Résultats d'apprentissage pour la main-d'œuvre en cybersécurité

Une base pour éduquer la main-d'œuvre canadienne en cybersécurité

TECHNATION CA

À propos de

TECHNATION

TECHNATION est le pont entre l'industrie et le gouvernement en ce qui a trait à la prospérité technologique du Canada. Comme organisme sans but lucratif dirigé par ses membres, TECHNATION rallie le secteur canadien des technologies, les différents paliers de gouvernement et les collectivités pour encourager la prospérité technologique au Canada. TECHNATION stimule cette dernière en offrant des occasions de sensibilisation, de développement professionnel et de réseautage à tous les niveaux de l'industrie et du gouvernement; en mettant en contact les entreprises canadiennes en croissance et les dirigeants technologiques mondiaux; en impliquant la chaîne d'approvisionnement mondiale; et en alimentant le bassin de talents dans le secteur des technologies. TECHNATION est le porte-parole national officiel de l'industrie des technologies de l'information et de la communication (TIC), qui représente une valeur de 210 milliards de dollars depuis plus de 60 ans. Plus de 43 200 entreprises canadiennes des TIC créent et fournissent des biens et services qui contribuent à créer une société plus productive, plus concurrentielle et plus novatrice. Le secteur des TIC génère plus de 666 500 emplois directs et indirects, et investit 7,5 milliards de dollars par an en recherche et développement, soit plus que tout autre jouer du secteur privé.
technationcanada.ca

Développement de la main-d'œuvre chez TECHNATION

La prospérité du Canada repose sur une main-d'œuvre en informatique qui possède les compétences nécessaires pour s'assurer que nos entreprises et le pays demeurent concurrentiels dans un marché mondial en constante évolution. TECHNATION contribue à développer les talents en informatique, que ce soit dans l'industrie ou en dehors, par un mélange de programmes de formation et de recyclage. En tant que service stratégique de TECHNATION, le Développement de la main-d'œuvre vise à constituer le bassin de personnel dont le Canada a besoin pour demeurer en tête dans l'économie numérique. Il vise notamment à encourager les jeunes à faire carrière dans les technologies, à agir comme consultants en matière d'enseignement technique et de résultats d'apprentissage, à guider ceux qui œuvrent dans des domaines non techniques ou les groupes sous-représentés vers l'obtention des compétences nécessaires pour se lancer dans une carrière en technologies, à encourager la diversité dans l'industrie et à contribuer à l'élaboration de politiques publiques visant à appuyer, à développer et à agrandir le bassin de travailleurs en technologies au Canada.

Remerciements

Bénévoles scolaires et industriels

La création de ces résultats d'apprentissage en cybersécurité pour la main-d'œuvre aurait été impossible sans le financement généreux, les idées et les conseils des partenaires scolaires et industriels. Nous les remercions chaleureusement pour leur dévouement et pour leur participation à cet effort, rendu particulièrement difficile en 2020 par la pandémie de COVID-19, qui a exercé d'énormes pressions sur ces communautés. Veuillez consulter l'Annexe A pour la liste complète des participants.

L'Alliance de talents en cybersécurité

TECHNATION souhaite féliciter les membres de l'Alliance de talents en cybersécurité et reconnaître leur esprit de direction, leur supervision et leurs conseils durant la rédaction du *Cadre des compétences en matière de cybersécurité au Canada et de la Norme professionnelle nationale (NPN)*. Ces documents de référence étaient essentiels pour déterminer les résultats d'apprentissage pour la main-d'œuvre en cybersécurité. Pour consulter ces documents, veuillez visiter le site technationcanada.ca/en/future-workforce-development/cybersecurity/

Professionnels du domaine de la cybersécurité

TECHNATION souhaite aussi exprimer sa sincère gratitude aux professionnels et aux parties prenantes du domaine de la cybersécurité ayant contribué, directement ou non, à l'élaboration de cette norme par l'intermédiaire d'entretiens, de sondages, de consultations et de réunions informelles. Bien qu'ils soient trop nombreux pour les mentionner individuellement, nous sommes sincèrement reconnaissants de l'intérêt et de l'expertise que les membres engagés de la communauté de cybersécurité ont apportés tout au long de ce projet. Leur point de vue et leur perspective ont été essentiels à l'atteinte des résultats. Nous les remercions d'avoir partagé avec nous leur temps, leur savoir, leurs recherches et leur expérience. Nous attendons également avec impatience leur contribution au processus de révision afin que les résultats d'apprentissage en cybersécurité pour la main-d'œuvre et la NPN restent actuels et pertinents.

Le Centre canadien pour la cybersécurité

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

National Initiative on Cybersecurity Education (NICE) – États-Unis

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

Gouvernement du Canada

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

Canada

Table des matières

Avant-propos

Ce document vise à suggérer aux fournisseurs de services de formation et d'enseignement des résultats d'apprentissage pour les candidats qui veulent faire carrière dans le domaine de la cybersécurité.

Ces résultats d'apprentissage ont été élaborés en consultation avec des experts industriels et pédagogiques. Les résultats d'apprentissage visent à garantir que les candidats souhaitant intégrer une équipe dans une organisation de cybersécurité ont su prouver leur maîtrise des bases de la cybersécurité, comme du domaine en général, avant de poursuivre leur spécialisation.

