

Expert en cybersécurité

RNCP42823 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326m, 326n
Formacode(s)	31045, 31067, 31009
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2031

Certificateur(s)

EPITECH ECOLE INFORMATIQUE NOUV TECHNO · SIRET : 42385519600014

Partenaires habilités

14 organismes habilités, d'après la liste publiée par France compétences : 14 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600022	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600030	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600048	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600055	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600063	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600097	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600105	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600121	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600147	Former et organiser l'évaluation
EPITECH ECOLE INFORMATIQUE NOUV TECHNOL	42385519600154	Former et organiser l'évaluation

Liste complète des 14 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp42823-expert-en-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'évolution rapide des technologies numériques et la multiplication des menaces informatiques ont profondément transformé la gestion de la sécurité au sein des organisations. La cybersécurité n'est plus seulement un enjeu technique, mais un enjeu stratégique, économique et sociétal. Les entreprises, collectivités et institutions publiques doivent aujourd'hui se doter de profils capables de concevoir, déployer et piloter des dispositifs de protection complets, en intégrant les dimensions techniques, réglementaires, humaines et environnementales.

La certification « Expert en cybersécurité » vise à répondre à ces besoins en formant des professionnels capables de : Élaborer et piloter une stratégie globale de cybersécurité, en cohérence avec les orientations de l'organisation ;

Déployer des solutions techniques de sécurisation des systèmes, des réseaux et des données, dans des environnements hybrides et distribués ; Renforcer la résilience face aux incidents de sécurité par la mise en place de politiques de gestion des risques, de tests d'intrusion, d'audits et de plans de continuité d'activité ; Conduire et coordonner des projets IT complexes, mobilisant des équipes pluridisciplinaires et des prestataires internes ou externes, dans une logique d'amélioration continue et d'inclusion.

L'Expert en cybersécurité agit à l'intersection de la gouvernance stratégique, de la sécurité opérationnelle et de la culture organisationnelle de la cybersécurité. Il est en mesure d'intervenir sur l'ensemble du cycle de vie des systèmes d'information : analyse, conception, déploiement, supervision, audit, sensibilisation et innovation défensive.

La certification s'inscrit dans un contexte de forte tension sur le marché de l'emploi : le besoin de spécialistes en cybersécurité est estimé à plusieurs dizaines de milliers de postes non pourvus en France. Les attentes des entreprises dépassent la maîtrise technique : elles recherchent des profils capables d'assurer la cohérence stratégique, la conformité réglementaire (RGPD, ISO 27001, ANSSI, NIS2) et l'intégration de la sécurité dans les démarches de développement durable et d'accessibilité numérique.

La certification « Expert en cybersécurité » répond ainsi à un double objectif : Professionnaliser des experts capables d'assurer la protection et la résilience des organisations face aux menaces cyber ; Contribuer à la souveraineté numérique et à la diffusion d'une culture de sécurité éthique, inclusive et durable au sein des entreprises françaises et internationales.

ACTIVITÉS VISÉES

L'Expert en Cybersécurité intervient à différents niveaux d'activités :

Il définit la stratégie de cybersécurité de l'organisation : Analyser l'existant du système d'information et cartographier les interconnexions et les risques. Évaluer les menaces techniques, humaines et organisationnelles. Déterminer les priorités d'action et concevoir une politique globale de sécurité conforme aux référentiels (ISO 27001, NIST, ANSSI, RGPD). Définir les indicateurs de performance et de suivi de la sécurité.

Il déploie la sécurisation des systèmes et des données : Concevoir et mettre en œuvre les politiques d'accès, d'authentification et de sauvegarde. Déployer les outils et dispositifs de protection : chiffrement, pare-feux, SIEM, antivirus, IDS/IPS, solutions cloud sécurisées. Piloter la mise en œuvre et l'évaluation continue de l'efficacité des solutions. Réaliser des audits réguliers et adapter les dispositifs en fonction des retours d'expérience.

Il renforce la résilience cybersécurité de l'entreprise : Mener des audits offensifs et tests de pénétration (pentests, red teaming, reverse engineering). Élaborer et tester des scénarios d'attaque et de crise pour évaluer la robustesse de l'organisation. Contribuer à la sensibilisation et à la formation des collaborateurs aux enjeux de cybersécurité. Mettre en place des plans de continuité et de reprise d'activité (PCA/PRA).

