

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

RNCP35612 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 344t
Formacode(s)	31006
Code(s) ROME	M1802, M1810, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/05/2021
Date d'échéance	19/05/2024

Certificateur(s)

2600 · SIRET : 89344030500017

Résumé de la certification

OBJECTIFS ET CONTEXTE

La numérisation croissante des échanges et des activités économiques ainsi que le développement et la complexification de la menace cyber obligent les entreprises et les administrations à se doter de personnels formés, qualifiés et compétents en matière de cybersécurité.

L'expert en cybersécurité est amené à réaliser des audits techniques et organisationnels, de définir la stratégie de sécurité nécessaire à la pérennité de l'entreprise. De mettre en place une gestion défensive de l'entreprise après une analyse de la structure et de réagir à mesure que la situation change.

Il peut notamment avoir la responsabilité des droits d'accès, des contrôles informatiques internes et externes, ainsi que de tout ce qui touche spécifiquement au domaine informatique. Les responsabilités peuvent également concerner les comportements humains, avec par exemple la création de contenus de sensibilisation destinés à toute l'entreprise, l'élaboration de politiques, directives et chartes de sécurité de l'information et l'évaluation des risques. Il est également tenu de gérer la conformité légale du stockage et de la gestion des données, sans pour autant en porter la responsabilité, qui en incombe à la direction et au DPO.

ACTIVITÉS VISÉES

Apporter son expertise SSI aux organes de direction.

Élaborer les stratégies de l'organisation dans le domaine de la SSI.

Réaliser une veille technologique sur l'actualité des vulnérabilités, des menaces et des produits dans le domaine de la cybersécurité.

Concevoir des solutions informatiques de façon sécurisée.

Auditer la sécurité informatique.

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.

Assurer la capitalisation des retours d'incident en mesure préventive et/ou corrective dans le PCA, le PRA, le SI ou la production.

Créer une entreprise innovante dans le domaine de la SSI.

COMPÉTENCES ATTESTÉES

Analyser les pratiques professionnelles des collaborateurs afin de proposer des améliorations dans leur application

des normes, des standards et du respect du droit relatifs à la sécurité informatique dans les architectures de SI, ou les applications.

Rédiger pour son organisation des notes, des guides, des présentations et/ou des directives d'application afin de réduire le risque en cybersécurité, qui s'appuient sur les éléments identifiés en phase d'analyse.

Conseiller son organisation sur l'utilisation et sur la portée stratégique des notes, guides, directives d'application rédigées après l'analyse.

Conseiller son organisation sur l'utilisation et sur la portée stratégique des notes, guides, directives d'application rédigées après l'analyse.

Analyser son organisation afin d'augmenter la cyber résilience de celle-ci, en étudiant les éléments suivants:

- Les menaces en cybersécurité relatives à l'activité de l'entreprise;
- Le plan de continuité d'activité relatif aux crises cyber sécurités (PCA);
- Le plan de reprise d'activité relatif aux crises cyber sécurités (PRA).

Rédiger des notes, des guides, des présentations afin d'éclairer sa hiérarchie et d'augmenter la cyber résilience, qui s'appuient sur les éléments identifiés en phase d'analyse de l'activité.

Défendre auprès de sa hiérarchie une vision stratégique en cybersécurité afin de prévenir le risque cyber sur le temps long.

Évaluer les solutions d'analyse de menace et de contre-mesure de type COTS (Component On The Shelf), OSINT (Open Source Intelligence), ou autre applicable sur le SI de l'organisation afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux.

Analyser les évolutions technologiques en cybersécurité (techniques d'attaque et de défense logiciels, matériels ou sociales) afin de maintenir son niveau d'expertise dans le domaine et d'identifier de "nouveaux" risques potentiels.

Participer aux innovations de la sécurité des SI publiés officiellement sur les canaux spécialisés (conférence, podcast, blog, ...) afin d'augmenter son expertise sur les potentiels risques pour le SI de l'organisation et mieux identifier de nouvelles attaques cyber.

