

Expert en cybersécurité et sécurité informatique

RNCP36924 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31006, 42881, 31094, 13235
Code(s) ROME	M1802, M1805, M1803, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/09/2022
Date d'échéance	29/09/2025

Certificateur(s)

ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE · SIRET : 39350481600355

ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM) · SIRET : 39350481600231

Partenaires habilités

26 organismes habilités, d'après la liste publiée par France compétences : 26 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600330	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600090	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600215	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600223	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600231	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600249	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600272	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600298	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600306	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600314	Former et organiser l'évaluation

Liste complète des 26 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp36924-expert-en-cybersecurite-et-securite-informatique/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Reconnue comme étant un enjeu majeur pour les entreprises, La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés.

Lors du dernier forum sur la cybersécurité organisé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), l'agence alertait sur le fait que la menace allait croître fortement entre 2019 et 2020 avec des attaques encore plus complexes, massives et sophistiquées. Face à cet enjeu de taille, la confiance dans le numérique est devenue une approche stratégique majeure pour toutes les grandes sociétés ces dernières années. Le développement de compétences en cybersécurité pour être capables de construire des systèmes sûrs s'impose plus que jamais comme une nécessité. De nouveaux métiers se créent

comme le métier d'expert en cybersécurité et sécurité informatique, chargé de veiller à la sécurité des données présentes dans un service d'information, d'évaluer le système et de tout mettre en œuvre pour éviter les intrusions ou les détournements de ces informations.

ACTIVITÉS VISÉES

Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance

: Analyse de la sécurité du S.I existant ; Définition de la stratégie de sécurité et cybersécurité ; Conseil et veille stratégique auprès de la gouvernance

Pilotage de projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante : Management d'équipe interne et externe à l'entreprise ; Manager selon une démarche agile ; Accompagnement de l'équipe en favorisant un processus de communication adéquat

Déploiement d'une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et faire face aux cyber-menaces : Organisation d'une architecture fonctionnelle de sécurité informatique et cybersécurité ; Déploiement d'une Architecture technique de sécurité ; Intégration de la Data science pour la détection et la prévention des menaces

Supervision, audit et gestion de la sécurité informatique et des cyberattaques : Supervision et audit de la sécurité ; Gestion des risques liés à la cybersécurité et accompagnement lors d'une cyberattaque

COMPÉTENCES ATTESTÉES

Étudier le système d'information d'une structure dans sa globalité, en identifiant les points faibles du système, afin d'évaluer le niveau de sécurité au sein de l'organisation

Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et vis-à-vis des tiers et sous-traitants et les exigences de conformité légale afin de garantir à l'entreprise d'être en conformité vis à vis de la réglementation française en matière de droit informatique ainsi que la bonne mise en application des normes et certifications du domaine

Décliner les axes et les objectifs stratégiques en matière de sécurité informatique et cybersécurité afin de sensibiliser la Direction générale au sujet et lui permettre de vérifier sa bonne correspondance avec la stratégie de développement de l'entreprise

Définir la feuille de route stratégique adaptée aux besoins et à la culture de la structure, en lien avec les parties prenantes (informaticiens et les responsables des services) concernés afin de répondre à des objectifs de sécurité métiers et IT stratégiques face à l'augmentation de la cybermenace

Définir une stratégie de mise en conformité en lien avec la réglementation RGPD et le droit informatique afin de proposer un descriptif du process de la sécurité tenant compte de ce paramètre et ainsi, faciliter les relations avec les autorités de régulation en cas de contrôle réglementaires (auditeur RGPD et CNIL principalement)

Définir les mesures organisationnelles et techniques permettant de minimiser les risques liés à la sécurité du système d'information dans le but d'assurer une protection optimale et appropriée des données de l'entreprise et atteindre ainsi les objectifs de sécurité définis par la gouvernance

Définir l'organisation de la cybersécurité en proposant une charte de sécurité informatique de l'organisation afin de sensibiliser régulièrement les équipes et évaluer leurs connaissances en matière de règle de sécurité informatique

Concevoir un référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes...) permettant de formaliser, de justifier les choix, de légitimer les plans d'action et de garantir la cohérence avec le contexte particulier de l'organisme

