

Expert en cybersécurité des systèmes d'information (BADGE CGE)

RNCP37989 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31038
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	20/09/2023
Date d'échéance	20/09/2026

Certificateur(s)

ECOLE POUR L'INFORMATIQUE ET LES TECHNIQUES AVANCEES (EPITA) · SIRET : 89819207500015

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
INSTITUT POLYTECHNIQUE DES SCIENCES AVANCEES (IPSA)	89812490400019	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La sécurité des systèmes d'information, ou cybersécurité, est considérée par la France comme priorité nationale et concerne désormais chaque entreprise, chaque administration et chaque citoyen.

Les données sont vitales pour toutes les structures. Les startups protègent leurs innovations, les grands groupes industriels leur patrimoine informationnel, les commerçants leurs données clients, les services de l'État les données régaliennes et les données des citoyens. La protection de l'accès au système d'information et aux réseaux informatiques est aussi cruciale comme le démontrent les attaques récentes ayant paralysé l'activité de nombreuses entreprises.

Pour se préserver de ces attaques, aborder sereinement leur transformation numérique et préserver leur patrimoine immatériel et humain, les entreprises doivent disposer, dans une approche de sécurité économique globale, de solutions humaines et techniques de cybersécurité.

Si les équipements techniques, matériels et logiciels, sont facilement disponibles, leur mise en œuvre est souvent retardée par manque de compétences humaines.

La certification « Expert en Cybersécurité des Systèmes d'Information » répond à l'attente des entreprises de disposer rapidement des talents indispensables à leur protection, à leur compétitivité et au maintien de l'emploi. Elle couvre un large spectre de compétences qui vont de la gouvernance sécurisée du Système d'Information (SI) à la gestion des incidents en passant par les phases de conception et les phases d'audit.

ACTIVITÉS VISÉES

Sécuriser et superviser le système d'information (SI)

- Sécurisation des réseaux et infrastructures
- Sécurisation du cloud

- Sécurisation des systèmes industriels
- Mise en œuvre des tests d'intrusion
- Protection des données personnelles
- Mise en place de la politique de sécurité

Sécuriser les données, les projets et les développements

- Suivi d'un projet informatique
- Sécurisation des projets informatiques
- Sécurisation des développements web
- Sécurisation des données
- Sécurisation des applications mobiles

Identifier les risques et organiser la cybersécurité

- Mesure des enjeux de sécurité et des facteurs de risques associés
- Inscription de la sécurité numérique dans démarche de sécurité globale
- Application du droit de la cybersécurité
- Identification des acteurs de l'écosystème de la sécurité
- Analyse et quantification des risques
- Utilisation des techniques d'influence et de négociation pour la mise en œuvre interne de la politique de sécurité

Détecter les incidents de sécurité numérique et y répondre

- Gestion d'une crise cyber
- Collecte et analyse forensiques
- Réponse aux intrusions et autres incidents

COMPÉTENCES ATTESTÉES

Mettre en œuvre dans l'entreprise les bonnes pratiques d'administration du réseau en créant une cartographie réseau intégrant tous ses composants, en configurant les contrôles d'accès, en cloisonnant les différentes parties du réseau et en interprétant les résultats des outils de surveillance d'infrastructures afin d'organiser, créer et maintenir la sécurité du système d'information.

Identifier les problématiques de sécurité au sein d'un réseau en interprétant les transactions entre les systèmes présents sur le réseau et en détectant les attaques de sécurité sur le réseau pour prévenir les incidents de sécurité dans l'entreprise.

Choisir et implémenter une stratégie de sécurité cloud en analysant les architectures de sécurité des fournisseurs de cloud, en identifiant les problématiques de sécurité spécifiques aux micro-services, en intégrant au besoin les micro-services au sein de l'infrastructure traditionnelle et en réalisant l'automatisation des tâches opérationnelles de sécurité dans le cloud afin de gérer la sécurité des services hébergés dans le cloud.

Remédier aux risques des systèmes industriels dans un SI en identifiant les composants d'un écosystème d'automates de gestion et de contrôle, les protocoles et architectures courants SCADA, en identifiant les vulnérabilités majeures de cybersécurité industrielle et les risques associés, en déterminant les risques inhérents à une architecture, et en choisissant les solutions appropriées, afin de prévenir les dangers de sécurité générés par les équipements industriels.

