Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Cadre des Compétences en Matière de Cybersécurité du Canada

Adapter le cadre de la National Initiative for Cyber Education (NICE) au marché du travail canadien

Série gestionnaires

Canada

Avant-propos

Le Cadre des Compétences en Matière de Cybersécurité du Canada (ITSM.00.039) est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, prière d'envoyer un courriel ou de téléphoner au Centre de coordination des services du Centre pour la cybersécurité :

Centre de coordination des services

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Étant donné la nature hautement dynamique de la cybersécurité, ce présent guide sera passé en revue chaque année par l'équipe du développement des cybercompétences du Centre canadien pour la cybersécurité. Toutes les modifications proposées à la présente publication devraient être envoyées par courriel à :

cyberskills-cybercompetences@cyber.gc.ca.

Date d'entrée en vigueur

Le présent document entre en vigueur en 19 avril 2023.

Historique des révisions

Version	Modifications	Date
1	Première version	19 avril 2023

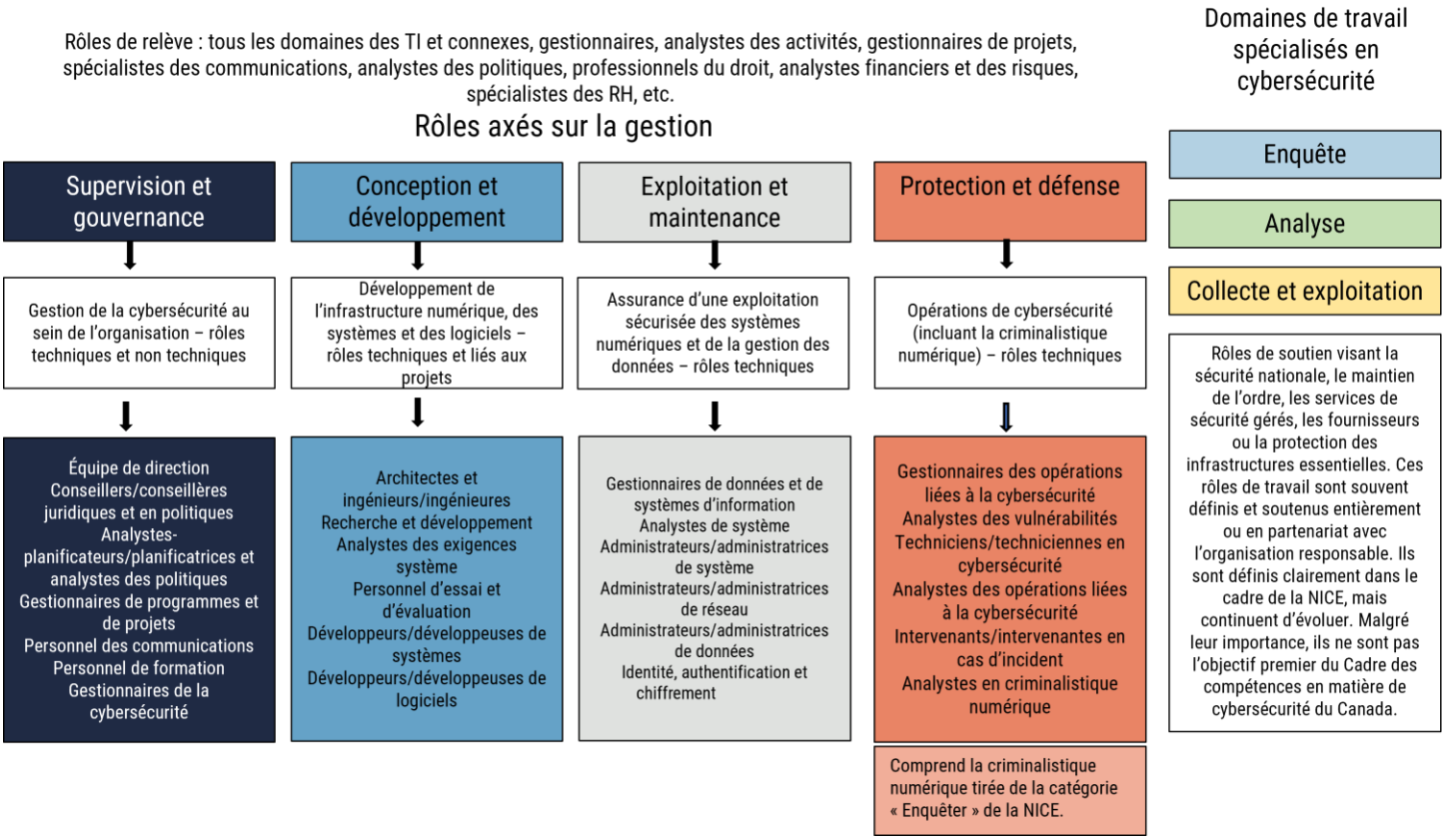
ISBN 978-0-660-46232-5

No de cat. D97-4/00-039-2022F-PDF

Vue d'ensemble

Le Cadre des compétences en matière de cybersécurité au Canada (figure 1) s'appuie sur les éléments du cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité de la National Initiative for Cyber Education (NICE) des États-Unis (ci-après désigné le cadre de la NICE) tout en s'adaptant au marché du travail canadien. Ce modèle, qui repose sur le cadre de la NICE et vise à le simplifier, est axé sur les activités, reconnaît les talents du point de vue de la sécurité organisationnelle et constitue un modèle plus accessible aux intervenantes et aux intervenants qui n'œuvrent pas dans le domaine de la cybersécurité.

Figure 1 : Cadre des compétences en matière de cybersécurité du Canada



Tirant avantage des principaux éléments et des principales caractéristiques du cadre de la NICE, le Cadre des compétences en matière de cybersécurité du Canada vise à faire ce qui suit :

- aider à préciser les lacunes dans la main-d'œuvre du domaine de la cybersécurité qui existent sur le marché du travail canadien en approchant la question du point de vue des entreprises et en établissant une distinction entre les rôles de base en cybersécurité et les rôles organisationnels qui assument certaines responsabilités en matière de cybersécurité ou des rôles connexes dans le domaine;
- simplifier la représentation du travail lié à la cybersécurité qui est commun à la plupart des organisations;

- adapter le cadre de manière à soutenir les responsabilités plus vastes ou généralistes qui sont communes aux petites et moyennes organisations (PMO), alors qu'elles s'efforcent de répondre aux exigences fondamentales en matière de technologies de l'information (TI) et de cybersécurité;
- continuer de mettre l'accent sur les responsabilités en cybersécurité des rôles de travail dans les secteurs de la supervision et de la gouvernance, de la conception et du développement, et de l'exploitation et de la maintenance.

Le Cadre des compétences en matière de cybersécurité au Canada présente avec simplicité le travail lié à la cybersécurité au sein de nombreuses organisations du secteur privé et de petits organismes du secteur public. L'objectif de ce cadre est d'aider à mieux guider les intervenantes et les intervenants en développement de la main-d'œuvre pour combler le déficit de compétences en cybersécurité. Il peut s'appliquer tant aux secteurs public et privé qu'au milieu universitaire aux fins de sensibilisation et de développement de carrières, de formation et d'éducation, de recrutement ou de planification de l'effectif.

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Canadianisation du cadre de la NICE

1.1 Contexte

La norme professionnelle nationale (NPN) définit les principaux éléments du travail en cybersécurité comme étant distincts des autres professions liées aux TI, à la sécurité, à la gestion des activités ou à l'administration publique. Cela dit, la cybersécurité ne se limite pas aux systèmes techniques. Elle englobe les gens, leurs comportements et la façon dont ils se connectent à ces systèmes et les utilisent.

On ne saurait trop insister sur l'importance que revêt l'efficacité de la cybersécurité, ainsi que des produits et services soutenus par les professionnels de la cybersécurité. Les emplois en cybersécurité sont désormais reconnus à travers le monde comme des carrières essentielles et durables dans l'économie numérique.

Au Canada, la dépendance aux systèmes d'information et de données a connu une augmentation exponentielle au cours de la dernière décennie alors que les organisations ont misé sur la numérisation de leurs activités et se sont tournées vers une présence en ligne. Pour ce faire, elles ont dû compter sur des professionnelles et professionnels capables de concevoir, de construire, de mettre en œuvre et de maintenir des systèmes d'information sûrs, sécurisés et fiables qui peuvent répondre à une multitude de besoins organisationnels, opérationnels et personnels.

Les citoyennes et citoyens canadiens sont de plus en plus conscients de leurs droits en matière de respect de la vie privée et se préoccupent de plus en plus de la façon dont les organisations protègent leurs données personnelles. Il faut donc compter sur des spécialistes en cybersécurité et en protection des renseignements personnels qui peuvent formuler des conseils sur les diverses normes nationales et internationales, élaborer des politiques, déterminer les besoins et soutenir la surveillance pour mieux protéger la vie privée des Canadiennes et des Canadiens.

La cybercriminalité est une menace en constante évolution. Selon l'Évaluation sur les cybermenaces nationales 2020 du Centre pour la cybersécurité, « [l]es auteurs de cybermenace représentent un risque pour l'économie canadienne en raison des coûts élevés que doivent subir les particuliers et les entreprises, notamment lors du vol de propriété intellectuelle et de renseignements exclusifs » [1]. De l'expertise est donc requise pour soutenir la détection des cybermenaces et la prise de mesures d'intervention, et aider les personnes qui mènent les enquêtes et collectent les preuves numériques pouvant servir à renforcer les protections et à poursuivre les contrevenants, le cas échéant.

La cybersécurité ne concerne pas seulement les systèmes. Elle touche aussi les personnes qui se connectent au moyen de ces systèmes. Elle continuera d'être nécessaire à un large éventail de technologies. Des possibilités de carrière importantes et durables s'offrent donc aux personnes qui travaillent dans ce domaine et leur permettent de toucher positivement la vie des Canadiennes et des Canadiens connectés et de soutenir l'avenir de l'économie numérique.

Par conséquent, les entreprises et les industries ont du mal à satisfaire leurs besoins en matière de cybersécurité. Le perfectionnement de la main-d'œuvre est confronté à quatre grands défis :

- générer et retenir des talents dans le domaine des opérations de cybersécurité pour répondre aux besoins du marché du travail canadien;
- s'assurer que les rôles techniques et non techniques contributifs possèdent les connaissances, compétences et aptitudes requises;

- être attentif à l'évolution du contexte technologique;
- normaliser l'emploi et les activités en cybersécurité en milieu de travail au Canada.

Pour aider à surmonter ces défis, un groupe d'intervenantes et d'intervenants de l'industrie, du gouvernement et du milieu universitaire a formé l'Alliance des talents en cybersécurité (ATC) (voir l'annexe F). Le groupe a travaillé de concert pour fournir les éléments suivants :

- un cadre de compétences en matière de cybersécurité, dont une taxonomie et un lexique commun qui décrit le travail et les travailleurs en cybersécurité, qui repose sur les éléments du cadre de la NICE des États-Unis[1] (ci-après désigné le cadre de la NICE) tout en s'adaptant au marché du travail canadien;
- les descriptions de la NPN basées sur le cadre de compétences;
- les résultats d'apprentissage tirés de domaines de main-d'œuvre pertinents;
- les ressources connexes qui appuient la main-d'œuvre, le développement de carrière et l'apprentissage.

[1] Le cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité de la NICE (ou en anglais, *NICE Workforce Framework for Cybersecurity*), anciennement appelé le NICE Cybersecurity Workforce Framework, a changé de nom en 2020 pour reconnaître que la cybersécurité est une préoccupation commune à tous les effectifs, et non pas unique aux effectifs de la cybersécurité.

2 Brève introduction au cadre de la NICE

Avant le cadre de la NICE, le travail en cybersécurité était perçu et décrit d'une multitude de façons au sein du gouvernement fédéral américain, ce qui s'avérait fort problématique pour ce qui est du recrutement, de la sélection, de la formation et des autres activités de perfectionnement de l'effectif dans les secteurs public et privé. Cette situation était insoutenable compte tenu des menaces grandissantes qui pesaient sur la sécurité nationale et économique. Fondé à la fin des années 2000, le premier groupe de travail de la NICE a été mis sur pied en 2011 par la National Institute of Standards and Technology (NIST) des États-Unis avec **d'autres** partenaires fédéraux américains. Depuis, plus de 20 ministères fédéraux américains, des intervenants des secteurs de la défense et de la sécurité, des établissements du milieu universitaire et, dans une moindre mesure, des alliés internationaux comme le Canada et l'Australie ont contribué au développement et à l'évolution du cadre de la NICE.

Le cadre de la NICE offre une vue intégrée de la main-d'œuvre en cybersécurité. Il permet ainsi d'identifier les rôles de travail qui ont une incidence sur la capacité de l'organisation à protéger ses données, ses systèmes et ses activités [2]. Cela comprend tant les rôles techniques que non techniques destinés à soutenir les efforts de l'organisation en matière de gestion des risques liés à la cybersécurité. De plus, le cadre de la NICE comprend des capacités de cyberopérations nationales, dont les rôles liés au renseignement et aux opérations offensives qui relèvent généralement du gouvernement fédéral ou d'institutions partenaires. Notamment, le cadre de la NICE comporte un processus de surveillance et de révision permettant de veiller à ce qu'il réponde aux besoins grandissants de la collectivité de la cybersécurité.

2.1 Le cadre américain de la NICE dans le contexte canadien

Le cadre de la NICE propose une vue exhaustive du travail effectué en cybersécurité. Ce projet visait à comprendre la mesure dans laquelle les entreprises et les organisations industrielles du Canada étaient prêtes à adopter un tel cadre. Il a d'ailleurs permis de répondre à quelques questions clés.

1. **Quels sont les principaux enjeux associés à la main-d'œuvre canadienne en cybersécurité?**

L'exploration des différences et des similitudes entre le marché du travail des États-Unis et du Canada dans le domaine de la cybersécurité soulève plusieurs problèmes.

Similitudes :

- On manque d'information sur le marché du travail en ce qui a trait aux emplois en cybersécurité, aux titres d'emplois connexes et aux rôles dans ces deux pays;
- Selon les rôles de travail tirés du cadre de la NICE, on estime que le Canada a un écart plus grand à combler comparativement aux États-Unis;
- Au Canada, moins de ressources sont consacrées aux enjeux liés à la main-d'œuvre en cybersécurité et on y porte moins attention;
- La cybersécurité est un environnement professionnel hautement concurrentiel dans les deux pays.

Différences :

- Bien qu'il soit similaire à celui des États-Unis, le marché du travail du Canada est beaucoup plus petit et la population active est plus dispersée;
- Au Canada, les ressources doivent être fournies dans les deux langues officielles;
- Une grande partie de l'économie canadienne est composée de petites et moyennes organisations (PMO) et leurs besoins diffèrent de ceux des grandes organisations;
- Le cadre de la NICE porte peu attention aux entreprises et aux industries canadiennes et à la façon dont il s'applique au marché du travail canadien.

2. **Dans quelle mesure l'adoption du cadre de la NICE sera-t-elle facile?**

Conformément à ce qui est indiqué dans le cadre de la NICE, d'autres pays peuvent adapter le cadre selon leur contexte respectif [3]. Par ailleurs, les pays de la collectivité des cinq[2] honorent une longue tradition et échangent leurs publications et leurs processus avec leurs partenaires. Le Canada partage son travail avec les États-Unis et, comme on peut le voir, plusieurs publications du gouvernement fédéral canadien, comme les conseils en matière de sécurité des TI, sont basées sur les publications du NIST[3] ou s'en inspirent fortement.

3. **Quels sont les avantages et les inconvénients d'adopter le cadre de la NICE dans sa forme actuelle?**

Avantages :

- Il est facilement accessible pour les intervenants du marché du travail canadien et du perfectionnement de l'effectif;
- Il normalise les descriptions des rôles de travail en cybersécurité et établit un lexique commun pour la collectivité du Canada, des États-Unis et d'autres pays;
- Il offre une description détaillée des connaissances, compétences et aptitudes communes aux rôles liés à la cybersécurité et a récemment introduit les compétences connexes qui faciliteront la formation, l'éducation et l'avancement professionnel;
- Il établit une base de référence connue pour évaluer les candidats qualifiés;
- Il est soutenu à l'échelle internationale par les autres gouvernements;
- Il tient compte de la transférabilité des travailleurs à l'échelle nationale et internationale;
- Plusieurs des rôles de travail, des tâches et des connaissances, compétences et aptitudes sont valides au sein de l'effectif canadien en cybersécurité.

Inconvénients :

- Il manque de précision en ce qui concerne les lacunes à combler sur le plan de l'effectif;
- Il est trop « vaste » ou trop granulaire pour le marché du travail général du Canada;
- Il est difficile à naviguer (p. ex. utilisation de codes pour établir des références entre les connaissances, compétences et aptitudes et les descriptions de mots);

[2] La collectivité des cinq est le nom informel de l'accord international d'échange de renseignement conclu entre le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.
[3] Pour des exemples de telles publications, prière de visiter le https://www.cyber.gc.ca/fr/publications.

- Il est axé sur l'« industrie de la défense » ou adapté aux grandes organisations dont les activités sont largement effectuées en ligne
- Il est structuré selon une perspective statique ou horizontale, puisqu'il est difficile de voir les cheminements de carrière ou les avancements latéraux ou verticaux dans le domaine de la cybersécurité
- Il ne convient pas aux petites organisations
- Il ne tient pas compte des fonctions des généralistes de la cybersécurité (p. ex. agents ou agentes de sécurité d'entreprise) ou des personnes qui soutiennent plusieurs rôles liés à la cybersécurité dans un cadre de travail typique que l'on retrouve souvent dans les petites et moyennes organisations non techniques
- Il minimise des rôles importants et distincts en les intégrant à des rôles plus élargis (p. ex. le génie en cybersécurité fait partie du rôle de recherche et de développement)
- Il ne tient pas compte des rôles liés à la sécurité des technologies opérationnelles et industrielles (p. ex. systèmes de contrôle industriels [SCI] et télésurveillance et acquisition de données [SCADA pour *Supervisory Control and Data Acquisition*])
- Il omet les rôles nouveaux et émergents qui émanent du domaine dynamique de la cybersécurité

Le cadre de la NICE ne reflète pas nécessairement une structure et des fonctions professionnelles communes à toutes les organisations des secteurs privé et public non fédéral du Canada.

Bien qu'il existe plusieurs autres rôles contributifs ou adjacents à la cybersécurité, tel qu'il est indiqué dans le cadre de la NICE, le présent document met l'accent sur les rôles principaux liés à la cybersécurité et les compétences connexes qui relèvent d'un contexte opérationnel canadien plus large où la majorité du travail dépend des objectifs et des résultats de la cybersécurité organisationnelle. Le cadre de la NICE répertorie principalement les spécialisations en cybersécurité qui relèvent du renseignement, de la sécurité nationale ou du maintien de l'ordre.

2.2 Remarque spéciale à l'intention des éducateurs et éducatrices

On reconnaît le rôle inestimable que jouent les éducateurs et éducatrices en cybersécurité. Par contre, comme ils sont régis par leur propre Classification nationale des professions (CNP) et un vaste réseau de normes professionnelles, il est inutile de répéter cette information dans la présente publication. Force est de constater qu'il nous faut compter sur des éducateurs et éducatrices qualifiés ayant l'expérience et les capacités nécessaires pour faciliter et évaluer l'apprentissage requis pour soutenir la demande de l'industrie conformément aux normes reconnues.

2.3 Normes professionnelles nationales (NPN)

Les normes professionnelles nationales (NPN) décrivent ce qu'une personne occupant un poste particulier doit savoir et être en mesure de faire pour être jugée « compétente » dans ce poste. On définit ces normes en fonction des compétences, y compris les connaissances, compétences et aptitudes exigées pour effectuer le travail efficacement, correctement et en toute sécurité. Les NPN établissent les bases d'un rendement compétent dans les lieux de travail comme en a convenu un échantillon représentatif de travailleurs, d'employeurs et d'autres intervenants. Les NPN peuvent également être régies ou dictées par d'autres exigences externes, comme la conformité juridique ou le respect des politiques.

Figure 2 : Utilisations des NPN

Praticiens/praticiennes	Employeurs	Éducateurs/éducatrices	Intervenants/intervenantes en perfectionnement de l'effectif
Poser les bases du développement de carrière Orienter leur apprentissage et leur perfectionnement au sein de la profession Appuyer la mobilité et la transition professionnelles	Déterminer les rôles et les tâches clés Déterminer les besoins en matière de perfectionnement professionnel Assurer une description objective des postes Orienter le recrutement	Déterminer les domaines nécessitant de l'expertise Poser les bases des programmes d'études, du développement de la formation et de l'éducation – fournisseurs des secteurs privé et public Améliorer les programmes d'études Poser les bases des programmes de certification et de l'accréditation des programmes	Créer des occasions de perfectionnement professionnel Déterminer les compétences requises pour des postes particuliers Adopter comme référence des pratiques exemplaires reconnues à l'échelle nationale et axées sur les secteurs Fournir de l'information sur le perfectionnement professionnel aux praticiens et praticiennes qui montent les échelons vers des postes de gestion

3 Adapter le cadre de la NICE au marché du travail canadien

3.1 Attributs d'un cadre de compétence réaliste pour le marché canadien

L'adoption et la simplification du cadre de la NICE pour le marché du travail du Canada rendent l'utilisation du cadre canadien plus facile pour les entreprises et les industries ayant du mal à interpréter le cadre de la NICE dans sa forme initiale.

Comme il est indiqué à la figure 3, l'adoption du cadre de la NICE dans un contexte canadien repose sur la considération de cinq attributs principaux. Ces attributs ont été déterminés en fonction de certaines critiques et de certains problèmes structurels entourant le cadre de la NICE, et en tenant compte de la rétroaction obtenue de la collectivité dans le cadre de consultations.

Figure 3 : Attributs souhaités pour le Cadre canadien des compétences en matière de cybersécurité

Spécificité et précision	Bien que le cadre de la NICE décrive l'ensemble complet des rôles de travail en cybersécurité, il devrait être possible de mettre l'accent sur ceux qui sont les plus pertinents pour combler les écarts de compétences en cybersécurité au Canada et répondre au contexte canadien.
Utilisabilité et accessibilité	Le cadre devrait faciliter l'utilisation, la lisibilité et l'accessibilité du contenu pour tous les lecteurs et utilisateurs potentiels, dont ceux qui ne sont pas familiers avec le travail en cybersécurité. Plus précisément, le cadre ne devrait pas isoler la cybersécurité, mais bien intégrer les concepts dans un contexte opérationnel et organisationnel plus large.
Clarté des concepts	Il convient de décrire clairement les rôles liés à la cybersécurité et de tenir compte tant des rôles techniques et multidisciplinaires que des rôles de spécialistes et de généralistes.
Adaptabilité	Compte tenu de la nature dynamique de ce document, il convient de mettre en place un mécanisme permettant d'intégrer rapidement les rôles nouveaux ou émergents qui résultent des technologies comme l'automatisation, l'infonuagique, l'intelligence artificielle, l'informatique quantique, ainsi que des connaissances, compétences et aptitudes qui soutiennent l'ensemble des activités de cybersécurité. Le cadre doit constamment évoluer en fonction du travail.
Évolutivité	Un cadre devrait pouvoir s'adapter facilement aux organisations de toutes tailles et aux différents contextes de l'industrie. Cela comprend la capacité des organisations à identifier et à développer les talents non techniques de sorte à soutenir leurs besoins en matière de sécurité.

3.1 Adapter le cadre canadien aux petites et moyennes organisations

Le cadre canadien peut être adapté aux PMO. En cybersécurité, la plupart des PMO présentent les caractéristiques suivantes :

- On y retrouve rarement des spécialistes en cybersécurité
- Les rôles liés à la conception et au développement sont externalisés ou on doit acquérir des systèmes ou des applications grand public
- Les personnes doivent souvent assumer plusieurs rôles, dont des tâches liées à la cybersécurité

Par conséquent, lorsque les organisations examinent le cadre de la NICE, elles peuvent se sentir dépassées par l'ampleur de la tâche. Il est toutefois possible d'établir des scénarios ou de présenter des exemples qui aideront les PMO à adapter le cadre de la NICE en fonction du cadre canadien des compétences en matière de cybersécurité, ainsi qu'à définir les connaissances, compétences et aptitudes basées sur le rôle qui soutiendront la cybersécurité au sein des organisations.

La section suivante traitera des deux scénarios qui se produisent généralement dans les PMO.

1. **Organisation de taille moyenne avec personnel informatique interne**

On y retrouve une expertise technique à l'interne, mais plusieurs rôles liés à la cybersécurité sont assumés par des personnes qui occupent d'autres fonctions et ne sont généralement pas des spécialistes en cybersécurité, ou par de petites équipes de TI responsables de la détection et de l'intervention en cas d'incident. Dans cet exemple, le dirigeant principal ou la dirigeante principale de l'information (DPI) dirigerait la petite équipe de TI et serait responsable des aspects techniques du programme de cybersécurité, alors que les gestionnaires du niveau de la direction resteraient responsables de l'établissement des priorités organisationnelles et de la définition du contexte de risque. Il incomberait probablement à l'équipe de TI d'assumer toutes les fonctions Protection et défense, alors que les activités spécialisées seraient externalisées et confiées à une tierce partie.

