement en anticipant les évolutions ultérieures.
Étude de cas portant sur un rapport d'audit d'entreprise :
le candidat identifie les besoins en sécurité en vue de proposer des solutions pertinentes.
Il doit reformuler les besoins en matière de sécurité du client et élaborer une liste d'exigences catégorisées et priorisées.
Etude de cas avec restitution orale, présentant le profil d'une entreprise :
le candidat élabore la démarche projet de cybersécurité la plus adaptée au contexte — planning, organisation, allocation des ressources et indicateurs de suivi — puis la présente et la défend oralement devant un évaluateur. La restitution orale comprend un temps de présentation structurée suivi d'un échange de questions réponses permettant au candidat de justifier ses choix méthodologiques et de démontrer sa capacité à adapter son discours à son interlocuteur

PRÉREQUIS À L'ENTRÉE

L'accès à ce bloc pris de façon indépendante est ouvert aux candidats justifiant d'une expérience ou d'une formation préalable en systèmes d'information ou en cybersécurité leur permettant de disposer des fondamentaux nécessaires — compréhension des architectures de systèmes d'information, connaissance des principes de base de la sécurité informatique et du cadre réglementaire applicable. Cet accès est notamment adapté aux professionnels exerçant des fonctions de gouvernance, de management des systèmes d'information, de conseil ou de pilotage, souhaitant développer ou faire reconnaître leurs compétences en stratégie de cybersécurité. L'admission est prononcée après étude du dossier de candidature et entretien individuel permettant de vérifier l'adéquation entre le profil du candidat et les exigences du bloc.

RNCP42939BC02 — Construire des solutions de sécurité en utilisant les technologies émergentes

LISTE DE COMPÉTENCES

Réaliser un audit de sécurité sur les solutions existantes et outils utilisés en listant leurs forces et leurs vulnérabilités afin de définir un plan de remise en conformité des équipements sensibles et vulnérables
Sélectionner des scénarii de développement de solutions potentielles en s'appuyant sur une étude de faisabilité et selon des critères bien définis afin de retenir la solution la plus adaptée par rapport aux exigences internes et externes exprimées par le client
Développer une solution de sécurité en appliquant les bonnes pratiques de cybersécurité afin de garantir un résultat respectant les normes et réglementations en vigueur en anticipant leurs évolutions éventuelles
Construire un plan d'automatisation s'appuyant sur les actions identifiées comme étant à risque afin d'élargir au maximum le périmètre d'action de l'outil de surveillance cyber
Développer une solution intégrant des outils à capacités décisionnelles automatisées en s'appuyant sur une analyse fine des fonctionnalités et évaluer sa pertinence par rapport au projet
Sélectionner et configurer les différents équipements en appliquant les bonnes pratiques cyber sécurité afin de renforcer la sécurité des systèmes embarqués

MODALITÉS D'ÉVALUATION

Étude de cas avec restitution orale, portant sur un audit de sécurité d'une entreprise fictive : le candidat doit établir le programme d'audit prenant en compte les référentiels de sécurité agréés. Le candidat formule différents scénarii de développement prenant en compte les risques intrinsèques. Il présente le programme d'audit lors d'un entretien oral et argumente ses choix par rapport aux préconisations définies en lien avec les exigences du client.
Questionnaire à visée professionnelle : le candidat répond aux différentes questions posées portant sur sa maîtrise professionnelle en matière de législation et des normes sécurité sur tous les aspects de protection de la donnée.
Mise en situation portant sur le déploiement d'un dispositif de surveillance automatisée au sein d'un environnement professionnel fictif, le candidat identifie et justifie les flux de données à surveiller en fonction des risques identifiés dans le contexte fourni. Il conçoit et paramètre un modèle de traitement automatisé adapté, en sélectionnant les données pertinentes et en appliquant les techniques de manipulation appropriées. Il rédige un protocole d'utilisation et de maintenance de l'outil dans le respect de la conformité règlementaire
Mise en situation portant sur l'implémentation d'un outil de surveillance : le candidat sélectionne la technologie adaptée et réalise des tests pour affiner le fonctionnement de l'outil
Mise en situation portant sur la sécurisation d'un système embarqué ou d'un objet connecté, le candidat configure, implémente et teste la sécurité du système. Il présente lors d'un entretien oral sa sélection et le résultat obtenu