Il conduit des projets IT et mobilise des équipes pluridisciplinaire : Cadrer et planifier les projets de sécurisation (besoins, objectifs, livrables, budget). Animer et coordonner des équipes pluridisciplinaires (techniques, métiers, prestataires). Assurer la communication, le reporting et la capitalisation des bonnes pratiques. Intégrer les principes d'accessibilité numérique, de sobriété et d'inclusion dans les solutions déployées.

Ces activités couvrent l'ensemble du cycle de vie de la sécurité de l'information — de la conception stratégique à la mise en œuvre opérationnelle et à la gestion humaine du risque cyber. Elles préparent à des fonctions telles que Expert cybersécurité, Responsable sécurité des systèmes d'information (RSSI), Consultant sécurité, Architecte sécurité, Chef de projet cybersécurité ou Pentester senior.

COMPÉTENCES ATTESTÉES

Réaliser un inventaire des actifs informationnels (matériels, logiciels, données) de l'organisation, en dressant une cartographie des interconnexions des systèmes pour obtenir une vision exhaustive du SI.

Cartographier les risques liés aux systèmes d'information, en analysant les menaces techniques, humaines et organisationnelles et en les hiérarchisant selon leur criticité.

Définir des indicateurs critiques de surveillance et de détection des menaces afin d'assurer une veille et un suivi des risques.

Concevoir une stratégie de réponse aux menaces informatiques conforme aux normes et objectifs de l'organisation (réduction, transfert ou acceptation du risque).

Planifier et prioriser des actions correctives adaptées aux menaces identifiées pour réduire les vulnérabilités.

Mettre en œuvre un dispositif de journalisation et de suivi des événements de sécurité, en exploitant les logs et audits pour ajuster les mesures.

Adapter les solutions de cybersécurité aux besoins d'ergonomie, d'accessibilité et aux situations de handicap pour garantir une utilisation inclusive et conforme aux standards.

Définir des politiques de gestion des accès et d'authentification forte (MFA), en assurant la traçabilité et la

proportionnalité des dispositifs.

Instaurer des procédures de sauvegarde et de restauration sécurisée des données, afin d'assurer la résilience, l'intégrité et la disponibilité des données critiques en cas d'incident.

Déployer des solutions de chiffrement adaptées aux environnements et données critiques, en sélectionnant les protocoles et algorithmes adéquats (SSL/TLS, AES, RSA, etc.).

Sélectionner, configurer et évaluer les solutions de sécurité (pares-feux, IDS/IPS, SIEM, antivirus, NAC, WAF) en fonction du contexte technique et des profils utilisateurs, y compris en situation de handicap.

Piloter la mise en œuvre des dispositifs de sécurité et définir les indicateurs de performance (taux de détection, couverture, temps de réaction).

Réaliser des audits et tests de sécurité réguliers selon les référentiels internes et externes (ISO 27001, NIST, ANSSI) et proposer des actions correctives.

Adapter en continu les dispositifs de sécurité en fonction des incidents, des retours d'expérience et de l'évolution des menaces.

Gérer la sécurité des environnements cloud et hybrides, en appliquant les bonnes pratiques de protection et de supervision des infrastructures et applications.

Effectuer des tests de pénétration et d'audits offensifs (boîte noire, grise, blanche) pour évaluer la robustesse des systèmes et formuler des recommandations.

Élaborer des scénarios d'attaque et d'incident (Red Teaming, phishing, environnement miroir) pour renforcer la résilience organisationnelle.

Réaliser des analyses de reverse engineering sur des composants suspects pour identifier des comportements malveillants et des vulnérabilités.

Identifier les collaborateurs et profils métiers à sensibiliser à la cybersécurité selon leur exposition et leurs usages numériques.

Concevoir des dispositifs et supports de sensibilisation adaptés aux différents publics pour développer la culture de sécurité.

Mettre en œuvre et animer des actions de sensibilisation et de simulation d'attaques pour améliorer la vigilance et la réactivité des utilisateurs.