Figure 4 : Rôles techniques possibles dans une organisation de taille moyenne

Supervision et gouvernance

Rôles de travail pris en compte dans le Cadre canadien des compétences en matière de cybersécurité	Dans une PMO, des responsabilités liées à la cybersécurité sont probablement confiées aux titulaires de ces postes
Équipe de direction en cybersécurité	Dirigeants principaux/dirigeantes principales de l'information (DPI) ou dirigeants principaux/dirigeantes principales de la sécurité de l'information (DPSI) et personnel de soutien
Autorisateurs/autorisatrices	
Planificateurs/planificatrices de politiques et de stratégies en cybersécurité	
Gestionnaires de la sécurité des systèmes d'information	Gestionnaires des systèmes d'information
Gestionnaires de programme	Gestionnaires de programme ou de secteur d'activités
Gestionnaires de projets de TI	DPI et personnel de soutien
Gestionnaires du soutien des produits	
Gestionnaires des investissements et des portefeuilles de TI	
Spécialistes de l'approvisionnement	
Analystes de l'intégrité de la chaîne d'approvisionnement	
Analystes financiers/financières et des risques	Dirigeants principaux/dirigeantes principales des finances
Spécialistes des communications	Agents/agentes de communications
Conseillers/conseillères juridiques	Avocats/avocates-conseil
Agents/agentes à la protection des renseignements personnels ou gestionnaires de la protection de la vie privée	
Développeurs/développeuses de curriculums pédagogiques en cybersécurité	Dirigeants principaux/dirigeantes principales de l'apprentissage ou des ressources humaines

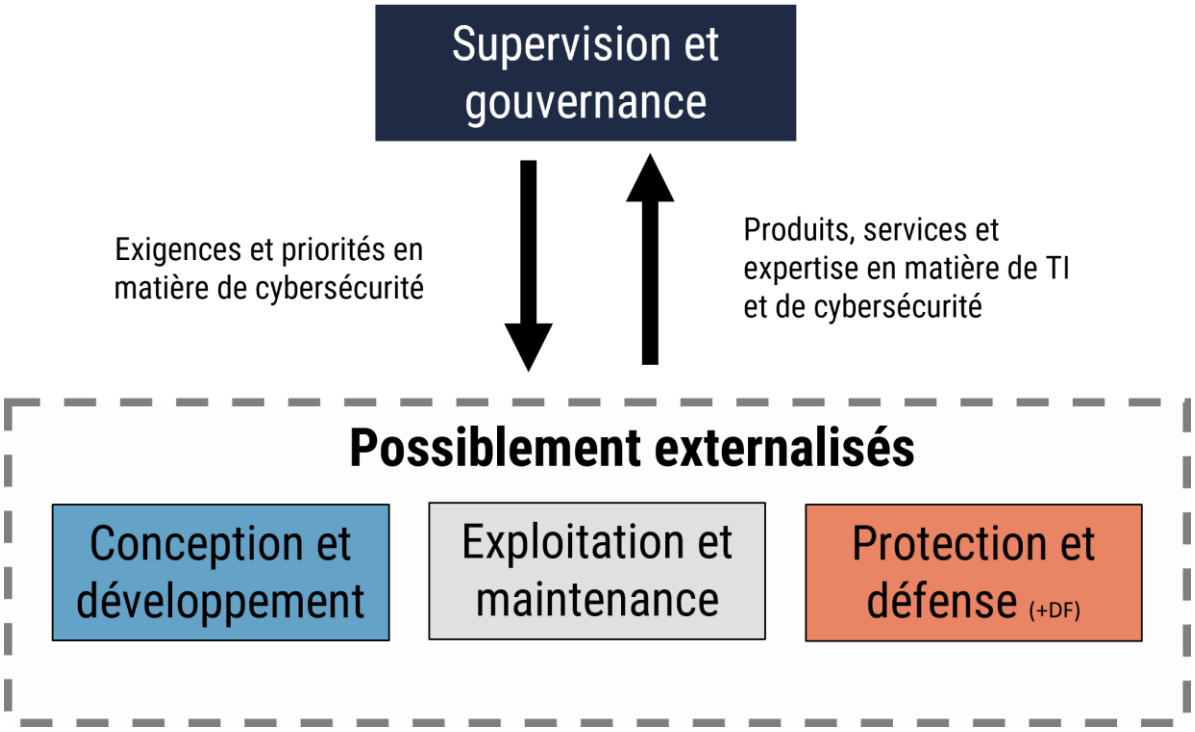
Protect et défense (+DF)

Rôles de travail pris en compte dans le Cadre canadien des compétences en matière de cybersécurité	Dans une PMO, des responsabilités liées à la cybersécurité sont probablement confiées aux titulaires de ces postes
Gestionnaires de la sécurité des systèmes d'information (opérations de cyberdéfense)	Gestionnaires des TI ou de systèmes, dirigeants principaux/dirigeantes principales de l'information ou dirigeants principaux/dirigeantes principales de la sécurité de l'information
Analystes de la cyberdéfense et soutien des infrastructures de cyberdéfense	Les tâches liées à la cyberdéfense sont souvent comprises dans les postes suivants : • Bureau des services TI ou services à la clientèle • Administrateurs/administratrices de système ou de réseau
Intervenants/intervenantes en cas d'incident lié à la cyberdéfense	
Évaluateurs/évaluatrices des vulnérabilités	
Analystes en criminalistique numérique	

2. Petite organisation avec une dépendance limitée à l'égard des TI et sans personnel informatique

La plupart des rôles de travail techniques seraient externalisés, mais l'organisation continuerait d'assumer les principales fonctions Supervision et gouvernance liées à la cybersécurité. Cette personne assumerait effectivement le rôle de généraliste de la sécurité.

Figure 5 : Rôles techniques possiblement externalisés dans une petite organisation



3.2 Généralistes en cybersécurité

Dans plusieurs PMO et même des organisations plus grandes dont les activités ne dépendent pas fortement d'Internet, on retrouve des personnes à qui des responsabilités en cybersécurité ont été confiées sans qu'elles aient nécessairement d'expérience en informatique ou en cybersécurité.

Si on tient compte du nombre de PMO dans l'environnement commercial du Canada, cela représente un très grand nombre de personnes sur le marché du travail canadien dont la principale responsabilité consiste à établir et à gérer la cybersécurité au sein de leur organisation et qui pourraient ne pas occuper l'un des rôles définis dans le cadre de la NICE ou le cadre canadien. En règle générale, ces personnes :

- accomplissent des tâches liées à la cybersécurité à temps partiel parallèlement à d'autres responsabilités;
- utilisent les connaissances, compétences et aptitudes en cybersécurité qui conviennent au contexte opérationnel, technique et de menace;
- ne sont pas considérées comme étant des professionnelles de la cybersécurité et ne suivent pas le parcours professionnel en cybersécurité.

À défaut d'avoir un terme précis, le présent document utilise « généraliste de la sécurité » pour les distinguer des spécialistes en cybersécurité mentionnés dans les rôles principaux. Dans un environnement organisationnel, le ou la généraliste de la sécurité n'est généralement pas spécialisé dans le domaine de la sécurité, mais est souvent responsable

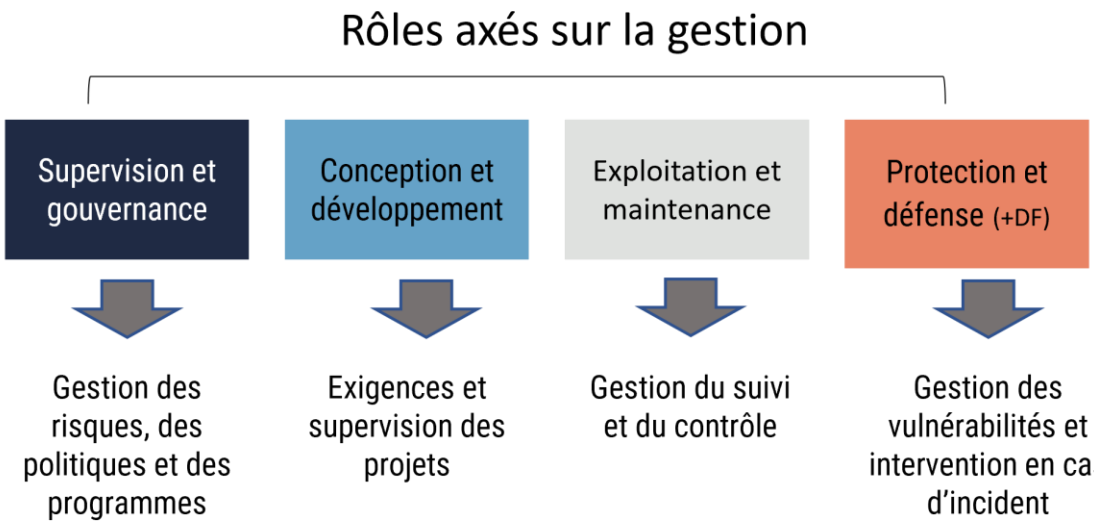
des activités liées à la sécurité physique, contractuelle, du personnel et de la prévention des pertes, en plus de la cybersécurité. Il arrive souvent, par exemple, que le ou la chef de la direction, le dirigeant principal ou la dirigeante principale de l'information (DPI), le dirigeant principal ou la dirigeante principale de l'information (DPF), l'agent ou l'agente de sécurité d'entreprise, le ou la gestionnaire des ressources humaines ou un haut fonctionnaire occupe un tel poste.

Ils doivent, entre autres, faire ce qui suit :

- évaluer la posture de cybersécurité de l'organisation;
- faciliter la détermination des risques de l'organisation en matière de cybersécurité;
- déterminer les contrôles de cybersécurité non techniques;
- identifier les spécialistes techniques internes ou externes et assurer la liaison avec eux pour ce qui est des contrôles techniques;
- élaborer des politiques et des plans organisationnels en matière de cybersécurité;
- conseiller les membres de la direction sur la formation et la sensibilisation à la sécurité;
- superviser et soutenir les spécialistes techniques, tant internes qu'externes, dans l'exercice de leurs fonctions en cybersécurité;
- coordonner la prise de mesures d'intervention en cas d'incident de cybersécurité;
- surveiller les mesures d'intervention et d'atténuation, en faire rapport et recommander des plans d'action basés sur conseils techniques;
- coordonner les activités d'analyse rétrospective des événements et des incidents et intégrer les leçons apprises aux politiques et procédures organisationnelles.

Pour bon nombre de ces tâches, on retrouve de multiples ressources en ligne pour guider les généralistes de la sécurité dans l'exécution de leurs tâches. L'efficacité de ces tâches repose toutefois sur les connaissances, compétences et aptitudes requises pour soutenir le processus décisionnel et la prise de mesures. Il est peu probable que les généralistes aient une formation ou une éducation approfondie en cybersécurité. On devrait donc leur offrir les occasions d'apprentissage nécessaires pour acquérir les compétences qui conviennent à leurs responsabilités, ainsi qu'au contexte technique, opérationnel et de menace. Comme le démontrent les exemples illustrés dans la figure ci-dessous, on doit souvent faire appel à des compétences tirées de certains des rôles de travail appartenant à chacune des grandes catégories d'emplois.

Figure 6 : Fonctions des généralistes de la sécurité



Connaissance de base :

- Contexte technique (p. ex. structure informatique organisationnelle, logiciels, dispositifs et politiques)
- Contexte de la cybermenace (dont les risques délibérés, accidentels et naturels)
- Contexte opérationnel (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 (propres à un domaine)
- Processus de cybersécurité, technologies, tendances et enjeux émergents
- Sources d'expertise et ressources en cybersécurité

Compétences et aptitudes de base :

- Prodiguer des conseils aux entreprises dans le contexte juridique et politique de la cybersécurité
- Faire preuve de prévoyance et planifier la sécurité de manière à soutenir les activités numériques et la croissance de l'organisation
- Transformer le cyberrisque en risque organisationnel
- Faire la distinction entre la conformité et le risque
- Interpréter les évaluations des menaces et des risques dans un contexte opérationnel
- Évaluer l'efficacité des contrôles de sécurité par rapport aux objectifs de sécurité de l'organisation

Compétences communes :

Pour tous les rôles principaux liés à la cybersécurité, peu importe le secteur d'activités ou la catégorie d'emplois, de nombreuses compétences communes s'appliquent, selon le rôle, au niveau de base, intermédiaire ou avancé. Tous les professionnels de la cybersécurité, peu importe leur rôle, devraient avoir les connaissances de base nécessaires pour appliquer les éléments suivants dans leur domaine ou contexte de travail :

- systèmes de TI et réseautique
- architecture de systèmes et modèles
- protocoles Internet, systèmes et dispositifs
- fondements de la cybersécurité
  - cadre de sécurité intégrée
  - stratégies et approches liées à la cybersécurité
  - contexte des menaces et exposition aux menaces courantes (du personnel, physiques, informatiques ou logiques, chaîne d'approvisionnement)
  - processus et sources de renseignement sur les cybermenaces
  - analyse de la cybersécurité
  - politiques, processus et pratiques exemplaires en matière de gestion de la cybersécurité
  - systèmes, outils et applications de cybersécurité
  - règlementation et conformité (p. ex. respect de la vie privée, échange d'information, production de rapports, normes obligatoires, etc.)
  - normes nationales et de l'industrie
- résolution de problème et réflexion complexe dans des environnements dynamiques
- assurance d'une connaissance plus vaste de la situation en matière de sécurité
- conscience de soi pour ce qui est des connaissances, compétences et aptitudes requises pour répondre aux changements organisationnels, techniques et liés aux menaces

3.3 Rôles principaux liés à la cybersécurité

Reconnaissant que la cybersécurité est une responsabilité partagée, la présente publication décrit la profession de la cybersécurité en fonction du travail qui est généralement effectué à temps plein et qui exige des connaissances, compétences et aptitudes uniques par rapport aux autres professions. Par ailleurs, conformément au cadre canadien des compétences en matière de cybersécurité, on décrit également la profession de la cybersécurité en fonction des titres et des rôles de travail qui sont pertinents au marché du travail du Canada et au milieu élargi des affaires dans les quatre principaux

secteurs d'activités ou catégories d'emplois en cybersécurité : Supervision et gouvernance, Conception et développement, Exploitation et maintenance et Protection et défense. On retrouve une définition détaillée de ces secteurs d'activités, de ces catégories d'emplois et des rôles de travail connexes dans les annexes A, B, C et D.

Les rôles principaux liés à la cybersécurité sont divisés en grandes catégories et sous-groupes professionnels semblables à ceux établis dans le cadre de la NICE[4].

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

Compétences communes (fondements pour les personnes spécialisées dans la cybersécurité)

Pour tous les rôles principaux liés à la cybersécurité, peu importe le secteur d'activités ou la catégorie d'emplois, de nombreuses compétences communes s'appliquent, selon le rôle, au niveau de base, intermédiaire ou avancé (comme indiqué à la section 3.2). Tous les professionnels de la cybersécurité, peu importe leur rôle, devraient avoir les connaissances de base nécessaires pour appliquer les éléments suivants dans leur domaine ou contexte de travail :

- apprentissage continu soutenant le perfectionnement des connaissances liées aux menaces émergentes, aux innovations technologiques sur le plan de la sécurité et à un environnement de cybersécurité en constante évolution
- communications (orales et verbales) adaptées au contexte de l'organisation, dont la rédaction de rapports techniques
- réflexion stratégique et sens des affaires pour comprendre le contexte opérationnel et des risques liés à la cybersécurité
- travail d'équipe et collaboration avec autrui, y compris des personnes non spécialisées dans la cybersécurité
- respect de l'éthique et responsabilités professionnelles
- formation et sensibilisation en matière de cybersécurité dans leur domaine

[4] Il importe de mentionner que les catégories d'emplois « Enquête », « Analyse » et « Collecte et exploitation » ne sont que résumées dans le présent document, puisqu'elles sont définies entièrement dans le cadre de la NICE et qu'elles relèvent généralement de la responsabilité des professions de nature militaire et politique.

3.4 Rôles connexes à la cybersécurité

Plusieurs rôles sont également liés aux autres fonctions organisationnelles qui contribuent généralement aux résultats de l'organisation en matière de cybersécurité à temps partiel ou de façon opportune[5]. Il s'agit de rôles connexes à la cybersécurité qui exigent certaines connaissances, compétences et aptitudes en cybersécurité, mais qui ne sont généralement pas considérés comme étant occupés par des spécialiste de la cybersécurité[6]. Par exemple, dans certaines organisations, un ou une analyste des activités et des politiques s'occupera probablement d'un large éventail d'enjeux et seulement quelques-uns de ces enjeux concerneront la prise en charge de la cybersécurité organisationnelle. Il ne s'agit pas de nuire à son rôle de soutien à la cybersécurité organisationnelle, mais plutôt de suggérer que le travail accompli concerne souvent bien plus que la cybersécurité à proprement dit.

De même, les cadres supérieurs, les gestionnaires de programme, les analystes de politiques, les analystes financiers, les spécialistes des communications, les architectes d'entreprise, les techniciens et techniciennes informatiques, etc. peuvent assumer des responsabilités liées à la cybersécurité sans avoir à s'y consacrer à temps plein. Leurs rôles ne sont donc pas compris dans les rôles principaux liés à la cybersécurité abordés dans la présente publication. Ces rôles sont mentionnés à l'annexe E. Par exemple, un échantillonnage de rôles de travail types associés à la cybersécurité est fourni dans le tableau 1 ci-dessous. Bien qu'ils exercent des responsabilités en cybersécurité et doivent démontrer des connaissances, compétences et aptitudes particulières en matière de cybersécurité, leurs principales responsabilités sont souvent plus vastes ou axées sur d'autres activités non liées à la cybersécurité. Il importe de souligner que la catégorie Protection et défense n'est pas incluse dans la figure, puisque ce secteur d'activités ou cette catégorie d'emplois est utilisé exclusivement dans le domaine de la cybersécurité.

[5] Cela ne tient pas compte des « utilisateurs » qui assument des responsabilités liées à la cybersécurité peu importe leur rôle dans l'organisation.

[6] Dans le cas de certains rôles et de certaines professions, il peut s'agir de personnes qui sont employées à temps plein dans le domaine de la cybersécurité et sont considérées des spécialistes, comme celles employées dans un domaine du droit, du respect de la vie privée ou de l'éthique, qui touche à la cybersécurité. Comme elles exercent déjà une autre profession et ne font souvent pas partie de l'effectif de l'organisation, elles ne sont pas prises en compte dans ce cadre. Elles sont toutefois représentées dans le cadre de la NICE.

Tableau 1 : Échantillonnage des rôles de travail types associés à la cybersécurité

Supervision et gouvernance	Conception et développement	Exploitation et maintenance
Dirigeants principaux/dirigeantes principales de l'information ou techniciens/techniciennes en chef	Architectes d'entreprise	Gestionnaires de systèmes
Agents ou agentes de sécurité d'entreprise	Planificateurs ou planificatrices des exigences système	Gestionnaires des systèmes
Gestionnaires de programme	Analystes des activités	Analystes des systèmes
Gestionnaires de projets de TI	Développeurs/développeuses de logiciels ou programmeurs/programmeuses	Administrateurs ou administratrices de bases de données
Analystes financiers	Analystes des systèmes de contrôle	Analystes de systèmes de données
Spécialistes de l'apprentissage et du perfectionnement (p. ex. sensibilisation et formation en matière de sécurité)	Développeurs ou développeuses Web	Spécialistes du soutien technique

4 Résumé du Cadre canadien des compétences en matière de cybersécurité et de ses attributs

Le Cadre des compétences en matière de cybersécurité du Canada (figure 1) aborde la sécurité organisationnelle sous l'angle du cadre de la NICE. Par conséquent, le cadre canadien met l'accent sur quatre des sept catégories d'emplois initiales qui représentent la majorité du travail en cybersécurité accompli dans les entreprises et les industries canadiennes. Chacune des catégories d'emplois correspond à un domaine de responsabilité en matière de cybersécurité et elles sont toutes interconnectées.

Tirant avantage des principaux éléments et des principales caractéristiques du cadre de la NICE, le Cadre des compétences en matière de cybersécurité du Canada permet de faire ce qui suit :

- aider à préciser les lacunes dans la main-d'œuvre du domaine de la cybersécurité qui existent sur le marché du travail canadien en approchant la question du point de vue des entreprises proposé dans le cadre de la NICE et en établissant une distinction entre les rôles de base en cybersécurité et les rôles organisationnels qui assument certaines responsabilités en cybersécurité ou les rôles connexes dans le domaine
- simplifier la représentation du travail lié à la cybersécurité qui est commun à la plupart des organisations
- adapter facilement le cadre de manière à soutenir les responsabilités plus vastes ou généralistes qui sont communes aux PMO, alors qu'elles s'efforcent de répondre aux exigences fondamentales en matière de TI et de cybersécurité
- analyser les catégories d'emplois « Analyse », « Collecte et exploitation » et « Enquête » qui mettent l'accent sur la sécurité nationale et les rôles associés à l'application de la loi
- utiliser des termes compris par toute la collectivité élargie des affaires et des TI, en particulier le terme « Conception et développement » plutôt que « Securely provision »
- continuer de mettre l'accent sur les responsabilités en cybersécurité des rôles de travail dans les secteurs de la supervision et de la gouvernance, de la conception et du développement, et de l'exploitation et de la maintenance
- reconnaître le rôle central que joue la catégorie « Protection et défense » dans les opérations de cybersécurité

5 Conclusion

Le cadre de la NICE est une représentation exhaustive de la main-d'œuvre en cybersécurité qui reflète essentiellement la structure de la main-d'œuvre du gouvernement fédéral des États-Unis. À mesure que le cadre évolue et qu'il est adopté par les intervenants du secteur privé, la présente publication abordera certaines des préoccupations liées à son application directe au marché du travail canadien.

Le Cadre canadien des compétences en matière de cybersécurité présenté dans ce document est une présentation simplifiée du travail réalisé en cybersécurité dans la majorité des organisations du secteur privé et les plus petits organismes du secteur public. Il traite plus précisément des lacunes qui existent au sein des entreprises et de l'industrie. Ce cadre aborde la sécurité sous un angle organisationnel plutôt que du point de vue de la sécurité nationale afin de mieux interpréter le travail en cybersécurité des entreprises et de l'industrie. Il permet également aux entreprises d'établir un lien avec l'information exhaustive et détaillée comprise dans le cadre de la NICE.

Dans l'ensemble, il devrait aider à mieux guider les intervenantes et les intervenants en développement de la main-d'œuvre pour combler le déficit de compétences en cybersécurité.

6 Contenu complémentaire

6.1 Liste des acronymes, des abréviations et des sigles

Terme	Définition
ATC	Alliance des talents en cybersécurité
CNP	Classification nationale des professions
DG	Directeur général ou directrice générale
DPF	Dirigeant principal ou dirigeante principale des finances
DPI	Dirigeant principal ou dirigeante principale de l'information
IA	Intelligence artificielle
NICE	National Initiative for Cyber Education
NIST	National Institute of Standards and Technology
NPN	Normes professionnelles nationales
PMO	Petites et moyennes organisations
SCADA	Télésurveillance et acquisition de données (*Supervisory Control and Data Acquisition*)
SCI	Systèmes de contrôle industriels
TI	Technologies de l'information

6.2 Glossaire

Pour une description détaillée des catégories de la NICE, les domaines spécialisés et les rôles de travail, prière de consulter le cadre de la NICE.

Terme	Définition
Auteur de cybermenace	Les auteurs de cybermenace sont des États, des groupes ou des personnes qui cherchent à profiter des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes. L'universalisation d'Internet a fait en sorte que ces auteurs de menace peuvent compromettre, peu importe où ils se trouvent dans le monde, la sécurité des systèmes d'information au Canada.
Capacité	Une capacité permet d'adopter un comportement observable ou un comportement qui résulte d'un produit observable.
Catégories	En ce qui a trait à la NICE, les catégories fournissent la structure organisationnelle globale du cadre de la NICE. On retrouve sept catégories composées de domaines spécialisés et de rôles de travail.
Centre des opérations de sécurité (COS)	Un COS fournit des services opérationnels et d'autres services de sécurité au ministère, notamment la protection des personnes, de la propriété, des biens et de l'information. Le COS contient normalement les installations dans lesquelles les utilisateurs du système peuvent surveiller, afficher et gérer l'information (applications, vidéos et systèmes d'alarme), puis effectuer la répartition et répondre aux incidents. La conception et l'élaboration d'un

Terme	Définition
	COS devraient déterminer toutes les pièces destinées à accueillir le personnel, l'équipement et les fournitures associés aux activités de contrôle, d'alarme et de surveillance.
Code source libre	Code source que l'on rend disponible gratuitement pour qu'il puisse être modifié et redistribué, dans un contexte de développement communautaire. Ce terme s'applique également à tous les produits offerts gratuitement en ligne qui sont présentés au public comme pouvant être reproduits et distribués sans restriction.
Compétence	Capacité d'appliquer ou d'utiliser des connaissances, des compétences, des aptitudes, des comportements et des caractéristiques personnelles de manière à accomplir des tâches essentielles et des fonctions particulières ou à assumer un rôle ou un poste donné.
Connaissance	La connaissance est un corpus d'information que l'on applique directement à l'exercice d'une fonction.
Cybermenace	Une cybermenace est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.
Cyberopérations actives (ou cyberopérations offensives)	Aux États-Unis, il s'agit de cyberopérations visant à démontrer sa puissance en faisant acte de force dans le cyberespace. Au Canada, les cyberopérations actives sont régies par le projet de loi C-59 et menées, en vertu d'un mandat, par le Centre de la sécurité des télécommunications, qui est l'autorité ministérielle responsable de la conduite des activités visant à réduire, à interrompre, à influencer ou à contrecarrer les capacités, les intentions ou les activités de toute personne ou de tout État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité.
Cybersécurité	La cybersécurité est la protection des données numériques et de l'infrastructure où elles sont stockées.
Domaine de spécialisation	Le cadre de la NICE se divise en 32 domaines de spécialisation. Chacun d'entre eux représente un domaine de travail intensif ou une fonction associée à la cybersécurité ou à un emploi connexe.
Effectif	Ensemble des personnes au service d'une entreprise ou d'un organisme; ensemble des salariés travaillant dans un secteur donné et, par extension, affectés à une catégorie d'activités.
Habilité	Souvent définie comme l'ensemble de savoir-faire qui permettent à une personne de maîtriser une activité et de réussir dans l'accomplissement d'une tâche. Du point de vue psychomoteur, les habilités sont la capacité de manipuler physiquement un outil ou un instrument, comme un marteau. Les habiletés nécessaires en cybersécurité relèvent moins d'une manipulation physique d'outils et d'instruments que de l'utilisation d'outils, de cadres, de processus et de contrôles susceptibles d'avoir une incidence sur la posture de cybersécurité d'une organisation ou d'une personne.
Marché du travail	Le terme marché du travail est un concept généralisé qui désigne l'interaction entre l'offre (nombre de personnes disponibles pour travailler) et la demande (nombre d'emplois disponibles)
National Institute for Standards and Technology (NIST)	Faisant partie du Département du commerce des États-Unis, l'agence NIST américaine est l'organisme fédéral de normalisation dont la mission est de promouvoir l'innovation et la compétitivité industrielle aux États-Unis en faisant progresser la science, les normes et la technologie des mesures de manière à renforcer la sécurité économique et à améliorer notre qualité de vie.
Petites et moyennes organisations (PMO)	Organisations qui comptent moins de 499 employés.
Rôle de travail	Dans le cadre de la NICE, les rôles de travail représentent les groupes les plus détaillés de la cybersécurité et du travail connexe. Ils comprennent une liste des attributs nécessaires pour assumer ce rôle, notamment les connaissances, compétences et aptitudes et les tâches effectuées.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2020, novembre 2020.
2	National Institute of Standards and Technology, NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework, août 2017 (en anglais seulement).
3	National Institute of Standards and Technology, NIST Special Publication 800-181 Revision 2, Workforce Framework for Cybersecurity (NICE Framework), novembre 2020 (en anglais seulement).