Conseiller l'organisation en proposant des préconisations et des recommandations sur l'amélioration du niveau de sécurité afin de lui permettre une meilleure compréhension des enjeux et risques de cybermenaces et augmenter sa

capacité de gestion de crises

Informar les directions générales et les directions métiers sur les enjeux de la sécurité informatique, cybersécurité et l'état de la menace afin de les sensibiliser sur l'évolution du contexte de la sécurité et la cybersécurité en utilisant des supports de communication inclusifs

Apporter une expertise juridique auprès de la gouvernance en matière de conformité (à une réglementation, à des référentiels d'exigences) afin de fournir aux dirigeants des entreprises les règles et les bonnes pratiques à appliquer face aux nouvelles exigences en matière de conformité réglementaire

Identifier l'ensemble des étapes de réalisation du système d'information pour organiser le projet en tâches et livrables en répartissant les activités en fonction des ressources humaines (tous profils confondus), techniques et financières à mobiliser

Concevoir les cahiers des charges technique et fonctionnel d'un projet de développement S.I. à l'aide des besoins utilisateurs collectés afin de cadrer le développement?

Piloter les prestataires extérieurs éventuels gérant les ressources informatiques d'un système d'information existant listées dans la cartographie établie afin de sécuriser la mise en œuvre technique

Établir des tableaux de bord de suivi de performance (qualitative et quantitative) de l'ensemble des ressources allouées à chaque étape-projet pour anticiper, visualiser et corriger les écarts en temps réel afin de limiter les contraintes de ressources et les retards

Gérer un projet agile en utilisant les méthodes et outils adaptés à ce mode de fonctionnement pour tester, modifier et procéder par itération afin de réduire les délais de remise des projets de développement S.I.

Conduire une équipe projet en diffusant les fondamentaux de l'agilité?: adaptation, flexibilité et amélioration continue au sein de l'équipe afin d'être en mesure d'absorber les changements de priorité qui peuvent intervenir dans un contexte de forte contrainte de temps et d'incertitudes

Proposer des solutions innovantes afin de favoriser les interactions et l'inclusion au sein de l'équipe et d'anticiper des conflits de travail liés aux malentendus multiculturels et des profils en situation d'handicap

Accompagner l'équipe dans l'appropriation du travail à distance ou du télétravail en proposant des solutions managériales afin de favoriser la motivation et la résilience et permettre ainsi de préserver l'équilibre entre vie professionnelle/vie privée dans un souci de productivité et de bien-être

Concevoir un processus de communication inclusif régulier au sein de l'équipe afin de synchroniser les activités quotidiennes et mettre en place un fil de discussion à l'aide d'outils numériques

Communiquer avec l'équipe en adoptant les modes de communication adéquats selon les cultures et la langue des collaborateurs afin de garantir l'intégration de tous les membres de l'équipe

Animer des réunions à distance afin de maintenir une dynamique de groupe et renforcer l'esprit d'équipe des membres en télétravail et/ou à distance

Concevoir un processus de partage d'information afin de faciliter la collaboration entre les membres (tous profils confondus) en télétravail et/ou à distance en utilisant des outils numériques

Assurer la mise en place des structures organisationnelles des plans d'actions de sécurité au sein des entités afin de garantir la protection de données et le niveau de sécurité du système d'information

Paramétrer les mesures organisationnelles permettant la surveillance de la sécurité globale d'une organisation (des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques) afin d'assurer la mise en place d'un SOC (Security Operation Center)

Déployer les mesures organisationnelles de sécurité en se basant sur la stratégie de sécurité informatique de l'organisation afin d'assurer le fonctionnement opérationnel et les maintenir à l'état de l'art

Déployer des architectures et ou des solutions de sécurité de la couche matériels et logiciels de l'entreprise permettant de garantir l'évolutivité et la haute-disponibilité du système d'information

Piloter la procédure de paramétrage des politiques (habilitations) et configuration des droits d'accès appliqués sur son périmètre et vis-à-vis des tiers et des sous-traitants afin de garantir une utilisation sécurisée des moyens informatiques mis à disposition des utilisateurs finaux

Contribuer au pilotage de la mise en œuvre des outils et des solutions de sécurité autour des données de l'organisation et leur sauvegarde en fournissant une assistance technique et méthodologiques aux équipes informatiques afin de s'assurer de la pertinence des solutions/ outils choisis et participer lui-même à la bonne mise en place de la stratégie

Assurer le déploiement du programme et des initiatives cybersécurité dans l'ensemble des entités tout en respectant la cohérence globale et la coordination entre ces différentes entités afin que chaque entité s'approprie les nouvelles solutions/plateformes techniques et les services en cybersécurité dans une organisation.

