

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

RNCP38951 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 344t
Formacode(s)	31006
Code(s) ROME	M1801, M1802, M1805, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	26/04/2024
Date d'échéance	26/04/2026

Certificateur(s)

2600 · SIRET : 89344030500025

2600 · SIRET : 89344030500017

Résumé de la certification

OBJECTIFS ET CONTEXTE

La croissance et la criticité des menaces et attaques cyber, alimentées par l'essor des échanges digitalisés et des innovations technologiques, exigent que les entreprises et les administrations renforcent leurs équipes avec des professionnels formés, qualifiés et compétents en matière de sécurité informatique. L'expert en cybersécurité joue un rôle crucial. Il réalise des audits techniques et organisationnels. Il définit des stratégies de sécurité essentielles à la pérennité de l'entreprise. Il lui revient de structurer une gestion défensive, basée sur une analyse approfondie de son organisation et de son système d'information, lui permettant d'agir de manière proactive face au risque cyber. Il est également tenu d'assurer la conformité légale du stockage et la gestion des données, en coordination avec la direction et le DPO (Délégué à la protection des données).

Ses missions englobent la prise en compte des comportements humains, l'élaboration de politiques, de directives de sécurité de l'information, ainsi que l'évaluation des risques. En outre, l'expert en cybersécurité est appelé à contribuer au développement de solutions sécurisées et à adopter une approche dynamique en intégrant des stratégies offensives, telles que des simulations d'attaques (RedTeam), afin de renforcer la résilience de l'entreprise. Parallèlement, il assume un rôle essentiel dans la gestion de crise et la planification de la continuité d'activité.

ACTIVITÉS VISÉES

- Apport de son expertise SSI aux organes de direction
- Prévention des risques de cybersécurité pour son organisation
- Gestion financière d'une entreprise ou d'un service dans le domaine de la SSI
- Réalisation d'une veille technologique sur l'actualité des vulnérabilités et des menaces dans le domaine de la cybersécurité
- Protection du SI
- Conduite d'un audit de sécurité technique d'une organisation
- Réalisation d'un rapport d'audit technique
- Respect de la législation lors de la réalisation d'un audit
- Conception sécurisée d'une architecture SI
- Conception sécurisée d'un logiciel
- Conception d'un outil de sécurité

Prévenir une crise en cybersécurité tout en permettant la continuité et/ou la reprise d'activité
Gérer une crise de cybersécurité en lien avec les équipes techniques et les institutions
Assurer la capitalisation des retours d'incident en mesure préventive et/ou corrective dans le PCA, le PRA, le SI ou la production

COMPÉTENCES ATTESTÉES

Auditer les pratiques professionnelles des collaborateurs pour identifier des possibilités d'amélioration dans leur mise en œuvre des normes (RGPD, ISO 2700x, ...), des standards et des règles liés à la sécurité informatique dans les architectures de systèmes d'information ou les applications

Élaborer des documents tels que des notes, des guides, des présentations et des directives pour l'organisation dans le but de minimiser les risques en matière de cybersécurité

Évaluer les risques de cybersécurité susceptibles de toucher son organisation
afin de renforcer sa résilience cyber

Sensibiliser ses collaborateurs, ses clients ou sa hiérarchie au risque cyber et à l'intérêt stratégique de la mise en place d'une politique de cybersécurité

Réaliser une veille technologique des solutions et des outils de cybersécurité dans le but de conseiller rapidement son organisation en prévention d'un danger imminent

Analyser l'écosystème cyber via une étude de marché et la création d'un business plan afin de convaincre de potentiels investisseurs

Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier (dashboards, outils de business intelligence, etc.) afin de garantir la viabilité de l'entreprise

Collecter et analyser les données provenant de sources de renseignements en sources ouvertes (OSINT = Open Source Intelligence) afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux

Analyser les menaces et les incidents (CTI - Cyber Threat Intelligence) après collecte d'informations en utilisant des sources ouvertes et privées ainsi que des outils spécialisés

Mettre en œuvre des outils de sécurité informatique pour surveiller, détecter et contrer les menaces, tels que les EDR, les XDR, les pare-feu, les systèmes de détection d'intrusion et les SIEM

Enquêter sur les intrusions et les incidents de sécurité à partir de journaux d'événements (logs), de rapports d'incidents et toute autre information disponible provenant d'un outil de défense