Effectuer des tests d'intrusions en considérant les problématiques de sécurité opérationnelle, en sélectionnant le type de tests d'intrusion approprié, en utilisant les outils pour identifier des vulnérabilités et en construisant une campagne ciblée d'hameçonnage afin d'identifier les vulnérabilités et faiblesses du SI et les failles humaines.

Vérifier la conformité des pratiques dans l'entreprise à la législation sur les données personnelles en prenant en compte les termes de la Loi Informatique et Libertés et du RGPD, en adoptant les bons réflexes dans la pratique quotidienne de la protection des données et en choisissant des solutions permettant une protection efficace des données à caractère personnel, pour s'assurer que l'ensemble des procédures respectent les exigences légales.

Concevoir un document de référence qui formalise la politique de sécurité en évaluant les problématiques de sécurité et de gestion des données au sein d'un SI, en appliquant la série de normes ISO 27000, en utilisant le système développé par le NIST et en suivant le guide de l'ANSSI pour orchestrer une politique de sécurité des SI pertinente.

Intégrer les problématiques d'accessibilité dans la politique de sécurité en évaluant les solutions retenues, en identifiant les aménagements raisonnables nécessaires et en appliquant le RGAA afin d'assurer un niveau d'accessibilité des politiques de sécurité à toutes les parties concernées dans la structure.

Intégrer les enjeux de cybersécurité dans les projets informatiques de l'entreprise, en cadrant l'expression du besoin par une note de synthèse, en structurant les différentes parties d'un cahier des charges liées à sécurité, en appliquant la méthodologie du projet (classique ou Agile) et en prenant en compte les étapes du projet, afin d'assurer la prise en

compte des enjeux de cybersécurité tout au long du cycle de vie des projets d'un point de vue métier.

Implémenter les éléments ayant un impact sur la sécurité informatique du projet tout au long de son cycle de vie, en concevant un système de droits et de privilèges, en organisant la gestion des vulnérabilités, en définissant et réalisant des tests de sécurité, en employant les technologies d'isolation et en organisant la mise en production, afin de mettre en place et de maintenir un projet informatique de manière sécurisée.

Prévenir et corriger les vulnérabilités des applications web, en appliquant les standards spécifiques aux applications web, en respectant les bonnes pratiques de développement et en apportant les corrections, afin de concevoir des applications web sécurisées et de pallier les failles des applications existantes.

Contrôler la sécurité d'une application en effectuant des audits de sécurité, en déployant des outils de protection et de surveillance, afin de garantir un haut niveau de sécurité et d'en assurer la pérennité.

Analyser les pratiques de chiffrements et de ségrégation des données en identifiant les principaux algorithmes de cryptographie moderne, en distinguant leurs différents cas d'utilisation (disque, réseau, base de données), en interprétant un résultat d'étude cryptographique et en sélectionnant la granularité de données à chiffrer afin de choisir et d'appliquer une solution pertinente pour sécuriser les données.

Proposer une méthodologie adaptée pour la sauvegarde des données en analysant les solutions existantes et en sélectionnant la solution adaptée aux données et au besoin de sécurité afin d'assurer la résilience de l'entreprise.

Prévenir et corriger les vulnérabilités des applications mobiles, en appliquant les standards spécifiques aux applications mobiles et à l'architecture de sécurité des téléphones, en reconnaissant les schémas classiques de vulnérabilités sur Android et iOS, en utilisant les systèmes de protections des données offerts par les systèmes mobiles, en respectant les bonnes pratiques de développement et en apportant les corrections adaptées, afin de concevoir des applications mobiles sécurisées et de pallier les failles des applications existantes.

Identifier les enjeux cyber auxquels l'entreprise est confrontée, en distinguant les différents types d'attaquants, en appréhendant la diversité des motivations, en identifiant les diverses sortes d'attaques et leurs conséquences et en reconnaissant les fragilités les plus courantes des systèmes d'information pour inscrire la démarche de sécurité dans le contexte global.

Concevoir les principes de sécurité d'une organisation, en appréhendant les enjeux de sécurité d'un point de vue structurel, en prenant en compte la place du facteur humain à côté du risque technique et en rédigeant un document de politique de sécurité numérique, afin d'inscrire la sécurité numérique dans la démarche de sécurité globale de la structure.