Assurer la mise en place d'un service de détection des incidents de sécurité SOC (Security Opération center) au sein

de l'organisation afin d'évaluer le niveau de vulnérabilité et détecter des activités suspectes en prenant compte des exigences réglementaires

Conduire des plans d'action sur la détection et la réaction aux incidents, en fournissant des informations pertinentes aux équipes afin d'assurer l'efficacité des outils de détection déployés dans le SOC

Analyser des données brutes issues de différentes sources (dark web, renseignement open source, média sociaux, CERT) en utilisant la data science afin d'étudier l'évolution des modes opératoires des hackers et ajuster ensuite sa stratégie de cybersécurité

Renforcer les capacités de détection des activités malveillantes menaçant le système d'information en utilisant des solutions IA afin de réduire le risque des cyber attaques et rendre plus performant le SI de l'entreprise

Proposer des nouvelles approches innovantes basées sur l'IA en s'appuyant sur une veille technologique et industrielle concernant les nouveaux produits et process métiers mobilisant de l'IA afin d'améliorer la procédure de prévention d'intrusion de l'organisation et réinterroger son dispositif interne en initiant la mise en place d'un processus d'amélioration continue efficace

Définir les plans d'audits et de contrôles au sein de l'organisation afin d'évaluer la bonne application, l'efficacité et la conformité des politiques et procédures de sécurité de l'entreprise

Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves, d'accès aux consoles et aux rapports des outils de sécurité ou de l'utilisation d'outils automatisés de contrôle de conformité afin de mettre à jour le niveau de la sécurité du SI de l'entreprise

Rédiger des rapports intégrant une analyse des vulnérabilités et écarts constatés ainsi que les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes et d'informer la direction générale de l'avancement du ou des projets de déploiement

Informar les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer en se basant sur sa veille technologique et son étude du marché afin d'impliquer l'ensemble des acteurs de l'entreprise et en particulier les directions métiers et ainsi favoriser la prévention des risques

Analyser les risques de sécurité liés à l'introduction des nouvelles technologies en se basant sur une méthode d'analyse de risque optimisé

afin d'atténuer les impacts sur le niveau de sécurité informatique d'une entreprise.

Assurer un appui opérationnel à la gestion de la cyber- crise avec les experts techniques, en cas d'incidents de sécurité majeurs, en coordonnant les équipes, afin d'agir de traiter tout actes malveillants impactant l'entreprise et mieux prévenir la cyber menace.

Assurer la formation et l'entraînement des acteurs métiers et support susceptible d'intervenir en cas de crise de cybersécurité afin d'améliorer la capacité de l'organisation à réagir à une attaque

Animer la cellule de crise décisionnelle et les cellules de crise opérationnelles en impliquant chaque membre de l'équipe afin de s'assurer de leur capacité à agir et à traiter la crise de cybersécurité

Piloter les actions de sensibilisation à la sécurité des SI et de conduite du changement auprès des utilisateurs en organisant des formations internes et externes dans le domaine de la sécurité des S.I afin de faire gagner en compétences les équipes internes en matière de cyber prévention et à terme faciliter la mise en place des nouveaux processus

Blocs de compétences

RNCP36924BC01 — Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance

LISTE DE COMPÉTENCES

Étudier le système d'information d'une structure dans sa globalité, en identifiant les points faibles du système, afin d'évaluer le niveau de sécurité au sein de l'organisation

Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et vis-à-vis des tiers et sous-traitants et les exigences de conformité légale afin de garantir à l'entreprise d'être en conformité vis à vis de la réglementation française en matière de droit informatique ainsi que la bonne mise en application des normes et certifications du domaine

Décliner les axes et les objectifs stratégiques en matière de sécurité informatique et cybersécurité afin de sensibiliser la Direction générale au sujet et lui permettre de vérifier sa bonne correspondance avec la stratégie de développement de l'entreprise

Définir la feuille de route stratégique adaptée aux besoins et à la culture de la structure, en lien avec les parties

prenantes (informaticiens et les responsables des services) concernés afin de répondre à des objectifs de sécurité métiers et IT stratégiques face à l'augmentation de la cybermenace