Annexe A Supervision et gouvernance

La responsabilité globale de ce secteur d'activités ou de cette catégorie d'emplois consiste à assurer la direction et la gestion du programme de cybersécurité de l'organisation. La majeure partie du travail réalisé par ce sous-groupe professionnel est effectuée par des personnes qui appartiennent à des groupes de compétences professionnelles reconnues, comme la gestion (cadres supérieurs, cadres intermédiaires) et le commerce, les finances et l'administration (analystes des activités, analystes financiers, analystes des risques, communications). Par conséquent, plusieurs des rôles de travail correspondant à cette catégorie sont des rôles connexes (non essentiels) comme les politiques, les communications, la formation et la sensibilisation. Ceux-ci sont définis à l'annexe E.

En ce qui a trait au secteur d'activités ou à la catégorie d'emplois Supervision et gouvernance, des capacités avancées sont généralement exigées pour assurer la planification organisationnelle, la mesure et la gestion de la cybersécurité.

Cliquez sur le titre du rôle lié à la cybersécurité pour en savoir plus sur les exigences relatives aux connaissances, aux compétences, aux tâches et aux aptitudes de chaque rôle.

Rôles principaux liés à la cybersécurité

- Dirigeants principaux ou dirigeantes principales de la sécurité de l'information (DPSI)
- Agents ou agentes de sécurité des systèmes d'information (ASSI)
- Vérificateurs ou vérificatrices de la sécurité de l'information (SI)

Rôles connexes

- Directeurs généraux/directrices principales, hauts dirigeants ou propriétaires
- Dirigeants principaux/dirigeantes principales de l'information ou techniciens/techniciennes en chef
- Conseillers ou conseillères juridiques en cybersécurité
- Agents ou agentes à la protection des renseignements personnels ou gestionnaires de la protection de la vie privée
- Gestionnaires de la sécurité des communications (COMSEC)
- Développeurs/développeuses et gestionnaires de l'effectif en cybersécurité
- Développeurs/développeuses de curriculums pédagogiques en cybersécurité
- Responsables de la formation en cybersécurité
- Planificateurs/planificatrices de politiques et de stratégies en cybersécurité
- Gestionnaires de programme
- Gestionnaires de projets de TI
- Gestionnaires du soutien des produits
- Gestionnaires des investissements et des portefeuilles de TI
- Vérificateurs ou vérificatrices de programmes informatiques
- Analystes des activités
- Analystes financiers
- Analystes des risques
- Spécialistes des communications

- Administrateurs/administratrices de sites Web ou gestionnaires de communications en ligne
- Spécialistes de l'apprentissage et du perfectionnement
- Planificateurs ou planificatrices de la continuité des activités et de la résilience
- Spécialistes de l'approvisionnement

A.1 Dirigeants principaux ou dirigeantes principales de la sécurité de l'information (DPSI)

Référence au cadre de la NICE	Oversee and Govern, OV-EXL-001, Executive Cyber Leadership
Description fonctionnelle	Rôle du niveau de la direction qui consiste à assurer le bon déroulement des activités de l'organisation en matière de sécurité numérique et de l'information, et à rendre des comptes à cet égard. Les tâches assumées par le ou la titulaire comprennent la planification, la supervision et la gestion de l'élaboration et de la mise en œuvre de stratégies, des opérations liées à la cybersécurité, ainsi que du budget et des ressources qui assurent la protection des actifs informationnels de l'organisation tout au long de la chaîne d'approvisionnement. Les titulaires sont employés dans l'ensemble des secteurs public et privé.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait faire en sorte que l'organisation prenne des décisions susceptibles d'avoir une incidence importante sur ses activités. Ne pas comprendre pleinement les besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face aux menaces grandissantes.
Parcours de perfectionnement	On considère souvent qu'il s'agit de l'apogée d'une carrière en cybersécurité au sein d'une organisation donnée. Le ou la DPSI possède généralement une vaste expérience (plus de dix ans) en TI ou en systèmes et a également, de préférence, de l'expérience en gestion de la cybersécurité. Comme il s'agit d'un poste de direction, le parcours comprend également le développement des compétences, dont la formation, les études et l'expérience de nature non technique.
Autres titres	▪ Dirigeants principaux/dirigeantes principales de la sécurité ▪ Agents/agentes de sécurité du ministère ▪ Directeurs/directrices de la sécurité de l'information Remarque : Selon la taille de l'organisation et sa dépendance à l'égard des TI, ces fonctions professionnelles peuvent s'intégrer aux responsabilités des dirigeants principaux/dirigeants principales de la sécurité de l'information, des directeurs/directrices des techniques informatiques, des dirigeants principaux/dirigeantes principales de la résilience ou d'autres rôles similaires.
Classification nationale des professions (CNP) connexes	00011 – Cadres supérieurs/cadres supérieures – administration publique 00012 – Cadres supérieurs/cadres supérieures – services financiers, communications et autres services aux entreprises
Tâches	▪ Collaborer avec les principaux intervenants pour planifier et mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Développer et mettre en œuvre des plans stratégiques qui respectent les objectifs et les exigences de l'organisation en matière de sécurité ▪ Diriger et approuver la conception de systèmes de cybersécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour appuyer les objectifs de cybersécurité ▪ Conseiller d'autres membres de la haute direction sur les programmes, les politiques, les processus, les systèmes et les éléments de cybersécurité ▪ Assurer le développement et la mise en œuvre de contrôles de sécurité pour soutenir les objectifs de l'organisation

	▪ Examiner, approuver et superviser le suivi des politiques et des contrôles relatifs à la cybersécurité ▪ Veiller à ce que les plans d'intervention en cas d'incident, de reprise après sinistre et de continuité des activités soient mis en place et mis à l'essai ▪ Rédiger le mandat, superviser les enquêtes liées à la cybersécurité et les passer en revue ▪ Maintenir une compréhension actuelle du contexte des menaces informatiques dans l'organisation ▪ Planifier et superviser les évaluations et les contrôles de sécurité ▪ Superviser et gérer les relations avec les fournisseurs des produits et services de sécurité des TI acquis par l'organisation ▪ Former et encadrer les membres de l'équipe de sécurité ▪ Superviser ou gérer les mesures de protection ou de correction lorsqu'une vulnérabilité ou un cyberincident est découvert
Compétences requises pour l'éducation	Baccalauréat en informatique ou discipline connexe ou formation et expérience équivalentes.
Formation requise	De préférence, une formation axée sur les rôles qui soutient la gestion de la sécurité au niveau de la haute direction.
Expérience professionnelle requise	Expérience considérable (de cinq à dix ans) du domaine des TI avec de trois à cinq années d'expérience dans des rôles de gestion de la cybersécurité.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports
Compétences	Cette profession repose sur les compétences démontrées à un niveau de cadre supérieur, ce qui comprend celles mentionnées dans le cadre de la NICE. Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au 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 connaissances, compétences et aptitudes suivantes : ☐ Menaces et vulnérabilités organisationnelles, dont celles ci-dessous ☐ Situation de la menace à la cybersécurité ☐ Exigences en matière de gestion des vulnérabilités et gamme des mesures d'atténuation potentielles disponibles en l'absence de protocole de gestion des vulnérabilités ☐ Infrastructure de sécurité organisationnelle, dont les systèmes de protection et de défense ☐ Développement, mise en œuvre et affectation des ressources, du personnel et des technologies de manière à atteindre les objectifs de l'organisation en matière de sécurité ☐ Détermination des besoins et élaboration des politiques et des procédures de gestion de la cybersécurité et des risques liés à la 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

Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liés à la cybersécurité. En tant que principaux conseillers ou conseillères en sécurité auprès de la haute direction, il incombe aux DPSI de diriger la discussion. Une bonne compréhension des risques opérationnels est donc essentielle. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur la sécurité. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité organisationnelle et des répercussions sur le personnel, les ressources, les procédures et les politiques. Une telle utilisation devra être intégrée à une stratégie de sécurité et à un plan d'action pour l'organisation. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que 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 de l'organisation. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences approfondies pour ce qui est de la mise en œuvre d'une stratégie post-quantique et du soutien des processus au sein de l'organisation.

A.2 Agents ou agentes de sécurité des systèmes d'information (ASSI)

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Il s'agit d'un poste de gestion spécial en cybersécurité qui touche principalement la supervision de la sécurité des systèmes d'information au sein d'un ministère, d'une direction générale ou d'une organisation, et la production de rapports à cet égard. Les fonctions consistent essentiellement à assurer la planification et la gestion locales de la sécurité des systèmes sous sa responsabilité. Le poste relève directement ou indirectement du DPSI ou d'une autre autorité (p. ex. agent/agente de sécurité de l'entreprise, dirigeant principal/dirigeante principale de l'information ou délégué/déléguée).
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à des décisions ou à des actions susceptibles de compromettre la sécurité du système sous la responsabilité de l'ASSI. Selon le système touché, une telle compromission pourrait avoir des répercussions considérables sur les activités. Ne pas comprendre pleinement les besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face aux menaces grandissantes.
Parcours de perfectionnement	Il s'agit généralement d'un poste à temps partiel assumé par des personnes possédant une certaine expérience technique, sans toutefois être des « professionnels de la cybersécurité ». Dans de petites et moyennes organisations, ce poste pourrait également être occupé par des gestionnaires des TI ou des cadres supérieurs possédant une certaine expérience technique ou en sécurité.
Autres titres	▪ Dirigeants principaux/dirigeantes principales de la sécurité ▪ Agents/agentes de sécurité du ministère ▪ Directeurs/directrices de la sécurité de l'information **Remarque :** Selon la taille de l'organisation et sa dépendance à l'égard des TI, ces fonctions professionnelles peuvent s'intégrer aux responsabilités des dirigeants principaux/dirigeants principales de l'information, des directeurs/directrices des techniques informatiques, des dirigeants principaux/dirigeantes principales de la résilience ou d'autres rôles similaires.
Classification nationale des professions (CNP) connexes	20012 – Gestionnaires des systèmes informatiques
Tâches	▪ Collaborer avec les principaux intervenants pour planifier et mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Développer et mettre en œuvre des plans stratégiques qui respectent les objectifs et les exigences de l'organisation en matière de sécurité ▪ Diriger et approuver la conception de systèmes de cybersécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour appuyer les objectifs de cybersécurité ▪ Conseiller d'autres membres de la haute direction sur les programmes, les politiques, les processus, les systèmes et les éléments de cybersécurité ▪ Assurer le développement et la mise en œuvre de contrôles de sécurité pour soutenir les objectifs de l'organisation

	▪ Examiner, approuver et superviser le suivi des politiques et des contrôles relatifs à la cybersécurité ▪ Veiller à ce que les plans d'intervention en cas d'incident, de reprise après sinistre et de continuité des activités soient mis en place et mis à l'essai ▪ Rédiger le mandat, superviser les enquêtes liées à la cybersécurité et les passer en revue ▪ Maintenir une compréhension actuelle du contexte des menaces informatiques dans l'organisation ▪ Planifier et superviser les évaluations et les contrôles de sécurité ▪ Superviser et gérer les relations avec les fournisseurs des produits et services de sécurité des TI acquis par l'organisation ▪ Superviser ou gérer les mesures de protection ou de correction lorsqu'une vulnérabilité ou un cyberincident est découvert
Compétences requises pour l'éducation	Études postsecondaires en cybersécurité ou dans un domaine lié à l'informatique (p. ex. génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent).
Formation requise	Pour soutenir ce rôle, par exemple, une formation en gestion d'une équipe de cybersécurité, en gestion des incidents et en planification de sécurité constituerait un atout.
Expérience professionnelle requise	De trois à cinq années d'expérience dans le domaine des TI avec une certaine expérience en gestion.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports
Compétences	Cette profession repose sur les compétences démontrées à un niveau de cadre supérieur, ce qui comprend celles mentionnées dans le cadre de la NICE. Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au 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 connaissances, compétences et aptitudes suivantes : ☐ Menaces et vulnérabilités organisationnelles, dont celles ci-dessous ○ Situation de la menace à la cybersécurité ○ Exigences en matière de gestion des vulnérabilités et gamme des mesures d'atténuation potentielles disponibles en l'absence de protocole de gestion des vulnérabilités ○ Infrastructure de sécurité organisationnelle, dont les systèmes de protection et de défense ☐ Gestion d'une équipe de cybersécurité ☐ Développement, mise en œuvre et affectation des ressources, du personnel et des technologies de manière à atteindre les objectifs de l'organisation en matière de sécurité ☐ Détermination des besoins et élaboration des politiques et des procédures de gestion de la cybersécurité et des risques liés à la 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
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liés à la cybersécurité. En tant que conseillers ou conseillères en sécurité auprès de la haute direction, les ASSI doivent avoir une bonne compréhension des risques opérationnels. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur la sécurité. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité organisationnelle et des répercussions sur le personnel, les ressources, les procédures et les politiques. Une telle utilisation devra être intégrée à une stratégie de sécurité et à un plan d'action pour l'organisation. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que 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 de l'organisation. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences approfondies pour ce qui est de la mise en œuvre d'une stratégie post-quantique et du soutien des processus au sein de l'organisation.

A.3 Auditeurs/auditrices de la sécurité de l'information (SI)

Référence au cadre de la NICE	Aucune. Associé au rôle OV-PMA-005, IT Program Auditor.
Description fonctionnelle	À titre d'auditeurs ou d'auditrices spécialisés, les auditeurs et auditrices de la sécurité de l'information sont responsables de l'évaluation et des rapports pour ce qui est de la sécurité et de l'efficacité des systèmes informatiques et des contrôles connexes mis en place pour soutenir les systèmes informatiques, d'information et de sécurité des données de l'organisation, ainsi que leurs composants. L'audit effectué fait souvent l'objet d'un rapport à un cadre supérieur avec des recommandations quant aux changements ou aux améliorations à apporter.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait mener à un audit incomplet ou erroné, empêcher la détection de problèmes de système ou de processus critiques et faire en sorte que l'organisation ne puisse pas atteindre ses exigences en matière de sécurité, ce qui augmenterait les risques de compromission ou d'une panne sur les systèmes de sécurité.
Parcours de perfectionnement	L'occupation d'un tel poste est généralement précédée par une éducation formelle avec un diplôme dans le domaine des TI et par une expérience dans un rôle lié à la cybersécurité organisationnelle. Il convient également d'avoir une formation et une éducation spécialisées dans les pratiques d'audit des systèmes d'information et de la sécurité de l'information.
Autres titres	Auditeurs/auditrices de la cybersécurité Évaluateurs/évaluatrices des contrôles de sécurité Auditeurs/auditrices de la sécurité des TI
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel)
Tâches	▪ Collaborer avec les principaux intervenants pour établir une stratégie efficace d'audit de la sécurité de l'information qui définit les exigences en matière de vérification interne et externe ▪ Assurer la liaison avec les auditeurs externes conformément aux exigences de l'organisation en matière de soutien ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Développer et mettre en œuvre des plans d'audit interne qui respectent les objectifs et les exigences de l'organisation en matière de sécurité ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour appuyer les activités d'audit de SI ▪ Développer et déployer la mise à l'essai de stratégies sur les systèmes de SI ▪ Passer en revue les activités d'évaluation et d'autorisation de la sécurité ▪ Conseiller d'autres membres de la haute direction sur les programmes, les politiques, les processus, les systèmes et les éléments de cybersécurité ▪ Passer en revue et interpréter les politiques et les contrôles liés à la cybersécurité et à la sécurité de l'information ▪ Maintenir une compréhension actuelle du contexte des menaces informatiques dans l'organisation ▪ Planifier et exécuter des audits de SI internes ▪ Analyser et interpréter les résultats des audits de SI externes

	▪ Faire rapport des résultats et formuler des recommandations à la haute direction et aux propriétaires des systèmes
Compétences requises pour l'éducation	Études postsecondaires en cybersécurité ou dans un domaine lié à l'informatique (p. ex. génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent).
Formation requise	Formation spécialisée dans le domaine des TI, en audit de systèmes d'information ou en audit de sécurité informatique.
Expérience professionnelle requise	De trois à cinq années d'expérience en cybersécurité, de préférence en analyse des systèmes (p. ex. analyste des opérations de cybersécurité, analyste des vulnérabilités, analyste de la sécurité des systèmes informatiques).
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Exigences de conformité, dont les lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports ▪ Outils et systèmes d'audit de SI ▪ Évaluations des vulnérabilités ▪ Résultats des tests de pénétration ▪ Mesure des performances des systèmes informatiques
Compétences	Application de base des connaissances, compétences et aptitudes suivantes : ☐ Gestion de projet et de programme ☐ Politiques, pratiques et procédures d'audit de SI Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Exigences juridiques et relatives aux politiques et à la conformité ☐ Objectifs organisationnels et façon dont les TI, les données et les systèmes permettent la conduite des activités ☐ Politiques, pratiques et procédures d'audit de la sécurité de l'information ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Ressources, compétences et capacités d'audit externe ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte ☐ Responsabilités liées à la sécurité organisationnelle, reddition de comptes et mesure des performances ☐ Gestion, mesures et suivi du programme de cybersécurité ☐ Contrôles de cybersécurité organisationnels et agents responsables ☐ Menaces et vulnérabilités organisationnelles, dont celles ci-dessous ○ Situation de la menace à la cybersécurité ○ Évaluation des vulnérabilités et application de mesures d'atténuation ○ Infrastructure de sécurité organisationnelle, dont les systèmes de protection et de défense ☐ Sécurité tout au long du cycle de développement des systèmes et des logiciels ☐ Sécurité de la chaîne d'approvisionnement ☐ Intégration, mise à l'essai et déploiement de systèmes ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) et arrangements en matière d'approvisionnement
Futures tendances ayant une incidence sur les	▪ La dépendance accrue aux 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 que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur la sécurité.

compétences clés	▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité de l'organisation, des implications sur les contrôles de sécurité et de la façon dont ils seront mesurés et évalués par rapport aux objectifs de sécurité. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Les audits des outils et systèmes de défense sont donc appelés à évoluer. ▪ Des mécanismes visant à soutenir le degré 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 sera nécessaire de comprendre la façon dont ces outils fonctionnent, comment leurs performances peuvent être mesurées et quelles activités d'audit pourraient être nécessaires. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation.

Annexe B Conception et développement

Ce secteur d'activités et cette catégorie d'emplois concernent le développement d'infrastructures, de systèmes et de logiciels sécurisés. Il s'agit d'un secteur hautement technique du travail en cybersécurité. La majeure partie de ce travail relève des responsabilités des ingénieurs informaticiens/ingénieures informaticiennes (CNP 21311), des développeurs/développeuses et programmeurs/programmeuses de systèmes informatiques (CNP 21230), des spécialistes en informatique (CNP 21222) et des spécialistes de la cybersécurité (CNP 21220). Comme il s'agit de professions courantes, et qu'elles sont également définies dans le cadre de la NICE, elles ne seront pas abordées dans le présent document.

Étant donné l'orientation de ce secteur d'activités, nous nous attarderons à l'application d'une compréhension technique approfondie dans un contexte opérationnel pour mieux soutenir les résultats de l'organisation en matière de cybersécurité.

Cliquez sur le titre du rôle lié à la cybersécurité pour en savoir plus sur les exigences relatives aux connaissances, aux compétences, aux tâches et aux aptitudes de chaque rôle.

Rôles principaux liés à la cybersécurité

- Architectes de la sécurité
- Technologues et ingénieurs/ingénieures en sécurité
- Technologues et ingénieurs/ingénieures en chiffrement
- Technologues et ingénieurs/ingénieures en technologie opérationnelle
- Évaluateurs/évaluatrices de logiciels sécurisés
- Spécialistes des tests et de l'évaluation de la sécurité
- Analystes des systèmes de technologie opérationnelle
- Analystes de la sécurité de la chaîne d'approvisionnement
- Développeurs/développeuses en sécurité des systèmes d'information
- Ingénieurs/ingénieures et analystes en automatisation de la sécurité
- Cryptographes et cryptanalystes

Rôles connexes

- Responsables de l'autorisation (généralement les DPI ou les propriétaires du système)
- Architectes d'entreprise
- Développeurs/développeuses de logiciels
- Planificateurs/planificatrices des exigences système
- Spécialistes des tests et de l'évaluation des systèmes
- Développeurs/développeuses de systèmes
- Développeurs ou développeuses Web

B.1 Architectes de la sécurité

Référence au cadre de la NICE	Securely Provision, SP-ARC 002, Security Architect
Description fonctionnelle	Le ou la titulaire conçoit, élabore et surveille la mise en œuvre des structures de sécurité des réseaux et des ordinateurs pour une organisation, s'assure que les exigences de sécurité sont prises en compte adéquatement dans tous les aspects de l'infrastructure et que le système soutient les processus organisationnels.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait mener à des conceptions ou à des architectures déficientes susceptibles de donner lieu à des défaillances ou à l'exploitation de vulnérabilités qui pourraient mettre en péril les systèmes informatiques dont dépend l'organisation. Ne pas comprendre pleinement les besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face aux menaces grandissantes.
Parcours de perfectionnement	Les personnes qui occupent ce poste suivent essentiellement l'éducation et le parcours de carrière du rôle d'architecte d'entreprise. Il s'agit d'un rôle de spécialiste émergent que l'on retrouve principalement dans de grandes sociétés des technologies ou des fournisseurs de services partagés, de systèmes ou de sécurité.
Autre titre	Architectes de sécurité d'entreprise
Classification nationale des professions (CNP) connexes	21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21220 – Spécialistes de la cybersécurité
Tâches	▪ Collaborer avec les principaux intervenants pour mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Définir et passer en revue les systèmes de technologie et d'information de l'organisation, et s'assurer qu'ils sont conformes aux exigences en matière de sécurité ▪ Reconnaître les plans de reprise après sinistre appropriés et les fonctions de continuité des activités, notamment les exigences en matière de basculement ou de sauvegarde pour la restauration des systèmes ▪ Planifier et développer des architectures de sécurité robustes pour les systèmes et les réseaux et faire des recherches à ce sujet ▪ Faire des recherches sur les technologies actuelles et nouvelles pour comprendre les capacités des réseaux ou des systèmes requis ▪ Préparer des estimations de coûts et cerner les problèmes d'intégration ▪ Effectuer des tests de vulnérabilité, des analyses des risques et des évaluations de sécurité ▪ Faire des recherches et élaborer un contexte de sécurité des systèmes, et définir les exigences d'assurance de la sécurité en fonction des normes de l'industrie et des politiques et pratiques en matière de cybersécurité ▪ S'assurer que les systèmes et les architectures acquis ou développés sont conformes aux politiques et aux pratiques de cybersécurité d'une organisation ▪ Effectuer des examens de sécurité, cerner les lacunes ou déterminer la capacité des architectures et des conceptions de sécurité (p. ex. pare-feu, réseaux privés virtuels, routeurs, serveurs, etc.) et élaborer un plan de gestion des risques pour la sécurité ▪ Préparer des rapports techniques qui documentent le processus de développement de l'architecture ▪ Documenter et traiter les exigences de l'organisation en matière de sécurité de l'information, d'architecture de cybersécurité et d'ingénierie de la sécurité des systèmes tout au long du cycle de vie des systèmes

	▪ Donner des conseils sur les exigences en matière de sécurité et les activités du processus de gestion des risques ▪ Soutenir la gestion des incidents et l'analyse postérieure qui oriente les opérations de reprise ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle
Compétences requises pour l'éducation	Études postsecondaires en infrastructure et architecture informatique (p. ex. génie informatique, architecture de systèmes informatiques).
Formation requise	Formation spécialisée dans les concepts, les principes et les pratiques de l'architecture de sécurité. Formation sur le soutien des outils de sécurité nécessaires à l'exécution des tâches liées au rôle.
Expérience professionnelle requise	Il est préférable d'avoir de la formation et de l'expérience en infrastructure de sécurité des TI, en analyse des besoins ou en gestion de programme – de cinq à dix ans d'expérience pertinente en TI pour un niveau avancé.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Architectures de système ▪ Outils et applications de mise en correspondance des TI ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports
Compétences	Cette profession repose sur les compétences démontrées à un niveau de cadre supérieur, ce qui comprend celles mentionnées dans le cadre de la NICE. Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Besoins opérationnels en matière de sécurité ☐ Exigences juridiques et relatives aux politiques et à la conformité ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte ☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet ☐ Concepts de la cryptographie et de la gestion des clés cryptographiques ☐ Dispositifs de réseau privé virtuel et chiffrement ☐ Concepts et pratiques d'ingénierie appliqués à la sécurité et à l'architecture des systèmes ☐ Concepts d'architecture de sécurité et modèles de référence relatifs à l'architecture d'entreprise ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Authentification, autorisation et méthodes de contrôle de l'accès ☐ Méthodes et processus de mise à l'essai et d'évaluation de la sécurité ☐ 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 des 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 exécution de la reprise des systèmes

Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance approfondie des architectures organisationnelles et des fournisseurs de services pour déterminer et gérer les risques liés à la cybersécurité. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) pourrait avoir sur la sécurité et la façon dont les contrôles de sécurité sont intégrés à l'architecture de l'organisation. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'architecture et à l'infrastructure de sécurité globales et des répercussions sur le personnel, les ressources, les procédures et les politiques. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes devront donc être intégrées localement à l'architecture de sécurité. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que 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 auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation et l'intégrer dans toute l'architecture.

