Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

GUIDE SUR LES PROGRAMMES D'ÉTUDES ET LE PERFECTIONNEMENT DE LA MAIN D'ŒUVRE

GUIDE AXÉ SUR LES RÔLES À L'INTENTION DES GESTIONNAIRES RESPONSABLES DE L'EMBAUCHE, DES ÉTABLISSEMENTS D'ÉDUCATION ET DES FOURNISSEURS DE FORMATION

Version 2

Canada

AVANT-PROPOS

Le *Guide sur les programmes d'études et le perfectionnement de la main d'œuvre : Guide axé sur les rôles à l'intention des gestionnaires responsables de l'embauche, des établissements d'éducation et des fournisseurs de formation* est une publication non classifiée. Le présent guide offre une perspective fondée sur les rôles des carrières dans le domaine de la cybersécurité et présente des programmes d'études postsecondaires en cybersécurité dans deux domaines : les domaines techniques et les domaines non techniques. En tant que guide sur les programmes d'études, il ne vise pas à prescrire, mais bien à proposer un catalogue des éléments de programmes d'études de manière à établir un point de repère national en fonction duquel les établissements d'enseignement postsecondaire peuvent évaluer leurs programmes et leurs cours.

Il a été élaboré à partir de sources multiples et avec l'appui de représentants du Centre de la sécurité des télécommunications, de l'École de la fonction publique du Canada, du ministère de la Défense nationale, de Sécurité publique Canada, de la Gendarmerie royale du Canada et du Secrétariat du Conseil du Trésor du Canada.

Le présent guide reconnaît que plusieurs établissements ont déjà mis en place des programmes ou des cours qui appuient les résultats de formation ou d'éducation en cybersécurité, dont certains peuvent dépasser les directives du programme d'études. Néanmoins, une pénurie de main-d'œuvre qualifiée est prévue pour les années à venir et les petites, moyennes et grandes entreprises des secteurs public et privé continueront à faire face à des défis cybernétiques. Le présent guide est distinct en ce sens qu'il met l'accent sur les éléments du programme qui préparent les diplômés à jouer des rôles dans un contexte de sécurité organisationnelle commun.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1.	Ébauche de l'examen public du projet.	31 janvier 2019
2.	Réorganisation de l'information, validation des rôles et ajout de nouveaux rôles, ajout de la liste des programmes offerts actuellement et nouveaux diagrammes.	17 juin 2020

Table des matières

1 INTRODUCTION

La demande de professionnels et de spécialistes qualifiés en cybersécurité continue de croître. Selon une prévision, il manquera 3,5 millions de professionnels de la cybersécurité dans le monde d'ici 2021 [1]. La nature dynamique du domaine de la cybersécurité s'est par la suite transformée et ne dépend plus uniquement des disciplines techniques/informatiques, mais exige maintenant l'intégration de domaines d'étude non techniques, notamment ceux des affaires, du droit, de la politique et de l'éthique, pour faire face aux changements croissants dans le domaine.

Pour perfectionner les talents requis, plusieurs établissements d'enseignement ont mis en place des programmes ou des trajectoires d'études dans le cadre des programmes existants afin d'appuyer les résultats de formation ou d'éducation en cybersécurité. Qu'il s'agisse d'élaborer des programmes complètement nouveaux, de définir de nouvelles concentrations dans les programmes existants ou d'enrichir le contenu des cours existants, les établissements d'enseignement auront peut-être besoin d'une orientation en matière de programmes fondée sur une vue d'ensemble du domaine de la cybersécurité, les besoins particuliers de la discipline et la relation entre les programmes d'études et les cadres régissant les effectifs de la cybersécurité [2].

En raison de la nature très dynamique de la cybersécurité, le présent guide sera revu régulièrement afin de tenir compte des exigences en matière d'études postsecondaires et de formation pour les rôles et les spécialisations de la main-d'œuvre du secteur de la cybersécurité. Les suggestions de modification peuvent être soumises par courriel à contact@cyber.gc.ca.

1.1 RÔLE DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a été officiellement mis sur pied en octobre 2018. L'équipe Relations et collaboration avec le milieu universitaire du Centre pour la cybersécurité travaille de concert avec les universités, les collèges, les associations et les comités ministériels à vocation éducative, ainsi que les pédagogues du secteur privé afin d'accroître les capacités et le bassin de candidats talentueux en cybersécurité du Canada. L'équipe collabore aussi avec les pédagogues afin d'améliorer la compréhension de la collectivité en matière de cybersécurité. Sa mission est de s'assurer que le Canada est un chef de file mondial en matière de cybersécurité en renforçant l'éducation dans ce domaine.

1.2 OBJECTIF

Le présent guide sur les programmes études vise un double objectif :

- fournir une perspective axée sur les rôles des carrières en cybersécurité :
    - pour aider les conseillers en orientation professionnelle à préparer les étudiants à des rôles techniques et non techniques dans le domaine de la cybersécurité;
    - pour aider les étudiants à comprendre les différents types de professions disponibles dans le domaine de la cybersécurité;
    - pour aider les employeurs à recruter des professionnels qualifiés;
- élaborer une orientation pédagogique complète en cybersécurité qui appuiera l'élaboration de programmes futurs et les efforts connexes au niveau postsecondaire.

1.3 PUBLIC

Le présent guide s'adresse principalement aux établissements d'enseignement qui désirent élaborer des programmes d'études en cybersécurité, définir de nouvelles concentrations en cybersécurité dans les programmes existants ou enrichir les programmes existants pour y intégrer du contenu relatif à la cybersécurité.

Les publics secondaires comprennent les suivants :

- les étudiants et les professionnels potentiels qui s'intéressent au domaine de la cybersécurité et qui souhaitent comprendre les tâches à accomplir et les exigences en matière de compétence, y compris les connaissances et les compétences attendues dans des rôles organisationnels techniques et non techniques;
- les membres de l'industrie de la cybersécurité qui peuvent contribuer à l'élaboration de programmes de cybersécurité dans les établissements d'enseignement, puis recruter et embaucher des étudiants dans le cadre de ces programmes;
- les associations ou organisations professionnelles qui ont un rôle à jouer pour appuyer le perfectionnement de la main-d'œuvre canadienne;
- les décideurs qui souhaitent obtenir des conseils sur les compétences et les capacités humaines à l'appui des exigences en matière de sécurité;
- les membres du milieu de l'éducation de la maternelle à la 12^{e} année qui préparent les étudiants à entreprendre des études postsecondaires en cybersécurité.

1.4 COMMENT UTILISER CE GUIDE

Ce guide encadre le programme d'études (ce qui est enseigné) ainsi que les méthodes (la façon dont il est enseigné), et il est présenté en quatre sections pour donner une perspective générale des rôles liés à la cybersécurité au sein d'une organisation :

1. Gouverner et soutenir;
2. Protéger et défendre;
3. Exploiter et maintenir;
4. Concevoir et développer.

Chaque section présente des suggestions de programmes d'études axées sur les rôles, passant des exigences de base aux rôles spécialisés. Chaque sujet du programme est divisé en composantes qui permettent de déterminer plus en détail les connaissances et les compétences requises. Chaque sujet peut être intégré au programme d'études existant, selon les besoins des personnes apprenantes, ou utilisé comme élément de programme autonome à l'appui de programmes nouveaux ou existants, ou de cours individuels.