Analyser les besoins et les enjeux d'un projet IT de cybersécurité en échangeant avec les parties prenantes et en formalisant les objectifs.

Élaborer le cahier des charges d'un projet, en définissant livrables, ressources et indicateurs de suivi.

Construire le rétroplanning du projet, estimer les charges, identifier les ressources et planifier les jalons clés.

Organiser la répartition des rôles et responsabilités au sein d'équipes pluridisciplinaires, selon les expertises techniques et métiers.

Animer et coordonner les activités d'équipes pluridisciplinaires, assurer le suivi, la communication et la résolution des points de blocage.

Déployer des dispositifs de communication et de collaboration entre les équipes, en utilisant des outils de partage et de reporting.

Mettre en œuvre les adaptations nécessaires à l'intégration de collaborateurs en situation de handicap ou à besoins spécifiques, pour garantir la cohésion et la performance collective.

Blocs de compétences

RNCP42823BC01 — Définir une stratégie de cybersécurité

LISTE DE COMPÉTENCES

Réaliser un inventaire des actifs informationnels (matériels, logiciels, données) de l'organisation, en se fondant sur la documentation existante et en dressant une cartographie des interconnexions entre les différents systèmes, afin d'avoir une vision objective et exhaustive de la situation de l'organisation en matière de SI.

Cartographier les risques liés aux systèmes d'information, en analysant les menaces selon leur nature (technique, humaine, organisationnelle), en évaluant leur criticité à l'aide d'outils méthodologiques (matrices de risque, grilles d'impact/probabilité), afin de prioriser les actions de sécurisation à mettre en œuvre

Définir des indicateurs critiques liés aux ressources de l'entreprise, en mobilisant des outils de veille et d'analyse de risque, afin de détecter la survenue des menaces identifiées comme critiques pour l'organisation.

Concevoir des stratégies de réponse aux menaces informatiques en respectant les normes en vigueur et les objectifs de l'entreprise (réduction, transfert, acceptation des risques), afin de limiter leur impact.

Planifier des actions correctives adaptées à la menace identifiée, en mobilisant des moyens appropriés (mise à jour des politiques de sécurité, déploiement de correctifs, sensibilisation des utilisateurs, ajustement des configurations systèmes, afin de traiter les problématiques sur le terrain.

Mettre en œuvre un dispositif de journalisation et de suivi des événements de sécurité, en structurant les types de logs à collecter, leur durée de conservation et leur accessibilité, et en s'appuyant sur des audits, des revues de conformité, l'analyse des journaux et des tableaux de bord, afin d'ajuster les mesures de sécurité

Adapter les solutions de cybersécurité aux besoins d'ergonomie et d'accessibilité des utilisateurs, en tenant compte des contraintes fonctionnelles et des situations de handicap, afin de garantir une utilisation inclusive et conforme aux principes d'accessibilité numérique.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle sous la forme d'un projet de groupe, suivi d'une soutenance individuelle

Le candidat présente, à partir d'un projet de mise en place d'une solution de cybersécurité, une analyse stratégique de l'organisation concernée, qui comprend : la démarche d'inventaire du SI et de cartographie des interconnexions ; l'évaluation des risques identifiés et leur priorisation ; la définition d'indicateurs de suivi ; la formulation d'une politique de cybersécurité (ex. : gouvernance IAM, journalisation, accessibilité, sobriété numérique) ; et les arbitrages réalisés dans la conception de cette stratégie, en lien avec les objectifs de l'organisation.

RNCP42823BC02 — Déployer la sécurisation des systèmes et des données

LISTE DE COMPÉTENCES

Définir des politiques de gestion des accès, en intégrant notamment des mécanismes d'authentification forte (MFA), de contrôle des droits et de traçabilité, tout en privilégiant des solutions sobres et proportionnées aux usages, afin de sécuriser l'accès aux ressources critiques et limiter les risques d'usurpation.

Instaurer des procédures de sauvegarde et de restauration sécurisée des données, en définissant des politiques de rétention, de chiffrement et de tests de restauration réguliers, afin d'assurer la résilience, l'intégrité et la disponibilité des données critiques en cas d'incident.

