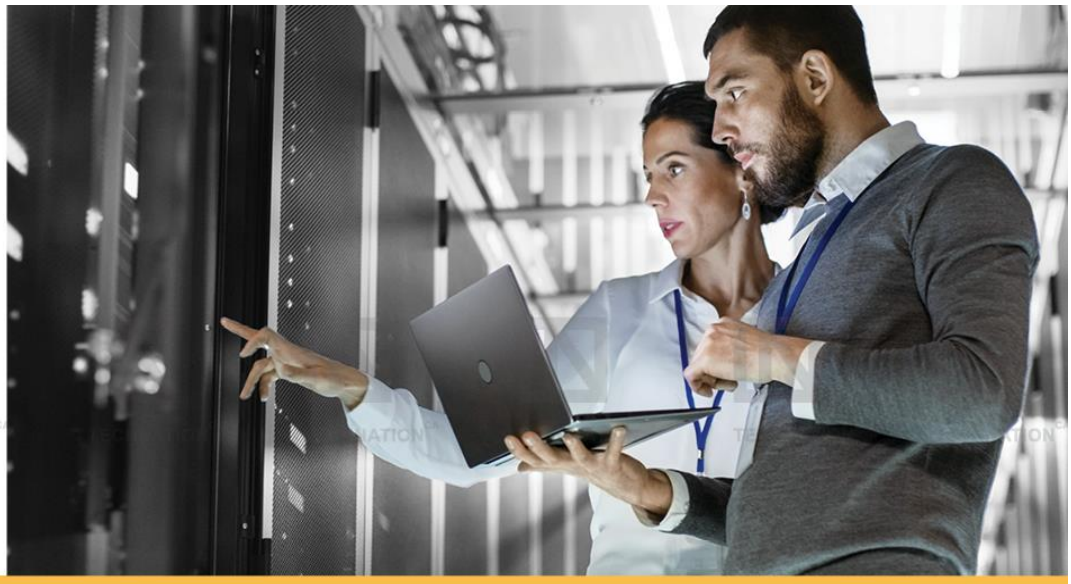

MAIN-D'ŒUVRE EN CYBERSÉCURITÉ

NORME PROFESSIONNELLE NATIONALE

Une main-d'œuvre pour sécuriser l'avenir numérique du Canada

AVRIL 2020

TECHNATION[CA]

À propos de TECHNATION

En tant qu'association nationale des entreprises du secteur des technologies de l'information et de la communication (TIC), TECHNATION soutient le développement d'une économie numérique solide et durable au Canada. Lien vital entre les entreprises et le gouvernement, nous fournissons à nos membres des services de représentation, de mise en réseau et de perfectionnement professionnel qui les aident à prospérer à l'échelle nationale et à être concurrentiels à l'échelle mondiale.

Défenderesse éminente de l'expansion de la capacité d'innovation du Canada, TECHNATION encourage l'adoption de technologies pour tirer parti des possibilités de productivité et de rendement dans tous les secteurs. En tant qu'organisation à but non lucratif dirigée par ses membres, TECHNATION a été la porte-parole nationale officielle de l'industrie des TIC, qui représente 184 milliards de dollars depuis plus de 60 ans. Plus de 39 000 entreprises canadiennes des TIC créent et fournissent des biens et services qui contribuent à une société plus productive, plus compétitive et plus innovante. Le secteur des TIC génère plus d'un million d'emplois directs et indirects et investit 6,1 milliards de dollars par an dans la R et D, soit plus que tout autre acteur du secteur privé.

Remerciements

L'alliance de talents en cybersécurité

TECHNATION souhaite féliciter et reconnaître les membres de l'alliance de talents en cybersécurité pour son leadership, sa supervision et ses idées au cours du processus de développement de la norme professionnelle nationale (NPN).

Professionnels de l'industrie de la cybersécurité

TECHNATION souhaite également exprimer sa sincère gratitude aux professionnels et aux parties prenantes de la cybersécurité qui ont contribué directement ou indirectement à l'élaboration de cette norme par l'intermédiaire d'entretiens, de sondages, de consultations et de discussions informelles. Bien qu'ils soient trop nombreux pour les mentionner individuellement, nous apprécions sincèrement l'intérêt et l'expertise que les membres engagés de la communauté de cybersécurité ont apportés tout au long de ce projet. Leurs points de vue et leurs perspectives ont été essentiels pour les résultats. Nous les remercions d'avoir partagé avec nous leur temps, leurs connaissances, leurs recherches et leurs expériences. Nous attendons également avec impatience leurs futures contributions au processus de révision afin que cette NPN reste actuelle et pertinente.

Le Centre canadien pour la cybersécurité

Le Centre canadien pour la cybersécurité mérite une reconnaissance particulière pour son expertise et son rôle de chef de file avec son Guide du programme d'études en cybersécurité qui a permis de définir le cadre des travaux sur la cybersécurité au Canada et les rôles de travail utilisés dans cette norme. En outre, nous travaillerons avec le Centre canadien pour la cybersécurité pour assurer une étroite harmonisation entre nos documents d'orientation.

La National Initiative on Cybersecurity Education (NICE) des États-Unis

Le bureau américain de la NICE, faisant partie du National Institute of Standards and Technology (NIST), a apporté à TECHNATION son soutien et ses conseils tout au long de ce processus et nous apprécions son travail approfondi sur son cadre de perfectionnement de la main-d'œuvre (Cybersecurity Workforce Framework) en cybersécurité, sur lequel s'est basé le cadre des compétences en matière de cybersécurité au Canada. De même, la NICE américaine a fourni des descriptions détaillées et rigoureuses des catégories d'emploi, des domaines de spécialisation et des rôles de travail en cybersécurité, ce qui a fortement influencé le contenu de ce document. Nous nous réjouissons de travailler plus étroitement avec le bureau de la NICE pour définir et affiner notre compréhension de ce nouveau domaine de travail et nous continuerons à contribuer au processus de révision de la NICE.

Gouvernement du Canada

Ce projet est financé en partie par le Programme d'appui aux initiatives sectorielles du gouvernement du Canada. Les opinions et interprétations contenues dans cette publication sont celles de l'auteur et ne reflètent pas nécessairement celles du gouvernement du Canada.

Canada

Table des matières

Introduction

Objectif

L'objectif de ce document est de décrire les normes professionnelles nationales pour l'emploi de base en cybersécurité pour le marché du travail canadien.

La cybersécurité – Un domaine de travail émergent et durable

La cybersécurité est définie comme « la protection de l'information numérique et de l'infrastructure qui héberge cette information ».[1] Toutefois, bien qu'Internet et l'informatique connectée existent depuis plus de deux décennies, la cybersécurité reste un domaine de travail émergent et en pleine évolution. En tant que tel, le travail n'a pas été bien défini en termes professionnels et l'emploi en cybersécurité est souvent confondu avec d'autres rôles organisationnels. En conséquence, la NPN définit l'emploi en cybersécurité primaire comme distinct des autres professions dans les technologies de l'information, la sécurité, la gestion des affaires ou l'administration publique. Toutefois, la cybersécurité ne se limite pas aux systèmes techniques; elle concerne également les personnes, leur comportement et la manière dont elles se connectent et s'engagent dans ces systèmes.

La valeur d'une cybersécurité efficace et des services et produits soutenus par le professionnel de la cybersécurité ne peut être sous-estimée. L'emploi en cybersécurité devient visible dans le monde entier comme une carrière essentielle et durable au sein de l'économie numérique. Au Canada, par exemple :

- Notre dépendance à l'égard des systèmes d'information et de données a augmenté de manière exponentielle au cours de la dernière décennie, alors que les organisations numérisent leurs activités et passent à une présence en ligne. Cela nécessite des professionnels capables de concevoir, de construire, de mettre en œuvre et de maintenir des systèmes d'information sûrs, sécurisés et fiables, capables de répondre à toute une série de besoins commerciaux, opérationnels et professionnels.
- Les citoyens canadiens sont de plus en plus conscients de leur droit à la vie privée et sont de plus en plus préoccupés par la manière dont leurs données personnelles sont protégées par les organisations. Cela nécessite des experts en cybersécurité et en protection de la vie privée qui peuvent donner des conseils sur les différentes normes nationales et internationales, élaborer des politiques, déterminer les besoins, intégrer en toute sécurité les systèmes et les logiciels, et soutenir la surveillance pour mieux protéger la vie privée des Canadiens.
- La cybercriminalité est une menace toujours croissante. La technologie étant soit une cible pouvant être exploitée, soit un outil pouvant être utilisé pour commettre d'autres actes criminels comme le vol, la fraude, le harcèlement sexuel et l'exploitation des enfants, la cybersécurité et la sécurité en ligne qui y est associée sont essentielles pour protéger les Canadiens. Cela nécessite une expertise pour aider à déterminer et

[1] Sécurité publique Canada (2019), Stratégie nationale de cybersécurité : Vision du canada pour la sécurité et la prospérité dans l'ère numérique, consultée le 3 avril 2020, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx#s11

détecter les cybermenaces, et y répondre, ainsi que pour aider ceux qui enquêtent et collectent des preuves numériques pouvant être utilisées pour améliorer les protections et, le cas échéant, poursuivre les contrevenants.

Notre expérience récente de la crise de la COVID-19 a amplifié le besoin de cybersécurité dans tous les secteurs. Bien qu'ils travaillent souvent en coulisses, les professionnels de la cybersécurité au Canada ont aidé des organisations à se mettre rapidement en place et à passer à des environnements virtuels sécurisés, ont assuré la sécurité de systèmes d'information sur la santé et de chaînes d'approvisionnement essentiels, ont contribué à la protection et à la défense d'autres systèmes importants pour le Canada et les Canadiens, et ont soutenu la sécurité et la sûreté en ligne de millions de Canadiens qui, chaque jour, affluent vers des systèmes et des applications Internet pour communiquer avec leur famille, leurs amis, leurs enseignants et leurs collègues.

La cybersécurité ne concerne pas seulement les systèmes, mais aussi les personnes qui se connectent à ces systèmes. Elle continuera d'être nécessaire dans un large éventail de technologies, et les personnes employées dans ce domaine émergent ont des possibilités de carrière importantes et durables qui peuvent avoir une incidence positive sur la vie des Canadiens connectés et soutenir l'avenir de l'économie numérique.

Champ d'application

Pour cette publication, la cybersécurité englobe la sécurité des TI, la sécurité de l'information qui implique des artefacts numériques et la sécurité numérique. La cybersécurité comporte des éléments inhérents à la sécurité physique, du personnel, des projets et contrats, qui sont déterminés en fonction de leur rôle. La cybersécurité étant un domaine très dynamique, les détails qui dépendent de technologies ou de techniques spécifiques ont été exclus.

Bien qu'il existe plusieurs autres rôles de soutien ou rôles adjacents en matière de cybersécurité, comme on le remarque dans le cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité (CWF) de la National Initiative on Cybersecurity Education (NICE) du National Institute of Standards and Technology (NIST) des États-Unis, le présent document se concentre sur les rôles **essentiels** en matière de cybersécurité et les compétences connexes qui se situent dans le contexte plus large des entreprises canadiennes où la majorité de leur travail est liée aux objectifs et aux résultats organisationnels en matière de cybersécurité.

Une note spéciale sur les éducateurs

Le rôle précieux que jouent les éducateurs dans le domaine de la cybersécurité est remarqué. Comme les éducateurs ont leur propre Classification nationale des professions (CNP) [4121, 4122, 4131] et un vaste réseau de normes professionnelles, il n'est pas nécessaire de réitérer ces renseignements dans le cadre de cette NPN. Il est à noter, cependant, que pour chaque rôle au sein de cette NPN, des éducateurs qualifiés sont requis, qui ont une expérience pertinente et la capacité de faciliter et d'évaluer l'apprentissage requis pour soutenir la demande de l'industrie.

Normes professionnelles nationales

Que sont les normes professionnelles?

Les normes professionnelles décrivent ce qu'une personne exerçant une profession particulière doit savoir et doit pouvoir faire pour être jugée « compétente » dans cette profession. Ces normes sont définies en matière de compétences, y compris les connaissances, compétences et habiletés (CCH), requises pour effectuer le travail correspondant de manière efficace, sûre et adéquate. Les normes professionnelles peuvent également inclure d'autres exigences externes, ou être influencées par ces dernières, comme la conformité à la loi ou aux politiques.

Pourquoi a-t-on besoin de normes professionnelles nationales (NPN)?

Les normes professionnelles décrivent les normes de comportement compétent et sécuritaire dans un domaine de travail spécifique. Les normes professionnelles peuvent servir à différentes fins. Elles sont souvent utilisées pour guider ce qui suit :

- Stratégies d'attraction et de recrutement
- Sélection et critères de promotion ou de mutation professionnelle
- Développement de l'éducation et de la formation
- Rédaction des descriptions de poste
- Apprentissage et perfectionnement des employés

Cette NPN soutient une variété de fonctions pour les praticiens de la cybersécurité, les employeurs, les éducateurs et les autres intervenants du perfectionnement de la main-d'œuvre comme le gouvernement, les associations professionnelles, les conseils sectoriels, les centres d'emploi, etc. (figure 1).

Dans le cas de la cybersécurité, elle sert un autre objectif. Comme nous l'avons vu, la cybersécurité est un domaine de travail relativement nouveau et émergent dans lequel divers rôles ont été confondus. En conséquence, cette NPN fournit une taxonomie indispensable de l'emploi en cybersécurité et le définit comme distinct d'autres professions notamment les technologies de l'information, la sécurité, la gestion des affaires ou l'administration publique.

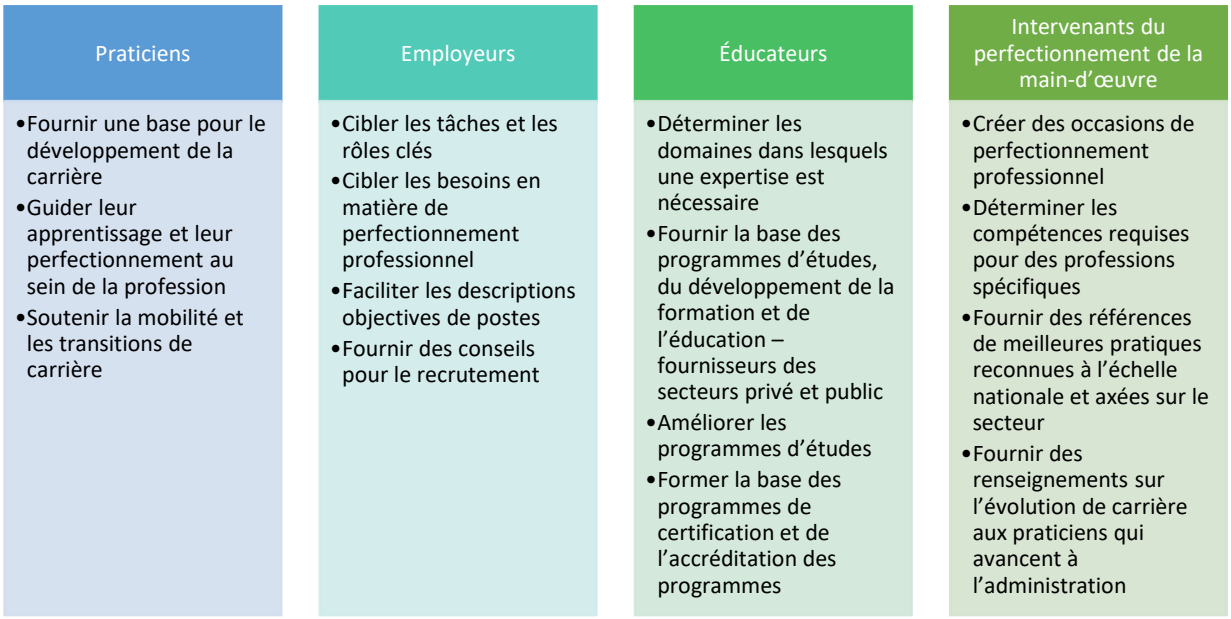

Figure 1 : Utilisations des NPN

Élaboration des NPN

Ces normes professionnelles nationales ont été élaborées à l'aide d'une combinaison de méthodologies standard de l'industrie. Celle-ci comprenait une analyse documentaire, des analyses fonctionnelles et professionnelles, des entretiens avec des experts et des processus de validation centrés sur la communauté qui incluent des praticiens, des éducateurs, des employeurs et des intervenants du perfectionnement de la main-d'œuvre.

Cadre des normes professionnelles nationales et exigences du marché du travail canadien

La NICE a élaboré un cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité (CWF). Ce cadre a établi sept domaines de spécialité et 52 rôles de travail au sein de la cybersécurité. En conjonction avec des recherches et des consultations sur le marché du travail canadien en cybersécurité, le modèle de la NICE a été affiné pour se concentrer sur quatre domaines de travail fonctionnels clés (figure 2). De plus, plutôt qu'un modèle centré sur la « cybersécurité », ce modèle soutient une optique orientée vers les entreprises et situe la cybersécurité dans le contexte plus large de la sécurité organisationnelle.

À l'exclusion de cela, un très faible pourcentage des rôles de spécialistes en cybersécurité sont définis et exercés dans des contextes gouvernementaux de sécurité nationale, de maintien de l'ordre ou militaires.[2] Ces rôles sont essentiels pour assurer la sécurité et la protection des Canadiens, même s'ils ont tendance à se situer en dehors du marché du travail général. Bien qu'ils puissent recevoir une formation de base par l'intermédiaire de

[2] Dans la zone ombrée en gris moyen de la figure 2, les rôles sont les suivants : enquête, analyse, collecte et exploitation.

fournisseurs de formation et d'éducation des secteurs privé et public, ils ont besoin d'une formation beaucoup plus importante pour soutenir des compétences spécifiques, des outils et des processus spécialisés et des mandats uniques. En général, les normes seront définies par les organisations fédérales qui soutiennent ces rôles. En conséquence, ils sont inclus dans le cadre des compétences en matière de cybersécurité, mais n'en constituent pas le point central. En outre, ces rôles et les connaissances, compétences et habiletés (CCH) associées sont bien définis dans le cadre de la NICE dans les domaines de spécialité suivants : enquête, analyse et collecte et exploitation. On en trouvera un résumé à l'annexe B et plus de détails sont accessibles sur le site Web de la NICE.

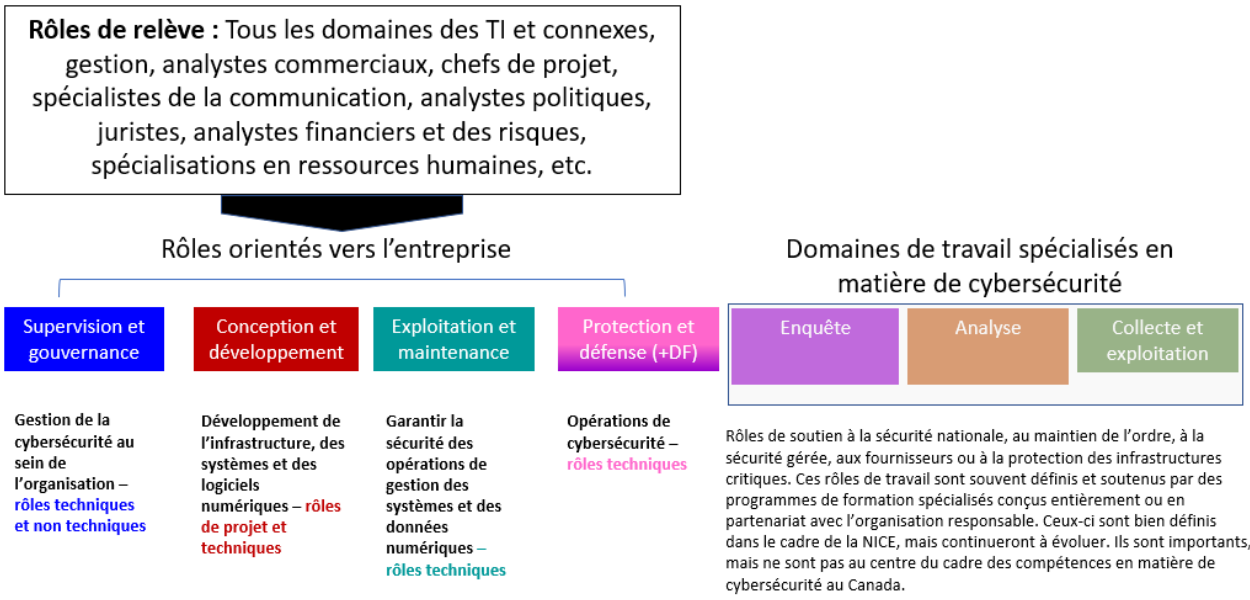

Figure 2 : Cadre des compétences en matière de cybersécurité au Canada

Rôles essentiels en matière de cybersécurité

Reconnaissant que la cybersécurité est une responsabilité partagée, cette NPN décrit la profession en cybersécurité en matière de travail qui est généralement effectué à plein temps et qui requiert des connaissances, des compétences et des habiletés uniques par rapport à d'autres professions. De plus, conformément au cadre des compétences en matière de cybersécurité au Canada évoqué plus haut, la profession en cybersécurité est définie plus précisément sous forme de titres/rôles professionnels qui sont pertinents pour le marché du travail canadien et le monde des affaires en général dans quatre grandes catégories d'emploi en cybersécurité : Supervision et gouvernance, conception et développement, exploitation et maintenance, et protection et défense. Ces catégories de travail sont alignées sur le cadre de la NICE; les rôles de travail inhérents sont définis plus en détail à l'annexe A.