Les établissements d'enseignement peuvent utiliser ce guide pour développer davantage les programmes de cybersécurité ou pour augmenter les programmes existants afin d'y intégrer du contenu sur la cybersécurité. Il est certain que les membres de l'industrie peuvent utiliser ce guide pour aider les établissements d'enseignement à élaborer des programmes de cybersécurité et, plus tard, recruter et embaucher des diplômés de ces programmes. Les étudiants et les conseillers en orientation professionnelle peuvent également utiliser ce guide pour comprendre les tâches fonctionnelles ainsi que les exigences en matière d'études, d'expérience et de compétences requises dans les rôles techniques et non techniques en cybersécurité.

Il n'est pas proposé que ces rôles liés à la cybersécurité correspondent à des emplois ou à des domaines de responsabilité personnelle. Les sections ont pour but de fournir une orientation pédagogique aux établissements

d'enseignement, aux conseillers en orientation professionnelle et aux étudiants, entre autres, afin de préparer les étudiants et les professionnels à des rôles techniques et non techniques en fonction d'une compréhension globale du paysage de la cybersécurité.

Après examen, les nouvelles versions de ce guide approfondiront et incluront des rôles nouveaux ou de rechange en matière de cybersécurité qui ont une incidence sur les industries, y compris, notamment, celles de l'énergie, de la santé, du droit et de la fabrication, à mesure qu'elles deviendront disponibles.

Pour obtenir des interprétations supplémentaires ou poser des questions sur la façon d'utiliser ce guide, communiquez par courriel à contact@cyber.gc.ca.

1.5 SOURCE

Le présent guide s'appuie sur les travaux antérieurs en matière d'éducation, de formation et de perfectionnement de la main-d'œuvre en cybersécurité. En plus des sources énumérées à la fin du présent guide dans la section Documents de référence, les principales sources utilisées pour l'élaboration du présent guide sont les suivantes :

- US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF);
- Requirements of the US National Security Agency and the US Department of Homeland Security National Centers of Academic Excellence in Cyber Defence and Cyber Operations;
- Global Information Technology (IT) Skills Framework for the Information Age (SFIA);
- NATO Cybersecurity: A Generic Reference Curriculum;
- Services professionnels en informatique centrés sur les tâches de Services publics et Approvisionnement Canada – Besoins en matière de services;
- Plans d'apprentissage du Carrefour de l'apprentissage du Centre canadien pour la cybersécurité.

1.6 CONTRIBUTION AU GUIDE

Le Centre canadien pour la cybersécurité reçoit régulièrement des demandes de renseignements sur les possibilités d'éducation et de formation en cybersécurité. Plusieurs établissements d'enseignement ont mis en place des programmes ou parcours d'études dans le cadre de programmes existants qui peuvent servir d'exemples ou de modèles pour l'ensemble de la collectivité. Si un établissement ou un organisme estime offrir un programme ou un cours qui devrait être considéré comme un exemple ou un modèle, veuillez le soumettre par courriel à contact@cyber.gc.ca.

2 DISCIPLINE EN MATIÈRE DE CYBERSÉCURITÉ

Le gouvernement du Canada définit la cybersécurité comme « la protection de l'information numérique et de l'infrastructure sur laquelle elle repose [3] ». La cybersécurité est principalement une discipline informatique qui fait appel à la technologie, à des personnes, à de l'information et à des processus pour permettre des opérations assurées qui protègent la confidentialité, l'intégrité et la disponibilité de l'information contre les menaces délibérées ou accidentelles à la cybersécurité [2].

Cinq disciplines primaires basées sur l'informatique sont reconnues comme le fondement de la cybersécurité :

- Génie informatique
- Informatique
- Systèmes d'information
- Technologies de l'information
- Génie logiciel

La cybersécurité est devenue une discipline à part entière essentielle avec l'évolution des technologies de l'information et de la communication (TIC). Les progrès technologiques ont modifié la façon dont les gens communiquent et échangent de l'information par voie électronique, ce qui pose des défis pour la sécurité de cette information. La menace croissante des cyberattaques a sensibilisé les gouvernements et les industries au besoin de protéger et de défendre les systèmes essentiels. Malgré la petite taille de son marché, le Canada figurait au troisième rang des pays les plus exposés aux cyberattaques en 2018 [4]. En raison de la dépendance croissante de la société à l'égard des réseaux et des systèmes informatiques, il n'est pas surprenant que la cybersécurité devienne une discipline reconnaissable avec une étendue et une profondeur de contenu qui englobe de multiples domaines dans l'écosystème informatique.

Bien que seul un sous-ensemble d'entreprises participe directement à l'industrie des TIC en produisant ou en vendant des solutions de TIC qui protègent contre les cybermenaces, ou en construisant ou en exploitant une infrastructure TI, dans les faits, toutes les entreprises utilisent les TIC pour offrir leurs propres biens et services sur le marché et contribuent au développement de l'industrie des TIC par leur expérience et leurs innovations. Les industries canadiennes créent un écheveau de relations qui se recoupent souvent, mais qui sont appuyées par des solutions technologiques qui communiquent entre elles en tant que réseau. Ainsi, la cybersécurité devient plus pertinente pour protéger les systèmes informatiques correspondants dans les industries canadiennes. Ces industries comprennent les dix principales infrastructures essentielles du Canada :

- Santé – une cible de premier plan pour les cyberattaques, car l'industrie détient une grande quantité de renseignements de nature délicate (p. ex. des dossiers électroniques et des renseignements sur les patients) et comprend des dispositifs d'implants médicaux comme des stimulateurs cardiaques exploitables;
- Alimentation – une industrie vulnérable aux menaces croissantes de cyberattaques, susceptibles de porter atteinte à la production et à la salubrité des aliments et d'entraîner des dommages à l'environnement et des pertes financières;
- Finances – une cible idéale pour les cyberattaques, car l'industrie conserve des renseignements précieux (p. ex. l'identité des clients, des renseignements sur les comptes bancaires, des actifs financiers et la propriété intellectuelle);
- Eau – une industrie vulnérable aux menaces croissantes de cyberattaques susceptibles de compromettre l'approvisionnement efficace en eau renouvelable et les installations de collecte et de traitement des eaux usées;

- Technologies de l'information et des communications – une cible de premier plan des cyberattaques, car l'industrie maintient une quantité importante de renseignements de nature délicate (p. ex. les transactions de détail en ligne, les messages électroniques, les activités de navigation sur le Web, les plateformes de médias sociaux et les renseignements personnels des utilisateurs);
- Sécurité – une industrie vulnérable aux menaces croissantes de cyberattaques contre les équipes d'intervention d'urgence, les organismes d'application de la loi, les logiciels de gestion des communications des centres d'appels, les systèmes de caméras de télévision en circuit fermé, les systèmes de réponse vocale interactive et les alertes d'urgence;
- Énergie et services publics – une cible idéale pour les cyberattaques contre les systèmes de contrôle industriel (SCI) et les systèmes d'acquisition et de contrôle des données (SCADA) déployées dans le but d'accéder à de grandes quantités de données et de causer des dommages physiques à l'infrastructure réseau;
- Fabrication – une industrie de plus en plus vulnérable aux attaques visant la chaîne d'approvisionnement qui peuvent avoir une incidence sur la production et la distribution de biens et de services. Les perturbations du secteur de la fabrication peuvent avoir pour conséquence des produits défectueux, des interruptions de production, des dommages physiques et la mise en danger de vies humaines;
- Gouvernement – une cible de premier plan pour les cyberattaques contre des entités gouvernementales aux échelles fédérale, provinciale/territoriale et municipale, et plus récemment contre des institutions démocratiques, pour avoir accès à d'immenses quantités de renseignements de nature privée et délicate (p. ex. des renseignements personnels, des déclarations de revenus et des dossiers gouvernementaux);
- Transport – une industrie de plus en plus vulnérable aux cyberattaques visant le transport ferroviaire de marchandises et de passagers, les systèmes d'aviation civile et de transport de marchandises et le transport terrestre. De plus, l'industrie du transport détient des renseignements précieux et de nature délicate, comme des dates de naissance et des numéros de passeport.

