

Expert cybersécurité

RNCP42345 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31038, 24231, 31094
Code(s) ROME	M1802, M1806, M1803
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/05/2026
Date d'échéance	29/05/2031

Certificateur(s)

CALTEA · SIRET : 93893471800017

Partenaires habilités

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

Organisme	SIRET	Habilitation
DATASCIENTEST	83145006900024	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100021	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Expert cybersécurité occupe une fonction stratégique au sein des organisations afin de protéger, sécuriser et renforcer la résilience de leurs systèmes d'information face à des menaces numériques de plus en plus sophistiquées. Il intervient à l'interface des enjeux techniques, organisationnels, juridiques et humains, en lien étroit avec la direction générale, les directions métiers, les équipes informatiques et les partenaires externes. Son rôle débute par l'analyse approfondie de l'environnement de l'organisation et de ses risques numériques. Il maîtrise les cadres législatifs, réglementaires et normatifs applicables et les intègre au contexte spécifique de l'organisation, en tenant compte des dimensions géopolitiques, économiques, sociétales et concurrentielles. À partir de méthodologies reconnues d'analyse de risques, il identifie les vulnérabilités techniques, organisationnelles et humaines, évalue les scénarios de menace et définit des priorités de cybersécurité. Cette démarche lui permet d'élaborer une politique de sécurité des systèmes d'information cohérente, proportionnée aux enjeux et intégrant les exigences de responsabilité sociétale, d'accessibilité, de protection des personnes et de transition écologique. Sur le plan opérationnel, l'Expert cybersécurité conçoit et déploie des architectures de sécurisation adaptées aux besoins métiers et aux contraintes de l'organisation. Il sélectionne et met en œuvre des solutions techniques performantes, intègre des mécanismes de chiffrement, sécurise les infrastructures et les environnements applicatifs, et veille à l'intégration de la sécurité tout au long du cycle de développement, notamment via les pratiques DevSecOps. Il pilote les projets de sécurisation en coordonnant les équipes, en assurant le suivi des indicateurs de performance et en garantissant la conformité aux normes de qualité, de sécurité et d'environnement. Il assure également le suivi continu du niveau de sécurité du système d'information. À ce titre, il met en place des dispositifs de supervision, réalise ou supervise des audits techniques et organisationnels, conduit des tests d'intrusion et organise la gestion des vulnérabilités et des correctifs. Sa mission s'inscrit dans une logique

d'amélioration continue, appuyée sur une veille technologique, réglementaire et sociétale permanente, intégrant notamment les évolutions liées à l'intelligence artificielle et aux nouveaux usages numériques.

L'Expert cybersécurité joue un rôle central dans la préparation et la gestion des crises cyber. Il élabore et maintient les plans de gestion de crise, de continuité et de reprise d'activité, organise des exercices et sensibilise les acteurs concernés. En cas d'incident majeur, il pilote la réponse à la crise, coordonne les investigations techniques et forensiques, supervise la remédiation et orchestre le retour à un fonctionnement sécurisé, tout en capitalisant sur le retour d'expérience pour renforcer durablement la résilience de l'organisation.

Par sa capacité à articuler vision stratégique, expertise technique de haut niveau et prise en compte des enjeux humains et sociétaux, l'Expert cybersécurité contribue directement à la protection des actifs numériques, à la continuité des activités et à la confiance des parties prenantes.

Le périmètre de cette certification présente une cohérence forte avec les réalités opérationnelles et stratégiques du métier visé. Il couvre de manière continue l'ensemble du cycle de sécurisation des systèmes d'information, depuis l'analyse de l'environnement et des risques numériques jusqu'à la gestion de crise et à l'amélioration continue du niveau de sécurité. Les compétences certifiées articulent de façon équilibrée les dimensions stratégiques (gouvernance cyber, définition des politiques, arbitrage des risques), techniques (architectures sécurisées, chiffrement, DevSecOps, supervision, audits) et organisationnelles (pilotage de projets, coordination des acteurs, conduite du changement).