Rôles adjacents à la cybersécurité

Il existe également de nombreux rôles associés à d'autres fonctions organisationnelles qui contribuent généralement aux résultats organisationnels en matière de cybersécurité à temps partiel ou de manière ponctuelle, et qui les soutiennent. Il s'agit de rôles **adjacents** à la cybersécurité où certaines connaissances, compétences et habiletés en matière de cybersécurité sont requises, mais qui ne font pas partie de la profession en cybersécurité.[3] Les rôles adjacents sont ceux de cadres, de gestionnaires de programme, d'analystes politiques, d'analystes financiers, de spécialistes de la communication, d'architectes d'entreprise, de techniciens en TI, etc., qui peuvent avoir des responsabilités en matière de cybersécurité, mais qui n'ont pas de fonctions de cybersécurité à plein temps. Ces rôles sont énumérés à l'annexe C.

Normes professionnelles nationales en matière de cybersécurité et la CNP

Selon la définition de la CNP[4], une profession est définie comme un ensemble d'emplois suffisamment similaires dans le travail effectué. La profession comme elle a été définie précédemment comprend des rôles essentiels en matière de cybersécurité. Pour les besoins du présent document, la profession est donc la cybersécurité, et elle comprend les principaux rôles de l'emploi en cybersécurité, comme définis dans la présente NPN. La profession et ces rôles sont distincts au sein du cadre professionnel national canadien et sont « en demande » sur le marché du travail canadien. Toutes les professions sont également employées dans le secteur public et privé. Veuillez noter que cela inclut les activités de cybersécurité et d'infrastructure qui se déroulent dans les environnements de sécurité, de renseignement, militaires et de maintien de l'ordre. Cela n'inclut pas, cependant, la politique opérationnelle, l'analyse opérationnelle ou les capacités de conception/développement, qui sont largement prescrites en interne et traitées au sein de ces organisations.

Pertinence par rapport à la Classification nationale des professions (CNP) – En ce qui concerne le système de la CNP, la majorité des rôles de travail dans le domaine de la cybersécurité relèvent des niveaux de compétence A ou B nécessitant une formation universitaire ou collégiale, bien que certains rôles puissent être soutenus par le niveau de compétence C nécessitant des études secondaires avec une formation professionnelle spécifique. La cybersécurité est un domaine de travail qui est influencé par tous les *types de compétences*[5] et qui a une incidence sur celles-ci, mais qui relève largement du domaine technique et est associée au *type de compétences 2* – Sciences naturelles et appliquées – et

[3] Certaines professions ou certains rôles peuvent être employés à plein temps dans le domaine de la cybersécurité et sont considérés comme des spécialistes, comme ceux qui travaillent dans le domaine du droit, de la vie privée ou de l'éthique liés à la cybersécurité. Comme ils exercent déjà une autre profession et ne font pas souvent partie de la main-d'œuvre d'une organisation, ils ne sont pas représentés dans cette NPN. Ils sont toutefois représentés dans le cadre de la NICE.

[4] Canada (2020), FAQ de la Classification nationale des professions, extraite le 19 mars 2020 de https://noc.esdc.gc.ca/Accueil/FoireAuxQuestions/c39deb7c02464ca59b2f1b58cebda69e?GoCTemplateCulture=fr-CA

[5] Le type de compétence de la CNP détermine l'industrie de la profession

est étroitement liée aux professionnels de l'informatique et des systèmes d'information et aux professions techniques dans le domaine de l'informatique et des systèmes d'information.

Examen et révision

Comme le domaine de la cybersécurité est très dynamique, cette NPN sera revue chaque année par l'alliance des talents pour la cybersécurité (ATC) et les intervenants du perfectionnement de la main-d'œuvre. Au fur et à mesure de l'introduction des modifications de la NPN, tout changement substantiel sera publié dans l'année suivant l'examen. En conséquence, toutes les propositions de modification de cette NPN doivent être adressées à info_CTA@technationcanada.ca.

Utilisation et disposition

La figure 3 présente la disposition de chacune des NPN contenues dans ce document. Bien que la majorité des NPN soient définies par une fonction spécifique, la tendance est d'aller au-delà des connaissances et des listes de compétences spécifiques et d'inclure les compétences qui comprennent également les habiletés et autres caractéristiques qui sous-tendent un rendement efficace. Par exemple, pour un praticien de la sécurité, il existe certaines habiletés comme la pensée critique, le jugement et l'intégrité qui ne sont pas prises en compte dans les connaissances traditionnelles et les analyses des emplois ou des tâches basées sur les compétences. En conséquence, cette NPN comprend des renseignements basés sur les compétences, comme indiqué à la figure 3. Il est à noter qu'en raison de l'adoption relativement récente de la cybersécurité comme domaine de travail, des renseignements supplémentaires ont été fournis dans chaque norme, qui profiteront aux utilisateurs potentiels, notamment l'évaluation fondée sur les risques liés au rôle, les parcours de perfectionnement communs et les tendances futures qui auront des répercussions sur les compétences clés.

Titre de profession

Cadre de référence de la NICE	Titre, catégorie de travail et ID du rôle de travail de la NICE
Description fonctionnelle et champ d'application	Brève description de la profession couverte
Conséquence des erreurs ou risque	Détermination des principaux risques
Parcours de perfectionnement commun	Description des rôles de travail/expériences professionnelles antérieurs et des rôles potentiels au-delà de la profession actuelle
Autres titres	Autres titres de postes
CNP connexes	Code(s) et titre(s) de Classification nationale des professions connexes
Tâches principales	Cette section définit les tâches communes associées à la profession. Les tâches importantes ou complexes peuvent être

	subdivisées en sous-tâches. Les tâches sont des activités distinctes, observables et mesurables qui ont un début et une fin.	
Qualifications requises	Éducation	Exigences en matière d'enseignement postsecondaire
	Formation	Exigences formelles de formation et de certification.
	Expérience professionnelle	Expérience générale pour soutenir l'apprentissage et la préparation aux tâches professionnelles.
Outils et technologie	Outils et technologies organisationnels communs qui soutiennent le rendement professionnel.	
Compétences clés	Connaissances, compétences, habiletés (CCH) et autres caractéristiques qui sous-tendent un rendement efficace dans la profession. Pour faciliter l'utilisation, les compétences sont regroupées et les principales CCH sont fournies à un niveau d'application de base ou avancé.	
Tendances futures ayant une incidence sur les compétences clés	Évaluation prospective de l'implication des tendances en matière de processus, personnes ou technologies qui auront une incidence sur les futures exigences professionnelles.	

Figure 3 : Définitions de la disposition et des sections de la NPN

Note sur les petites et moyennes organisations (PMO)

Si certaines PMO[6] ont des employés qui se consacrent à plein temps à la cybersécurité, la majorité d'entre elles n'en ont pas. L'expertise et les services en matière de cybersécurité sont souvent externalisés, tandis que d'autres peuvent confier certaines responsabilités en matière de cybersécurité à des personnes au sein de leur organisation. Dans les deux cas, on s'appuie de plus en plus sur les personnes occupant des *rôles adjacents* à la cybersécurité pour s'assurer que les besoins organisationnels en matière de cybersécurité sont satisfaits. Il peut s'agir, par exemple, d'un directeur de l'informatique, d'un gestionnaire en TI ou d'un analyste commercial qui en l'absence d'un spécialiste en cybersécurité a une responsabilité accrue pour assurer une cybersécurité efficace au sein de son organisation. Décrit comme un « généraliste de la cybersécurité », un compte rendu plus détaillé de ces responsabilités et compétences clés en matière de cybersécurité est fourni à l'annexe D.

[6] Cela comprend les petites et moyennes entreprises (PME) ainsi que d'autres types d'entreprises non commerciales.

Annexe A – Rôles essentiels en matière de cybersécurité

Les rôles essentiels en matière de cybersécurité sont divisés en principales catégories de travail ou en sous-groupes professionnels similaires à ceux établis dans la NICE[7] :

- **Supervision et gouvernance –** La responsabilité principale de ce sous-groupe professionnel est la direction et la gestion du programme de cybersécurité. Cela comprend les rôles techniques et non techniques.
- **Conception et développement (Fourniture sécurisée dans la NICE)** – Ce sous-groupe professionnel soutient la conception et le développement de l'infrastructure, des systèmes et des logiciels numériques. Cela comprend des rôles essentiellement techniques.
- **Exploitation et maintenance** – La principale responsabilité de ce sous-groupe professionnel est d'assurer la sécurité de l'exploitation des systèmes numériques et de la gestion des données. Tous les rôles au sein de ce sous-groupe sont des rôles techniques.
- **Protection et défense** – Ce sous-groupe professionnel est axé sur les opérations de cybersécurité. Tous les rôles au sein de ce sous-groupe professionnel sont des rôles techniques.

Compétences communes (bases professionnelles de la cybersécurité)

Pour tous les rôles essentiels en matière de cybersécurité, quel que soit le domaine d'activité ou la catégorie de travail, il existe un certain nombre de compétences communes qui sont appliquées au niveau de base, intermédiaire ou avancé selon le rôle. Tous les professionnels de la cybersécurité, quel que soit leur rôle, devraient avoir une **capacité de base à appliquer** les éléments suivants dans leur domaine/contexte de travail :

- Systèmes de TI et réseaux
- Architecture et modèles de systèmes
- Protocoles, systèmes et dispositifs Internet
- Bases de la cybersécurité
    - Cadre de sécurité intégrée
    - Stratégies et approches en matière de cybersécurité
    - Contexte des cybermenaces et exposition aux menaces communes (personnel, physique, TI/logique, chaîne d'approvisionnement)
    - Processus et sources de renseignements sur les cybermenaces
    - Analyse de la cybersécurité
    - Politiques, processus et meilleures pratiques en matière de gestion de la cybersécurité
    - Systèmes, outils et applications de cybersécurité
    - Législation et conformité (par exemple, respect de la vie privée, échange de renseignements, création de rapports, normes obligatoires, etc.)
    - Normes nationales et industrielles
- Résolution de problèmes et réflexion complexe dans des environnements dynamiques

[7] Il est à noter que les catégories de travail « Enquête », « Analyse » et « Collecte et exploitation » ne sont résumées que dans le présent document, car elles sont entièrement définies dans le cadre de la NICE et relèvent généralement de la responsabilité des professions militaires et policières.

- Maintien d’une plus grande conscience de la situation en matière de sécurité
- Conscience de soi concernant les connaissances, les compétences et les habiletés requises pour répondre aux changements commerciaux, techniques et aux menaces
- Apprentissage continu pour soutenir l’actualisation des connaissances sur les menaces émergentes, les innovations technologiques en matière de sécurité et l’évolution du paysage de la cybersécurité
- Communications (orales et verbales) adaptées au contexte organisationnel, y compris la rédaction et l’écriture de rapports techniques
- Réflexion stratégique et sens des affaires pour comprendre le contexte commercial et les risques liés à la cybersécurité
- Travail d’équipe/collaboration avec d’autres personnes, y compris des professionnels non spécialisés dans la cybersécurité
- Intégrité professionnelle
- Éthique et responsabilités professionnelles
- Formation et sensibilisation à la cybersécurité dans leur domaine

Supervision et gouvernance

La responsabilité principale de cette catégorie de travail est la direction et la gestion du programme de cybersécurité pour l'organisation. La majorité du travail au sein de ce sous-groupe professionnel est effectuée par des personnes appartenant à des groupes de compétences professionnelles reconnus, comme les cadres (cadres supérieurs, cadres intermédiaires) et les professions commerciales, financières et administratives (par exemple, analystes commerciaux, analystes financiers, analystes de risques, communications). Par conséquent, de nombreux rôles de travail pertinents dans cette catégorie sont des rôles adjacents comme la politique, la communication, la formation et la sensibilisation, qui sont définis à l'annexe C. Les principaux rôles de travail dans ce domaine d'activité/cette catégorie de travail sont les suivants :

- Responsable de la sécurité de l'information (RSI)
- Agent de sécurité des systèmes d'information
- Auditeur de la sécurité de l'information

Pour le domaine d'activité/la catégorie de travail Supervision et gouvernance, ils auront généralement besoin de capacités avancées en matière de planification organisationnelle, de mesure et de gestion de la cybersécurité.

Responsable de la sécurité de l'information (RSI)

Cadre de référence de la NICE	Supervision et gouvernance, OV-EXL-001, leadership exécutif en matière de cybersécurité
Description fonctionnelle	Un rôle de niveau exécutif avec responsabilité et obligation de rendre compte des activités de l'organisation en matière de sécurité numérique et de l'information. Cela comprend la planification, la supervision et la gestion de l'élaboration et de la mise en œuvre de la stratégie, les opérations de cybersécurité, ainsi que le budget et les ressources qui assurent la protection des ressources d'information de l'entreprise tout au long de la chaîne d'approvisionnement. Employé dans les secteurs public et privé.
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	On considère souvent qu'il s'agit là de l'apogée d'une carrière dans la cybersécurité au sein d'une organisation donnée. Un RSI a souvent une vaste expérience (plus de 10 ans) en TI ou en systèmes, de préférence avec une expérience de la gestion de la cybersécurité. Puisqu'il s'agit d'un poste de cadre, le parcours comprend également le perfectionnement des compétences, y compris la formation, l'éducation et l'expérience en dehors du domaine technique.
Autres titres	▪ Chef de la sécurité ▪ Agent de sécurité du ministère ▪ Directeur de la sécurité de l'information Remarque : selon la taille de l'organisation et la dépendance à l'égard des technologies de l'information, ce rôle professionnel peut être subsumé dans les responsabilités du directeur de l'informatique, du directeur de la technologie, du directeur de la résilience ou d'un rôle similaire.
CNP connexes	0012 – Cadres supérieurs/cadres supérieures – administration publique 0013 – Cadres supérieurs/cadres supérieures – services financiers, communications et autres services aux entreprises
Tâches	▪ Collaborer avec les intervenants clés pour planifier et établir un programme efficace de gestion des risques liés à la cybersécurité ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Élaborer et mettre en œuvre des plans stratégiques alignés sur les objectifs organisationnels et les exigences de sécurité ▪ Diriger et approuver la conception des systèmes de cybersécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour soutenir les objectifs de cybersécurité ▪ Conseiller d'autres cadres supérieurs sur les programmes, politiques, processus, systèmes et éléments de cybersécurité ▪ Assurer l'élaboration et la mise en œuvre de contrôles de sécurité pour soutenir les objectifs organisationnels ▪ Examiner, approuver et superviser le suivi des politiques et des contrôles en matière de cybersécurité

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

- Veiller à ce que des plans de réponse aux incidents, de reprise après sinistre et de continuité des activités soient mis en place et mis à l'essai
- Rédiger le mandat, superviser et examiner les enquêtes de cybersécurité
- Maintenir une compréhension actuelle du contexte des cybermenaces pour les entreprises
- Programmer et superviser les évaluations et les audits de sécurité
- Superviser et gérer les relations avec les fournisseurs de produits et services de sécurité des TI acquis
- Former et encadrer les membres de l'équipe de sécurité
- Superviser ou gérer les mesures préventives ou correctives lorsqu'un incident ou une vulnérabilité en matière de cybersécurité est découvert

</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Baccalauréat en informatique ou dans une discipline connexe ou formation et expérience équivalentes.</td></tr>
<tr><td>Formation</td><td>Une formation en fonction des rôles pour soutenir la gestion de la sécurité au niveau supérieur est préférable.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience significative (5 à 10 ans) dans le domaine des TI avec 3 à 5 ans d'expérience dans des rôles de gestion de la cybersécurité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">

- 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

</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 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
- ☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet
- ☐ Vulnérabilité et intégrité de la chaîne d'approvisionnement

Application avancée des CCH suivantes :

- ☐ Menaces et vulnérabilités organisationnelles, y compris :
- ☐ Situation de la menace à la cybersécurité

</td></tr>
</table>

	☐ Exigences en matière de gestion de vulnérabilité et gamme des mesures d'atténuation potentielles disponibles lorsqu'il n'existe pas de protocole de gestion de vulnérabilité ☐ Infrastructure de sécurité organisationnelle, y compris les systèmes de protection et de défense ☐ Élaboration, mise en œuvre et allocation des ressources, du personnel et des technologies pour répondre aux objectifs de sécurité organisationnelle ☐ Détermination des besoins et élaboration des politiques et des procédures de gestion de la cybersécurité et des risques en matière de cybersécurité ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) ☐ Communications organisationnelles, communications publiques et communications en cas de crise ☐ Gestion, mesures et suivi du programme de cybersécurité
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 tant que principal conseiller en sécurité auprès de la direction générale, cette discussion sera menée par le RSI; il est donc nécessaire d'avoir une appréciation complète des risques opérationnels. ▪ 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. ▪ 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 et les implications pour le personnel, les ressources, les procédures et les politiques. Il faudra l'intégrer dans une stratégie de sécurité et un plan d'action pour l'organisation. ▪ 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. ▪ 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. Les mesures devront également tenir compte des contraintes et des solutions de rechange organisationnelles. ▪ 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 avancées liées à la mise en œuvre d'une stratégie de sécurité quantique et aux processus de soutien au sein de l'organisation.

