

Spécialiste en cybersécurité

RNCP42503 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31045, 31038, 31032, 24220
Code(s) ROME	M1801, M1802, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	26/06/2026
Date d'échéance	26/06/2029

Certificateur(s)

CSB EDUCATION GROUP · SIRET : 92991594000019

Partenaires habilités

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

Organisme	SIRET	Habilitation
ASSOCIATION D'ENSEIGNEMENT TECHNIQUE SUPERIEUR AN21 ACADEMIE NUMERIQUE DU XXIEME SIECLE	8513778460 0023	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La cybersécurité constitue aujourd'hui un levier fondamental de la souveraineté numérique et un impératif de résilience pour l'ensemble du tissu économique national. Dans un contexte marqué par l'intensification et la professionnalisation des cybermenaces, dont l'impact macro-économique est désormais systémique, la protection de la confidentialité, de l'intégrité et de la disponibilité des données est devenue une condition sine qua non de la stabilité des organisations.

Le renforcement du cadre réglementaire européen, notamment via les directives NIS 2, DORA et l'AI Act, fait de la sécurité numérique un pilier de conformité incontournable, incitant les organisations à structurer leur posture de protection autour des meilleures pratiques et référentiels en vigueur. Parallèlement, la transformation numérique des entreprises s'inscrit désormais dans une trajectoire de responsabilité sociétale et environnementale. La sécurisation des systèmes d'information ne peut plus être pensée indépendamment des enjeux de sobriété numérique : la conception des architectures, le recours aux environnements virtualisés et l'usage de l'intelligence artificielle doivent dorénavant intégrer des principes d'optimisation énergétique et de durabilité.

La certification « Spécialiste en Cybersécurité » répond à ces défis en formant des professionnels capables de piloter et d'améliorer la posture de sécurité des organisations. Positionné comme un pivot opérationnel entre les fonctions d'exécution technique et de management stratégique, le titulaire de la certification maîtrise les mécanismes de protection des infrastructures, la détection des menaces ainsi que la gestion des vulnérabilités. Il est en capacité d'analyser des risques complexes et de mettre en œuvre des solutions proportionnées, en cohérence avec le cadre réglementaire et les engagements de responsabilité numérique de son organisation.

En répondant à la pénurie structurelle de compétences identifiée par les autorités nationales, cette certification assure le déploiement de talents opérationnels indispensables à la sécurisation des entreprises, des établissements de santé, des collectivités territoriales ou des infrastructures critiques, garantissant ainsi la continuité d'activité et la

confiance numérique globale.

ACTIVITÉS VISÉES

Collecte et analyse des informations nécessaires à la conduite d'un test d'intrusion éthique.

Test d'intrusion éthique et évaluation de l'impact de compromission du périmètre ciblé.

Présentation des résultats et des recommandations d'un test d'intrusion éthique.

Configuration des éléments de sécurité des réseaux.

Durcissement de la configuration des infrastructures informatique et industrielle.

Sécurisation des nouvelles technologies de l'information et des communications (robotique, objets connectés, intelligence artificielle...).

Maintien de la sécurité des données d'un système d'information.

Contrôle des identités et des accès à privilèges au sein d'un système d'information.

Elaboration des standards techniques associés aux solutions de sécurité technique mises en œuvre.

Définition et analyse du fonctionnement nominal du système d'information.

Définition du processus de collecte des journaux d'événements en fonction des menaces (playbook).

Automatisation et orchestration des règles de détection d'événements de sécurité.

COMPÉTENCES ATTESTÉES

Recueillir les données et renseignements relatifs à la cible, à l'aide de pratiques d'investigation légalement autorisées et d'analyse d'information préalablement dissimulée, en récoltant, croisant ou analysant des données numériques disponibles en source ouverte (OSINT), afin d'identifier les faiblesses du système d'information cible et de déterminer la nature du test d'intrusion.

Recueillir les données et renseignements relatifs aux actifs du système d'information de la cible, à l'aide d'outils et de techniques d'investigation légalement autorisés (discovery) afin de cartographier les systèmes les plus critiques et les plus exposés, d'identifier leurs vulnérabilités et de déterminer les chemins d'attaque possibles sur ces systèmes.