Il est donc important de mettre en évidence le domaine croissant de la cybersécurité pour répondre à la demande de professionnels dans un éventail de rôles afin d'assurer la sécurité des réseaux et des systèmes informatiques canadiens [5].

2.1 CYBERSÉCURITÉ : UN DOMAINE INTERDISCIPLINAIRE

Bien que la cybersécurité soit principalement une discipline informatique, où la majorité des programmes d'éducation et de formation est axée sur les aspects techniques, le domaine a évolué pour devenir interdisciplinaire et comprend des aspects liés à différentes disciplines comme celles des affaires, du droit, des politiques, des facteurs humains, de l'éthique et de la gestion des risques [2]. La cybersécurité comprend non seulement des aspects techniques, mais aussi des aspects non techniques et, plus important encore, elle doit répondre aux préoccupations commerciales des gouvernements et des industries. Les organisations ont de plus en plus besoin de professionnels qui possèdent les compétences nécessaires pour gérer les politiques, les procédures et les pratiques en matière de sécurité de l'information ainsi que des compétences en gestion et en communication [5]. La figure 1 illustre le lien entre les dimensions techniques et opérationnelles de la cybersécurité, qui, ensemble, sont essentielles au développement d'une culture organisationnelle qui permettra de repérer et de contrer rapidement les menaces délibérées ou accidentelles à la cybersécurité.

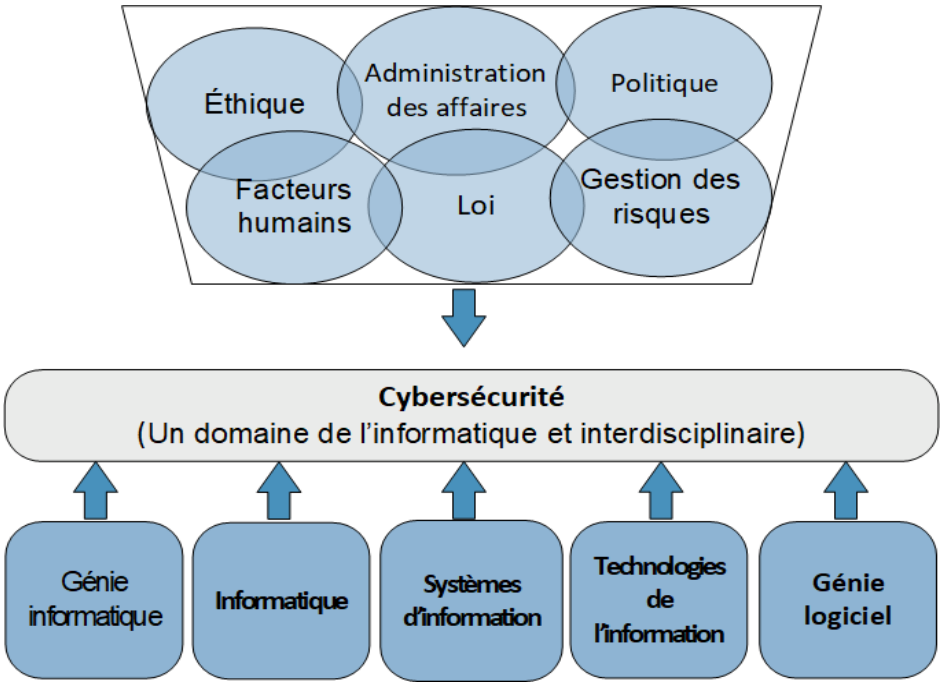

Figure 1: Structure de la discipline de la cybersécurité

La cybersécurité en tant que discipline à part entière est toujours en développement. Sous l'impulsion de la demande de main-d'œuvre, plusieurs établissements d'enseignement ont introduit des programmes d'études ou des cours de formation dans les programmes existants. Ainsi, les programmes universitaires en cybersécurité doivent offrir un programme qui comprend les caractéristiques suivantes :

- les aspects des principes fondamentaux tant informatiques que commerciaux;
- les concepts largement applicables dans un vaste éventail de domaines liés à la cybersécurité;
- un ensemble de connaissances regroupant des connaissances et des compétences essentielles en cybersécurité, y compris les neuf compétences essentielles requises, quel que soit l'objectif du programme;
- une relation directe avec l'éventail des disciplines qui répondent aux exigences de l'effectif;
- un accent mis sur la conduite éthique et les responsabilités professionnelles associées au domaine de la cybersécurité. [5]

Le présent guide vise à aider les établissements d'enseignement à élaborer des programmes et des cours sur la cybersécurité qui répondent à chacun de ces critères.

2.2 TECHNOLOGIES ÉMERGENTES

Le domaine de la cybersécurité continue d'évoluer à mesure que les industries produisent plus de données et d'information qu'auparavant. Les applications des technologies émergentes dans les industries, y compris l'intelligence artificielle (IA), la technologie de la chaîne de blocs, l'informatique en nuage, l'Internet des objets (IdO) et l'informatique quantique ont permis de connecter davantage d'appareils et de systèmes dans un réseau, favorisant un meilleur contrôle et un meilleur rendement des processus. Toutefois, ces technologies augmentent également le risque de devenir la cible d'une cyberattaque. L'attaque au rançongiciel Wannacry en 2017 est un exemple frappant où des entreprises et des particuliers de plus de 150 pays ont été touchés par une vulnérabilité exploitée dans les systèmes Windows de Microsoft [6].

Les possibilités d'innover pour défendre et protéger les technologies émergentes contre les cybermenaces continuent de se multiplier et, par conséquent, de nouveaux types de connaissances et de compétences dans des domaines comme la science et l'analyse des données créent de nouveaux rôles en matière de cybersécurité sur le marché du travail.

Ce guide vise à élargir et à inclure de nouveaux rôles en matière de cybersécurité alors que les tendances technologiques futures ouvrent la voie à l'avenir.

3 CADRE AXÉ SUR LES RÔLES

Le présent guide a été structuré de manière à fournir une perspective axée sur les rôles en fonction des besoins et des résultats d'apprentissage attendus du programme d'études en cybersécurité, de manière à pouvoir remplir des rôles organisationnels techniques et non techniques précis. Dans la figure 2 ci-dessus, le modèle axé sur les rôles catégorise les rôles de l'effectif de cybersécurité en quatre fonctions principales fondées sur les connaissances et les compétences souhaitées sans négliger les tâches adjacentes et contributives.