Agent de sécurité des systèmes d'information (ASSI)

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Il s'agit d'un rôle de gestion ponctuel au sein de la cybersécurité qui consiste principalement à surveiller la sécurité des systèmes d'information dans un ministère, une direction ou une organisation et à signaler tout problème. Ce rôle est principalement responsable de la planification locale et de la gestion de la sécurité du ou des systèmes sur lesquels il a été investi d'une autorité. Ce rôle peut relever directement ou indirectement du RSI ou d'une autre autorité (par exemple, l'agent de sécurité d'entreprise ou le directeur de l'informatique ou son délégué).
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou le mauvais jugement pourraient entraîner des décisions ou des mesures susceptibles de compromettre la sécurité du système sur lequel l'ASSI a autorité. Selon le système, cela pourrait 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 généralement d'un rôle à temps partiel attribué à une personne, ou assumé par celle-ci, ayant une certaine expérience technique, mais qui n'est généralement pas une « professionnelle de la cybersécurité ». Dans les petites et moyennes organisations, ce rôle peut également être celui d'un gestionnaire en TI ou d'un cadre supérieur ayant une certaine expérience technique ou en matière de sécurité.
Autres titres	▪ Chef de la sécurité ▪ Agent de sécurité du ministère ▪ Directeur de la sécurité de l'information Remarque : selon la taille de l'organisation et la dépendance à l'égard des technologies de l'information, ce rôle professionnel peut être subsumé dans les responsabilités du directeur de l'informatique, du directeur de la technologie, du directeur de la résilience ou d'un rôle similaire.
CNP connexes	0213 – Gestionnaires des systèmes informatiques
Tâches	▪ Collaborer avec les intervenants clés pour planifier et établir un programme efficace de gestion des risques liés à la cybersécurité ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Élaborer et mettre en œuvre des plans stratégiques alignés sur les objectifs organisationnels et les exigences de sécurité ▪ Diriger et approuver la conception des systèmes de cybersécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour soutenir les objectifs de cybersécurité ▪ Conseiller d'autres cadres supérieurs sur les programmes, politiques, processus, systèmes et éléments de cybersécurité ▪ Assurer l'élaboration et la mise en œuvre de contrôles de sécurité pour soutenir les objectifs organisationnels ▪ Examiner, approuver et superviser le suivi des politiques et des contrôles en matière de cybersécurité

<table>
<tr><td></td><td colspan="2">Veiller à ce que des plans de réponse aux incidents, de reprise après sinistre et de continuité des activités soient mis en place et mis à l'essai
Rédiger le mandat, superviser et examiner les enquêtes de cybersécurité
Maintenir une compréhension actuelle du contexte des cybermenaces pour les entreprises
Programmer et superviser les évaluations et les audits de sécurité
Superviser et gérer les relations avec les fournisseurs de produits et services de sécurité des TI acquis
Superviser ou gérer les mesures préventives ou correctives lorsqu'un incident ou une vulnérabilité en matière de cybersécurité est découvert</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires dans un domaine lié à la cybernétique ou aux TI (par exemple : génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent)</td></tr>
<tr><td>Formation</td><td>Pour soutenir le rôle, par exemple, de gestion de l'équipe de cybersécurité, la gestion des incidents et la planification de la cybersécurité seraient un atout.</td></tr>
<tr><td>Expérience professionnelle</td><td>3 à 5 ans d'expérience dans le domaine des TI avec une certaine expérience de la gestion.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">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</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 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
☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet
☐ Vulnérabilité et intégrité de la chaîne d'approvisionnement

Application avancée des CCH suivantes :
☐ Menaces et vulnérabilités organisationnelles, y compris :
o Situation de la menace à la cybersécurité</td></tr>
</table>

	○ Exigences en matière de gestion de vulnérabilité et gamme des mesures d'atténuation potentielles disponibles lorsqu'il n'existe pas de protocole de gestion de vulnérabilité ○ Infrastructure de sécurité organisationnelle, y compris les systèmes de protection et de défense ☐ Gestion de l'équipe de cybersécurité ☐ Élaboration, mise en œuvre et allocation des ressources, du personnel et des technologies pour répondre aux objectifs de sécurité organisationnelle ☐ Détermination des besoins et élaboration des politiques et des procédures de gestion de la cybersécurité et des risques en matière de cybersécurité ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) ☐ Communications organisationnelles, communications publiques et communications en cas de crise ☐ Gestion, mesures et suivi du programme de cybersécurité
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 tant que conseiller principal en sécurité auprès de la direction, ce rôle nécessitera une appréciation complète des risques opérationnels. ▪ 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. ▪ 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 et les implications pour le personnel, les ressources, les procédures et les politiques. Il faudra l'intégrer dans une stratégie de sécurité et un plan d'action pour l'organisation. ▪ 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. ▪ 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. Les mesures devront également tenir compte des contraintes et des solutions de rechange organisationnelles. ▪ 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 avancées liées à la mise en œuvre d'une stratégie de sécurité quantique et aux processus de soutien au sein de l'organisation.

Auditeur de la sécurité de l'information (SI)

Cadre de référence de la NICE	Aucun. Associé à OV-PMA-005 – Auditeur de programmes de TI
Description fonctionnelle	Un auditeur spécialisé dans la sécurité de l'information est chargé d'évaluer la sécurité et l'efficacité des systèmes de TI et des contrôles connexes à l'appui de la sécurité des renseignements/données organisationnels, des systèmes de TI et de leurs composants. L'audit réalisé fait souvent l'objet d'un rapport à un cadre supérieur, avec des recommandations de changements ou d'améliorations.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou le mauvais jugement peuvent entraîner un audit incomplet ou inexact qui ne permet pas de déterminer les problèmes critiques des systèmes ou des processus et ne répond pas aux exigences de sécurité organisationnelle, ce qui augmente les risques potentiels de compromission ou de défaillance du système de sécurité.
Parcours de perfectionnement	L'emploi à ce poste est souvent précédé d'une éducation formelle avec un diplôme dans un domaine des TI ainsi qu'une expérience dans un rôle organisationnel de cybersécurité. Une formation et des études spécialisées dans les pratiques d'audit des systèmes d'information et de la sécurité de l'information sont également nécessaires.
Autres titres	Auditeur de cybersécurité Évaluateur de contrôle de la sécurité Auditeur de sécurité des TI
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes
Tâches	▪ Collaborer avec les intervenants clés pour établir une stratégie efficace d'audit de la sécurité de l'information qui définit les exigences en matière d'audit interne et externe ▪ Assurer la liaison avec les auditeurs externes, selon les besoins, pour répondre aux exigences organisationnelles ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Élaborer et mettre en œuvre des plans d'audit interne détaillé alignés sur les objectifs organisationnels et les exigences de sécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour soutenir les activités d'audit de sécurité de l'information (SI) ▪ Développer et déployer des essais de politique sur les systèmes de SI ▪ Examiner les activités d'évaluation de la sécurité et d'autorisation ▪ Conseiller d'autres cadres supérieurs sur les programmes, politiques, processus, systèmes et éléments de cybersécurité ▪ Examiner et interpréter les politiques et les contrôles en matière de cybersécurité et de sécurité de l'information ▪ Maintenir une compréhension actuelle du contexte des cybermenaces pour les entreprises ▪ Programmer et réaliser des audits internes de la SI ▪ Analyser et interpréter les résultats de l'audit externe de la SI ▪ Rendre compte des résultats et formuler des recommandations à la direction et aux propriétaires du système

<table>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires dans un domaine lié à la cybernétique ou aux TI (par exemple : génie informatique, informatique, technologies de l’information, gestion des technologies des affaires – sécurité numérique ou équivalent)</td></tr>
<tr><td>Formation</td><td>Formation spécialisée en audit des TI ou des systèmes d’information et en audit de sécurité.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience (3 à 5 ans) en cybersécurité avec une préférence pour l’analyse des systèmes (par exemple, analyste des opérations de cybersécurité, analyste de vulnérabilité, analyste de la sécurité des systèmes de TI)</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ 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
▪ Processus et politiques de gestion des risques en matière de cybersécurité
▪ Exigences de conformité, y compris la législation sur la protection de la vie privée et la sécurité
▪ Infrastructure de sécurité organisationnelle et systèmes de compte rendu
▪ Outils et systèmes d’audit des SI
▪ Évaluations de vulnérabilité
▪ Résultats des essais de pénétration
▪ Mesures du rendement des systèmes de TI</td></tr>
<tr><td>Compétences</td><td colspan="2">Application de base des CCH suivantes :
☐ Gestion de projets et programmes
☐ Politiques, pratiques et procédures d’audit des TI

Application avancée des CCH suivantes :
☐ Exigences juridiques, politiques et de conformité
☐ Objectifs opérationnels et manière dont les TI/données/systèmes aident l’entreprise
☐ Politiques, pratiques et procédures d’audit en matière de sécurité de l’information
☐ Concepts, principes et pratiques de sécurité intégrée/organisationnelle (logiciels, systèmes, données, matériel et personnel)
☐ Ressources, compétences et habiletés en matière d’audit externe
☐ Menaces, besoins opérationnels et infrastructures techniques liés au secteur/contexte
☐ Responsabilités, obligations de rendre compte et mesures de rendement en matière de sécurité organisationnelle
☐ Gestion, mesures et suivi du programme de cybersécurité
☐ Contrôles organisationnels de cybersécurité et agents responsables
☐ Menaces et vulnérabilités organisationnelles, y compris :
o Situation de la menace à la cybersécurité
o Évaluation de vulnérabilité et application de mesures d’atténuation
o Infrastructure de sécurité organisationnelle, y compris les systèmes de protection et de défense</td></tr>
</table>

	☐ Sécurité tout au long du cycle de vie du développement du système/logiciel ☐ Sécurité de la chaîne d'approvisionnement ☐ Intégration, essai et déploiement du système ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) et ententes d'approvisionnement
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 et des liens avec les systèmes organisationnels. ▪ 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. ▪ 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, les implications pour les contrôles de sécurité et la façon dont ils seront mesurés et évalués par rapport aux objectifs de sécurité. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Par conséquent, les audits des outils et systèmes de défense évolueront. ▪ 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 comment ces outils fonctionnent, comment leur rendement peut être mesuré et quelles activités d'audit peuvent être nécessaires. ▪ 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.

Conception et développement

Cette catégorie de travail concerne le développement d'infrastructures, de systèmes et de logiciels sécurisés. Il s'agit d'une branche très technique de l'emploi en cybersécurité. La majorité de ce travail relève de la responsabilité des ingénieurs informaticiens (2147), des programmeurs et des développeurs en médias interactifs (2174), des évaluateurs de systèmes informatiques (2283), et des analystes et consultants en informatique (2171), en plus des rôles suivants au sein de cette NPN :

- Architecte de la sécurité
- Ingénieur en sécurité/technologue en ingénierie de la sécurité
- Évaluateur de logiciels sécurisés
- Spécialiste d'essai et d'évaluation de sécurité
- Analyste des systèmes de technologie opérationnelle
- Analyste de la sécurité de la chaîne d'approvisionnement
- Développeur de la sécurité des systèmes d'information
- Ingénieur/analyste en automatisation de la sécurité
- Cryptanalyste/cryptographe

Étant donné l'orientation de ce domaine d'activité, l'accent est mis sur l'application d'une compréhension technique approfondie dans un contexte opérationnel afin de mieux soutenir les résultats organisationnels en matière de cybersécurité.

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.

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.

Évaluateur de logiciels sécurisés

Cadre de référence de la NICE	Dispositions relatives à la sécurité, SP Dev-001, Évaluateur de logiciels sécurisés
Description fonctionnelle	En fonction des références, de la documentation sur la sécurité organisationnelle, des orientations en matière de cybersécurité et des outils et ressources nécessaires, le titulaire analyse la sécurité des applications informatiques, des logiciels ou des programmes utilitaires spécialisés, nouveaux ou existants, et fournit des résultats exploitables.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes peuvent entraîner des vulnérabilités dans les logiciels et les outils sur le Web peuvent mettre en danger les systèmes et services organisationnels.
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans d'expérience dans le domaine du développement de logiciels. Ce rôle nécessite souvent une formation spécialisée, des études ou une expérience correspondant aux logiciels sécurisés et aux activités d'évaluation de vulnérabilité pour la sécurité des logiciels/applications.
Autres titres	▪ Développeur/programmeur de logiciels sécurisés ▪ Spécialistes d'essai et d'évaluation de logiciels ▪ Analyste/évaluateur de vulnérabilité
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 2174 – Programmeurs/programmeuses et développeurs/développeuses en médias interactifs
Tâches	▪ 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, 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 ▪ Rechercher, analyser et mettre en œuvre des processus et des techniques de développement d'applications sécurisées ▪ Analyser les données de sécurité et fournir des conseils et des rapports ▪ Élaborer et mener des procédures d'essais et de validation de systèmes ou d'applications logicielles, de programmation et de codage sécurisé, et faire rapport sur les fonctionnalités et la résilience ▪ Créer et examiner les cas d'utilisation du système ▪ Effectuer des balayages et des examens de vulnérabilité des systèmes ou des applications logicielles, et examiner les contrôles et les mesures nécessaires pour protéger les systèmes ou les applications logicielles ▪ Préparer des rapports sur les systèmes logiciels, le développement et les applications, les correctifs ou les versions qui laisseraient les systèmes vulnérables ▪ Développer des contre-mesures contre les exploitations potentielles des vulnérabilités des systèmes ▪ Effectuer une analyse des risques chaque fois qu'une application ou un système subit un changement

<table>
<tr><td></td><td colspan="2">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 validation par un tiers (VVT) sur les projets de logiciels
Fournir des conseils sur les politiques, plans et pratiques de sécurité logicielle
Examiner, élaborer et fournir du matériel de formation</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme en informatique pertinent lié à la programmation, à la conception ou au développement de logiciels</td></tr>
<tr><td>Formation</td><td>Certification valide au niveau de l’industrie pour le développement de logiciels sécurisés et les essais de sécurité logicielle</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience modérée (3 à 5 ans) dans le développement de logiciels, suivie d’une expérience modérée (3 à 5 ans) dans des activités de développement de logiciels sécurisés.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">Outils, processus et protocoles de développement de logiciels
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
Information sur la sécurité des logiciels et des applications à source ouverte (par exemple, OWASP)
Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents
Outils et techniques d’essai et d’évaluation de la sécurité des logiciels
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
Bases de données communes sur la vulnérabilité
Sites de collaboration sociale pour le développement de logiciels (par exemple GITHUB)
Services de sécurité fournis, le cas échéant</td></tr>
<tr><td>Compétences</td><td colspan="2">Application de base des CCH suivantes :
☐ Concepts d’architecture de sécurité et modèle d’architecture de sécurité des renseignements d’entreprise
☐ Processus d’évaluation de la sécurité et d’autorisation
☐ Processus d’achat de logiciels et évaluations de l’intégrité de la chaîne d’approvisionnement
☐ Outils, procédures et pratiques d’essai et d’évaluation des systèmes de sécurité des TI

Application avancée des CCH suivantes :
☐ Modèles, processus et principes du génie logiciel
☐ Cycle de vie du développement de logiciels et gestion de projets de logiciels
☐ Processus, procédures, pratiques, outils et techniques d’opérations de codage et de développement de logiciels sécurisés
☐ Besoins opérationnels en matière de sécurité, y compris les exigences de conformité
☐ Caractéristiques et exigences en matière de sécurité des données</td></tr>
</table>

	☐ Contrôles de sécurité pour le développement de logiciels ☐ Normes de développement de logiciels ☐ Normes de logiciels sécurisés ☐ Méthodes et processus sécurisés d'essai et d'évaluation des logiciels ☐ Méthodes et applications d'évaluation de vulnérabilité et d'essais de pénétration ☐ Création et essai des modèles de menace ☐ Analyse, évaluation et balayage des vulnérabilités ☐ Activités et techniques d'essais de pénétration ☐ Enquête et analyse sur les vulnérabilités et les failles des logiciels ☐ Mise en place et gestion de l'environnement sécurisé d'essais de logiciels et d'applications Web ☐ 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)
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, des systèmes logiciels et applications utilisés, 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 les outils susceptibles de soutenir le développement, l'essai et l'intégration de logiciels seront utilisés ainsi que les implications potentielles en matière de sécurité. Si des outils de sécurité automatisés sont utilisés dans le développement et l'évaluation des logiciels, les responsabilités en matière d'essais, d'intégration et de suivi des exigences devront être définies et les responsables de ces activités devront être conseillés/formés sur les changements de processus et de procédures qui en résultent. ▪ 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, il faudra procéder à des évaluations créatives et localement pertinentes de la robustesse de la sécurité des logiciels/applications et des stratégies d'atténuation potentielles. 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 appliquée à l'environnement de logiciel/d'application.

Spécialiste d’essai et d’évaluation de sécurité

Cadre de référence de la NICE	Fourniture sécurisée, essais et évaluation de la sécurité, SP-TST-001	
Description fonctionnelle	Le titulaire planifie, prépare et exécute des essais de dispositifs de sécurité, de systèmes d’exploitation, de logiciels et de matériel afin d’évaluer les résultats par rapport à des spécifications, des politiques et des exigences définies, et documente les résultats et fait des recommandations qui peuvent améliorer la confidentialité, l’intégrité et la disponibilité des renseignements.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement peuvent entraîner l’intégration et le déploiement de systèmes, de logiciels ou de services de TI présentant des vulnérabilités qui augmentent l’exposition aux menaces et le risque organisationnel. Les compromissions qui en résulteraient pourraient avoir une incidence importante sur l’entreprise.	
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans dans le domaine de la sécurité des TI. Ce rôle nécessite souvent une formation spécialisée, des études ou une expérience en lien avec les essais et les mesures des systèmes.	
Autres titres	Évaluateur de la sécurité des systèmes	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel)	
Tâches	▪ Mettre à l’essai, évaluer et vérifier les systèmes en cours de développement, les systèmes échangeant des renseignements électroniques avec d’autres systèmes, les logiciels et le matériel des systèmes d’exploitation associés, ainsi que les contrôles, et les dispositifs de sécurité utilisés au sein d’une organisation pour déterminer le niveau de conformité aux spécifications, aux politiques et aux exigences définies ▪ Analyser les résultats des essais des systèmes d’exploitation, des logiciels et du matériel et formuler des recommandations sur la base des résultats ▪ Élaborer des plans d’essai pour répondre aux spécifications, aux politiques et aux exigences ▪ Valider les spécifications, les politiques et les exigences en matière de testabilité ▪ Créer des preuves vérifiables des mesures de sécurité ▪ Préparer des évaluations qui documentent les résultats des essais et les éventuelles vulnérabilités en matière de sécurité ▪ Déployer, valider et vérifier le fonctionnement des dispositifs d’infrastructure de réseau ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs ▪ Former et encadrer les membres de l’équipe de sécurité	
Qualifications requises	Éducation	Baccalauréat en informatique ou dans une discipline connexe ou formation et expérience équivalentes
	Formation	Formation à la mesure, à l’évaluation et aux essais de la sécurité des systèmes.

	Expérience professionnelle	Expérience importante (5-10 ans) dans le domaine des TI, avec une expérience de 3 à 5 ans dans un rôle de sécurité des systèmes à l'appui des évaluations de la sécurité et des audits des TI est préférable. Expérience de travail dans des environnements d'essais sécurisés.
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 ▪ Architecture de système ▪ 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 ▪ Outils, techniques, procédures et protocoles des politiques d'essais et d'évaluation des systèmes ▪ Législation et exigences de conformité	
Compétences	Application de base des CCH suivantes : ☐ Processus d'achat en matière de sécurité et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Processus d'ingénierie des systèmes Application avancée des CCH suivantes : ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Stratégies d'essai et d'évaluation des systèmes de TI ☐ Infrastructure et ressources d'essai et d'évaluation des systèmes de TI ☐ Outils, procédures et pratiques d'essai et d'évaluation des systèmes de sécurité des TI ☐ Connaissance technique des réseaux, des composants informatiques, de la technologie d'alimentation électrique, des protocoles de système, des logiciels de cybersécurité ☐ Architecture et modèles de sécurité des réseaux ☐ Réalisation d'essais de sécurité indépendants de validation et de vérification ☐ Méthodes et techniques d'essai et d'évaluation des systèmes ☐ Conception d'essais, élaboration de scénarios et examen de l'état de préparation ☐ Essai d'intégration des systèmes ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Concepts d'architecture de sécurité et modèle d'architecture de sécurité des renseignements d'entreprise ☐ Détermination des politiques et exigences en matière d'essai et d'évaluation ☐ Collecte, analyse, vérification et validation des données d'essais et traduction des données et des résultats des essais en conclusion ☐ Conception et documentation des stratégies d'essai et d'évaluation ☐ Rédaction des rapports techniques et rapports d'essai et d'évaluation.	

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 ses responsabilités en matière de cybersécurité par rapport aux systèmes organisationnels, la manière dont ces systèmes sont intégrés et la manière dont ils peuvent être testés et évalués. ▪ 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 aux systèmes organisationnels. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils seront intégrés dans l'infrastructure de sécurité organisationnelle et les implications sur les pratiques d'essais et d'évaluation. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des défis qui nécessiteront une évaluation continue des pratiques d'essai et d'évaluation et des outils requis. ▪ 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, ainsi que leurs implications sur les essais et l'évaluation de la sécurité. ▪ 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 permettant de mettre à l'essai et d'évaluer le chiffrement et le degré de résistance quantique.