B.2 Technologues et ingénieurs/ingénieures en sécurité

Cela comprend les technologues et ingénieurs/ingénieures en chiffrement et les technologues et ingénieurs/ingénieures en technologie opérationnelle.

Référence au cadre de la NICE	Securely Provision, R&D Specialist, SP-TRD-001
Description fonctionnelle	En tenant compte des références, de la documentation sur la sécurité organisationnelle, des conseils en matière de sécurité des TI et des outils et ressources nécessaires, le ou la 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 des systèmes et toutes les phases du cycle de développement de système (CDS).
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou l'omission de tenir compte des exigences organisationnelles, des besoins opérationnels et des menaces pourrait mener à une mauvaise conception du système ou à l'intégration de systèmes ou dispositifs vulnérables à la compromission, ce qui peut avoir des implications importantes sur les objectifs de l'organisation, y compris mener à une possible défaillance irrémédiable des systèmes.
Parcours de perfectionnement	Le ou la titulaire du rôle a généralement reçu une éducation formelle et possède de cinq à dix ans d'expérience dans des fonctions connexes liées à l'ingénierie des TI, à la conception de systèmes ou à l'intégration de systèmes. L'occupation d'un tel poste est généralement précédée par une formation, une éducation ou une expérience spécialisée dans les capacités des systèmes. Il peut être utilisé dans des contextes généraux ou spécialisés comme la cryptographie et le chiffrement, la mise à l'essai et l'évaluation de la sécurité, ou les technologies opérationnelles (SCI, SCO/SCADA).
Autres titres	▪ Concepteurs/conceptrices en sécurité ▪ Analystes des exigences de sécurité ▪ Ingénieurs/ingénieures de la sécurité réseau ▪ Technologues et ingénieurs/ingénieures en sécurité ▪ Ingénieurs/ingénieures en technologie opérationnelle ▪ Ingénieurs/ingénieures en chiffrement
Classification nationale des professions (CNP) connexes	21310 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21222 – Spécialistes en informatique 22310 – Technologues et techniciens/techniciennes en génie électrique et électronique
Tâches	▪ Définir ou valider les besoins opérationnels en matière de sécurité et les exigences de sécurité ▪ Examiner et analyser les architectures et les documents de conception des TI et de la TO, ainsi que les systèmes, les protocoles, les services, les contrôles, les appareils, les applications, les algorithmes cryptographiques et de chiffrements connexes conformément aux exigences de sécurité et aux normes de l'industrie ▪ Élaborer et passer en revue les cas d'utilisation des systèmes ▪ Identifier les menaces techniques et les vulnérabilités qui touchent les systèmes ▪ Gérer la configuration de la sécurité des TI et de la TO ▪ Analyser les outils et techniques de sécurité liés aux TI et à la TO ▪ Analyser les données de sécurité et fournir des conseils et des rapports ▪ Analyser les statistiques de sécurité liées aux TI et à la TO

	▪ Préparer des rapports techniques comme l'analyse des options relatives à des solutions de sécurité informatique et des plans de mise en œuvre ▪ Procéder à la vérification et à la validation indépendantes (VVI) des projets de sécurité des TI et de la TO ▪ Superviser les audits de sécurité informatique liés aux TI et à la TO ▪ Prodiguer des conseils sur la sécurité des projets des TI ou de la TO ▪ Prodiguer des conseils sur les politiques, les plans et les pratiques liés à la sécurité des TI ou de la TO ▪ Passer en revue les plans de systèmes, les plans de continuité des activités (PCA) et les plans de reprise après sinistre (PRS) ▪ Concevoir, développer et exécuter des tests et exercices des protocoles de sécurité liés aux TI et à la TO ▪ Passer en revue, concevoir et fournir le matériel de formation
Compétences requises pour l'éducation	Diplôme d'ingénieur/ingénieure ou de technologue pertinent (selon les exigences de l'organisation).
Formation requise	Certificat valide de l'industrie avec spécialisation en cybersécurité (p. ex. sécurité de réseau, cryptographie, intégration de systèmes, etc.).
Expérience professionnelle requise	Expérience modérée (de trois à cinq ans) de la sécurité, ainsi que de la conception, de l'intégration, de la mise à l'essai et du soutien des systèmes connexes.
Outils et technologies	▪ 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 des intrusions et de protection contre les intrusions, les scanneurs et les alarmes ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Logiciels et systèmes d'authentification ▪ Processus de gestion des vulnérabilités et systèmes d'évaluation des vulnérabilités, y compris les tests de pénétration le cas échéant ▪ Services de sécurité fournis, le cas échéant ▪ Outils et techniques d'essai et d'évaluation de la sécurité
Compétences	Les technologues et ingénieurs/ingénieures en sécurité doivent posséder des connaissances, compétences et aptitudes de base, tandis que les ingénieurs/ingénieures de la sécurité doivent posséder des connaissances, compétences et aptitudes avancées dans les domaines suivants : ☐ 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 sécurité et modèles de référence relatifs à l'architecture d'entreprise ☐ Réseautage logiciel (SDN), virtualisation des fonctions réseau (NFV) et fonctions réseau virtualisées (VNF) ☐ Sécurité des systèmes pendant l'intégration et la configuration ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Méthodes et processus de mise à l'essai et d'évaluation de la sécurité ☐ Sécurité tout au long du cycle de développement de systèmes et de logiciels ☐ Méthodologies et applications d'évaluation des vulnérabilités et de tests de pénétration ☐ Méthodes d'essais et d'évaluation des systèmes et des logiciels ☐ Conception de la sécurité basée sur les preuves ☐ Élaboration et mise à l'essai des modèles de menace ☐ Gestion de projet et évaluation de la sécurité tout au long du cycle de vie du projet ☐ Processus d'approvisionnement et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Prestation de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et prestation de séances d'information et de rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres) De plus, dans les environnements à assurance élevée, de chiffrement et de cryptographie :

	☐ Gouvernance de la sécurité dans les environnements à assurance élevée, de chiffrement et de cryptographie : ☐ Modélisation avancée des menaces et gestion des risques dans les environnements comportant de l'information sensible ☐ Politiques et pratiques liées à la gestion des clés (y compris la sécurité des communications [COMSEC pour *Communications Security*]) ☐ Normes de sécurité des émissions ☐ Établissement de zones de sécurité physiques et des TI ☐ Cryptographie et chiffrement, dont les algorithmes et les chiffres ☐ Sténographie ☐ Mise à l'essai et en œuvre de solutions interdomaines ☐ Gestion des clés, produits de gestion des clés et cycle de vie de la certification ☐ Tactiques, techniques et procédures employées par des auteurs de menaces persistantes avancées dotés de moyens sophistiqués ☐ Technologie post-quantique et à résistance quantique ☐ Évaluation et audit des réseaux et des systèmes cryptographiques et de chiffrement De plus, dans des environnements de technologie opérationnelle (SCI, SCO/SCADA) : ☐ Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation ☐ Système de contrôle : ○ Défenses de l'architecture et des systèmes ○ Gouvernance et gestion dans des environnements divers ○ Surfaces d'attaque, menaces et vulnérabilités ○ Surveillance de la sécurité, outils et techniques ☐ Systèmes et protocoles de TI dans les configurations des systèmes de contrôle ☐ Intégration des systèmes de contrôles de TI et de TO ☐ Renforcement de la sécurité et surveillance des systèmes de contrôle liés à la TO ☐ Processus d'évaluation et d'autorisation de sécurité des systèmes de TO ☐ Plans et activités d'intervention en cas d'incident dans les environnements des systèmes de contrôle ☐ Planification de la continuité des activités et plans et activités de reprise après sinistre dans les environnements de systèmes de contrôle
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités des services à offrir et de la façon dont ils sont intégrés aux réseaux de l'organisation. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités du dispositif, il faudra évaluer les risques qui pèsent sur l'organisation et mettre en œuvre des mesures d'atténuation au niveau de risque acceptable. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront dans l'organisation et des possibles implications sur le plan de la sécurité. Si des outils de sécurité automatisés sont utilisés, il conviendra de définir les exigences en matière de mise à l'essai, d'intégration et de contrôle, ainsi que de conseiller ou de former les responsables de ces activités par rapport aux changements de processus et de procédures qui en découleront. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation.

B.3 Évaluateurs/évaluatrices de logiciels sécurisés

Référence au cadre de la NICE	Security Provision, SP Dev-001, Secure Software Assessor
Description fonctionnelle	En tenant compte des références, de la documentation sur la sécurité organisationnelle, des conseils en matière de sécurité des TI et des outils et ressources nécessaires, le ou la titulaire analyse la sécurité des applications, des logiciels ou des programmes utilitaires spécialisés et produit des résultats exploitables.
Conséquence d'une erreur ou risque	Une erreur, une négligence ou une information désuète pourrait faire en sorte que des vulnérabilités touchant des logiciels et des outils Web mettent en péril les systèmes et les services d'une organisation.
Parcours de perfectionnement	L'occupation de ce poste exige généralement une éducation formelle et de cinq à dix ans d'expérience dans le domaine du développement de logiciels. Ce rôle exige souvent une formation, une éducation ou de l'expérience spécialisée dans le domaine des logiciels sécurisés et de l'évaluation des vulnérabilités pour assurer la sécurité des logiciels et des applications.
Autres titres	▪ Développeurs/développeuses et programmeurs/programmeurs de logiciels sécurisés ▪ Spécialistes de la mise à l'essai et de l'évaluation de logiciels ▪ Analystes et évaluateurs/évaluatrices des vulnérabilités
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 21232 – Développeurs/développeuses et programmeurs/programmeuses de logiciels
Tâches	▪ Définir ou valider les besoins opérationnels en matière de sécurité et les exigences de sécurité ▪ Examiner et analyser les architectures et les documents de conception des TI, ainsi que les systèmes, les protocoles, les services, les contrôles, les appareils, les applications, les algorithmes cryptographiques et de chiffrements connexes conformément aux exigences de sécurité et aux normes de l'industrie ▪ Chercher, analyser et utiliser des techniques et processus de développement d'applications sécurisées ▪ Analyser les données de sécurité et fournir des conseils et des rapports ▪ Élaborer et mettre en œuvre des procédures de mise à l'essai et de validation de systèmes logiciels ou d'applications, de programmation et de codage sécurisé, et rendre compte de la fonctionnalité et de la résilience ▪ Élaborer et passer en revue les cas d'utilisation des systèmes ▪ Effectuer des analyses des vulnérabilités et des examens des systèmes ou applications logiciels, et examiner les contrôles et les mesures nécessaires pour protéger les systèmes ou les applications logiciels ▪ Préparer des rapports sur les systèmes logiciels, le développement, les applications, les correctifs ou les versions qui rendraient les systèmes vulnérables ▪ Élaborer des contre-mesures contre l'exploitation potentielle de vulnérabilités dans les systèmes ▪ Effectuer une analyse des risques chaque fois qu'une application ou un système fait l'objet d'une modification ▪ Préparer des rapports techniques comme l'analyse des options relatives à des solutions de sécurité informatique et des plans de mise en œuvre ▪ Procéder à la vérification et à la validation indépendantes (VVI) des projets de logiciels ▪ Prodiguer des conseils sur les politiques, les plans et les pratiques liés à la sécurité des logiciels ▪ Passer en revue, concevoir et fournir le matériel de formation

Compétences requises pour l'éducation	Diplôme pertinent en informatique ou lié à la programmation, à la conception de logiciels ou au développement de logiciels.
Formation requise	Certificat valide de l'industrie en développement de logiciels sécurisés et en mise à l'essai de la sécurité logicielle.
Expérience professionnelle requise	Expérience modérée (de trois à cinq ans) en développement de logiciels avec expérience modérée (de trois à cinq ans) des activités de développement de logiciels sécurisés.
Outils et technologies	▪ 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 des intrusions et de protection contre les intrusions, les scanneurs et les alarmes ▪ Information de source ouverte sur la sécurité des logiciels et des applications (p. ex. OWASP) ▪ Systèmes de gestion des événements et des 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 des vulnérabilités et systèmes d'évaluation des vulnérabilités, y compris les tests de pénétration le cas échéant ▪ Bases de données communes sur les vulnérabilités ▪ Sites de collaboration sociale sur le développement de logiciels (p. ex. GitHub) ▪ Services de sécurité fournis, le cas échéant
Compétences	Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts d'architecture de sécurité et modèles d'architecture de sécurité de l'information d'entreprise ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Processus d'approvisionnement en logiciels et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Outils, procédures et pratiques de mise à l'essai et d'évaluation des systèmes de sécurité des TI Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Modèles, processus et principes du génie logiciel ☐ Cycle de développement des logiciels et gestion de projets de logiciels ☐ Processus, procédures, pratiques, outils et techniques de codage et de développement de logiciels sécurisés ☐ Besoins opérationnels en matière de sécurité, dont les exigences relatives à la conformité ☐ Caractéristiques et exigences relatives à la sécurité des données ☐ Contrôles de sécurité pour le développement de logiciels ☐ Normes de développement de logiciels ☐ Normes relatives aux logiciels sécurisés ☐ Méthodes et processus de mise à l'essai et d'évaluation de logiciels sécurisés ☐ Méthodologies et applications d'évaluation des vulnérabilités et de tests de pénétration ☐ Élaboration et mise à l'essai des modèles de menace ☐ Analyse et évaluation des vulnérabilités ☐ Techniques et activités relatives aux tests de pénétration ☐ Investigation et analyse des vulnérabilités logicielles et des violations ☐ Mise en place et gestion d'un environnement de test sécurisé des logiciels et des applications Web ☐ Prestation de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et prestation de séances d'information et de rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres)
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités des services à offrir, des applications et systèmes logiciels utilisés et de la façon dont ils sont intégrés aux réseaux de l'organisation. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités du dispositif, il

	faudra évaluer les risques qui pèsent sur l'organisation et mettre en œuvre des mesures d'atténuation au niveau de risque acceptable. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils susceptibles de soutenir le développement, la mise à l'essai et l'intégration des logiciels seront utilisés et des possibles implications sur le plan de la sécurité. Si des outils de sécurité automatisés sont utilisés pour le développement et l'évaluation des logiciels, il conviendra de définir les exigences en matière de mise à l'essai, d'intégration et de contrôle, ainsi que de conseiller ou de former les responsables de ces activités par rapport aux changements de processus et de procédures qui en découleront. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Il faudra donc procéder localement à des évaluations créatives de la robustesse de la sécurité des logiciels et des applications, ainsi que des possibles stratégies d'atténuation. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique qui s'applique à l'environnement des logiciels et des applications.

B.4 Spécialistes des tests et de l'évaluation de la sécurité

Référence au cadre de la NICE	Securely Provision, Security Testing and Evaluation, SP-TST-001
Description fonctionnelle	Le ou la titulaire planifie, prépare et met à l'essai des dispositifs de sécurité, des systèmes d'exploitation, des logiciels et du matériel pour évaluer les résultats en fonction des spécifications, des politiques et des exigences définies. Il documente les résultats et formule des recommandations qui peuvent améliorer la confidentialité, l'intégrité et la disponibilité de l'information.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais justement pourrait faire en sorte que des systèmes, des logiciels ou des services de TI soient intégrés et mis en œuvre avec des vulnérabilités susceptibles d'accroître l'exposition aux menaces et de mettre l'organisation à risque. Une telle compromission pourrait avoir des répercussions considérables sur les activités.
Parcours de perfectionnement	L'occupation de ce poste exige généralement une éducation formelle et de cinq à dix ans d'expérience en sécurité des TI. L'occupation d'un tel poste est généralement précédée par une formation, une éducation ou une expérience spécialisée dans la mise à l'essai et la mesure des systèmes.
Autre titre	Évaluateurs/évaluatrices de la sécurité
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel)
Tâches	▪ Tester, évaluer et vérifier les systèmes en développement, les systèmes échangeant des renseignements électroniques avec d'autres systèmes, les logiciels et le matériel du système d'exploitation connexe, 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 fondées sur les constatations ▪ Élaborer des plans d'essai pour tenir compte des spécifications, des politiques et des exigences ▪ Valider les spécifications, les politiques et les exigences relatives à la testabilité ▪ Créer des preuves vérifiables des mesures de sécurité ▪ Préparer des évaluations qui documentent les résultats des tests et toute vulnérabilité à la sécurité présente ▪ Déployer, valider et vérifier le logiciel du système d'exploitation de l'infrastructure réseau ▪ Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation ▪ Former et encadrer les membres de l'équipe de sécurité
Compétences requises pour l'éducation	Baccalauréat en informatique ou discipline connexe ou formation et expérience équivalentes.
Formation requise	Formation en mesure, évaluation et mise à l'essai des systèmes.
Expérience professionnelle requise	Expérience considérable (de cinq à dix ans) dans le domaine des TI avec, de préférence, de trois à cinq ans d'expérience dans un rôle lié à la sécurité des systèmes visant à soutenir les évaluations de sécurité et les audits informatiques. Expérience de travail dans des environnements de test sécurisés.

Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Architecture de système ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports ▪ Outils, techniques, procédures et protocoles liés aux stratégies de mise à l'essai et d'évaluation des systèmes ▪ Exigences juridiques et de conformité
Compétences	Application de base des connaissances, compétences et aptitudes suivantes : ☐ Processus d'approvisionnement en matière de sécurité et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Processus d'ingénierie des systèmes Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Stratégies de mise à l'essai et d'évaluation des systèmes informatiques ☐ Infrastructure et ressources liées à la mise à l'essai et l'évaluation des systèmes informatiques ☐ Outils, procédures et pratiques de mise à l'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 et des logiciels de cybersécurité ☐ Modèles et architecture de sécurité réseau ☐ Conduite de tests indépendants de validation et de vérification de la sécurité ☐ Méthodes et techniques d'essai et d'évaluation des systèmes ☐ Conception de tests, élaboration de scénarios et examen du niveau de préparation ☐ Mise à l'essai de l'intégration des systèmes ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Concepts d'architecture de sécurité et modèles d'architecture de sécurité de l'information d'entreprise ☐ Établissement des politiques et des exigences en matière d'essai et d'évaluation ☐ Collecte, analyse, vérification et validation des données d'essai, et traduction des données et des résultats d'essai en conclusions ☐ Conception et documentation de stratégies d'essai et d'évaluation ☐ Rédaction de rapports techniques, d'essai et d'évaluation
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 systèmes organisationnels, à la façon dont ces systèmes sont intégrés et comment ils seront mis à l'essai et évalués. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur les systèmes de l'organisation. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité organisationnelle et des répercussions sur les pratiques en matière de mise à l'essai et d'évaluation. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes qui exigeront une évaluation continue des pratiques et des outils de mise à l'essai et d'évaluation. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place et les répercussions sur la mise à l'essai et l'évaluation de la sécurité. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce

	qui est de la mise en œuvre d'une stratégie post-quantique pertinente pour la mise à l'essai et l'évaluation du chiffrement et du degré de résistance à l'informatique quantique.

B.5 Analystes des systèmes de technologie opérationnelle

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Formuler des conseils et assurer l'efficacité de la cybersécurité dans des contextes liés à la technologie opérationnelle (TO) (SCI/SCO/SCADA). Collaborer avec les technologues et ingénieurs/ingénieures et des systèmes provenant de diverses disciplines associées aux systèmes gérés au moyen de la TO (p. ex. ingénieurs/ingénieures en mécanique des fluides, de centrales ou de systèmes mécaniques).
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait donner lieu à une défaillance irrémédiable de la TO et des systèmes connexes qui sont utilisés aux fins de gestion. Dans plusieurs cas, une telle situation peut avoir des répercussions considérables sur les activités de l'organisation et, dans certains cas, peut entraîner de graves dommages pour des personnes (p. ex. dans les systèmes d'infrastructures essentielles).
Parcours de perfectionnement	Après une formation technique, le ou la titulaire mène souvent des activités liées aux systèmes de TI ou de TO qui posent les bases d'un travail plus spécialisé en cybersécurité dans l'environnement de la TO. De même, les professionnels de la cybersécurité qui travaillent généralement dans un environnement informatique peuvent passer aux systèmes de TO s'ils bénéficient d'une formation et d'un enseignement spécialisés en TO et en intégration de systèmes.
Autres titres	Conseillers/conseillères en sécurité de la TO Techniciens/techniciennes en sécurité de la TO Analystes de la sécurité – SCI/SCO/SCADA
Classification nationale des professions (CNP) connexes	21310 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21220 – Spécialistes de la cybersécurité 21222 – Spécialistes en informatique 22310 – Technologues et techniciens/techniciennes en génie électrique et électronique
Tâches	▪ Collaborer avec les principaux intervenants pour mettre en place un programme efficace de gestion des risques liés à la cybersécurité dans tout l'environnement de TO ▪ Rechercher et soutenir la conception de solutions de cybersécurité dans un contexte de TO ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Rédiger, mettre en œuvre et maintenir des politiques, des normes et des procédures de sécurité de TI ou de TO ▪ Contrôler et gérer les exigences et contrôles de cybersécurité dans tout l'environnement de TO ▪ Évaluer et analyser la posture de cybersécurité sur l'ensemble des systèmes de TO et recommander des mesures d'atténuation et de gestion des risques pour les vulnérabilités ▪ Collaborer avec les autres intervenants, soutenir la conception et le développement de solutions visant à satisfaire aux exigences organisationnelles et techniques dans l'environnement de TO ▪ Gérer l'intégration technique entre les TI et la TO

	▪ Définir et tenir à jour les jeux d'outils et les procédures qui soutiennent la surveillance et la gestion de la TO ▪ Avec les autres intervenants, développer des plans d'intervention en cas d'incidents liés à la cybersécurité qui définissent clairement le rôle des personnes prenant part à la gestion et à la maintenance des systèmes de la TO ▪ Préparer des rapports techniques ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés à la TO
Compétences requises pour l'éducation	Baccalauréat en informatique ou en génie informatique ou discipline connexe ou formation et expérience équivalentes.
Formation requise	Formation spécialisée en cybersécurité de la TO, ainsi que dans les outils et techniques obligatoires qui sont propres aux systèmes.
Expérience professionnelle requise	Le rôle de premier échelon exige, de préférence, une expérience de travail modérée de deux à trois ans dans un environnement de TO.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités liées à la TO et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Système de gestion des événements et des incidents de sécurité et/ou systèmes et réseaux de signalement des incidents qui peuvent être utilisés pour les incidents de cybersécurité liés à la TO ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports ▪ Outils, techniques et procédures liées à la sécurité de la TO
Compétences	Sachant que les analystes de la TO n'auront pas nécessairement les mêmes antécédents en TI, il convient d'être en mesure de mettre en pratique les connaissances, compétences et aptitudes suivantes : ☐ Systèmes de télémétrie, communications de données, acquisition de données et contrôle des processus ☐ Systèmes d'exploitation, réseaux et 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 ☐ Systèmes et applications de gestion des bases de données ☐ Administration et optimisation de bases de données ☐ Méthodes et processus de mise à l'essai et d'évaluation de la sécurité ☐ Mesures ou indicateurs des problèmes de rendement, de disponibilité, de capacité ou de configuration du système ☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défaillances Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Logiciels et matériel de la TO, contrôleurs logiques programmables et relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris l'incidence et l'évaluation des dispositifs de l'IdO) ☐ Exigences juridiques et relatives à la conformité, dont les responsabilités organisationnelles en matière de sécurité publique et dans les lieux de travail liées à la TO ou à la production ☐ Normes et pratiques exemplaires de l'industrie, en particulier celles liées aux environnements industriels dans l'espace de cybersécurité

	☐ Gestion, mesure et surveillance de la cybersécurité ☐ Systèmes de contrôle (applicables aux environnements industriels et de production) ☐ Intégration et convergence des TI et de la TO ☐ Sécurité des processus et analyse des risques ☐ Analyse et intégration des systèmes ☐ Résolution de problèmes dans des environnements de systèmes complexes ☐ Communications techniques, notamment la rédaction de rapports sur les problèmes techniques multidisciplinaires
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 la TO, ainsi que 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 que l'option « Prenez vos appareils personnels » (PAP) et la surveillance et l'exploitation à distance pourraient avoir sur l'IdO et les dispositifs. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité organisationnelle et des répercussions sur les exigences liées à la TO, les procédures et les politiques. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Pour le chiffrement depuis des systèmes de TO, des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation.