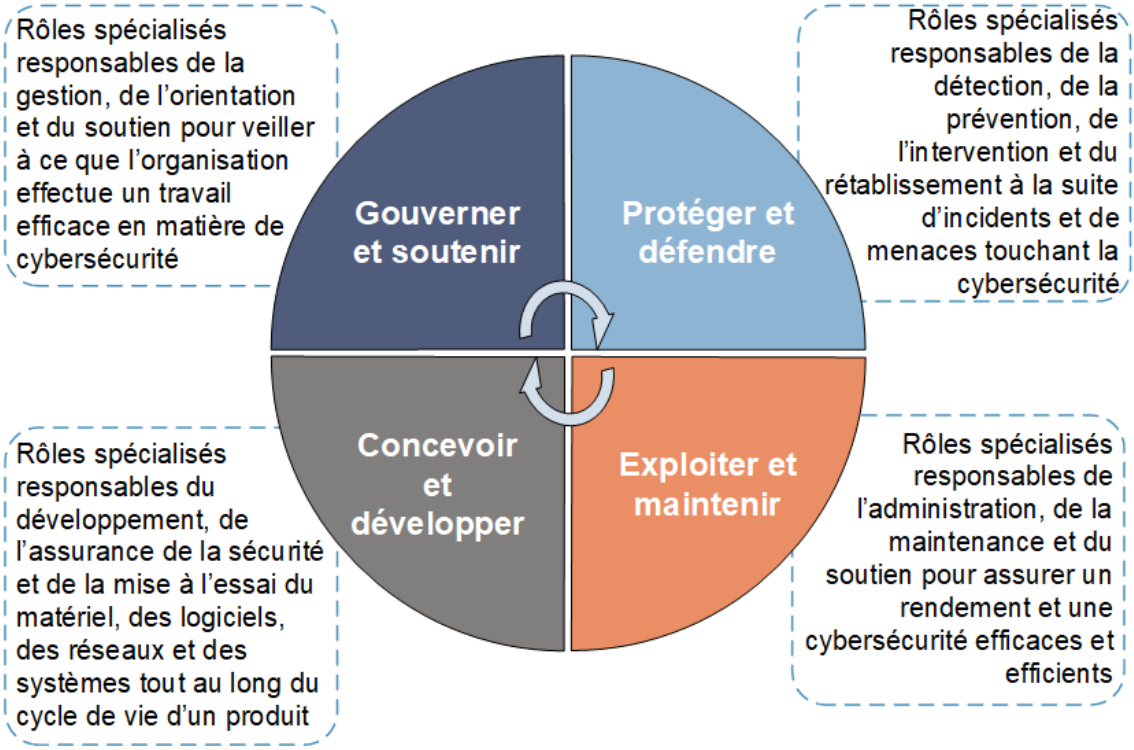

Figure 2 : Rôles et spécialisations en matière de cybersécurité

Étant donné que la cybersécurité est un domaine d'étude interdisciplinaire, les disciplines axées sur l'informatique et les affaires font partie de l'objectif de ce guide, qui vise à fournir une compréhension plus complète du domaine de la main-d'œuvre en cybersécurité. La majorité des rôles non techniques liés à la cybersécurité sont regroupés sous la fonction Gouverner et soutenir, car les postes concernent principalement la prise de décisions et la gouvernance. Les rôles et les spécialisations de la main-d'œuvre technique sont regroupés sous les trois autres fonctions, car il s'agit davantage de professions axées sur l'informatique. Ces fonctions principales sont orientées par un niveau approprié de leadership et s'étendent à des spécialisations qui exigent souvent une formation et une expertise supplémentaires axées sur les tâches dans le domaine de travail pour que la personne qui les exerce devienne compétente. Certains de ces rôles techniques et non techniques, cependant, peuvent chevaucher d'autres rôles au sein d'autres fonctions, particulièrement lorsque des compétences fonctionnelles clés sont requises. Les personnes d'autres domaines qui cumulent de l'expérience peuvent occuper ces postes.

Les personnes qui connaissent bien le Cybersecurity Workforce Framework (CWF) du National Initiative on Cybersecurity Education (NICE) remarqueront qu'il y a de nombreux points communs dans les tâches, les connaissances et les compétences spécialisées. Le présent guide se limite aux seuls éléments de cybersécurité, sans faire référence à d'autres programmes d'études techniques et non techniques communs. De plus, le présent guide propose des compétences communes qui devraient être incluses dans le perfectionnement de praticiens de la cybersécurité afin d'appuyer les exigences de sécurité de l'organisation.

3.1 RÔLES DES EFFECTIFS EN CYBERSÉCURITÉ

3.1.1 GOUVERNER ET SOUTENIR

Les rôles des effectifs de la cybersécurité au sein de la fonction Gouverner et soutenir (tableau 1) sont responsables d'assurer la gestion, l'orientation et le soutien nécessaires pour qu'une organisation déploie des initiatives efficaces en matière de cybersécurité. Les rôles s'adressent à des effectifs du niveau d'entrée, du niveau intermédiaire et du niveau avancé et exigent ainsi souvent beaucoup d'études, de formation et d'expérience de travail. Chacun des rôles de l'effectif est expliqué plus en détail dans les tableaux de la section **Gouverner et soutenir**.

Gouverner	Conseiller juridique en cybersécurité Analyste des politiques Agent à la protection des renseignements personnels Analyste des risques Planificateur stratégique
Soutenir	Analyste des activités Communications Planificateur de la reprise après sinistre Analyste de l'approvisionnement
Gérer	Dirigeant principal de la sécurité de l'information Gestionnaire de la cybersécurité Gestionnaires de la sécurité des systèmes d'information Gestionnaire de projet Responsable de la chaîne d'approvisionnement

Tableau 1 : Rôles de gouvernance et de soutien

3.1.2 PROTÉGER ET DÉFENDRE

Les rôles des effectifs de la cybersécurité au sein de la fonction Protéger et défendre (tableau 2) sont responsables de la détection, de la prévention, de l'intervention et du rétablissement en cas d'incident et de menaces touchant la cybersécurité. Les rôles s'adressent à des effectifs du niveau d'entrée, du niveau intermédiaire et du niveau avancé et exigent ainsi souvent beaucoup d'études, de formation et d'expérience de travail. Chacun des rôles de l'effectif est expliqué plus en détail dans les tableaux de la section **Protéger et défendre**.

Cyberdéfense	Analyste en cybersécurité Analyste de la sécurité des systèmes de contrôle industriel Analyste de la sécurité de l'information
Évaluation des vulnérabilités	Analyste de l'évaluation des vulnérabilités Testeur de pénétration
Intervention en cas d'incident	Intervenant/responsable en cas d'incident de cybersécurité
Criminalistique numérique	Analyste en criminalistique numérique

Tableau 2 : Rôles de protection et de défense

3.1.3 EXPLOITER ET MAINTENIR

Les rôles des effectifs en cybersécurité au sein de la fonction Exploiter et maintenir (tableau 3) sont responsables de l'administration, de la maintenance et du soutien pour assurer un rendement et une cybersécurité efficaces et efficients. Les rôles s'adressent à des effectifs du niveau d'entrée, du niveau intermédiaire et du niveau avancé et exigent ainsi souvent beaucoup d'études, de formation et d'expérience de travail. Chacun des rôles de l'effectif est expliqué plus en détail dans les tableaux de la section **Exploiter et maintenir**.

Systèmes et réseaux	Opérateur/spécialiste de la sécurité des réseaux Administrateur de systèmes
Données	Cryptographe/cryptanalyste
Soutien technique	Spécialiste du soutien technique

Tableau 3 : Rôles liés à l'exploitation et au maintien

3.1.4 CONCEVOIR ET DÉVELOPPER

Les rôles des effectifs de la cybersécurité au sein de la fonction Concevoir et développer (tableau 4) sont responsables du développement, de la sécurité, de la mise à l'essai et de l'intégration du matériel, des logiciels et des systèmes tout au long du cycle de vie d'un produit. Les rôles s'adressent à des effectifs du niveau d'entrée, du niveau intermédiaire et du niveau avancé et exigent ainsi souvent beaucoup d'études, de formation et d'expérience de travail. Chacun des rôles de l'effectif est expliqué plus en détail dans les tableaux de la section **Concevoir et développer**.