Analyste des systèmes de technologie opérationnelle

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire est responsable de fournir des conseils et d'assurer une cybersécurité efficace dans les contextes de technologie opérationnelle (TO)(SCI/SCO/SCADA). Il travaille de concert avec les ingénieurs systèmes/technologues de différentes disciplines qui sont associés aux systèmes gérés par la TO (par exemple, les ingénieurs en mécanique des fluides, les ingénieurs spécialistes des systèmes de puissance, les ingénieurs de systèmes mécaniques).
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement pourraient entraîner une défaillance catastrophique de la TO et des systèmes connexes qu'ils utilisent pour la gestion. Dans de nombreux cas, cela peut avoir une incidence importante sur les opérations organisationnelles et, dans certains cas, peut directement entraîner des dommages importants pour les êtres humains (par exemple dans les systèmes d'infrastructures critiques).
Parcours de perfectionnement	Après une formation technique, le titulaire est souvent employé dans des activités liées aux systèmes de TI ou de TO qui constituent la base d'un travail de cybersécurité plus spécialisé dans l'environnement de TO. De même, les professionnels de la cybersécurité qui travaillent normalement dans un environnement informatique peuvent passer aux systèmes de TO en bénéficiant d'une formation et d'un enseignement spécialisés en TO et en intégration de systèmes.
Autres titres	Conseiller en sécurité de la TO Technicien en sécurité de la TO Analyste de la sécurité – SCI/SCO/SCADA
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
Tâches	▪ Collaborer avec les intervenants clés pour mettre en place un programme efficace de gestion des risques liés à la cybersécurité dans l'environnement de TO. ▪ Rechercher et soutenir la conception de solutions de cybersécurité dans le contexte de la TO ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Rédiger, mettre en œuvre et maintenir les politiques, normes et procédures de sécurité des TI/TO ▪ Surveiller et gérer les exigences et les contrôles de cybersécurité dans l'environnement de TO ▪ Évaluer et analyser la position en matière de cybersécurité dans les systèmes de TO et recommander des mesures correctives/de gestion des risques pour les vulnérabilités ▪ Travailler avec d'autres parties prenantes, soutenir la conception et le développement de solutions de sécurité pour répondre aux exigences commerciales et techniques dans l'environnement de TO

<table>
<tr><td></td><td colspan="2">▪ Gérer l'intégration technique entre les TI et les TO
▪ Définir et maintenir des ensembles d'outils et des procédures qui soutiennent le suivi et la gestion des TO
▪ En concertation avec les autres parties prenantes, élaborer des plans d'intervention en cas d'incident de cybersécurité définissant clairement le rôle des personnes chargées de la gestion et de la maintenance des systèmes de TO
▪ Préparer des rapports techniques
▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés aux TO</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Baccalauréat en informatique, en génie informatique ou dans une discipline connexe ou formation et expérience équivalentes</td></tr>
<tr><td>Formation</td><td>Formation spécialisée associée à la cybersécurité de la TO ainsi qu'aux outils et techniques spécifiques aux systèmes requis</td></tr>
<tr><td>Expérience professionnelle</td><td>L'expérience préférée pour le rôle de premier échelon requiert une expérience modérée de 2 à 3 ans dans l'environnement de TO</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Plans stratégiques et d'affaires
▪ Évaluation de la menace et des risques
▪ Processus de gestion de vulnérabilité et évaluations de vulnérabilité des TO
▪ Processus et procédures de gestion des incidents
▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents qui peuvent être utilisés pour les incidents de cybersécurité de TO
▪ 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
▪ Outils, techniques et procédures de sécurité des TO</td></tr>
<tr><td>Compétences</td><td colspan="2">Tout en sachant que tous les analystes de TO n'auront pas nécessairement une formation en TI, il convient de se référer aux applications de base des CCH suivantes :

☐ Systèmes de télémétrie, communication de données, acquisition de données et contrôle de processus
☐ Concepts de systèmes d'exploitation, de réseaux et de systèmes de communication
☐ Réseaux de distribution électrique, équipement du système électrique, fonctionnement des stations de transformation et théorie de l'électricité
☐ Procédures de dépannage et de maintenance des ordinateurs et des réseaux
☐ Principes et pratiques de l'administration des réseaux
☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels
☐ Applications et systèmes de gestion de bases de données
☐ Administration et optimisation des bases de données
☐ Méthodes et processus d'essai et d'évaluation des systèmes
☐ Mesures ou indicateurs du rendement, de la disponibilité, de la capacité ou des problèmes de configuration du système</td></tr>
</table>

	☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défauts Application avancée des CCH suivantes : ☐ Logiciels et matériel des systèmes de TO, contrôleurs logiques programmables, relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris les implications et l'évaluation des dispositifs IdO) ☐ Exigences juridiques et de conformité, y compris les responsabilités organisationnelles en matière de sécurité du lieu de travail et du public liées à la TO/production ☐ Normes et meilleures pratiques de l'industrie, notamment en ce qui concerne les environnements industriels dans l'espace de cybersécurité ☐ Gestion, mesures et suivi du programme de cybersécurité Systèmes de contrôle – applicables à l'industrie/aux environnements de production ☐ Intégration et convergence des TI/TO ☐ Sécurité des processus et analyse des dangers ☐ Analyse et intégration de système ☐ Résolution de problèmes dans les environnements de systèmes complexes ☐ Communications techniques, y compris la rédaction de rapports pour traiter des questions techniques interdisciplinaires
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, et plus particulièrement ceux liés aux TO et à l'exploitation et l'accès à distance. ▪ 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 surveillance et des opérations à distance par l'IdO et les dispositifs. ▪ 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 et les implications pour les exigences, les procédures et les politiques de TO. ▪ 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. ▪ 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. Pour le chiffrement au sein des systèmes de TO, cela nécessitera des connaissances et des compétences liées à la mise en œuvre d'une stratégie de sécurité quantique au sein de l'organisation.

Analyste de la sécurité de la chaîne d'approvisionnement

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire est le principal responsable de la collecte et de l'analyse des données pour cibler les failles et les vulnérabilités de la cybersécurité dans les opérations de la chaîne d'approvisionnement d'une organisation, et fournit des conseils et des orientations pour aider à réduire ces risques de la chaîne d'approvisionnement.
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	Généralement tiré de rôles d'analyse de la cybersécurité (par exemple, analyste des opérations de cybersécurité, analyste de vulnérabilité, etc.), ce rôle peut néanmoins être assumé par un large éventail de professionnels qui peuvent évaluer et fournir des renseignements sur les menaces potentielles pesant sur la chaîne d'approvisionnement. Cela inclut ceux qui peuvent se spécialiser dans les aspects liés aux facteurs humains de la chaîne d'approvisionnement (par exemple, accès proche, menace interne).
Autres titres	Analyste de la cybersécurité Analyste de l'intégrité de la chaîne d'approvisionnement
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 ▪ Élaborer et mettre en œuvre des plans alignés sur les objectifs organisationnels et les exigences de sécurité ▪ Recueillir et analyser les renseignements relatifs à la chaîne d'approvisionnement afin de cibler et d'atténuer les défauts et les vulnérabilités, y compris l'intégrité des composants, dans les réseaux ou les systèmes informatiques d'une organisation ▪ Analyser les configurations matérielles et logicielles des systèmes ▪ Recommander du matériel, des logiciels et des contre-mesures à installer ou à mettre à jour en fonction des cybermenaces et des vulnérabilités en matière de sécurité ▪ Collaborer avec les collègues pour mettre en œuvre les changements et les nouveaux systèmes ▪ Suivre et signaler les cybermenaces et les vulnérabilités de sécurité qui ont des répercussions sur le rendement de la chaîne d'approvisionnement ▪ Définir, développer, mettre en œuvre et maintenir des plans, des politiques et des procédures de cybersécurité ▪ Veiller au respect des politiques, réglementations et procédures de cybersécurité de l'organisation

	▪ Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation ▪ Élaborer et tenir à jour des évaluations des risques et des rapports connexes sur les fournisseurs, les produits et les services ▪ Définir et maintenir des ensembles d'outils et des procédures qui soutiennent l'intégrité de la chaîne d'approvisionnement ▪ Préparer des rapports techniques ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés à la cybersécurité et à l'intégrité de la chaîne d'approvisionnement	
Qualifications requises	Éducation	Études postsecondaires dans un domaine lié à la cybernétique ou aux TI (par exemple : génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent)
	Formation	Outre une formation structurée à l'analyse de la cybersécurité, une formation spécialisée et des compétences en matière d'analyse de vulnérabilité et des menaces pesant sur la chaîne d'approvisionnement sont nécessaires.
	Expérience professionnelle	Les personnes employées dans ce rôle peuvent avoir différents niveaux d'expertise en matière de cybersécurité. L'expérience requise dépendra du besoin organisationnel et de la complexité des systèmes à analyser.
Outils et technologie	▪ Plans stratégiques et d'affaires ▪ Évaluation de la menace et des risques ▪ Processus de gestion de vulnérabilité et outils et applications d'évaluation de vulnérabilité ▪ Processus et procédures de gestion des incidents ▪ Infrastructure de sécurité organisationnelle et systèmes de compte rendu Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des risques de cybersécurité dans la chaîne d'approvisionnement ▪ Accords et contrats de tiers et de niveau de service	
Compétences	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 ☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet ☐ Processus d'approvisionnement et exigences de sécurité Application avancée des CCH suivantes : ☐ Infrastructure de sécurité organisationnelle, y compris les systèmes de protection et de défense tout au long de la chaîne d'approvisionnement	

	☐ Situation de la menace à la cybersécurité et sources de renseignements sur la menace liée à la chaîne d'approvisionnement ☐ Exigences juridiques et de conformité alors qu'elles s'étendent aux accords avec des tiers ☐ Analyse de vulnérabilité et outils ☐ Analyse et techniques avancées de sécurité des renseignements et des données ☐ Conception fonctionnelle et technique des réseaux et des systèmes, et solutions de cybersécurité ☐ Processus, responsabilités et pouvoirs de gestion des risques au sein de l'organisation et tout au long de la chaîne d'approvisionnement ☐ Gestion des risques et responsabilité des tiers ☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels ☐ Processus actuels de la chaîne d'approvisionnement nationale
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. ▪ 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. ▪ 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 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 seront nécessaires localement. ▪ 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.

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.

Ingénieur/analyste en automatisation de la sécurité

REMARQUE : *Il s'agit d'un rôle de travail émergent. Il existe des échantillons limités de ce rôle de travail et les tâches et activités des experts en la matière varient en fonction des exigences organisationnelles. En conséquence, les renseignements ci-dessous se fondent sur des représentations actuelles basées sur les exigences de la demande et sur une compréhension de l'intelligence artificielle, de l'apprentissage machine et des exigences de la science des données pour soutenir l'ingénierie et l'analyse des processus automatisés*. *On s'attend à ce que le rôle évolue considérablement au cours des prochaines années.*

Cadre de référence de la NICE	Aucun.
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 ressources nécessaires, le titulaire recherche et définit les besoins opérationnels en matière de sécurité, détermine les besoins et conçoit des solutions automatisées qui soutiennent la sécurité organisationnelle.
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. Formation supplémentaire, études ou expérience en automatisation des processus et activités connexes d'intelligence artificielle/d'ingénierie de l'apprentissage machine.
Autres titres	▪ Ingénieur automaticien de système ▪ Concepteur de systèmes automatisés ▪ Ingénieur en automatisation et contrôles de sécurité
CNP connexes	2133 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 2241 – Technologues et techniciens/techniciennes en génie électronique et électrique
Tâches	▪ Rechercher, développer, intégrer, mettre à l'essai et mettre en œuvre des solutions d'automatisation de la sécurité pour les nuages ou les systèmes ▪ Déterminer l'étendue et planifier les travaux d'automatisation afin de respecter les délais ▪ Gérer/surveiller les activités automatisées de solution de sécurité, y compris les correctifs, les mises à jour et les processus connexes ▪ Élaborer et tenir à jour des outils et des processus pour soutenir les activités d'automatisation de la sécurité ▪ Examiner et mettre à l'essai les scripts d'automatisation de la sécurité avant la mise en œuvre ▪ Dépanner tout problème survenant au cours des essais, de la production ou de l'utilisation

	▪ Créer, utiliser et maintenir une documentation de référence ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour soutenir les activités d'automatisation de la sécurité ▪ Examiner, approuver et superviser les modifications des politiques et contrôles en matière de cybersécurité et leurs implications pour les activités automatisées ▪ Programmer et superviser les évaluations et les audits de sécurité ▪ Superviser et gérer les relations avec les fournisseurs de produits et services de sécurité des TI acquis ▪ Veiller à ce que les exigences de sécurité soient déterminées pour tous les systèmes de TI tout au long de leur cycle de vie ▪ Superviser ou gérer les mesures préventives ou correctives lorsqu'un incident ou une vulnérabilité en matière de cybersécurité est découvert ▪ Évaluer les menaces et élaborer des contre-mesures et des stratégies d'atténuation des risques contre les vulnérabilités des systèmes automatisés ▪ Effectuer une analyse des risques et faire des essais chaque fois qu'un système automatisé subit un changement ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle	
Qualifications requises	Éducation	Diplôme pertinent d'ingénieur ou d'informatique avec une formation de troisième cycle ou équivalente en automatisation des systèmes, apprentissage artificiel ou apprentissage machine.
	Formation	Formation pertinente en matière de cybersécurité pour soutenir les fonctions d'ingénieur en sécurité.
	Expérience professionnelle	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. Expérience en programmation et en essai d'applications. 2 à 3 ans d'expérience pratique dans l'automatisation des processus du système.
Outils et technologie	▪ 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 ▪ Outils, techniques et procédures d'automatisation des processus ▪ Langages de programmation applicables	
Compétences	Niveau d'application avancé des CCH suivantes : ☐ Automatisation des processus dans un cadre de sécurité ☐ API, automatisation et langages de script ☐ Fonctions SDN, NFV et VNF ☐ Modèles d'ingénierie de la sécurité	

	☐ 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 ☐ 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)
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. ▪ 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. ▪ 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. En outre, en tant que responsable technique potentiel de l'automatisation de la sécurité, il peut être nécessaire de former les responsables des organisations aux avantages et aux risques de l'automatisation et à la gestion des changements nécessaires. ▪ 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 nécessitera une bien meilleure appréciation des capacités des acteurs de menace et des contre-mesures potentielles. ▪ 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 et la compréhension des implications sur les mécanismes de sécurité basés sur l’IA.

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.

Exploitation et maintenance

Cette catégorie de travail participe à l'exploitation et au maintien de la sécurité des systèmes et des données, conformément aux spécifications de l'architecture et de la conception de la sécurité. Toutes ces fonctions sont exercées principalement dans des professions liées aux technologies de l'information (CNP 0213, 2147, 2174, 2171 et 2283) sur le marché du travail canadien, à l'exception de celles indiquées ci-dessous qui se sont établies comme des professions dépendant de plus en plus des systèmes connectés à Internet et des menaces qui y sont associées :

- Spécialiste du soutien à la gestion de l'identité et de l'authentification
- Spécialiste du chiffrement/soutien à la gestion des clés
- Spécialiste de la protection des données/agent de la protection de la vie privée

Pour le spécialiste en cybersécurité travaillant dans cette catégorie de travail, il doit non seulement apporter son expertise technique, mais aussi s'intégrer étroitement aux exigences opérationnelles quotidiennes de l'organisation en matière de TI. Cela implique généralement, outre les compétences techniques, des services aux clients améliorés et des compétences accrues en matière de communication.

Spécialiste de la gestion de l’identité et du soutien à l’authentification

Rôle du cadre de la NICE	Aucun.
Description fonctionnelle	Le titulaire fournit un soutien continu à la gestion de l’identité, des justificatifs d’identité, de l’accès et de l’authentification afin de soutenir la sécurité organisationnelle des TI.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d’attention aux détails ou un mauvais jugement peuvent entraîner une compromission du système qui, selon le type, peut avoir un impact important sur les systèmes, les capacités ou les fonctions informatiques de l’organisation.
Parcours de perfectionnement	Il s’agit souvent d’un emploi de premier échelon dans le domaine de la sécurité après avoir acquis de l’expérience dans la gestion de l’accès et des justificatifs d’identité pour l’administration du réseau ou du système. Avec une formation et une expérience supplémentaires, il existe un potentiel pour des rôles plus techniques ou plus opérationnels ainsi que des possibilités de gestion.
Autres titres	▪ Analyste en gestion d’accès ▪ Analyste de système ▪ Spécialiste de la gestion de l’identité, des justificatifs d’identité et de l’accès (GIJIA)
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2281 – Techniciens/techniciennes de réseau informatique 2282 – Agents/agentes de soutien aux utilisateurs
Tâches	▪ Déterminer les besoins des clients et proposer des solutions techniques ▪ Modéliser et associer les utilisateurs aux ressources (par exemple, en fonction de leur rôle) ▪ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ▪ Déployer, configurer et gérer l’approvisionnement des utilisateurs, y compris la synchronisation de l’identité, l’approvisionnement automatique et la désactivation automatique de l’accès, le flux de travail d’approbation des demandes de sécurité en libre-service et les rapports consolidés ▪ Configurer et gérer les solutions de gestion des accès de l’entreprise sur le Web (authentification unique, gestion des mots de passe, authentification et autorisation, administration déléguée) ▪ Analyser les schémas ou les tendances des incidents en vue d’une résolution ultérieure ▪ Gérer les processus d’approbation des demandes de changement d’identité ▪ Auditer, enregistrer et signaler les étapes de gestion du cycle de vie des utilisateurs par rapport à la liste de contrôle d’accès sur les plateformes gérées ▪ Configurer et gérer l’identité, les justificatifs d’identité et l’accès fédérés en conformité avec la politique, les normes et les procédures de sécurité ▪ Effectuer des tâches liées à l’autorisation et à l’authentification dans des environnements physiques et logiques

<table>
<tr><td></td><td colspan="2">▪ 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>Diplôme d’études collégiales dans le domaine des technologies de l’information.</td></tr>
<tr><td>Formation</td><td>Formation sur les politiques, protocoles, outils et procédures d’identité, de justificatifs d’identité, de gestion de l’accès et d’authentification pertinents.
Développement et application d’un système de gestion des éléments d’identification de l’utilisateur.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience dans la gestion de services d’annuaire et travail dans un environnement de sécurité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Systèmes de gestion de l’identité et de l’accès
▪ Services d’annuaire
▪ Outils et services d’authentification
▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH s’appliquent au niveau de base :
☐ Architectures et normes de gestion de l’identité, des justificatifs d’identité et de l’accès
☐ Processus liés au cycle de vie des applications
☐ Mise en correspondance et modélisation des justificatifs d’identité
☐ Contrôles d’accès basés sur des politiques et adaptés aux risques
☐ Développement et application d’un système de gestion des éléments d’identification de l’utilisateur
☐ Analyse organisationnelle des tendances des utilisateurs et des affaires
☐ Consultation des clients et résolution des problèmes

Les CCH sont appliquées à un niveau avancé :
☐ Protocoles, outils et procédures d’accès au réseau, de gestion de l’identité et de l’accès
☐ Méthodes d’authentification, d’autorisation et de contrôle d’accès
☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes
☐ Développement et application des contrôles d’accès aux systèmes de sécurité
☐ Gestion des services d’annuaire
☐ Politiques de sécurité des utilisateurs des technologies de la technologie de l’information (TI) de l’organisation (par exemple, création de compte, règles relatives aux mots de passe, contrôle d’accès)</td></tr>
<tr><td>Tendances futures ayant une incidence sur les compétences clés</td><td colspan="2">▪ La dépendance accrue sur les services virtualisés ou « basés sur l’infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités dans la gestion des systèmes de cybersécurité.
▪ 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 de l’appareil, il faudra évaluer les risques posés pour l’organisation, les mesures d’atténuation pour tenir compte d’une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d’incident.</td></tr>
</table>

	▪ L’utilisation accrue des outils automatisés, aidée par l’intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans les processus de gestion de l’identité et de l’accès, y compris les changements techniques et de processus connexes. ▪ 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 et les réponses potentielles 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 ainsi qu’une compréhension approfondie des implications pour les protocoles d’authentification et de la manière de se défendre contre les menaces potentielles de l’informatique quantique.

Spécialiste du chiffrement/soutien à la gestion des clés

Cadre de référence de la NICE	Aucun.	
Description fonctionnelle	Le titulaire fournit un soutien continu à la gestion et à la maintenance des réseaux privés virtuels, du chiffrement, de l'infrastructure à clés publiques et, dans certains cas, de la sécurité des communications (SECOM) pour soutenir la sécurité organisationnelle des TI.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une compromission du système qui, selon le type, peut avoir un impact important sur les systèmes, les capacités ou les fonctions informatiques de l'organisation.	
Parcours de perfectionnement	Il s'agit souvent d'un emploi de premier échelon dans le domaine de la sécurité après avoir acquis de l'expérience dans la gestion de l'accès et des justificatifs d'identité pour l'administration du réseau ou du système. Avec une formation et une expérience supplémentaires, il existe un potentiel pour des rôles plus techniques ou plus opérationnels ainsi que des possibilités de gestion.	
Autres titres	▪ Analyste en gestion d'accès ▪ Analyste de système ▪ Spécialiste de la gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2281 – Techniciens/techniciennes de réseau informatique 2282 – Agents/agentes de soutien aux utilisateurs	
Tâches	▪ Déterminer les besoins des clients et proposer des solutions techniques ▪ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ▪ Développer et appliquer des contrôles d'accès aux systèmes de sécurité ▪ Déployer, configurer et gérer les services de chiffrement/gestion de clés ▪ Mettre en place des VPN ▪ Analyser des modèles ou des tendances pour mieux les résoudre ▪ Gérer les processus d'approbation des demandes de changement d'identité ▪ Auditer, enregistrer et signaler les étapes de gestion du cycle de vie des utilisateurs par rapport à la liste de contrôle d'accès sur les plateformes gérées ▪ Configurer et gérer l'identité, les justificatifs d'identité et l'accès fédérés en conformité avec la politique, les normes et les procédures de sécurité ▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle	
Qualifications requises	Éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information.