Réaliser une investigation par examen de la mémoire d'un matériel numérique et des artefacts des systèmes d'exploitation et des réseaux

Réaliser des tests d'intrusion sur les systèmes et les réseaux afin d'identifier leurs vulnérabilités

Réaliser des tests d'intrusion sur les applications web ou mobiles afin d'identifier leurs vulnérabilités

Auditer le code source d'une solution logicielle pour identifier les vulnérabilités et les failles de sécurité

Conduire une simulation d'intrusion malveillante multifactorielle en élaborant puis en exécutant des scénarios d'intrusion qui reproduisent les actions de cybercriminels en utilisant des techniques telles que l'ingénierie sociale, le vol, l'intrusion physique, et autres

Rapporter et communiquer les résultats d'un audit ou d'une investigation cyber en adaptant son support et son discours à la diversité du niveau d'expertise du public concerné afin de faire prendre des contre-mesures adaptées et ainsi réduire les risques d'attaque sur l'organisation

Réaliser un audit technique en respectant la législation en vigueur (en particulier le code pénal) et l'éthique

Concevoir l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de répondre au besoin fonctionnel de l'organisation en prenant en compte le plan de routage, le cloud, la localisation des services, le besoin exprimé de fonctionnalité du SI

Mettre en place des outils et des mesures de protection sur l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les solutions logicielles de déploiement d'architecture (ansible, puppet, ...) et les spécificités des systèmes visées (windows, linux, ...)

Concevoir des solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de répondre aux besoins fonctionnels du produit visé
en fonction des problématiques algorithmique, de performance, de l'architecture du code, et les interactions avec les bases de données.

Mettre en œuvre les solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les spécificités des

langages employés, des bibliothèques de fonctions, et des API de services tiers
Concevoir un outil de sécurité pour répondre à un besoin précis de son organisation
Contrôler l'application des consignes préventives de sécurité émises en phase conseil et lors de retour d'expérience à destination des équipes techniques afin de se préparer à une crise cyber
Planifier les missions des équipes techniques concernant l'application des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité
Piloter les équipes techniques en situation de crise de cybersécurité afin d'apporter, par son expertise, la capacité de réagir rapidement et de s'adapter aux imprévus non couverts par les documents préventifs préalablement établis (PCA,PRA, autres...)
S'appuyer sur les acteurs institutionnels de l'écosystème cyber (DGSI, ComCyberGend, ANSSI, CNIL...) pour aider à la résolution de la crise et initier une action auprès des acteurs appropriés
Analyser, en situation de crise de cybersécurité, les écarts entre les documents préventifs préalablement établis (PCA, PRA, autres...) et les incidents rencontrés afin d'alimenter le retour d'expérience
Conduire des enquêtes techniques de réponse à incident lors d'une crise cyber, permettant une identification des origines de l'attaque et une compréhension détaillée du modus operandi des attaquants

Blocs de compétences

RNCP38951BC01 — Conseiller une organisation en sécurité des systèmes d'information

LISTE DE COMPÉTENCES

Auditer les pratiques professionnelles des collaborateurs pour identifier des possibilités d'amélioration dans leur mise en œuvre des normes (RGPD, ISO 2700x, ...), des standards et des règles liés à la sécurité informatique dans les architectures de systèmes d'information ou les applications
Élaborer des documents tels que des notes, des guides, des présentations et des directives pour l'organisation dans le but de minimiser les risques en matière de cybersécurité
Évaluer les risques de cybersécurité susceptibles de toucher son organisation
afin de renforcer sa résilience cyber
Sensibiliser ses collaborateurs, ses clients ou sa hiérarchie au risque cyber et à l'intérêt stratégique de la mise en place d'une politique de cybersécurité
Réaliser une veille technologique des solutions et des outils de cybersécurité dans le but de conseiller rapidement son organisation en prévention d'un danger imminent
Analyser l'écosystème cyber via une étude de marché et la création d'un business plan afin de convaincre de potentiels investisseurs
Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier (dashboards, outils de business intelligence, etc.) afin de garantir la viabilité de l'entreprise

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

PRÉREQUIS À L'ENTRÉE

En formation continue : disposer d'une expérience professionnelle dans les domaines de l'informatique, du numérique ou dans un domaine connexe à la cybersécurité ou dans un domaine juridique, commercial ou RH