Architecture et génie	Ingénieur des infrastructures essentielles Analyste des exigences Architecte de la sécurité Ingénieur de la sécurité
Recherche et développement, mise à l'essai et évaluation	Chercheur en cybersécurité Testeur et évaluateur de la sécurité Analyste de l'intégrité de la chaîne d'approvisionnement
Développement de systèmes et de logiciels	Développeur d'applications Développeur en sécurité des systèmes d'information Développeur de logiciels sécurisés

Tableau 4 : Rôles liés à la conception et à la construction

3.2 SUJETS DU PROGRAMME DE BASE

Le programme d'études pour les rôles de spécialistes techniques suppose que les personnes ont reçu une formation générale technique, ont suivi des séances de formation techniques et/ou cumulent de l'expérience dans un domaine des TI ou de la cybersécurité et que, par conséquent, elles satisfont aux exigences relatives aux connaissances fondamentales des réseaux et des systèmes/logiciels TI.

Les personnes qui ont reçu une formation technique limitée ou n'ont aucune formation technique devraient avoir la possibilité d'acquérir des connaissances de base des sujets suivants :

- Analyse de données;
- Création de scripts ou programmation de base;
- Cyberdéfense;
- Cybermenaces;
- Principes fondamentaux de la conception de la sécurité;
- Cryptographie;
- Composants des systèmes TI;
- Concepts de mise en réseau;
- Administration de système;
- Approches et modèles de sécurité;
- Cadres de gestion de la sécurité;
- Gestion des vulnérabilités;
- Protocoles de communication, protocoles de sécurité Internet, normes de répertoire;
- Technologies de l'informatique en nuage et de la virtualisation;
- Architecture de réseau et modèles d'architecture d'entreprise;
- Cycle de développement des systèmes et/ou des logiciels, processus de développement des logiciels.

En règle générale, une connaissance de base des éléments suivants est exigée de tous les praticiens techniques et non techniques. La profondeur de compréhension variera selon les rôles au sein des entreprises ou des organisations :

- Contexte de la cybermenace (y compris les classes d'attaque [active, passive, interne]); le type de cybermenace; le type d'auteurs de cybermenace et leurs tactiques, techniques et procédures (TTP);
- Aspects juridiques, politiques et éthiques ainsi que ceux liés à la conformité en matière de cybersécurité et de protection des renseignements personnels;
- Processus de gestion des incidents de cybersécurité;
- Gestion des incidents de cybersécurité – intervention en cas d'incident et atténuation;
- Processus de cybersécurité, technologies, tendances et enjeux émergents;
- Sources d'expertise et ressources en cybersécurité;
- Continuité des activités et reprise après sinistre;
- Recherche, analyse et production de rapports.

3.3 STRUCTURE DES COMPOSANTES DU PROGRAMME AXÉ SUR LES RÔLES

Chacune des composantes suggérées du programme en cybersécurité offre ce qui suit :

- Titre basé sur le rôle;
- Description de travail de base;
- Principales tâches liées à la cybersécurité;
- Études, formation et expérience de travail fréquemment demandées;
- Exigences primaires en matière de formation – résultats d'apprentissage;
- Compétences clés.

Les exigences relatives à des rôles précis sont indiquées dans les tableaux de la section suivante.

4 GOUVERNER ET SOUTENIR

4.1 CONSEILLER JURIDIQUE EN CYBERSÉCURITÉ

Description de travail de base

- Formuler des conseils et des recommandations juridiques sur des sujets pertinents liés à la cybersécurité.

Principales tâches liées à la cybersécurité

- Défendre la position officielle de l'organisation dans les procédures juridiques et législatives;
- Interpréter et appliquer des lois, des règlements, des politiques, des normes ou des procédures par rapport à des questions précises;
- Évaluer l'efficacité des lois, des règlements, des politiques, des normes ou des procédures;
- Résoudre les conflits dans les lois, les règlements, les politiques, les normes ou les procédures;
- Maintenir une connaissance pratique des questions constitutionnelles qui se posent dans les lois, règlements, politiques, normes, procédures ou autres publications pertinentes;
- Encadrer les procédures judiciaires afin de bien cerner les infractions présumées à la loi, aux règlements ou aux politiques;
- Effectuer des recherches et des analyses sur diverses questions juridiques de l'organisation à l'aide de sources multiples;
- Fournir des analyses et des décisions juridiques au personnel de la conformité, à la direction et aux agents de la protection des renseignements personnels, concernant entre autres la conformité aux lois, aux règlements et aux politiques en matière de cybersécurité;
- Prêter conseils et orientation sur les lois, règlements, politiques, normes ou procédures à la direction, au personnel ou aux clients;
- Surveiller et évaluer l'incidence potentielle des technologies émergentes sur les lois, les règlements, les politiques, les normes ou les procédures;
- Évaluer l'incidence des modifications apportées aux lois, aux règlements, aux politiques, aux normes ou aux procédures;
- Mettre en œuvre des lois, des règlements, des politiques, des normes ou des procédures nouveaux ou révisés;
- Préparer des rapports juridiques, des notes d'information et d'autres documents pertinents.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires en droit et permis d'exercice provincial. Une maîtrise est préférable;
- Attestations constituant un atout : Computing Technology Industry Association (CompTIA); Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Il est préférable d'avoir reçu une formation et de cumuler de l'expérience en droit et en cybersécurité : de deux à cinq ans d'expérience au niveau d'entrée; de cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Éthique, lois et règlements nationaux et internationaux en matière de cybersécurité et de protection des renseignements personnels;

- Politiques, procédures et règlements en matière de sécurité de l'information;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Connaissances techniques pour comprendre la sécurité et l'intégrité des données, les exigences de sécurité, ainsi que la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- Répercussions particulières des lacunes en matière de cybersécurité et des atteintes à la cybersécurité;
- Principes, politiques et procédures de collecte de renseignements, y compris les autorisations et restrictions légales;
- Outils d'enquête, rapports, lois et règlements;
- Plans, ordres, politiques et règles d'engagement sur les plans opérationnels ou militaires;
- Déclarations de confidentialité fondée sur les lois et les règlements.

Principales compétences

- Recherche et analyse, souci du détail, résolution de problèmes, relations interpersonnelles, négociation et communication.

4.2 ANALYSTE DES POLITIQUES

Description de travail de base

- Élaborer et maintenir des politiques de cybersécurité pour soutenir et harmoniser les initiatives de cybersécurité de l'organisation et appuyer la conformité réglementaire.

Principales tâches liées à la cybersécurité

- Élaborer et mettre en œuvre des politiques et des lignes directrices en matière de cybersécurité;
- Étudier et analyser les politiques, les lignes directrices et les exigences de l'organisation en matière de cybersécurité;
- Évaluer les besoins en matière de politiques et collaborer avec la direction et le personnel pour élaborer des politiques régissant les activités de cybersécurité;
- Examiner les politiques et les lignes directrices existantes et proposées avec la direction;
- Préparer et publier des politiques de cybersécurité;
- Interpréter et appliquer les lois et les documents d'application de la réglementation applicables à la politique de cybersécurité;
- Surveiller l'application des politiques et des lignes directrices en matière de cybersécurité;
- Établir et maintenir des voies de communication avec la direction et le personnel sur les politiques existantes et proposées, et communiquer tout changement de politique;
- Prêter conseils à la direction et au personnel;
- Veiller à ce que les politiques et les lignes directrices en matière de cybersécurité soient prises en compte dans la mission et les objectifs de l'organisation.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine pertinent lié à la cybersécurité (p. ex. administration des affaires, économie, droit, sciences politiques, sciences sociales ou l'équivalent);
- Formation et expérience antérieure en analyse de politiques/élaboration de politiques – un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé.
- Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité et ne pas avoir d'expérience dans le domaine de travail. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Tendances technologiques et risques pour la sécurité ainsi que leur incidence potentielle sur les politiques de cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité;
- Mise à contribution des pratiques exemplaires et des leçons apprises des organisations externes et des établissements d'enseignement en mettant l'accent sur la cybersécurité;
- Détection des lacunes dans les politiques de cybersécurité;
- Élaboration, rédaction et communication des politiques de cybersécurité à l'appui des activités organisationnelles.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communication.