	Formation	Formation aux technologies de chiffrement et de gestion des clés pertinentes au niveau appliqué.
	Expérience professionnelle	Expérience dans la gestion de services d'annuaire et travail dans un environnement de sécurité.
Outils et technologie	▪ Systèmes de gestion de l'identité et de l'accès ▪ Outils, processus et procédures de chiffrement et de gestion des clés ▪ Outils et procédures de chiffrement par VPN et Wi-Fi ▪ Outils et services d'authentification ▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents	
Compétences	Les CCH s'appliquent au niveau de base : ☐ Cryptanalyse ☐ Concepts et méthodes de cryptographie et de chiffrement ☐ Cryptographie symétrique et asymétrique ☐ Stéganographie et stéganalyse ☐ Autorités cryptologiques nationales (Centre de la sécurité des télécommunications) ☐ Fournisseurs d'infrastructures à clés publiques Les CCH sont appliquées au niveau avancé : ☐ Politiques de sécurité des utilisateurs des technologies de la technologie de l'information (TI) de l'organisation (par exemple, création de compte, règles relatives aux mots de passe, contrôle d'accès) ☐ Protocoles, outils et procédures d'accès au réseau, de gestion de l'identité et de l'accès ☐ Normes nationales et internationales ☐ Méthodes d'authentification, d'autorisation et de contrôle d'accès ☐ ICP (infrastructure à clés publiques), MSM (module de sécurité matérielle), certificat numérique, protocole SSL/TLS (sécurité de la couche transport), protocole SSH, technologies de chiffrement actuelles ☐ Processus liés au cycle de vie des applications ☐ Signatures numériques, certificats numériques et gestion des certificats numériques ☐ Protocoles d'authentification ☐ VPN et protocoles ☐ Chiffrement des fichiers et des disques ☐ Algorithmes de chiffrement ☐ Analyse organisationnelle des tendances des utilisateurs et des affaires ☐ Consultation des clients et résolution des problèmes	
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. Cela comprend la connaissance et la compétence des algorithmes de sécurité quantique utilisés, l'intégration et la mise en œuvre de technologies de sécurité quantique au sein de l'organisation et les protocoles d'essai et d'évaluation du matériel, des logiciels et des protocoles de sécurité quantique et de résistance quantique.

Spécialiste de la protection des données/agent de la protection de la vie privée

Cadre de référence de la NICE	Supervision et gouvernance, OV-LGA-002, agent de protection de la vie privée/gestionnaire du respect de la vie privée
Description fonctionnelle	Le titulaire élabore, met en œuvre, conseille et administre le programme de respect de la vie privée qui soutient les exigences de protection des renseignements personnels.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une compromission ou une violation des renseignements personnels, ce qui outre les conséquences et la responsabilité individuelles potentielles, peut entraîner des amendes importantes pour la violation, ainsi qu'une perte de réputation et de confiance.
Parcours de perfectionnement	Ce rôle peut être soutenu par des voies techniques ou non techniques qui mènent à un rôle de premier échelon lié à la gestion de la vie privée/des données sensibles et à la progression vers le niveau de conseiller en politique. Les personnes peuvent se spécialiser davantage dans la sécurité des données ou comme analyste des politiques ou conseiller principal.
Autres titres	▪ Agent de la protection de la vie privée ▪ Agent/gestionnaire du respect de la vie privée
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 416X – Chercheurs, experts-conseils/expertes-conseils et agents/agentes des politiques et des programmes (en fonction du contexte)
Tâches	▪ Interpréter et appliquer les lois, règlements, politiques, normes ou procédures à des questions relatives à la protection de la vie privée ▪ Mener des évaluations de l'impact périodiques et des activités de contrôle de conformité continues pour repérer les lacunes en matière de conformité ou les domaines à risque afin de garantir que les préoccupations, les exigences et les responsabilités en matière de protection de la vie privée sont traitées ▪ Mettre en place et maintenir un mécanisme de suivi de l'accès aux renseignements dans le cadre de l'organisation et conformément à la loi, afin de permettre au personnel qualifié d'examiner ou de recevoir ces renseignements ▪ Établir et mettre en œuvre un programme d'audit interne sur la protection de la vie privée, et préparer des rapports d'audit qui tirent des conclusions techniques et procédurales, déterminent les violations de la vie privée, et recommandent des solutions correctives ▪ Fournir des conseils et des orientations sur les lois, les règlements, les politiques, les normes ou les procédures à la direction, au personnel ou aux principaux services ▪ Veiller au respect des lois, règlements et politiques en matière de vie privée et de cybersécurité, et à l'application cohérente des sanctions en cas de non-respect des mesures énoncées pour l'ensemble du personnel de l'organisation ▪ Lancer, faciliter et promouvoir des activités de sensibilisation à la protection de la vie privée au sein de l'organisation, notamment la collecte, l'utilisation et le partage des renseignements ▪ Suivre les progrès des technologies renforçant la protection de la vie privée et veiller à ce que l'utilisation des technologies soit conforme

<table>
<tr><td></td><td colspan="2">aux exigences en matière de respect de la vie privée et de cybersécurité, y compris la collecte, l’utilisation et la divulgation de renseignements
▪ Examiner les plans et projets de sécurité des réseaux de l’organisation pour s’assurer qu’ils sont conformes aux objectifs et politiques en matière de protection de la vie privée et de cybersécurité
▪ Collaborer avec le conseil juridique et la direction pour s’assurer que l’organisation dispose d’un consentement approprié en matière de vie privée et de confidentialité, que les formulaires d’autorisation et les documents pertinents sont conformes aux pratiques et exigences juridiques
▪ Élaborer, fournir et superviser le matériel de formation et les activités de sensibilisation à la protection de la vie privée</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires dans un domaine applicable (par exemple : administration des affaires, droit, sciences politiques, sciences sociales ou domaine équivalent)</td></tr>
<tr><td>Formation</td><td>Formation spécialisée sur la confidentialité et la sécurité des données, les bases de la cybersécurité, l’analyse des répercussions sur la vie privée, la législation relative à la protection de la vie privée et la conformité</td></tr>
<tr><td>Expérience professionnelle</td><td>Formation et expérience antérieures (2 à 3 ans) dans un rôle d’analyse des politiques liées à la sécurité ou à la vie privée, généralement requises pour un rôle de premier échelon</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Législation et politiques en matière de vie privée et d’information
▪ Exigences de conformité
▪ Mécanismes et modèles de rapports
▪ Évaluations des répercussions sur la vie privée et énoncés de sensibilité
▪ Évaluation de la menace et des risques
▪ Exigences en matière de données et de renseignements
▪ Outils et méthodologies d’évaluation de la protection de la vie privée</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH s’appliquent au niveau de base :
☐ Connaissance pratique des principes et des éléments de la cybersécurité
☐ Connaissances techniques permettant de comprendre la sécurité et l’intégrité des données, les exigences de sécurité et la conception fonctionnelle et technique des réseaux et des systèmes, ainsi que les solutions de cybersécurité
☐ Conceptions et fonctions de sécurité des données, méthodologies d’analyse, essais et protocoles
☐ Gestion, mesures et suivi du programme de cybersécurité

Les CCH sont appliquées à un niveau avancé :
☐ Évaluation de la menace et des risques (axée sur la protection de la vie privée/la sécurité des données)
☐ Lois, règlements, politiques et procédures nationales et internationales
☐ Politiques, procédures et réglementations en matière de sécurité de l’information</td></tr>
</table>

	☐ Incidences spécifiques des lacunes et des failles de la cybersécurité ☐ Suivi des progrès des lois et des politiques en matière de protection de la vie privée ☐ Évaluations des répercussions sur la vie privée ☐ Déclarations de confidentialité fondées sur les lois et règlements ☐ Signalement des infractions
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités dans la protection des données sensibles et la réponse aux violations potentielles et le signalement de ces dernières. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils seront intégrés à la protection des renseignements personnels au sein de l'organisation et comment cela doit se traduire en politiques, procédures et pratiques. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace remettra probablement en question les technologies et les ressources existantes destinées à gérer la protection des renseignements personnels. En conséquence, des outils, des processus ou des formations supplémentaires seront nécessaires pour garder une longueur d'avance sur les menaces. ▪ 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 pour les renseignements personnels/données, 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. Le chiffrement utilisé pour protéger les renseignements personnels exigera des connaissances et des compétences pour garantir que les renseignements personnels restent protégés contre la menace quantique.

Protection et défense

Cette catégorie de travail soutient les opérations de cybersécurité qui englobent la protection active, la détection des événements, la réponse aux incidents et la récupération des systèmes numériques organisationnels. Bien que des personnes exercent des emplois connexes depuis des décennies, les principaux rôles de travail n'ont pas été identifiés comme des professions, mais ont plutôt été typiquement associés à des groupes professionnels : gestionnaires des systèmes informatiques (CNP 0213); analystes et consultants/consultantes en informatique (2171); et évaluateurs/évaluatrices de systèmes informatiques (2283). Les personnes appartenant à cette catégorie de travail se concentrent donc sur l'exploitation, la maintenance et la gestion des technologies, des processus et du personnel de cybersécurité, ce qui nécessite une expérience unique et des connaissances, compétences et habiletés distinctes qui les différencient de leurs autres collègues des TI.

Les professions suivantes ont été plus clairement définies comme soutenant les opérations de cybersécurité.

- Gestionnaire de la sécurité des systèmes d'information (opérations de cybersécurité)
- Analyste des opérations de cybersécurité (dans le cadre de la NICE, connu sous le nom d'analyste en cyberdéfense)
- Spécialiste du soutien aux infrastructures des opérations de cybersécurité (dans le cadre de la NICE, connu sous le nom de spécialiste du soutien aux infrastructures de cyberdéfense)
- Responsable des incidents de cybersécurité (dans le cadre de la NICE, connu sous le nom de responsable des incidents de cyberdéfense)
- Technicien des opérations de cybersécurité
- Analyste d'évaluation de vulnérabilité
- Testeur de pénétration
- Analyste en investigation informatique numérique (dans le cadre de la NICE, connu sous le nom d'analyste en investigation informatique numérique de la cyberdéfense)

Gestionnaire de la sécurité des systèmes d'information – opérations de cybersécurité

Cadre de référence de la NICE	Supervision et gouvernance, OV-MGT-001, gestionnaire de la sécurité des systèmes d'information
Description fonctionnelle	Le titulaire planifie, organise, dirige, contrôle et évalue les activités du centre des opérations de cybersécurité au sein d'une organisation. Employé dans les secteurs public et privé.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement peuvent entraîner une défaillance catastrophique des systèmes de TI et de données de l'organisation et des conséquences pour les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Le titulaire suit généralement une période de 5 à 10 ans dans des rôles connexes dans les opérations de TI ou de cybersécurité ou dans un emploi similaire. Ce rôle soutient l'augmentation des responsabilités au niveau de la gestion en fonction d'une base technique solide dans les opérations de cybersécurité ou d'un rôle de travail connexe (par exemple, évaluation et gestion de vulnérabilité, investigation informatique numérique, analyse de la cybersécurité).
Autres titres	▪ Gestionnaire des opérations de cybersécurité (GOC) ▪ Gestionnaire des opérations de sécurité (COS) ▪ Gestionnaire de la cybersécurité ▪ Gestionnaire de la sécurité des systèmes d'information (opérations de cybersécurité)
CNP connexes	0213 – Gestionnaires des systèmes informatiques
Tâches	▪ Diriger et gérer le personnel du COS, y compris l'embauche, la formation, le perfectionnement, la gestion du rendement et la réalisation d'examens annuels du rendement ▪ Demeurer à l'affût de la situation de la menace à la cybersécurité et des technologies de sécurité ▪ Élaborer et mettre en œuvre un programme de COS intégré qui répond aux exigences législatives et organisationnelles ▪ Élaborer et publier des mécanismes de gouvernance du COS (politiques, procédures et orientations) ▪ Élaborer et mettre en œuvre un programme de mesure et d'assurance qualité ▪ Surveiller l'efficacité du programme de COS et en rendre compte à la direction générale ▪ Surveiller et gérer les relations avec les fournisseurs de services et de technologies de sécurité ▪ Fournir des évaluations stratégiques sur le contexte des menaces, les tendances technologiques du COS et les technologies de sécurité émergentes ▪ Rechercher et interpréter les renseignements sur la menace en fonction des risques organisationnels ▪ Gérer les événements et incidents de cybersécurité au sein du COS ▪ Fournir des rapports, des exposés et des recommandations fondés sur les risques concernant les événements et incidents de cybersécurité courants et non courants, y compris la réponse aux crises organisationnelles (par exemple, les interruptions des systèmes d'entreprise)

<table>
<tr><td></td><td colspan="2">▪ Diriger et faciliter les leçons apprises, les activités rétrospectives et les meilleures pratiques concernant les événements et incidents liés à la cybersécurité
▪ Élaborer et superviser la mise en œuvre de plans d'action visant à soutenir l'amélioration continue de la position en matière de cybersécurité</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Baccalauréat en informatique ou dans une discipline connexe ou diplôme d'études collégiales dans le domaine des technologies de l'information.</td></tr>
<tr><td>Formation</td><td>Formation aux opérations de cybersécurité avec une certification de niveau industriel dans un domaine connexe (par exemple, sécurité des réseaux, traitement des incidents, détection et atténuation des menaces, investigation informatique numérique).
Formation à la gestion des équipes d'opérations de sécurité, ou perfectionnement et expérience équivalents.
Formation sur les outils et les technologies pertinents pour l'organisation qui soutiennent les opérations de cybersécurité.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience significative (5 à 10 ans) dans le domaine des TI avec 3 à 5 ans d'expérience dans des opérations ou domaine connexe de la cybersécurité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Processus et procédures de gestion des incidents
▪ Systèmes de défense, y compris les pare-feu, les logiciels et les 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</td></tr>
<tr><td>Compétences</td><td colspan="2">Cette profession repose sur les compétences démontrées pour un gestionnaire d'activité ainsi que pour le gestionnaire de la sécurité des systèmes d'information dans le cadre de la NICE. Plus précisément, ce travail exige ce qui suit :

Niveau d'application de base des CCH suivantes :
☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles

Niveau avancé d'application des CCH suivantes :
☐ Menaces et vulnérabilités organisationnelles, y compris :
o Situation de la menace à la cybersécurité et adaptation des processus du COS pour répondre à l'évolution de la menace
o Exigences en matière de gestion de vulnérabilité et gamme des mesures d'atténuation potentielles disponibles lorsqu'il n'existe pas de protocole de gestion de vulnérabilité
☐ Gestion des systèmes défensifs, y compris :
o Pare-feu, antivirus, systèmes de détection et de protection contre les intrusions
o Paramètres manuels et automatisés requis
o Exigences en matière de surveillance, d'essais et de maintenance
☐ Création, mise en œuvre et gestion :</td></tr>
</table>

	○ Processus et politiques de gestion des incidents ○ Responsabilités en matière de gestion des incidents ○ Pratiques de suivi et de signalement des incidents conformément aux exigences législatives et aux politiques organisationnelles ○ Analyses et rapports post-incident ○ Leçons organisationnelles tirées à l'appui de l'amélioration continue ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) : ○ Rôles et responsabilités des contrôles de sécurité des services fournis ○ Rôles et responsabilités du fournisseur dans la gestion et le signalement des incidents ○ Exigences en matière de suivi, d'évaluation et de signalement des incidents pendant le cycle de vie du contrat ○ Responsabilités organisationnelles en réponse à une compromission/un manquement de la part du fournisseur ○ Gestion des communications et des relations avec les fournisseurs en cas de crise ☐ 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) ☐ Maintien d'une plus grande conscience de la situation en matière de sécurité ☐ Conscience de soi concernant les connaissances, les compétences et les habiletés requises pour répondre aux changements commerciaux, techniques et aux menaces ☐ Apprentissage continu pour soutenir l'actualisation des connaissances sur les menaces émergentes, les innovations technologiques en matière de sécurité et l'évolution du paysage de la cybersécurité
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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. Il sera nécessaire de comprendre les capacités de menace quantique et les connaissances et compétences liées à la mise en œuvre d'une stratégie de sécurité quantique.

Analyste des opérations de cybersécurité

Remarque : Ce rôle comprend les rôles suivants :

Analyste de niveau I – analyste des opérations de cybersécurité

Analyste de niveau II – spécialiste des logiciels malveillants

Analyste de niveau III – chercheur de la menace : gestion et défense active

Cadre de référence de la NICE	Protection et défense, analyste en cyberdéfense, PR-CDA-001
Description fonctionnelle	Opérateur de centre des opérations de cybersécurité de première ligne chargé de surveiller et d'entretenir les dispositifs de sécurité des TI et souvent responsable de la détection initiale, de la réponse aux incidents et de leur atténuation
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une défaillance catastrophique des systèmes de TI et de données de l'organisation et des conséquences pour les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Il s'agit d'un emploi de premier échelon commun au sein du centre des opérations de sécurité (COS). Avec une formation et une expérience supplémentaires, il est possible de jouer des rôles plus techniques ou plus opérationnels dans les opérations de cybersécurité (p. ex. l'évaluation et la gestion de vulnérabilité, l'investigation informatique numérique, l'analyse de menace et des logiciels malveillants) ainsi que des possibilités de gestion. Il est à noter que les rôles de niveau II et III peuvent nécessiter une formation et une éducation plus approfondies en plus d'une expérience pertinente. Souvent, un diplôme en informatique ou en génie informatique est une condition préalable étant donné le niveau de connaissances et de compétences requis pour des tâches plus complexes. Toutefois, nombreux sont ceux qui ont progressé de postes d'analystes de la cybersécurité à des rôles avancés dans le domaine de la cybersécurité sans diplôme connexe.
Autres titres	▪ Opérateur du COS ▪ Opérateur de cybersécurité ▪ Analyste de la sécurité des infrastructures ▪ Analyste en sécurité des réseaux ▪ Administrateur de la sécurité des réseaux ▪ Analyste en sécurité des données
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Cibler et analyser les menaces techniques et les vulnérabilités des réseaux ▪ Déterminer, contenir, mener des mesures d'atténuation initiales et signaler les compromissions du système ▪ Examiner, analyser ou appliquer les protocoles de sécurité Internet, les algorithmes cryptographiques, les normes d'annuaire, les protocoles de réseau, le renforcement des réseaux, les contrôles techniques de sécurité des TI, les outils et techniques de sécurité des TI, les systèmes d'exploitation, les systèmes de détection et protection contre les

<table>
<tr><td></td><td colspan="2">intrusions, les pare-feu, les routeurs, les multiplexeurs et les commutateurs, et les dispositifs sans fil
▪ Analyser les données de sécurité et fournir des alertes, des conseils et des rapports
▪ Installer, configurer, intégrer, ajuster, faire fonctionner, surveiller le rendement et détecter les défauts des dispositifs et systèmes de sécurité
▪ Effectuer une analyse d'impact pour les nouvelles implémentations de logiciels, les changements majeurs de configuration et la gestion des correctifs
▪ Développer des modèles de validation et d'essais pour les produits et services de sécurité des TI
▪ Dépanner les produits de sécurité et les incidents
▪ Concevoir/élaborer des protocoles de sécurité des TI
▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques
▪ Élaborer des options et des solutions pour atteindre les objectifs du projet liés à la sécurité
▪ Choisir les produits de sécurité et leur configuration pour répondre aux objectifs du projet liés à la sécurité
▪ Mettre en œuvre et à l'essai les spécifications de configuration
▪ Créer des livres de configuration et de construction opérationnelle
▪ Examiner, élaborer et fournir du matériel de formation pertinent</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme d'études collégiales dans le domaine des technologies de l'information avec une spécialisation en TI/cybersécurité, sécurité des réseaux ou similaire.</td></tr>
<tr><td>Formation</td><td>Formation aux opérations de cybersécurité avec une certification de niveau industriel dans un domaine connexe (par exemple, opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, exploitation d'appareils de sécurité). Une formation spécialisée est nécessaire pour les analystes de niveau II et III.</td></tr>
<tr><td>Expérience professionnelle</td><td>L'expérience initiale requise est d'avoir réussi à travailler dans un environnement de TI et dans une équipe technique.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Processus et procédures de gestion des incidents
▪ Systèmes de défense, y compris les pare-feu, les logiciels et les 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</td></tr>
<tr><td>Compétences</td><td colspan="2">Dans les COS plus importants, il peut y avoir la possibilité de passer d'analyste de niveau 1 à analyste de niveau 2. Les analystes de niveau 3 sont rares et presque exclusivement employés dans des contextes de sécurité nationale et militaire. Les compétences requises pour les niveaux 1 et 2 sont indiquées ci-dessous.