Intégrer les problématiques de développement durable dans la mise en place d'une démarche de sécurité globale, en évaluant le coût énergétique des mesures envisagées et en identifiant les moyens de réduire la consommation énergétique de ces mesures afin de limiter l'impact de ces mesures sur l'évolution du climat.

Réaliser une veille relative aux problématiques légales liées à la cybersécurité, en identifiant les règles de droit applicables en matière de sécurité numérique, en différenciant les responsabilités civile et pénale et en suivant les évolutions légales et les exigences de conformité afin d'échanger avec les services juridiques et de prendre des décisions qui respectent la réglementation en vigueur.

Identifier les différents acteurs de l'écosystème de la cybersécurité étatiques ou industriels, en comprenant les rôles respectifs des acteurs étatiques et en évaluant les solutions technologiques proposées par différents fournisseurs, afin de solliciter les acteurs appropriés et de choisir les solutions de sécurité pertinentes et adaptées à la structure.

Classifier et mesurer les risques de sécurité liés à un système d'information complexe en identifiant les menaces, en utilisant les normes (ISO 27005, NIST8000) et méthodes (EBIOS, FAIR) de gestion de risques afin de réaliser une analyse de risque.

Interpréter les résultats de l'analyse de risque en intégrant les contraintes liées aux métiers de l'entreprise, en rapprochant la gestion des risques de la sécurité numérique de la gestion des autres risques de sécurité afin de définir les objectifs de sécurité numérique de l'entreprise.

Sensibiliser les décideurs de l'entreprise sur la nécessité de la mise en œuvre interne de la politique de sécurité, en argumentant la pertinence des solutions retenues, en utilisant des techniques d'influence et de négociation et en interagissant avec des acteurs décisionnaires d'une entreprise, afin de défendre ses solutions et ses préconisations auprès des décideurs et de les faire adhérer à la politique de sécurité.

Préparer la structure à une crise cyber en créant une cellule de crise, en identifiant le rôle des différents acteurs lors d'une crise, en mettant en place des entraînements et en adaptant ces entraînements aux personnes en situation de handicap pour être capable de réagir promptement et efficacement en cas de survenue de la crise.

Activer la cellule de crise, en assurant la coordination entre les acteurs techniques et décisionnaires de la structure, en contrôlant les relations entre les acteurs externes et internes en charge de résoudre le problème et en échangeant avec les assurances afin de remédier à l'attaque et d'assurer une continuité de l'activité.

Piloter la mise en place du plan de continuité d'activité, en activant les solutions prévues en cas de crise, et en coordonnant les différents acteurs concernés, afin d'assurer la résilience des applications et des données.

Gérer la sortie de crise en estimant les impacts techniques et financiers de l'attaque et en identifiant les correctifs à appliquer et les coûts associés (tout en préservant au maximum les opérations métiers de l'entreprise), pour régénérer un environnement informatique sécurisé après la compromission.

Assurer la communication en interne et en externe lors d'une crise, en mettant en place des canaux spécifiques en interne, en informant les parties tierces concernées, en échangeant avec les autorités appropriées et en expliquant les conséquences aux clients et prestataires, tout en adaptant cette communication aux personnes en situation de handicap afin de préserver la réputation de la structure, circonscrire les conséquences de la compromission et augmenter l'efficacité de la remédiation.

Rassembler les données nécessaires à une analyse forensique, en collectant les journaux d'événements, en utilisant un système de management des informations de sécurité (SIEM), en interfaçant différents équipements réseau au sein du SIEM et en déployant des agents de collecte d'information, afin de réunir les éléments nécessaires pour identifier un attaquant.

Analyser les données collectées en détectant les comportements anormaux, en réalisant une levée de doute et en créant des systèmes d'alertes automatisés afin de détecter les compromissions.

Analyser une attaque informatique, en utilisant les informations forensiques collectées, en identifiant les différents types de virus informatique et leurs comportements, en réalisant une investigation numérique pour remonter à l'origine de l'intrusion, en observant le comportement de l'attaquant et en interprétant ces résultats avec les outils de renseignement de menace (threat intelligence), pour établir un faisceau de preuves et choisir une réponse stratégique appropriée.