4.3 AGENT À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Description de travail de base

- Élaborer, mettre en œuvre et administrer tous les aspects du programme de conformité de la protection des renseignements personnels de l'organisation et prendre en charge la protection des renseignements personnels et confidentiels.

Principales tâches liées à la cybersécurité

- 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;
- Prêter conseils et 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;
- Signaler les atteintes à la sécurité à la direction et aux autorités compétentes;
- Élaborer et fournir du matériel de formation et superviser des activités de sensibilisation sur la protection des renseignements personnels.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine pertinent lié à la cybersécurité (p. ex. administration des affaires, droit, sciences politiques, sciences sociales ou l'équivalent);

- Attestations constituant un atout : International Association of Privacy Professionals (IAPP);
- Formation antérieure et expérience en analyse de politiques – 2 à 3 ans d'expérience au niveau d'entrée. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Lois, règlements, politiques et procédures nationaux et internationaux;
- Politiques, procédures et règlements en matière de sécurité de l'information;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Connaissances techniques pour comprendre la sécurité et l'intégrité des données, les exigences de sécurité, ainsi que la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- 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 (EFVP);
- Déclarations de confidentialité fondées sur les lois et les règlements.

Principales compétences

- Analyse, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

4.4 ANALYSTE DES RISQUES

Description de travail de base

- Évaluer et gérer les risques liés à la sécurité de l'information et à la cybersécurité, et veiller à ce que les risques et les contrôles soient évalués avec exactitude, objectivité et indépendance;
- Mener des recherches, analyser de l'information, préparer des rapports et des plans pour résoudre les problèmes organisationnels liés à la cybersécurité à des niveaux acceptables.

Principales tâches liées à la cybersécurité

- Enquêter sur les risques et les exceptions et en faire rapport régulièrement à la direction, et formuler des plans d'action pour y remédier;
- Effectuer des recherches et élaborer des modèles pour analyser, expliquer et prévoir les tendances, et concevoir des méthodes de collecte et d'analyse des données;
- Déterminer les profils de risque de divers projets et stratégies par rapport à la cybersécurité;
- Évaluer les risques liés à la mise en œuvre d'outils et de technologies de cybersécurité au sein de l'organisation;
- Élaborer et tenir à jour des évaluations des risques et des répercussions pour divers projets et stratégies;
- Tenir à jour le registre des risques organisationnels et en faire rapport périodiquement à la direction.
- Définir, élaborer et gérer des politiques, des procédures et des lignes directrices sur les exigences en matière de cybersécurité;
- Assurer la conformité aux politiques, aux lois, aux règlements et aux pratiques en matière de cybersécurité;
- Élaborer ou contribuer à l'examen des projets et des stratégies mis en œuvre pour cerner les risques;
- Intégrer le risque lié à la cybersécurité aux autres activités organisationnelles de gestion des risques.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. sécurité de l'information, gestion de l'information, gestion des risques liés aux TI ou l'équivalent);
- Attestations constituant un atout : Certificat de contrôle des risques des systèmes d'information (CRISC);
- Il est préférable de posséder de la formation et de l'expérience en gestion des risques ou en cybersécurité – de deux à cinq ans d'expérience au niveau d'entrée et de cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse de l'information et des données;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Détermination, documentation, analyse et atténuation des risques, et production de rapports sur les risques;
- Planification de la continuité des activités et de l'intervention en cas de sinistre;
- Analyse coûts-avantages;
- Connaissance pratique des principes et des éléments de la cybersécurité;
- Connaissances techniques pour comprendre les exigences en matière de sécurité et d'intégrité des données;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité.

Principales compétences

- Analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

4.5 PLANIFICATEUR STRATÉGIQUE

Description de travail de base

- Élaborer et tenir à jour des plans et des stratégies de cybersécurité pour appuyer et harmoniser les initiatives de cybersécurité de l'organisation et la conformité réglementaire.

Principales tâches liées à la cybersécurité

- Concevoir et mettre en œuvre des stratégies et des programmes de cybersécurité qui décrivent les objectifs et les activités de l'organisation et s'y alignent;
- Étudier et analyser les pratiques et les procédures de cybersécurité de l'organisation qui définissent l'orientation et les contraintes opérationnelles particulières;
- Évaluer les besoins organisationnels et collaborer avec la direction et le personnel à l'élaboration de plans stratégiques pour promouvoir la cybersécurité;
- Examiner les programmes et les projets de cybersécurité de l'organisation et diriger des audits sur ceux-ci ou y participer;
- Rédiger et publier des plans et des pratiques de cybersécurité;
- Interpréter et intégrer les textes de lois et de règlements applicables aux stratégies et aux objectifs de cybersécurité;
- Surveiller l'application des plans de cybersécurité;
- Établir et maintenir des voies de communication avec la direction, le personnel et les utilisateurs sur les plans stratégiques existants et proposés et communiquer tout changement.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine pertinent lié à la cybersécurité (p. ex. administration des affaires, économie, sciences politiques, sciences sociales ou l'équivalent);
- Formation et expérience antérieures en sécurité ou en planification et perfectionnement stratégiques – un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé.
- Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité et ne pas avoir d'expérience dans le domaine de travail. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Tendances technologiques et risques pour la sécurité ainsi que leur incidence possible sur les pratiques de cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité;
- Mise à contribution des pratiques exemplaires et des leçons apprises des organisations externes en mettant l'accent sur la cybersécurité;
- Établissement des lacunes dans les pratiques et les programmes de cybersécurité;
- Utilisation des évaluations des risques ou des menaces dans la préparation des plans stratégiques;
- Élaboration, rédaction et communication des pratiques de cybersécurité à l'appui des objectifs et des activités de l'organisation.

Principales compétences

- Recherche, analyse, résolution de problèmes, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

4.6 ANALYSTE DES ACTIVITÉS

Description de travail de base

- Effectuer une vaste gamme de travaux techniques et/ou professionnels complexes, comme évaluer et améliorer les processus et les systèmes d'une organisation, et analyser son modèle opérationnel.

Principales tâches liées à la cybersécurité

- Rendre compte des principaux paramètres liés à la qualité et à la sécurité de l'information, aux questions de cybersécurité, etc.;
- Définir, élaborer et gérer des politiques, des contrôles, des normes et des processus pour la création de mesures de sécurité opérationnelles régulières en vue de l'amélioration continue;
- Assurer la conformité aux politiques, aux lois, aux règlements et aux pratiques en matière de cybersécurité;
- Élaborer des analyses de rentabilisation ou y contribuer, y compris évaluer les coûts et les risques liés à la mise en œuvre de solutions efficaces de cybersécurité;
- Collaborer avec les intervenants pour réaliser des initiatives stratégiques tout au long du cycle de vie du système;
- Donner des conseils et faire rapport sur les exigences en matière de sécurité et les activités du processus de gestion des risques, y compris la réalisation d'évaluations des répercussions dans le cadre des plans de reprise après sinistre et d'urgence;
- Veiller à la bonne gestion des risques au niveau des programmes et des projets.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, commerce, économie, gestion des technologies, gestion des risques liés aux TI ou l'équivalent);
- Il est souhaitable d'avoir une formation et de l'expérience en cybersécurité.
- Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité et ne pas avoir d'expérience dans le domaine de travail. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Techniques d'analyse de l'information et des données;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Connaissances techniques pour comprendre la sécurité et l'intégrité des données, les exigences de sécurité, la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Analyse coûts-avantages, prévision des revenus et des coûts, etc.;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Élaboration d'évaluations des risques ou des répercussions, d'analyses de rentabilisation et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, souci du détail, organisation, gestion du temps, relations interpersonnelles, communications.