B.6 Analystes de la sécurité de la chaîne d'approvisionnement

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Le ou la titulaire recueille et analyse des données afin de cerner les failles et les vulnérabilités en matière de cybersécurité dans les opérations de la chaîne d'approvisionnement d'une organisation. Il donne des conseils et de l'orientation pour aider à réduire ces risques liés à la chaîne d'approvisionnement.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait faire en sorte que l'organisation prenne des décisions susceptibles d'avoir une incidence importante sur ses activités. Ne pas comprendre pleinement les besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face aux menaces grandissantes.
Parcours de perfectionnement	S'inspirant généralement des rôles d'analystes de la cybersécurité (p. ex. analystes des opérations de cybersécurité, analystes des vulnérabilités, etc.), ce rôle peut être assumé par un large éventail de professionnels capables d'évaluer et de fournir des renseignements sur les menaces potentielles qui pèsent sur la chaîne d'approvisionnement. Cela comprend les personnes qui peuvent se spécialiser dans les aspects liés aux facteurs humains de la chaîne d'approvisionnement, comme la proximité d'accès et la menace interne.
Autres titres	Analystes en cybersécurité Analystes de l'intégrité de la chaîne d'approvisionnement
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21230 – Développeurs/développeuses et programmeurs/programmeuses de systèmes informatiques
Tâches	▪ Collaborer avec les principaux intervenants pour mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Développer et mettre en œuvre des plans qui respectent les objectifs et les exigences de l'organisation en matière de sécurité ▪ Recueillir et analyser l'information pertinente sur la chaîne d'approvisionnement afin de cerner et d'atténuer les lacunes 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 du système ▪ 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 ▪ Assurer la coordination avec les collègues pour mettre en œuvre les changements et les nouveaux systèmes ▪ Faire le suivi des cybermenaces et des vulnérabilités en matière de sécurité qui ont une incidence sur le rendement de la chaîne d'approvisionnement et en faire rapport ▪ Définir, élaborer, mettre en œuvre et tenir à jour les plans, les politiques et les procédures de cybersécurité ▪ Veiller au respect des politiques, des règlements et des procédures de l'organisation en matière de cybersécurité ▪ Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation ▪ Développer et tenir à jour les évaluations des risques et les rapports connexes sur les fournisseurs, les produits et les services

	▪ Définir et tenir à jour les jeux d'outils et les 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 d'éducation liés à la cybersécurité et à l'intégrité de la chaîne d'approvisionnement
Compétences requises pour l'éducation	Études postsecondaires en cybersécurité ou dans un domaine lié à l'informatique (p. ex. génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent).
Formation requise	En plus d'avoir suivi une formation officielle en analyse de la cybersécurité, le ou la titulaire devrait acquérir des connaissances et des compétences spécialisées en analyse des vulnérabilités et sur les menaces liées à la chaîne d'approvisionnement.
Expérience professionnelle requise	Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité. L'expérience demandée dépendra du besoin organisationnel et de la complexité des systèmes à analyser.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et outils et applications d'évaluation des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des risques liés à la cybersécurité dans l'ensemble de la chaîne d'approvisionnement ▪ Contrats et accords sur les niveaux de service conclus avec des tierces parties
Compétences	Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte ☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet ☐ Processus d'approvisionnement et exigences en matière de sécurité Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Infrastructure de sécurité organisationnelle, dont les systèmes de protection et de défense dans l'ensemble de la chaîne d'approvisionnement ☐ La situation de la menace à la cybersécurité et les sources de renseignement sur les menaces qui pèsent sur la chaîne d'approvisionnement ☐ Exigences juridiques et de conformité telles qu'elles s'appliquent aux accords organisationnels avec des tierces parties ☐ Outils et analyse des vulnérabilités ☐ Information avancée sur la sécurité et analyse et techniques en matière de sécurité des données ☐ Conception fonctionnelle et technique des réseaux, des systèmes et des solutions de cybersécurité ☐ Processus, responsabilités et pouvoirs en matière de gestion des risques au sein de l'organisation et dans l'ensemble de la chaîne d'approvisionnement ☐ Gestion des risques et responsabilités des tierces parties ☐ 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
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liés à la cybersécurité.

	▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur la sécurité. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront à l'infrastructure de sécurité organisationnelle et des répercussions sur le personnel, les ressources, les procédures et les politiques. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation.

B.7 Développeurs/développeuses en sécurité des systèmes d'information

Référence au cadre de la NICE	Securely Provision, SP-SYS-001, Information Systems Security Developer
Description fonctionnelle	Le ou la titulaire développe, crée, intègre, teste et maintient la sécurité du système d'information tout au long du cycle de vie des systèmes. Il rend compte du rendement du système en assurant la confidentialité, l'intégrité et la disponibilité, et recommande des mesures correctives pour corriger les lacunes.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait faire en sorte que l'organisation prenne des décisions susceptibles d'avoir une incidence importante sur ses activités. Ne pas comprendre pleinement les besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face aux menaces grandissantes.
Parcours de perfectionnement	Ce rôle de premier échelon en cybersécurité tire avantage d'une expérience antérieure en matière de TI et de système. Après une formation technique en cybersécurité, le ou la titulaire pourra assumer de plus amples responsabilités dans l'infrastructure de cybersécurité et acquérir une expertise technique.
Autres titres	Administrateurs/administratrices de systèmes de sécurité des TI Techniciens/techniciennes de systèmes de cybersécurité
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21230 – Développeurs/développeuses et programmeurs/programmeuses de systèmes informatiques
Tâches	▪ Collaborer avec les principaux intervenants pour mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Définir et examiner les systèmes d'information d'une organisation et veiller à ce que les exigences en matière de sécurité tiennent compte des plans de reprise après sinistre et des fonctions de continuité des activités appropriées, y compris des besoins en matière de basculement ou de sauvegarde pour la restauration des systèmes ▪ Analyser les systèmes de sécurité existants et recommander des changements ou des améliorations ▪ Préparer des estimations des coûts et des contraintes, et cerner les problèmes ou les risques liés à l'intégration pour l'organisation ▪ Faire des recherches et élaborer un contexte de sécurité des systèmes, et définir les exigences d'assurance de la sécurité en fonction des normes de l'industrie et des politiques et pratiques en matière de cybersécurité ▪ S'assurer que les systèmes acquis ou développés sont conformes aux politiques et aux pratiques de cybersécurité d'une organisation ▪ Élaborer et exécuter des procédures de mise à l'essai et de validation du système d'information et rendre compte de la fonctionnalité et de la résilience ▪ Planifier et soutenir les tests de vulnérabilité et les examens de sécurité sur les systèmes d'information ou les réseaux afin de cerner les lacunes, et examiner les contrôles et les mesures nécessaires pour protéger la confidentialité et l'intégrité de l'information dans différentes conditions d'exploitation ▪ Effectuer des essais préliminaires des systèmes d'information pour s'assurer que les niveaux et les procédures de sécurité sont appropriés, et élaborer un plan de gestion des risques pour la sécurité

	▪ Soutenir l'élaboration des plans de reprise après sinistre et de continuité des activités pour les systèmes d'information en développement ▪ Préparer des rapports techniques qui documentent le processus de développement des systèmes et les révisions subséquentes ▪ Documenter et traiter la sécurité tout au long du cycle de vie des systèmes ▪ Mettre à jour et mettre à niveau les systèmes d'information au besoin 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 ▪ Élaborer des contre-mesures et des stratégies d'atténuation des risques contre l'exploitation potentielle de vulnérabilités dans les réseaux ou les systèmes ▪ Effectuer une analyse des risques chaque fois qu'un système fait l'objet d'une modification ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle
Compétences requises pour l'éducation	Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, administration de systèmes informatiques, génie informatique ou équivalent).
Formation requise	La formation d'appui peut comprendre les outils, les techniques et les pratiques de développement de systèmes de cybersécurité, ainsi que la sécurité tout au long du cycle de développement des logiciels.
Expérience professionnelle requise	Formation et expérience préalables en développement de systèmes.
Outils et technologies	▪ Plans stratégiques et d'activités ▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports
Compétences	Cette profession repose sur les compétences démontrées à un niveau de cadre supérieur, ce qui comprend celles mentionnées dans le cadre de la NICE. Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Politiques, exigences et pratiques en matière de gestion des risques ☐ Planification de la continuité des activités et de l'intervention en cas de sinistre ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte ☐ Gestion de projets ☐ Modèles de coûts et analyse coût-avantage ☐ Concepts de la cryptographie et de la gestion des clés cryptographiques ☐ Gestion de l'identité et de l'accès ☐ Gestion des vulnérabilités et planification et processus des tests de pénétration ☐ Conceptions et fonctions de sécurité des données, méthodes d'analyse, tests et protocoles ☐ Techniques de codage et de configuration sécurisés ☐ Gestion, mesures et suivi du programme de cybersécurité Application avancée des connaissances, compétences et aptitudes 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 informatique, structures des données et algorithmes ☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels ☐ Méthodes et processus de mise à l'essai et d'évaluation de la sécurité ☐ Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données ☐ Conception de contre-mesures aux risques de sécurité relevés ☐ Configuration et utilisation des outils de protection informatique basés sur des logiciels ☐ Points à considérer en matière de conception et solutions matérielles et logicielles ☐ Gestion des incidents et reprise des systèmes
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités en matière de cybersécurité, des interactions entre les systèmes, de l'accès et de la reddition de compte. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur le cycle de développement des systèmes. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront dans l'infrastructure de sécurité de l'organisation. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Il conviendra également de développer et de mettre en œuvre des mesures d'intervention pour la sécurité des systèmes. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation et l'intégrer dans l'ensemble des systèmes qui traitent les données sensibles.

B.8 Ingénieurs/ingénieures et analystes en automatisation de la sécurité

Remarque : Il s'agit d'un rôle de travail émergent. On ne retrouve que des exemples limités de ce rôle et les tâches et les activités des spécialistes en la matière varient selon les exigences de l'organisation. Par conséquent, l'information ci-dessous repose sur des représentations fondées sur des exigences axées sur la demande et une bonne compréhension des exigences en matière d'intelligence artificielle, d'apprentissage machine et de science des données qui soutiennent l'ingénierie et l'analyse des processus automatisés. On s'attend à ce que ce rôle évolue considérablement au cours des prochaines années.

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	En tenant compte des références, de la documentation sur la sécurité organisationnelle, des conseils en matière de sécurité des TI et des outils et ressources nécessaires, le ou la titulaire recherche et définit les besoins opérationnels en matière de sécurité, détermine les exigences et développe des solutions automatisées qui soutiennent la sécurité de l'organisation.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou l'omission de tenir compte des exigences organisationnelles, des besoins opérationnels et des menaces pourrait mener à une mauvaise conception du système ou à l'intégration de systèmes ou dispositifs vulnérables à la compromission, ce qui peut avoir des implications importantes sur les objectifs de l'organisation, y compris mener à une possible défaillance irrémédiable des systèmes.
Parcours de perfectionnement	Le ou la titulaire du rôle a généralement reçu une éducation formelle et possède de cinq à dix ans d'expérience dans des fonctions connexes liées à l'ingénierie des TI, à la conception de systèmes ou à l'intégration de systèmes. Formation, éducation et/ou expérience additionnelles en automatisation des processus et dans des activités connexes en ingénierie de l'intelligence artificielle et de l'apprentissage machine.
Autres titres	▪ Ingénieurs automaticiens/ingénieures automaticiennes des systèmes ▪ Concepteurs/conceptrices de systèmes automatisés ▪ Ingénieurs/ingénieures de contrôles et d'automatisation de la sécurité
Classification nationale des professions (CNP) connexes	21310 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 22310 – Technologues et techniciens/techniciennes en génie électrique et électronique
Tâches	▪ Rechercher, développer, intégrer, mettre à l'essai et mettre en œuvre des solutions d'automatisation de la sécurité pour le nuage ou les systèmes ▪ Définir et planifier les tâches d'automatisation de manière à respecter les échéances ▪ Gérer et surveiller les activités des solutions de sécurité automatisées comme les correctifs, les mises à jour et les processus connexes ▪ Développer et maintenir les outils et les processus qui soutiennent les activités d'automatisation de la sécurité ▪ Passer en revue et mettre à l'essai le script d'automatisation de la sécurité avant sa mise en œuvre ▪ Résoudre les problèmes qui surviennent lors des tests, de la production ou de l'utilisation

	▪ Créer, utiliser et maintenir la documentation des ressources aux fins de référence ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour appuyer les activités d'automatisation de la sécurité ▪ Passer en revue, approuver et superviser les changements apportés aux politiques et aux contrôles de cybersécurité, ainsi que leurs répercussions sur les activités automatisées ▪ Planifier et superviser les évaluations et les contrôles de sécurité ▪ Superviser et gérer les relations avec les fournisseurs des produits et services de sécurité des TI acquis par l'organisation ▪ S'assurer de déterminer les exigences en matière de sécurité pour tous les systèmes informatiques tout au long de leur cycle de vie ▪ Superviser ou gérer les mesures de protection ou de correction lorsqu'une vulnérabilité ou un cyberincident est découvert ▪ Évaluer les menaces et développer des contre-mesures et des stratégies d'atténuation des risques contre les vulnérabilités touchant les systèmes automatisés ▪ Effectuer une analyse des risques et procéder à une mise à l'essai chaque fois qu'un système automatisé fait l'objet d'une modification ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle
Compétences requises pour l'éducation	Diplôme pertinent en génie ou en informatique avec études supérieures ou formation équivalente en automatisation des systèmes, en intelligence artificielle ou en apprentissage machine.
Formation requise	Formation pertinente en cybersécurité pour effectuer les tâches en tant qu'ingénieur ou ingénieure de la sécurité.
Expérience professionnelle requise	Expérience modérée (de trois à cinq ans) de la sécurité, ainsi que de la conception, de l'intégration, de la mise à l'essai et du soutien des systèmes connexes. Expérience en programmation et en mise à l'essai d'applications. De deux à trois années d'expérience pratique dans l'automatisation des processus des systèmes.
Outils et technologies	▪ 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 des intrusions et de protection contre les intrusions, les scanneurs et les alarmes ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Logiciels et systèmes d'authentification ▪ Processus de gestion des vulnérabilités et systèmes d'évaluation des vulnérabilités, y compris les tests de pénétration le cas échéant ▪ Services de sécurité fournis, le cas échéant ▪ Outils et techniques d'essai et d'évaluation de la sécurité ▪ Outils, techniques et procédures liés à l'automatisation des processus ▪ Langages de programmation applicables
Compétences	Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Automatisation des processus dans un cadre de sécurité ☐ Interface API, automatisation et langages de script ☐ Réseautage logiciel (SDN), virtualisation des fonctions réseau (NFV) et fonctions réseau virtualisées (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 sécurité et modèles de référence relatifs à l'architecture d'entreprise ☐ Sécurité des systèmes pendant l'intégration et la configuration ☐ Processus d'évaluation et d'autorisation de sécurité ☐ Méthodes et processus de mise à l'essai et d'évaluation de la sécurité ☐ Sécurité tout au long du cycle de développement de systèmes et de logiciels

	☐ Méthodologies et applications d'évaluation des vulnérabilités et de tests de pénétration ☐ Méthodes d'essais et d'évaluation des systèmes et des logiciels ☐ Conception de la sécurité basée sur les preuves ☐ Élaboration et mise à l'essai des modèles de menace ☐ Gestion de projet et évaluation de la sécurité tout au long du cycle de vie du projet ☐ Processus d'approvisionnement et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Prestation de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et prestation de séances d'information et de rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres)
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liés à la cybersécurité. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications que l'option « Prenez vos appareils personnels » (PAP) et la gestion des risques connexes pourraient avoir sur la sécurité. ▪ Si des outils de sécurité automatisés sont utilisés, il conviendra de définir les exigences en matière de mise à l'essai, d'intégration et de contrôle, ainsi que de conseiller ou de former les responsables de ces activités par rapport aux changements de processus et de procédures qui en découleront. Par ailleurs, en tant que possible responsable technique de l'automatisation de la sécurité, le ou la titulaire du poste pourrait devoir sensibiliser les responsables organisationnels aux avantages de l'automatisation et aux risques qu'elle pose, et les informer s'il convient d'assurer la gestion des changement. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Il sera impératif d'acquérir une meilleure compréhension des capacités des auteurs de menace et des contre-mesures possibles. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique et il faudra comprendre les répercussions sur les mécanismes de sécurité facilités par l'intelligence artificielle.

B.9 Cryptographes et cryptanalystes

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Le ou la titulaire développe des algorithmes, des chiffres et des systèmes de sécurité pour chiffrer l'information. Il analyse et décode les messages secrets et les systèmes de codage.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait donner lieu à des artéfacts cryptologiques, des protocoles et des systèmes déficients susceptibles de mettre en péril la sécurité prévue des systèmes et de l'information qui sont protégés. L'omission de se tenir au courant des sciences et des technologies émergentes et connexes fait courir un risque équivalent.
Parcours de perfectionnement	Cette activité de cybersécurité hautement spécialisée est menée par des professionnels expérimentés et qualifiés qui démontrent de l'intérêt pour ce domaine. Il existe des possibilités de spécialisation accrue et de recherche et d'études avancées dans ce domaine.
Autre titre	Aucune.
Classification nationale des professions (CNP) connexes	21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21210 – Mathématiciens/mathématiciennes, statisticiens/statisticiennes et actuaires 21220 – Spécialistes de la cybersécurité 21222 – Spécialistes en informatique
Tâches	▪ Collaborer avec les principaux intervenants pour mettre en place un programme efficace de gestion des risques liés à la sécurité ▪ Assurer la conformité aux lois et aux réglementations en vigueur ▪ Développer des systèmes permettant de protéger l'information importante ou sensible contre l'interception, la copie, la modifications et/ou la suppression ▪ Évaluer, analyser et cibler les faiblesses et les vulnérabilités dans les systèmes et les algorithmes ▪ Élaborer des modèles statistiques et mathématiques pour analyser les données et régler les problèmes de sécurité ▪ Développer et mettre à l'essai les modèles informatiques pour en vérifier la fiabilité et l'exactitude ▪ Déterminer, rechercher et mettre à l'essai de nouvelles théories et applications de cryptologie ▪ Décoder des messages cryptiques et des systèmes de codage pour l'organisation ▪ Élaborer et mettre à jour des méthodes de traitement efficace des processus cryptiques ▪ 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 ▪ Appuyer les contre-mesures et les stratégies d'atténuation des risques qui sont prises pour contrer l'exploitation potentielle des vulnérabilités touchant les systèmes cryptographiques et les algorithmes ▪ Fournir de l'information et des conseils sur la sécurité quantique et les stratégies post-quantiques ▪ Soutenir la gestion des incidents et l'analyse postérieure advenant la compromission de processus ou de systèmes cryptographiques ou de chiffrement ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle

	▪ Orienter et soutenir les spécialistes en chiffrement, le cas échéant
Compétences requises pour l'éducation	Diplôme d'études postsecondaires en génie informatique, en informatique ou en mathématiques. Une maîtrise ou un doctorat en sciences est préférable.
Formation requise	Comme l'exige le contexte technique de l'organisation (p. ex. outils, procédures et processus locaux)
Expérience professionnelle requise	En plus de l'obtention d'attestations d'études, les rôles de premier échelon exigent généralement de trois à cinq années d'expérience dans le domaine de l'informatique et des systèmes et une bonne connaissance des activités de chiffrement et de gestion des clés.
Outils et technologies	▪ Évaluations des menaces et des risques ▪ Processus de gestion des vulnérabilités et évaluations des vulnérabilités ▪ Processus et procédures de gestion des incidents (liés à la cryptographie ou au chiffrement) ▪ Processus et politiques de gestion des incidents de cybersécurité ▪ Lois relatives à la sécurité et au respect de la vie privée ▪ Algorithmes de chiffrement, chiffres et systèmes ▪ Politiques et plans de gestion des clés ▪ Infrastructure de sécurité organisationnelle et systèmes de production de rapports
Compétences	Cette profession repose sur les compétences démontrées à un niveau de cadre supérieur, ce qui comprend celles mentionnées dans le cadre de la NICE. Application de base des connaissances, compétences et aptitudes suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte ☐ Exigences en matière d'information et de données, dont la sensibilité, l'intégrité et le cycle de vie ☐ Langages de programmation applicables ☐ Gestion, mesures et suivi du programme de cybersécurité Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Menaces avancées et capacités de décryptage et de déchiffrement ☐ Lois, codes juridiques, règlements, politiques et éthique applicables en matière de cybersécurité ☐ Architecture informatique, structures des données et algorithmes ☐ Algèbre linéaire/matricielle et/ou mathématiques discrètes ☐ Théorie des probabilités, théorie de l'information, théorie de la complexité et théorie des nombres ☐ Concepts de la cryptographie et de la gestion des clés cryptographiques ☐ Principes de la cryptographie symétrique (p. ex. 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 d'intervention en cas d'incident découlant d'une compromission cryptographique ☐ Rédaction de rapports techniques
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liées au chiffrement de données. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils cryptographiques sont touchés et automatisés pour répondre aux besoins de l'organisation. ▪ L'utilisation accrue des outils automatisés par les auteurs 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. En cas de 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 degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation. Les cryptographes et cryptanalystes jouent un rôle déterminant dans la conception de solutions post-quantiques et peuvent prendre part à la mise à l'essai des algorithmes, des protocoles de chiffrement et de l'équipement.

Annexe C Exploitation et maintenance

Ce secteur d'activités ou cette catégorie d'emplois participe à l'exploitation et au maintien de la sécurité des systèmes et des données, conformément aux spécifications relatives à l'architecture de sécurité et à la conception. Toutes ces fonctions sont exercées dans les professions existantes du marché du travail canadien, à l'exception de celles indiquées ci-dessous qui font maintenant office de professions dépendant de plus en plus des systèmes connectés à Internet et des menaces qui y sont associées.

Un ou une spécialiste en cybersécurité appartenant à cette catégorie d'emploi doit non seulement apporter son expertise technique, mais aussi se conformer étroitement aux exigences opérationnelles quotidiennes de l'organisation en matière de TI. Outre les compétences techniques, cela se traduit généralement par des services aux clients améliorés et des compétences accrues en communication.

Cliquez sur le titre du rôle lié à la cybersécurité pour en savoir plus sur les exigences relatives aux connaissances, aux compétences, aux tâches et aux aptitudes de chaque rôle.

Rôles principaux liés à la cybersécurité

- Spécialistes de la gestion de l'identité et du soutien de l'authentification
- Spécialistes du chiffrement ou du soutien à la gestion des clés
- Spécialistes de la confidentialité des données et agents/agentes à la protection des renseignements personnels

Rôles connexes

- Administrateurs ou administratrices de bases de données
- Analystes des données
- Gestionnaires de l'information (gestionnaires des connaissances de la NICE)
- Spécialistes du soutien technique
- Spécialistes des opérations réseau
- Administrateurs/administratrices de système
- Analystes de systèmes de données
- Gestionnaires de système (dont les rôles de gestionnaires de système, de logiciels et de systèmes de données)

C.1 Spécialistes de la gestion de l'identité et du soutien de l'authentification

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Le ou la titulaire fournit une assistance continue à la gestion de l'identité, des justificatifs, de l'accès et de l'authentification afin de soutenir la sécurité des TI de l'organisation.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à la compromission du système, ce qui peut avoir, selon le type de compromission, une incidence importante sur les systèmes, les capacités et 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 des justificatifs d'identité et de l'accès pour ce qui est de l'administration de réseaux ou de systèmes. Une formation et une expérience supplémentaires pourraient permettre d'accéder à des rôles plus techniques ou plus opérationnels et offrir des possibilités d'emploi en gestion.
Autres titres	▪ Analystes en gestion de l'accès ▪ Analystes de système ▪ Spécialistes de la gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 22220 – Techniciens/techniciennes de réseau informatique et Web 22221 – Agents/agentes de soutien aux utilisateurs
Tâches	▪ Déterminer les besoins des clients et proposer des solutions techniques ▪ Modéliser et associer les utilisateurs aux ressources (p. ex. en fonction des rôles) ▪ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ▪ Déployer, configurer et gérer l'approvisionnement des utilisateurs, notamment la synchronisation de l'identité, l'approvisionnement automatique et la désactivation automatique de l'accès, le flux de travaux de l'approbation des demandes de sécurité en libre-service et la production de rapports consolidés ▪ Configurer et gérer les solutions de gestion des accès Web et d'entreprise (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 ▪ Consigner les étapes de gestion du cycle de vie des utilisateurs, les valider par rapport à la liste de contrôle d'accès sur les plateformes gérées et produire des rapports à ce sujet ▪ Configurer et gérer l'identité, les justificatifs d'identité et l'accès fédérés conformément à la politique, aux normes et aux procédures de sécurité ▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle
Compétences requises pour l'éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information.
Formation requise	Formation sur les politiques, les protocoles, les outils et les procédures d'authentification et de gestion de l'identité, des justificatifs et de l'accès.