Cette approche globale permet de former des professionnels capables d'intervenir à un niveau d'expertise élevé, en autonomie et en responsabilité, dans des contextes complexes et évolutifs, tout en intégrant les exigences réglementaires, sociétales et environnementales propres aux organisations contemporaines.

ACTIVITÉS VISÉES

Étude du contexte de l'organisation

Analyse du risque numérique d'une organisation

Élaboration d'une politique et d'une organisation cyber adaptées au contexte de l'organisation

Définition d'architectures sécurisées

Utilisation de la cryptologie et des outils cryptographiques pour sécuriser un système d'information (SI)

Sécurisation des développements DevSecOps et des infrastructures

Management d'un projet portant sur la sécurisation d'un système d'information (SI)

Mise en œuvre d'audits organisationnels et techniques

Mise en place d'une organisation pour la supervision des systèmes d'information (SI)

Maintien en condition de sécurité du système d'information (SI)

Mise en place d'une veille concurrentielle, technologique, économique et sociale dans un contexte international

Conception d'un plan de gestion de crise et un plan de continuité et de reprise d'activité

Prise en charge d'un incident

Restauration de systèmes en application d'un plan de continuité d'activité et/ou de reprise d'activité

COMPÉTENCES ATTESTÉES

Identifier les enjeux stratégiques de la cybersécurité d'une organisation, en s'appuyant sur l'appréhension des normes et procédures internes, des textes législatifs, réglementaires et normatifs, en communiquant avec les parties prenantes et en utilisant le vocabulaire propre à l'organisation, afin d'acquérir une vision d'ensemble des activités de l'organisation.

Évaluer l'environnement dans lequel évolue une organisation, par l'application d'une méthodologie de sélection, de recherche, de collecte et d'analyse d'informations, en identifiant les priorités stratégiques de la cybersécurité/cybersécurité, afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation dans son contexte propre.

Mettre en œuvre une méthode d'analyse du risque numérique, en déterminant l'objet d'étude et les parties prenantes (partenaires, filiales, sous-traitants...), en analysant les usages (notamment l'IA) et les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité (par rapport au cadre normatif et réglementaire applicable, à l'éthique...), afin de déceler les failles et les vulnérabilités de l'organisation.

Déterminer des mesures de sécurité idoines au contexte d'une organisation, en réalisant une cartographie des sources de risque, des menaces numériques, des scénarios d'attaque et par la prise en compte de ses moyens (financiers, humains...), afin de permettre l'adoption d'une politique cyber adaptée à l'organisation et à ses activités.

Formuler la politique de sécurité d'une organisation, à partir du guide PSSI de l'ANSSI, en tenant compte de l'existant et des usages, notamment en matière environnementale, en intégrant une démarche qualité, en définissant les objectifs, les orientations et les responsabilités de chacun et en intégrant un cadre de suivi, afin de garantir l'usage

sécurisé et efficace de l'ensemble du SI.

Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation sur les enjeux cyber, à l'écrit et à l'oral, en français et en anglais, en adoptant un langage et/ou des outils inclusifs adaptés aux éventuelles situations de handicap et à la multiculturalité, par l'organisation d'ateliers, réunions ou actions de sensibilisation afin de les impliquer dans la prévention et la gestion du risque cyber.

Identifier les équipements (logiciels, solutions d'IA, matériels...) présents sur le marché apportant performance, confidentialité, intégrité et/ou disponibilité, grâce à l'étude de leurs qualifications (CSPN de l'ANSSI, EAL, Critères communs), le recueil de leurs vulnérabilités connues et leur capacité à s'intégrer à une solution de supervision et journalisation des événements ou à automatiser les actions, afin de constituer un catalogue d'éléments de sécurisation adaptés aux capacités, moyens et enjeux de l'organisation.

Rédiger un cahier des charges fonctionnel portant sur un projet de sécurisation du SI, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation (politique RSE, de responsabilité/hygiène numérique...), en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la réglementation et aux normes, afin de traduire les enjeux de l'organisation et des exigences en termes de sécurité, de façon adaptée et pérenne.