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 œuvre 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.

Contrôler la bonne application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimées pendant l'activité de conseil concernant:

- La conception et le développement sécurisé d'applications lourdes, web ou embarquées.
- En conception et mise en œuvre d'architecture sécurisée de système d'information sur le SI de l'organisation.

Analyser les écarts entre les recommandations rédigées/exprimées pendant l'activité de conseil et la mise en œuvre technique afin d'établir des points de contrôle en utilisant les techniques d'attaques informatiques et les outils associés.

Contrôler l'application par le personnel en charge du SI de l'entreprise des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité.

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.

Évaluer les équipes techniques afin de réduire le risque en cybersécurité sur leur compréhension et leur application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimés pendant l'activité d'audit

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...)

Contrôler l'application des consignes 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.

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.

Rédiger un retour d'expérience sur les incidents rencontrés en crise cyber afin de maintenir et faire évoluer tous les documents préventifs préalablement établis (PCA, PRA, autres...).

Analyser l'écosystème cyber via une étude de marché afin d'identifier des opportunités de création d'entreprise.

Concevoir un business plan prenant en compte les éléments financiers prévisionnels, les opportunités du marché et les éléments commerciaux et marketing afin de convaincre de la solidité du projet auprès des futurs investisseurs.

Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier afin de garantir la viabilité de l'entreprise.

Blocs de compétences

RNCP35612BC01 — Conseiller son entreprise en sécurité des systèmes d'informations.

LISTE DE COMPÉTENCES

Analyser les pratiques professionnelles des collaborateurs afin de proposer des améliorations dans leur application des normes, des standards et du respect du droit relatifs à la sécurité informatique dans les architectures de SI, ou les applications.

Rédiger pour son organisation des notes, des guides, des présentations et/ou des directives d'application afin de réduire le risque en cybersécurité, qui s'appuient sur les éléments identifiés en phase d'analyse.

Conseiller son organisation sur l'utilisation et sur la portée stratégique des notes, guides, directives d'application rédigées après l'analyse.

Analyser son organisation afin d'augmenter la cyber résilience de celle-ci, en étudiant les éléments suivants:

- Les menaces en cybersécurité relatives à l'activité de l'entreprise;
- Le plan de continuité d'activité relatif aux crises cyber sécurités (PCA);
- Le plan de reprise d'activité relatif aux crises cyber sécurités (PRA).

Rédiger des notes, des guides, des présentations afin d'éclairer sa hiérarchie et d'augmenter la cyber résilience, qui s'appuient sur les éléments identifiés en phase d'analyse de l'activité.

Défendre auprès de sa hiérarchie une vision stratégique en cybersécurité afin de prévenir le risque cyber sur le temps long.

MODALITÉS D'ÉVALUATION

Exercices pratiques qui portent sur la conception, puis la rédaction des documents permettant de structurer l'organisation de la sécurité des SI en articulant un aspect sécurité (norme, standard, droit, ...) à la réalité de terrain de l'entreprise). Les documents sont ensuite défendus devant un jury.

Mise en situation au travers d'étude de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe, ...) nécessitant la rédaction d'un PCA (Plan de continuité d'activité) cyber et d'un PRA (Plan de reprise d'activité) cyber soutenu devant jury.

Mise en situation au travers d'étude de cas sur les stratégies cybers déployables dans des contextes précis et relatives à un type d'entreprise au choix (OIV, PMI, TPE, Grand groupe, ...). Les stratégies déployées sont soutenues devant jury.

RNCP35612BC02 — Évaluer techniquement la sécurité de l'entreprise.

LISTE DE COMPÉTENCES

Évaluer les solutions d'analyse de menace et de contre-mesure de type COTS (Component On The Shelf), OSINT (Open Source Intelligence), ou autre applicable sur le SI de l'organisation afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux.