	Développement et application d'un système de gestion des justificatifs d'identité des utilisateurs.
Expérience professionnelle requise	Expérience de la gestion de services d'annuaire et du travail dans un environnement de sécurité.
Outils et technologies	▪ Systèmes de gestion de l'identité et de l'accès ▪ Services d'annuaire ▪ Outils et services d'authentification ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents
Compétences	Les connaissances, compétences et aptitudes suivantes 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 de l'accès basés sur les stratégies et adaptés au risque ☐ Développement et application d'un système de gestion des justificatifs d'identité des utilisateurs ☐ Analyse organisationnelle des tendances commerciales et inhérentes aux utilisateurs ☐ Consultation des clients et résolution des problèmes Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Protocoles, outils et procédures liés à l'accès réseau et à la gestion de l'identité et de l'accès ☐ Authentification, autorisation et méthodes de contrôle de l'accès ☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ☐ Développer et appliquer les contrôles d'accès aux systèmes de sécurité ☐ Maintenir les services d'annuaire ☐ Politiques organisationnelles sur la sécurité des utilisateurs de technologies de l'information (TI) (p. ex. création de comptes, règles relatives aux mots de passe, contrôle d'accès)
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à 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 sur les dispositifs « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront aux processus de gestion de l'identité et de l'accès et aux changements techniques et de processus connexes. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, ainsi qu'une compréhension approfondie des répercussions sur les protocoles d'authentification et la façon de se défendre contre de possibles menaces liées à l'informatique quantique.

C.2 Spécialistes du chiffrement ou du soutien à la gestion des clés

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Le ou la titulaire fournit une assistance continue à la gestion et à la maintenance des réseaux virtuels privés, du chiffrement, de l'infrastructure à clé publique et, dans certains cas, de la sécurité des communications (COMSEC pour *Communications Security*) afin de soutenir la sécurité des TI de l'organisation.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à la compromission du système, ce qui peut avoir, selon le type de compromission, une incidence importante sur les systèmes, les capacités et 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 des justificatifs d'identité et de l'accès pour ce qui est de l'administration de réseaux ou de systèmes. Une formation et une expérience supplémentaires pourraient permettre d'accéder à des rôles plus techniques ou plus opérationnels et offrir des possibilités d'emploi en gestion.
Autres titres	▪ Analystes en gestion de l'accès ▪ Analystes de système ▪ Spécialistes de la gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 22220 – Techniciens/techniciennes de réseau informatique et Web 22221 – 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 les contrôles d'accès aux systèmes de sécurité ▪ Déployer, configurer et gérer les services de chiffrement et de gestion des clés ▪ Mettre en place des RPV ▪ Analyser les schémas ou les tendances en vue d'une résolution ultérieure ▪ Gérer les processus d'approbation des demandes de changement d'identité ▪ Consigner les étapes de gestion du cycle de vie des utilisateurs, les valider par rapport à la liste de contrôle d'accès sur les plateformes gérées et produire des rapports à ce sujet ▪ Configurer et gérer l'identité, les justificatifs d'identité et l'accès fédérés conformément à la politique, aux normes et aux procédures de sécurité ▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques ▪ Concevoir, fournir et superviser le matériel de formation sur la cybersécurité et les efforts d'éducation liés au rôle
Compétences requises pour l'éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information.
Formation requise	Formation sur les technologies pertinentes de chiffrement et de gestion des clés au niveau demandé.
Expérience professionnelle requise	Expérience de la gestion de services d'annuaire et du travail dans un environnement de sécurité.
Outils et technologies	▪ Systèmes de gestion de l'identité et de l'accès ▪ Outils, processus et procédures liés au chiffrement et à la gestion des clés ▪ Outils et procédures de chiffrement des RPV et du Wi-Fi

	▪ Outils et services d'authentification ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents
Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent au niveau de base : ☐ Cryptanalyse ☐ Concepts et méthodologies de cryptographie et de chiffrement ☐ Cryptographie symétrique et asymétrique ☐ Stéganographie et stéganalyse ☐ Autorités cryptographiques nationales (Centre de la sécurité des télécommunications) ☐ Fournisseurs d'infrastructures à clé publique Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Politiques organisationnelles sur la sécurité des utilisateurs de technologies de l'information (TI) (p. ex. création de comptes, règles relatives aux mots de passe, contrôle d'accès) ☐ Protocoles, outils et procédures liés à l'accès réseau et à la gestion de l'identité et de l'accès ☐ Normes nationales et internationales ☐ Authentification, autorisation et méthodes de contrôle de l'accès ☐ ICP (infrastructure à clé publique), HSM (module de sécurité matériel [Hardware Security Module]), certificat numérique, protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security), protocole SSH (Secure Shell), technologies de chiffrement actuelles ☐ Processus liés au cycle de vie des applications ☐ Gestion des signatures numériques, des certificats numériques et des certificats numériques ☐ Protocoles d'authentification ☐ RPV et protocoles ☐ Chiffrement de fichiers et de disques ☐ Algorithmes de chiffrement ☐ Analyse organisationnelle des tendances commerciales et inhérentes aux utilisateurs ☐ Consultation des clients et résolution des problèmes
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux 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 liées au chiffrement de données. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils cryptographiques sont touchés et automatisés pour répondre aux besoins de l'organisation. ▪ L'utilisation accrue des outils automatisés par les auteurs 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. En cas de 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 degré 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 qui pèsent sur l'organisation, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Des connaissances et des compétences seront nécessaires pour mettre en œuvre une stratégie post-quantique au sein de l'organisation. Cela comprend des connaissances et des compétences par rapport aux algorithmes post-quantiques utilisés, à l'intégration et à la mise en œuvre de technologies post-quantiques au sein de l'organisation et aux protocoles d'essai et d'évaluation du matériel, des logiciels et des protocoles post-quantiques et à résistance quantique.

C.3 Spécialistes de la confidentialité des données et agents/agentes à la protection des renseignements personnels

Référence au cadre de la NICE	Oversee and Govern, OV-LGA-002, Privacy Officer/Privacy Compliance Manager
Description fonctionnelle	Le ou la titulaire développe, met en œuvre et administre le programme de conformité à la protection de la vie privée de l'organisation à l'appui des exigences qu'il convient de mettre en place pour protéger les renseignements personnels, et fournit des conseils en la matière.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à une compromission ou à une violation des renseignements personnels, ce qui pourrait entraîner des conséquences personnelles, engager des responsabilités, donner lieu à l'imposition d'amendes importantes et donner lieu à une atteinte à la réputation et une perte de confiance.
Parcours de perfectionnement	Ce rôle peut être assumé par un ou une titulaire qui a suivi un parcours technique ou non technique ayant mené à un rôle de premier échelon lié à la gestion du respect de la vie privée et des données sensibles avant d'atteindre le niveau de conseiller ou de conseillère en politiques. Les titulaires peuvent se spécialiser dans la sécurité des données ou comme analystes des politiques ou conseillers principal/conseillères principales.
Autres titres	▪ Agents/agentes de la protection de la vie privée ▪ Agents/agentes et gestionnaires de la conformité à la protection de la vie privée
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 41400 – Recherchistes, experts-conseils/expertes-conseils et agents/agentes de programmes, en sciences naturelles et appliquées
Tâches	▪ Interpréter et appliquer des lois, des règlements, des politiques, des normes ou des procédures par rapport à des questions précises de protection des renseignements personnels ▪ Effectuer des évaluations des répercussions périodiques et des activités de surveillance continue de la conformité pour cerner les lacunes en matière de conformité et/ou les secteurs de risque afin de s'assurer que les préoccupations, les exigences et les responsabilités en matière de protection des renseignements personnels sont prises en compte ▪ Établir et tenir à jour un mécanisme de suivi de l'accès à l'information, selon la mission de l'organisation et les exigences législatives pour permettre au personnel qualifié d'examiner ou de recevoir ces renseignements ▪ Établir et mettre en œuvre un programme interne de vérification de la protection des renseignements personnels, et préparer des rapports d'audit qui cernent les constatations techniques et procédurales, ainsi que les violations de la vie privée, et recommander des solutions correctives ▪ Fournir des conseils et de l'orientation sur les lois, les règlements, les politiques, les normes ou les procédures à la direction, au personnel ou aux ministères clés ▪ Veiller au respect des lois, des règlements et des politiques en matière de protection des renseignements personnels et de cybersécurité, et à l'application uniforme des sanctions en cas de non-respect des mesures énoncées pour tout le personnel de l'organisation ▪ Entreprendre, faciliter et promouvoir des activités de sensibilisation à la protection des renseignements personnels au sein de l'organisation, notamment en ce qui concerne la collecte, l'utilisation et l'échange de renseignements ▪ Surveiller les progrès de la technologie d'amélioration de la protection des renseignements personnels et veiller à ce que l'utilisation des technologies soit conforme aux exigences en matière de protection des renseignements personnels et de cybersécurité, y compris en ce qui concerne la collecte, l'utilisation et la divulgation de l'information

	▪ Examiner les plans et les projets de sécurité réseau de l'organisation pour s'assurer qu'ils sont conformes aux objectifs et aux politiques en matière de protection des renseignements personnels et de cybersécurité ▪ Collaborer avec les avocats et la direction pour veiller à ce que l'organisation obtienne et maintienne un consentement approprié en matière de protection des renseignements personnels et de confidentialité, des formulaires d'autorisation et des documents pertinents conformes aux pratiques et aux exigences juridiques ▪ Élaborer et fournir du matériel de formation et superviser des activités de sensibilisation sur la protection des renseignements personnels
Compétences requises pour l'éducation	Études postsecondaires dans un domaine pertinent (p. ex. administration des affaires, droit, sciences politiques, sciences sociales ou l'équivalent)
Formation requise	Formation spécialisée en protection et en sécurité des données, ainsi que sur les rudiments de la cybersécurité, l'analyse des facteurs relatifs à la vie privée, les lois sur la protection de la vie privée et la conformité.
Expérience professionnelle requise	Formation et expérience antérieures (de deux à trois ans) en tant qu'analyste des politiques liées à la sécurité et au respect de la vie privée généralement exigées pour un rôle de premier échelon.
Outils et technologies	▪ Lois et politiques relatives à la protection des renseignements personnels et à l'information ▪ Exigences relatives à la conformité ▪ Mécanismes et modèles de communication ▪ Évaluations des facteurs relatifs à la vie privée et énoncés de sensibilité ▪ Évaluations des menaces et des risques ▪ Exigences relatives aux données et à l'information ▪ Outils et méthodologies d'évaluation de la protection des renseignements personnels
Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent au niveau de base : ☐ Connaissances pratiques des principes et des éléments de la cybersécurité ☐ Connaissances techniques des exigences en matière de sécurité et d'intégrité des données, des exigences de sécurité, ainsi que de la conception fonctionnelle et technique des réseaux et des systèmes, et des solutions de cybersécurité ☐ Conceptions et fonctions de sécurité des données, méthodes d'analyse, tests et protocoles ☐ Gestion, mesures et suivi du programme de cybersécurité Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Évaluation des menaces et des risques (axée sur le respect de la vie privée ou la sécurité de la protection des données) ☐ Lois, politiques, procédures et règlements nationaux et internationaux ☐ Politiques, procédures et règlements en matière de sécurité de l'information ☐ Répercussions particulières des lacunes en matière de cybersécurité et des atteintes à la cybersécurité ☐ Surveillance des progrès des lois et des politiques relativement à la protection des renseignements personnels ☐ Évaluations des facteurs relatifs à la vie privée ☐ Déclarations de confidentialité fondées sur les lois et les règlements ☐ Signalement d'une violation
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la protection des données sensibles, ainsi qu'au signalement de possibles violations et aux mesures d'intervention qui en découlent. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront dans la protection des renseignements personnels au sein de l'organisation et quelles seraient les politiques, les procédures et les pratiques qui devraient en découler. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace remettra probablement en question les technologies et les ressources qui servent actuellement à gérer la protection des renseignements

	personnels. Par ailleurs, des outils, des processus et de la formation supplémentaires seront nécessaires pour conserver une longueur d'avance sur les menaces. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur les renseignements personnels et les données, ainsi que les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Le chiffrement utilisé pour protéger les renseignements personnels exigera l'acquisition des connaissances et des compétences nécessaires pour garantir leur protection contre la menace quantique.

Annexe D Protection et défense

Ce sous-groupe professionnel prend part aux activités liées à la cybersécurité qui englobent la protection active, la détection des événements, l'intervention en cas d'incident et la reprise des systèmes numériques de l'organisation. Bien que des personnes exercent des emplois connexes depuis des décennies, les principaux rôles de travail n'ont pas été identifiés comme des professions. Ils ont plutôt été typiquement associés à des groupes professionnels : gestionnaires des systèmes informatiques (CNP 20012); spécialistes de la cybersécurité (CNP 21220) et spécialistes en informatique (CNP 21222). Les personnes appartenant à cette catégorie de travail se concentrent donc sur la gestion des technologies, des processus et du personnel de cybersécurité, ce qui nécessite une expérience unique et des connaissances, des compétences et des aptitudes distinctes de celles possédées par leurs autres collègues des TI.

Cliquez sur le titre du rôle lié à la cybersécurité pour en savoir plus sur les exigences relatives aux connaissances, aux compétences, aux tâches et aux aptitudes de chaque rôle.

Rôles principaux liés à la cybersécurité

- Gestionnaires de la sécurité des systèmes d'information – Opérations de cybersécurité
- Analystes des opérations de cybersécurité
  - Analystes de niveau 1 – Analystes des opérations de cybersécurité
  - Analystes de niveau 2 – Spécialistes des maliciels
  - Analystes de niveau 3 – Analystes en menaces informatiques : gestion et défense active
- Intervenants/intervenantes en cas d'incident lié à la sécurité
- Intervenants/intervenantes en cas d'incident lié à la TO
- Techniciens et techniciennes des opérations de cybersécurité
- Analystes de l'évaluation des vulnérabilités
- Testeurs ou testeuses de pénétration
- Analystes en criminalistique numérique

Rôles connexes

Aucun

D.1 Gestionnaires de la sécurité des systèmes d'information – Opérations de cybersécurité

Référence au cadre de la NICE	Oversee & Govern, OV-MGT-001, Information Systems Security Manager,
Description fonctionnelle	Le ou la titulaire planifie, organise, dirige, contrôle et évalue les activités du centre des opérations de cybersécurité au sein d'une organisation. Les titulaires sont employés dans l'ensemble des secteurs public et privé.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète ou un mauvais jugement pourrait mener à une défaillance catastrophique des systèmes de TI et de données de l'organisation et avoir des répercussions graves sur les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Les titulaires suivent généralement un parcours de cinq à dix ans au cours duquel ils occupent un rôle associé aux opérations de TI ou de cybersécurité ou un autre emploi similaire. Dans ce rôle, ils doivent assumer de plus amples responsabilités liées à la gestion pour acquérir de solides bases techniques dans les opérations de cybersécurité ou un rôle de travail connexe comme l'évaluation et la gestion des vulnérabilités, la criminalistique numérique ou l'analyse de la cybersécurité.
Autres titres	▪ Gestionnaires des opérations de cybersécurité (GOC) ▪ Gestionnaires des opérations de sécurité (COS) ▪ Gestionnaires de la cybersécurité ▪ Gestionnaires de la sécurité des systèmes d'information (opérations de cybersécurité)
Classification nationale des professions (CNP) connexes	20012 – Gestionnaires des systèmes informatiques
Tâches	▪ Diriger et gérer le personnel du COS, ce qui comprend l'embauche, la formation, le perfectionnement du personnel, la gestion du rendement et la réalisation d'examens annuels du rendement ▪ Rester à l'affût du contexte 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 de la qualité ▪ Surveiller l'efficacité du programme de COS et en rendre compte à la haute direction ▪ 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 le renseignement sur la menace selon les risques organisationnels ▪ Gérer les événements et incidents de cybersécurité au sein du COS ▪ Produire des rapports, des exposés et des recommandations fondés sur les risques concernant les événements et incidents de cybersécurité courants et non courants, notamment la réponse aux crises organisationnelles comme l'interruption des systèmes d'entreprise ▪ Diriger et faciliter les leçons apprises, les analyses rétrospectives et les pratiques exemplaires relatives aux événements et incidents liés à la cybersécurité ▪ Assurer et superviser la mise en œuvre de plans d'action visant à soutenir l'amélioration continue de la posture de cybersécurité

Compétences requises pour l'éducation	Baccalauréat en informatique ou discipline connexe ou diplôme d'études collégiales dans le domaine des TI
Formation requise	Formation en opérations de cybersécurité avec certification de niveau industriel dans un domaine connexe (p. ex. sécurité de réseau, traitement des incidents, détection et atténuation des menaces, criminalistique numérique). Formation en gestion d'équipes responsables des opérations de cybersécurité ou perfectionnement et expérience équivalents. Formation sur l'utilisation des outils et des technologies pertinents pour l'organisation qui soutiennent les opérations de cybersécurité.
Expérience professionnelle requise	Expérience considérable (de cinq à dix ans) du domaine des TI avec de trois à cinq ans d'expérience dans les opérations de cybersécurité ou un domaine connexe.
Outils et technologies	▪ Processus et procédures de gestion des incidents ▪ Systèmes de défense, y compris les pare-feu, les logiciels et systèmes antivirus, les systèmes de détection des intrusions et de protection contre les intrusions, les scanneurs et les alarmes. ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Logiciels et systèmes d'authentification ▪ Processus de gestion des vulnérabilités et systèmes d'évaluation des vulnérabilités, y compris les tests de pénétration le cas échéant ▪ Services de sécurité fournis, le cas échéant
Compétences	Cette profession repose sur les compétences démontrées pour un rôle de gestionnaire d'activités, ainsi que pour le rôle de gestionnaire de la sécurité des systèmes d'information décrit dans le cadre de la NICE. Plus précisément, ce travail exige ce qui suit : Application de base des connaissances, compétences et aptitudes suivantes : ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles Application avancée des connaissances, compétences et aptitudes suivantes : ☐ Menaces et vulnérabilités organisationnelles, dont celles ci-dessous o Contexte de la menace à la cybersécurité et adaptation des processus du COS de manière à répondre à une menace en constante évolution o Exigences en matière de gestion des vulnérabilités et gamme des mesures d'atténuation potentielles disponibles en l'absence de protocole de gestion des vulnérabilités ☐ Gestion des systèmes défensifs : o Pare-feu, antivirus, systèmes de détection et de prévention d'intrusion o Paramètres manuels et automatisés obligatoires o Exigences en matière de surveillance, de mise à l'essai et de maintenance ☐ Développement, mise en œuvre et gestion : o Processus et politiques de gestion des incidents o Responsabilités liées à la gestion des incidents o Pratiques de suivi et de signalement des incidents en vertu des exigences législatives et des politiques organisationnelles o Analyses et rapports après incident o Leçons apprises par l'organisation aux fins d'amélioration permanente ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) : o Rôles et responsabilités associés aux contrôles de sécurité des services fournis o Rôles et responsabilités des fournisseurs en matière de gestion et de signalement des incidents

	○ Exigences en matière de surveillance, d'évaluation et de signalement des incidents au cours du cycle de vie des contrats ○ Responsabilités de l'organisation advenant une compromission ou une violation causée par le fournisseur ○ Gestion des communications et des relations avec le fournisseur en temps de crise ☐ Prestation de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et prestation de séances d'information et de rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres) ☐ Assurance d'une connaissance plus vaste de la situation en matière de sécurité ☐ Conscience de soi pour ce qui est des connaissances, des compétences et des aptitudes requises pour répondre aux changements organisationnels, techniques et liés aux menaces ☐ apprentissage continu soutenant le perfectionnement des connaissances liées aux menaces émergentes, aux innovations technologiques sur le plan de la sécurité et à un environnement de cybersécurité en constante évolution;
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités pour ce qui est de détecter les incidents de cybersécurité, d'intervenir dans de telles circonstances et d'assurer la reprise des activités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront au COS, ce qui comprend la mise en œuvre des changements liés au personnel et aux processus. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Il sera nécessaire de comprendre les capacités de la menace quantique et les connaissances et compétences requises pour la mise en œuvre d'une stratégie post-quantique.

D.2 Analystes des opérations de cybersécurité

Remarque : Ce rôle comprend ce qui suit :

- Analystes des opérations de cybersécurité
- Spécialistes des maliciels
- Analystes en menaces informatiques : gestion et défense active

Référence au cadre de la NICE	Protect and Defend, Cyber Defence Analyst, PR-CDA-001
Description fonctionnelle	Le ou la titulaire occupe un poste d'opérateur ou opératrice de centre des opérations de cybersécurité de première ligne chargé de surveiller et de maintenir les dispositifs de sécurité des TI. Il est souvent responsable de la détection initiale et de la prise de mesures d'intervention et d'atténuation
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à une défaillance catastrophique des systèmes de TI et de données de l'organisation et avoir des répercussions graves sur les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Il s'agit d'un emploi de premier échelon courant au sein du Centre des opérations de sécurité (COS). Une formation et une expérience supplémentaires pourraient permettre d'accéder à des rôles plus techniques ou plus opérationnels axés sur les opérations de cybersécurité (p. ex. l'évaluation et la gestion des vulnérabilités, la criminalistique numérique, l'analyse des menaces et l'analyse des maliciels) et offrir des possibilités de gestion. Il est à noter que les rôles de niveau 2 et 3 peuvent nécessiter une formation et une éducation plus poussées en plus d'une expérience pertinente. Un diplôme en informatique ou en génie informatique est souvent une condition préalable étant donné le niveau de connaissances et de compétences requis pour des tâches plus complexes. Cela dit, plusieurs titulaires sont passés d'un poste d'analyste en cybersécurité à un poste supérieur lié à la cybersécurité sans détenir un diplôme connexe.
Autres titres	▪ Opérateurs/opératrices de COS ▪ Opérateurs/opératrices de cybersécurité ▪ Analystes de la sécurité des infrastructures ▪ Analystes de la sécurité des réseaux ▪ Administrateurs/administratrices de la sécurité des réseaux ▪ Analystes de la sécurité des données
Classification nationale des professions (CNP) connexes	21222 – Spécialistes en informatique 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Identifier et analyser les menaces techniques et les vulnérabilités qui touchent les réseaux ▪ Identifier, contenir et signaler les compromission de système et prendre les mesures d'atténuation initiales ▪ Examiner, analyser ou appliquer les protocoles de sécurité Internet, les algorithmes cryptographiques, les normes d'annuaire, les protocoles de réseau, le renforcement de la sécurité 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 de prévention d'intrusion, les pare-feu, les routeurs, les multiplexeurs, les commutateurs et les dispositifs sans fil

	▪ Analyser les données de sécurité et fournir des conseils, des bulletins et des rapports ▪ Installer, configurer, intégrer et régler les dispositifs et systèmes de sécurité, surveiller leurs performances et détecter les lacunes sur ceux-ci ▪ Effectuer une analyse des répercussions entraînées par le déploiement de nouveaux logiciels, les changements majeurs apportés à la configuration et la gestion des correctifs ▪ Développer des modèles de validation de principe et de tests pour les produits et services de sécurité des TI ▪ Résoudre les problèmes touchant les produits et les incidents de sécurité ▪ Concevoir et développer des protocoles de sécurité des TI ▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques ▪ Développer des options et des solutions qui permettent d'atteindre les objectifs des projets en matière de sécurité ▪ Choisir des produits de sécurité et des configurations qui permettent d'atteindre les objectifs des projets en matière de sécurité ▪ Mettre en œuvre et à l'essai les caractéristiques des configurations ▪ Développer des manuels de configuration et de conception opérationnelle ▪ Passer en revue, concevoir et fournir du matériel de formation pertinent
Compétences requises pour l'éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information avec une spécialisation en informatique, en cybersécurité, en sécurité des réseaux ou dans un domaine équivalent.
Formation requise	Formation en opérations de cybersécurité avec certification de niveau industriel dans un domaine connexe (p. ex. opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, exploitation d'appliances de sécurité). Une formation plus poussée est exigée pour les analystes de niveau 2 et de niveau 3.
Expérience professionnelle requise	L'expérience initiale requise est d'avoir travaillé avec succès dans un environnement informatique et au sein d'une équipe technique.
Outils et technologies	▪ Processus et procédures de gestion des incidents ▪ Systèmes de défense, y compris les pare-feu, les logiciels et systèmes antivirus, les systèmes de détection des intrusions et de protection contre les intrusions, les scanneurs et les alarmes. ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents
Compétences	Dans les COS plus importants, les analystes pourraient avoir l'occasion de passer d'un niveau 1 à un niveau 2. Les analystes de niveau 3 sont rares et on les retrouve presque exclusivement dans des environnements militaires ou liés à la sécurité nationale. Les compétences nécessaires aux niveaux 1 et 2 sont mentionnées ci-dessous. **Pour les analystes des opérations de cybersécurité de niveau 1** Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau de base : ☐ Administration et gestion de la sécurité des réseaux ☐ Architecture de sécurité des réseaux ☐ Sécurité du matériel et des micrologiciels ☐ Sécurité définie par logiciel et sécurité des applications ☐ Virtualisation et sécurité des réseaux privés virtuels (RPV) ☐ Sécurité infonuagique ☐ Sécurité des dispositifs mobiles et sans fil ☐ Établissement de zones de sécurité des TI ☐ Chiffrement et cryptographie, dont les concepts et les principes de gestion des clés ☐ Analyse des vulnérabilités ☐ Outils, processus et procédures de gestion des vulnérabilités ☐ Sécurité des applications Web

	☐ Livres de configuration et de construction opérationnelle ☐ Acquisitions de systèmes et projets ☐ Responsabilités juridiques et en matière d'éthique associées aux opérations de cybersécurité, y compris la conduite des enquêtes, le respect de la vie privée et la préservation de la preuve ☐ Rédaction et présentation des questions techniques (p. ex. rapports d'incident, rapports techniques, etc.) pour assurer la compréhension des membres de la direction Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Concepts, exploitation et configuration des appliances de sécurité réseau (équipements basés sur le rôle – systèmes ou appliances de cyberdéfense des réseaux, des serveurs et des postes de travail) ☐ Types d'intrusions et indicateurs de compromission (IC) ☐ Sources d'information sur les menaces ☐ Tactiques, techniques et procédures (TTP) communes aux auteurs de cybermenace ☐ Processus, responsabilités et pouvoirs en matière de gestion des risques ☐ Méthodes, outils et systèmes de détection et de prévention des intrusions ☐ Analyse des intrusions et techniques d'atténuation ☐ Analyse de base des maliciels **Pour les analystes de niveau 2 – Spécialistes des maliciels** Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé. Tout ce qui précède, en plus de ce qui suit : ☐ Tactiques, techniques et procédures employées par des auteurs de menaces persistantes dotés de moyens sophistiqués ☐ Outils, techniques et procédures liés à la cyberdéfense ☐ Développement et mise à l'essai des appliances de sécurité réseau (comme les scripts et le codage) ☐ Analyse avancée des maliciels et rétro-ingénierie des maliciels ☐ Mise en œuvre de contrôles de sécurité avancés en réponse à des menaces persistantes avancées ☐ Activités avancées d'intervention et de reprise en cas d'incident **Pour les analystes de niveau 3 – Analystes en menaces informatiques : gestion et défense active** Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Gestion avancée des menaces ☐ TTP employées par les auteurs de menaces avancées, dont la spécialisation des auteurs de menaces persistantes (p. ex. États-nations, crime organisé) ☐ Interprétation et synthèse du renseignement classifié et sensible sur les menaces tiré de sources multiples ☐ Responsabilités juridiques et éthiques associées aux techniques de défense active ☐ Analyse de l'exploitation ☐ Chasse aux cybermenaces et cadres de défense active ☐ Élaboration de plans d'action complexes, dont des plans d'évaluation et d'atténuation des risques ☐ Tactiques, outils et procédures de défense active, dont des contre-mesures et contre-contre-mesures avancées aux menaces ☐ Approche antagoniste ☐ Développement, mise à l'essai et déploiement d'outils techniques dans un cadre de défense active pour protéger l'information et les systèmes à risque de l'organisation
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités pour ce qui est de détecter les incidents de cybersécurité, d'intervenir dans de telles circonstances et d'assurer la reprise des activités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de

	l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront au COS, ce qui comprend la mise en œuvre des changements liés au personnel et aux processus. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, ainsi que les outils, les techniques et les protocoles employés par les auteurs de menace pour mener des attaques basées sur l'informatique quantique et la manière de se défendre contre celles-ci.