Pour l'analyste des opérations de cybersécurité de niveau 1

Les CCH suivantes sont appliquées à un niveau de base :
☐ Administration et gestion de la sécurité des réseaux
☐ Architecture de sécurité des réseaux
☐ Sécurité du matériel et des microprogrammes</td></tr>
</table>

	☐ Sécurité définie par les logiciels et sécurité des applications ☐ Virtualisation et sécurité des réseaux privés virtuels (VPN) ☐ Sécurité basée sur l'infonuagique ☐ Sécurité des appareils sans fil/mobiles ☐ Zones de sécurité des TI ☐ Chiffrement et cryptographie, y compris les concepts et principes de gestion de clés ☐ Analyse et balayage des vulnérabilités ☐ Outils, processus et procédures de gestion de vulnérabilité ☐ Sécurité des applications Web ☐ Livres de configuration et de construction opérationnelle ☐ Acquisitions de systèmes et projets ☐ Responsabilités juridiques et éthiques associées aux opérations de cybersécurité, y compris la conduite des enquêtes, le respect de la vie privée et la préservation des preuves ☐ Rédaction et exposé sur des questions techniques (par exemple, rapports d'incidents, rapports techniques, etc.) pour une compréhension au niveau de la direction Les CCH suivantes sont appliquées à un niveau avancé : ☐ Concepts, opération et configuration des appareils de sécurité des réseaux (équipements spécifiques en fonction du rôle – systèmes ou appareils de cyberdéfense des réseaux, des serveurs et des postes de travail) ☐ Types d'intrusions et indicateurs de compromission ☐ Sources d'information sur la menace ☐ Tactiques, techniques et procédures (TTP) communes aux acteurs de menace ☐ Processus, responsabilités et autorités de gestion des incidents ☐ Méthodes, outils et systèmes de détection et de prévention d'intrusion ☐ Analyse des intrusions et techniques d'atténuation ☐ Analyse de base des logiciels malveillants **Pour l'analyste de niveau II – spécialiste des logiciels malveillants** Les CCH suivantes sont appliquées à un niveau avancé. Tout ce qui précède, en plus de ce qui suit : ☐ Menaces persistantes et sophistiquées aux TTP ☐ Outils, techniques et procédures de cyberdéfense ☐ Développement et essais des dispositifs de sécurité des réseaux (y compris les scripts et le codage). ☐ Analyse avancée des logiciels malveillants et rétroingénierie des logiciels malveillants ☐ Mise en œuvre des contrôles de sécurité avancés en réponse à des menaces persistantes ☐ Activités avancées de réponse aux incidents et de récupération **Pour l'analyste de niveau III – chercheur de la menace : gestion et défense active** Les CCH suivantes sont appliquées à un niveau avancé : ☐ Gestion avancée des menaces

	☐ TTP avancées pour les acteurs de menace, y compris la spécialisation des acteurs de menace persistante (par exemple, l'État-nation, le crime organisé) ☐ Interprétation/synthèse de renseignements classifiés/sensibles sur la menace provenant de sources multiples ☐ Responsabilités juridiques et éthiques liées aux techniques de défense active ☐ Analyse de l'exploitation ☐ Chasse aux menaces et cadres de défense active ☐ Élaboration de plans d'action complexes, y compris l'évaluation des risques et le plan d'atténuation ☐ Tactiques, outils et procédures de défense active, y compris des contre-mesures et des contre-contre-mesures avancées contre la menace ☐ Pensée antagoniste ☐ Développement, essai et déploiement d'outils techniques dans un cadre de défense active pour protéger les renseignements et les systèmes organisationnels à risque
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 et les réponses potentielles 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 ainsi que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.

Responsable des incidents de cybersécurité

Responsable en cas d'incident relatif à la TO

Cadre de référence de la NICE	Protection et défense, responsable des incidents de cyberdéfense, PR-CIR-001
Description fonctionnelle	Le titulaire fournit des activités de réponse immédiate et détaillée pour atténuer ou limiter les menaces et les incidents liés à la cybersécurité non autorisés au sein d'une organisation. Cela comprend la planification et l'élaboration de plans d'action, la hiérarchisation des activités et le soutien aux opérations de reprise et à l'analyse post-incident.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une défaillance catastrophique des systèmes de TI et de données de l'organisation et des conséquences pour les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Il s'agit d'un emploi de premier échelon commun au sein du centre des opérations de sécurité (COS). Avec une formation et une expérience supplémentaires, il est possible de jouer des rôles plus techniques ou plus opérationnels dans les opérations de cybersécurité, comme l'évaluation et la gestion de vulnérabilité, l'investigation informatique numérique, l'analyse de menace et des logiciels malveillants) ainsi que des possibilités de gestion.
Autres titres	▪ Responsable des incidents de cybersécurité ▪ Responsable d'incidents – centre des opérations de sécurité ▪ Premier intervenant en matière de cybersécurité ▪ Responsable en cas d'incident de sécurité relatif à la technologie opérationnelle
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	Ces tâches s'appliquent aussi bien aux systèmes de TI qu'aux systèmes de TO. ▪ Effectuer des tâches de traitement des incidents de cyberdéfense en temps réel (par exemple, collecte de preuves, corrélation et suivi des intrusions, analyse de la menace et remédiation directe du système) ▪ Effectuer un triage de sécurité pour cibler et analyser les incidents et menaces cybernétiques ▪ Surveiller activement les réseaux et les systèmes pour détecter les incidents et menaces cybernétiques ▪ Procéder à une analyse des risques et à un examen de sécurité des journaux du système afin de repérer les éventuelles cybermenaces ▪ Procéder à des analyses et à des examens ou appliquer des scanneurs de réseau, des outils d'évaluation de vulnérabilité, des protocoles de réseau, des protocoles de sécurité Internet, des systèmes de détection d'intrusion, des pare-feu, des contrôleurs de contenu et des logiciels de point d'extrémité ▪ Collecter et analyser les données pour déterminer les failles et les vulnérabilités de la cybersécurité et formuler des recommandations permettant d'y remédier rapidement ▪ Élaborer et préparer l'analyse et le rapport des incidents de cyberdéfense ▪ Définir et maintenir des ensembles d'outils et des procédures

<table>
<tr><td></td><td colspan="2">▪ Élaborer, mettre en œuvre et évaluer les plans et activités de prévention et de réponse aux incidents, et s'adapter pour contenir, atténuer ou éradiquer les effets des incidents de cybersécurité
▪ Fournir un soutien à l'analyse des incidents dans le cadre des plans et activités de réponse
▪ Mener des activités de recherche et de développement sur les incidents de cybersécurité et les mesures d'atténuation
▪ Créer un plan de développement du programme qui comprend des évaluations des lacunes en matière de sécurité, des politiques, des procédures, des stratégies et des manuels de formation
▪ Examiner, élaborer et fournir du matériel de formation pertinent</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme d'études collégiales dans le domaine des technologies de l'information avec une spécialisation en TI/cybersécurité, sécurité des réseaux ou similaire.</td></tr>
<tr><td>Formation</td><td>Formation aux opérations de cybersécurité avec une certification de niveau industriel dans un domaine connexe (par exemple, opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, exploitation d'appareils de sécurité).

Formation spécialisée requise pour la technologie opérationnelle et les systèmes connexes.</td></tr>
<tr><td>Expérience professionnelle</td><td>L'expérience initiale requise est d'avoir réussi à travailler dans un environnement de TI et dans une équipe technique.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Processus et procédures de gestion des incidents
▪ Systèmes de défense, y compris les pare-feu, les logiciels et les 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</td></tr>
<tr><td>Compétences</td><td colspan="2">Responsable des incidents de cybersécurité
Les CCH suivantes sont appliquées à un niveau de base :
☐ Administration et gestion de la sécurité des réseaux
☐ Architecture de sécurité des réseaux
☐ Sécurité du matériel et des microprogrammes
☐ Sécurité définie par les logiciels et sécurité des applications
☐ Virtualisation et sécurité des VPN
☐ Sécurité basée sur l'infonuagique
☐ Sécurité des appareils sans fil/mobiles
☐ Zones de sécurité des TI
☐ Chiffrement et cryptographie, y compris les concepts et principes de gestion de clés
☐ Analyse et balayage des vulnérabilités
☐ Outils, processus et procédures de gestion de vulnérabilité
☐ Sécurité des applications Web
☐ Livres de configuration et de construction opérationnelle
☐ Acquisitions de systèmes et projets
☐ Responsabilités juridiques et éthiques associées aux opérations de cybersécurité, y compris la conduite des enquêtes, le respect de la vie privée et la préservation des preuves</td></tr>
</table>

	☐ Rédaction et exposé sur des questions techniques (par exemple, rapports d'incidents, rapports techniques, etc.) pour une compréhension au niveau de la direction ☐ Bases de la continuité des activités et de la réponse aux catastrophes Les CCH suivantes sont appliquées à un niveau avancé : ☐ Concepts, opération et configuration des appareils de sécurité des réseaux (équipements spécifiques en fonction du rôle – systèmes ou appareils de cyberdéfense des réseaux, des serveurs et des postes de travail) ☐ Types d'intrusions et indicateurs de compromission ☐ Sources d'information sur la menace ☐ Tactiques, techniques et procédures (TTP) communes aux acteurs de menace ☐ Processus, responsabilités et autorités de gestion des incidents ☐ Méthodes, outils et systèmes de détection et de prévention d'intrusion ☐ Analyse des intrusions et techniques d'atténuation ☐ Analyse de base des logiciels malveillants ☐ Enquêtes de cybersécurité et préservation des preuves **Pour les responsables en cas d'incident relatif à la technologie opérationnelle** En plus des CCH pertinentes ci-dessus, les éléments suivants s'appliquent au niveau de base : ☐ Logiciels et matériel des systèmes de TO, contrôleurs logiques programmables, relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris les implications et l'évaluation des dispositifs IdO) ☐ Exigences juridiques et de conformité, y compris les responsabilités organisationnelles en matière de sécurité du lieu de travail et du public liées à la TO/production ☐ Systèmes de télémétrie, communication de données, acquisition de données et contrôle de processus ☐ Concepts de systèmes d'exploitation, de réseaux et de systèmes de communication ☐ Réseaux de distribution électrique, équipement du système électrique, fonctionnement des stations de transformation et théorie de l'électricité ☐ Applications et systèmes de gestion de bases de données ☐ Mesures ou indicateurs du rendement, de la disponibilité, de la capacité ou des problèmes de configuration du système de TO ☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défauts
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les

	mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 et les réponses potentielles 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 ainsi que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.

Technicien des opérations de cybersécurité

Cadre de référence de la NICE	Protection et défense, PR-INF-001, soutien aux infrastructures de défense en matière de cybersécurité	
Description fonctionnelle	Le titulaire met à l'essai, met en œuvre, déploie, entretient et administre le matériel et les logiciels de l'infrastructure des opérations de sécurité.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une défaillance de sécurité ou une compromission du système qui peut avoir un impact important sur les systèmes, les capacités ou les fonctions informatiques de l'organisation.	
Parcours de perfectionnement	Il s'agit souvent d'un emploi de premier échelon dans le domaine de la sécurité après avoir acquis de l'expérience dans des fonctions techniques, administratives de réseau ou autres fonctions similaires. Avec une formation et une expérience supplémentaires, il existe un potentiel pour des rôles plus techniques ou plus opérationnels ainsi que des possibilités de gestion.	
Autres titres	▪ Spécialiste/technicien du soutien aux infrastructures de sécurité ▪ Analyste des systèmes de sécurité ▪ Technicien en systèmes de sécurité ▪ Analyste du contrôle de la sécurité	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2281 – Techniciens/techniciennes de réseau informatique 2282 – Agents/agentes de soutien aux utilisateurs	
Tâches	▪ Surveiller activement le rendement du système de sécurité, dépanner et résoudre les problèmes d'interopérabilité matérielle ou logicielle, ainsi que les pannes et les défauts du système ▪ Installer, configurer et entretenir les logiciels, le matériel et les équipements périphériques du système de sécurité ▪ Élaborer, rédiger et tenir à jour des rapports d'incidents et des évaluations de vulnérabilité et d'impact ▪ Développer et maintenir une base de données de suivi et de solutions ▪ Analyser et recommander des améliorations et des changements pour soutenir l'amélioration des opérations de sécurité ▪ Auditer, enregistrer et signaler des activités de gestion du cycle de vie ▪ Administrer les comptes, les privilèges et l'accès aux systèmes et équipements de sécurité ▪ Effectuer la gestion des actifs ou le contrôle de l'inventaire des ressources des systèmes et des équipements ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs	
Qualifications requises	Éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)
	Formation	Formation aux systèmes de cybersécurité, au fonctionnement des systèmes de sécurité et aux outils basés sur les fournisseurs (par exemple, systèmes de détection des intrusions, pare-feu, antivirus, gestion des incidents, etc.)

	Expérience professionnelle	2 à 3 ans dans l'exploitation et la sécurité des réseaux
Outils et technologie	▪ Outils, journaux et procédures des systèmes de cybersécurité ▪ Politiques et directives organisationnelles ▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents	
Compétences	Les CCH s'appliquent au niveau de base : ☐ Menaces pour les systèmes d'information et leur sécurité ☐ Concepts, protocoles, composants et principes de l'architecture de sécurité des réseaux (par exemple, application de la défense en profondeur) ☐ Techniques de base de renforcement des systèmes, des réseaux et des systèmes d'exploitation ☐ Enregistrements et modes de transmission (par exemple, Bluetooth, identification par radiofréquence [RFID], réseau infrarouge [RI], technologie Wi-Fi, radiomessagerie, cellulaire, antennes paraboliques, voix par IP [VoIP]) ☐ Analyse du trafic du réseau (outils, méthodologies, processus) ☐ Architectures et normes de gestion de l'identité, des justificatifs d'identité et de l'accès ☐ Politique, procédures et pratiques de gestion des incidents de cybersécurité ☐ Analyse organisationnelle des tendances des utilisateurs et des affaires ☐ Consultation des clients et résolution des problèmes Les CCH sont appliquées à un niveau avancé : ☐ Procédures, principes et méthodologies d'essai des systèmes de cybersécurité ☐ Outils et applications du système de détection d'intrusion (SDI)/système de prévention d'intrusion (SPI) ☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ☐ Dépannage, analyse et réparation des infrastructures de cybersécurité ☐ Politiques, gestion des comptes et contrôles des systèmes de cybersécurité	
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités dans la gestion des systèmes de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans les processus de gestion de l'identité et de l'accès, y compris les changements techniques et de processus connexes.	

	▪ 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 et les réponses potentielles 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 ainsi que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.

Analyste d’évaluation de vulnérabilité

Cadre de référence de la NICE	Protection et défense, PR-VAM-001, analyste d’évaluation de vulnérabilité (VA)	
Description fonctionnelle	Le titulaire balaye les applications et les systèmes d’exploitation pour repérer les failles et les vulnérabilités; et effectue et présente des évaluations de vulnérabilité des réseaux et des systèmes d’une organisation.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d’attention aux détails ou le mauvais jugement peuvent entraîner une mauvaise identification ou une non-détection des vulnérabilités qui pourraient être comprises. Cela peut avoir un impact important sur les systèmes, les capacités et les fonctions informatiques de l’organisation.	
Parcours de perfectionnement	Il s’agit souvent d’un poste de niveau 2 dans un environnement des opérations de cybersécurité qui est normalement précédé de 2 à 3 ans dans un rôle de sécurité des réseaux ou de sécurité opérationnelle. Cela peut conduire à une spécialisation accrue comme analyste de vulnérabilité, chef d’équipe rouge/bleu, testeur de pénétration ou rôles de gestion.	
Autres titres	▪ Testeur de vulnérabilité ▪ Évaluateur de vulnérabilité ▪ Gestionnaire de l’évaluation de vulnérabilité	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel	
Tâches	▪ Repérer les failles critiques des applications et des systèmes que les cyberacteurs pourraient exploiter ▪ Effectuer des évaluations de vulnérabilité des technologies concernées (par exemple, l’environnement informatique, le réseau et l’infrastructure de soutien, et les applications) ▪ Préparer et présenter des évaluations complètes de vulnérabilité ▪ Effectuer des audits et des balayages de sécurité des réseaux ▪ Maintenir un ensemble d’outils d’audit de cyberdéfense déployables (par exemple, des logiciels et du matériel spécialisés de cyberdéfense) pour soutenir les opérations de cyberdéfense ▪ Préparer des rapports d’audit qui tirent des conclusions techniques et procédurales, et faire des recommandations sur les stratégies et solutions correctives ▪ Mener ou soutenir les essais de pénétration autorisés sur les réseaux et systèmes des organisations ▪ Définir et revoir les exigences relatives aux solutions de sécurité de l’information ▪ Formuler des recommandations sur la sélection de contrôles de sécurité rentables pour atténuer les risques ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs	
Qualifications requises	Éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)
	Formation	Formation aux systèmes de cybersécurité, à l’évaluation et à l’analyse de vulnérabilité. Formation

		au système de vulnérabilité basé sur les fournisseurs.
	Expérience professionnelle	2 à 3 ans dans un rôle d'opérations de réseau ou de cybersécurité.
Outils et technologie	▪ Politiques, procédures et pratiques de sécurité organisationnelle ▪ Outils d'évaluation de vulnérabilité ▪ Politiques, processus et pratiques de gestion de vulnérabilité ▪ Bases de données des vulnérabilités communes	
Compétences	Les CCH s'appliquent au niveau de base : ☐ Outils, techniques et protocoles évolués pour les acteurs de menace ☐ Principes, outils et techniques d'essais de pénétration ☐ Processus de gestion des risques pour l'évaluation et l'atténuation des risques ☐ Concepts d'administration du système ☐ Concepts de gestion de la cryptographie et des clés cryptographiques ☐ Cryptologie ☐ Détermination des problèmes de sécurité sur la base de l'analyse de vulnérabilité et des données de configuration ☐ Politiques, processus et pratiques de gestion de vulnérabilité Les CCH sont appliquées à un niveau avancé : ☐ Planification et programmation d'évaluation de vulnérabilité, y compris les risques et les mesures d'atténuation du système ☐ Menaces à la sécurité des systèmes et des applications et vulnérabilités ☐ Techniques de renforcement de la sécurité de l'administration du système, du réseau et des systèmes d'exploitation ☐ Analyse des paquets à l'aide d'outils appropriés ☐ Exécution de balayages des vulnérabilités et reconnaissance des vulnérabilités des systèmes de sécurité ☐ Réalisation d'évaluations de la vulnérabilité/des impacts/des risques ☐ Examen des journaux du système pour identifier les preuves d'intrusions passées ☐ Utilisation d'outils d'analyse de réseau pour déterminer les vulnérabilités	
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront	

	intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 et les réponses potentielles 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, à la compréhension des vulnérabilités du système et à la manière d'atténuer les menaces liées à la sécurité quantique.