Modéliser une base de données des flux d'information et traitements, à l'aide du relevé des échanges d'informations existants ou nécessaires entre les différentes briques (logicielles et matérielles) de sécurisation du SI, afin d'établir la cartographie de l'architecture de sécurisation du SI à mettre en place.

Déterminer les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et l'analyse des forces et faiblesses de chacune des solutions, afin d'opter pour la solution la plus adaptée en fonction des besoins de l'organisation (recherche de confidentialité et/ou d'intégrité et/ou d'authenticité).

Déployer une infrastructure de gestion de clés par la mise en place d'une autorité de certification répondant aux objectifs (niveau de résistance, facilité d'utilisation, intégration aux chiffreurs matériels, exigences environnementales...), afin de permettre la mise en place du chiffrement et de la signature au sein des échanges/outils de l'organisation.

Mettre en place une usine de développement sécurisé par l'utilisation de pipeline d'intégration et de déploiement continu (CI/CD), par l'intégration de tests unitaires/non régression tournés vers la sécurité, par l'exploitation d'une pile logicielle (bibliothèque d'outils éprouvés), afin d'assurer la production d'outils logiciels conformes à la politique de sécurité de l'organisation.

Organiser des tests de sécurité, au travers de simulations d'attaques et de réponses (dépassements mémoire, injections, brute force...), avec et sans recours à l'IA, à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces des solutions du SI pour identifier des faiblesses et vulnérabilités, anticiper les réponses possibles et garantir le maintien au niveau de sécurité attendu de l'organisation.

Déployer des outils méthodologiques dans un cadre de projet de sécurisation d'un SI, grâce à la sélection d'une méthode de gestion de projet (Agile, cycle en V) et à la mobilisation responsable des outils d'organisation, de suivi et d'IA, en prenant en compte les normes applicables (ISO 9001, 14001...), afin de garantir les conditions les plus favorables à son orchestration.

Faciliter la résolution des difficultés pouvant mettre en péril la réussite du projet, en mettant en œuvre un suivi régulier des réalisations des équipes à chaque étape/jalon, via des entretiens individuels, des outils numériques (planification, automatisation, suivi général de type Gantt...) et des grilles d'évaluation, pour assurer le déroulement du projet dans le respect du cahier des charges/du rétroplanning défini et des exigences spécifiques aux profils des acteurs mobilisés (situations de handicap, limites/interdépendances de compétences, risques de RPS...).

Réaliser un audit des SI grâce à la conduite de tests et simulations in situ (intrusions), de l'évaluation du code source et de remontées statistiques cadrés par le référentiel PASSI et les règles d'engagement (entre l'auditeur et l'audité) pour acquérir les données nécessaires à l'évaluation du niveau de sécurisation du SI.

Présenter les conclusions d'un audit des SI par l'analyse des résultats et comportements obtenus (techniques, humains et organisationnels) et leur comparaison avec les référentiels de l'organisation (politique SSI) et le cadre normatif et réglementaire applicable (RSE...), en identifiant des axes d'amélioration réalistes afin de proposer des recommandations contribuant à l'élévation du niveau de sécurité de l'organisation ou permettant d'obtenir son homologation de sécurité.

Intégrer la conduite de changement du SI de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus à mettre en place, pour garantir l'adoption et l'application continue de la politique de sécurisation du SI dans le contexte évolutif de l'organisation (nouveaux usages de l'IA, nouveaux profils de collaborateurs, nouveaux équipements pour les PSH...).

Développer un SOC (Security Operating Center) par la mise en place de la remontée en temps réel des signaux d'états des outils de sécurité (sondes, EDRs, pare feux...) au sein d'une plateforme de supervision/monitoring

(SIEM), afin d'assurer le maintien en fonction et la performance de la détection d'alertes de sécurité liées au SI. Mettre en place un suivi des alarmes de sécurité par la définition de critères d'évaluation (origine, occurrence – fréquence, nature), par l'analyse de comportements suspects au travers de l'IA et par la définition des parties impliquées (départements, victimes), afin d'en déterminer le niveau de gravité et de proposer rapidement un plan d'action et une réponse adaptée à l'incident.