Comme le montre le graphique ci-dessous, le parcours d'apprentissage comprend des *exigences initiales d'apprentissage* qui s'appliquent à tous les candidats en cybersécurité, quel que soit le domaine. Elles constituent les *bases de la cybersécurité*, qui sous-tendent les compétences transversales des emplois en cybersécurité.

Après les *bases de la cybersécurité* suivent les résultats d'apprentissage pour chaque secteur d'activité aligné sur les principales catégories du Cadre des compétences en matière de cybersécurité au Canada : supervision et gouvernance, conception et développement, exploitation et maintenance, protection et défense. Ces sujets approfondissent le thème de la cybersécurité dans les catégories de métiers ciblées nécessaires à l'efficacité dans ce domaine. Une fois ces résultats d'apprentissage atteints, les candidats devraient pouvoir occuper des postes de premier plan en cybersécurité, dans une organisation qui œuvre dans ce secteur/cette catégorie de travail. Cela permet aussi de faire un pont important entre le travail de base et le travail spécialisé, qui n'était généralement pas offert par les programmes d'études postsecondaires.

Une fois ces résultats d'apprentissage atteints, les candidats peuvent continuer à développer leurs compétences dans cette catégorie de travail en tant que généralistes, ou progresser dans des travaux plus spécialisés ou plus techniques en cybersécurité, comme le montre le graphique.

Postes en cybersécurité

Progression de l'apprentissage et du développement

Principes fondamentaux pour tous les postes essentiels en matière de cybersécurité	Bases de la catégorie de travail (encourage le travail dans le domaine)	Apprentissage à l'appui des postes spécialisés (spécialisation, programme menant à un diplôme ou programmes/cours fondés sur les fournisseurs + expérience)	
Bases de la cybersécurité; exigences initiales d'apprentissage	**Supervision et gouvernance** (Gestion de la cybersécurité)	• Responsable de la sécurité de l'information • Agent de sécurité des systèmes d'information • Auditeur de la sécurité de l'information	Spécialisation technique, conseil ou gestion
	Conception et développement (Exigences techniques de sécurité)	• Architecte de la sécurité • Ingénieur en sécurité/Ing. en sécurité Technologue • Évaluateur de logiciels sécurisés • Spécialiste de test et d'évaluation de sécurité • Analyste de la sécurité de la chaîne d'approvisionnement • Analyste de la sécurité de la chaîne d'approvisionnement • Développeur de la sécurité des systèmes d'information • Ingénieur/analyste en automatisation de la sécurité • Cryptanalyste/cryptographe	
	Exploitation et maintenance (Infrastructure de cybersécurité)	• Spécialiste du soutien à la gestion de l'identité et de l'authentification • Spécialiste du chiffrement/soutien à la gestion des clés • Spécialiste de la protection des données/agent de la protection de la vie privée	
	Protection et défense (Opérations de cybersécurité)	• Gestionnaire des opérations de cybersécurité • Analyste des opérations de cybersécurité • Spécialiste du soutien aux infrastructures des opérations de cybersécurité • Responsable des incidents de cybersécurité • Technicien des opérations de cybersécurité • Analyste d'évaluation de vulnérabilité • Testeur de pénétration • Analyste en investigation informatique numérique	

Progression de l'apprentissage et du développement →

Bases de la cybersécurité; exigences initiales d'apprentissage

Prérequis

Tous les professionnels de la cybersécurité, quel que soit leur poste, devraient posséder des compétences de niveau d'entrée pour pouvoir appliquer les bases des éléments suivants dans leur domaine de travail fonctionnel (supervision et gouvernance, conception et développement, exploitation et maintenance, protection et défense) :

- Systèmes de TI et réseaux
- Architecture et modèles de systèmes
- Protocoles, systèmes et dispositifs Internet
- Bases de la cybersécurité
    - Cadre de sécurité intégrée
    - Stratégies et approches en matière de cybersécurité
    - Contexte des cybermenaces et exposition aux menaces communes (personnel, physique, TI/logique, chaîne d'approvisionnement)
    - Processus et sources de renseignements sur les cybermenaces
    - Analyse de la cybersécurité
    - Politiques, processus et meilleures pratiques

Bases de la cybersécurité; exigences initiales d'apprentissage

(suite)

en matière de gestion de la cybersécurité
    - Systèmes, outils et applications de cybersécurité
    - Législation et conformité (par exemple, respect de la vie privée, échange de renseignements, création de rapports, normes obligatoires, etc.)
    - Normes nationales et industrielles
- Résolution de problèmes et réflexion complexe dans des environnements dynamiques
- Maintien d'une plus grande conscience de la situation en matière de sécurité
- Conscience de soi concernant les connaissances, les compétences et les habiletés requises pour répondre aux changements commerciaux, techniques et aux menaces
- Pensée critique et méthodes d'analyse
- Apprentissage continu pour soutenir l'actualisation des connaissances sur les menaces émergentes, les innovations technologiques en matière de sécurité et l'évolution du paysage de la cybersécurité
- Communications (orales et verbales) adaptées au contexte organisationnel, y compris la rédaction et l'écriture de rapports techniques
- Réflexion stratégique et sens des affaires pour comprendre le contexte commercial et les risques liés à la cybersécurité
- Travail d'équipe/collaboration avec d'autres personnes, y compris des professionnels non spécialisés dans la cybersécurité
- Intégrité professionnelle
- Éthique et responsabilités professionnelles
- Formation et sensibilisation à la cybersécurité dans leur domaine

Supervision et gouvernance

Résultats d'apprentissage

La responsabilité principale de cette catégorie de travail est la direction et la gestion du programme de cybersécurité pour l'organisation.