Conduire des techniques et tactiques d'attaques de cybersécurité sur base des éléments collectés, en collaboration avec les experts (opérationnels métiers et informatiques) afin de prendre le contrôle du système cible.

Déterminer les risques et dommages pour le système d'information cible en évaluant l'impact fonctionnel d'une attaque en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données, afin de rédiger un rapport de test d'intrusion dans un format prenant en compte les éventuelles situations de handicap.

Communiquer l'ensemble des résultats d'un test d'intrusion à travers un rapport de synthèse, dans un format prenant en compte les éventuelles situations de handicap, afin de présenter à l'organisation sa surface d'exposition, ses vulnérabilités, leur criticité et leur impact.

Déterminer les mesures de sécurité permettant de traiter les risques et dommages présents dans le rapport de test d'intrusion, en collaboration avec les opérationnels métiers et informatiques, afin d'établir un plan de remédiation adapté.

Etablir les mesures de sécurité applicables en concevant une infrastructure réseau sécurisée afin de protéger les réseaux WAN, LAN et sans fil.

Configurer les éléments de sécurité des réseaux afin de mettre en place un réseau sécurisé répondant aux exigences de sécurité applicables à l'organisation

Mettre en œuvre les règles de durcissement de la configuration des infrastructures informatiques et industrielles en s'appuyant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux, afin de renforcer la sécurité du système d'information.

Déployer des mesures de sécurité opérationnelles (chiffrement, contrôle d'accès, etc.) en s'appuyant sur les politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de prévenir les risques de fuite de données.

Configurer les éléments de sécurité des systèmes connectés, en intégrant les spécificités de l'environnement et les enjeux du numérique responsable, afin de garantir l'intégrité et la disponibilité des systèmes.

Déployer des mesures de sécurité s'appuyant sur l'intelligence artificielle en collaboration avec les experts cybersécurité et les opérationnels métiers, afin de contenir les risques liés au déploiement de l'Intelligence Artificielle au sein d'un Système d'Information.

Mettre en œuvre les mesures de sécurité des données, en fonction des contraintes et besoins fonctionnels de l'organisation, afin de garantir le niveau de confidentialité, d'intégrité et de disponibilité des données.

Traiter les vulnérabilités d'un projet à déployer sur un système d'information industriel existant, en prenant en compte les enjeux de souveraineté numérique, afin de limiter les impacts et les risques inhérents à la sécurité des données.

Déployer des solutions de sécurité permettant de prévenir les risques de fuite de données d'un système d'information

existant, afin d'être conforme au système de management de la sécurité de l'information (SMSI) et aux normes environnementales.

Mettre en œuvre les mesures de sécurité et les solutions techniques associées (contrôle d'accès, authentification...) adéquates pour assurer la sécurité des identités humaines, machines et services d'un environnement industriel.

Déployer des mesures de sécurité en adéquation avec les enjeux de souveraineté numérique et de numérique responsable, afin de contrôler les accès à privilèges.

Élaborer les standards techniques de sécurité et la documentation technique, applicables et accessibles aux personnes en situation de handicap, en fonction des solutions techniques mises en œuvres, afin de répondre aux exigences du système de management de la sécurité de l'information (SMSI) et des normes environnementales.

Qualifier un événement de cybersécurité en fonction du comportement nominal du système d'information et des scénarios de gestion d'événements cyber (playbook), afin de le documenter, de déterminer son niveau de criticité et d'appliquer le traitement associé

Définir la collecte, la conservation et l'archivage des journaux d'événements (logs) nécessaires, en fonction des scénarios de gestion d'événements cyber (playbook) et en accord avec les contraintes et exigences de l'organisation (conformité, budget...), pour analyser le fonctionnement du système d'information

Adapter les scénarios de gestion d'événements cyber (playbook) en fonction de l'état la menace afin d'optimiser les détections des évènements de sécurité dans une optique d'amélioration continue

Programmer des règles de détection d'événements cyber en s'appuyant sur un usage raisonné des modèles d'intelligence artificielle en vue de qualifier les alertes de sécurité de façon automatisée

Documenter les évènements de sécurité en adoptant un langage et/ou des outils inclusifs adaptés pour permettre la mesure de l'impact au sein de l'organisation

Blocs de compétences

RNCP42503BC01 — Conduire des tests d'intrusion éthiques

LISTE DE COMPÉTENCES

Recueillir les données et renseignements relatifs à la cible, à l'aide de pratiques d'investigation légalement autorisées et d'analyse d'information préalablement dissimulée, en récoltant, croisant ou analysant des données numériques disponibles en source ouverte (OSINT), afin d'identifier les faiblesses du système d'information cible et de déterminer la nature du test d'intrusion.

