

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

RNCP37796 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31006, 31038, 24231, 31094
Code(s) ROME	M1810, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/07/2023
Date d'échéance	19/07/2026

Certificateur(s)

CALTEA · SIRET : 93893471800017

ECOLE HEXAGONE · SIRET : 88408480700046

<https://www.ecole-hexagone.com/fr/fr/>

Partenaires habilités

8 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation et 3 à former.

Organisme	SIRET	Habilitation
CALTEA	93893471800017	Former et organiser l'évaluation
CALTEA	93893471800025	Former et organiser l'évaluation
CALTEA	93893471800033	Former et organiser l'évaluation
DATASCIENTEST	83145006900024	Former
DATASCIENTEST	83145006900057	Former et organiser l'évaluation
EFREI PARIS	39889833800023	Former
HEXAGONE	88408480700020	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100021	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

La cybersécurité et la cyberdéfense sont des enjeux cruciaux au regard du développement des nouvelles technologies numériques telles l'Intelligence Artificielle avec les deepfakes par exemple ou l'émergence de l'Informatique quantique qui rendra obsolète les politiques de mots de passe. Du fait de la numérisation des processus et modes de travail, la cybersécurité touche aujourd'hui l'ensemble des secteurs d'activités. La gestion et le stockage de données imposent à n'importe quelle organisation de mettre en place les moyens nécessaires à sa sécurité et sa pérennité. C'est pourquoi, le secteur d'activité du gestionnaire de la sécurité des données, des réseaux et des systèmes peut varier. Il peut officier au sein d'une société d'informatique, dans le secteur industriel mais aussi pour les banques, les assurances et mutuelles. Les opérateurs d'importance vitales privés ou publics représentent

également un enjeu majeur de l'exercice des métiers liés à la sécurité des systèmes d'information.

Le gestionnaire de la sécurité des données, des réseaux et des systèmes a pour principale mission de garantir la protection du système d'information d'une organisation. Il doit en effet assurer la confidentialité, l'intégrité et la disponibilité des données, maintenir l'accessibilité, la pérennité et l'intégrité des réseaux et des systèmes, des équipements matériels et logiciels et garantir la conformité aux normes et aux règlements en vigueur.

Il procède à une analyse afin de mettre en lumière les éventuels besoins et risques que l'organisation encourt. Il définit des solutions à adopter et propose puis déploie la politique sécurité et les processus s'y rattachant. Il pilote l'organisation stratégique en cas d'incident de sécurité. Il maîtrise les outils de gestion de crise, les processus de suivi et est en mesure d'apporter une réponse adaptée en cas de cyberattaque, d'un point de vue organisationnel et technique. Depuis la crise de la Covid-19, les modes de travail tendent vers une numérisation. Parallèlement, le nombre de cyberattaques est en hausse ces dernières années, la veille technologique représente donc un levier d'action essentiel dans l'exercice de ce métier. Enfin, il a un rôle d'ambassadeur auprès du personnel car il doit informer, mettre en oeuvre de la documentation, des outils et des actions de communication

Cette certification vise à répondre au fort besoin en compétences pour le métier, identifié sur le marché du travail en proposant un dispositif certifiant construit au plus proche des enjeux des entreprises, dans un contexte cyber tendu.

ACTIVITÉS VISÉES

Formulation et formalisation de la politique de la sécurité des systèmes d'information d'une organisation en adéquation avec son environnement et les risques auxquels elle doit faire face

Mise en place des outils techniques et humains nécessaires à la sécurisation du système d'information d'une organisation

Suivi de l'évolution du niveau de sécurité d'un système d'information d'une organisation

Organisation d'une réponse adaptée en cas de crise

COMPÉTENCES ATTESTÉES

Identifier les enjeux stratégiques de la cybersécurité d'une organisation en s'appuyant sur la lecture des normes et procédures internes, des textes législatif, 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 dans une synthèse afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation.

Mettre en œuvre une méthode d'analyse du risque numérique en établissant l'objet d'étude, en mettant en lumière les parties prenantes (partenaires, filiales, sous-traitants, etc.), en analysant les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité, tout en appliquant le cadre normatif et réglementaire 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, par la prise en compte de ses moyens (financiers, humains, etc.) et en synthétisant ces informations 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, 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 système d'information.

Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation, 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 et 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 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 système d'information, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation, en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la réglementation et aux normes, afin de proposer une traduction des enjeux de l'organisation et des exigences en termes de sécurité 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 système d'information afin d'établir la cartographie de l'architecture de sécurisation du système d'information à mettre en place.

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

Identifier les difficultés pouvant mettre en péril la réussite du projet à l'aide du suivi régulier des étapes du projet, des réalisations de chaque équipe via des entretiens individuels, d'outils de planification et de suivi général (Gantt) et des grilles d'évaluation pour assurer le déroulement du projet dans le respect du cahier des charges/du rétroplanning défini.

Maîtriser les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et par 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) 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 (dépassements mémoire, injections, bruteforce, etc.) à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces présentées par les outils pour identifier des faiblesses et vulnérabilités et garantir le maintien au niveau de sécurité attendu des développements logiciels de l'organisation.

Réaliser un audit des systèmes d'information 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 système d'information.

Présenter les conclusions d'un audit des systèmes d'information 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, en identifiant des axes d'amélioration afin de proposer des recommandations qui contribueront à l'élévation du niveau de sécurité de l'organisation ou lui permettront d'obtenir son homologation de sécurité.

Intégrer la conduite de changement du système d'information de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus qui seront mis en place pour garantir l'adoption et l'application continue de la politique de sécurisation du système d'information.

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 système d'information.

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'intelligence artificielle 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 et des contraintes de l'organisation, en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel en fonction des 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 système d'information.

Établir un suivi actif des vulnérabilités des briques du système d'information, 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 système d'information.

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 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 système d'information et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle).

Rédiger 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 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 de la part de la cellule de crise.

Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyen pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du système d'information, par la mise en place d'un canal de communication régulier, fluide et contrôlé, 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 exemple), par l'utilisation de la rétro-ingénierie (reverse engineering) et l'étude des comportements tracés dans des journaux et par 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, par la remise en service des équipements et par 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, par la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), par l'établissement d'un bilan post-crise et la mise à jour et le renforcement des procédures et des outils du système d'information 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

RNCP37796BC01 — Formuler et formaliser la politique de la sécurité des systèmes d'information d'une organisation, en adéquation avec son environnement et les risques auxquels elle doit faire face

LISTE DE COMPÉTENCES

Identifier les enjeux stratégiques de la cyberdéfense d'une organisation en s'appuyant sur la lecture des normes et procédures internes, des textes législatif, 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 dans une synthèse afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation.

Mettre en œuvre une méthode d'analyse du risque numérique en établissant l'objet d'étude, en mettant en lumière les parties prenantes (partenaires, filiales, sous-traitants, etc.), en analysant les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité, tout en appliquant le cadre normatif et réglementaire 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, par la prise en compte de ses moyens (financiers, humains, etc.) et en synthétisant ces informations 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, 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 système d'information.

Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation, 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

Étude de cas : analyse de l'environnement d'une organisation. Le candidat doit analyser l'environnement juridique, économique et géopolitique d'une organisation et rédiger, à partir d'un dossier d'analyse et individuellement, une cartographie et une note de synthèse. Le candidat doit s'approprier le contexte cyber de l'organisation, les procédures et normes internes, le vocabulaire propre au secteur d'activité et les besoins métiers. Le candidat doit témoigner d'un esprit synthétique, d'une méthode de recherche de l'information à l'aide d'outils et analyser le contexte géopolitique et concurrentiel au regard des activités de l'organisation. Les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités sont fournis par l'organisme de formation. Le candidat doit alimenter son travail de ses recherches personnelles.

Mise en situation professionnelle reconstituée : analyse de risque à l'occasion de l'étude préalable à la mise en place d'un outil numérique sur le système d'information d'une organisation. Le candidat doit appliquer, individuellement, une méthode reconnue d'analyse de risque pour évaluer les conséquences sur la cybersécurité de la mise en place du nouvel outil. Le candidat doit proposer des recommandations et interpréter les risques identifiés au regard des pertes potentielles et de la mise en place du nouvel outil dans un rapport d'analyse du risque. Les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités ainsi que sur la méthode d'analyse du risque sont fournis par l'organisme de formation.