Assurer la mise à jour des outils matériels et logiciels au regard des processus métiers, des profils des utilisateurs (situations de handicap...) et des contraintes de l'organisation (liées à une politique économique, environnementale ...), en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel selon les nouvelles technologies et des nouveaux besoins, en actualisant la gestion des contrats fournisseurs et de l'organisation, afin de maintenir le niveau de sécurisation du SI et la protection de son utilisation/de ses utilisateurs.

Établir un suivi actif des vulnérabilités des briques du SI, en surveillant l'obsolescence des produits et les demandes automatiques constructeurs de mise à jour de la version du logiciel en cas de remontée de vulnérabilité, pour maintenir les outils à jour et garantir le niveau de sécurisation du SI.

Réaliser une veille technologique, économique et sociale dans un contexte international en définissant les thèmes critiques, en sélectionnant des sources vérifiées et authentiques, en mettant en place une plateforme centralisée recensant les évolutions en termes d'attaques et de concurrence de l'organisation, afin d'anticiper l'apparition de nouvelles menaces.

Identifier les mutations et innovations technologiques impactant la cybersécurité et la cyberdéfense, en s'appuyant sur l'analyse des signaux faibles (économiques, politiques, sociaux ou techniques) recensés à partir d'une base de données de veille et des outils associés, afin d'orienter la stratégie de sécurisation du SI et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle, protection des données stratégiques/sensibles des clients/des collaborateurs ...).

Elaborer un plan d'action de gestion de crise, par la collecte des moyens et services essentiels à son fonctionnement, en respectant le cadre normatif, réglementaire et législatif, par l'analyse de la résilience des services selon différents scénarios afin de permettre aux parties prenantes de l'organisation de définir les ressources allouables à l'établissement d'une cellule de crise selon ses ambitions, moyens et priorités.

Maintenir à jour le plan de gestion de crise, par l'entretien régulier des moyens (matériels et documentations) participant à la résilience de l'organisation, par la sensibilisation continue des acteurs concernés et par la conduite d'exercices à grande échelle, pour garantir la fourniture d'une réponse rapide et adaptée à la protection de l'organisation et de ses collaborateurs, y compris en situation de handicap, de la part de la cellule de crise.

Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyens pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du SI et des données associées, par la mise en place d'un canal de communication régulier, fluide et contrôlé, ainsi que le partage d'éléments d'information adaptés, afin de permettre la sortie progressive de crise.

Procéder à la recherche d'éléments de preuve techniques grâce à une méthodologie d'investigation et d'outils d'analyse forensique (Volatility ...), par l'utilisation de la rétro-ingénierie (reverse engineering), l'étude des comportements tracés dans des journaux et la rédaction d'un rapport, afin de déterminer les marqueurs facilitant la détection de l'attaque et son élimination (contre-mesures).

Déployer une stratégie de reprise d'activité à la suite d'un contexte de crise/d'incident, par l'utilisation des mécanismes de restauration des sauvegardes existantes, la remise en service des équipements et l'application des contre-mesures déterminées sur l'ensemble du système d'exploitation, afin de retrouver un niveau de fonctionnement et de sécurité équivalent ou supérieur au niveau pré crise.

Enrichir les plans de continuité et de reprise d'activité par la consolidation des éléments de preuve et relevés techniques, la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), l'établissement d'un bilan post crise et la mise à jour ou le renforcement des procédures et des outils du SI, à l'aide des conclusions tirées de l'analyse post crise, pour rendre plus réactives et performantes les réponses à incident futurs.