RNCP38951BC02 — Protéger une organisation contre les menaces numériques

LISTE DE COMPÉTENCES

Collecter et analyser les données provenant de sources de renseignements en sources ouvertes (OSINT = Open Source Intelligence) afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux
Analyser les menaces et les incidents (CTI - Cyber Threat Intelligence) après collecte d'informations en utilisant des sources ouvertes et privées ainsi que des outils spécialisés
Mettre en œuvre des outils de sécurité informatique pour surveiller, détecter et contrer les menaces, tels que les EDR, les XDR, les pare-feu, les systèmes de détection d'intrusion et les SIEM
Enquêter sur les intrusions et les incidents de sécurité à partir de journaux d'événements (logs), de rapports d'incidents et toute autre information disponible provenant d'un outil de défense
Réaliser une investigation par examen de la mémoire d'un matériel numérique et des artefacts des systèmes

d'exploitation et des réseaux

MODALITÉS D'ÉVALUATION

Mise en situation : le candidat est chargé de la protection des systèmes d'information d'une entreprise technologique qui est régulièrement ciblée par des attaques sophistiquées

Le candidat doit mettre en place une stratégie complète de veille et de protection

Production d'un rapport et soutenance devant un jury d'experts

PRÉREQUIS À L'ENTRÉE

En formation continue : disposer d'une expérience professionnelle dans les domaines de l'informatique, du numérique ou dans un domaine connexe à la cybersécurité

RNCP38951BC03 — Auditer la sécurité technique d'une organisation

LISTE DE COMPÉTENCES

Réaliser des tests d'intrusion sur les systèmes et les réseaux afin d'identifier leurs vulnérabilités

Réaliser des tests d'intrusion sur les applications web ou mobiles afin d'identifier leurs vulnérabilités

Auditer le code source d'une solution logicielle pour identifier les vulnérabilités et les failles de sécurité

Conduire une simulation d'intrusion malveillante multifactorielle en élaborant puis en exécutant des scénarios d'intrusion qui reproduisent les actions de cybercriminels en utilisant des techniques telles que l'ingénierie sociale, le vol, l'intrusion physique, et autres

Rapporter et communiquer les résultats d'un audit ou d'une investigation cyber en adaptant son support et son discours à la diversité du niveau d'expertise du public concerné afin de faire prendre des contre-mesures adaptées et ainsi réduire les risques d'attaque sur l'organisation

Réaliser un audit technique en respectant la législation en vigueur (en particulier le code pénal) et l'éthique

MODALITÉS D'ÉVALUATION

Mise en situation : audit technique d'une organisation

Production d'un rapport technique détaillé et présentation devant un jury d'experts

PRÉREQUIS À L'ENTRÉE

En formation continue : disposer d'une expérience professionnelle dans les domaines de l'informatique, du numérique ou dans un domaine connexe à la cybersécurité

RNCP38951BC04 — Concevoir des solutions techniques sécurisées

LISTE DE COMPÉTENCES

Concevoir l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de répondre au besoin fonctionnel de l'organisation en prenant en compte le plan de routage, le cloud, la localisation des services, le besoin exprimé de fonctionnalité du SI

Mettre en place des outils et des mesures de protection sur l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les solutions logicielles de déploiement d'architecture (ansible, puppet, ...) et les spécificités des systèmes visés (windows, linux, ...)

Concevoir des solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de répondre aux besoins fonctionnels du produit visé en fonction des problématiques algorithmique, de performance, de l'architecture du code, et les interactions avec les bases de données

Mettre en œuvre les solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les spécificités des langages employés, des bibliothèques de fonctions, et des API de services tiers

Concevoir un outil de sécurité pour répondre à un besoin précis de son organisation

MODALITÉS D'ÉVALUATION

Exercice pratique d'élaboration d'une architecture SI sécurisée

Exercice pratique de développement d'une solution logicielle sécurisée

Exercice pratique de développement d'un outil de sécurité

PRÉREQUIS À L'ENTRÉE

En formation continue : disposer d'une expérience professionnelle dans les domaines de l'informatique, du numérique ou dans un domaine connexe à la cybersécurité

RNCP38951BC05 — Gérer une crise cyber

LISTE DE COMPÉTENCES

Contrôler l'application des consignes préventives de sécurité émises en phase conseil et lors de retour d'expérience à destination des équipes techniques afin de se préparer à une crise cyber

Planifier les missions des équipes techniques concernant l'application des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité

Piloter les équipes techniques en situation de crise de cybersécurité afin d'apporter, par son expertise, la capacité de réagir rapidement et de s'adapter aux imprévus non couverts par les documents préventifs préalablement établis (PCA, PRA, autres...)