La majorité du travail au sein de ce sous-groupe professionnel est effectuée par des personnes appartenant à des groupes de compétences professionnelles reconnus, comme les cadres (cadres supérieurs, cadres intermédiaires) et les professions commerciales, financières et administratives (par exemple, analystes commerciaux, analystes financiers, analystes de risques, communications). Par conséquent, de nombreux postes pertinents dans cette catégorie sont des postes adjacents, comme les professionnels des politiques, des communications, de la formation et de la sensibilisation.

Voici les principaux postes de travail au sein de ce domaine d'activité/cette catégorie de travail :

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

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

Les compétences, y compris les compétences CCH essentielles pour ces spécialisations, sont incluses dans la Norme professionnelle nationale. Les résultats d'apprentissage suivants sont le fruit d'une analyse de tous les postes de cette catégorie et sont pertinents pour les programmes de grade, de diplôme ou de certification axés sur la gestion en cybersécurité. Ils seront aussi utiles à ceux qui souhaitent intégrer du contenu de cybersécurité dans des programmes de gestion existants (financiers, commerciaux, génie sanitaire, etc.). Les résultats d'apprentissage sont présentés dans une séquence d'enseignement suggérée.

TÂCHE COMMUNE	SOUS-CATÉGORIE	N° du RA	DOMAINE DE COMPÉTENCE (dérivé en partie de NICE)	COMPÉTENCES CLÉS	RÉSULTATS D'APPRENTISSAGE À l'issue du programme d'études, les apprenants devraient être en mesure de faire ce qui suit.
Déterminer la conformité et superviser le développement des mécanismes de conformité.	**Conformité**	1	Conformité : Législation, gouvernement et jurisprudence	Interpréter et appliquer les lois, règlements, politiques, normes ou procédures.	Identifier la législation, les normes, la réglementation et les politiques relatives aux exigences de cybersécurité dans les organisations.
		2	Conformité : Législation, gouvernement et jurisprudence; Confidentialité et protection de données	Interpréter et appliquer les lois, règlements, politiques, normes ou procédures.	Analyser de façon critique les politiques, les pratiques et les procédures en matière de cybersécurité relatives à la législation sur la protection de la vie privée, à l'intervention en cas de brèche, à la divulgation et au signalement.
		3	Conformité : Législation, gouvernement et jurisprudence	Donner des conseils sur les exigences de conformité en cybersécurité.	Fournir des conseils et de l'orientation sur l'application à la stratégie de cybersécurité des lois, règlements, politiques, normes ou procédures à l'intention de plusieurs publics.
		4	Conformité : Législation, gouvernement et jurisprudence	Surveiller et évaluer la conformité	Concevoir des mécanismes pour suivre la conformité organisationnelle et élaborer des protocoles correctifs cohérents.
		5	Gestion des risques, confidentialité et protection de données	Coordination des évaluations de l'impact	Élaborer des évaluations opérationnelles et des répercussions sur la vie privée.
Collaborer avec les intervenants clés pour établir un programme efficace de gestion des risques liés à la cybersécurité.	**Gestion des risques**	1	Gestion des risques, analyse des besoins, confidentialité et protection de données	Pensée et esprit critique, sens des affaires	Évaluer les menaces et les risques potentiels. Documenter les exigences en matière de gestion des risques liés à la cybersécurité à l'appui des objectifs organisationnels.
		2	Gestion des risques, gestion des relations	Communications, habiletés interpersonnelles	Collaborer avec les intervenants clés pour établir un programme efficace de gestion des risques liés à la cybersécurité.
		3	Sécurité des systèmes informatiques et des réseaux/ infrastructures organisationnelles, gestion des risques	Pensée et esprit critique, sens des affaires	Examiner les postures de sécurité organisationnelles existantes et l'exposition aux risques.

Affecter les ressources nécessaires pour garantir l'efficacité des mesures de cybersécurité.	**Affectation des ressources**	1	Sécurité des systèmes informatiques et des réseaux, infrastructure organisationnelle	Application de concepts de sécurité dans le contexte organisationnel	Intégrer la sécurité informatique et des réseaux dans un plan plus large de sécurité organisationnelle.
		2	Gestion de projet, analyse des besoins	Gestion de projet	Estimer l'expertise, le temps et l'effort nécessaires à l'exécution des tâches de sécurité.
		3	Affectation des ressources	Planification des activités et des ressources humaines	Identifier les techniques, les ressources et les processus appropriés nécessaires à l'appui des objectifs de sécurité organisationnelle.
		4	Contrôles de sécurité	Pensée critique, évaluation	Évaluer la répartition des postes et des responsabilités en matière de contrôles de sécurité dans l'ensemble de l'organisation.
Examiner et interpréter l'information liée à la cybersécurité, ainsi que les politiques et contrôles en matière de cybersécurité.	**Instruments relatifs aux politiques**	1	Élaboration de politiques	Communications, pensée critique, sens des affaires	Évaluer les politiques organisationnelles liées à la sécurité.
		2	Gestion de politiques	Communications écrites, rédaction	Fournir des recommandations au niveau du programme pour l'élaboration et la mise en œuvre de politiques de cybersécurité organisationnelles.
Tenir à jour notre portrait de la menace à la cybersécurité dans le contexte opérationnel.	**Contexte de la menace**	1	Évaluation de la menace	Analyse de la menace (haut niveau)	Dresser le portrait de la menace de cybersécurité dans le contexte opérationnel.
		2	Passation de marchés et achats, gestion de projets	Pensée critique, sens des affaires, surveillance par un tiers	Déterminer les mesures correctives appropriées pour les risques liés à la cybersécurité dans la chaîne d'approvisionnement et les risques tout au long du cycle de vie du développement de systèmes/logiciels.
		3	Évaluation de vulnérabilité	Évaluation de vulnérabilité (haut-niveau)	Surveiller les activités de gestion de vulnérabilité par rapport au risque organisationnel.