Testeur de pénétration

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire effectue des essais formels et contrôlés et des évaluations de la sécurité physique des applications, réseaux et autres systèmes basés sur le Web, selon les besoins, afin de déterminer et d'exploiter les vulnérabilités de sécurité.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou le mauvais jugement peuvent entraîner une mauvaise identification ou une non-détection des vulnérabilités qui pourraient être comprises. Cela peut avoir un impact important sur les systèmes, les capacités et les fonctions informatiques de l'organisation.
Parcours de perfectionnement	Il s'agit souvent d'un poste de niveau 2 ou 3 dans un environnement des opérations de cybersécurité qui est normalement précédé d'une expérience importante (3 à 5 ans) dans un rôle d'opérations de cybersécurité, y compris un emploi dans l'analyse de vulnérabilité, l'analyse des logiciels malveillants ou l'analyse technique des systèmes de sécurité. Il s'agit d'un rôle technique avancé, qui peut conduire à une spécialisation technique croissante, à des rôles de direction ou de gestion d'une équipe rouge.
Autres titres	▪ Spécialiste d'essai et d'évaluation de sécurité ▪ Analyste spécialisé dans l'évaluation de la vulnérabilité
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Effectuer des essais de pénétration sur les applications Web, les connexions réseau et les systèmes informatiques afin de cibler les cybermenaces et les vulnérabilités techniques

<table>
<tr><td></td><td colspan="2">▪ Effectuer des évaluations de la sécurité physique du réseau, des dispositifs, des serveurs et des systèmes d'une organisation
▪ Développer des essais de pénétration et les outils nécessaires à leur exécution (par exemple, normes, risques, atténuations)
▪ Rechercher des vulnérabilités et des faiblesses de sécurité inconnues dans les applications Web, les réseaux et les systèmes pertinents que les cyberacteurs peuvent facilement exploiter
▪ Élaborer et tenir à jour des documents sur les résultats des activités d'essais de pénétration
▪ Recourir à l'ingénierie sociale pour découvrir les lacunes en matière de sécurité
▪ Définir et revoir les exigences relatives aux solutions de sécurité de l'information
▪ Analyser, documenter et partager les résultats en matière de sécurité avec la direction et le personnel technique
▪ Fournir des recommandations et des lignes directrices sur la manière d'améliorer les pratiques de sécurité organisationnelle
▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)</td></tr>
<tr><td>Formation</td><td>Formation aux outils, techniques et procédures d'analyse de la vulnérabilité et d'essais de pénétration.</td></tr>
<tr><td>Expérience professionnelle</td><td>2 à 3 ans d'expérience dans un rôle avancé d'opérations de cybersécurité, de préférence avec une expérience en évaluation de vulnérabilité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Politiques, procédures et pratiques de sécurité organisationnelle
▪ Carte des systèmes organisationnels et architecture de réseau
▪ Outils d'évaluation de vulnérabilité
▪ Politiques, processus et pratiques de gestion de vulnérabilité
▪ Bases de données des vulnérabilités communes
▪ Outils et protocoles d'essais de pénétration</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH sont appliquées à un niveau avancé :
☐ Architecture de sécurité des réseaux
☐ Outils, techniques et protocoles évolués pour les acteurs de menace
☐ Principes, outils et techniques d'essais de pénétration
☐ Processus de gestion des risques pour l'évaluation et l'atténuation des risques
☐ Concepts d'administration du système
☐ Concepts de gestion de la cryptographie et des clés cryptographiques
☐ Cryptologie
☐ Détermination des problèmes de sécurité sur la base de l'analyse de vulnérabilité et des données de configuration
☐ Politiques, processus et pratiques de gestion de vulnérabilité
☐ Planification et programmation des essais de pénétration, y compris les risques et les mesures d'atténuation du système
☐ Menaces à la sécurité des systèmes et des applications et vulnérabilités
☐ Techniques de renforcement de la sécurité de l'administration du système, du réseau et des systèmes d'exploitation</td></tr>
</table>

	☐ Analyse des paquets à l'aide d'outils appropriés ☐ Exécution de balayages des vulnérabilités et reconnaissance des vulnérabilités des systèmes de sécurité ☐ Réalisation d'évaluations de la vulnérabilité/des impacts/des risques ☐ Examen des journaux du système pour identifier les preuves d'intrusions passées ☐ Utilisation d'outils d'analyse de réseau pour déterminer les vulnérabilités
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 et les réponses potentielles 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, à la compréhension des vulnérabilités du système et à la manière d'atténuer les menaces liées à la sécurité quantique.

Analyste en investigation informatique numérique

Cadre de référence de la NICE	Enquête, analyste en investigation informatique de cyberdéfense, INV-FOR-002
Description fonctionnelle	**La description suivante, basée sur les rôles, concerne uniquement les opérations de sécurité et ne comprend pas les fonctions d'investigation informatique numérique ou d'audit qui sont prévues dans le cadre des professions connexes liées à l'application de la loi ou à l'audit**. Le titulaire effectue des investigations informatiques numériques pour analyser les preuves provenant d'ordinateurs, de réseaux et d'autres dispositifs de stockage de données. Il s'agit notamment d'enquêter sur les preuves électroniques et de les conserver, de planifier et de développer des outils, de hiérarchiser les activités et de soutenir les opérations de reprise et l'analyse après l'incident.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner l'incapacité à déterminer la source et à atténuer une compromission, mais peuvent également avoir des répercussions sur les systèmes d'information des organisations, notamment en ce qui concerne les accusations criminelles ou les litiges civils.
Parcours de perfectionnement	Il s'agit souvent d'un poste de niveau 2/3 dans un environnement des opérations de cybersécurité qui est normalement précédé d'un minimum de 2 à 3 ans dans un rôle de sécurité des réseaux ou de sécurité opérationnelle, y compris analyste des logiciels malveillants. Cela peut conduire à une spécialisation accrue dans les activités d'investigation informatique numérique ou d'évaluation de la sécurité, ainsi qu'à des rôles de chef d'équipe rouge/bleue, de testeur de pénétration ou de gestionnaire.
Autres titres	▪ Investigateur en investigation informatique numérique (normalement réservé à l'environnement de la cybercriminalité) ▪ Examinateur en investigation informatique numérique (normalement réservé aux environnements de cyberaudit)
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Effectuer des enquêtes en temps réel sur les incidents de cyberdéfense (par exemple, collectes de preuves, corrélation et suivi des intrusions, et analyse des menaces) ▪ Enquêter sur les incidents de sécurité conformément au mandat ▪ Planifier des activités d'investigation informatique numérique pour les cyberincidents ▪ Collecter et analyser les artefacts d'intrusion (par exemple, le code source, les logiciels malveillants et la configuration du système) et utiliser les données découvertes pour permettre d'atténuer les incidents potentiels de cyberdéfense ▪ Identifier et rendre compte avec précision des artefacts d'investigation informatique numérique ▪ Capturer et analyser le trafic du réseau associé aux activités malveillantes à l'aide d'outils de surveillance du réseau

<table>
<tr><td></td><td colspan="2">▪ Contribuer à la post-analyse des incidents de sécurité et formuler des recommandations basées sur les activités d'investigation
▪ Élaborer et tenir à jour des rapports d'enquête et des rapports techniques
▪ Fournir une assistance technique sur les questions de preuves numériques au personnel approprié
▪ Rassembler des preuves pour les affaires judiciaires et fournir des témoignages d'experts lors des procédures judiciaires
▪ Gérer les preuves numériques conformément aux exigences appropriées de la chaîne de possession
▪ Établir et gérer une infrastructure/un laboratoire d'analyse sécurisé
▪ Exploiter des systèmes d'investigation informatique numérique (selon les besoins et les fonctions et systèmes disponibles)
▪ Préparer et examiner les politiques, normes, procédures et lignes directrices en matière d'investigation
▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)</td></tr>
<tr><td>Formation</td><td>Formation aux outils, techniques et procédures d'investigation informatique numérique. En outre, en fonction du contexte technique de l'organisation et des systèmes/dispositifs utilisés, une formation spécialisée en matière d'investigation informatique numérique peut être nécessaire (par exemple, appareil mobile, média numérique, etc.)</td></tr>
<tr><td>Expérience professionnelle</td><td>2 à 3 ans d'expérience dans un rôle avancé d'opérations de cybersécurité, de préférence avec une expérience de l'analyse des logiciels malveillants dans des environnements actifs et de la « boîte morte ».</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Politiques, procédures et pratiques de sécurité organisationnelle
▪ Carte des systèmes organisationnels et architecture de réseau
▪ Outils, techniques et procédures d'investigation informatique numérique
▪ Outils d'analyse des logiciels malveillants
▪ Système de gestion des événements et incidents de sécurité
▪ Bases de données des vulnérabilités communes
▪ Mandats, responsabilités et limites de l'autorité en matière d'enquêtes de sécurité</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH sont appliquées à un niveau avancé :
☐ Outils, techniques et procédures des acteurs de menace
☐ Méthodes de réponse aux incidents et de traitement des incidents
☐ Système de gestion des événements et incidents de sécurité
☐ Méthodes, processus et pratiques d'investigation informatique numérique
☐ Tactiques, techniques et procédures de lutte contre la cybercriminalité
☐ Processus de collecte, d'emballage, de transport et de stockage des preuves électroniques pour éviter l'altération, la perte, les dommages physiques ou la destruction des données
☐ Capture et préservation des preuves numériques</td></tr>
</table>

	☐ Lois, règlements, politiques et éthiques applicables en matière d'enquêtes et de gouvernance ☐ Règles juridiques de preuve et procédures judiciaires, présentation de preuves numériques, témoignage en tant que témoin expert ☐ Expertise judiciaire spécifique à un système ou à un appareil (par exemple, mémoire, directeur actif, appareil mobile, réseau, ordinateur [boîte morte], etc.) ☐ Outils et techniques d'analyse des logiciels malveillants ☐ Rétroingénierie ☐ Capacités déployables en matière d'investigation informatique numérique ☐ Types d'investigation informatique numérique, y compris les outils, les techniques et les procédures (en fonction de l'organisation et du système d'information) qui peuvent inclure les investigations informatiques numériques suivantes : o l'ordinateur o le réseau et le répertoire actif o les appareils mobiles o les médias numériques (image, vidéo, audio) o la mémoire
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités dans la gestion des systèmes de cybersécurité. ▪ 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 de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans les processus de gestion de l'identité et de l'accès, y compris les changements techniques et de processus connexes. ▪ 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 et les réponses potentielles 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 ainsi que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.

Annexe B – Rôles de la cybersécurité en matière de sécurité nationale et d'application de la loi

Comme indiqué précédemment, voici un résumé des rôles de la cybersécurité qui sont généralement exercés dans le cadre des professions liées à la sécurité nationale, à l'armée, au renseignement et à l'application de la loi. Peu fréquents sur le marché du travail canadien, ces extraits sont tirés directement du supplément américain de la NICE qui énumère les rôles et les tâches professionnelles.

En particulier, les personnes qui remplissent ces rôles proviennent généralement d'un groupe de main-d'œuvre plus large, sur la base d'une expérience connexe et de la preuve de compétences appropriées, puis elles participent à une formation et à un enseignement spécifiques au domaine par l'intermédiaire de l'employeur qui fixe également les normes requises. Par exemple, les personnes employées dans des rôles techniques, comme analyste de l'exploitation ou cyberopérateur, sont souvent issues du domaine d'activité/des catégories de travail de la protection et de la défense, ou bénéficient d'une formation et d'études pour assumer leurs responsabilités supplémentaires au sein de leur organisation, sur la base de normes professionnelles définies (par exemple, militaires, renseignement, police, etc.).

Analyse (AN)			
Analyse de menace (TWA)	Analyste de la menace/des avertissements	Développe des cyberindicateurs pour maintenir la conscience de l'état de l'environnement opérationnel hautement dynamique. Collecte, traite, analyse et diffuse les évaluations des cybermenaces/avertissements.	AN-TWA-001
Analyse de l'exploitation (EXP)	Analyste de l'exploitation	Collabore à la détermination des lacunes en matière d'accès et de collecte qui peuvent être comblées par des activités de cybercollecte ou de préparation. Exploite toutes les ressources autorisées et les techniques analytiques pour pénétrer les réseaux ciblés.	AN-EXP-001

Analyse toutes sources (ASA)	Analyste toutes sources	Analyse les données/renseignements provenant d'une ou de plusieurs sources pour effectuer la préparation de l'environnement, répond aux demandes d'information et soumet les exigences de collecte et de production de renseignements à l'appui de la planification et des opérations.	AN-ASA-001
	Spécialiste de l'évaluation des missions	Élabore des plans d'évaluation et des mesures du rendement/de l'efficacité. Effectue des évaluations de l'efficacité stratégique et opérationnelle en fonction des besoins des cyberévénements. Détermine si les systèmes ont fonctionné comme prévu et contribue à la détermination de l'efficacité opérationnelle.	AN-ASA-002
Cibles (TGT)	Développeur cible	Effectue l'analyse des systèmes cibles, construit ou maintient des dossiers de cibles électroniques pour inclure les apports de la préparation de l'environnement, ou des sources de renseignement internes ou externes. Coordonne les activités des partenaires cibles et des organismes de renseignement et présente les cibles candidates pour vérification et validation.	AN-TGT-001
	Analyste de réseau cible	Effectue une analyse avancée de la collecte et des données de source ouverte afin d'assurer la continuité des cibles, de dresser le profil des cibles et de leurs activités et de développer des techniques pour obtenir davantage de renseignements sur les cibles. Détermine la façon dont les cibles communiquent, se déplacent, fonctionnent et vivent en fonction de la connaissance des technologies cibles, des réseaux numériques et des applications qui s'y rattachent.	AN-TGT-002

Analyse linguistique (LNG)	Analyste linguistique pluridisciplinaire	Applique une expertise linguistique et culturelle avec des connaissances sur les cibles/menaces et des connaissances techniques pour traiter, analyser ou diffuser des renseignements dérivés du langage, de la voix ou de matériel graphique. Crée et maintient des bases de données et des outils de travail spécifiques à chaque langue pour soutenir l'exécution de cyberopératioons et assurer le partage des connaissances essentielles. Fournit une expertise dans le cadre de projets à forte intensité linguistique ou interdisciplinaires.	AN-LNG-001
Collecte et exploitation (CO)			
Opérations de collecte (CLO)	Gestionnaire de la collecte toutes sources	Détermine les autorités de collecte et l'environnement, intègre les besoins prioritaires en matière d'information dans la gestion de la collecte, développe des concepts pour répondre à l'intention des dirigeants. Détermine les capacités des ressources de collecte disponibles, établit les nouvelles capacités de collecte et élabore et diffuse des plans de collecte. Surveille l'exécution de la collecte confiée afin de garantir l'exécution efficace du plan de collecte.	CO-CLO-001
	Gestionnaire des exigences en matière de collecte toutes sources	Évalue les opérations de collecte et élabore des stratégies d'exigences de collecte basées sur les effets en utilisant les sources et les méthodes disponibles pour améliorer la collecte. Élabore, traite, valide et coordonne la soumission des exigences de collecte. Évalue le rendement des actifs et des opérations de collecte.	CO-CLO-002

Planification des cyberopérations (OPL)	Planificateur du cyberespionnage	Élabore des plans de renseignement détaillés pour répondre aux besoins des cyberopérations. Collabore avec les planificateurs des cyberopérations pour déterminer, valider et prélever les besoins de collecte et d'analyse. Participe à la sélection, la validation, la synchronisation et l'exécution des cyberopérations. Synchronise les activités de renseignement pour soutenir les objectifs organisationnels dans le cyberespace.	CO-OPL-001
	Planificateur de cyberopérations	Élabore des plans détaillés pour la conduite ou le soutien de la gamme applicable de cyberopérations en collaborant avec d'autres planificateurs, opérateurs ou analystes. Participe à la sélection, la validation et la synchronisation des cibles et permet l'intégration pendant l'exécution des cyberopérations.	CO-OPL-002
	Planificateur d'intégration des partenaires	S'emploie à faire progresser la coopération entre les partenaires des cyberopérations au-delà des frontières organisationnelles ou nationales. Aide à l'intégration des cyberéquipes partenaires en fournissant des conseils, des ressources et une collaboration pour développer les meilleures pratiques et faciliter le soutien organisationnel pour atteindre les objectifs des cyberopérations intégrées.	CO-OPL-003
Cyberopérations (OPS)	Cyberopérateur	Effectue la collecte, le traitement ou la géolocalisation de systèmes pour exploiter, localiser ou suivre des cibles d'intérêt. Effectue la navigation sur le réseau, l'analyse tactique d'investigation informatique, et, lorsqu'on le lui demande, exécute des opérations sur le réseau.	CO-OPS-001

Enquête (IN)			
Cyberenquête (INV)	Enquêteur sur la cybercriminalité	Détermine, recueille, examine et conserve les preuves en utilisant des techniques d'analyse et d'enquête contrôlées et documentées.	IN-INV-001
Investigation informatique numérique (FOR)	Analyste en investigation informatique de contre-ingérence/d'application de la loi	Mène des enquêtes détaillées sur les crimes informatiques en établissant des preuves documentaires ou physiques, y compris les médias numériques et les journaux associés aux incidents de cyberintrusion.	IN-FOR-001
	Analyste en investigation informatique de cyberdéfense	Analyse les preuves numériques et enquête sur les incidents de sécurité informatique pour en tirer des renseignements utiles à l'appui de l'atténuation de la vulnérabilité des systèmes/réseaux.	IN-FOR-002

Annexe C – Rôles adjacents à la cybersécurité au sein des organisations

En plus des rôles **principaux** qui définissent la profession en cybersécurité dont il est question dans cette NPN, il existe un certain nombre de rôles **adjacents** qui ont des responsabilités en matière de cybersécurité qui ne constituent normalement qu'une partie de leurs responsabilités générales au sein d'une organisation. Bien qu'ils soient souvent employés dans le domaine de la cybersécurité qu'à temps partiel, la portée et l'étendue dans laquelle ils remplissent ces rôles varient en fonction de la taille de l'organisation, du type et du degré d'infrastructure informatique ou Internet. Par exemple, pour les grandes organisations qui utilisent les technologies de l'information, tous les rôles suivants peuvent s'appliquer. Pour les petites organisations qui ne dépendent pas trop des TI ou de la connectivité Internet pour la conduite de leurs affaires, il est probable qu'une majorité de l'expertise et des services techniques seront externalisés. En conséquence, les autres responsabilités non techniques en matière de cybersécurité seront réparties au sein de l'organisation.

Ce tableau présente brièvement les rôles adjacents communs en matière de cybersécurité[9], l'ID NICE correspondante le cas échéant, la CNP associée et les principales responsabilités en matière de cybersécurité. En supposant que la majorité des personnes occupant ces fonctions possèdent déjà les compétences requises pour leurs rôles et fonctions principaux, seules les fonctions de cybersécurité sont dotées de compétences clés.[10] Plus précisément, pour la communauté de la main-d'œuvre existante et en particulier, les éducateurs, ceux-ci devraient orienter la discussion sur l'adaptation des programmes de formation et d'éducation afin de mieux refléter les réalités de la cybersécurité sur le marché du travail canadien.

[9] D'autres rôles seront ajoutés au fur et à mesure de leur détermination ou de leur émergence et suivront le processus de mise à jour de la NPN décrit dans la section *Examen et révision* présentée plus haut dans ce document.

[10] Le préfixe « cyber » indique une spécialisation dans le domaine cybernétique, mais tous les postes ci-dessous sont censés avoir les compétences requises pour soutenir leur fonction organisationnelle principale. Par exemple, un cyberinstructeur est censé avoir toutes les compétences nécessaires pour soutenir l'enseignement en plus de la connaissance/l'expérience du domaine cybernétique.