Blocs de compétences

RNCP37989BC01 — Sécuriser et superviser le système d'information (SI)

LISTE DE COMPÉTENCES

Mettre en œuvre dans l'entreprise les bonnes pratiques d'administration du réseau en créant une cartographie réseau intégrant tous ses composants, en configurant les contrôles d'accès, en cloisonnant les différentes parties du réseau et en interprétant les résultats des outils de surveillance d'infrastructures afin d'organiser, créer et maintenir la sécurité du système d'information.

Identifier les problématiques de sécurité au sein d'un réseau en interprétant les transactions entre les systèmes présents sur le réseau et en détectant les attaques de sécurité sur le réseau pour prévenir les incidents de sécurité dans l'entreprise.

Choisir et implémenter une stratégie de sécurité cloud en analysant les architectures de sécurité des fournisseurs de cloud, en identifiant les problématiques de sécurité spécifiques aux micro-services, en intégrant au besoin les micro-services au sein de l'infrastructure traditionnelle et en réalisant l'automatisation des tâches opérationnelles de sécurité dans le cloud afin de gérer la sécurité des services hébergés dans le cloud.

Remédier aux risques des systèmes industriels dans un SI en identifiant les composants d'un écosystème d'automates de gestion et de contrôle, les protocoles et architectures courants SCADA, en identifiant les vulnérabilités majeures de cybersécurité industrielle et les risques associés, en déterminant les risques inhérents à une architecture, et en choisissant les solutions appropriées, afin de prévenir les dangers de sécurité générés par les équipements industriels.

Effectuer des tests d'intrusions en considérant les problématiques de sécurité opérationnelle, en sélectionnant le type de tests d'intrusion approprié, en utilisant les outils pour identifier des vulnérabilités et en construisant une campagne ciblée d'hameçonnage afin d'identifier les vulnérabilités et faiblesses du SI et les failles humaines.

Vérifier la conformité des pratiques dans l'entreprise à la législation sur les données personnelles en prenant en compte les termes de la Loi Informatique et Libertés et du RGPD, en adoptant les bons réflexes dans la pratique quotidienne de la protection des données et en choisissant des solutions permettant une protection efficace des données à caractère personnel, pour s'assurer que l'ensemble des procédures respectent les exigences légales.

Concevoir un document de référence qui formalise la politique de sécurité en évaluant les problématiques de sécurité et de gestion des données au sein d'un SI, en appliquant la série de normes ISO 27000, en utilisant le système développé par le NIST et en suivant le guide de l'ANSSI pour orchestrer une politique de sécurité des SI pertinente.

Intégrer les problématiques d'accessibilité dans la politique de sécurité en évaluant les solutions retenues, en identifiant les aménagements raisonnables nécessaires et en appliquant le RGAA afin d'assurer un niveau

d'accessibilité des politiques de sécurité à toutes les parties concernées dans la structure.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Sous la forme d'un projet pédagogique, le candidat devra créer l'organisation d'un réseau et sa cartographie. Il devra statuer sur la configuration des équipements et proposer des solutions permettant de détecter des attaques. Il devra aussi identifier les problématiques de sécurité en fonction de l'environnement et les corriger si besoin.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sous forme d'exercices pratiques, le candidat devra retrouver des failles de sécurité au sein d'un système informatique, exploiter ces vulnérabilités et ensuite sélectionner parmi plusieurs choix la solution appropriée.

Pour valider, le candidat devra avoir résolu les deux tiers des épreuves.

Mise en situation professionnelle

Sous la forme d'un projet pédagogique, le candidat rédige un document décrivant le comportement attendu des collaborateurs d'une structure pour le respect de la protection des données à caractère personnel.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sous la forme d'un projet pédagogique, le candidat rédige un document de référence destiné à l'ensemble de la structure documentant la politique de sécurité.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

RNCP37989BC02 — Sécuriser les données, les projets et les développements

LISTE DE COMPÉTENCES

Intégrer les enjeux de cybersécurité dans les projets informatiques de l'entreprise, en cadrant l'expression du besoin par une note de synthèse, en structurant les différentes parties d'un cahier des charges liées à sécurité, en appliquant la méthodologie du projet (classique ou Agile) et en prenant en compte les étapes du projet, afin d'assurer la prise en compte des enjeux de cybersécurité tout au long du cycle de vie des projets d'un point de vue métier.

