Ingénieur[8]/technologue en sécurité

Cela comprend les rôles suivants :

Ingénieur/technologue en chiffrement

Ingénieur/technologue en technologie opérationnelle

Cadre de référence de la NICE	Fourniture sécurisée, spécialiste en R et D, SP-TRD-001
Description fonctionnelle	Compte tenu des références, de la documentation sur la sécurité organisationnelle, des orientations en matière de sécurité des TI et des outils et des ressources nécessaires, le titulaire recherche et définit les besoins opérationnels en matière de sécurité et il veille à ce qu'ils soient pris en compte dans tous les aspects de l'ingénierie du système et dans toutes les phases du cycle de développement de système (CDS).
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou l'absence de prise en compte des exigences organisationnelles, des besoins opérationnels et des menaces peuvent entraîner une mauvaise conception des systèmes ou une mauvaise intégration des systèmes/dispositifs qui créent des vulnérabilités exploitables pouvant avoir des conséquences importantes sur les objectifs organisationnels, y compris le risque de défaillance catastrophique des systèmes.
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans dans des fonctions connexes d'ingénierie des TI, de conception de systèmes ou d'intégration de systèmes. Ce rôle nécessite souvent une formation spécialisée, des études ou une expérience correspondant aux capacités du système. Peut être employé dans des contextes généraux ou spécialisés comme la cryptographie/le chiffrement, les essais et évaluation de la sécurité ou la technologie opérationnelle (SCI/SCO/SCADA).
Autres titres	▪ Concepteur de sécurité ▪ Analyste des exigences de sécurité ▪ Ingénieur en sécurité des réseaux ▪ Technologue en ingénierie de la sécurité ▪ Ingénieur en technologie opérationnelle ▪ Ingénieur en chiffrement
CNP connexes	2133 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2171 – Analystes et consultants/consultantes en informatique 2241 – Technologues et techniciens/techniciennes en génie électronique et électrique

[8] **Remarque importante :** L'ingénierie en sécurité est un domaine naissant qui est normalement développé à partir des domaines professionnels de l'ingénierie des communications et de l'électronique, de l'ingénierie des systèmes de TI ou d'un domaine similaire. Au Canada, le terme « ingénieur » désigne un ingénieur agréé comme décrit par l'autorité locale. Par conséquent, tous les ingénieurs en sécurité doivent être autorisés à exercer la profession d'« ingénieur » dans leur sphère de compétence. Toutefois, cette NPN est destinée à traiter des normes professionnelles spécifiques en matière de cybersécurité pour ceux qui remplissent un rôle d'ingénieur en sécurité ou de technologue en ingénierie de la sécurité, étant entendu que les tâches purement techniques ne sont pas du ressort du technologue en ingénierie.

<table>
<tr><td>Tâches</td><td colspan="2">

Définir/valider les besoins opérationnels en matière de sécurité et les exigences de sécurité
Examiner et analyser les architectures et les documents de conception de la sécurité des TI/TO, ainsi que les systèmes, protocoles, services, contrôles, appareils, applications, chiffrements et algorithmes de chiffrement connexes, en fonction des exigences de sécurité et des normes de l'industrie
Créer et examiner les cas d'utilisation du système
Déterminer les menaces techniques et les vulnérabilités des systèmes
Gérer la configuration de sécurité des TI/TO
Analyser les outils et techniques de sécurité des TI/TO
Analyser les données de sécurité et fournir des conseils et des rapports
Analyser les statistiques de sécurité des TI/TO
Préparer des rapports techniques comme l'analyse des options de solutions de sécurité des TI et les plans de mise en œuvre
Fournir une vérification et une validation par un tiers (VVT) sur les projets de sécurité des TI/TO
Superviser les audits de sécurité des TI/TO
Conseiller sur la sécurité des projets de TI/TO
Fournir des conseils sur les politiques, plans et pratiques de sécurité des TI/TO
Examiner les plans des systèmes, les plans d'urgence, les plans de continuité des activités (PCA) et les plans d'intervention en cas de catastrophe (PIC)
Concevoir/créer et mener des essais et des exercices sur les protocoles de sécurité des TI/TO
Examiner, élaborer et fournir du matériel de formation

</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme d'ingénieur ou de technologue pertinent (selon les exigences organisationnelles).</td></tr>
<tr><td>Formation</td><td>Une certification valide au niveau de l'industrie dans une spécialisation connexe en cybersécurité (par exemple, sécurité des réseaux, cryptographie, intégration de systèmes, etc.)</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience modérée (3 à 5 ans) dans le domaine de la sécurité et de la conception, de l'intégration, des essais et du soutien des systèmes associés.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">