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
Supervision et gouvernance	Directeur général/haute direction/propriétaire	OV-EXL-001	0012 0013	Exécute les pouvoirs de décision et établit une vision et une orientation pour les ressources ou les opérations cybernétiques et connexes d'une organisation.	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité
	Directeur de l'informatique/directeur de la technologie	Aucune	0012 0013 0211 0213	Dirige et exécute les pouvoirs décisionnels liés aux TI organisationnelles, à l'infrastructure et aux services techniques. Cela inclut souvent les services de cybersécurité.	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Cyberconseiller juridique	OV-LGA-001	4112 4211	Fournit des conseils juridiques et des recommandations sur des sujets pertinents liés au droit de la cybernétique.	Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contexte de menace

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Agent de protection de la vie privée/gestionnaire du respect de la vie privée	OV-LGA-002	0213	Élabore et supervise le programme de respect de la vie privée et le personnel chargé de ce programme, en soutenant les besoins des responsables de la protection de la vie privée et de la sécurité et de leurs équipes en matière de conformité, de gouvernance/politique et de réponse aux incidents.	Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contexte de menace Contrôles de sécurité relatifs à la protection de la vie privée
	Gestionnaire de la sécurité des communications (SECOM)	OV-MGT-002	0131 0213	Personne qui gère les ressources de sécurité des communications (SECOM) d'une organisation (CNSSI 4009) ou le gardien des clés d'un système de gestion de clés de chiffrement	Gestion du programme de sécurité PCA/PIC Gestion des risques liés à la chaîne d'approvisionnement Politiques, lignes directrices et exigences de gestion de la SECOM Comptabilité de la SECOM Infrastructure et applications de chiffrement/d'ICP Gestion des incidents de la SECOM
	Développeur et gestionnaire de la main-d'œuvre du cyberespace	OV-SPP-001	4156	Élabore des plans, des stratégies et des orientations pour la main-d'œuvre du cyberespace afin de répondre aux besoins en matière de main-d'œuvre, de personnel, de formation et d'éducation et de tenir compte des changements apportés à la politique, à la doctrine, au matériel, à la structure des forces et aux besoins en matière d'éducation et de formation dans le cyberespace.	Parcours professionnel dans le domaine de la cybersécurité Sources et renseignements sur le marché du travail en cybersécurité Normes professionnelles en matière de cybersécurité Certifications et accréditations de cybersécurité Évaluation des compétences en matière de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Développeur de programmes d'enseignement en ligne	OV-TEA-001	4011 4021 4216	Élabore, planifie, coordonne et évalue les cours, méthodes et techniques de cyberformation/d'éducation en fonction des besoins pédagogiques.	Connaissance pertinente du domaine cybernétique (par thème) Évaluation des compétences en matière de cybersécurité
	Cyberinstructeur	OV-TEA-002	4011 4021 4216	Élabore et mène la formation ou l'éducation du personnel dans le domaine cybernétique.	Connaissance pertinente du domaine cybernétique (par thème) Évaluation des compétences en matière de cybersécurité
	Planificateur de cyberpolitiques et de stratégies	OV-SPP-002	0412 4161	Élabore et maintient des plans, une stratégie et une politique de cybersécurité pour soutenir les initiatives organisationnelles de cybersécurité et la conformité réglementaire, et s'y aligner.	Gestion du programme de cybersécurité PCA/PIC Contexte juridique et politique du cyberespace Contexte d'entreprise et de menace Planification et développement de la cyberpolitique Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Gestionnaire de programme	OV-PMA-001	0012 0013 0211	Dirige, coordonne, communique et intègre la réussite globale du programme, et en est responsable, en veillant à l'alignement avec les priorités de l'agence ou de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Gestion du programme de cybersécurité PCA/PIC Gestion des risques liés à la chaîne d'approvisionnement Modèles de cybermaturité Normes de cybersécurité Évaluation et mesure de la cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Chef de projet des TI	OV-PMA-002	0211 0213	Gère directement les projets de technologie de l'information.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes Gestion de projets de cybersécurité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Gestionnaire du soutien des produits	OV-PMA-003	0211 0213	Gère l'ensemble des fonctions de soutien nécessaires pour mettre en œuvre et maintenir l'état de préparation et la capacité opérationnelle des systèmes et des composants.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes Gestion de projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Processus d'essais et d'évaluation des produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Gestionnaire d'investissement/de portefeuille de TI	OV-PMA-004	0211 0213	Gère un portefeuille d'investissements dans les TI qui s'alignent sur les besoins globaux de la mission et les priorités de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Gestion du programme de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Modèles de cybermaturité Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Auditeur de programmes de TI	OV-PMA-005	0211 0213	Effectue des évaluations d'un programme de TI ou de ses composantes individuelles pour déterminer la conformité aux normes publiées.	Politiques, pratiques et procédures d'audit de cybersécurité Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Contexte juridique et politique Exigences de conformité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Évaluation de vulnérabilité Processus d'essai et d'évaluation de la cybersécurité
	Analyste commercial	Aucune	1122 2171 4162	Analyse et détermine les besoins, recommande des solutions qui apportent une valeur commerciale aux parties prenantes.	Gouvernance, rôles et responsabilités de la cybersécurité Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Contexte juridique et politique Exigences de conformité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Évaluation de vulnérabilité Processus d'essai et d'évaluation de la cybersécurité
	Analyste financier	Aucune	1112	Collecte et analyse les renseignements financiers et les risques. Fournit des estimations, des prévisions et des tendances financières connexes. Fournit des	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				conseils pour soutenir les activités financières et d'investissement.	Contexte juridique, politique et financier Exigences du programme de cybersécurité Approvisionnement et acquisition dans le domaine de la cybersécurité Évaluation et mesure de la cybersécurité
	Analyste des risques	Aucune	1112 4162	Collecte et analyse les risques organisationnels. Fournit des évaluations des risques connexes et des conseils sur les mesures d'atténuation.	Gestion des risques liés à la cybersécurité Méthodes d'évaluation de la menace et des risques Contexte d'entreprise et de menace Contexte juridique, politique et financier Exigences du programme de cybersécurité
	Spécialiste de la communication	Aucune	0124 1123	Planifie, organise et développe la publicité, le marketing et les relations publiques.	Contexte de la cybermenace Contexte juridique et politique Exigences de conformité PCA/PIC Communications lors d'un cyberincident (communications de crise)
	Webmestre/gestionnaire des communications en ligne	Aucune	2175	Recherche, conceptualise, développe et produit des sites Internet et intranet et de médias basés sur le Web.	Menaces à la cybersécurité Vulnérabilités des applications Web Essai et évaluation de logiciels Exigences en matière de réponse aux incidents de cybersécurité
	Spécialiste de l'apprentissage et du développement	Aucune	4011 4021 4216	Élabore, planifie, coordonne et évalue les programmes et activités d'apprentissage et de	Exigences organisationnelles en matière de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				perfectionnement organisationnel et individuel	Rôles et responsabilités en matière de cybersécurité Parcours professionnel dans le domaine de la cybersécurité Évaluation des compétences en matière de cybersécurité
	Planificateur de continuité des activités et de résilience	Aucune	1112 2171	Détermine, coordonne et supervise l'élaboration d'un plan de continuité des activités afin de soutenir la résilience de l'organisation face à la fraude, à la criminalité financière, aux cyberattaques, au terrorisme et aux défaillances des infrastructures.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Exigences organisationnelles en matière de cybersécurité Rôles et responsabilités en matière de cybersécurité Plans, processus et procédures de cybersécurité Gestion des incidents de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Spécialiste de l'approvisionnement	Aucune	1225	Détermine et acquiert des équipements généraux et spécialisés, des matériaux, des droits fonciers ou d'accès et des services commerciaux pour leur utilisation ou leur transformation ultérieure par leur organisation.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Gestion de projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Contrôles de cybersécurité (de gestion, opérationnels, techniques) Processus d'essais et d'évaluation des produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
Conception et développement (Fourniture sécurisée dans la NICE)	Autorisateur (souvent le DI ou le propriétaire du système)	SP-RSK-001	0012 0013 0211	Haut fonctionnaire ou cadre supérieur ayant le pouvoir d'assumer officiellement la responsabilité de l'exploitation d'un système d'information à un niveau de risque acceptable pour les opérations organisationnelles (y compris la mission, les fonctions, l'image ou la réputation), les actifs de l'organisation, les personnes, les autres organisations et la nation (CNSSI 4009).	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Architecte d'entreprise	SP-ARC-001	0211 2147	Développe et maintient des processus d'affaires, des systèmes et des processus d'information pour soutenir les besoins de la mission de l'entreprise; développe des règles et des exigences en matière de technologie de l'information (TI) qui décrivent les architectures de base et cibles.	Cyberobjectifs organisationnels Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Intégration des cybersystèmes Chiffrement/ICP
	Développeur de logiciels	SP-DEV-001	2241 2233 2243	Développe, crée, entretient et écrit/code de nouvelles applications informatiques, des logiciels ou des programmes utilitaires spécialisés (ou modifie ceux qui existent déjà).	Vulnérabilités des systèmes et des logiciels Essais et évaluation de la sécurité logicielle Outils, techniques et procédures de sécurité logicielle Pratiques et outils d'évaluation de la vulnérabilité et d'essais de pénétration Identité, justificatifs d'identité et authentification
	Planificateur des besoins en systèmes	SP-SRP-001	2147 2171 2261	Consulte les clients pour évaluer les exigences fonctionnelles et traduire ces exigences en solutions techniques	Cyberobjectifs organisationnels Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement/ICP Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité Identité, justificatifs d'identité et authentification

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Spécialiste d'essai et d'évaluation de système	SP-TST-001	2173 2171 2174 2283	Planifie, prépare et exécute des essais de systèmes pour évaluer les résultats par rapport aux spécifications et aux exigences, et analyse/rapporte les résultats des essais.	Vulnérabilités des systèmes et des logiciels Essais et évaluation de la sécurité des systèmes et des logiciels Outils, techniques et procédures de sécurité logicielle Pratiques et outils d'évaluation de la vulnérabilité et d'essais de pénétration Normes de cybersécurité Évaluation et mesure de la cybersécurité
	Développeur de systèmes	SP-SYS-002	2147 2173 2174	Conçoit, développe, met à l'essai et évalue les systèmes d'information tout au long du cycle de vie du développement de système.	Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement/ICP Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité Identité, justificatifs d'identité et authentification
	Développeur Web	Aucune	2175	Recherche, conceptualise, développe et produit des sites	Menaces à la cybersécurité Vulnérabilités des applications Web

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				Internet et intranet et de médias basés sur le Web.	Essai et évaluation de logiciels Exigences en matière de réponse aux incidents de cybersécurité
	Administrateur des bases de données	OM-DTA-001	2172	Administre les bases de données ou les systèmes de gestion des données qui permettent le stockage, l'interrogation, la protection et l'utilisation des données en toute sécurité.	Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Analyste de données	OM-DTA-002	2172	Examine des données provenant de multiples sources disparates dans le but de fournir des renseignements sur la sécurité et la vie privée. Conçoit et met en œuvre des algorithmes personnalisés, des processus de flux de travail et des configurations pour des ensembles de données complexes à l'échelle de l'entreprise, utilisés à des fins de modélisation, d'exploration de données et de recherche.	Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Gestionnaire de l'information (gestionnaire des connaissances de la NICE)	OM-KMG-001	0213 1523	Responsable de la gestion et de l'administration des processus et des outils qui permettent à l'organisation de déterminer et de documenter le capital intellectuel et le contenu de l'information, et d'y accéder.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Catégorisation des renseignements/données Sécurité des systèmes et des données

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Spécialiste en soutien technique	OM-STS-001	2281 2282	Fournit un soutien technique aux clients qui ont besoin d'aide en utilisant du matériel et des logiciels au niveau du client, conformément aux composantes des processus organisationnels établis ou approuvés (c'est-à-dire le plan directeur de gestion des incidents, le cas échéant).	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes
	Spécialiste des opérations réseau	OM-NET-001	2281 2282	Planifie, met en œuvre et exploite des services/systèmes de réseau, y compris le matériel et les environnements virtuels.	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes
	Administrateur du système	OM-ADM-001	2281	Responsable de la mise en place et de la maintenance d'un système ou d'éléments spécifiques d'un système (par exemple, installation, configuration et mise à jour du matériel et des logiciels; création et	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				gestion des comptes d'utilisateurs; supervision ou réalisation de tâches de sauvegarde et de récupération; mise en œuvre de contrôles de sécurité opérationnels et techniques; et respect des politiques et procédures de sécurité organisationnelle).	Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes Identité, justificatifs d'identité et authentification
	Analyste des systèmes de données	Aucune	2172	Détermine, développe et analyse les besoins en matière de systèmes de données pour l'organisation. Prend en charge, conçoit et met en œuvre des systèmes de données.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification Outils, techniques et procédures de cybersécurité utilisés pour protéger les données et les systèmes de données Chiffrement et ICP
	Gestionnaire des systèmes (comprend les rôles de gestionnaire des systèmes, des logiciels et des systèmes de données)	Aucune	0213	Planifie, organise, dirige, contrôle et évalue les activités des organisations qui analysent, conçoivent, développent, mettent en œuvre, exploitent et administrent des logiciels informatiques et de	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				télécommunications, des réseaux et des systèmes d'information	Gestion de projets de cybersécurité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)

Annexe D – Le généraliste de la cybersécurité

Au sein de nombreuses petites et moyennes organisations (PMO), et même dans les grandes organisations qui ne dépendent pas fortement des activités basées sur Internet, il y a des personnes chargées de responsabilités en matière de cybersécurité qui n'ont pas forcément d'expérience en TI ou en cybersécurité. Bien qu'elle ne concerne pas spécifiquement la province de la NPN, cette annexe fournit une description plus détaillée des compétences en matière de cybersécurité qui peut servir de référence aux employeurs, aux éducateurs et aux professionnels du perfectionnement de la main-d'œuvre qui cherchent à mieux comprendre les exigences de ce rôle.

Comme chaque entreprise est unique, elles doivent examiner attentivement où se situent les principales responsabilités et déterminer les renseignements, les réseaux et les possibilités d'apprentissage qui soutiennent ceux qui ont des responsabilités en matière de cybersécurité. Lorsque des employés comme des analystes des TI ou commerciaux assument directement des responsabilités en matière de conception, de développement ou d'exploitation de la cybersécurité, cette NPN ainsi que les renseignements détaillés sur les rôles de l'emploi en cybersécurité dans le cadre de la NICE peuvent être utilisés comme guide pour mieux comprendre quelles compétences peuvent être requises pour la situation et le contexte organisationnels.

Exemples de titres des postes : agent de sécurité d'entreprise, analyste de la sécurité, agent de sécurité, gestionnaire de la sécurité, etc.

Généralistes de la cybersécurité :

- Exercer des fonctions de cybersécurité à temps partiel en conjonction avec d'autres responsabilités
- N'exige que des connaissances, compétences et habiletés en matière de cybersécurité qui soient à la mesure du contexte commercial, technique et de menace
- Ne sont pas considérés comme des professionnels de la cybersécurité et n'ont pas de trajectoire de carrière dans le domaine de la cybersécurité

Les tâches communes comprennent :

- Évaluer la position de l'organisation en matière de cybersécurité
- Faciliter la détermination des cyberrisques organisationnels
- Déterminer les contrôles de cybersécurité non techniques
- Identifier les experts techniques, internes ou externes, en matière de contrôles techniques et assurer la liaison avec eux
- Élaborer des plans et des politiques organisationnels en matière de cybersécurité

- Conseiller les dirigeants en matière de sensibilisation et de formation à la sécurité
- Surveiller et soutenir les experts techniques, qu'ils soient internes ou externes, dans leurs fonctions de cybersécurité
- Coordonner l'intervention en cas d'incident de cybersécurité
- Suivre et signaler les mesures de réponse et d'atténuation et recommander des actions sur la base d'avis techniques
- Coordonner les activités rétrospectives sur les événements et incidents, en intégrant les leçons apprises dans les politiques et procédures organisationnelles

Pour bon nombre de ces tâches, il existe de nombreuses ressources en ligne pour guider les généralistes de la sécurité dans leurs fonctions. Toutefois, l'efficacité de ces tâches repose sur les connaissances, compétences et habiletés (CCH) de base nécessaires pour soutenir la prise de décision et l'action. Toutefois, il est peu probable qu'ils aient une formation ou une éducation approfondie en matière de cybersécurité. En conséquence, ils devraient se voir offrir des possibilités d'apprentissage suffisantes pour acquérir les compétences requises en fonction de leurs responsabilités ainsi que de la menace et du contexte technique et commercial. Comme le montrent les exemples de la figure ci-dessous, cela nécessite généralement des compétences empruntées à certains des rôles de travail au sein de chaque grande catégorie de travail.

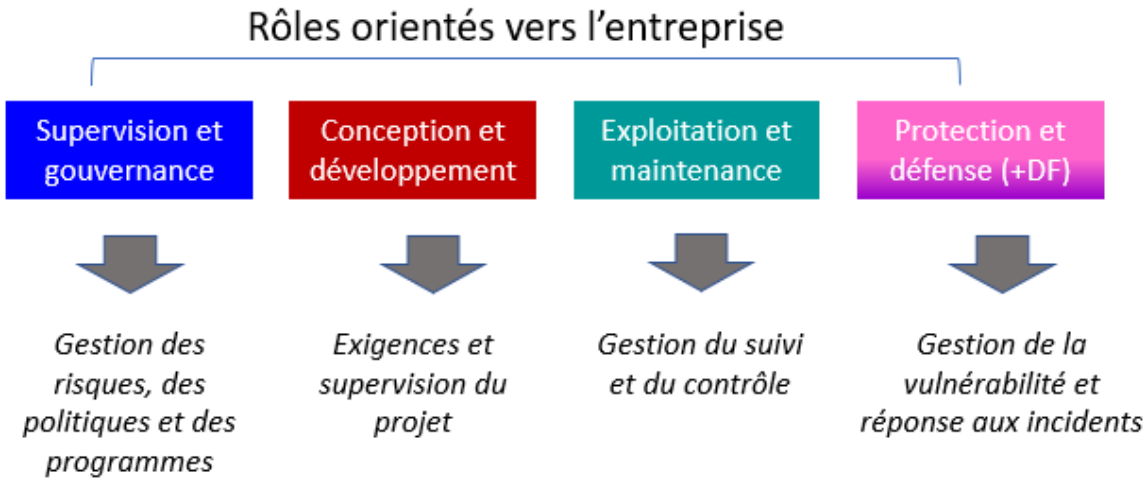

Figure – Fonctions généralistes de la cybersécurité tirées des domaines d'activité existants

Connaissances de base :

- Contexte technique (par exemple, infrastructure organisationnelle de TI, logiciels, dispositifs et politiques)
- Contexte de la cybermenace (y compris les risques délibérés, accidentels et naturels)
- Contexte de l'entreprise (priorités, objectifs, marché, tendances)
- Contexte juridique, politique et éthique de la sécurité
- Gestion des risques liés à la cybersécurité dans le cadre du risque organisationnel
- Gestion des incidents de cybersécurité (spécifique à un domaine)
- Processus, technologies, tendances et questions émergents en matière de cybersécurité
- Sources d'expertise et de ressources en matière de cybersécurité

Compétences et aptitudes de base :

- Fournir des conseils aux entreprises dans le contexte juridique et politique de la cybersécurité
- Faire preuve de prévoyance et planifier la sécurité pour soutenir les activités et la croissance des entreprises numériques
- Traduire le risque cybernétique en risque d'entreprise
- Faire la distinction entre conformité et risque
- Interpréter les évaluations de la menace et des risques dans le contexte opérationnel
- Évaluer l'efficacité des contrôles de sécurité par rapport aux objectifs de sécurité organisationnelle

Annexe E – Liste des acronymes

TIC	Technologies de l'information et de la communication
PCA	Plan de continuité des activités
AVEC	Apportez votre équipement personnel de communication
DI	Directeur de l'informatique
SECOM	Sécurité des communications
GOC	Gestionnaire des opérations de cybersécurité
ATC	Alliance des talents en cybersécurité
CWF	Cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité (États-Unis)
CN	Certificat numérique
SCD	Système de contrôle distribué
PIC	Plan d'intervention en cas de catastrophe
MSM	Module de sécurité matérielle
GIJIA	Gestion de l'identité, des justificatifs d'identité et de l'accès
SCI	Système de contrôle industriel
SDI	Système de détection d'intrusion
	Indicateurs de compromission
SPI	Système de prévention d'intrusion
RI	Réseaux infrarouges
TI	Technologie de l'information
CCH	Connaissances, compétences et habiletés
NICE	National Initiative on Cybersecurity Education (États-Unis)
CNP	Classification nationale des professions
NIST	National Institute of Standards and Technology (États-Unis)
SCO	Systèmes de contrôle opérationnel
SO	Système d'exploitation
TO	Technologie opérationnelle
ICP	Infrastructure à clés publiques
RFID	Identification par radiofréquence
SCADA	Commande de surveillance et acquisition de données
COS	Centre des opérations de sécurité
SSH	Protocole SSH
SSL	Protocole SSL
TLS	Sécurité de la couche transport
TTP	Tactiques, techniques et procédures
VoIP	Voix par protocole Internet
VPN	Réseau privé virtuel
Wi-Fi	Technologie Wi-Fi