4.7 COMMUNICATIONS

Description de travail de base

- Élaborer et mettre en œuvre des stratégies et des ressources de communication à l'appui des buts et des objectifs d'une organisation en matière de cybersécurité.

Principales tâches liées à la cybersécurité

- Élaborer et mettre en œuvre des produits de communication sur la cybersécurité, y compris traduire les politiques de l'organisation en messages clairs et directs sur la cybersécurité;
- Examiner les communications entrantes de l'organisation en ce qui a trait à la cybersécurité;
- Fournir une orientation sur le processus d'analyse coûts-avantages en établissant et en administrant des politiques, des processus et des procédures;
- Communiquer la valeur de la cybersécurité à tous les niveaux de l'organisation;
- Prêter conseils en matière de cybersécurité et de gestion des risques aux fins de l'élaboration d'opérations de continuité des activités, de plans stratégiques et de procédures;
- Veiller à ce que les plans d'action en matière de cybersécurité soient examinés, validés et mis en œuvre au besoin;
- Élaborer des analyses de rentabilisation ou y contribuer, y compris effectuer des analyses coûts-avantages et des analyses des risques pour la mise en œuvre de produits de communication efficaces en matière de cybersécurité;
- Reconnaître un incident de cybersécurité possible et prendre les mesures appropriées pour le signaler;
- Formuler des conseils sur la diffusion de messages clés lors d'événements courants et de crise liés à la cybersécurité;
- Organiser et coordonner des événements médiatiques pour diffuser des solutions efficaces en matière de cybersécurité.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine connexe (p. ex. administration des affaires, commerce, communications, relations publiques, gestion des risques liés aux TI ou l'équivalent);
- Il est préférable d'avoir de la formation et de l'expérience en communications ou en cybersécurité – d'un à quatre ans d'expérience au niveau d'entrée. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Maintien d'une connaissance pratique des principes et des éléments de cybersécurité;
- Connaissances techniques pour comprendre la sécurité et l'intégrité des données, les exigences de sécurité et la conception fonctionnelle et technique des solutions de cybersécurité;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Terminologie, lignes directrices et procédures relatives à la sécurité des communications;
- Analyse coûts-avantages, analyse des risques, etc.;
- Principes et techniques de gestion des ressources;
- Élaboration d'analyses de rentabilisation et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, souci du détail, organisation, gestion du temps, relations interpersonnelles et communication.

4.8 PLANIFICATEUR DE LA REPRISE APRÈS SINISTRE

Description de travail de base

- Élaborer, mettre à l'essai, mettre en œuvre et gérer les interventions d'urgence, les processus, les procédures et/ou les plans de rétablissement et de reprise, au besoin, pour rétablir et protéger l'infrastructure TI d'une organisation (p. ex. réseaux, systèmes, contrôles) en cas de catastrophe.

Principales tâches liées à la cybersécurité

- Établir, tenir à jour et mettre à l'essai des plans de reprise après sinistre et des plans d'urgence pour les scénarios de catastrophe et d'interruption des activités;
- Établir des budgets de reprise après sinistre et d'urgence;
- Interpréter les lois et règlements nationaux et provinciaux, et assurer la conformité aux plans d'urgence et de reprise après sinistre;
- Élaborer et tenir à jour des évaluations des risques et des répercussions des catastrophes sur les fonctions organisationnelles et les systèmes d'information;
- Élaborer et administrer la formation sur la reprise après sinistre et les plans d'urgence;
- Coordonner les communications en situation de crise.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, commerce, économie, gestion des risques liés aux TI ou l'équivalent);
- Attestations constituant un atout : Certifications de l'EC-Council;
- Les personnes qui remplissent habituellement ce rôle ont une vaste expérience de la coordination ou de la gestion de l'intervention en cas d'incident de sécurité ou touchant les TI. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Établissement, documentation, analyse et atténuation des risques, et production de rapports sur les risques;
- Planification de la continuité des activités et de l'intervention en cas de sinistre;
- Analyse coûts-avantages, prévision des revenus et des coûts, etc.;
- Maintien d'une connaissance pratique des principes et des éléments de cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité.

Principales compétences

- Sens des affaires, résolution de problèmes, organisation, gestion du temps, souci du détail, relations interpersonnelles et communications.

4.9 ANALYSTE DE L'APPROVISIONNEMENT

Description de travail de base

- Chercher, analyser et acquérir des stocks et des services pour l'organisation.

Principales tâches liées à la cybersécurité

- Étudier et analyser les solutions techniques et de cybersécurité offertes sur le marché qui répondent le mieux aux besoins de l'organisation;
- Évaluer et documenter les risques liés à la cybersécurité tout au long du cycle de vie de l'approvisionnement;
- Assurer la conformité aux lignes directrices en matière d'achat et aux politiques, règlements et procédures de l'organisation en matière de cybersécurité;
- Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation;
- Assurer la coordination avec les experts en cybersécurité afin de surveiller les systèmes et de mettre à jour régulièrement les politiques et les procédures de l'organisation;
- Élaborer et tenir à jour des évaluations des risques et des rapports connexes sur les fournisseurs et les produits et services acquis, en fonction de la fiabilité et de la crédibilité;
- Assurer la coordination avec le service des finances, l'organisation et le fournisseur pour négocier des modalités ou une entente et des conditions;
- Étudier et analyser les tendances du marché en fonction des données sur les ventes et le rendement, prévoir les possibilités futures et formuler des recommandations en matière d'approvisionnement à la direction.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, économie ou l'équivalent);
- Il est souhaitable d'avoir une formation et de l'expérience en cybersécurité;
- Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Analyse coûts-avantages et prévision, etc.;
- Maintien d'une connaissance pratique des principes et des éléments de cybersécurité;
- Connaissances techniques pour comprendre les exigences en matière de sécurité des données, ainsi que la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Élaboration d'évaluations des risques.

Principales compétences

- Analyse, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

4.10 DIRIGEANT PRINCIPAL DE LA SÉCURITÉ DE L'INFORMATION

Description de travail de base

- Établir, maintenir et superviser les opérations et les programmes, les procédures et les politiques, les systèmes et les biens relatifs à la cybersécurité à l'échelle de l'organisation, ainsi que le budget et les ressources, afin d'assurer la protection des biens d'information.

Principales tâches liées à la cybersécurité

- Diriger et approuver la conception de programmes et de systèmes de gestion des risques liés à la cybersécurité;
- Diriger et aligner les priorités en matière de cybersécurité avec les plans stratégiques;
- Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour appuyer les objectifs de cybersécurité;
- Conseiller la haute direction sur les programmes, les politiques, les processus, les normes et les procédures de cybersécurité;
- Superviser les stratégies et les exigences de mise en œuvre pour veiller à ce que les procédures et les lignes directrices soient conformes aux politiques de cybersécurité;
- Veiller à la mise en œuvre et à la mise à l'essai des plans de reprise après sinistre, des opérations de continuité des activités et des procédures;
- Examiner et approuver les politiques, les contrôles et la planification d'intervention en cas d'incident en matière de cybersécurité;
- Entreprendre, faciliter et promouvoir la sensibilisation aux questions de cybersécurité au sein de l'organisation et veiller à ce que les priorités en matière de cybersécurité soient reflétées dans la vision et les objectifs de l'organisation;
- Examiner les enquêtes après les cyberincidents, y compris l'analyse des répercussions et les recommandations pour éviter des vulnérabilités semblables;
- Surveiller les mesures de protection ou de correction lorsqu'un cyberincident ou une vulnérabilité est découvert;
- Maintenir une compréhension actuelle du contexte des cybermenaces dans l'organisation;
- Assurer la conformité aux politiques, aux lois, aux règlements et aux procédures en matière de cybersécurité;
- Prévoir des audits et des examens périodiques de la sécurité;
- Surveiller la gestion de l'identité et de l'accès;
- Préparer des prévisions financières pour les opérations de cybersécurité et assurer la maintenance adéquate des biens d'information et de sécurité;
- Fournir du leadership, des possibilités de formation et des conseils au personnel.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, informatique, gestion des TI, sécurité de l'information ou l'équivalent). Une maîtrise en administration des affaires ou une maîtrise en cybersécurité est un atout;
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Computing Technology Industry Association (CompTIA); Professionnel certifié en sécurité des systèmes d'information (CISSP);