PRÉREQUIS À L'ENTRÉE

L'accès à ce bloc pris de façon indépendante est ouvert aux candidats justifiant d'une expérience ou d'une formation préalable attestant de la maîtrise des fondamentaux techniques nécessaires : bases en développement logiciel, compréhension des architectures logicielles et applicatives, et connaissance des principes de la sécurité offensive et défensive. La maîtrise de ces prérequis techniques est vérifiée lors de l'admission, à travers l'étude du dossier de candidature, un entretien individuel et, le cas échéant, un test technique permettant de s'assurer que le candidat dispose du niveau requis pour aborder les compétences d'audit de sécurité, de développement de solutions et d'exploitation de vulnérabilités que comporte ce bloc.

RNCP42939BC03 — Intégrer des solutions de sécurité dans le système d'information

LISTE DE COMPÉTENCES

Valider la solution sur les aspects de sécurité en construisant un prototype afin de garantir la faisabilité de l'architecture dans les systèmes réseaux avant sa mise en œuvre.
Conduire un plan de tests techniques en déployant des méthodologies de tests afin de contrôler la qualité du code, la performance et la sécurité de la solution.
Déployer la solution en communiquant tous les protocoles nécessaires aux équipes d'exploitation et de maintenance afin de garantir la réalisation des bénéfices attendus de la solution
Superviser l'assistance auprès des parties prenantes en charge de l'installation de la solution en production afin de résoudre les dysfonctionnements de la solution
Élaborer des scénarii d'évolution de la solution en tenant compte des retours des équipes d'exploitation, du client et du contexte d'utilisation afin de garantir la cohérence globale de la solution

MODALITÉS D'ÉVALUATION

Mise en situation portant sur le profil d'une entreprise : le candidat réalise un prototype respectueux des règles imposées. Il présente lors d'un entretien oral le prototype et le plan de test technique à mettre en œuvre afin de confirmer la pertinence de la solution envisagée.
Étude de cas portant sur la rédaction d'un plan de déploiement : le candidat rédige une fiche technique et propose un dispositif pour assurer le transfert de connaissance aux personnes en charge de l'exploitation et de la maintenance.
Mise en situation professionnelle sur la base d'une simulation d'un incident de sécurité : le candidat devra proposer une méthodologie pour traiter l'incident en coordination avec les équipes support et sera évalué sur la qualité de l'analyse des causes racines, sa capacité à solutionner l'incident, et la qualité du plan d'action pour la mise en œuvre du correctif
Étude de cas avec restitution, portant sur le profil d'une entreprise : le candidat instruit une demande d'évolution d'une solution et établit des préconisations. Il présente lors d'un entretien oral un plan de maintenance argumenté et sera évalué sur la pertinence des propositions d'évolution et le choix des options, la qualité écrite du plan de maintenance, l'analyse des impacts sur la solution, la prise en compte des exigences du client, et la clarté de la restitution technique

PRÉREQUIS À L'ENTRÉE

L'accès à ce bloc pris de façon indépendante est ouvert aux candidats justifiant d'une expérience ou d'une formation préalable attestant de la maîtrise des fondamentaux techniques en architecture des systèmes d'information : conception et administration d'architectures réseau et systèmes, principes de la sécurité des infrastructures, et compréhension des mécanismes d'intégration de solutions dans un système d'information existant. La maîtrise de ces prérequis techniques est vérifiée lors de l'admission, à travers l'étude du dossier de candidature, un entretien individuel et, le cas échéant, un test technique permettant de s'assurer que le candidat dispose du niveau requis pour aborder les compétences de conception de prototypes sécurisés, d'intégration dans le système d'information, de sécurisation des architectures réseau et de tests d'intrusion que comporte ce bloc.