Implémenter les éléments ayant un impact sur la sécurité informatique du projet tout au long de son cycle de vie, en concevant un système de droits et de privilèges, en organisant la gestion des vulnérabilités, en définissant et réalisant des tests de sécurité, en employant les technologies d'isolation et en organisant la mise en production, afin de mettre en place et de maintenir un projet informatique de manière sécurisée.

Prévenir et corriger les vulnérabilités des applications web, en appliquant les standards spécifiques aux applications web, en respectant les bonnes pratiques de développement et en apportant les corrections, afin de concevoir des applications web sécurisées et de pallier les failles des applications existantes.

Contrôler la sécurité d'une application en effectuant des audits de sécurité, en déployant des outils de protection et de surveillance, afin de garantir un haut niveau de sécurité et d'en assurer la pérennité.

Analyser les pratiques de chiffrements et de ségrégation des données en identifiant les principaux algorithmes de cryptographie moderne, en distinguant leurs différents cas d'utilisation (disque, réseau, base de données), en interprétant un résultat d'étude cryptographique et en sélectionnant la granularité de données à chiffrer afin de choisir et d'appliquer une solution pertinente pour sécuriser les données.

Proposer une méthodologie adaptée pour la sauvegarde des données en analysant les solutions existantes et en sélectionnant la solution adaptée aux données et au besoin de sécurité afin d'assurer la résilience de l'entreprise.

Prévenir et corriger les vulnérabilités des applications mobiles, en appliquant les standards spécifiques aux applications mobiles et à l'architecture de sécurité des téléphones, en reconnaissant les schémas classiques de vulnérabilités sur Android et iOS, en utilisant les systèmes de protections des données offerts par les systèmes mobiles, en respectant les bonnes pratiques de développement et en apportant les corrections adaptées, afin de concevoir des applications mobiles sécurisées et de pallier les failles des applications existantes.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Sur la base d'un projet pédagogique d'analyse d'un projet informatique, le candidat expose son analyse en tenant compte des informations qui lui sont données et propose l'intégration de la sécurité dans ce projet.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sous forme d'exercices pratiques, le candidat devra retrouver des failles de sécurité dans des applications qui lui sont soumises, exploiter ces vulnérabilités et ensuite sélectionner parmi plusieurs choix la solution appropriée.

Pour valider, le candidat devra avoir résolu les deux tiers des épreuves.

Mise en situation professionnelle

Sous la forme d'un projet pédagogique, le candidat devra choisir des solutions de cryptographie, sélectionner une méthode pour isoler les données et proposer un système de sauvegarde.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sous la forme d'un projet pédagogique, le candidat identifie les processus de stockage des données et prévoit un plan de tests de sécurité.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

RNCP37989BC03 — Identifier les risques et organiser la cybersécurité

LISTE DE COMPÉTENCES

Identifier les enjeux cyber auxquels l'entreprise est confrontée, en distinguant les différents types d'attaquants, en appréhendant la diversité des motivations, en identifiant les diverses sortes d'attaques et leurs conséquences et en reconnaissant les fragilités les plus courantes des systèmes d'information pour inscrire la démarche de sécurité dans le contexte global.

Concevoir les principes de sécurité d'une organisation, en appréhendant les enjeux de sécurité d'un point de vue structurel, en prenant en compte la place du facteur humain à côté du risque technique et en rédigeant un document de politique de sécurité numérique, afin d'inscrire la sécurité numérique dans la démarche de sécurité globale de la structure.

Intégrer les problématiques de développement durable dans la mise en place d'une démarche de sécurité globale, en évaluant le coût énergétique des mesures envisagées et en identifiant les moyens de réduire la consommation énergétique de ces mesures afin de limiter l'impact de ces mesures sur l'évolution du climat.

Réaliser une veille relative aux problématiques légales liées à la cybersécurité, en identifiant les règles de droit applicables en matière de sécurité numérique, en différenciant les responsabilités civile et pénale et en suivant les évolutions légales et les exigences de conformité afin d'échanger avec les services juridiques et de prendre des décisions qui respectent la réglementation en vigueur.