Recueillir les données et renseignements relatifs aux actifs du système d'information de la cible, à l'aide d'outils et de techniques d'investigation légalement autorisés (discovery) afin de cartographier les systèmes les plus critiques et les plus exposés, d'identifier leurs vulnérabilités et de déterminer les chemins d'attaque possibles sur ces systèmes.

Conduire des techniques et tactiques d'attaques de cybersécurité sur base des éléments collectés, en collaboration avec les experts (opérationnels métiers et informatiques) afin de prendre le contrôle du système cible.

Déterminer les risques et dommages pour le système d'information cible en évaluant l'impact fonctionnel d'une attaque en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données, afin de rédiger un rapport de test d'intrusion dans un format prenant en compte les éventuelles situations de handicap.

Communiquer l'ensemble des résultats d'un test d'intrusion à travers un rapport de synthèse, dans un format prenant en compte les éventuelles situations de handicap, afin de présenter à l'organisation sa surface d'exposition, ses vulnérabilités, leur criticité et leur impact.

Déterminer les mesures de sécurité permettant de traiter les risques et dommages présents dans le rapport de test d'intrusion, en collaboration avec les opérationnels métiers et informatiques, afin d'établir un plan de remédiation adapté.

MODALITÉS D'ÉVALUATION

Mise en situation simulée

Le candidat devra collecter les informations permettant de déterminer et de déployer une ou plusieurs techniques de tests d'intrusion éthiques. Il sera demandé au candidat d'explicitier sa démarche et de présenter les impacts et les résultats du test d'intrusion conduit.

Cette mise en situation s'appuie sur un environnement simulé d'une entreprise fictive et de son Système d'Information, d'une gouvernance (organigramme, politiques de sécurité...) et présentant une activité internationale multi-sites permettant au candidat de mener à bien un audit. Le candidat devra ensuite soumettre un rapport et le présenter en soutenance orale.

RNCP42503BC02 — Configurer les éléments de sécurité des infrastructures et des réseaux

LISTE DE COMPÉTENCES

Etablir les mesures de sécurité applicables en concevant une infrastructure réseau sécurisée afin de protéger les réseaux WAN, LAN et sans fil.

Configurer les éléments de sécurité des réseaux afin de mettre en place un réseau sécurisé répondant aux exigences de sécurité applicables à l'organisation

Mettre en oeuvre les règles de durcissement de la configuration des infrastructures informatiques et industrielles en s'appuyant sur des politiques internes, guides de bonnes pratiques, référentiels et cadrage internationaux, afin de renforcer la sécurité du système d'information.

Déployer des mesures de sécurité opérationnelles (chiffrement, contrôle d'accès, etc.) en s'appuyant sur les politiques internes, guides de bonnes pratiques, référentiels et cadrage internationaux afin de prévenir les risques de fuite de données.

Configurer les éléments de sécurité des systèmes connectés, en intégrant les spécificités de l'environnement et les enjeux du numérique responsable, afin de garantir l'intégrité et la disponibilité des systèmes.

Déployer des mesures de sécurité s'appuyant sur l'intelligence artificielle en collaboration avec les experts cybersécurité et les opérationnels métiers, afin de contenir les risques liés au déploiement de l'Intelligence Artificielle au sein d'un Système d'Information.

MODALITÉS D'ÉVALUATION

Etude de cas pratique

Il sera demandé au candidat, sur la base d'un ou plusieurs cas pratiques, de sélectionner et configurer les solutions techniques appropriées pour sécuriser une architecture réseau.