Donner des conseils sur les programmes, les politiques, les processus et les systèmes de cybersécurité.	**Direction et gestion**	1	Gestion de programme	Planification des affaires, pensée critique	Contribuer à l'élaboration et à la mise en œuvre d'améliorations du programme de cybersécurité.
		2	Évaluation du programme	Mesure du rendement et analyse des programmes	Définir les mesures et les paramètres du programme de sécurité. Communiquer les améliorations recommandées du programme à des publics multiples.
Programmer et superviser les évaluations et les audits de sécurité.	**Évaluation et audits**	1	Audit	Interprétation de l'information d'audit	Examiner les processus d'audit de la sécurité de l'information internes et externes aux fins de conformité aux lois, normes et réglementations pertinentes.
		2	Évaluation de la sécurité	Pensée critique, évaluation	Examiner les activités d'évaluation de la sécurité, de contrôle et d'autorisation.

Conception et développement

Résultats d'apprentissage

Cette catégorie de travail concerne le développement d'infrastructures, de systèmes et de logiciels sécurisés.

Il s'agit d'une branche très technique de l'emploi en cybersécurité. La majorité de ce travail est la responsabilité des ingénieurs en informatique (2147), des programmeurs informatiquestechniciens chargés de tester les systèmes d'information et des développeurs de médias interactifs (2174), des techniciens chargés de tester les systèmes d'information (2283), et des analystes et consultants en informatique (2171), en plus des postes suivants au sein de cette Norme professionnelle nationale :

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

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

Les compétences, y compris les CCH essentielles pour ces spécialisations, sont incluses dans la Norme professionnelle nationale. Les résultats d'apprentissage suivants sont le fruit d'une analyse de tous les postes de cette catégorie et sont fondamentaux pour ceux qui suivent des programmes spécialisés de cybersécurité menant à un grade, un diplôme ou un certificat. Ces programmes seraient également intéressants pour ceux qui offrent des programmes techniques appliqués menant à un grade, un diplôme ou un certificat, et dont le contenu de cybersécurité est limité ou inexistant. Les résultats d'apprentissage sont présentés dans une séquence d'enseignement suggérée.

SOUS-CATÉGORIE	Nº du RA	DOMAINE DE COMPÉTENCE (dérivé en partie de NICE)	COMPÉTENCES CLÉS	RÉSULTATS D'APPRENTISSAGE À l'issue du programme d'études, les apprenants devraient être en mesure de faire ce qui suit.
Gestion des risques	1	Gestion des risques, sensibilisation des organisations	Évaluation des risques, relations avec les clients	Évaluer les risques informatiques de l'organisation (TI et TO).
	2	Gestion des risques, analyse des besoins	Analyse des besoins	Définir les besoins opérationnels de l'organisation (TI et TO).
	3	Gestion des risques, gestion des relations	Communications, relations avec les clients, recherche	Documenter les exigences en matière de gestion des risques liés à la cybersécurité à l'appui des objectifs organisationnels.
	4	Gestion des risques, analyse des besoins	Communications, évaluation des risques, pensée critique	Fournir des conseils techniques et une expertise dans l'élaboration de politiques, d'exigences et de pratiques de gestion des risques.
	5	Gestion des risques, surveillance par un tiers	Évaluation des risques	Donner des conseils sur les aspects techniques élémentaires de la gestion des risques par des tiers et de la chaîne d'approvisionnement (TI et TO).
Évaluation de la menace et des risques	1	Gestion des risques, analyse des menaces	Analyse des menaces, pensée critique et systémique	Évaluer les menaces et les risques.
	2	Gestion des risques, analyse des menaces	Analyse des menaces, pensée critique	Repérer les menaces selon le contexte.
	3	Modélisation et simulation	Analyse des menaces, modélisation des systèmes	Modéliser les cybermenaces potentielles.
Conformité	1	Conformité : Législation, gouvernement et jurisprudence	Interprétation de documents ainsi que de normes juridiques et réglementaires, pensée critique	Examiner de façon critique les exigences de conformité pertinentes pour son contexte organisationnel.

