

Expert en cybersécurité

RNCP39999 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1801, M1802, M1805, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/12/2024
Date d'échéance	18/12/2027

Certificateur(s)

IKAI · SIRET : 90005795100031

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
THE PROGRESS FACTORY	85118370700013	Former et organiser l'évaluation
THE PROGRESS FACTORY	85118370700047	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Au cœur de la transformation numérique, la cybersécurité est essentielle au bon fonctionnement de nos entreprises, de nos institutions et plus largement, de nos sociétés. Un grand panel de métiers est nécessaire pour couvrir l'ensemble des enjeux stratégiques, techniques, opérationnels et organisationnels du secteur.

La certification atteste de l'acquisition à la fois des compétences globales essentielles pour travailler en cybersécurité et de certaines compétences spécifiques en fonction du métier visé. La spécialisation est clé pour atteindre le niveau requis pour devenir expert en cybersécurité. Cette certification d'expert en cybersécurité propose 3 spécialisations en audit, sécurité opérationnelle et développement sécurisé.

ACTIVITÉS VISÉES

- Évaluation des risques
- Gestion des risques
- Identification des besoins de sécurité de l'organisation.
- Définition d'un ensemble de mesures de protections des données du SI
- Mise en conformité légale et réglementaire
- Suivi de la mise en conformité
- Réalisation d'un projet de cybersécurité
- Communication d'une démarche de cybersécurité
- Mise en place un système de management d'audit de sécurité
- Réalisation d'un audit de sécurité d'un système d'information
- Gestion des événements et les incidents de sécurité de l'information
- Traitement des incidents de sécurité

COMPÉTENCES ATTESTÉES

Pour gérer les risques liés à la sécurité de l'information :

Identifier les actifs informationnels afin de déterminer leur importance pour l'organisation en réalisant un inventaire exhaustif et en évaluant leur criticité.

Identifier les sources de menaces en cybersécurité afin de déterminer leur probabilité en utilisant des méthodes d'analyse appropriées.

Évaluer les scénarios stratégiques et opérationnels des sources de menaces identifiées afin d'évaluer leur probabilité d'occurrences en se basant sur une méthode d'analyse de risques (Ex : EBIOS RM)

Estimer l'impact potentiel des risques en cybersécurité pour l'organisation en analysant les conséquences possibles sur les actifs informationnels.

Classifier les risques identifiés pour prioriser les actions de traitement en utilisant des critères d'impact et de probabilité en hiérarchisant les actions à mener.

Élaborer des stratégies de traitement des risques pour répondre aux résultats de l'évaluation des risques en proposant des méthodes de traitement du risque appropriées à l'organisation (réduction / transfert / refus) et en proposant des mesures en adéquation avec la méthode de traitement choisie

Mettre en œuvre le plan de traitement des risques en respectant les recommandations de l'analyse de risques afin de répondre aux exigences des normes et des politiques applicables au sein de l'organisation.

Suivre et réévaluer les risques de manière continue pour assurer une démarche d'amélioration continue en établissant des indicateurs de performance et de conformité

Proposer un plan de remédiation pour le traitement des risques en garantissant la conformité aux besoins et contraintes de l'organisation.

Pour protéger un système d'information face à la cyber-menace :

Cartographier un système d'information pour maintenir une vision claire des actifs à protéger en identifiant, classifiant et documentant tous les composants physiques et logiques du système leurs interconnexions, leurs dépendances et leur niveau de criticité.

Mettre en place un système de veille pour suivre les flux d'information liés aux menaces et aux vulnérabilités en identifiant et utilisant les sources d'informations pertinentes et en analysant les données recueillies.

Évaluer la pertinence des solutions de sécurité en réalisant un audit des mesures mises en œuvre et en évaluant leur impact sur la sécurité du système d'information.

Mettre en œuvre des mesures de durcissement du SI pour renforcer sa sécurité et réduire la surface d'attaque en configurant les paramètres de sécurité et en choisissant des mesures de sécurité adaptées à l'organisation.

Définir les paramètres de sécurité des composants logiques d'un système d'information, y compris les hyperviseurs, les containers, les orchestrateurs, les applications et les différents services critiques, afin de renforcer leur sécurité en suivant les politiques de l'organisation, et en se basant sur des référentiels de sécurité.