Définir une stratégie de mise en conformité en lien avec la réglementation RGPD et le droit informatique afin de proposer un descriptif du process de la sécurité tenant compte de ce paramètre et ainsi, faciliter les relations avec les autorités de régulation en cas de contrôle réglementaires (auditeur RGPD et CNIL principalement)

Définir les mesures organisationnelles et techniques permettant de minimiser les risques liés à la sécurité du système d'information dans le but d'assurer une protection optimale et appropriée des données de l'entreprise et atteindre ainsi les objectifs de sécurité définis par la gouvernance

Définir l'organisation de la cybersécurité en proposant une charte de sécurité informatique de l'organisation afin de sensibiliser régulièrement les équipes et évaluer leurs connaissances en matière de règle de sécurité informatique

Concevoir un référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes...) permettant de formaliser, de justifier les choix, de légitimer les plans d'action et de garantir la cohérence avec le contexte particulier de l'organisme

Conseiller l'organisation en proposant des préconisations et des recommandations sur l'amélioration du niveau de sécurité afin de lui permettre une meilleure compréhension des enjeux et risques de cybermenaces et augmenter sa capacité de gestion de crises

Informers les directions générales et les directions métiers sur les enjeux de la sécurité informatique, cybersécurité et l'état de la menace afin de les sensibiliser sur l'évolution du contexte de la sécurité et la cybersécurité en utilisant des supports de communication inclusifs

Apporter une expertise juridique auprès de la gouvernance en matière de conformité (à une réglementation, à des référentiels d'exigences) afin de fournir aux dirigeants des entreprises les règles et les bonnes pratiques à appliquer faces aux nouvelles exigences en matière de conformité réglementaire

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée (MSPR)

Analyse et conseil d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur

Phase I- Préparation tutorée de la MSPR par équipe de 3 max

- Durée de préparation :

21 h

Phase II-Production écrite individuelle à réaliser

Phase III -Soutenance orale devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min d'entretien individuel (questions en lien avec les compétences)

RNCP36924BC02 — Pilotage de projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante

LISTE DE COMPÉTENCES

Identifier l'ensemble des étapes de réalisation du système d'information pour organiser le projet en tâches et livrables en répartissant les activités en

fonction des ressources humaines, techniques et financières à mobiliser

Concevoir les cahiers des charges technique et fonctionnel d'un projet de développement S.I. à l'aide des besoins utilisateurs collectés afin de cadrer le développement?

Piloter les prestataires extérieurs éventuels gérant les ressources informatiques d'un système d'information existant listées dans la cartographie établie afin de sécuriser la mise en œuvre technique

Établir des tableaux de bord de suivi de performance (qualitative et quantitative) de l'ensemble des ressources allouées à chaque

étape-projet pour anticiper, visualiser et corriger les écarts en temps réel afin de limiter les contraintes de ressources et les retards

Gérer un projet agile en utilisant les méthodes et outils adaptés à ce mode de fonctionnement pour tester, modifier et procéder par itération afin de réduire les délais de remise des projets de développement S.I.

Conduire une équipe projet en diffusant les fondamentaux de l'agilité?: adaptation, flexibilité et amélioration continue au sein de l'équipe afin d'être en mesure d'absorber les changements de priorité qui peuvent intervenir dans un contexte de forte contrainte de temps et d'incertitudes

Proposer des solutions innovantes afin de favoriser les interactions et l'inclusion au sein de l'équipe et d'anticiper des conflits de travail liés aux malentendus multiculturels et des profils en situation d'handicap

Accompagner l'équipe dans l'appropriation du travail à distance ou du télétravail en proposant des solutions

managériales afin de favoriser la motivation et la résilience et permettre ainsi de préserver l'équilibre entre vie professionnelle/vie privée dans un souci de productivité et de bien-être

Concevoir un processus de communication inclusif régulier au sein de l'équipe afin de synchroniser les activités quotidiennes et mettre en place un fil de discussion à l'aide d'outils numériques

Communiquer avec l'équipe en adoptant les modes de communication adéquats selon les cultures et la langue des collaborateurs afin de garantir l'intégration de tous les membres de l'équipe

Animer des réunions à distance afin de maintenir une dynamique de groupe et renforcer l'esprit d'équipe des membres en télétravail et/ou à distance