Déployer des solutions de chiffrement adaptées aux données et aux environnements concernés, en sélectionnant les protocoles, algorithmes et niveaux de protection selon les usages (SSL/TLS, chiffrement symétrique ou asymétrique, chiffrement de disque ou de fichier), afin de garantir la confidentialité, l'intégrité et la conformité des données sensibles.

Sélectionner des solutions de sécurité (pares-feux hardware ou software, IDS/IPS, SIEM, antivirus, NAC, WAF...), en fonction des besoins techniques et organisationnels l'entreprise et de la criticité des menaces, des profils utilisateurs – y compris en situation de handicap – et de leur impact environnemental afin de garantir une protection accessible, durable et conforme aux exigences du système d'information.

Piloter l'implémentation des solutions retenues, en définissant des indicateurs de performance (taux de détection, temps de réaction, couverture des segments critiques), et en assurant la coordination avec les équipes opérationnelles, afin de mesurer l'efficacité des dispositifs déployés et d'assurer leur amélioration continue.

Réaliser des tests et audits réguliers des dispositifs de sécurité, en s'appuyant sur des référentiels internes et externes (ISO 27001, NIST, ANSSI), afin d'assurer leur conformité aux bonnes pratiques et aux exigences de l'organisation et de proposer les actions correctives nécessaires.

Adapter en continu les dispositifs de sécurité en fonction des tests effectués, des retours d'expérience, des incidents survenus et de l'évolution des menaces, en mobilisant des outils de veille, d'analyse post-incident et de capitalisation, afin d'assurer une amélioration continue de la posture de sécurité.

Gérer la sécurité des environnements cloud et hybrides, en appliquant des bonnes pratiques spécifiques à la protection des infrastructures, plateformes et applications déployées hors site, afin d'assurer la confidentialité, l'intégrité et la disponibilité des données et services dans des environnements multi-sites.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle sous la forme d'un projet de groupe, suivi d'une soutenance individuelle

Le candidat expose les solutions techniques déployées ou préconisées dans le cadre d'un projet défensif, en explicitant : la définition des politiques d'accès, de sauvegarde, de chiffrement ; les choix des outils (SIEM, antivirus, pare-feux, etc.) ; les contraintes environnementales et d'accessibilité prises en compte ; le pilotage de l'implémentation, les indicateurs de performance suivis ; les audits réalisés, les ajustements effectués ; et la gestion des environnements cloud et hybrides.

RNCP42823BC03 — Renforcer la résilience cybersécurité de l'entreprise

LISTE DE COMPÉTENCES

Effectuer des tests de pénétration sur les systèmes et applications, en mobilisant des méthodologies d'audit offensif (tests en boîte noire, blanche ou grise, élévation de privilèges, injection, contournement), afin d'évaluer la robustesse des mesures de sécurité déployées et de formuler des recommandations correctives.

Élaborer des scénarios d'attaques et d'incidents de cybersécurité, en croisant l'analyse de risques, les typologies de menaces, les retours d'expérience et le contexte de l'organisation (Red Teaming, Purple Team, phishing ciblé, environnement miroir), afin de renforcer la résilience organisationnelle.

Réaliser des analyses de reverse engineering sur des exécutables ou composants logiciels suspects, en mobilisant des outils de désassemblage, de débogage et d'analyse statique/dynamique, pour identifier des vulnérabilités, des comportements malveillants ou des mécanismes de protection.

Identifier les collaborateurs concernés par les actions de sensibilisation à la cybersécurité, en cartographiant les profils métiers, les usages numériques et les niveaux d'exposition, afin de définir les publics prioritaires et adapter les dispositifs pédagogiques.

Concevoir des dispositifs de sensibilisation à la cybersécurité, en définissant des objectifs pédagogiques différenciés et en élaborant des supports adaptés (guides, modules, visuels, vidéos), afin de renforcer la culture de sécurité des collaborateurs.