Classifier les données sensibles et s'assurer de l'efficacité des mesures de sécurité pour en assurer la confidentialité et l'intégrité en garantissant la conformité des usages aux politiques de gestion des identités et des données

Appliquer des mesures de sécurité sur les données pour assurer leur confidentialité et leur intégrité en fonction de leur niveau de criticité en se basant sur les référentiels, politiques, normes, lois et règlements auxquels sont soumis l'organisation.

Pour assurer la conformité du traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation :

Identifier les lois, règlements et normes applicables au sein de l'organisation afin de garantir la conformité en matière de sécurité des données traitées en effectuant une veille.

Évaluer la conformité actuelle des pratiques de l'organisation afin de détecter les écarts par rapport aux exigences légales en réalisant des audits et des revues documentaires.

Développer des politiques et des procédures de conformité pour répondre aux exigences légales et réglementaires en élaborant des documents clairs et détaillés.

Mettre en œuvre les mesures de conformité nécessaires afin de corriger les écarts identifiés et de prévenir les non-conformités en suivant un plan d'action structuré et une démarche d'amélioration continue.

Former et sensibiliser les employés sur les exigences légales et normatives afin d'assurer une compréhension et une application adéquates des règlements et procédures en organisant des sessions de formation et en fournissant des ressources pédagogiques adaptées aux personnes en situation de handicap et en évaluant l'efficacité des

campagnes de sensibilisation.

Suivre la conformité de manière continue pour assurer le respect des exigences légales et normatives en établissant des indicateurs de performance et en réalisant des audits réguliers.

Gérer les incidents de non-conformité afin de minimiser les impacts légaux et opérationnels en appliquant des procédures de gestion des incidents et des correctifs appropriés.

Documenter et communiquer les efforts de conformité pour démontrer l'engagement de l'organisation en matière de sécurité des données en produisant des rapports détaillés et accessibles.

Pour piloter un projet et communiquer en cybersécurité :

Identifier une problématique en cybersécurité afin de mettre en place un projet pour la résoudre en intégrant les besoins de l'organisation et en réalisant une veille sur les solutions existantes.

Rédiger un cahier des charges du projet pour répondre à la problématique de sécurité identifiée en normalisant le cadre de gestion du projet et les livrables du projet.

Concevoir un plan de gestion de projet afin d'assurer sa mise en œuvre en appliquant une méthode de gestion de projet définissant des objectifs, un calendrier, un budget et les livrables.

Identifier les risques liés au projet pour définir les mesures de sécurité nécessaires à mettre en œuvre en respectant l'ensemble des objectifs et contraintes du cahier des charges, du calendrier et du budget.

Assurer le suivi de la gestion de l'équipe projet afin d'atteindre les objectifs du projet, par l'application de technique de communication et leadership, en tenant compte des situations de handicap éventuelles de chacun.

Sensibiliser tous les membres de l'organisation aux enjeux de la cybersécurité afin de promouvoir des comportements sécurisés et responsables, en adaptant les supports et les méthodes de communication pour les personnes souffrant d'un handicap.

Développer un plan de communication adapté à l'ensemble des parties prenantes afin de veiller à la bonne exécution du projet en impliquant la direction et adaptant le plan à leurs fonctions et aux éventuels enjeux de communication pour les personnes en situation de handicap.

Synthétiser les résultats de la démarche afin de communiquer de manière claire et convaincante en identifiant et structurant les éléments clés du projet dans un rapport écrit et une présentation orale tenant compte des éventuelles personnes en situation de handicap.

Pour la spécialisation - Mener un audit de sécurité d'un système d'information :

Définir un contrat et un programme d'audit pour atteindre les objectifs fixés par l'organisation en identifiant les différents rôles et responsabilités et en fixant le périmètre d'audit.

Définir un système de management de suivi du programme d'audit pour assurer le suivi de l'audit en réalisant une analyse des résultats et en mettant en œuvre un système de gestion et de conservation des enregistrements des résultats d'audit.

Préparer les activités d'audit afin de suivre le plan d'audit défini en réalisant une revue documentaire et en préparant la répartition des tâches au sein de l'équipe de travail.