Mise en situation professionnelle reconstituée : formalisation d'une politique de sécurité d'une organisation. Dans le cadre d'un projet fictif portant sur une organisation souhaitant mettre à jour une politique de sécurité de son système d'information, le candidat doit formaliser la politique à l'écrit et la présenter à l'oral. Partie 1 : le candidat doit rédiger, individuellement, la politique de sécurité en se basant sur le guide PASSI relatif à la politique de sécurité d'un système d'information. Partie 2 : le candidat doit, individuellement, présenter au personnel technique et non technique, à l'oral, sa politique et sa pertinence. Les supports et ressources documentaires portant sur le cas d'étude sont fournis par l'organisme de formation.

RNCP37796BC02 — Mettre en place les outils techniques nécessaires à la sécurisation du système d'information d'une organisation

LISTE DE COMPÉTENCES

Identifier les équipements (logiciels et 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 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 système d'information, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation, en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la réglementation et aux normes, afin de proposer une traduction des enjeux de l'organisation et des exigences en termes de sécurité 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 système d'information afin d'établir la cartographie de l'architecture de sécurisation du système d'information à mettre en place.

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

Identifier les difficultés pouvant mettre en péril la réussite du projet à l'aide du suivi régulier des étapes du projet, des réalisations de chaque équipe via des entretiens individuels, d'outils de planification et de suivi général (Gantt) et des grilles d'évaluation pour assurer le déroulement du projet dans le respect du cahier des charges/du rétroplanning défini.

Maîtriser les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et par 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) 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 (dépassements mémoire, injections, bruteforce, etc.) à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces présentées par les outils pour identifier des faiblesses et vulnérabilités et garantir le maintien au niveau de sécurité attendu des développements logiciels de l'organisation.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée : équiper le système d'information d'un hôpital. Attendus du candidat : Dans un contexte de projet de sécurisation d'un système d'information d'un hôpital (opérateur d'importance vitale), le candidat doit établir un cahier des charges fonctionnel et identifier les équipements nécessaires. Partie 1 : le candidat doit, en groupe de 3 à 4 personnes, produire un dossier écrit contenant un inventaire de l'ensemble des ressources, une synthèse des différents services/outils et leur agencement logique sous forme de documentation technique et un rapport d'analyse sur les forces et faiblesses des solutions en place ainsi que des pistes d'amélioration. Les supports et ressources documentaires portant sur l'entreprise et sa situation sont fournis au candidat. Partie 2 : Le candidat doit réaliser, individuellement, un cahier des charges fonctionnel dans le cadre d'un projet de sécurisation d'un système d'information. Le candidat doit se baser sur le dossier établi en partie 1.

Étude de cas/Travaux pratiques : modélisation d'une base de données. Attendus du candidat : À partir d'un dossier technique, le candidat doit réaliser, individuellement, une cartographie d'une base de données. Les supports et ressources documentaires nécessaires sont fournis par l'organisme de formation.

Mise en situation professionnelle reconstituée : gestion d'un projet de sécurisation d'un système d'information d'une organisation. Attendus du candidat : Le candidat doit réaliser, individuellement un dossier écrit présentant le plan d'action du projet, les méthodes et les outils qui seront utilisées, dans le cadre d'un projet fictif d'une organisation témoin souhaitant sécuriser son système d'information dans un contexte international. Le candidat doit élaborer un planning, prévoir une méthode et des outils de gestion et de suivi du projet et des équipes. Le candidat doit également identifier et anticiper les éventuelles difficultés et les possibles remédiations. Les supports et ressources documentaires portant sur l'entreprise et nécessaires à la définition des objectifs du projet sont fournis par l'organisme de formation.

Mise en situation professionnelle reconstituée : sécurisation d'un système d'information. Attendus du candidat : À partir d'éléments de contextualisation d'une organisation et de différents cas d'utilisation supposés d'une messagerie chiffrée, le candidat doit, individuellement, définir les outils répondant aux besoins la solution de cryptologie la plus judicieuse et conforme au contexte. Le candidat doit déployer une solution technique dans un environnement mis à sa disposition. Il doit tester des scénarios potentiels pour vérifier la pertinence et la robustesse de ses choix techniques. La documentation et l'environnement simulé sont fournis par le centre d'examen.

Étude de cas : développement d'une digital factory. Attendus du candidat : Dans le cadre du développement d'une digital factory pour une organisation, le candidat doit proposer une sélection d'outils permettant de prendre en compte la sécurité lors du développement d'applications et lors de leur déploiement. Le candidat doit proposer également un organigramme avec les différentes équipes de la digital factory. La documentation et l'environnement simulé sont fournis par le centre d'examen.