Blocs de compétences

RNCP42345BC01 — Elaborer une stratégie de sécurité des systèmes d'information d'une organisation en adéquation avec son environnement et ses risques

LISTE DE COMPÉTENCES

Identifier les enjeux stratégiques de la cyberdéfense d'une organisation, en s'appuyant sur l'appréhension des

normes et procédures internes, des textes législatifs, réglementaires et normatifs, en communiquant avec les parties prenantes et en utilisant le vocabulaire propre à l'organisation, afin d'acquérir une vision d'ensemble des activités de l'organisation.

Évaluer l'environnement dans lequel évolue une organisation, par l'application d'une méthodologie de sélection, de recherche, de collecte et d'analyse d'informations, en identifiant les priorités stratégiques de la cybersécurité/cyberdéfense, afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation dans son contexte propre.

Mettre en œuvre une méthode d'analyse du risque numérique, en déterminant l'objet d'étude et les parties prenantes (partenaires, filiales, sous-traitants...), en analysant les usages (notamment l'IA) et les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité (par rapport au cadre normatif et réglementaire applicable, à l'éthique...), afin de déceler les failles et les vulnérabilités de l'organisation.

Déterminer des mesures de sécurité idoines au contexte d'une organisation, en réalisant une cartographie des sources de risque, des menaces numériques, des scénarios d'attaque et par la prise en compte de ses moyens (financiers, humains...), afin de permettre l'adoption d'une politique cyber adaptée à l'organisation et à ses activités.

Formuler la politique de sécurité d'une organisation, à partir du guide PSSI de l'ANSSI, en tenant compte de l'existant et des usages, notamment en matière environnementale, en intégrant une démarche qualité, en définissant les objectifs, les orientations et les responsabilités de chacun et en intégrant un cadre de suivi, afin de garantir l'usage sécurisé et efficace de l'ensemble du SI.

Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation sur les enjeux cyber, à l'écrit et à l'oral, en français et en anglais, en adoptant un langage et/ou des outils inclusifs adaptés aux éventuelles situations de handicap et à la multiculturalité, par l'organisation d'ateliers, réunions ou actions de sensibilisation afin de les impliquer dans la prévention et la gestion du risque cyber.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur l'élaboration d'une politique de sécurité du SI d'une organisation

RNCP42345BC02 — Mettre en place les outils techniques nécessaires à la sécurisation du système d'information d'une organisation

LISTE DE COMPÉTENCES

Identifier les équipements (logiciels, solutions d'IA, matériels...) présents sur le marché apportant performance, confidentialité, intégrité et/ou disponibilité, grâce à l'étude de leurs qualifications (CSPN de l'ANSSI, EAL, Critères communs), le recueil de leurs vulnérabilités connues et leur capacité à s'intégrer à une solution de supervision et journalisation des événements ou à automatiser les actions, afin de constituer un catalogue d'éléments de sécurisation adaptés aux capacités, moyens et enjeux de l'organisation.

Rédiger un cahier des charges fonctionnel portant sur un projet de sécurisation du SI, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation (politique RSE, de responsabilité/hygiène numérique...), en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la réglementation et aux normes, afin de traduire les enjeux de l'organisation et des exigences en termes de sécurité, de façon adaptée et pérenne.

Modéliser une base de données des flux d'information et traitements, à l'aide du relevé des échanges d'informations existants ou nécessaires entre les différentes briques (logicielles et matérielles) de sécurisation du SI, afin d'établir la cartographie de l'architecture de sécurisation du SI à mettre en place.

Déterminer les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et l'analyse des forces et faiblesses de chacune des solutions, afin d'opter pour la solution la plus adaptée en fonction des besoins de l'organisation (recherche de confidentialité et/ou d'intégrité et/ou d'authenticité).

Déployer une infrastructure de gestion de clés par la mise en place d'une autorité de certification répondant aux objectifs (niveau de résistance, facilité d'utilisation, intégration aux chiffreurs matériels, exigences environnementales...), afin de permettre la mise en place du chiffrement et de la signature au sein des échanges/outils de l'organisation.