Conseils techniques	1	Sécurité des systèmes informatiques et des réseaux	Recherche, analyse des besoins, communications	Donner des conseils sur les exigences, les politiques, les plans et les activités techniques de sécurité de base (TI et TO). Établir des concepts qui incluent la sécurité dès le départ.
	2	Gestion de projets, passation de marchés et achats	Gestion de projet, analyse des besoins	Déterminer les exigences de sécurité tout au long des phases du cycle de développement de système (CDS) et du cycle de la vie du projet.
	3	Conformité : Législation, gouvernement et jurisprudence	Interprétation de documents ainsi que de normes juridiques et réglementaires, pensée critique	Définir les exigences en matière de sécurité et de confidentialité pour les organisations.
	4	Sécurité des systèmes informatiques et des réseaux, gestion de programme	Mesure du rendement et analyse des programmes	Déterminer les mesures et les paramètres de base du programme de sécurité technique.
	5	Passation de marchés et achats	Analyse de la menace, analyse des besoins, communications	Passer en revue les exigences techniques de sécurité des activités de passation de marchés et de la chaîne d'approvisionnement, et fournir des conseils à cet effet.
	6	Résolution de problèmes	Résolution de problèmes complexes	Résoudre des problèmes dans des contextes de cybersécurité complexes, peu importe le domaine.
Conseils techniques	1	Architecture d'entreprise, sécurité des systèmes informatiques et des réseaux, gestion de programme	Pensée systémique, pensée critique, analyse des besoins, modélisation des systèmes	Donner des conseils sur l'architecture de sécurité de base et les principes d'ingénierie, à l'appui des objectifs organisationnels, y compris les coûts.
	2	Sécurité des systèmes informatiques et des réseaux, gestion de programme	Analyse des besoins, résolution de problèmes, communications	Déterminer les exigences et les contrôles de sécurité technique de base pour les données, les systèmes, les applications et les appareils dans leur contexte opérationnel (TI et TO).
	3	Cyberdéfense	Pensée critique	Appliquer les concepts de sécurité, les modèles de référence et les normes au contexte opérationnel.
	4	Architecture d'entreprise, sécurité des systèmes informatiques et des réseaux, gestion de programme	Pensée systémique et critique, résolution de problèmes	Donner des conseils sur les exigences fonctionnelles et techniques de base pour les solutions de cybersécurité.
	5	Essai et évaluation	Essai de fonctionnement du système, évaluation	Aider aux processus d'essai et d'évaluation de la sécurité.

Conseils techniques	1	Gestion des incidents	Planification, communications, relations avec les clients	Fournir des conseils techniques durant la planification et la préparation de la gestion des incidents. Fournir des conseils techniques et des recommandations sur les menaces à la cybersécurité et les mesures d'atténuation.
	2	Gestion des risques, gestion des incidents	Mesure du rendement et analyse des programmes	Fournir des conseils techniques sur l'évaluation des risques organisationnels et des dommages.
	3	Continuité des activités	Planification, communications, relations avec les clients	Planifier la continuité des activités et des interventions en cas de catastrophe.
Conseils techniques	1	Communications	Rédaction technique et commerciale	Fournir des rapports techniques sur les questions de cybersécurité.
	2	Communications, présentation	Présentation	Fournir des informations et des perspectives techniques à divers publics cibles. Présenter les résultats de l'analyse de sécurité aux intervenants.
Évaluation de la sécurité	1	Évaluation de la sécurité	Analyse, communications, pensée critique, évaluation	Examiner les activités d'évaluation de la sécurité et d'autorisation.
	2	Évaluation de la sécurité	Analyse, communications, pensée critique, évaluation	Contribuer à la confidentialité et aux exigences en matière de sécurité des données à évaluer.
	3	Essai et évaluation	Utilisation et calibrage des critères d'évaluation et des outils d'essai, pensée critique	Recueillir, analyser, vérifier et valider les données d'essai et traduire les données et les résultats d'essai en conclusions.
	4	Essai et évaluation	Évaluation des systèmes et outils utilisés, résolution de problèmes	Comparer les conceptions matérielles et logicielles existantes en matière de sécurité afin de déterminer leur adaptabilité à des situations spécifiques.
	5	Défense des réseaux informatiques	Évaluation des systèmes et outils utilisés, résolution de problèmes, communications	Évaluer l'efficacité des systèmes et des logiciels de cybersécurité. Recommander des mesures pour remédier aux menaces organisationnelles et soutenir l'atténuation des risques en fonction des résultats de l'évaluation/de l'audit.

Gestion des vulnérabilités	1	Évaluation de vulnérabilité	Pensée systémique et critique, évaluation de la menace et des risques	Participer aux activités de gestion des vulnérabilités et fournir des conseils élémentaires.
	2	Évaluation de vulnérabilité	Évaluation des risques de vulnérabilité; évaluation, utilisation et interprétation des outils d'évaluation de vulnérabilité	Mener des évaluations de vulnérabilité.
Formation	1	Formation, sensibilisation à l'organisation	Analyse des besoins en formation, méthodes de formation	Aider à l'élaboration et à la mise en œuvre d'activités de formation et de sensibilisation à la cybersécurité.

Exploitation et maintenance

Résultats d'apprentissage

Cette catégorie de travail participe à l'exploitation et au maintien de la sécurité des systèmes et des données, conformément aux spécifications de l'architecture et de la conception de la sécurité.

Toutes ces fonctions sont exercées principalement dans les métiers liés aux technologies de l'information (CNP 0213, 2147, 2174, 2171 et 2283) sur le marché du travail canadien, à l'exception de celles indiquées ci-dessous et qui se sont établies comme des métiers qui dépendent de plus en plus des systèmes connectés à l'Internet et des menaces associées :

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

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

Les compétences, y compris les compétences CCH essentielles pour ces spécialisations, sont incluses dans la Norme professionnelle nationale. Les résultats d'apprentissage suivants sont le fruit d'une analyse de tous les postes de cette catégorie; ils sont destinés à servir dans le cadre de programmes de diplomation ou de certification existants en informatique et en sécurité informatique qui appuient ces postes, ainsi que d'autres. Les résultats d'apprentissage sont placés dans l'ordre d'enseignement suggéré.