D.3 Intervenants/intervenantes en cas de cyberincident

Intervenants/intervenantes en cas d'incident lié à la technologie opérationnelle (TO)

Référence au cadre de la NICE	Protect and Defend, Cyber Defence Incident Responder, PR-CIR-001
Description fonctionnelle	Le ou la titulaire propose des activités d'intervention immédiates et détaillées pour atténuer ou limiter les menaces et les incidents non autorisés de cybersécurité au sein d'une organisation, notamment la planification et l'élaboration de plans d'action, l'établissement des priorités des activités et le soutien des opérations de reprise et de l'analyse après incident.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à une défaillance catastrophique des systèmes de TI et de données de l'organisation et avoir des répercussions graves sur les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Il s'agit d'un emploi de premier échelon courant au sein du Centre des opérations de sécurité (COS). Une formation et une expérience supplémentaires pourraient permettre d'accéder à des rôles plus techniques ou plus opérationnels axés sur les opérations de cybersécurité (p. ex. l'évaluation et la gestion des vulnérabilités, la criminalistique numérique, l'analyse des menaces et l'analyse des maliciels) et offrir des possibilités de gestion.
Autres titres	▪ Intervenants/intervenantes en cas d'incident lié à la cybersécurité ▪ Responsables du traitement des incidents – centre des opérations de sécurité ▪ Premiers intervenants/premières intervenantes en cybersécurité ▪ Intervenants/intervenantes en cas d'incident de sécurité lié à la technologie opérationnelle
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	Ces tâches visent tant les systèmes des TI que les systèmes de la TO. ▪ Exécuter des tâches de prise en charge des incidents de cyberdéfense en temps réel (p. ex. collecte d'éléments de preuve, corrélation et suivi des intrusions, analyse des menaces et correction directe du système) ▪ Procéder au triage de la sécurité pour déterminer et analyser les cyberincidents et les cybermenaces ▪ Surveiller activement les réseaux et les systèmes en cas de cyberincident et de cybermenace ▪ Procéder à l'analyse des risques et à l'examen de la sécurité des journaux du système afin de cerner les cybermenaces possibles ▪ Effectuer des analyses et des examens ou déployer des scanneurs de réseau, des outils d'évaluation des vulnérabilités, des protocoles de réseau, des protocoles de sécurité Internet, des systèmes de détection des intrusions, des pare-feu, des vérificateurs de contenu et des logiciels de point terminal ▪ Recueillir et analyser des données pour cerner les lacunes et les vulnérabilités en matière de cybersécurité et formuler des recommandations qui permettent de les corriger rapidement ▪ Élaborer et préparer des analyses et des rapports sur les incidents de cyberdéfense ▪ Définir et tenir à jour les jeux d'outils et les procédures ▪ Élaborer, mettre en œuvre et évaluer des plans et des activités de prévention et d'intervention en cas d'incident, et les adapter pour contenir, atténuer ou éliminer les effets des incidents de cybersécurité ▪ Fournir un soutien à l'analyse des incidents sur les plans et les activités d'intervention

	▪ Effectuer de la recherche et du développement sur les incidents et les mesures d'atténuation en matière de cybersécurité ▪ Créer un plan d'élaboration de programme qui comprend des évaluations des lacunes en matière de sécurité, des politiques, des procédures, des manuels et des manuels de formation ▪ Passer en revue, concevoir et fournir du matériel de formation pertinent
Compétences requises pour l'éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information avec une spécialisation en informatique, en cybersécurité, en sécurité des réseaux ou dans un domaine équivalent.
Formation requise	Formation en opérations de cybersécurité avec certification de niveau industriel dans un domaine connexe (p. ex. opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, exploitation d'appliances de sécurité). Formation spécialisée obligatoire pour la technologie opérationnelle et les systèmes connexes.
Expérience professionnelle requise	L'expérience initiale requise est d'avoir travaillé avec succès dans un environnement informatique et au sein d'une équipe technique.
Outils et technologies	▪ Processus et procédures de gestion des incidents ▪ Systèmes de défense, y compris les pare-feu, les logiciels et systèmes antivirus, les systèmes de détection des intrusions et de protection contre les intrusions, les scanneurs et les alarmes. ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents
Compétences	**Intervenants/intervenantes en cas d'incident lié à la cybersécurité** Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau de base : ☐ Administration et gestion de la sécurité des réseaux ☐ Architecture de sécurité des réseaux ☐ Sécurité du matériel et des micrologiciels ☐ Sécurité définie par logiciel et sécurité des applications ☐ Virtualisation et sécurité des RPV ☐ Sécurité infonuagique ☐ Sécurité des dispositifs mobiles et sans fil ☐ Établissement de zones de sécurité des TI ☐ Chiffrement et cryptographie, dont les concepts et les principes de gestion des clés ☐ Analyse des vulnérabilités ☐ Outils, processus et procédures de gestion des vulnérabilités ☐ Sécurité des applications Web ☐ Livres de configuration et de construction opérationnelle ☐ Acquisitions de systèmes et projets ☐ Responsabilités juridiques et en matière d'éthique associées aux opérations de cybersécurité, y compris la conduite des enquêtes, le respect de la vie privée et la préservation de la preuve ☐ Rédaction et présentation des questions techniques (p. ex. rapports d'incident, rapports techniques, etc.) pour assurer la compréhension des membres de la direction ☐ Rudiments de la continuité des activités et de l'intervention en cas de sinistre Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Concepts, exploitation et configuration des appliances de sécurité réseau (équipements basés sur le rôle – systèmes ou appliances de cyberdéfense des réseaux, des serveurs et des postes de travail) ☐ Types d'intrusions et indicateurs de compromission (IC) ☐ Sources d'information sur les menaces ☐ Tactiques, techniques et procédures (TTP) communes aux auteurs de cybermenace ☐ Processus, responsabilités et pouvoirs en matière de gestion des risques ☐ Méthodes, outils et systèmes de détection et de prévention des intrusions ☐ Analyse des intrusions et techniques d'atténuation ☐ Analyse de base des maliciels

	☐ Enquêtes de cybersécurité et préservation des preuves **Pour les intervenants/intervenantes en cas d'incident lié à la technologie opérationnelle** En plus des connaissances, compétences et aptitudes pertinentes susmentionnées, les suivantes s'appliquent au niveau de base : ☐ Logiciels et matériel de la TO, contrôleurs logiques programmables et relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris l'incidence et l'évaluation des dispositifs de l'IdO) ☐ Exigences juridiques et relatives à la conformité, dont les responsabilités organisationnelles en matière de sécurité publique et dans les lieux de travail liées à la TO ou à la production ☐ Systèmes de télémétrie, communications de données, acquisition de données et contrôle des processus ☐ Systèmes d'exploitation, réseaux et systèmes de communication ☐ Réseaux de distribution électrique, équipement du système électrique, fonctionnement des stations de transformation et théorie de l'électricité ☐ Systèmes et applications de gestion des bases de données ☐ Mesures ou indicateurs des problèmes de performances, de disponibilité, de capacité ou de configuration des systèmes de la TO ☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défaillances
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités pour ce qui est de détecter les incidents de cybersécurité, d'intervenir dans de telles circonstances et d'assurer la reprise des activités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront au COS, ce qui comprend la mise en œuvre des changements liés au personnel et aux processus. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, ainsi que les outils, les techniques et les protocoles employés par les auteurs de menace pour mener des attaques basées sur l'informatique quantique et la manière de se défendre contre celles-ci.

D.4 Techniciens et techniciennes des opérations de cybersécurité

Référence au cadre de la NICE	Protect and Defend, PR-INF-001, Cyber security Defence Infrastructure Support
Description fonctionnelle	Le ou la titulaire du poste met à l'essai, met en œuvre, déploie, tient à jour et administre le matériel et les logiciels de l'infrastructure des opérations de sécurité.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait mener à la compromission ou à la défaillance du système de sécurité, ce qui peut avoir une incidence importante sur les systèmes, les capacités et 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 l'administration de réseaux, des fonctions techniques ou d'autres fonctions similaires. Une formation et une expérience supplémentaires pourraient permettre d'accéder à des rôles plus techniques ou plus opérationnels et offrir des possibilités d'emploi en gestion.
Autres titres	▪ Spécialistes et techniciens/techniciennes en soutien des infrastructures de sécurité ▪ Analystes des systèmes de sécurité ▪ Techniciens/techniciennes de systèmes de sécurité ▪ Analystes de contrôles de sécurité
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 22220 – Techniciens/techniciennes de réseau informatique et Web 22221 – Agents/agentes de soutien aux utilisateurs
Tâches	▪ Surveiller activement les performances du système de sécurité et résoudre les problèmes d'interopérabilité du matériel ou des logiciels, ainsi que les pannes et les défaillances du système ▪ Installer, configurer et tenir à jour les logiciels, le matériel et l'équipement périphérique ▪ Élaborer, produire et tenir à jour des rapports d'incident et des évaluations des vulnérabilités et des répercussions ▪ Élaborer et tenir à jour une base de données de suivi et de solutions ▪ Analyser les opérations de sécurité et recommander des améliorations et des changements à y apporter ▪ Vérifier et journaliser les activités de gestion du cycle de vie et produire des rapports à cet égard ▪ Administrer les comptes, les privilèges et les accès aux systèmes et à l'équipement ▪ Effectuer la gestion des biens ou le contrôle des stocks des ressources des systèmes et de l'équipement ▪ Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation
Compétences requises pour l'éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des technologies de l'information connexe)
Formation requise	Formation dans les systèmes de cybersécurité, les opérations liées aux systèmes de sécurité et les outils fournis par les fournisseurs (p. ex. systèmes de détection d'intrusion, pare-feu, antivirus, gestion des incidents, etc.)
Expérience professionnelle requise	De deux à trois ans d'expérience dans les opérations et la sécurité des réseaux
Outils et technologies	▪ Outils, journaux et procédures des systèmes de cybersécurité ▪ Politiques et directives organisationnelles ▪ Systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents

Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent au niveau de base : ☐ Menaces qui pèsent sur les systèmes d'information et leur sécurité ☐ Concepts, protocoles, composants et principes liés à l'architecture de sécurité des réseaux (p. ex. application d'une défense en profondeur) ☐ Techniques de base de renforcement de la sécurité des systèmes, des réseaux et des SE ☐ Enregistrements et modes de transmission (p. ex. Bluetooth, identification par radiofréquence [RFID pour *Radio Frequency Identification*], réseaux infrarouges, technologie sans fil [Wi-Fi pour *Wireless Fidelity*], radiomessagerie, réseaux cellulaires, antennes paraboliques, voix sur IP [VoIP pour *Voice over Internet Protocol*]) ☐ Analyse du trafic réseau (outils, méthodologies, processus) ☐ Architectures et normes de gestion de l'identité, des justificatifs d'identité et de l'accès ☐ Politiques, procédures et pratiques en matière de gestion des incidents de cybersécurité ☐ Analyse organisationnelle des tendances commerciales et inhérentes aux utilisateurs ☐ Consultation des clients et résolution des problèmes Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Procédures, principes et méthodologies en matière de mise à l'essai des systèmes de cybersécurité ☐ Outils et applications relatifs aux systèmes de détection d'intrusion (SDI) ou aux systèmes de prévention d'intrusion (SPI) ☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ☐ Résolution, analyse et atténuation des problèmes liés aux infrastructures de cybersécurité ☐ Politiques et contrôles liés aux systèmes de cybersécurité et à la gestion des comptes
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la gestion des systèmes de cybersécurité. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront aux processus de gestion de l'identité et de l'accès et aux changements techniques et de processus connexes. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, ainsi que les outils, les techniques et les protocoles employés par les auteurs de menace pour mener des attaques basées sur l'informatique quantique et la manière de se défendre contre celles-ci.

D.5 Analystes de l'évaluation des vulnérabilités

Référence au cadre de la NICE	Protect and Defend, PR-VAM-001, Vulnerability Assessment (VA) Analyst
Description fonctionnelle	Le ou la titulaire du poste analyse les applications et les systèmes d'exploitation pour déceler les lacunes et les vulnérabilités. Il effectue et présente des évaluations de vulnérabilité sur les réseaux et les systèmes d'une organisation.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait faire en sorte que des vulnérabilités ne soient pas détectées ou soient identifiées de façon erronée, ce qui pourrait donner lieu à une compromission. Cela peut avoir des répercussions importantes 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 opérationnel lié à la cybersécurité qui est généralement précédé par de deux à trois ans d'expérience dans un poste lié aux réseaux ou à la sécurité opérationnelle. Ce parcours pourrait mener à une spécialisation en tant qu'analystes des vulnérabilités, de chefs d'équipe rouge ou bleu, de testeurs ou testeuses de pénétration ou de gestion.
Autres titres	▪ Testeurs/testeuses des vulnérabilités ▪ Évaluateurs/évaluatrices des vulnérabilités ▪ Gestionnaires des évaluations des vulnérabilités
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Cerner les failles critiques dans les applications et les systèmes que les auteurs de cybermenace pourraient exploiter ▪ Effectuer des évaluations des vulnérabilités des technologies pertinentes (p. ex. environnement informatique, réseau et infrastructure de soutien, et applications) ▪ Préparer et présenter des évaluations exhaustives des vulnérabilités ▪ Effectuer des audits et des balayages de la sécurité du réseau ▪ Tenir à jour la trousse de vérification déployable de la cyberdéfense (p. ex. logiciels et matériel de cyberdéfense spécialisés) pour appuyer les opérations de cyberdéfense ▪ Préparer des rapports de vérification qui cernent les constatations techniques et procédurales, et formuler des recommandations sur les stratégies et les solutions correctives ▪ Effectuer ou soutenir des tests de pénétration autorisés sur les réseaux et systèmes de l'organisation ▪ Définir et examiner 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 et fournir le matériel de formation, et surveiller les efforts d'éducation
Compétences requises pour l'éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des technologies de l'information connexe).
Formation requise	Formation dans les systèmes de cybersécurité, l'évaluation des vulnérabilités et l'analyse. Formulation sur les systèmes de vulnérabilités des fournisseurs.

Expérience professionnelle requise	De deux à trois ans d'expérience à un poste lié aux opérations réseau ou de cybersécurité.
Outils et technologies	▪ Politiques, procédures et pratiques de sécurité organisationnelle ▪ Outils d'évaluation des vulnérabilités ▪ Politiques, processus et pratiques en matière de gestion des vulnérabilités ▪ Bases de données des vulnérabilités communes
Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent au niveau de base : ☐ Outils, techniques et protocoles avancés utilisés par les auteurs de menace ☐ Principes, outils et techniques relatifs aux tests de pénétration ☐ Processus de gestion des risques visant à évaluer et à atténuer les risques ☐ Concepts d'administration des systèmes ☐ Concepts de la cryptographie et de la gestion des clés cryptographiques ☐ Cryptologie ☐ Établissement des problèmes de sécurité en fonction de l'analyse des données sur les vulnérabilités et la configuration ☐ Politiques, processus et pratiques en matière de gestion des vulnérabilités Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Planification des EV, dont les risques qui pèsent sur les systèmes et les mesures d'atténuation connexes ☐ Menaces et vulnérabilités pour la sécurité des systèmes et des applications ☐ Techniques d'administration des systèmes et techniques de renforcement des réseaux et des systèmes d'exploitation ☐ Analyse des paquets à l'aide des outils appropriés ☐ Conduite d'analyses des vulnérabilités et établissement des vulnérabilités dans les systèmes de sécurité ☐ Exécution d'évaluations des vulnérabilités, des répercussions et des risques ☐ Examen des registres du système pour repérer les traces d'intrusion ☐ Utilisation d'outils d'analyse réseau pour déterminer les vulnérabilités
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités pour ce qui est de détecter les incidents de cybersécurité, d'intervenir dans de telles circonstances et d'assurer la reprise des activités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront au COS, ce qui comprend la mise en œuvre des changements liés au personnel et aux processus. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, de la compréhension des vulnérabilités du système et de la manière d'atténuer les menaces de nature quantique.

D.6 Testeurs ou testeuses de pénétration

Référence au cadre de la NICE	Aucune.
Description fonctionnelle	Le ou la titulaire du poste effectue des tests officiels et contrôlés ainsi que des évaluations de la sécurité physique sur des applications Web, des réseaux et d'autres systèmes, au besoin, pour détecter et exploiter les vulnérabilités de sécurité.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait faire en sorte que des vulnérabilités ne soient pas détectées ou soient identifiées de façon erronée, ce qui pourrait donner lieu à une compromission. Cela peut avoir des répercussions importantes 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 généralement précédé par une expérience considérable (de trois à cinq ans) dans un poste lié aux opérations de cybersécurité, notamment en analyse des vulnérabilités, en analyse des maliciels ou en analyse technique des systèmes de sécurité. Il s'agit d'un rôle technique qui peut mener à une spécialisation technique ou à des rôles de leadership et de gestion dans des équipes de testeurs.
Autres titres	▪ Spécialistes des tests et de l'évaluation de la sécurité ▪ Analystes spécialisés/spécialisées dans l'évaluation des vulnérabilités
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Effectuer des tests de pénétration sur des applications Web, des connexions réseau et des systèmes informatiques afin de déterminer les cybermenaces et les vulnérabilités techniques ▪ Effectuer des évaluations de la sécurité physique du réseau, des dispositifs, des serveurs et des systèmes d'une organisation ▪ Concevoir des tests de pénétration et les outils nécessaires à leur exécution (p. ex. normes, risques, mesures d'atténuation) ▪ Enquêter sur les vulnérabilités et les failles de sécurité inconnues dans les applications Web, les réseaux et les systèmes pertinents que des auteurs de cybermenace peuvent facilement exploiter ▪ Rédiger et tenir à jour des documents sur les résultats des tests de pénétration exécutés ▪ Utiliser le piratage psychologique pour mettre au jour les lacunes en matière de sécurité ▪ Définir et examiner les exigences relatives aux solutions de sécurité de l'information ▪ Analyser et documenter les constatations en matière de sécurité et en discuter avec la direction et le personnel technique ▪ Fournir des recommandations et des lignes directrices sur la façon d'améliorer les pratiques de sécurité d'une organisation ▪ Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation
Compétences requises pour l'éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des technologies de l'information connexe)
Formation requise	Formation axée sur les outils, les techniques et les procédures d'analyse des vulnérabilités et de tests de pénétration.

Expérience professionnelle requise	De deux à trois ans d'expérience à un poste spécialisé lié aux opérations de cybersécurité et, de préférence, de l'expérience en EV.
Outils et technologies	▪ Politiques, procédures et pratiques de sécurité organisationnelle ▪ Mappage des systèmes organisationnels et architecture des réseaux ▪ Outils d'évaluation des vulnérabilités ▪ Politiques, processus et pratiques en matière de gestion des vulnérabilités ▪ Bases de données des vulnérabilités communes ▪ Outils et protocole relatifs aux tests de pénétration
Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Architecture de sécurité des réseaux ☐ Outils, techniques et protocoles avancés utilisés par les auteurs de menace ☐ Principes, outils et techniques relatifs aux tests de pénétration ☐ Processus de gestion des risques visant à évaluer et à atténuer les risques ☐ Concepts d'administration des systèmes ☐ Concepts de la cryptographie et de la gestion des clés cryptographiques ☐ Cryptologie ☐ Établissement des problèmes de sécurité en fonction de l'analyse des données sur les vulnérabilités et la configuration ☐ Politiques, processus et pratiques en matière de gestion des vulnérabilités ☐ Planification des tests de pénétration, dont les risques qui pèsent sur les systèmes et les mesures d'atténuation connexes ☐ Menaces et vulnérabilités pour la sécurité des systèmes et des applications ☐ Techniques d'administration des systèmes et techniques de renforcement des réseaux et des systèmes d'exploitation ☐ Analyse des paquets à l'aide des outils appropriés ☐ Conduite d'analyses des vulnérabilités et établissement des vulnérabilités dans les systèmes de sécurité ☐ Exécution d'évaluations des vulnérabilités, des répercussions et des risques ☐ Examen des registres du système pour repérer les traces d'intrusion ☐ Utilisation d'outils d'analyse réseau pour déterminer les vulnérabilités
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités pour ce qui est de détecter les incidents de cybersécurité, d'intervenir dans de telles circonstances et d'assurer la reprise des activités. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront au COS, ce qui comprend la mise en œuvre des changements liés au personnel et aux processus. ▪ L'utilisation accrue des outils automatisés par les auteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. Des stratégies d'atténuation créatives et pertinentes seront donc nécessaires localement. Cela exigera une bonne maîtrise de la pensée critique et abstraite. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, de la compréhension des vulnérabilités du système et de la manière d'atténuer les menaces de nature quantique.