Cette mise en situation s'appuie sur un environnement simulé d'une entreprise fictive et de son Système d'Information, d'une gouvernance (organigramme, politiques de sécurité...) et présentant une activité internationale multi-sites permettant au candidat de mener à bien un audit technique.

Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.

RNCP42503BC03 — Sécuriser les données et les identités d'un système d'information existant

LISTE DE COMPÉTENCES

Mettre en oeuvre les mesures de sécurité des données, en fonction des contraintes et besoins fonctionnels de l'organisation, afin de garantir le niveau de confidentialité, d'intégrité et de disponibilité des données.

Traiter les vulnérabilités d'un projet à déployer sur un système d'information industriel existant, en prenant en compte les enjeux de souveraineté numérique, afin de limiter les impacts et les risques inhérents à la sécurité des données.

Déployer des solutions de sécurité permettant de prévenir les risques de fuite de données d'un système d'information existant, afin d'être conforme au système de management de la sécurité de l'information (SMSI) et aux normes environnementales.

Mettre en oeuvre les mesures de sécurité et les solutions techniques associées (contrôle d'accès, authentification...) adéquates pour assurer la sécurité des identités humaines, machines et services d'un environnement industriel.

Déployer des mesures de sécurité en adéquation avec les enjeux de souveraineté numérique et de numérique responsable, afin de contrôler les accès à privilèges.

Élaborer les standards techniques de sécurité et la documentation technique, applicables et accessibles aux personnes en situation de handicap, en fonction des solutions techniques mises en oeuvre, afin de répondre aux exigences du système de management de la sécurité de l'information (SMSI) et des normes environnementales.

MODALITÉS D'ÉVALUATION

Etude de cas pratique

Sur la base d'un ou plusieurs cas pratique, il sera demandé au candidat, dans le cadre d'un cas pratique, de mettre en oeuvre des mesures techniques de sécurité afin de sécuriser les données, des identités et des comptes à privilèges d'un Système d'Information existant.

Cette mise en situation s'appuie sur un environnement simulé d'une entreprise fictive, de journaux d'événements cyber et de rapports d'analyse. Les travaux seront formalisés dans un rapport.

RNCP42503BC04 — Détecter et analyser les événements de cybersécurité

LISTE DE COMPÉTENCES

Qualifier un événement de cybersécurité en fonction du comportement nominal du système d'information et des scénarios de gestion d'événements cyber (playbook), afin de le documenter, de déterminer son niveau de criticité et

d'appliquer le traitement associé

Définir la collecte, la conservation et l'archivage des journaux d'événements (logs) nécessaires, en fonction des scénarios de gestion d'événements cyber (playbooks) et en accord avec les contraintes et exigences de l'organisation (conformité, budget...), pour analyser le fonctionnement du système d'information

Adapter les scénarios de gestion d'événements cyber (playbook) en fonction de l'état la menace afin d'optimiser les détections des évènements de sécurité dans une optique d'amélioration continue

Programmer des règles de détection d'événements cyber en s'appuyant sur un usage raisonné des modèles d'intelligence artificielle en vue de qualifier les alertes de sécurité de façon automatisée

Documenter les évènements de sécurité en adoptant un langage et/ou des outils inclusifs adaptés pour permettre la mesure de l'impact au sein de l'organisation

MODALITÉS D'ÉVALUATION

Etude de cas pratique

Sur la base d'un ou plusieurs cas pratiques, il sera demandé au candidat de collecter, d'analyser et documenter les éléments techniques permettant de détecter et qualifier des événements de cybersécurité.

Cette mise en situation s'appuie sur un environnement simulé d'une entreprise fictive, de journaux d'évènements cyber et de rapports d'analyse. Les travaux seront formalisés dans un rapport.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le métier de spécialiste en cybersécurité s'exerce dans l'ensemble des organisations disposant d'un système d'information, indépendamment de leur taille ou de leur secteur d'activité. La transformation numérique généralisée des processus métiers a conduit toutes les structures – publiques comme privées – à dépendre fortement de leurs infrastructures numériques. Cette dépendance crée mécaniquement une exposition accrue aux risques cyber, rendant la fonction cybersécurité indispensable.