Suivre les activités d'audit pour répondre au plan d'audit établi en réalisant le suivi documentaire, la communication et la revue des informations produites.

Elaborer l'ensemble des documents nécessaire à la restitution de l'audit pour présenter les résultats obtenus en rédigeant un rapport et une synthèse claire à destination de la direction.

Présenter les conclusions de l'audit de manière claire et objective pour permettre à l'organisation de prendre des décisions stratégiques en se basant sur des indicateurs et les conclusions de l'audit.

Pour la spécialisation – Opérer et surveiller les mesures de sécurité d'un SI :

Déployer un système de surveillance de l'activité en sécurité de l'information pour détecter les événements et les incidents de sécurité, en intégrant leur traitement dans un processus de gestion d'incident et en prenant comptes des utilisateurs pouvant souffrir de handicap.

Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents.

Identifier et classer les alertes d'incidents des différents outils de sécurité présent (SIEM, XDR, EDR, IDS...) pour les intégrer au processus de gestion des incidents de sécurité en les priorisant en fonction du niveau de criticité et de leurs impacts.

Définir une stratégie de traitement des incidents de sécurité pour l'intégrer à l'organisation en veillant à ce qu'elle soit conforme aux processus et procédures en place dans l'organisation (Ex : PRA/PCA).

Définir un plan de traitement d'un incident de sécurité pour identifier son impact sur l'organisation en identifiant les différents sous-systèmes impactés par l'attaque et en documentant un plan de résolution d'incident.

Suivre le traitement des incidents de sécurité afin d'être en mesure d'identifier les forces et faiblesses de

l'organisation en mesurant l'efficacité des processus et en l'intégrant dans une démarche d'amélioration continue.

Vérifier l'efficacité de la stratégie de traitement des incidents de sécurité pour l'intégrer dans une démarche d'amélioration continue en réalisant des tests réguliers des procédures et processus établis (Ex : PRA/PCA).

Pour la spécialisation – Intégrer des outils de sécurité dans un environnement hétérogène :

Identifier l'ensemble des actifs matériels, logiciels et humains nécessaires pour intégrer une solution de sécurité en prenant en compte les différentes interactions des sous-systèmes (e.g SCADA, IoT, cloud...).

Identifier l'ensemble des interconnexions des sous-systèmes pour mettre en œuvre une stratégie de déploiement des outils de sécurité en les intégrant dans un environnement hybride.

Identifier les potentiels impacts de la mise en production d'une solution de sécurité afin de l'intégrer dans une infrastructure existante en évitant les phénomènes de régression et en limitant les pannes.

Mettre en œuvre des stratégies de déploiement de mesures et services de sécurité pour rendre les sous-systèmes inter-opérables en les intégrant dans la chaîne d'approvisionnement de l'organisation et en respectant les contraintes métiers.

Intégrer des mesures et services de sécurité dans un système hybride (e.g Cloud privé/public, hyperviseurs/containers...) afin de réduire l'impact d'une attaque sur un sous-système en intégrant cette solution dans l'infrastructure existante.

Mettre en place des moyens de contrôle et de surveillance des flux pour en garantir la sécurité en prenant en compte l'ensemble des contraintes métiers liées à l'activité de l'organisation.

Contrôler l'efficacité des mesures et services de sécurité pour les intégrer dans une démarche d'amélioration continue en définissant des indicateurs et en réalisant des audits réguliers.

Blocs de compétences

RNCP39999BC01 — Gérer les risques liés à la sécurité de l'information

LISTE DE COMPÉTENCES

Identifier les actifs informationnels afin de déterminer leur importance pour l'organisation en réalisant un inventaire exhaustif et en évaluant leur criticité.

Identifier les sources de menaces en cybersécurité afin de déterminer leur probabilité en utilisant des méthodes d'analyse appropriées.

Évaluer les scénarios stratégiques et opérationnels des sources de menaces identifiées afin d'évaluer leur probabilité d'occurrences en se basant sur une méthode d'analyse de risques (Ex : EBIOS RM)

Estimer l'impact potentiel des risques en cybersécurité pour l'organisation en analysant les conséquences possibles sur les actifs informationnels.

Classifier les risques identifiés pour prioriser les actions de traitement en utilisant des critères d'impact et de probabilité en hiérarchisant les actions à mener.