Identifier les différents acteurs de l'écosystème de la cybersécurité étatiques ou industriels, en comprenant les rôles respectifs des acteurs étatiques et en évaluant les solutions technologiques proposées par différents fournisseurs, afin de solliciter les acteurs appropriés et de choisir les solutions de sécurité pertinentes et adaptées à la structure.

Classifier et mesurer les risques de sécurité liés à un système d'information complexe en identifiant les menaces, en utilisant les normes (ISO 27005, NIST8000) et méthodes (EBIOS, FAIR) de gestion de risques afin de réaliser une analyse de risque.

Interpréter les résultats de l'analyse de risque en intégrant les contraintes liées aux métiers de l'entreprise, en rapprochant la gestion des risques de la sécurité numérique de la gestion des autres risques de sécurité afin de définir les objectifs de sécurité numérique de l'entreprise.

Sensibiliser les décideurs de l'entreprise sur la nécessité de la mise en œuvre interne de la politique de sécurité, en argumentant la pertinence des solutions retenues, en utilisant des techniques d'influence et de négociation et en interagissant avec des acteurs décisionnaires d'une entreprise, afin de défendre ses solutions et ses préconisations auprès des décideurs et de les faire adhérer à la politique de sécurité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Sur la base d'un projet pédagogique, le candidat rédige les documents afférents à la politique de sécurité numérique d'une structure et destinés à l'ensemble des collaborateurs.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sur la base d'un projet pédagogique, le candidat réalise une analyse de risque sur des problématiques de cybersécurité, interprète les résultats de cette analyse et rédige un argumentaire pour faire adopter les solutions qu'il préconise.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

RNCP37989BC04 — Détecter les incidents de sécurité numérique et y répondre

LISTE DE COMPÉTENCES

Préparer la structure à une crise cyber en créant une cellule de crise, en identifiant le rôle des différents acteurs lors d'une crise, en mettant en place des entraînements et en adaptant ces entraînements aux personnes en situation de handicap pour être capable de réagir promptement et efficacement en cas de survenue de la crise.

Activer la cellule de crise, en assurant la coordination entre les acteurs techniques et décisionnaires de la structure, en contrôlant les relations entre les acteurs externes et internes en charge de résoudre le problème et en échangeant avec les assurances afin de remédier à l'attaque et d'assurer une continuité de l'activité.

Piloter la mise en place du plan de continuité d'activité, en activant les solutions prévues en cas de crise, et en coordonnant les différents acteurs concernés, afin d'assurer la résilience des applications et des données.

Gérer la sortie de crise en estimant les impacts techniques et financiers de l'attaque et en identifiant les correctifs à appliquer et les coûts associés (tout en préservant au maximum les opérations métiers de l'entreprise), pour régénérer un environnement informatique sécurisé après la compromission.

Assurer la communication en interne et en externe lors d'une crise, en mettant en place des canaux spécifiques en interne, en informant les parties tierces concernées, en échangeant avec les autorités appropriées et en expliquant les conséquences aux clients et prestataires, tout en adaptant cette communication aux personnes en situation de handicap afin de préserver la réputation de la structure, circonscrire les conséquences de la compromission et augmenter l'efficacité de la remédiation.

Rassembler les données nécessaires à une analyse forensique, en collectant les journaux d'événements, en utilisant un système de management des informations de sécurité (SIEM), en interfaçant différents équipements réseau au sein du SIEM et en déployant des agents de collecte d'information, afin de réunir les éléments nécessaires pour identifier un attaquant.

Analyser les données collectées en détectant les comportements anormaux, en réalisant une levée de doute et en créant des systèmes d'alertes automatisés afin de détecter les compromissions.

Analyser une attaque informatique, en utilisant les informations forensiques collectées, en identifiant les différents types de virus informatique et leurs comportements, en réalisant une investigation numérique pour remonter à l'origine de l'intrusion, en observant le comportement de l'attaquant et en interprétant ces résultats avec les outils de renseignement de menace (threat intelligence), pour établir un faisceau de preuves et choisir une réponse stratégique appropriée.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

Sur la base d'un projet pédagogique de simulation de crise cyber, le candidat réunit la cellule de crise et en supervise le fonctionnement du début de la crise jusqu'à la reprise complète d'activité.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Mise en situation professionnelle

Sur la base d'un projet pédagogique de simulation de crise cyber, le candidat réalise une collecte et une analyse forensique pour détecter un incident. Il procède ensuite à une analyse technique de l'attaque détectée pour choisir la réponse adaptée.

Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Ce métier est susceptible de s'exercer dans tous les secteurs d'activités puisqu'ils sont tous concernés par la cybersécurité et

doivent tous faire face à la menace croissante. Néanmoins, les secteurs d'activité principalement visés sont :

- Les entreprises utilisatrices des TIC (tous secteurs d'activité) ;
- Les entreprises de Services Numériques – ESN ;
- Les administrations nationales (services informatiques) ;
- Les banques (services informatique) ;
- Les assurances (services informatique) ;
- Les établissements de soin (privés et publics) ;
- Les établissements d'enseignement (publics et privés) ;

- Les éditeurs de logiciels ;
- Les entreprises spécialisées dans l'audit et le conseil en informatique.
- Les entreprises spécialisées en cybersécurité.

La taille des entreprises pourra être très variable, étant donné la nature du besoin auquel répond la certification :

- Startups : toutes tailles ;
- Entreprises de conseil : toutes tailles ;
- Entreprises des Services Numériques (ESN) : toutes tailles ;
- Banques : toutes tailles ;
- Assurances : toutes tailles ;
- Finance : toutes tailles ;
- Administrations nationales : toutes tailles

TYPE D'EMPLOIS ACCESSIBLES

L'Expert en cybersécurité des Systèmes d'Information pourra accéder aux emplois suivants :

- Gestionnaire de la sécurité des données, des réseaux et des systèmes ;
- Architecte Sécurité des SI ;
- Responsable de la sécurité des systèmes d'information (RSSI) ;
- Directeur Cybersécurité ;
- Coordinateur sécurité ;
- Directeur de programme sécurité ;
- Responsable de SOC (Security Operation Center)
- Analyste SOC ;
- Intégrateur de sécurité ;
- Analyste de la menace cybersécurité ;
- Administrateur de solutions de sécurité ;
- Auditeur de sécurité technique ;
- Maître d'œuvre ou d'ouvrage de projets à forte composante sécurité ;

RÈGLEMENTATIONS D'ACTIVITÉ

L'accès à ce métier n'est pas réglementé. Néanmoins, dans l'exercice de son activité, l'expert en Cybersécurité des Systèmes d'Information doit respecter un certain nombre de réglementations.

- La Loi de Programmation militaire de 2013

Dès 2013, faisant suite aux préconisations du Livre blanc sur la défense et la sécurité nationale, la Loi de Programmation Militaire de décembre 2013 a adopté un volet cyber. Son article 22 contraint les Opérateurs d'Importance Vitale (OIV) au renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les Systèmes d'Information d'Importance Vitale (SIIV). Ces OIV qui représentent plus de 200 opérateurs publics ou privés dont les activités sont indispensables au bon fonctionnement et à la survie de la nation (la liste est gardée confidentielle pour des questions de sécurité nationale) doivent mettre en place des mesures de protection contre des actes malveillants portant atteinte à leur bon fonctionnement.

- La Directive « Network and Information System Security » (NIS)

En complément du dispositif précédent, la directive Network and Information System Security (NIS) a été adoptée par les institutions européennes le 6 juillet 2016. Elle vise à assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Le 1er chapitre de cette directive NIS prévoit la création d'un cadre réglementaire pour renforcer la cybersécurité des Opérateurs de Services qui sont Essentiels au fonctionnement de l'économie et de la société (OSE). Ces OSE, à l'instar des OIV, apparaissent essentiels pour la vie quotidienne des français et doivent donc se protéger des cyber malveillances en mettant en œuvre un dispositif de cybersécurité dédié. Ce dispositif est entré en vigueur en France en 2018.

- La Directive SRI.

La Directive SRI a pour finalité de garantir un niveau de sécurité des réseaux et des systèmes d'information uniformément élevé dans l'ensemble de l'UE.

Le Conseil vient d'adopter une nouvelle directive sur un niveau élevé commun de cybersécurité dans l'ensemble de l'Union : La directive SRI 2. Elle constituera la base des mesures de gestion des risques en matière de cybersécurité et des obligations en matière de signalement dans tous les secteurs couverts par la directive, et notamment l'énergie, les transports, la santé et l'infrastructure numérique.