Outils et méthodologies d'évaluation de la menace et des risques
Systèmes de protection et de défense, y compris les pare-feu, les logiciels et systèmes antivirus, les systèmes de détection et de protection contre les intrusions, les scanneurs et les alarmes
Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents
Logiciels et systèmes d'authentification
Processus de gestion de vulnérabilité et systèmes d'évaluation de vulnérabilité, y compris les essais de pénétration s'ils sont utilisés
Services de sécurité fournis, le cas échéant
Outils et techniques d'essai et d'évaluation de la sécurité

</td></tr>
<tr><td>Compétences</td><td colspan="2">L'ingénieur en sécurité/le technologue en ingénierie doit avoir un niveau d'application de base des CCH suivantes, tandis que l'ingénieur en sécurité doit avoir un niveau d'application avancé des CCH suivantes :

☐ Modèles d'ingénierie de la sécurité</td></tr>
</table>

	☐ Définition et communication des approches de sécurité qui soutiennent les exigences organisationnelles ☐ Normes de sécurité internationales et conformité ☐ Concepts d'architecture de la sécurité et modèles de référence pour l'architecture d'entreprise ☐ Fonctions SDN, NFV et VNF ☐ Sécurité des systèmes pendant l'intégration et la configuration ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Méthodes et processus d'essais et d'évaluation de la sécurité ☐ Sécurité tout au long du cycle de vie de développement du système/logiciel ☐ Méthodes et applications d'évaluation de vulnérabilité et d'essais de pénétration ☐ Méthodes d'essais et d'évaluation des systèmes et des logiciels ☐ Conception de la sécurité basée sur les preuves ☐ Création et essai des modèles de menace ☐ Gestion de projet et évaluation de la sécurité tout au long du cycle de vie du projet ☐ Processus d'achat et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Offre de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et fourniture des exposés et des rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres) En outre, dans les environnements d'assurance de niveau élevé, de chiffrement et de cryptographie : ☐ Gouvernance de la sécurité dans les environnements d'assurance de niveau élevé, de chiffrement et de cryptographie ☐ Modélisation avancée des menaces et gestion des risques dans les environnements d'informations sensibles ☐ Principales politiques et pratiques de gestion (y compris la sécurité des communications [SECOM]) ☐ Normes de sécurité des émissions ☐ Zones de sécurité physique et des TI ☐ Cryptographie et chiffrement, y compris les algorithmes et les chiffres ☐ Sténographie ☐ Essai et mise en œuvre des solutions interdomaines ☐ Gestion des clés, produits de gestion des clés et cycle de vie de la certification ☐ Tactiques, techniques et procédures avancées pour les acteurs de la menace persistante et sophistiquée. ☐ Technologie de sécurité/résistance quantique ☐ Évaluation et audit des réseaux et systèmes de chiffrement/cryptographie En outre, dans les environnements de technologie opérationnelle (SCI/SCO/SCADA) : ☐ Normes de l'industrie et principes et méthodes d'analyse acceptés par l'organisation ☐ Système de contrôle : o l'architecture et les systèmes de défense o la gouvernance et la gestion dans divers environnements o les surfaces d'attaque, les menaces et les vulnérabilités o la surveillance de la sécurité, les outils et les techniques

	☐ Systèmes et protocoles de TI dans les configurations des systèmes de contrôle ☐ Intégration des systèmes de contrôle des TI et des TO ☐ Renforcement et surveillance des systèmes de contrôle des TO ☐ Évaluation de la sécurité et processus d'autorisation des systèmes de TO ☐ Planification et activités de réponse aux incidents dans les environnements des systèmes de contrôle ☐ Plans de continuité des activités et plans de reprise après sinistre et activités dans un environnement de système de contrôle
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 des services à fournir et de la manière dont ils sont intégrés dans les réseaux organisationnels. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications des politiques « apportez votre équipement personnel de communication » (AVEC). Cela signifie que, quelles que soient les capacités du dispositif, il faudra évaluer les risques posés pour l'organisation et mettre en œuvre des mesures d'atténuation au niveau de risque acceptable. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans l'organisation et les implications potentielles en matière de sécurité. Si des outils de sécurité automatisés sont utilisés, il faudra définir les exigences en matière d'essai, d'intégration et de contrôle et conseiller/former les responsables de ces activités sur les changements de processus et de procédures qui en résulteront. ▪ 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. Cela exigera des capacités de réflexion critique et abstraite bien affinées. ▪ 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 mieux comprendre les risques organisationnels posés dans l'environnement dynamique de la menace. ▪ 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.