Élaborer des stratégies de traitement des risques pour répondre aux résultats de l'évaluation des risques en proposant des méthodes de traitement du risque appropriées à l'organisation (réduction / transfert / refus) et en proposant des mesures en adéquation avec la méthode de traitement choisie

Mettre en œuvre le plan de traitement des risques en respectant les recommandations de l'analyse de risques afin de répondre aux exigences des normes et des politiques applicables au sein de l'organisation.

Suivre et réévaluer les risques de manière continue pour assurer une démarche d'amélioration continue en établissant des indicateurs de performance et de conformité

Proposer un plan de remédiation pour le traitement des risques en garantissant la conformité aux besoins et contraintes de l'organisation.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Analyse de risque d'un SI : Les candidats se voient présenter un cas d'une entreprise réelle ou fictive à l'aide d'une documentation précise sur son activité et ses ressources incluant son système d'information. Leur tâche est de réaliser et présenter une analyse de risque en adéquation avec les besoins et contraintes de l'organisation et de proposer un plan de traitement des risques.

RNCP39999BC02 — Protéger un système d'information face à la cyber-menace

LISTE DE COMPÉTENCES

Cartographier un système d'information pour maintenir une vision claire des actifs à protéger en identifiant, classifiant et documentant tous les composants physiques et logiques du système leurs interconnexions, leurs dépendances et

leur niveau de criticité.

Mettre en place un système de veille pour suivre les flux d'information liés aux menaces et aux vulnérabilités en identifiant et utilisant les sources d'informations pertinentes et en analysant les données recueillies.

Évaluer la pertinence des solutions de sécurité en réalisant un audit des mesures mises en œuvre et en évaluant leur impact sur la sécurité du système d'information.

Mettre en œuvre des mesures de durcissement du SI pour renforcer sa sécurité et réduire la surface d'attaque en configurant les paramètres de sécurité et en choisissant des mesures de sécurité adaptées à l'organisation.

Définir les paramètres de sécurité des composants logiques d'un système d'information, y compris les hyperviseurs, les containers, les orchestrateurs, les applications et les différents services critiques, afin de renforcer leur sécurité en suivant les politiques de l'organisation, et en se basant sur des référentiels de sécurité.

Classer les données sensibles et s'assurer de l'efficacité des mesures de sécurité pour en assurer la confidentialité et l'intégrité en garantissant la conformité des usages aux politiques de gestion des identités et des données

Appliquer des mesures de sécurité sur les données pour assurer leur confidentialité et leur intégrité en fonction de leur niveau de criticité en se basant sur les référentiels, politiques, normes, lois et règlements auxquels sont soumis l'organisation.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Renforcer la sécurité technique d'un SI : Les candidats se voient présenter le système d'information d'une organisation réelle ou fictive comprenant notamment : un schéma d'infrastructure, la description des caractéristiques techniques, le registre des données utilisées ainsi qu'un cahier des charges. Leur tâche est de proposer un plan d'action en vue de sécuriser l'infrastructure en veillant à la conformité des solutions proposées vis-à-vis des normes et standards en fonction de l'activité de l'organisation tout en respectant les exigences du cahier des charges.

RNCP39999BC03 — Assurer la conformité du traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation

LISTE DE COMPÉTENCES

Identifier les lois, règlements et normes applicables au sein de l'organisation afin de garantir la conformité en matière de sécurité des données traitées en effectuant une veille.

Évaluer la conformité actuelle des pratiques de l'organisation afin de détecter les écarts par rapport aux exigences légales en réalisant des audits et des revues documentaires.

Développer des politiques et des procédures de conformité pour répondre aux exigences légales et réglementaires en élaborant des documents clairs et détaillés.

Mettre en œuvre les mesures de conformité nécessaires afin de corriger les écarts identifiés et de prévenir les non-conformités en suivant un plan d'action structuré et une démarche d'amélioration continue.

Former et sensibiliser les employés sur les exigences légales et normatives afin d'assurer une compréhension et une application adéquates des règlements et procédures en organisant des sessions de formation et en fournissant des ressources pédagogiques adaptées aux personnes en situation de handicap et en évaluant l'efficacité des campagnes de sensibilisation.