Analyser les évolutions technologiques en cybersécurité (techniques d'attaque et de défense logicielles, matériels ou sociales) afin de maintenir son niveau d'expertise dans le domaine et d'identifier de "nouveaux" risques potentiels.

Participer aux innovations de la sécurité des SI publiés officiellement sur les canaux spécialisés (conférence, podcast, blog, ...) afin d'augmenter son expertise sur les potentiels risques pour le SI de l'organisation et mieux identifier de nouvelles attaques cyber.

Contrôler la bonne application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimées pendant l'activité de conseil concernant:

- La conception et le développement sécurisé d'applications lourdes, web ou embarquées.
- En conception et mise en œuvre d'architecture sécurisée de système d'information sur le SI de l'organisation

Analyser les écarts entre les recommandations rédigées/exprimées pendant l'activité de conseil et la mise en œuvre

technique afin d'établir des points de contrôle en utilisant les techniques d'attaques informatiques et les outils associés.

MODALITÉS D'ÉVALUATION

Exercices pratiques qui portent sur la mise en œuvre des techniques d'attaque/défense ou d'outils spécialisés sur une infrastructure de simulation et de correction automatique suivie de l'écriture de compte rendu technique.

Exercices pratiques qui portent sur l'investigation technique d'un projet informatique (SI, application, ...) afin de contrôler la présence ou l'absence de faille exploitable à des fins malveillantes soit manuellement, soit par des outils.

Mise en situation au travers de projets d'actualité de la cybersécurité afin de juger sa proactivité face à celle-ci. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de l'innovation apportée et sera soutenue oralement devant jury.

Mise en situation au travers d'étude de cas nécessitant la réalisation d'un Audit sécurité soutenus devant un jury.

RNCP35612BC03 — 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 œuvre 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.

MODALITÉS D'ÉVALUATION

Exercices pratiques qui portent sur la conception et la mise en œuvre d'un projet informatique (SI, application, ...) respectant l'application des bonnes pratiques en sécurité informatique.

Mise en situation au travers de projets informatiques complets et concrets respectant toutes les consignes de production sécurisée:

- Infrastructure SI partiel ou complète
- Applications (standard, web, embarquée, ...) d'une entreprise répondant à une expression de besoin. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de la solution apportée (en intégrant la composante sécurité) et sera soutenue oralement devant jury.

RNCP35612BC04 — Gérer une crise cyber

LISTE DE COMPÉTENCES

Evaluer les équipes techniques afin de réduire le risque en cybersécurité sur leur compréhension et leur application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimés pendant l'activité d'audit

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...)

Contrôler l'application des consignes 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.

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.

Rédiger un retour d'expérience sur les incidents rencontrés en crise cyber afin de maintenir et faire évoluer tous les documents préventifs préalablement établie (PCA, PRA, autres...).

MODALITÉS D'ÉVALUATION

Exercices pratiques sur le management humain, la prise de décision, le développement des "soft-skills" via des jeux de rôle.

Mise en situation au travers d'étude de cas portant sur l'analyse de PCA (Plan de continuité d'activité) cyber et de PRA (Plan de reprise d'activité) cyber sur lequel il faut identifier les points de contrôles dans l'organisation, planifier

les missions des équipes techniques pour la mise en conformité , synthétiser le tout dans un rapport soutenus devant un jury.

Mise en situation au travers de projets informatiques de groupe complets et concrets respectant toutes les consignes de production sécurisée:

- Infrastructure SI partiel ou complète
- Applications (standard, web, embarquée, ...) d'une entreprise répondant à une expression de besoin.

Mise en situation au travers de compétitions en équipe de sécurité chronométrées de type CTF (Capture the Flags) Jeopardy et/ou en Red/Blue team (attaque/défense) suivie de l'écriture de compte rendu technique et situationnel sur le déroulement du concours.

Mise en situation au travers de scénario de crise (type red/blue team), de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe) nécessitant la mise en application d'un PCA (Plan de continuité d'activité) cyber puis d'un PRA (Plan de reprise d'activité) cyber. Suivie de l'écriture de compte rendu technique et situationnel sur le déroulement de la crise soutenu devant jury.