Mettre en place une usine de développement sécurisé par l'utilisation de pipeline d'intégration et de déploiement continu (CI/CD), par l'intégration de tests unitaires/non régression tournés vers la sécurité, par l'exploitation d'une pile logicielle (bibliothèque d'outils éprouvés), afin d'assurer la production d'outils logiciels conformes à la politique de sécurité de l'organisation.

Organiser des tests de sécurité, au travers de simulations d'attaques et de réponses (dépassements mémoire, injections, brute force...), avec et sans recours à l'IA, à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces des solutions du SI pour identifier des faiblesses et vulnérabilités, anticiper les réponses possibles et garantir le maintien au niveau de sécurité attendu de l'organisation.

Déployer des outils méthodologiques dans un cadre de projet de sécurisation d'un SI, grâce à la sélection d'une méthode de gestion de projet (Agile, cycle en V) et à la mobilisation responsable des outils d'organisation, de suivi et d'IA, en prenant en compte les normes applicables (ISO 9001, 14001...), afin de garantir les conditions les plus favorables à son orchestration.

Faciliter la résolution des difficultés pouvant mettre en péril la réussite du projet, en mettant en œuvre un suivi régulier des réalisations des équipes à chaque étape/jalon, via des entretiens individuels, des outils numériques (planification, automatisation, suivi général de type Gantt...) et des grilles d'évaluation, pour assurer le déroulement du projet dans le respect du cahier des charges/du rétroplanning défini et des exigences spécifiques aux profils des acteurs mobilisés (situations de handicap, limites/interdépendances de compétences, risques de RPS...).

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur la conception d'une architecture de sécurisation du SI d'une organisation et la planification de son déploiement

Mise en situation professionnelle portant sur la mise en œuvre d'une solution de sécurisation du SI d'une organisation

RNCP42345BC03 — Suivre l'évolution du niveau de sécurité du système d'information d'une organisation

LISTE DE COMPÉTENCES

Réaliser un audit des SI grâce à la conduite de tests et simulations in situ (intrusions), de l'évaluation du code source et de remontées statistiques cadrés par le référentiel PASSI et les règles d'engagement (entre l'auditeur et l'audité) pour acquérir les données nécessaires à l'évaluation du niveau de sécurisation du SI.

Présenter les conclusions d'un audit des SI par l'analyse des résultats et comportements obtenus (techniques, humains et organisationnels) et leur comparaison avec les référentiels de l'organisation (politique SSI) et le cadre normatif et réglementaire applicable (RSE...), en identifiant des axes d'amélioration réalistes afin de proposer des recommandations contribuant à l'élévation du niveau de sécurité de l'organisation ou permettant d'obtenir son homologation de sécurité.

Intégrer la conduite de changement du SI de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus à mettre en place, pour garantir l'adoption et l'application continue de la politique de sécurisation du SI dans le contexte évolutif de l'organisation (nouveaux usages de l'IA, nouveaux profils de collaborateurs, nouveaux équipements pour les PSH...).

Développer un SOC (Security Operating Center) par la mise en place de la remontée en temps réel des signaux d'états des outils de sécurité (sondes, EDRs, pare feux...) au sein d'une plateforme de supervision/monitoring (SIEM), afin d'assurer le maintien en fonction et la performance de la détection d'alertes de sécurité liées au SI.

Mettre en place un suivi des alarmes de sécurité par la définition de critères d'évaluation (origine, occurrence – fréquence, nature), par l'analyse de comportements suspects au travers de l'IA et par la définition des parties impliquées (départements, victimes), afin d'en déterminer le niveau de gravité et de proposer rapidement un plan d'action et une réponse adaptée à l'incident.

Assurer la mise à jour des outils matériels et logiciels au regard des processus métiers, des profils des utilisateurs (situations de handicap...) et des contraintes de l'organisation (liées à une politique économique, environnementale ...), en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel selon les nouvelles technologies et des nouveaux besoins, en actualisant la gestion des contrats fournisseurs et de l'organisation, afin de maintenir le niveau de sécurisation du SI et la protection de son utilisation/de ses utilisateurs.