Suivre la conformité de manière continue pour assurer le respect des exigences légales et normatives en établissant des indicateurs de performance et en réalisant des audits réguliers.

Gérer les incidents de non-conformité afin de minimiser les impacts légaux et opérationnels en appliquant des procédures de gestion des incidents et des correctifs appropriés.

Documenter et communiquer les efforts de conformité pour démontrer l'engagement de l'organisation en matière de sécurité des données en produisant des rapports détaillés et accessibles.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Etude de conformité légale, réglementaire ou normatif : Le candidat présente un projet d'étude de conformité légale, réglementaire ou normatif mené de bout en bout sur un sujet de sécurité des données personnelles ou de la sécurité des systèmes d'information par rapport à une loi, une réglementation ou une norme.

RNCP39999BC04 — Piloter un projet et communiquer en cybersécurité

LISTE DE COMPÉTENCES

Identifier une problématique en cybersécurité afin de mettre en place un projet pour la résoudre en intégrant les besoins de l'organisation et en réalisant une veille sur les solutions existantes.

Rédiger un cahier des charges du projet pour répondre à la problématique de sécurité identifiée en normalisant le

cadre de gestion du projet et les livrables du projet.

Concevoir un plan de gestion de projet afin d'assurer sa mise en œuvre en appliquant une méthode de gestion de projet définissant des objectifs, un calendrier, un budget et les livrables.

Identifier les risques liés au projet pour définir les mesures de sécurité nécessaires à mettre en œuvre en respectant l'ensemble des objectifs et contraintes du cahier des charges, du calendrier et du budget.

Assurer le suivi de la gestion de l'équipe projet afin d'atteindre les objectifs du projet, par l'application de technique de communication et leadership, en tenant compte des situations de handicap éventuelles de chacun.

Sensibiliser tous les membres de l'organisation aux enjeux de la cybersécurité afin de promouvoir des comportements sécurisés et responsables, en adaptant les supports et les méthodes de communication pour les personnes souffrant d'un handicap.

Développer un plan de communication adapté à l'ensemble des parties prenantes afin de veiller à la bonne exécution du projet en impliquant la direction et adaptant le plan à leurs fonctions et aux éventuels enjeux de communication pour les personnes en situation de handicap.

Synthétiser les résultats de la démarche afin de communiquer de manière claire et convaincante en identifiant et structurant les éléments clés du projet dans un rapport écrit et une présentation orale tenant compte des éventuelles personnes en situation de handicap.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Gestion de projet en cybersécurité : Le candidat doit travailler sur un projet ayant une problématique de cybersécurité clairement définie. Le candidat est libre de choisir la problématique et peut réaliser le projet en groupe. L'évaluation finale se fera au travers d'une soutenance où les résultats et l'impact du projet seront présentés et devront répondre à la problématique de sécurité identifiée au lancement du projet.

RNCP39999BC05 — Mener un audit de sécurité d'un système d'information (spécialisation)

LISTE DE COMPÉTENCES

Définir un contrat et un programme d'audit pour atteindre les objectifs fixés par l'organisation en identifiant les différents rôles et responsabilités et en fixant le périmètre d'audit.

Définir un système de management de suivi du programme d'audit pour assurer le suivi de l'audit en réalisant une analyse des résultats et en mettant en œuvre un système de gestion et de conservation des enregistrements des résultats d'audit.

Préparer les activités d'audit afin de suivre le plan d'audit défini en réalisant une revue documentaire et en préparant la répartition des tâches au sein de l'équipe de travail.

Mettre en œuvre les activités d'audit (tests d'intrusion, évaluations de vulnérabilités, etc.) afin d'identifier les failles de sécurité en suivant les procédures d'audit établies et en utilisant des outils et techniques appropriés.

Suivre les activités d'audit pour répondre au plan d'audit établi en réalisant le suivi documentaire, la communication et la revue des informations produites.

Elaborer l'ensemble des documents nécessaire à la restitution de l'audit pour présenter les résultats obtenus en rédigeant un rapport et une synthèse claire à destination de la direction.