- Le Règlement général sur la Protection des Données

De plus, le régime de la protection des données à caractère personnel renforcé par le Règlement général sur la

Protection des Données entré en vigueur le 25 mai 2018 (RGPD) contient également un volet consacré à la sécurité numérique puisqu'il impose à l'ensemble des entreprises et administrations la mise en œuvre de « mesures techniques ou organisationnelles appropriées », qui peuvent notamment inclure le « chiffrement des données » et des « moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience ».

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)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
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)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS
Formation continue, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Tout candidat doit satisfaire à l'une des conditions suivantes :

- Être titulaire d'un diplôme de niveau supérieur ou égal au niveau 7 en rapport avec l'intitulé de la formation.
- Être titulaire d'un diplôme de niveau supérieur ou égal au niveau 6 en rapport direct avec l'intitulé de la formation.
- Être titulaire d'un diplôme de niveau supérieur ou égal au niveau 5 en rapport avec l'intitulé de la formation et posséder une expérience professionnelle solide de 5 années apportant les prérequis nécessaires, et éventuellement une expérience professionnelle en rapport direct avec l'objet de la formation

Pour suivre ce programme, il est également requis :

- D'avoir des connaissances générales de l'outil informatique
- De savoir programmer dans un langage "bas niveau" (par exemple C ou C++)
- De savoir programmer dans un langage "haut niveau" (par exemple Python ou Java, Python est recommandé)
- D'avoir des connaissances de base en réseaux (TCP/IP, modèle OSI ...)
- D'avoir des connaissances de base en système (utilisation d'une ligne de commande Linux, concept de ce qu'est un appel système ...)

PRÉREQUIS À LA VALIDATION

Les conditions de présentation d'un candidat à la certification sont les suivantes :

- Avoir suivi l'ensemble des cours, travaux dirigés, travaux pratiques, etc. et avoir participé aux évaluations en cours de formation
- Avoir réalisé l'ensemble des projets
- Avoir remis un mémoire professionnel
- Avoir participé à la soutenance finale devant le jury de validation

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

Le jury de certification est composé de cinq membres, dont au moins trois experts en sécurité numérique :

- Un président du jury, personne extérieure à EPITA
- Un vice-président, personne extérieure à EPITA
- Un expert en sécurité numérique, personne extérieure à EPITA
- Le directeur général ou la directrice de la formation continue EPITA
- Le responsable pédagogique de la certification

En début de jury, un président est désigné parmi les membres professionnels. En cas de nécessité, sa voix compte double.

COMPOSITION DU JURY — VAE

Le jury de certification est constitué de cinq membres :

- Un président du jury, personne extérieure à EPITA
- Un vice-président, personne extérieure à EPITA
- Un expert en sécurité numérique, personne extérieure à EPITA
- Le directeur général ou la directrice de la formation continue EPITA
- Le responsable pédagogique de la certification

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	9 992 €
Selon la branche	7 700 € – 10 952 €
Prise en charge	Branches concernées
9 992 €	Valeur par défaut · 184 branches
10 952 €	CPNE Casinos, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEF de la Publicité
10 000 €	CPNE des industries de santé (CPNEIS), CPNEFP de l'enseignement privé indépendant
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP du Négoce de l'ameublement
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
8 500 €	CPNEFP de la Mutualité Sociale Agricole, CPNEFP de la métallurgie
10 514 €	CPNE Travail Temporaire
10 268 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
9 200 €	CPNEFP des industries électriques et gazières
9 055 €	CPNEFP Habillement succursaliste
8 750 €	CPNEFP Commerce à distance
8 700 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 195 €	CPNE FP Branche des magasins du Bricolage
8 000 €	CPNE chimie
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date de décision	20/09/2023
-------------------------	------------

Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	20/09/2026
Date de dernière délivrance possible	20/09/2030

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.securesphere.fr/formation/formation-badge-expert-en-cybersecurite-des-systemes-information/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37989/>

Entrées et sorties de formation

Entrées en formation	3
Parcours menés à terme	3
Taux d'achèvement	100 %
Période	12/2025 – 03/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	4
Montant total engagé	28 660 €
Coût moyen par dossier	7 165 €
Durée moyenne	282 h
Période	10/2025 – 07/2026
France Travail	57 %
France compétences	42 %
Reste à charge titulaire	1 %

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