Établir un suivi actif des vulnérabilités des briques du SI, en surveillant l'obsolescence des produits et les demandes automatiques constructeurs de mise à jour de la version du logiciel en cas de remontée de vulnérabilité, pour maintenir les outils à jour et garantir le niveau de sécurisation du SI.

Réaliser une veille technologique, économique et sociale dans un contexte international en définissant les thèmes critiques, en sélectionnant des sources vérifiées et authentiques, en mettant en place une plateforme centralisée recensant les évolutions en termes d'attaques et de concurrence de l'organisation, afin d'anticiper l'apparition de nouvelles menaces.

Identifier les mutations et innovations technologiques impactant la cybersécurité et la cyberdéfense, en s'appuyant sur l'analyse des signaux faibles (économiques, politiques, sociaux ou techniques) recensés à partir d'une base de données de veille et des outils associés, afin d'orienter la stratégie de sécurisation du SI et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle, protection des données stratégiques/sensibles des clients/des collaborateurs ...).

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur l'audit, la supervision et l'amélioration continue de la cybersécurité d'un

RNCP42345BC04 — Organiser une réponse adaptée en cas de crise impactant une organisation

LISTE DE COMPÉTENCES

Elaborer un plan d'action de gestion de crise, par la collecte des moyens et services essentiels à son fonctionnement, en respectant le cadre normatif, réglementaire et législatif, par l'analyse de la résilience des services selon différents scénarios afin de permettre aux parties prenantes de l'organisation de définir les ressources allouables à l'établissement d'une cellule de crise selon ses ambitions, moyens et priorités.

Maintenir à jour le plan de gestion de crise, par l'entretien régulier des moyens (matériels et documentations) participant à la résilience de l'organisation, par la sensibilisation continue des acteurs concernés et par la conduite d'exercices à grande échelle, pour garantir la fourniture d'une réponse rapide et adaptée à la protection de l'organisation et de ses collaborateurs, y compris en situation de handicap, de la part de la cellule de crise.

Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyens pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du SI et des données associées, par la mise en place d'un canal de communication régulier, fluide et contrôlé, ainsi que le partage d'éléments d'information adaptés, afin de permettre la sortie progressive de crise.

Procéder à la recherche d'éléments de preuve techniques grâce à une méthodologie d'investigation et d'outils d'analyse forensique (Volatility ...), par l'utilisation de la rétro-ingénierie (reverse engineering), l'étude des comportements tracés dans des journaux et la rédaction d'un rapport, afin de déterminer les marqueurs facilitant la détection de l'attaque et son élimination (contre-mesures).

Déployer une stratégie de reprise d'activité à la suite d'un contexte de crise/d'incident, par l'utilisation des mécanismes de restauration des sauvegardes existantes, la remise en service des équipements et l'application des contre-mesures déterminées sur l'ensemble du système d'exploitation, afin de retrouver un niveau de fonctionnement et de sécurité équivalent ou supérieur au niveau pré-crise.

Enrichir les plans de continuité et de reprise d'activité par la consolidation des éléments de preuve et relevés techniques, la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), l'établissement d'un bilan post crise et la mise à jour ou le renforcement des procédures et des outils du SI, à l'aide des conclusions tirées de l'analyse post crise, pour rendre plus réactives et performantes les réponses à incident futurs.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur la préparation d'un plan de gestion de crise et d'un plan de continuité et de reprise d'activité

Mise en situation professionnelle portant sur la gestion d'un incident cyber et la remédiation post crise

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert cybersécurité

exerce dans un secteur caractérisé par une transformation numérique accélérée, une dépendance croissante des organisations aux systèmes d'information et une exposition accrue aux menaces cyber.

Les cadres d'exercice les plus fréquents correspondent à des environnements organisationnels disposant d'infrastructures numériques structurées et critiques. Cet expert intervient majoritairement au sein de grandes entreprises, d'entreprises de taille intermédiaire, d'administrations publiques, d'opérateurs d'importance vitale ou d'organisations fortement régulées.