Concevoir un processus de partage d'information afin de faciliter la collaboration entre les membres (tous profils confondus) en télétravail et/ou à distance en utilisant des outils numériques

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée (MSPR)

Gestion d'un projet de mise en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur

Phase I- Préparation tutorée de la MSPR par équipe de 3 max - Durée de préparation :

21 h

Phase II-Production écrite individuelle à réaliser

Phase III -Soutenance orale devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min d'entretien individuel (questions en lien avec les compétences)

RNCP36924BC03 — Déploiement d'une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et faire face aux cybermenaces

LISTE DE COMPÉTENCES

Assurer la mise en place des structures organisationnelles des plans d'actions de sécurité au sein des entités afin de garantir la protection de données et le niveau de sécurité du système d'information

Paramétrer les mesures organisationnelles permettant la surveillance de la sécurité globale d'une organisation (des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques) afin d'assurer la mise en place d'un SOC (Security Operation Center)

Déployer les mesures organisationnelles de sécurité en se basant sur la stratégie de sécurité informatique de l'organisation afin d'assurer le fonctionnement opérationnel et les maintenir à l'état de l'art

Déployer des architectures et ou des solutions de sécurité de la couche matériels et logiciels de l'entreprise permettant de garantir l'évolutivité et la haute-disponibilité du système d'information

Piloter la procédure de paramétrage des politiques (habilitations) et configuration des droits d'accès appliqués sur son périmètre et vis-à-vis des tiers et des sous-traitants afin de garantir une utilisation sécurisée des moyens informatiques mis à disposition des utilisateurs finaux

Contribuer au pilotage de la mise en œuvre des outils et des solutions de sécurité autour des données de l'organisation et leur sauvegarde en fournissant une assistance technique et méthodologiques aux équipes informatiques afin de s'assurer de la pertinence des solutions/ outils choisis et participer lui-même à la bonne mise en place de la stratégie

Assurer le déploiement du programme et des initiatives cybersécurité dans l'ensemble des entités tout en respectant la cohérence globale et la coordination entre ces différentes entités afin que chaque entité s'approprie les nouvelles solutions/plateformes techniques et les services en cybersécurité dans une organisation

Assurer la mise en place d'un service de détection des incidents de sécurité SOC (Security Opération center) au sein de l'organisation afin d'évaluer le niveau de vulnérabilité et détecter des activités suspectes en prenant compte des exigences réglementaires

Conduire des plans d'action sur la détection et la réaction aux incidents, en fournissant des informations pertinentes aux équipes afin d'assurer l'efficacité des outils de détection déployés dans le SOC

Analyser des données brutes issues de différentes sources (dark web, renseignement open source, média sociaux, CERT) en utilisant la data science afin d'étudier l'évolution des modes opératoires des hackers et ajuster ensuite sa stratégie de cybersécurité

Renforcer les capacités de détection des activités malveillantes menaçant le système d'information en utilisant des solutions IA afin de réduire le risque des cyber attaques et rendre plus performant le SI de l'entreprise

Proposer des nouvelles approches innovantes basées sur l'IA en s'appuyant sur une veille technologique et industrielle concernant les nouveaux produits et process métiers mobilisant de l'IA afin d'améliorer la procédure de prévention d'intrusion de l'organisation et réinterroger son dispositif interne en initiant la mise en place d'un processus

d'amélioration continue efficace

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée (MSPR)

Déploiement d'une architecture ou solution de sécurité / cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur

Phase I- Préparation tutorée de la MSPR par équipe de 3 max - Durée de préparation :

28 h

Phase II - Production écrite individuelle à réaliser

Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min de démonstration technique et entretien individuel (questions en lien avec les compétences)

RNCP36924BC04 — Supervision, audit et gestion de la sécurité informatique et des cyberattaques

LISTE DE COMPÉTENCES

Définir les plans d'audits et de contrôles au sein de l'organisation afin d'évaluer la bonne application, l'efficacité et la conformité des politiques et procédures de sécurité de l'entreprise

Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves, d'accès aux consoles et aux rapports des outils de sécurité ou de l'utilisation d'outils automatisés de contrôle de conformité afin de mettre à jour le niveau de la sécurité du SI de l'entreprise