Mise en situation professionnelle reconstituée : tester la sécurité d'un environnement. Attendus du candidat : À partir d'une plateforme de simulation, le candidat doit effectuer des tests de sécurité en suivant une fiche d'audit. Il doit rédiger un rapport qui comprend une synthèse écrite des tests réalisés à l'attention des non-techniques et une liste de recommandations. L'environnement technique simulé et la fiche d'audit sont fournis par l'organisme de formation.

RNCP37796BC03 — Suivre l'évolution du niveau de sécurité d'un système d'information d'une organisation

LISTE DE COMPÉTENCES

Réaliser un audit des systèmes d'information 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 système d'information.

Présenter les conclusions d'un audit des systèmes d'information 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, en identifiant des axes d'amélioration afin de proposer des recommandations qui contribueront à l'élévation du niveau de sécurité de l'organisation ou lui permettront d'obtenir son homologation de sécurité.

Intégrer la conduite de changement du système d'information de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus qui seront mis en place pour garantir l'adoption et l'application continue de la politique de sécurisation du système d'information.

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 système d'information.

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'intelligence artificielle 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 et des contraintes de l'organisation, en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel en fonction des 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 système d'information.

Établir un suivi actif des vulnérabilités des briques du système d'information, 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 système d'information.

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 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 système d'information et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle).

MODALITÉS D'ÉVALUATION

Étude de cas : conduite d'un audit de sécurité. Attendus du candidat : Le candidat doit, individuellement, réaliser un audit et produire un rapport. À partir d'une infrastructure technique existante fictive, d'une envergure similaire à celle que l'on retrouve dans une PME de 200 collaborateurs, le candidat doit conduire, individuellement, un audit technique et organisationnel à partir du référentiel PASSI. Le candidat doit rédiger le rapport de cet audit. Celui-ci doit témoigner du niveau de sécurisation du système d'information évalué et mettre en valeur les axes d'amélioration, des vulnérabilités, des écarts entre le cadre (légal, normatif interne, etc.) et la réalité observée. Le candidat doit formuler des recommandations d'évolution et de changement afin que le système d'information évalué respecte l'état de l'art. Il doit réaliser justifier une note à l'attention des parties prenantes leur enjoignant d'appliquer ces recommandations. L'environnement technique, les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités sont fournis par l'organisme de formation.

Mise en situation professionnelle reconstituée – Jeu de rôle : Officier en tant que RSSI. Attendus du candidat : Le candidat doit réaliser le développement et la mise en place d'un SOC. Pour cela, le candidat doit adopter la posture d'un responsable de la sécurité des systèmes d'information officiant pour une Ambassade française à l'étranger. Celle-ci vient d'emménager dans de nouveaux locaux. Il n'y a pas de reprise de l'existant. Ce travail se matérialise, dans un premier temps, par la conception, l'installation et la configuration de paramètres, de logiciels ou d'équipements sécurisés. Ce travail se matérialise également par le développement d'outils d'analyse et de suivi en temps réel des signaux d'états des équipements et services, par la définition d'une politique d'alerte correspondante. L'environnement simulé à superviser est fourni par l'organisme de formation.

Questionnaires à visée professionnelle : comment garantir la maintenance de la sécurité d'un système d'information ? Attendus du candidat : Le candidat doit, individuellement, répondre à un questionnaire portant sur sa capacité à mener des actions pour assurer le maintien en condition de sécurité d'un système d'information. Le questionnaire est composé de mini-cas relatifs à la mise à jour des équipements logiciels et matériels, à la gestion et au traitement des vulnérabilités d'un système d'information, à l'anticipation du suivi et de ses mises à jour.

Mise en situation professionnelle reconstituée : conception d'un outil de veille. Attendus du candidat : Le candidat doit réaliser, pour une entreprise fictive, une plateforme de veille et identifier des signes de mutations et innovations technologiques. Partie 1 : création d'une plateforme de veille - Le candidat doit, individuellement, sélectionner un ensemble de sources d'informations adapté au secteur d'activité de l'organisation visée, les intégrer au sein d'un outil de son choix (ou de sa propre création) et constituer une base de données de veille. Le candidat doit remettre son code et un support de son choix présentant son outil. Les supports et ressources documentaires portant sur l'entreprise et sa situation sont fournis par l'organisme de formation. Partie 2 : analyse et interprétation des données de la plateforme - Le candidat doit réaliser, à partir de l'outil déployé dans la partie 1, l'analyse des résultats obtenus pour identifier les signaux faibles indiquant une mutation technologique. Le candidat doit présenter à l'oral et avec un support de présentation son analyse.