Présenter les conclusions de l'audit de manière claire et objective pour permettre à l'organisation de prendre des décisions stratégiques en se basant sur des indicateurs et les conclusions de l'audit.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Réalisation d'un audit de sécurité : Le candidat réalise un audit de sécurité qu'il soit organisationnel, intrusif, réseau, de vulnérabilités, de code ou de conformité sur une organisation réelle ou fictive. L'ensemble des données nécessaire pour réaliser l'audit est mis à disposition du candidat. Le candidat réalisera l'audit et produira un rapport d'audit conforme au plan d'audit et permettant à l'organisation d'avoir une vision claire de sa maturité sur le sujet de l'audit. Il défendra ce rapport lors d'une soutenance orale.

RNCP39999BC06 — Opérer et surveiller les mesures de sécurité d'un SI (spécialisation)

LISTE DE COMPÉTENCES

Déployer un système de surveillance de l'activité en sécurité de l'information pour détecter les événements et les incidents de sécurité, en intégrant leur traitement dans un processus de gestion d'incident et en prenant comptes des utilisateurs pouvant souffrir de handicap.

Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents.

Identifier et classer les alertes d'incidents des différents outils de sécurité présent (SIEM, XDR, EDR, IDS...) pour

les intégrer au processus de gestion des incidents de sécurité en les priorisant en fonction du niveau de criticité et de leurs impacts.

Définir une stratégie de traitement des incidents de sécurité pour l'intégrer à l'organisation en veillant à ce qu'elle soit conforme aux processus et procédures en place dans l'organisation (Ex : PRA/PCA).

Définir un plan de traitement d'un incident de sécurité pour identifier son impact sur l'organisation en identifiant les différents sous-systèmes impactés par l'attaque et en documentant un plan de résolution d'incident.

Suivre le traitement des incidents de sécurité afin d'être en mesure d'identifier les forces et faiblesses de l'organisation en mesurant l'efficacité des processus et en l'intégrant dans une démarche d'amélioration continue.

Vérifier l'efficacité de la stratégie de traitement des incidents de sécurité pour l'intégrer dans une démarche d'amélioration continue en réalisant des tests réguliers des procédures et processus établis (Ex : PRA/PCA).

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Mise en œuvre d'un SOC : A partir de l'étude d'une organisation fictive ou réelle, le candidat doit créer un « proof of concept » de mise en œuvre d'un SOC dans l'organisation. Ce « proof of concept » comprend une infrastructure web sur laquelle un SIEM est déployé, des indicateurs sont créés, les processus et procédures de résolution d'incidents établies, suivis et évalués. Le système est testé par la simulation d'un incident de sécurité.

RNCP39999BC07 — Intégrer des outils de sécurité dans un environnement hétérogène (spécialisation)

LISTE DE COMPÉTENCES

Identifier l'ensemble des actifs matériels, logiciels et humains nécessaires pour intégrer une solution de sécurité en prenant en compte les différentes interactions des sous-systèmes (e.g SCADA, IoT, cloud...).

Identifier l'ensemble des interconnexions des sous-systèmes pour mettre en œuvre une stratégie de déploiement des outils de sécurité en les intégrant dans un environnement hybride.

Identifier les potentiels impacts de la mise en production d'une solution de sécurité afin de l'intégrer dans une infrastructure existante en évitant les phénomènes de régression et en limitant les pannes.

Mettre en œuvre des stratégies de déploiement de mesures et services de sécurité pour rendre les sous-systèmes inter-opérables en les intégrant dans la chaîne d'approvisionnement de l'organisation et en respectant les contraintes métiers.

Intégrer des mesures et services de sécurité dans un système hybride (e.g Cloud privé/public, hyperviseurs/containers...) afin de réduire l'impact d'une attaque sur un sous-système en intégrant cette solution dans l'infrastructure existante.

Mettre en place des moyens de contrôle et de surveillance des flux pour en garantir la sécurité en prenant en compte l'ensemble des contraintes métiers liées à l'activité de l'organisation.

Contrôler l'efficacité des mesures et services de sécurité pour les intégrer dans une démarche d'amélioration continue en définissant des indicateurs et en réalisant des audits réguliers.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle - Intégration d'un outil de sécurité : A partir d'une infrastructure hétérogène (Industriel ; logistique ; IoT embarqué...) fictive ou réelle, le candidat propose diverses solutions de sécurité à mettre en œuvre pour augmenter la sécurité du traitement et des échanges d'informations. Les solutions mises en œuvre peuvent être du type firewall, IDS, XDR, WAF, NAC, data diode...