Le spécialiste en cybersécurité peut ainsi intervenir au sein d'entreprises de services numériques (ESN) et de cabinets de conseil spécialisés, où il réalise des missions pour le compte de clients variés. Il peut également exercer en interne dans des entreprises industrielles intégrant des systèmes d'information industriels (OT) ou des environnements connectés critiques. Les secteurs de l'énergie, des transports, de la défense, de l'aéronautique ou encore de la production manufacturière sont particulièrement concernés par les enjeux de sécurisation des systèmes industriels.

Le secteur tertiaire constitue également un important vivier d'emplois. Les établissements bancaires, les assurances, les acteurs du commerce en ligne, les entreprises de télécommunications ou les structures de santé manipulent des volumes significatifs de données sensibles et sont soumis à des obligations réglementaires renforcées en matière de protection des données et de continuité d'activité.

Les administrations publiques, les collectivités territoriales et les opérateurs d'importance vitale renforcent également leurs équipes de cybersécurité afin de répondre aux exigences de résilience numérique et aux obligations issues du cadre réglementaire européen. La cybersécurité devient ainsi un enjeu de service public et de souveraineté numérique.

Enfin, les éditeurs de logiciels, les fournisseurs de services cloud et les entreprises développant des solutions intégrant de l'intelligence artificielle ou des objets connectés mobilisent des spécialistes capables d'intégrer la sécurité dès la conception des produits et services.

Selon la structure d'accueil, le spécialiste en cybersécurité peut évoluer dans un environnement projet, au sein d'un centre opérationnel de sécurité (SOC), dans une équipe d'ingénierie ou dans une cellule dédiée à la gouvernance des systèmes d'information. Le contexte de travail peut être national ou international, avec des interventions sur site ou à distance, et impliquer une collaboration étroite avec des équipes techniques, métiers et de direction.

TYPE D'EMPLOIS ACCESSIBLES

Spécialiste en cybersécurité - Analyste cybersécurité - Analyste SOC - Analyste sécurité des systèmes d'information - Pentester - Administrateur systèmes et sécurité

RÉGLEMENTATIONS D'ACTIVITÉ

Le spécialiste en cybersécurité n'est pas une profession réglementée au sens strict, mais son exercice est fortement structuré par des obligations réglementaires, sectorielles et normatives.

Parmi les principaux textes structurant leurs activités figurent :

RGPD - règlement européen sur la protection des données personnelles
Directive NIS2 - renforcement des obligations de cybersécurité pour les Opérateurs de Services Essentiels (OSE)
Cyber Resilience Act (CRA) - exigences de sécurité pour les produits numériques tout au long de leur cycle de vie.
Digital Operational Resilience Act (DORA) - résilience opérationnelle du secteur financier.
Loi de Programmation Militaire (LPM) - obligations propres aux OIV.
European Digital Identity Wallet (e-DAS) - règlement européen sur l'identification électronique et les services de confiance (signature électronique, cachet serveur, horodatage, recommandés électroniques, etc.).
Payment Card Industry Data Security Standard (PCI-DSS) - standard international privé pour assurer la sécurité des données de cartes bancaires et réduire les risques de fraude et compromission des numéros de cartes

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
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)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (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)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique 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
Etre titulaire d'une certification professionnelle de niveau 5 ou équivalent, ayant une spécialité informatique ou cybersécurité, ou avoir une expérience significative ayant permis l'acquisition de compétences en informatique ou cybersécurité ; et avoir un niveau d'anglais permettant d'avoir une conversation professionnelle et de lire de la documentation technique

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE
Le jury de certification est constitué de trois membres :
un membre représentant du champ professionnel de la cybersécurité encadrant une ou plusieurs personnes exerçant le métier visé par la certification

un membre représentant du champ professionnel de la cybersécurité exerçant le métier visé par la certification
un membre de l'organisme certificateur

Base légale

Date de décision	26/06/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	26/06/2029
Date de dernière délivrance possible	26/06/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	17	0	100 %	—
2024	15	0	100 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP37987

CORRESPONDANCES (PAR BLOCS)
RNCP37987

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www.csb.school/formations/bachelor-cybersecurite-specialiste-cybersecurite/>

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/42503/>