TÂCHE COMMUNE	SOUS-CATÉGORIE	N° du RA	DOMAINE DE COMPÉTENCE (dérivé en partie de NICE)	COMPÉTENCES CLÉS	RÉSULTATS D'APPRENTISSAGE À l'issue du programme d'études, les apprenants devraient être en mesure de faire ce qui suit.
Service client et soutien technique	**Service** **Client ou ligne d'aide**	1	Administration du système, gestion des incidents	Tri et hiérarchisation des priorités	Évaluer les demandes et les requêtes en niveaux de priorités pour dégager des résultats exploitables.
		2	Communications, résolution de problèmes	Communication	Fournir un processus de résolution ou d'escalade.
		3	Résolution de problèmes, administration du système	Gestion de personnel	Gérer les demandes et les requêtes des clients.
		4	Réponse aux incidents	Coordination	Contribuer à la réponse aux incidents et au plan de continuité des activités.
Administration de bases de données	**Systèmes de données**	1	Confidentialité et protection de données, gestion des politiques	Communication, examen et interprétation des politiques	Fournir des avis sur les opérations de TI, y compris la conception, la création, l'évaluation et la communication des politiques de gouvernance et de confidentialité des données.
		2	Protection et confidentialité des données, gestion des risques, gestion de l'identité	Gestion des données, classification de l'information, analyse de données	Fournir des avis sur la conception, la création et l'évaluation de systèmes (1) qui garantissent que les données inactives ou en mouvement sont cryptées, (2) qui relient les pratiques de gouvernance des données (c'est-à-dire les droits d'accès, la collecte, la conservation, etc.) aux règles de protection de la vie privée, à la conformité de l'industrie et aux exigences législatives dans les infrastructures sur place ou dans le nuage. Évaluer les actifs, les menaces, les vulnérabilités et les mesures d'atténuation des systèmes de données.
		3	Gestion des données, gestion de l'identité	Gestion des processus, analyse des données	Faire participer les analystes de système à la conception, à la création et à l'évaluation de systèmes (1) qui relient les postes et les responsabilités aux systèmes de RH pour garantir qu'un changement de poste modifie les droits d'accès automatiquement, et (2) qui documentent les données et le déroulement des opérations du système.

Gestion du savoir	**Outils de savoir** **Services du savoir**	1	Gestion du savoir	Recherche, analyse des données	Classer les résultats de l'analyse.
		2	Gestion du savoir, gestion des données	Cartographie du savoir	Modéliser des données, structurées ou non, sous forme de diagrammes qui reflètent le contexte et les besoins.
		3	Gestion du savoir, gestion des données	Planification de l'information	Participer à la conception, à la création et à l'évaluation de la documentation des systèmes et des pratiques offrant des perspectives d'exploitation et de maintenance.
		4	Gestion du savoir	Rapports, communications	Participer à la conception, à la création et à l'évaluation de rapports et d'un système de compte rendu pour accéder à l'information stockée et dérivée, et la présenter. Comprendre les heuristiques de Nielsen.
Services réseau	**Réseaux** **Pare-feu** (matériel et logiciel) **Routeurs, interrupteurs et concentrateurs** **Ponts et multiplexeurs** **Serveurs**	1	Gestion réseau	Gestion technique	Bâtir un système dont les composants matériels et logiciels réseau sont interconnectés.
		2	Gestion réseau	Gestion de projet	Organiser et hiérarchiser les exigences techniques en tâches.
		3	Gestion réseau, conception de l'infrastructure	Configuration	Définir les exigences et les contrôles de sécurité technique de base pour les systèmes de bout en bout dans différents contextes techniques (sur les lieux, infonuagique, opérations à distance, technologie opérationnelle).
		4	Évaluation des vulnérabilités, protection des systèmes et réseaux informatiques, essai et évaluation de système	Essais	Fournir des conseils élémentaires techniques et sur les systèmes pour la conception, la création et l'évaluation d'exigences, fonctionnelles ou non, et les tests de vulnérabilité.
		5	Gestion réseau, conception de l'infrastructure	Maintenance	Fournir des conseils élémentaires techniques et sur les systèmes pour la conception, la création et l'évaluation ainsi que pour les procédures de maintenance, les calendriers.

Administrateur du système	**Matériel** **Logiciel**	1	Administration du système	Installation	Choisir des applications logicielles qui répondent à des exigences définies.
		2	Administration et intégration du système, évaluation de vulnérabilité	Configuration	S'assurer que les dispositifs matériels et les logiciels restent configurés de manière optimale pour répondre aux exigences de sécurité et réduire les vulnérabilités.
		3	Administration du système, systèmes informatiques/ sécurité des réseaux	Administration	Appliquer les politiques de sécurité aux systèmes utilisés.
		4	Administration du système, résolution de problèmes	Dépannage	Résoudre les problèmes de sécurité liés au matériel/logiciel des systèmes.
		5	Administration du système, communications	Rapports	Fournir des rapports techniques sur les problèmes de systèmes.
Analyse de système	**Exigences organisationnelles** **Exigences système** **Systèmes informatiques**	1	Gestion réseau, conception de l'infrastructure, communications	Analyse technique	Traduire les spécifications techniques et non techniques en cas d'utilisation de sécurité.
		2	Gestion réseau, conception de l'infrastructure, communications	Analyse de l'information	Donner des conseils sur les exigences, les politiques, les plans et les activités de base en matière de sécurité technique et aider à les prioriser.
		3	Gestion réseau, conception de l'infrastructure, communications	Communication	Documenter les exigences techniques des systèmes adaptées au public cible. Fournir un aperçu et une perspective techniques à divers publics cibles. Présenter le résultat des analyses de système aux intervenants.
		4	Gestion réseau, gestion de projet	Gestion de projet	Identifier les tâches et les dépendances liées à la sécurité requises dans un projet. Estimer le temps et l'effort nécessaires à l'exécution des tâches.