RNCP42939BC04 — Assurer la mise en exploitation et la maintenance de solutions de sécurité

LISTE DE COMPÉTENCES

Mettre en exploitation la solution en veillant à son adaptation au regard des besoins utilisateurs et en maintenant un regard critique sur les dispositifs de supervision automatisée, afin de faciliter son appropriation et garantir la fiabilité de la détection.
Résoudre des opérations de maintenance complexes en effectuant une analyse des causes afin d'évaluer les vulnérabilités, les menaces et de les corriger, y compris lorsqu'elles impliquent des systèmes de surveillance automatisés ou des composants à logique décisionnelle.
Rendre compte des incidents et dysfonctionnements de la solution dans le logiciel de suivi à disposition afin de

contribuer à l'amélioration continue de la solution tout au long de son cycle de vie ainsi qu'à sa bonne diffusion auprès des utilisateurs

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle sur la base d'une simulation d'un incident de sécurité grave et complexe : le candidat devra proposer une procédure de maintenance afin de résoudre l'incident. Il élabore un plan d'amélioration de la solution qui intègre la traçabilité et l'évolution des modifications et la prise en compte des publics-utilisateurs

PRÉREQUIS À L'ENTRÉE

L'accès à ce bloc pris de façon indépendante est ouvert aux candidats justifiant d'une expérience ou d'une formation préalable attestant de la maîtrise des fondamentaux en exploitation et en supervision des systèmes d'information : administration de systèmes, principes de supervision et de maintenance, gestion des incidents de sécurité, et connaissance des outils de détection et de suivi. La maîtrise de ces prérequis techniques est vérifiée lors de l'admission, à travers l'étude du dossier de candidature, un entretien individuel et, le cas échéant, un test technique permettant de s'assurer que le candidat dispose du niveau requis pour aborder les compétences de supervision des dispositifs de détection automatisée, de maintenance des solutions, de résolution d'incidents complexes et d'investigation post-incident que comporte ce bloc.

RNCP42939BC05 — Animer et gérer une équipe en mode projet

LISTE DE COMPÉTENCES

Constituer, gérer et animer une équipe projet en mettant en œuvre des méthodes et des outils efficients pour faciliter la réalisation du projet et travailler efficacement avec les parties prenantes et décisionnaires

Conduire des réunions de projet en structurant sa présentation orale et écrite afin de faciliter l'avancement du projet, partager les informations, prendre des décisions sur des sujets critiques et assumer les responsabilités associées

Mettre en place une communication adaptée en démocratisant le processus technique cybersécurité et sa diffusion auprès des parties prenantes et des collaborateurs, en intégrant les risques émergents liés aux outils autonomes déployés dans l'organisation, afin de faciliter l'adhésion de l'ensemble des parties prenantes.

MODALITÉS D'ÉVALUATION

Étude de cas et Mise en situation portant sur un profil d'entreprise, le candidat met en place une organisation d'équipe projet en adéquation avec la problématique projet à traiter. Puis, à partir d'un jeu de rôle, ce dernier conduira une réunion de lancement de projet.

Étude de cas portant sur le profil d'une entreprise, le candidat formalise un plan de communication de sensibilisation et de vulgarisation destiné à l'ensemble des parties prenantes. Le candidat présente lors d'un entretien oral le plan de communication et argumente ses choix

PRÉREQUIS À L'ENTRÉE

L'accès à ce bloc pris de façon indépendante est ouvert aux candidats justifiant d'une expérience ou d'une formation préalable en gestion de projet, en management d'équipe ou en conduite d'activité, ainsi que d'une connaissance du contexte professionnel de la cybersécurité leur permettant de situer leur action managériale dans les spécificités du secteur. L'admission est prononcée après étude du dossier de candidature et entretien individuel permettant de vérifier l'adéquation entre le profil du candidat, son expérience de l'encadrement ou du pilotage de projet, et les exigences du bloc.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert en développement de solutions de cybersécurité exerce dans l'ensemble des secteurs d'activité, la cybersécurité constituant un enjeu transversal pour toute organisation manipulant des données ou dépendant de systèmes d'information. Il intervient à la fois au sein des entreprises dont la cybersécurité est le cœur de métier — éditeurs de solutions de sécurité, entreprises de services du numérique, cabinets d'audit et de conseil spécialisés, prestataires de services de sécurité managés et centres opérationnels —, au sein d'organisations de tous secteurs disposant d'une direction des systèmes d'information — industrie, banque et assurance, santé, télécommunications, énergie, administration et collectivités territoriales — ainsi qu'auprès des structures ne disposant pas de compétences internes en cybersécurité et souhaitant intégrer un relais cyber dans leur effectif ou faisant appel à une expertise externalisée.