Mettre en œuvre des actions de sensibilisation, en animant des sessions collectives ou individuelles, en organisant des campagnes thématiques (phishing, mots de passe, etc.) et en réalisant des simulations collectives d'attaques, afin d'évaluer et d'améliorer le niveau de vigilance des utilisateurs.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle sous la forme d'un projet de groupe, suivi d'une soutenance individuelle

Le candidat restitue les actions menées dans le cadre d'un projet de test offensif, puis développe : la préparation, l'exécution et l'analyse des tests (pentests, reverse engineering, etc.) ; la conception de scénarios d'attaque réalistes (Red Teaming, phishing...) ; la formulation de recommandations correctives et leur impact ; les actions de sensibilisation envisagées ou mises en œuvre auprès des collaborateurs (supports, simulations, campagnes) ; et l'articulation entre retour d'expérience, prévention, formation et gestion de crise.

RNCP42823BC04 — Conduire des projets IT et mobiliser des équipes pluridisciplinaires

LISTE DE COMPÉTENCES

Analyser le besoin exprimé et les enjeux opérationnels d'un projet IT, en mobilisant des échanges avec les parties prenantes et des techniques de recueil structuré, pour cadrer les attentes et formaliser les objectifs

Élaborer le cahier des charges d'un projet IT, en définissant les objectifs, les livrables attendus, les indicateurs de suivi et les ressources mobilisables, afin de structurer la planification et garantir la faisabilité opérationnelle.

Construire le rétroplanning d'un projet IT, en estimant les charges, en identifiant les ressources internes et externes nécessaires et en intégrant les jalons clés, afin d'assurer une exécution cohérente avec les contraintes de délai et de budget

Organiser la répartition des rôles et responsabilités au sein d'équipes pluridisciplinaires, en tenant compte des expertises techniques, métiers et fonctionnelles, afin d'assurer une coordination efficace et alignée sur les objectifs du projet.

Animer les activités d'équipes pluridisciplinaires, en organisant des réunions de coordination, en assurant le suivi de l'avancement et la gestion des points de blocage, pour garantir la progression du projet

Déployer des dispositifs de communication et de collaboration entre les équipes, en utilisant des outils de partage et de reporting, afin de favoriser la circulation de l'information dans l'entreprise et l'implication des parties prenantes

Mettre en œuvre les adaptations nécessaires pour intégrer efficacement les membres d'équipes en situation de handicap ou avec besoins spécifiques, en évaluant leurs contraintes, en ajustant les rôles, les outils, et les modes de communication, afin d'assurer une pleine participation, la continuité opérationnelle et la performance collective du projet IT.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle sous la forme d'un projet de groupe, suivi d'une soutenance individuelle

Le candidat présente les dimensions projet et organisation humaine d'un projet de cybersécurité, en s'appuyant sur : l'analyse du besoin et la rédaction du cahier des charges ; la planification du projet (jalons, budget, charges) ; la gestion des risques projet ; la répartition des rôles au sein des équipes mobilisées ; les modalités de communication, de reporting, de coordination ; et les dispositifs mis en place pour l'intégration de profils divers, notamment en

situation de handicap.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Cybersécurité ; DATA/IA ; Industrie/santé ; Administration / social ; Conseil IT ; Réseaux Télécom ; Banque / Assurance / Mutuelles ; LegalTech

TYPE D'EMPLOIS ACCESSIBLES

Expert en cybersécurité - Consultant / Responsable / Administrateur / Architecte cybersécurité - Ingénieur SOC - Ingénieur / Administrateur DevOps / DevSecOps - Pentester

RÈGLEMENTATIONS D'ACTIVITÉ

L'expert en cybersécurité évolue dans un contexte réglementaire en pleine expansion. Ses missions sont ainsi encadrées par plusieurs textes européens :

Cybersecurity Act - Directives NIS2, REC et DORA - Cyber Resilience Act

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)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre titulaire d'un diplôme de niveau 6 minimum en informatique ou domaine connexe

PRÉREQUIS À LA VALIDATION

Le candidat doit avoir validé une période d'au moins six mois en entreprise (stage, alternance, expérience professionnelle en lien avec le titre)

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

Deux référents pédagogiques de la direction d'EPITECH et trois professionnels externes à EPITECH, relevant du secteur de la cybersécurité

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	5 ans

Date d'échéance de l'enregistrement 30/09/2031

Date de dernière délivrance possible 30/09/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	53	0	66 %	—
2023	59	0	90 %	50 %

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP38114, RNCP39999

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://epitech.eu>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42823/>