S'appuyer sur les acteurs institutionnels de l'écosystème cyber (DGSI, ComCyberGend, ANSSI, CNIL...) pour aider à la résolution de la crise et initier une action auprès des acteurs appropriés

Analyser, en situation de crise de cybersécurité, les écarts entre les documents préventifs préalablement établis (PCA, PRA, autres...) et les incidents rencontrés afin d'alimenter le retour d'expérience

Conduire des enquêtes techniques de réponse à incident lors d'une crise cyber, permettant une identification des origines de l'attaque et une compréhension détaillée du modus operandi des attaquants

MODALITÉS D'ÉVALUATION

Production d'un rapport contenant un compte rendu technique et situationnel sur le déroulement de la crise ainsi qu'un retour d'expérience dans le but d'améliorer la résilience cyber de l'organisation

Ce rapport est ensuite soutenu devant jury

PRÉREQUIS À L'ENTRÉE

En formation continue : disposer d'une expérience professionnelle dans les domaines de l'informatique, du numérique ou dans un domaine connexe à la cybersécurité ou dans un domaine juridique, commercial ou RH

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le professionnel peut exercer dans des entreprises de toute taille : de la TPE à la grande entreprise, et dans des secteurs d'activités variés.

TYPE D'EMPLOIS ACCESSIBLES

Analyste de la menace

Architecte SSI

Consultant en sécurité informatique

Chef de projet en management de la sécurité

DevSecOps

Expert cybersécurité

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

Ingénieur R&D en sécurité

Ingénieur sécurité des systèmes

Responsable de la sécurité des systèmes d'information

Responsable de SOC

Pentester

Expert DFIR

RÉGLEMENTATIONS D'ACTIVITÉ

Un expert en cyber sécurité ne relève pas d'une activité réglementée. En revanche, le domaine de la cybersécurité présente un certain nombre de réglementations :

Règlement général sur la protection des données (RGPD)

Normes de l'industrie : de nombreuses industries, telles que les services financiers et la santé, sont soumises à des réglementations spécifiques en matière de cybersécurité.

Directives sectorielles : certains secteurs, comme l'énergie et les infrastructures critiques, sont soumis à des directives spécifiques en matière de cybersécurité pour protéger leurs systèmes et leurs opérations.

Normes internationales : des normes internationales telles que ISO 27001 fournissent des directives pour l'établissement de systèmes de gestion de la sécurité de l'information (SMSI) efficaces.

Instruction ministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Instruction ministérielle n°300/SGDSN/ANSSI sur la protection contre les signaux compromettants
Cybersecurity Act européen.
De façon générale, l'ANSSI compile et diffuse la réglementation relative à la sécurité des systèmes d'informations.

Marché du travail

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

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION
En formation initiale : Etre titulaire d'un titre ou diplôme de niveau 5 ou 6 (mathématiques, informatique, numérique ou domaine connexe à la cybersécurité) ou équivalent (diplôme étranger...) ou d'une expérience professionnelle équivalente.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, CANDIDATURE INDIVIDUELLE, VAE
Le jury est composé de 4 membres dont 2 membres externes, professionnels de la cybersécurité

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	8 583 €
Selon la branche	7 600 € – 8 684 €
Prise en charge	Branches concernées
8 583 €	Valeur par défaut · 203 branches
8 684 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des Télécoms, CPNEFP des jardineries et graineteries
8 668 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 500 €	CNPE de la Plasturgie et des Composites, CPNEFP de la métallurgie
8 000 €	CPNE des industries de santé (CPNEIS)
7 912 €	CPNEFP dans les établissements d'enseignement privés sous contrat
7 600 €	CPNE Banque

Base légale

Date de décision	26/04/2024
Durée de l'enregistrement	2 ans
Date d'échéance de l'enregistrement	26/04/2026
Date de dernière délivrance possible	26/04/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	5	0	100 %	—
2023	5	5	100 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP35612

NOUVELLE(S) CERTIFICATION(S)
RNCP42335

CORRESPONDANCES (PAR BLOCS)
RNCP32121, RNCP35612, RNCP36072

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://ecole2600.com>

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/38951/>