TYPE D'EMPLOIS ACCESSIBLES

Responsable de la sécurité des systèmes d'information (RSSI) - Architecte sécurité / Security Solution Architect - Consultant en cyber-résilience et gouvernance - Ingénieur détection et réponse (SOC nouvelle génération) - Ingénieur automatisation de la sécurité (SOAR) - Purple Team Engineer - DevSecOps Platform Engineer - Responsable de centre opérationnel de sécurité (SOC)

RÉGLEMENTATIONS D'ACTIVITÉ

L'exercice du métier d'expert en développement de solutions de cybersécurité n'est pas subordonné à une réglementation spécifique conditionnant l'accès à la profession ou sa pratique. Aucune disposition légale ou réglementaire n'impose la détention d'une certification, d'un agrément ou d'une habilitation particulière pour exercer les activités du métier. Cet expert intervient néanmoins dans un environnement fortement normé, dont la maîtrise constitue une compétence certifiée par le titre : réglementations européennes et nationales relatives à la sécurité des systèmes d'information et à la protection des données — notamment la directive NIS2, le règlement DORA, le Règlement Général sur la Protection des Données, le Cyber Resilience Act et le règlement sur l'intelligence artificielle. Ces textes encadrent l'objet du travail de cet expert sans conditionner l'accès à la profession.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
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) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	32 216
Jugés difficiles à recruter	51 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en 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

La certification s'adresse aux candidats titulaires d'une certification de niveau 6 dans le domaine de l'informatique ou des sciences de l'ingénieur, ou justifiant d'une expérience professionnelle d'au moins trois années dans le champ de la certification visée.

À titre dérogatoire, pourront être considérées comme recevables les candidatures qui, tout en ne répondant pas aux critères formels ci-dessus, apparaîtraient exceptionnelles au vu du dossier. Ces dérogations visent en particulier à autoriser l'admission de personnes ayant exercé pendant plusieurs années des fonctions en lien avec des activités informatiques de haut niveau et dont l'employeur propose un changement d'activité, de personnes en reconversion

professionnelle, ou de candidats engagés dans une démarche de validation des acquis de l'expérience.
Les candidats dont le dossier satisfait aux critères énoncés ci-dessus sont convoqués à un entretien individuel, conduit en présentiel ou à distance par le responsable pédagogique en charge de la certification. Cet entretien complète le dossier de candidature : il a pour objet de comprendre la motivation du candidat, de vérifier la cohérence de la certification avec son projet professionnel et de s'assurer de sa capacité à suivre une formation de niveau 7.

PRÉREQUIS À LA VALIDATION

La validation de la certification requiert la validation des cinq blocs de compétences qui la composent, ainsi que la réussite à l'épreuve finale transverse attestant de la capacité du candidat à mobiliser et à articuler l'ensemble des compétences du titre.

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

Le jury de délivrance de la certification est composé d'au moins trois membres, dont au minimum deux professionnels externes à l'organisme certificateur. Ces membres externes sont des professionnels en activité dans le champ de la cybersécurité, disposant d'une expérience de terrain leur conférant la capacité à évaluer objectivement les compétences des candidats.

COMPOSITION DU JURY — VAE

Le jury de délivrance de la certification est composé d'au moins trois membres, dont au minimum deux professionnels externes à l'organisme certificateur. Ces membres externes sont des professionnels en activité dans le champ de la cybersécurité, disposant d'une expérience de terrain leur conférant la capacité à évaluer objectivement les compétences des candidats avec lesquels ils ne doivent avoir aucun lien.

Financement en alternance (NPEC)

Cette certification ne figure pas au référentiel des niveaux de prise en charge (NPEC) en vigueur. En attendant que son niveau soit fixé, l'OPCO peut financer un contrat d'apprentissage sur la base d'une valeur d'amorçage (arrêté du 31 août 2022).

Base légale

Date de décision	30/10/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/10/2029
Date de dernière délivrance possible	29/10/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2026	24	0	90 %	—
2025	6	0	90 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP38463

CORRESPONDANCES (PAR BLOCS)

RNCP40897, RNCP38463

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

https://an21-acoccitanie.fr/master/

Fiche officielle (France Compétences)
https://www.francecompetences.fr/recherche/rncp/42939/