Architecte de la sécurité

Cadre de référence de la NICE	Fourniture sécurisée, SP-ARC 002, architecte de la sécurité
Description fonctionnelle	Le titulaire conçoit, développe et supervise la mise en œuvre des structures de sécurité des réseaux et des ordinateurs d'une organisation; il s'assure que les exigences de sécurité sont correctement prises en compte dans tous les aspects de l'infrastructure et que le système soutient les processus de l'organisation.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou le mauvais jugement peuvent entraîner des conceptions ou des architectures défectueuses qui peuvent échouer ou présenter des vulnérabilités exploitables qui peuvent mettre en danger les systèmes de TI sur lesquels l'organisation compte. 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	Suivant principalement des études et un parcours professionnel à partir d'un rôle d'architecte d'entreprise existant, il s'agit d'un rôle de spécialiste émergent, principalement employé dans les grandes organisations technologiques, les services ou systèmes partagés ou les fournisseurs de sécurité.
Autres titres	Architecte de la sécurité d'entreprise
CNP connexes	2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 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 ▪ Définir et examiner les technologies et les systèmes d'information d'une organisation, et veiller aux exigences de sécurité ▪ Reconnaître les plans de reprise après sinistre et les fonctions de continuité des activités appropriés, y compris les exigences de reprise ou de sauvegarde pour la restauration des systèmes ▪ Planifier, rechercher et développer des architectures de la sécurité robustes pour les systèmes et les réseaux ▪ Rechercher les technologies actuelles et émergentes pour comprendre les capacités des réseaux ou systèmes requis ▪ Préparer des estimations de coûts et cibler les problèmes d'intégration ▪ Effectuer des essais de vulnérabilité, des analyses des risques et des évaluations de la sécurité ▪ 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 et architectures acquis ou développés soient conformes aux politiques et pratiques en matière de cybersécurité d'une organisation ▪ Effectuer des examens de sécurité et repérer les lacunes ou déterminer la capacité des architectures et des conceptions de la sécurité (par exemple, pare-feu, réseaux privés virtuels, routeurs,

<table>
<tr><td></td><td colspan="2">serveurs, etc.) et élaborer un plan de gestion des risques de sécurité
▪ Préparer des rapports techniques qui documentent le processus de développement de l’architecture
▪ Documenter et traiter les besoins d’une organisation en matière de sécurité de l’information, d’architecture de cybersécurité et d’ingénierie en sécurité des systèmes tout au long du cycle de vie d’un système
▪ Donner des conseils sur les exigences de sécurité et les activités du processus de gestion des risques
▪ Soutenir la gestion des incidents et le conseil post-analyse sur les opérations de reprise
▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires en infrastructure et architecture des TI (par exemple, génie informatique, architecture des systèmes de TI)</td></tr>
<tr><td>Formation</td><td>Formation spécialisée sur les concepts, les principes et les pratiques de l’architecture de la sécurité Formation sur les outils de sécurité nécessaires au rôle de soutien</td></tr>
<tr><td>Expérience professionnelle</td><td>Une formation et une expérience antérieures en infrastructure de sécurité des TI, en analyse des besoins ou en gestion de programmes sont préférables – 5 à 10 ans d’expérience pertinente en TI pour le niveau avancé.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Plans stratégiques et d’affaires
▪ Évaluation de la menace et des risques
▪ Architectures de systèmes
▪ Outils et applications de mise en correspondance des TI
▪ 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</td></tr>
<tr><td>Compétences</td><td colspan="2">Cette profession repose sur les compétences démontrées pour un niveau de direction qui comprennent celles identifiées dans le cadre de la NICE.

Application avancée des CCH suivantes :
☐ Besoins des entreprises en matière de sécurité
☐ Exigences juridiques, politiques et de conformité
☐ 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</td></tr>
</table>

	☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet ☐ Cryptographie et concepts de gestion des clés cryptographiques ☐ Dispositifs de réseaux privés virtuels et chiffrement ☐ Concepts et pratiques d'ingénierie appliqués à la sécurité des systèmes et à l'architecture des systèmes ☐ Concepts d'architecture de la sécurité et modèles de référence pour l'architecture d'entreprise ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Méthodes d'authentification, d'autorisation et de contrôle d'accès ☐ Méthodes et processus d'essai et d'évaluation des systèmes ☐ Concepts et fonctions des systèmes de sécurité des applications ☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels ☐ Normes de l'industrie et principes et méthodes d'analyse acceptés par l'organisation ☐ Configuration et utilisation d'outils de protection informatique basés sur des logiciels ☐ Conception de solutions matérielles et logicielles ☐ Gestion, mesures et suivi du programme de cybersécurité ☐ Gestion des incidents et planification et opérations de remise en état des systèmes
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtuels ou « basés sur l'infonuagique » exigera des connaissances approfondies à l'intersection des architectures des organisations et des fournisseurs de services pour déterminer les risques liés à la cybersécurité et les gérer. ▪ 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 façon dont les contrôles de sécurité sont intégrés dans l'infrastructure organisationnelle. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans l'infrastructure et l'architecture de la sécurité générales et les implications pour le personnel, les ressources, les procédures et les politiques. ▪ 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 au niveau local seront nécessaires et devront être intégrées dans l'architecture de la sécurité. ▪ 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 pour soutenir une architecture de sécurité intégrée. ▪ 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 à son intégration dans toute l’architecture.