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La certification permet de travailler dans tous les secteurs d'activités, la cybersécurité étant un enjeu pour toutes les entreprises petites, grandes et moyennes ainsi que pour les organismes publics.

Les secteurs d'activités les plus exposés au risque cyber sont les suivants :

Technologies de l'information (TI) : Les entreprises de ce secteur, y compris les fournisseurs de cloud, les hébergeurs, et les entreprises de développement logiciel, sont constamment exposées aux cybermenaces. Elles doivent donc intégrer des outils de sécurité adaptés à des environnements diversifiés, surveiller les systèmes en temps réel, et s'assurer de leur conformité.

Finance et Assurance : La protection des données financières et personnelles est critique. Les institutions financières doivent se conformer à des réglementations strictes (ex. : RGPD, PCI-DSS) tout en surveillant en permanence les systèmes pour détecter et prévenir les intrusions.

Secteur Public : Les organismes publics gèrent des infrastructures critiques et des données sensibles et stratégiques. Ils doivent non seulement se protéger contre les cybermenaces, mais aussi se conformer à des réglementations spécifiques tout en intégrant des solutions de sécurité dans des environnements souvent hétérogènes et faisant intervenir de nombreux prestataires externes.

Santé : Les systèmes d'information de santé doivent protéger les données des patients tout en respectant des réglementations strictes (ex. : HDS / HIPAA). Les professionnels doivent être capables d'intégrer des outils de sécurité et de surveiller en continu la sécurité des systèmes dans des environnements souvent repartis sur plusieurs sites.

Industrie et Énergie : La cybersécurité est cruciale pour protéger les systèmes de contrôle industriels (ICS/SCADA) contre les attaques. Les professionnels doivent être capables de mener des audits, de gérer les risques, d'intégrer des outils de sécurité, et de surveiller en temps réel les systèmes pour éviter des perturbations dans des secteurs stratégiques.

TYPE D'EMPLOIS ACCESSIBLES

Responsable de la sécurité des systèmes d'information (RSSI) ; Consultant en cybersécurité ; Chef de Projet cybersécurité ; Responsable d'audit de Sécurité ; Pentester ; Opérateur de Sécurité (Analyste SOC) ; Intégrateur de Solutions de Sécurité ; Analyste de la menace ; Analyste DFIR (Digital Forensic & Incident Response) ; Architecte de la sécurité des systèmes d'information

RÉGLEMENTATIONS D'ACTIVITÉ

Le Règlement UE n°2016/679 dit « RGPD »

La directive "Network and Information System Security" dit "NIS" adoptée le 6 juillet 2016

La directive "Network and Information Systems Security 2" dite "NIS2", adoptée le 28 novembre 2022

Le règlement UE n°2019/881 dit « Cybersecurity Act » adopté le 12 mars 2019

La loi pour la confiance dans l'économie numérique (LCEN), promulguée le 21 juin 2004

Le code pénal français

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

Pour intégrer la formation en alternance, respecter au moins une des conditions suivantes :

- maîtriser les compétences de base en réseau, programmation et système informatique
- être titulaire d'une certification de niveau 5 ou 6 en informatique, mathématiques ou domaines connexes à la cybersécurité
- justifier d'une expérience professionnelle en informatique d'au moins 530 heures

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

1 responsable pédagogique du centre de formation (Directeur pédagogique ou enseignant en charge d'un module lié au bloc de compétences évalué) et 2 professionnels exerçant en entreprise, externes au centre de formation

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	9 000 €
Selon la branche	7 697 € – 9 157 €
Prise en charge	Branches concernées
9 000 €	Valeur par défaut · 186 branches
9 157 €	CPNE Casinos, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms
8 696 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Import-Export
9 005 €	CPNE FP Branche des magasins du Bricolage
8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 711 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 519 €	CPNE Industrie pétrolière
8 500 €	CPNEFP de la métallurgie
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	18/12/2024
------------------	------------

Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	18/12/2027
Date de dernière délivrance possible	18/12/2031

Statistiques

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

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36122

CORRESPONDANCES (PAR BLOCS)

RNCP36122, RNCP38951

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39999/>