TYPE D'EMPLOIS ACCESSIBLES

Appellations principales : Expert (en) cybersécurité - Expert sécurité des systèmes d'information - Expert SSI (Sécurité des Systèmes d'Information)

Appellations à dominante stratégique et gouvernance : Consultant expert en cybersécurité - Architecte sécurité des systèmes d'information - Responsable de la stratégie cybersécurité - Responsable sécurité des systèmes d'information (RSSI) - Cybersecurity Manager - Cybersecurity Governance Expert

Appellations à dominante technique et opérationnelle : Architecte cybersécurité - Ingénieur expert en cybersécurité - Expert sécurité infrastructure et cloud - Expert DevSecOps - Expert en sécurité applicative - Expert en cryptographie et infrastructures de confiance

Appellations orientées supervision, audit et résilience : Expert en supervision et détection des incidents cyber -

Expert SOC (Security Operations Center) - Responsable SOC - Auditeur expert en cybersécurité - Expert en audit et conformité cybersécurité - Expert en gestion des risques cyber
Appellations orientées gestion de crise : Expert en gestion de crise cyber - Expert en réponse à incident (Incident Response Expert) - Expert en cyber-résilience

RÈGLEMENTATIONS D'ACTIVITÉ

La cybersécurité en France s'inscrit dans un cadre réglementaire structurant, notamment avec la transposition de la directive européenne NIS2, qui impose aux entités importantes des obligations de gestion des risques, de notification des incidents et de gouvernance de la sécurité.
D'autre part le Règlement général sur la protection des données (RGPD) requiert des mesures de sécurité spécifiques pour la protection des données personnelles.
De plus, des dispositions nationales et l'action de l'ANSSI renforcent ces exigences pour les organisations de secteurs sensibles.

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 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 913 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) 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)	14 615
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique 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'un diplôme de niveau 6 ou équivalent dans le domaine du numérique (informatique, systèmes d'information, réseaux et systèmes, etc.). Un test de positionnement et un entretien d'admission sont effectués pour chaque candidat.
Toute candidature de candidats ayant un niveau inférieur à celui requis pourront être étudiées, dans ce cas des tests techniques plus poussés seront imposés.

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

Deux personnes sont désignées pour représenter le jury : un représentant de l'organisme certificateur et un professionnel externe dont la qualité est en lien avec la certification visée. Le professionnel occupe la fonction de

Président du Jury.

COMPOSITION DU JURY — VAE

Selon l'article D. 6412-6 du Code du travail, le jury VAE est composé d'au moins deux membres ; Comprend obligatoirement au moins une personne qualifiée au titre de la certification visée ; Est désigné par l'organisme certificateur selon les règles spécifiques à chaque certification ; Est présidé par un président de jury ayant voix prépondérante en cas de partage égal des voix ; Assure une représentation équilibrée femmes/hommes ; Respecte les principes d'impartialité : Aucun membre ne doit avoir accompagné le candidat dans sa démarche VAE ; Aucun membre ne doit entretenir ou avoir entretenu de relation professionnelle ou personnelle avec le candidat.

Base légale

Date de décision	29/05/2026
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	29/05/2031
Date de dernière délivrance possible	29/05/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	53	0	78 %	—
2024	12	9	100 %	85 %
2023	1	1	100 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP37796

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Cursus Cyberdéfense en 2 ans - École Hexagone

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42345/>

Où se former

Formations référencées	3
Organismes	1
Régions couvertes	0
Prix indicatif	7 190 € – 11 990 €

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1

Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Sessions	de 10/2025 à 09/2027

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).

Demande CPF — formations engagées

Dossiers CPF engagés	5
Montant total engagé	46 680 €
Coût moyen par dossier	9 336 €
Durée moyenne	756 h
Période	08/2026
France compétences	41 %
Entreprise	40 %
France Travail	19 %
Reste à charge titulaire	0 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.