RNCP37796BC04 — Organiser une réponse adaptée en cas de crise

LISTE DE COMPÉTENCES

Rédiger 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 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 de la part de la cellule de crise.

Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyen pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du système d'information, par la mise en place d'un canal de communication régulier, fluide et contrôlé, 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 exemple), par l'utilisation de la rétro-ingénierie (reverse engineering) et l'étude des comportements tracés dans des journaux et par 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, par la remise en service des équipements et par 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, par la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), par l'établissement d'un bilan post-crise et la mise à jour et le renforcement des procédures et des outils du système d'information 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 : Préparation à une crise cyber. Attendus du candidat : Le candidat doit démontrer, individuellement, qu'il est apte à préparer avec efficacité une crise cyber. Une plateforme technique permet de simuler les infrastructures numériques de l'organisation attaquée. Le candidat doit mettre en place des outils avant la crise (niveau de résilience, annuaires, fiches de compte rendu, cartographie du système d'information).

Questionnaires à visée professionnelle : Prévenir une cyber crise. Attendus du candidat : Le candidat doit, individuellement, répondre à un questionnaire portant sur sa capacité à maintenir à jour une stratégie de gestion de crise pour être en mesure de réagir en cas de cyberattaque. Le questionnaire est composé de mini-cas relatifs à une ou des organisations.

Mise en situation professionnelle reconstituée : - Jeu de rôle : gestion de crise cyber. Attendus du candidat : À l'occasion d'un exercice s'étalant sur cinq jours, le candidat doit démontrer, individuellement, qu'il est apte à conduire avec efficacité une crise cyber. Une plateforme technique permet de simuler les infrastructures numériques de l'organisation attaquée. Des encadrants jouent le rôle des acteurs de la crise (directions, métiers, média.). Partie 1 : Dans un environnement adapté (réseaux et parc de machines d'entreprise simulés), le candidat en groupe de 4 à 6 personnes, est amené à gérer une situation de crise (scénarios variés : attaques de type ransomware, pannes matérielles, etc.). Le candidat doit se coordonner avec les membres de son groupe pour élaborer une stratégie dans le but de relancer/maintenir les activités de l'entreprise. Le candidat doit comprendre la nature technique de la crise et

commencer le dialogue avec les acteurs clés de la crise (direction de l'organisation attaquées, personnels représentant les métiers attaqués, médias, clients et sous-traitants). Lors d'un entretien auprès d'un jury, le candidat doit présenter l'ensemble des modalités à dérouler et justifier son propos au regard de la crise, des enjeux du contexte de l'organisation et des priorités afin de limiter les perturbations de l'activité. Partie 2 : Le candidat doit, individuellement, identifier l'attaquer et lancer l'analyse à l'aide d'outils. Le candidat doit déterminer les impacts techniques et opérationnels de l'attaque et effectuer des prélèvements numériques et une investigation numérique. Le candidat doit remettre un rapport d'investigation rédigé en fournissant des preuves techniques afin d'engager des poursuites judiciaires, et établir une note sur les impacts liés à cet incident. Partie 3 : Le candidat doit, de nouveau en groupe de 4 à 6 personnes, remettre en service le système d'information impacté en déroulant un plan de reprise d'activité. Le candidat doit rédiger un rapport et proposer des mesures techniques et organisationnelles permettant de renforcer la résilience de l'organisation. Il propose d'éventuelles suites judiciaires.

L'environnement technique simulé et l'ensemble des ressources documentaires est fourni par l'organisme de formation.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Du fait de la numérisation des processus et modes de travail, la cybersécurité touche aujourd'hui l'ensemble des secteurs d'activités. La gestion et le stockage de données impose à n'importe quelle organisation de mettre en place les moyens nécessaires à sa sécurité et sa pérennité. C'est pourquoi, le secteur d'activité du gestionnaire de la sécurité des données, des réseaux et des systèmes peut varier. Il peut officier au sein de société d'informatique, dans le secteur industriel mais aussi pour les banques, les assurances et mutuelles. Les opérateurs d'importance vitales privés ou publics représentent également un enjeu majeur de l'exercice des métiers liés à la sécurité des systèmes d'information.