Protection et défense

Résultats d'apprentissage

Cette catégorie de travail soutient les opérations de cybersécurité qui englobent la protection active, la détection des événements, la réponse aux incidents et la récupération des systèmes numériques organisationnels.

Bien que des personnes exercent des emplois connexes depuis des décennies, les principaux postes n'ont pas été identifiés comme des professions, mais ont plutôt été typiquement associés à des groupes professionnels : gestionnaires des systèmes informatiques (CNP 0213); analystes et consultants/consultantes en informatique (2171);
et techniciens chargés de tester les systèmes d'information (2283). Les personnes appartenant à cette catégorie de travail se concentrent donc sur l'exploitation, la maintenance et la gestion des technologies, des processus et du personnel de cybersécurité, ce qui nécessite une expérience unique et des connaissances, compétences et habiletés distinctes qui les différencient de leurs autres collègues des TI.

Protection et défense

(suite)

Voici les métiers qui aujourd'hui appuient les opérations de cybersécurité :

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

Les compétences, y compris les compétences CCH essentielles pour ces spécialisations, sont incluses dans la Norme professionnelle nationale. Les résultats d'apprentissage suivants sont le fruit d'une analyse de tous les postes de cette catégorie; ils sont destinés à appuyer les composantes éducatives initiales dans le cadre d'un grade, diplôme ou certificat spécialisé en opérations de cybersécurité. Les résultats d'apprentissage sont présentés dans une séquence d'enseignement suggérée.

TÂCHE COMMUNE	SOUS-CATÉGORIE	N° du RA	DOMAINE DE COMPÉTENCE (dérivé en partie de NICE)	COMPÉTENCES CLÉS	RÉSULTATS D'APPRENTISSAGE À l'issue du programme d'études, les apprenants devraient être en mesure de faire ce qui suit.
Surveiller, analyser et déterminer les menaces et les incidents de cybersécurité.	**Analyse de menace**	1	Opérations de sécurité	Conscience organisationnelle, évaluation des risques et de la menace, interprétation des exigences juridiques et réglementaires, communications, relations avec les clients	Diriger la planification des opérations de cybersécurité (niveau analyste).
		2	Opérations de sécurité	Analyse de menace, du trafic, pensée critique et systémique, outils d'analyse cybernétique, détection et identification des activités anormales/malveillantes	Mener des activités d'analyse des opérations élémentaires de sécurité.
		3	Analyse de menace, opérations de sécurité	Analyse de menace, pensée critique, esprit de contradiction, analyse élémentaire des logiciels malveillants et outils	Appliquer ses connaissances relatives aux auteurs de menace et sa capacité de pensée antagoniste dans le contexte organisationnel.
		4	Analyse du renseignement	Interprétation de l'information sur les menaces, recherche en cybermenace, pensée critique	Appliquer les renseignements sur les cybermenaces au risque organisationnel
		5	Gestion des risques, évaluation de vulnérabilité	Évaluation des risques, pensée critique	Fournir des conseils (niveau analyste) et contribuer aux activités d'évaluation des risques liés aux menaces et aux vulnérabilités organisationnelles. Déterminer les options d'atténuation des risques pour résoudre les problèmes potentiels de cybersécurité. Évaluer l'efficacité des contrôles de sécurité pour atténuer les risques organisationnels et remédier aux problèmes.
Installer, tester, maintenir, surveiller et gérer les systèmes et logiciels de cybersécurité.	**Systèmes et logiciels de sécurité**	1	Systèmes et logiciels de cybersécurité	Analyse de menace, pensée critique et systémique	Configurer des systems et des outils communs de cybersécurité.
		2	Systèmes et logiciels de cybersécurité	Dépannage, pensée critique, résolution de problèmes	Dépanner les systèmes et les applications de sécurité.
		3	Systèmes et logiciels de cybersécurité	Évaluation des systèmes et des outils utilisés, mesure de la performance, communications	Rendre compte de la performance des systèmes et outils de cybersécurité.

