Développeur de la sécurité des systèmes d'information

Cadre de référence de la NICE	Fourniture sécurisée, SP-SYS-001, développeur de la sécurité des systèmes d'information
Description fonctionnelle	Le titulaire développe, crée, intègre, met à l'essai et maintient la sécurité des systèmes d'information tout au long de leur cycle de vie, et rend compte du rendement des systèmes d'information en matière de confidentialité, d'intégrité et de disponibilité, et recommande des mesures correctives pour remédier aux lacunes.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou le mauvais jugement peuvent entraîner des décisions organisationnelles qui peuvent avoir une incidence importante sur l'entreprise. L'absence d'une appréciation complète des besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face à l'évolution des menaces.
Parcours de perfectionnement	Il s'agit d'un rôle de premier échelon dans le domaine de la cybersécurité qui tire parti d'une expérience antérieure en matière de TI et de systèmes. Après une formation technique en cybersécurité, ce travail peut déboucher sur des responsabilités accrues dans les rôles d'infrastructure et l'expertise technique en matière de cybersécurité.
Autres titres	Administrateur des systèmes de sécurité des TI Technicien en systèmes de cybersécurité
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2174 – Programmeurs/programmeuses et développeurs/développeuses en médias interactifs
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 ▪ Définir et examiner les systèmes d'information d'une organisation, et veiller à ce que les exigences de sécurité tiennent compte des plans de reprise après sinistre et des fonctions de continuité des activités, y compris les exigences de reprise ou de sauvegarde pour la restauration des systèmes ▪ Analyser les systèmes de sécurité existants et formuler des recommandations de modifications ou d'améliorations ▪ Préparer des estimations des coûts et des contraintes, et repérer les problèmes d'intégration ou les risques pour l'organisation ▪ Rechercher et développer un contexte de sécurité des systèmes, et définir les exigences en matière d'assurance de la sécurité sur la base des normes de l'industrie et des politiques et pratiques en matière de cybersécurité ▪ Veiller à ce que les systèmes acquis ou développés soient conformes aux politiques et pratiques en matière de cybersécurité d'une organisation ▪ Élaborer et mener des procédures d'essais et de validation des systèmes d'information et faire rapport sur leur fonctionnalité et leur résilience ▪ Planifier et soutenir les essais de vulnérabilité et les examens de sécurité des systèmes ou réseaux d'information afin de déterminer les lacunes, et examiner les contrôles et les mesures nécessaires

	pour protéger la confidentialité et l'intégrité des renseignements dans différentes conditions de fonctionnement ▪ Mener des essais de systèmes d'information pour s'assurer que les niveaux et les procédures de sécurité sont corrects et élaborer un plan de gestion des risques de sécurité ▪ Soutenir l'élaboration de plans de reprise après sinistre et de continuité des activités pour les systèmes d'information en cours de développement ▪ Préparer des rapports techniques qui documentent le processus de développement du système et les révisions ultérieures ▪ Documenter et traiter la sécurité tout au long du cycle de vie du système ▪ Mettre à jour et améliorer les systèmes d'information, si nécessaire, pour corriger les erreurs et améliorer le rendement et les interfaces ▪ Préparer des rapports sur les correctifs ou les versions des systèmes d'information qui rendraient les réseaux ou les systèmes vulnérables ▪ Développer des contre-mesures et des stratégies d'atténuation des risques contre les exploitations potentielles des vulnérabilités des réseaux ou des systèmes ▪ Effectuer une analyse des risques chaque fois qu'un système est modifié ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle	
Qualifications requises	Éducation	Études postsecondaires dans un domaine lié à la cybernétique ou aux TI (par exemple : informatique, administration de systèmes de TI, génie informatique ou équivalent).
	Formation	Le soutien à la formation peut inclure des outils, des techniques et des pratiques de développement de systèmes de cybersécurité ainsi que la sécurité tout au long du cycle de vie du développement de système
	Expérience professionnelle	Formation et expérience antérieures en matière de développement de systèmes
Outils et technologie	▪ Plans stratégiques et d'affaires ▪ Évaluation de la menace et des risques ▪ Processus de gestion de vulnérabilité et évaluations de vulnérabilité ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des risques en matière de cybersécurité ▪ Législation sur la protection de la vie privée et la sécurité ▪ 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) ☐ Politiques, exigences et pratiques en matière de gestion des risques ☐ Planification de la continuité des activités et des interventions en cas de catastrophe ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, besoins opérationnels et infrastructures techniques liés au secteur/contexte ☐ Gestion de projet ☐ Modèles de coûts et analyse coûts-avantages ☐ Cryptographie et concepts de gestion des clés cryptographiques ☐ Gestion de l'identité et de l'accès ☐ Gestion de la vulnérabilité et planification et processus d'essais de pénétration ☐ Conceptions et fonctions de sécurité des données, méthodologies d'analyse, essais et protocoles ☐ Techniques de codage et de configuration sécurisées ☐ Gestion, mesures et suivi du programme de cybersécurité Application avancée des CCH suivantes : ☐ Normes de l'industrie et principes et méthodes d'analyse des systèmes acceptés par l'organisation ☐ Outils, méthodes et techniques de conception de systèmes ☐ Architecture d'ordinateur, structures de données et algorithmes ☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels ☐ Méthodes et processus d'essais et d'évaluation des systèmes ☐ Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données ☐ Conception de contre-mesures en fonction des risques de sécurité déterminés ☐ Configuration et utilisation d'outils de protection informatique basés sur des logiciels ☐ Considérations relatives à la conception et aux solutions matérielles et logicielles ☐ Gestion des incidents et restauration des systèmes
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités en matière de cybersécurité et des interactions entre systèmes, de l'accès et des responsabilités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications en matière de sécurité de l'option « apportez votre équipement personnel de communication » (AVEC) et de la gestion des risques associés tout au long du cycle du développement du système. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans l'infrastructure de sécurité organisationnelle. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des problèmes aux organisations qui ne disposent

	pas d'outils défensifs complémentaires. En conséquence, des stratégies d'atténuation créatives et pertinentes seront nécessaires localement, et des réponses de sécurité du système seront élaborées 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 et dans tous les systèmes qui traitent des données sensibles.