TYPE D'EMPLOIS ACCESSIBLES

- Responsable de la sécurité des systèmes d'information
- Ingénieur cybersécurité
- Consultant cybersécurité
- Architecte cybersécurité
- Analyste cybersécurité
- Expert cybersécurité/sécurité des systèmes d'information
- Responsable de la cybersécurité
- Ingénieur réseau et sécurité

RÈGLEMENTATIONS D'ACTIVITÉ

La menace numérique accroît, à ce jour, sans cesse. Dans ce contexte, se conformer aux normes et réglementations en vigueur est un atout majeur pour une entreprise. Les activités du gestionnaire de la sécurité des données, des réseaux et des systèmes s'exercent dans le cadre des réglementations et normes suivantes :

- Loi Godfrain ;
- Le cadre réglementaire défini par la CNIL ;
- Les recommandations de l'ANSSI ;
- La réglementation de l'ARCEP ;
- Le Règlement Général sur la Protection des Données ;
- Digital Services Act : législation sur les services numériques de la Commission Européenne ;
- Le règlement sur les marchés numériques (DMA) ;
- L'ensemble des normes de la famille ISO 27000 ;
- La norme ISO 14001 ;
- Loi de programmation militaire (LPM) ;
- Guide EBIOS Risk Manager (ANSSI) ;
- Référentiel PASSI (ANSSI).

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % 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) 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)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le parcours proposé sur 2 années en alternance s'adresse d'une part aux titulaires d'un niveau 6 dans les métiers de l'informatique et souhaitant poursuivre leurs études vers un niveau 7, et d'autre part aux personnes en transition professionnelle.

PRÉREQUIS À LA VALIDATION

Validation des 4 blocs, complétée de la validation d'un mémoire de recherche professionnel de fin d'études et de sa soutenance orale.

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

- Le Président du jury (interne)
- Le Président de l'école ou son représentant (Directeur du cursus)
- Trois professionnels exerçant le métier visé et strictement indépendants de l'École Hexagone (externes).

Aucun des membres du jury de certification, quelle que soit la voie d'accès, ne peut avoir de lien personnel et/ou professionnel avec un candidat

COMPOSITION DU JURY — VAE

- Le Directeur du cursus
- Deux professionnels exerçant le métier visé dont un consultant-formateur

Aucun des membres du jury de certification, quelle que soit la voie d'accès, ne peut avoir de lien personnel et/ou professionnel avec un candidat

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	9 157 €
Selon la branche	7 500 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 173 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Branche des organismes de formation, CPNEF de la Publicité
9 000 €	CPNE Banque, CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire, CPNEFP de la branche des prestataires de services du secteur tertiaire
8 696 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP des jardineries et graineteries, CPNEFP du Négoce de l'ameublement
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 098 €	CPNEFP des industries des jeux, jouets, articles de fêtes et ornements de Noël, articles de puériculture et voitures d'enfants, modélisme et industries connexes
11 050 €	CPNEFP de la Mutualité Sociale Agricole
10 500 €	CPNEFP des industries des tuiles et briques
10 164 €	CPNE Casinos
10 163 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
10 000 €	CPNE des exploitations frigorifiques
9 800 €	CPNEF de l'audiovisuel
9 500 €	CPNE de l'ingénierie, des services informatiques et du conseil
9 264 €	CPNE de la branche de la Distribution Directe
9 231 €	CPNEFP Commerce à distance
9 200 €	CPNE des sociétés financières
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 701 €	CPNE FP Branche des magasins du Bricolage
8 500 €	CPNEFP de la métallurgie
8 000 €	CPNE chimie
7 748 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	19/07/2023
Durée de l'enregistrement	3 ans

Date d'échéance de l'enregistrement	19/07/2026
Date de dernière délivrance possible	19/07/2030

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42345

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www.ecole-hexagone.com/fr/fr/cursus/cyberdefense/>

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/37796/>

Entrées et sorties de formation

Entrées en formation	86
Parcours menés à terme	52
Taux d'achèvement	60 %
Période	03/2024 – 07/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	89
Montant total engagé	426 359 €
Coût moyen par dossier	4 791 €
Durée moyenne	653 h
Période	02/2024 – 05/2026
France compétences	58 %
France Travail	32 %
OPCO	6 %
Entreprise	3 %
Reste à charge titulaire	1 %

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