Rédiger des rapports intégrant une analyse des vulnérabilités et écarts constatés ainsi que les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes et d'informer la direction générale de l'avancement du ou des projets de déploiement

Informar les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer en se basant sur sa veille technologique et son étude du marché afin d'impliquer l'ensemble des acteurs de l'entreprise et en particulier les directions métiers et ainsi favoriser la prévention des risques

Analyser les risques de sécurité liés à l'introduction des nouvelles technologies en se basant sur une méthode d'analyse de risque optimisé

afin d'atténuer les impacts sur le niveau de sécurité informatique d'une entreprise

Assurer un appui opérationnel à la gestion de la cyber- crise avec les experts techniques, en cas d'incidents de sécurité majeurs, en coordonnant les équipes, afin d'agir de traiter tout actes malveillants impactant l'entreprise et mieux prévenir la cyber menace

Assurer la formation et l'entraînement des acteurs métiers et support susceptible d'intervenir en cas de crise de cybersécurité afin d'améliorer la capacité de l'organisation à réagir à une attaque

Animer la cellule de crise décisionnelle et les cellules de crise opérationnelles en impliquant chaque membre de l'équipe afin de s'assurer de leur capacité à agir et à traiter la crise de cybersécurité

Piloter les actions de sensibilisation à la sécurité des SI et de conduite du changement auprès des utilisateurs en organisant des formations internes et externes dans le domaine de la sécurité des S.I afin de faire gagner en compétences les équipes internes en matière de cyber prévention et à terme faciliter la mise en place des nouveaux processus

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée (MSPR)

Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur

Phase II - Production écrite individuelle à réaliser

Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn -

15 min de présentation de la réalisation en groupe - 15 min d'entretien individuel (questions en lien avec les compétences)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en cybersécurité et sécurité informatique peut exercer ses activités dans des entreprises de différentes tailles : PME-PMI, start-up, grandes entreprise, ou encore grand groupe. Dans la pratique, il peut être embauché au sein d'une entreprise, d'une structure gouvernementale ou d'une association. Il peut même être employé par une société

de services externe qui le mettra sous contrat de mission avec diverses structures clientes.

TYPE D'EMPLOIS ACCESSIBLES

Les appellations courantes de l'emploi évoluent en fonction des caractéristiques des entreprises, du niveau d'expérience et de la certification obtenue. Selon les activités de l'entreprise, ses contraintes et ses besoins, le champ d'actions de l'expert en cybersécurité et sécurité informatique peut varier et il peut assurer les fonctions suivantes :

Responsable de la Sécurité des Systèmes d'information (RSSI) · Architecte SSI(I) · Conseiller(ère) en SSI(I) auprès de décideurs · Consultant en cybersécurité · Analyst SOC (Security Operation Center)

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier n'est pas réglementé, mais l'expert en cybersécurité et sécurité informatique exerce ses activités dans le respect des contraintes réglementaires liées à son domaine d'intervention.

Marché du travail

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

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 892 €
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) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
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 M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'une certification de niveau 6 en informatique (développement d'applications, réseaux informatiques, infrastructures et systèmes), ou d'une certification de niveau 5 en informatique avec une expérience professionnelle d'au moins un an dans un métier informatique. Les conditions et principes d'accès diffèrent selon la voie choisie.

PRÉREQUIS À LA VALIDATION

La certification s'acquiert par la validation des 4 blocs de compétences, à laquelle s'ajoute la validation d'une épreuve

finale composée de la production d'un dossier professionnel présenté dans le cadre d'une soutenance orale

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

Le jury est composé de : deux membres externes professionnels (employeur ou salarié) de métier Expert en sécurité informatique et cyber sécurité (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification), l'un de ces deux membres étant président du jury ; Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant qui peut être le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat. 70% des membres du jury de certification sont donc des membres externes et des professionnels qualifiés.

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	8 909 €
Selon la branche	7 697 € – 9 157 €
Prise en charge	Branches concernées
8 909 €	Valeur par défaut · 186 branches
9 157 €	CPNE Casinos, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNE des industries de santé (CPNEIS)
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)
8 600 €	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	29/09/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	29/09/2025

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP41976

CORRESPONDANCES (PAR BLOCS)
RNCP35584

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.epsi.fr/msc-expert-en-cybersecurite-niveau-bac-5/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36924/>