RNCP35612BC05 — Entreprendre dans le secteur cyber.

LISTE DE COMPÉTENCES

Analyser l'écosystème cyber via une étude de marché afin d'identifier des opportunités de création d'entreprise.

Concevoir un business plan prenant en compte les éléments financiers prévisionnels, les opportunités du marché et les éléments commerciaux et marketing afin de convaincre de la solidité du projet auprès des futurs investisseurs.

Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier afin de garantir la viabilité de l'entreprise.

MODALITÉS D'ÉVALUATION

Exercices pratiques sur les activités courantes de la gestion d'entreprise: comptes de résultat, bilan, tableau de flux...

Mise en situation par la rédaction d'une analyse technologique du marché de la sécurité et des opportunités de création d'entreprise.

Mise en situation par la rédaction d'un Business Plan pour une entreprise type "moonshot".

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le secteur de la cybersécurité est devenu un enjeu majeur pour toutes les organisations, qu'il s'agisse des entreprises ou des institutions publiques. Les secteurs d'activité visés sont principalement ceux des Opérateurs d'Infrastructures Vitales des domaines suivants (250 OIV sont recensés en France) ou des OSE (Opérateurs de Services Essentiels)

L'Etat et l'armée, les banques et les finances, les opérateurs Internet et télécom, l'énergie : EDF, nucléaire, pétrole, gestion de l'eau, l'automobile, le naval, l'aéronautique, l'espace, la santé, le transport routier, portuaire, aérien, électronique.

Les secteurs d'activités suivants sont aussi adressés par cette certification:

- Les entreprises industrielles ou de services qui réalisent, maintiennent et supervisent les infrastructures des Opérateurs d'Infrastructures Vitales ou les Opérateurs de Services Essentiels

- Toutes entreprises industrielles, PME

ou de services dont le système d'information est ouvert sur l'Internet.

- Les entreprises de conseil en technologies.
- Les entreprises spécialisées dans le domaine de la cybersécurité

o PDIS

o PASSI

o PRIS

o FSN

Les secteurs d'activités couverts par cette formation sont donc très étendus.

La taille des entreprises varie donc de la PME où le salarié assume seul toutes les fonctions et activités, aux grandes entreprises ou institutions publiques. Ses fonctions sont alors définies par son employeur.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur(trice) système/réseau/base de donnée - Analyste de la menace - Architecte SSI - Consultant(e) en sécurité informatique - Chef(fe) de projet en management de la sécurité - Dev Sec Ops -Expert(e) cybersécurité -

Gestionnaire de la sécurité des données, des réseaux et des systèmes - Ingénieur(e) R&D en sécurité - Ingénieur(e) sécurité des systèmes - Responsable de la sécurité des systèmes d'information - Responsable de SOC.

Marché du travail

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

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

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre titulaire à minima d'un titre ou diplôme de niveau 5 ou 6 (mathématiques ou informatique) ou d'une expérience professionnelle équivalente.

COMPOSITION DU JURY — FORMATION INITIALE

Deux membres externes experts occupant l'une des fonctions suivantes : Directeur de la sécurité, RSSI, responsable SOC, entrepreneur dans le domaine de la cybersécurité (etc.) membres extérieurs à l'autorité délivrant la certification et n'ayant eu aucune part dans la délivrance de la formation.

Deux membres internes : le directeur de l'école et le directeur pédagogique.

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

Deux membres externes experts occupant l'une des fonctions suivantes : Directeur de la sécurité, RSSI, responsable

SOC, entrepreneur dans le domaine de la cybersécurité (etc.) membres extérieurs à l'autorité délivrant la certification et n'ayant eu aucune part dans la délivrance de la formation.

Deux membres internes : le directeur de l'école et le directeur pédagogique.

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	19/05/2021
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	19/05/2024

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP38951

Pour plus d'informations

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

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/35612/>