Cryptographe/cryptanalyste

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire crée des algorithmes, des chiffres et des systèmes de sécurité pour chiffrer les renseignements/analyse et décode les messages secrets et les systèmes de codage.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement peuvent entraîner des artefacts, des protocoles et des systèmes cryptologiques de mauvaise qualité qui mettront en péril la sécurité des systèmes/renseignements qu'ils protègent. Le fait de ne pas se tenir au courant des sciences et des technologies émergentes connexes comporte le même risque.
Parcours de perfectionnement	Il s'agit d'une activité de cybersécurité hautement spécialisée, qui est remplie par des professionnels expérimentés et instruits qui s'intéressent à ce domaine. Il existe des possibilités de spécialisation accrue et de recherche et d'études avancées dans ce domaine.
Autres titres	Aucun.
CNP connexes	2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2161 – Mathématiciens/mathématiciennes, statisticiens/statisticiennes et actuaires 2171 – Analystes et consultants/consultantes en informatique
Tâches	▪ Collaborer avec les intervenants clés pour établir un programme efficace de gestion des risques liés à la cybersécurité ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Élaborer des systèmes de protection des renseignements importants/sensibles contre l'interception, la copie, la modification ou la suppression ▪ Évaluer, analyser et cibler les faiblesses et les vulnérabilités des systèmes et des algorithmes de sécurité ▪ Créer des modèles statistiques et mathématiques pour analyser les données et résoudre les problèmes de sécurité ▪ Développer et mettre à l'essai des modèles de calcul pour en assurer la fiabilité et la précision ▪ Établir, rechercher et mettre à l'essai de nouvelles théories et applications de la cryptologie ▪ Décoder les messages cryptés et les systèmes de codage de l'organisation ▪ Développer et mettre à jour des méthodes pour le traitement efficace des processus cryptographiques ▪ Préparer des rapports techniques qui documentent les processus de sécurité ou les vulnérabilités ▪ Fournir des conseils à la direction et au personnel sur les méthodes et applications cryptiques ou mathématiques ▪ Soutenir les contre-mesures et les stratégies d'atténuation des risques contre les exploitations potentielles des vulnérabilités liées aux systèmes cryptographiques et aux algorithmes ▪ Fournir des renseignements et des conseils sur la sécurité quantique et les stratégies de résistance quantique

	▪ Soutenir la gestion des incidents et la post-analyse en cas de compromission des processus ou systèmes de chiffrement/cryptographie ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle ▪ Guider et soutenir les spécialistes du chiffrement en fonction des besoins	
Qualifications requises	Éducation	Diplôme universitaire en génie informatique, en informatique ou en mathématiques. Une maîtrise ès sciences ou un doctorat est préférable.
	Formation	Selon les besoins pour soutenir le contexte technique de l'organisation (par exemple, outils, processus et procédures locaux)
	Expérience professionnelle	En plus des diplômes universitaires, les rôles de premier échelon exigent normalement 3 à 5 ans d'expérience dans un domaine des TI/systèmes avec une bonne connaissance du chiffrement et des activités clés de gestion.
Outils et technologie	▪ Évaluation de la menace et des risques ▪ Processus de gestion de vulnérabilité et évaluations de vulnérabilité ▪ Processus et procédures de gestion des incidents (liés à la cryptographie/au chiffrement) ▪ Processus et politiques de gestion des risques en matière de cybersécurité ▪ Législation sur la protection de la vie privée et la sécurité ▪ Algorithmes, chiffres et systèmes cryptographiques ▪ Politiques et plans de gestion de clés ▪ Infrastructure de sécurité organisationnelle et systèmes de compte rendu	
Compétences	Cette profession repose sur les compétences démontrées pour un niveau de direction qui comprennent celles identifiées dans le cadre de la NICE. Application de base des CCH suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée/organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, besoins opérationnels et infrastructures techniques liés au secteur/contexte ☐ Exigences en matière de renseignements et de données, y compris la sensibilité, l'intégrité et le cycle de vie ☐ Langages de programmation informatique applicables ☐ Gestion, mesures et suivi du programme de cybersécurité Application avancée des CCH suivantes : ☐ Menaces avancées et capacités de bris de chiffrement/déchiffrement ☐ Lois, codes juridiques, règlements, politiques et éthiques applicables en matière de cybersécurité ☐ Architecture d'ordinateur, structures de données et algorithmes ☐ Algèbre linéaire/matricelle ou mathématiques discrètes	

	☐ Théorie des probabilités, théorie de l'information, théorie de la complexité et théorie des nombres ☐ Cryptographie et concepts de gestion des clés cryptographiques ☐ Principes de la cryptographie symétrique (par exemple, chiffrement symétrique, fonctions de hachage, codes d'authentification de message, etc.) ☐ Principes de la cryptographie asymétrique (chiffrement asymétrique, échange de clés, signatures numériques, etc.) ☐ Exigences en matière de réponse aux incidents pour la compromission cryptographique ☐ Rédaction du rapport technique
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités en matière de cybersécurité par rapport aux risques organisationnels en matière de cybersécurité, en particulier en ce qui concerne les exigences de chiffrement des données. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils cryptographiques sont touchés et automatisés pour répondre aux besoins organisationnels. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires pour assurer la robustesse des systèmes cryptographiques, des chiffres et des algorithmes. S'il existe des disparités connues entre la menace et la capacité de défense, des mesures d'atténuation doivent être définies et mises en œuvre. ▪ Des mécanismes visant à soutenir le niveau requis de confiance et de risque organisationnel devront être mis en place pour soutenir le suivi et la communication des résultats des outils automatisés. Par conséquent, il faudra comprendre les risques organisationnels posés, les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les acteurs de menace vont fondamentalement modifier la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences liées à la mise en œuvre d'une stratégie de sécurité quantique au sein de l'organisation. Le cryptographe/cryptanalyste jouera un rôle clé pour assurer une sécurité quantique/conception résistante et pourra participer aux essais des algorithmes, des protocoles de chiffrement et des équipements.