Gérer l'assistance en cas d'incident de cybersécurité.	**Gestion des incidents**	1	Gestion des incidents	Planification, pensée critique, communications, conscience organisationnelle, protocoles de gestion de crise, relations avec les clients	Conseiller sur les efforts de planification de la gestion des incidents de cybersécurité. Contribuer à la planification de la communication de crise pour les incidents de cybersécurité. Organiser des points de presse sur les incidents de cybersécurité.
		2	Gestion des incidents	Analyse des intrusions, des causes profondes et des risques, utilisation des outils et interprétation, enregistrement et rapports	Effectuer le triage. Mettre en œuvre des protocoles de réponse aux incidents.
		3	Gestion des risques, gestion des incidents	Mesure du rendement et analyse des programmes	Donner des conseils sur l'évaluation des risques organisationnels et des dommages.
		4	Enquête sur les incidents de cybersécurité	Évaluation des preuves, maintien de la chaîne de contrôle, utilisation des outils de collecte de preuves, communications	Recueillir des preuves numériques Appliquer les techniques de base de la criminalistique et enquêter sur les incidents de cybersécurité en soutien aux forces de l'ordre.
		5	Leçons apprises en matière de cybersécurité	Évaluation des systèmes et des outils utilisés, mesure de la performance, communications	Recommander des changements aux politiques et procédures de cybersécurité en réponse à un incident.
		6	PCA/PIC, récupération	Outils d'analyse, d'essai et d'évaluation, évaluation de vulnérabilité	Donner des conseils sur les activités de récupération.
Fournir des conseils techniques et des recommandations sur les menaces opérationnelles à la cybersécurité et les mesures d'atténuation.	**Conseils techniques**	1	Défense des réseaux informatiques	Évaluation des systèmes et outils utilisés, résolution de problèmes, communications	Évaluer l'efficacité des systèmes de cybersécurité et des logiciels d'exploitation et recommander des façons de faire face aux menaces organisationnelles.
		2	Cyberdéfense	Analyse de menace, pensée critique et systémique, conscience organisationnelle	Conseiller sur les menaces et les mesures d'atténuation en matière de cybersécurité.

Développer, fournir et appuyer les efforts de formation et de sensibilisation en matière de cybersécurité.	**Formation**	1	Formation, sensibilisation à l'organisation	Analyse des besoins en formation, méthodes de formation	Aider à l'identification des besoins en formation ainsi qu'à l'élaboration et à la prestation d'activités de formation et de sensibilisation à la cybersécurité.

Annexe A

Contributeurs

George Al-Koura, ADGA

Peter Aruja, ADGA

Joel Black, ADGA

David Cramb, Université Ryerson

Kevin Deveau, Centennial College

Dillon Donahue, CyberNB

Rushmi Dua Hasham, Rogers Cybersecure Catalyst, Université Ryerson

Ed Dubrovsky, Université York

Anthony Elton, Amazon Web Services (AWS)

Isabelle Hertanto, ADGA

Nicholas Johnston, Collège Sheridan

Tahmeed Khan, ADGA

Kathy Knight, Institut des métiers et de la technologie du Manitoba (MITT)

David Knox, Université d'Ottawa

Murray Lee, BulletProof

Sophia Leong, Université d'Ottawa

Heather MacLean, EC-Council Canada

Angela McAllister, Centre canadien pour la cybersécurité

Alan McCafferty, Groupe de conseil stratégique, myscg

Ron McLeod, Collège communautaire de la Nouvelle-Écosse

Karen Murkar, consultante

Jeff Musson, Dynamite Network Solutions

John Olaonipekun, ADGA

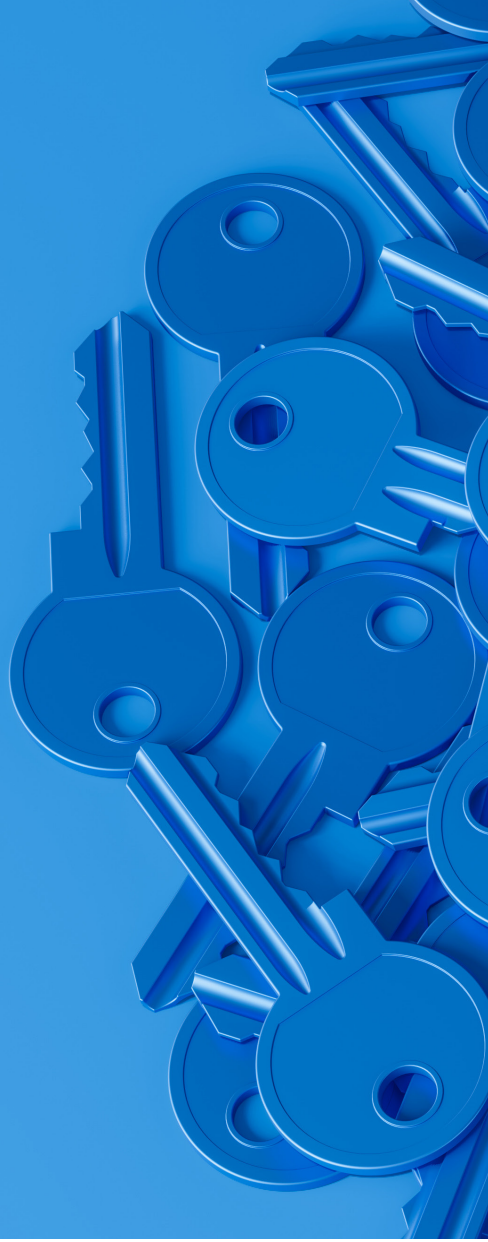
Krishna Raj Kumar, Service de cybersécurité et de protection de la vie privée du cabinet CGI dans l'Atlantique

Rob Samuel, Amazon Web Services (AWS)

Juliana Scharrer, Rogers Cybersecure Catalyst, Université Ryerson

Sumbal Syed, Collège TriOS

Ramy Taraboulsi, VeritableSoft Innovations



TECHNATION CA

Financé en partie
par le gouvernement du
Canada

Canada