D.7 Analystes en criminalistique numérique

Référence au cadre de la NICE	Investigate, Cyber Defence Forensic Analyst, INV-FOR-002
Description fonctionnelle	**La description basée sur les rôles qui suit ne concerne que les opérations de sécurité et ne comprend pas les fonctions de criminalistique numérique ou d'audit informatique qui doivent être assumées dans des professions connexes liées à l'application de la loi ou à l'audit.** Le ou la titulaire fait appel à la criminalistique numérique afin d'analyser les preuves tirées d'ordinateurs, de réseaux et d'autres dispositifs de stockage de données. Les tâches consistent notamment à faire ce qui suit : enquêter sur les preuves électroniques et les conserver, planifier et développer des outils, hiérarchiser les activités et soutenir les opérations de reprise et d'analyse après incident.
Conséquence d'une erreur ou risque	Une erreur, une négligence, une information désuète, un manque d'attention aux détails ou un mauvais jugement pourrait se traduire par l'incapacité de déterminer la source d'une compromission ou de l'atténuer, en plus d'avoir une incidence sur les systèmes d'information de l'organisation, ce qui ferait en sorte qu'il soit impossible de déposer des accusations criminelles ou d'engager des poursuites civiles.
Parcours de perfectionnement	Il s'agit souvent d'un poste de niveau 3 ou 3 dans un environnement opérationnel lié à la cybersécurité qui est généralement précédé par un minimum de deux à trois ans d'expérience dans un poste lié aux réseaux ou à la sécurité opérationnelle, notamment à titre d'analyste des maliciels. Ce parcours pourrait mener à une spécialisation en criminalistique numérique ou en évaluation de sécurité, ainsi qu'à des postes de chef d'équipe rouge ou bleu, de testeurs ou testeuses de pénétration ou de gestionnaire.
Autres titres	▪ Enquêteurs/enquêtrices en criminalistique numérique (postes généralement retrouvés dans des environnements liés à la cybercriminalité) ▪ Examinateurs/examinatrices en criminalistique numérique (postes généralement retrouvés dans des environnements d'audit informatique)
Classification nationale des professions (CNP) connexes	21220 – Spécialistes de la cybersécurité 21311 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 21231 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Effectuer des enquêtes en temps réel sur les incidents liés à la cyberdéfense (p. ex. collecte de preuves, corrélation et suivi des intrusions et analyse des menaces) ▪ Enquêter sur les incidents de sécurité conformément au mandat ▪ Planifier les activités d'analyse de criminalistique numérique dans le cadre des incidents de sécurité ▪ Recueillir et analyser des artéfacts d'intrusion (p. ex. code source, maliciel et configuration du système) et utiliser les données découvertes pour atténuer les incidents potentiels liés à la cyberdéfense ▪ Déterminer les artéfacts de l'analyse de criminalistique numérique et en rendre compte avec exactitude ▪ Capter et analyser le trafic réseau associé aux activités malveillantes à l'aide d'outils de surveillance réseau ▪ Contribuer à l'analyse après les incidents de sécurité et présenter des recommandations en fonction des activités de criminalistique numérique ▪ Rédiger et tenir à jour des rapports d'enquête et des rapports techniques ▪ Fournir une assistance technique sur les questions de preuve numérique au personnel approprié ▪ Compiler des éléments de preuve pour les dossiers judiciaires et fournir des témoignages d'expert lors des procédures judiciaires ▪ Gérer les preuves numériques conformément aux exigences appropriées de la chaîne de possession

	▪ Déterminer et gérer l'infrastructure ou le laboratoire d'analyse sécurisé ▪ Utiliser des systèmes judiciaires numériques (au besoin, selon les fonctions et les systèmes offerts) ▪ Préparer et examiner les politiques, les normes, les procédures et les lignes directrices en matière de criminalistique ▪ Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation
Compétences requises pour l'éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des technologies de l'information connexe)
Formation requise	Formation axée sur les outils, les techniques et les procédures de criminalistique numérique. De plus, selon le contexte technique de l'organisation et les systèmes et dispositifs utilisés, une formation spécialisée en criminalistique numérique pourrait être exigée (p. ex. appareil mobile, support numérique, etc.).
Expérience professionnelle requise	De deux à trois ans d'expérience dans un poste supérieur lié aux opérations de cybersécurité et, de préférence, de l'expérience dans des environnements actifs et hors ligne (*dead-box*).
Outils et technologies	▪ Politiques, procédures et pratiques de sécurité organisationnelle ▪ Mappage des systèmes organisationnels et architecture des réseaux ▪ Outils, techniques et procédures de criminalistique numérique ▪ Outils d'analyse de maliciels ▪ Système de gestion des événements et des incidents de sécurité ▪ Bases de données des vulnérabilités communes ▪ Mandat, responsabilités et limitations des pouvoirs en matière d'enquête de sécurité
Compétences	Les connaissances, compétences et aptitudes suivantes s'appliquent à un niveau avancé : ☐ Outils, techniques et procédures employés par les auteurs de menace ☐ Méthodes d'intervention et de prise en charge des incidents ☐ Système de gestion des événements et des incidents de sécurité ☐ Méthodologies, processus et pratiques de criminalistique numérique ☐ Tactiques, techniques et procédures d'obscurcissement ☐ Processus de collecte, d'emballage, de transport et d'entreposage des preuves électroniques pour éviter la modification, la perte, les dommages physiques ou la destruction des données ☐ Saisie et préservation des preuves numériques ☐ Lois, règlements, politiques et éthique applicables aux enquêtes et à la gouvernance ☐ Règles juridiques relatives aux preuves et procédures judiciaires, présentation de preuves numériques, témoignage à titre de témoin expert ☐ Criminalistique liée aux systèmes ou aux appareils (p. ex. mémoire, Active Directory, appareil mobile, réseau, ordinateur [inactif], etc.) ☐ Outils et techniques d'analyse des logiciels malveillants ☐ Rétro-ingénierie ☐ Capacités de criminalistique numérique déployables ☐ Types de criminalistique numérique, dont les outils, les techniques et les procédures (qui dépendent de systèmes organisationnels et d'information), ce qui peut comprendre ce qui suit : ○ Ordinateur ○ Réseau et Active Directory ○ Appareils mobiles ○ Supports numériques (image, vidéo, audio) ○ Mémoire
Futures tendances ayant une incidence sur les compétences clés	▪ La dépendance accrue aux services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la gestion des systèmes de cybersécurité. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les répercussions de l'option « Prenez vos appareils personnels » (PAP). Cela signifie que, peu importe les capacités de l'appareil, il faudra évaluer les risques qui pèsent sur l'organisation, mettre en œuvre des mesures d'atténuation pour tenir compte des possibles compromissions qui pourraient résulter de

	l'utilisation d'appareils personnels et déterminer les mesures que le Centre des opérations de sécurité (COS) devra prendre advenant un incident. ▪ L'utilisation accrue des outils automatisés, facilitée par l'intelligence artificielle, nécessitera une bonne compréhension de la façon dont ces outils s'intégreront aux processus de gestion de l'identité et de l'accès et aux changements techniques et de processus connexes. ▪ Des mécanismes visant à soutenir le degré 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 qui pèsent sur l'organisation et les possibles réponses dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les auteurs de menace modifieront fondamentalement la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences pour ce qui est de la mise en œuvre d'une stratégie post-quantique, ainsi que les outils, les techniques et les protocoles employés par les auteurs de menace pour mener des attaques basées sur l'informatique quantique et la manière de se défendre contre celles-ci.

Annexe E Rôles connexes à la cybersécurité

En plus des rôles principaux qui définissent la profession en cybersécurité dont il est question dans la présente publication, bon nombre de rôles connexes impliquent des responsabilités liées à la cybersécurité qui ne constituent généralement qu'une partie des responsabilités globales assumées au sein d'une organisation. Les titulaires de tels postes ne travaillent souvent en cybersécurité qu'à temps partiel, mais la portée et l'étendue de leurs rôles varient selon la taille de l'organisation, ainsi que le type et l'ampleur de l'infrastructure informatique ou Internet. Par exemple, au sein de grandes organisations faisant appel aux technologies de l'information, tous les rôles ci-dessous peuvent s'appliquer. Il est probable que les petites organisations qui dépendent peu des TI ou d'une connectivité à Internet pour la conduite de leurs activités externalisent une majeure partie de l'expertise et des services de nature technique. Les autres responsabilités non techniques en matière de cybersécurité seront donc réparties au sein de l'organisation.

Ce tableau présente brièvement les rôles connexes qui sont communs au domaine de la cybersécurité, l'identifiant du cadre de la NICE correspondant (le cas échéant), la CNP correspondante et les principales responsabilités en cybersécurité. En supposant que la majorité des personnes occupant ces fonctions possèdent déjà les compétences requises pour leurs fonctions et rôles principaux, les compétences clés ne sont fournies que pour les fonctions liées à la cybersécurité. Les membres actuels de l'effectif en général et les éducateurs et éducatrices en particulier devraient orienter la discussion sur le sujet de l'adaptation des programmes de formation et d'éducation afin de mieux refléter la réalité de la cybersécurité sur le marché du travail canadien.

Il importe de souligner que la catégorie « Protection et défense » n'est pas incluse dans la figure, puisque ce secteur d'activité ou cette catégorie d'emplois est réservé exclusivement à la cybersécurité.

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
Supervision et gouvernance	Directeurs généraux/Directrices générales, hauts dirigeants/hautes dirigeants ou propriétaires	OV-EXL-001	00011 00012	Exercer les pouvoirs de décision et établir une vision et une orientation pour les ressources et/ou les cyberopérations ou liées à la cybersécurité.	Cyberplanification stratégique Contexte opérationnel et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
	Dirigeants principaux/ dirigeantes principales de l'information ou techniciens/techniciennes en chef	Aucun	00011 00012 20010 20012	Diriger les services techniques et d'infrastructure des TI de l'organisation et exercer les pouvoirs de décision à ce sujet. Cela comprend souvent les services de cybersécurité.	Cyberplanification stratégique Contexte opérationnel et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Conseillers ou conseillères juridiques en cybersécurité	OV-LGA-001	41101 42200	Formuler des conseils et des recommandations juridiques sur des sujets pertinents liés au droit de l'informatique.	Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contexte de menace
	Agents ou agentes à la protection des renseignements personnels ou gestionnaires de la protection de la vie privée	OV-LGA-002	20012	Élaborer le programme de conformité à la protection de la vie privée et superviser le programme et le personnel responsable de manière à soutenir les besoins des cadres supérieurs chargés de la protection de la vie privée et de la sécurité et de leurs équipes en matière de conformité, de gouvernance, de politique et d'intervention en cas d'incident.	Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contexte de menace Contrôles de sécurité liés au respect de la vie privée
	Gestionnaires de la sécurité des communications (COMSEC)	OV-MGT-002	10030 20012	Personne responsable de la gestion des ressources de la sécurité des communications (COMSEC) d'une organisation (CNSSI 4009) ou gardien des clés pour un système de gestion des clés cryptographiques.	Gestion du programme de sécurité PCA et PRS Gestion des risques liés à la chaîne d'approvisionnement

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Politiques, directives et exigences de gestion en matière de COMSEC Comptabilité COMSEC Infrastructure et applications liées au chiffrement et à l'ICP Gestion des incidents COMSEC
	Développeurs/ développeuses et gestionnaires de l'effectif en cybersécurité	OV-SPP-001	41321	Élaborer des plans, des stratégies et de l'orientation à l'intention de l'effectif du cyberespace afin de répondre à leurs 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 de forces, ainsi qu'aux exigences en matière d'éducation et de formation dans le cyberespace.	Parcours de carrière en cybersécurité Sources et information sur le marché du travail en cybersécurité Normes professionnelles en cybersécurité Certifications et accréditations en cybersécurité Évaluation des compétences en cybersécurité
	Développeurs/ développeuses de curriculums pédagogiques en cybersécurité	OV-TEA-001	41200 41210 43109	Développer, planifier, coordonner et évaluer des cours de formation ou de sensibilisation sur la cybersécurité, des méthodes et des techniques selon les besoins pédagogiques.	Connaissances pertinentes du domaine cybernétique (par thème) Évaluation des compétences en cybersécurité
	Responsables de la formation en cybersécurité	OV-TEA-002	41200 41210 43109	Développer et offrir de la formation ou de l'éducation au personnel du domaine de la cybersécurité.	Connaissances pertinentes du domaine cybernétique (par thème) Évaluation des compétences en cybersécurité
	Planificateurs/ planificatrices de politiques et de stratégies en cybersécurité	OV-SPP-002	40011 41400	Élaborer et tenir à jour des plans, des stratégies et des politiques de cybersécurité pour soutenir et harmoniser les initiatives de cybersécurité de l'organisation et la conformité réglementaire.	Gestion du programme de cybersécurité PCA et PRS Contexte juridique et politique du cyberespace Contexte opérationnel et de menace

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Planification et développement de politiques en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Gestionnaires de programme	OV-PMA-001	00011 00012 20010	Diriger, coordonner, communiquer et intégrer la réussite globale du programme et rendre des comptes à cet égard conformément aux priorités de l'organisme ou de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Gestion du programme de cybersécurité PCA et PRS Gestion des risques liés à la chaîne d'approvisionnement Modèles de maturité de la cybersécurité Normes de cybersécurité Évaluation et mesure de la cybersécurité
	Gestionnaires de projets de TI	OV-PMA-002	20010 20012	Assurer la gestion des projets de TI.	Évaluation des menaces et des risques Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Intégration des cybersystèmes Gestion des projets de cybersécurité Exigences relatives à l'approvisionnement en produits de cybersécurité 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)

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
	Gestionnaires du soutien des produits	OV-PMA-003	20010 20012	Gérer l'ensemble des fonctions de soutien nécessaires à la mise en œuvre et au maintien de l'état de préparation et de la capacité opérationnelle des systèmes et des composants	Évaluation des menaces et des risques Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Intégration des cybersystèmes Gestion des projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Processus d'évaluation et de mise à l'essai de produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Gestionnaires des investissements et des portefeuilles de TI	OV-PMA-004	20010 20012	Gérer un portefeuille d'investissements en TI qui satisfait les besoins globaux de la mission et les priorités de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Gestion du programme de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Modèles de maturité de la cybersécurité Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Vérificateurs ou vérificatrices de programmes informatiques	OV-PMA-005	20010 20012	Procéder à l'évaluation d'un programme de TI ou de ses composantes individuelles en vue de déterminer la	Politiques, pratiques et procédures d'audit de cybersécurité Évaluation des menaces et des risques

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
				mesure dans laquelle il répond aux normes publiées.	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Contexte juridique et politique Exigences relatives à la conformité Exigences relatives à l'approvisionnement en produits de cybersécurité 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 des vulnérabilités Processus d'évaluation et de mise à l'essai de produits de cybersécurité
	Analystes des activités	Aucun	11201 21221 41401	Analyser et déterminer les besoins afin de recommander des solutions qui apportent une valeur opérationnelle aux intervenants.	Gouvernance, rôles et responsabilités associés à la cybersécurité Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Contexte juridique et politique Exigences relatives à la conformité Exigences relatives à l'approvisionnement en produits de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Évaluation des vulnérabilités Processus d'évaluation et de mise à l'essai de produits de cybersécurité
	Analystes financiers	Aucun	11101	Recueillir et analyser les renseignements financiers et les risques. Fournir des estimations financières, établir des prévisions et relever les tendances à ce sujet. Formuler des conseils afin de soutenir les activités de nature financière et en matière d'investissement.	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contextes juridique, politique et financier Exigences du programme de cybersécurité Approvisionnement et acquisition dans le domaine de la cybersécurité Évaluation et mesure de la cybersécurité
	Analystes des risques	Aucun	41401	Recueillir et analyser les risques organisationnels. Procéder aux évaluations des risques connexes et orienter la prise de mesures d'atténuation.	Gestion des risques liés à la cybersécurité Méthodes d'évaluation des menaces et des risques Contexte opérationnel et de menace Contextes juridique, politique et financier Exigences du programme de cybersécurité
	Spécialistes des communications	Aucun	10022 11202	Planifier, organiser et développer les activités liées à la publicité, au marketing et aux relations publiques.	Contexte de cybermenace Contexte juridique et politique Exigences relatives à la conformité PCA et PRS Communications durant un cyberincident (communications en période de crise)
	Administrateurs/ administratrices de sites Web ou	Aucun	21233 21234	Rechercher, concevoir, développer et produire des sites Internet et intranet et des médias basés sur le Web.	Menaces à la cybersécurité Vulnérabilités des applications Web

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
	gestionnaires de communications en ligne				Mise à l'essai et évaluation de logiciels Exigences relatives aux interventions en cas d'incidents liés à la cybersécurité
	Spécialistes de l'apprentissage et du perfectionnement	Aucun	41200 41210 43109	Développer, planifier, coordonner et évaluer les programmes et les activités d'apprentissage et de perfectionnement de l'organisation et du personnel.	Exigences organisationnelles en matière de cybersécurité Rôles et responsabilités associés à la sécurité Parcours de carrière en cybersécurité Évaluation des compétences en cybersécurité
	Planificateurs ou planificatrices de la continuité des activités et de la résilience	Aucun	11101 21220	Déterminer, coordonner et superviser l'élaboration d'un plan de continuité des activités afin de soutenir la résilience de l'organisation par rapport à la fraude, aux crimes financiers, aux cyberattaques, au terrorisme et aux défaillances des infrastructures.	Évaluation des menaces et des risques Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Exigences organisationnelles en matière de cybersécurité Rôles et responsabilités associés à la sécurité Plans, processus et procédures liés à la cybersécurité Gestion des incidents liés à la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Spécialistes de l'approvisionnement	Aucun	12102	Déterminer et acquérir l'équipement général et spécialisé, le matériel, les droits fonciers ou d'accès et les services organisationnels nécessaires au bon fonctionnement de l'organisation ou à un traitement ultérieur.	Évaluation des menaces et des risques Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Gestion des projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Processus d'évaluation et de mise à l'essai de produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
Conception et développe-ment (« Securely Provision » dans le cadre de la NICE)	Responsables de l'autorisation (généralement les DPI ou les propriétaires du système)	SP-RSK-001	00011 00012 20010	Haut fonctionnaire ou cadre supérieur à qui on a conféré les pouvoirs nécessaires pour prendre en charge l'exploitation d'un système d'information à niveau de risque acceptable pour les opérations organisationnelles (y compris la mission, les fonctions, l'image ou la réputation), aux actifs organisationnels, aux personnes, aux autres organisations et à la nation (CNSSI 4009).	Cyberplanification stratégique Contexte opérationnel et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Architectes d'entreprise	SP-ARC-001	20010 21311	Développer et maintenir les processus opérationnels, des systèmes et de l'information de manière à soutenir les besoins de la mission de l'entreprise. Développer des règles et des exigences en matière de technologies de l'information (TI) qui décrivent les architectures de base et cibles.	Objectifs organisationnels en matière de cybersécurité Architecture et conception de cybersécurité Génie en cybersécurité Évaluation des menaces et des risques Contexte juridique et politique du cyberespace

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement et ICP
	Développeurs/ développeuses de logiciels	SP-DEV-001	21232 22302 22312	Développer, créer, maintenir, écrire ou coder de nouveaux logiciels, applications informatiques ou utilitaires spécialisés (ou modifier ceux qui existent déjà).	Vulnérabilités des systèmes et des logiciels Mise à l'essai et évaluation de la sécurité des logiciels Outils, techniques et procédures liés à la sécurité des logiciels Pratiques et outils d'évaluation des vulnérabilités et de tests de pénétration Identité, justificatifs d'identité et authentification
	Planificateurs/ planificatrices des exigences système	SP-SRP-001	21311 21220 21222	Consulter les clients afin d'évaluer les exigences fonctionnelles et de traduire ces exigences en solutions techniques.	Objectifs organisationnels en matière de cybersécurité Architecture et conception de cybersécurité Génie en cybersécurité Évaluation des menaces et des risques Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement et ICP Normes de cybersécurité

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité Identité, justificatifs d'identité et authentification
	Spécialistes des tests et de l'évaluation des systèmes	SP-TST-001	21220 21222 21230 21231 22222	Planifier, préparer et exécuter les essais de systèmes pour évaluer les résultats par rapport aux spécifications et aux exigences. Analyser les résultats et en faire rapport.	Vulnérabilités des systèmes et des logiciels Mise à l'essai et évaluation de la sécurité des logiciels et des systèmes Outils, techniques et procédures liés à la sécurité des logiciels Pratiques et outils d'évaluation des vulnérabilités et de tests de pénétration Normes liées à la cybersécurité Mesure et évaluation de la cybersécurité
	Développeurs/ développeuses de systèmes	SP-SYS-002	21311 21230 21231	Concevoir, développer, mettre à l'essai et évaluer les systèmes d'information tout au long de leur cycle de développement.	Architecture et conception de cybersécurité Génie en cybersécurité Évaluation des menaces et des risques Contexte juridique et politique du cyberespace Exigences relatives à la conformité en matière de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement et ICP Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Identité, justificatifs d'identité et authentification
	Développeurs ou développeuses Web	Aucun	21234	Rechercher, concevoir, développer et produire des sites Internet et intranet et des médias basés sur le Web.	Menaces à la cybersécurité Vulnérabilités des applications Web Mise à l'essai et évaluation de logiciels Exigences relatives aux interventions en cas d'incidents liés à la cybersécurité
Exploitation et maintenance	Administrateurs ou administratrices de bases de données	OM-DTA-001	21223	Administrer les bases de données ou les systèmes de gestion des données qui permettent de stocker, d'interroger, de protéger et d'utiliser les données en toute sécurité.	Sécurité des systèmes et des données Menaces et vulnérabilités touchant les systèmes de données Plan de reprise après sinistre Sauvegarde et récupération de données Identité, justificatifs d'identité et authentification
	Analystes des données	OM-DTA-002	21223	Examiner les données tirées de multiples sources disparates dans le but de fournir des renseignements sur la sécurité et le respect de la vie privée. Concevoir et mettre en œuvre des algorithmes personnalisés, des processus de flux de travaux et des configurations pour les jeux de données complexes utilisés à l'échelle de l'entreprise aux fins de modélisation, d'exploration de données et de recherche.	Sécurité des systèmes et des données Menaces et vulnérabilités touchant les systèmes de données Plan de reprise après sinistre Sauvegarde et récupération de données Identité, justificatifs d'identité et authentification
	Gestionnaires de l'information (gestionnaires des	OM-KMG-001	20012	Assurer la gestion et l'administration des processus et des outils qui permettent à l'organisation de déterminer et de	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
	connaissances de la NICE)			documenter le capital intellectuel et le contenu de l'information, et d'y accéder.	Catégorisation de l'information et des données Sécurité des systèmes et des données Menaces et vulnérabilités touchant les systèmes de données Plan de reprise après sinistre Sauvegarde et récupération de données Identité, justificatifs d'identité et authentification
	Spécialistes du soutien technique	OM-STS-001	22220 22221	Fournir un soutien technique aux clients qui ont besoin d'assistance en utilisant du matériel et des logiciels au niveau du client conformément aux composantes des processus organisationnels établis ou approuvés (c.-à-d., plan directeur de gestion des incidents, le cas échéant).	Contexte opérationnel et de menace Sécurité des systèmes et des données Sauvegarde et récupération de données Cybermenaces et vulnérabilités Intervention en cas d'incident Politiques, pratiques et opérations liées aux cybersystèmes
	Spécialistes des opérations réseau	OM-NET-001	22220 22221	Planifier, mettre en œuvre et exploiter les services ou systèmes réseau de manière à inclure le matériel et les environnements virtuels.	Contexte opérationnel et de menace Sécurité des systèmes et des données Sauvegarde et récupération de données Cybermenaces et vulnérabilités Intervention en cas d'incident Politiques, pratiques et opérations liées aux cybersystèmes
	Administrateurs/ administratrices de système	OM-ADM-001	22220	Assurer la mise en place et la maintenance d'un système ou des éléments particuliers d'un système (p. ex.	Contexte opérationnel et de menace Sécurité des systèmes et des données

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
				installation, configuration et mise à jour du matériel et des logiciels; création et gestion des comptes utilisateur; supervision ou exécution des 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).	Sauvegarde et récupération de données Cybermenaces et vulnérabilités Intervention en cas d'incident Politiques, pratiques et opérations liées aux cybersystèmes Identité, justificatifs d'identité et authentification
	Analystes de systèmes de données	Aucun	21223	Établir, développer et analyser les besoins de l'organisation en matière de systèmes de données. Concevoir et mettre en œuvre les systèmes de données et en assurer le soutien.	Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Sécurité des systèmes et des données Menaces et vulnérabilités touchant les systèmes de données Plan de reprise après sinistre Sauvegarde et récupération de données Identité, justificatifs d'identité et authentification Outils, techniques et procédures de cybersécurité servant à protéger les données et les systèmes de données Chiffrement et ICP
	Gestionnaires de système (dont les rôles de gestionnaires de système, de logiciels et de systèmes de données)	Aucun	20012	Planifier, organiser, diriger, contrôler et évaluer les activités menées par les organisations qui analysent, conçoivent, développent, mettent en œuvre, exploitent et administrent des logiciels informatiques et de télécommunications, des réseaux et des systèmes d'information.	Évaluation des menaces et des risques Gestion des risques liés à la cybersécurité Contexte opérationnel et de menace Contexte technique Intégration des cybersystèmes Gestion des projets de cybersécurité

Secteur d'activités ou catégorie d'emplois	Titre ou rôle de travail courant	Identifiant de la NICE	CNP	Principale responsabilité en matière de cybersécurité (NICE et autres sources)	Principales compétences en cybersécurité
					Exigences relatives à l'approvisionnement en produits de cybersécurité 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 F

Mise en place en 2019, l'Alliance des talents en cybersécurité (ATC) est un partenariat regroupant le gouvernement, le milieu universitaire et les chefs de file de l'industrie qui vise à tirer avantage des programmes existants, à faciliter le changement et l'innovation, ainsi qu'à fournir le leadership et la vision nécessaires pour accroître le nombre de professionnels de la cybersécurité qualifiés dans les secteurs privé et public du Canada. Les membres de ce partenariat collaborent à l'élaboration des stratégies, au développement et à la promotion des initiatives, et à l'exécution des actions nécessaires pour faire progresser l'éducation, la formation et le perfectionnement de l'effectif en ce qui a trait à la cybersécurité.
Parmi les membres de l'ATC, on retrouve :

- Banque du Canada
- Laboratoires Nucléaires Canadiens
- Chambre de commerce du Canada
- Centre canadien pour la cybersécurité
- Cyber Nouveau-Brunswick (CyberNB)
- CyberQuébec
- Digital Nova Scotia
- Emploi et Développement social Canada
- Gouvernement de la Saskatchewan
- IBM Canada Ltée
- Innovation, Sciences et Développement économique Canada
- Sécurité publique Canada
- Quantum-Safe Canada
- Rogers Cybersecure Catalyst
- Réseau intégré sur la cybersécurité (SERENE-RISC)
- TECHNATION
- Toronto Finance International
- Université de Waterloo, Institute for Quantum Computing