- Il est préférable d'avoir reçu une formation et cumulé de l'expérience en matière d'infrastructure de sécurité des TI, d'analyse des besoins ou de gestion de programme – plus de 10 ans d'expérience pertinente en TI, dont au moins cinq ans d'expérience en gestion. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, de l'architecture informatique, des structures de données et des algorithmes;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Maintien d'une connaissance pratique des principes et des éléments de la cybersécurité et de la protection des renseignements personnels;
- Accès réseau, identité et gestion de l'accès;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Techniques d'analyse opérationnelle;
- Techniques d'analyse de l'information et des données;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Analyse coûts-avantages, prévision des revenus et des coûts, analyse des risques, etc.;
- Principes et techniques de gestion des ressources;
- Lois, règlements, politiques et éthique applicables en matière de cybersécurité;
- Tendances technologiques et risques pour la sécurité ainsi que leur incidence potentielle sur les politiques de cybersécurité.

Principales compétences

- Recherche, analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

4.11 GESTIONNAIRE DE LA CYBERSÉCURITÉ

Description de travail de base

- Gérer la détection, la prévention, l'intervention et la reprise des activités en cas de cyberincident et de cybermenace; veiller à ce que les réseaux et les systèmes informatiques soient bien protégés contre les cyberattaques, les intrusions et divers types d'atteintes à la sécurité des données.

Principales tâches liées à la cybersécurité

- Surveiller et évaluer tous les aspects des activités et de l'infrastructure de cybersécurité et régler tout problème;
- Prêter conseils, orientation et soutien d'expert relativement aux stratégies, menaces et techniques concernant les activités irrégulières ou malveillantes et les menaces pour les ressources du réseau;
- Définir, élaborer, mettre en œuvre, tenir à jour et examiner les politiques et les procédures en matière de cybersécurité;
- Veiller au respect des politiques, des règlements et des procédures de l'organisation en matière de cybersécurité.
- Mettre en œuvre des mesures, des contrôles et des protocoles de sécurité pour protéger les fichiers numériques et les systèmes d'information contre les cyberincidents ou les cybermenaces;
- Maintenir la sensibilisation aux principales tendances et aux signalements, et comprendre leur incidence sur les interventions en cas de cyberincident ou de cybermenace;
- Diriger les activités et les procédures sous-jacentes qui appuient les activités de l'organisation;
- Établir et maintenir des voies de communication avec les intervenants sur la cybersécurité;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;
- Cerner et régler les problèmes de planification et de gestion des effectifs en cybersécurité.

Études, formation et expérience de travail couramment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique, technologies de l'information ou l'équivalent). Une maîtrise est un atout;
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP); Certification « Certified Information Security Manager (CISM);
- Il est préférable d'avoir de la formation et de l'expérience en sécurité réseau – de cinq à dix ans d'expérience. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, de l'architecture informatique, des structures de données et des algorithmes;
- C, C++, Java, Python et autres langages de programmation similaires;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex. pare-feu, chiffrement, dispositifs de réseau privé virtuel);
- Authentification, autorisation et méthodes de contrôle de l'accès;
- Contrôles liés à l'utilisation, au traitement, au stockage et à la transmission des données;
- Accès réseau, identité et gestion de l'accès;

- Protocoles de réseau et outils d'analyse de paquets;
- Techniques de renforcement des systèmes d'exploitation et de l'administration des systèmes;
- Système de détection des intrusions (SDI)/système de prévention des intrusions (SPI), tests de pénétration et de vulnérabilité;
- Méthodes et processus de mise à l'essai et d'évaluation de la sécurité;
- Prévention de la perte de données (PPD), antivirus et antimaliciels;
- Méthodes d'intervention et de prise en charge des incidents;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Politiques, exigences et pratiques en matière de gestion des risques;
- Principes et techniques de gestion des ressources;
- Élaboration d'évaluations des menaces, de rapports de vérification et de documents de gestion des risques;
- Lois, règlements, politiques et éthique applicables en matière de cybersécurité.

Principales compétences

- Analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

4.12 GESTIONNAIRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Description de travail de base

- Gérer la sécurité des systèmes d'information tout au long du cycle de vie des systèmes et rendre compte du rendement des systèmes d'information en assurant la confidentialité, l'intégrité et la disponibilité.

Principales tâches liées à la cybersécurité

- Surveiller et évaluer tous les aspects du développement de la sécurité des systèmes d'information et régler tout problème;
- Évaluer les tendances et les risques technologiques et déterminer les répercussions possibles sur le développement des systèmes;
- Élaborer des mécanismes pour surveiller et mesurer les risques, la conformité et les efforts d'assurance de l'information;
- Élaborer, exécuter et tenir à jour des examens de sécurité et des évaluations des vulnérabilités et des répercussions, et réagir directement aux intrusions dans les réseaux ou les systèmes;
- Fournir des conseils pour l'élaboration de plans de reprise après sinistre, d'opérations de continuité des activités et de procédures;
- Examiner les coûts des projets, les concepts de design et tout changement;
- Examiner, mettre en œuvre, mettre à jour et documenter les politiques, les normes et les procédures de cybersécurité pour l'organisation;
- Assurer la conformité aux politiques, aux règlements et aux procédures de l'organisation en matière de cybersécurité;
- Résoudre les conflits dans les lois, les règlements, les politiques ou les procédures;
- Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation;
- Assurer la coordination avec les experts en sécurité des systèmes d'information afin de surveiller régulièrement les systèmes et les contrôles et de mettre à jour les politiques et les procédures de l'organisation;
- Diriger les activités et les procédures sous-jacentes qui appuient les activités de l'organisation;
- Établir et maintenir des voies de communication avec les intervenants sur la sécurité des systèmes d'information;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;
- Cerner et régler les problèmes de planification et de gestion des effectifs en cybersécurité.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, mathématiques, technologies réseau, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certified Secure Software Lifecycle Professional (CSSLP);
- Il est souhaitable de posséder une formation et une expérience antérieures en développement de systèmes et en gestion de systèmes ou de la sécurité. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;

- Principes dans les domaines de la sécurité de l'information, de l'ingénierie, du réseautage et des mathématiques;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Concepts des systèmes d'exploitation, des microprocesseurs, de l'accès réseau, de l'identité, de la gestion de l'accès et des tests de pénétration;
- Conceptions et fonctions de sécurité des données;
- Méthodologies, essais et protocoles d'analyse de la sécurité des données;
- Outils, méthodes et techniques de conception de systèmes;
- Techniques de codage et de configuration sécurisés;
- 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;
- Effectuer des analyses de vulnérabilité et cerner les vulnérabilités dans les systèmes de sécurité;
- Protocoles de réseautage et processus de conception;
- Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données;
- Conception de contre-mesures aux risques de sécurité cernés;
- Politiques, exigences et pratiques en matière de gestion des risques;
- Planification de la continuité des activités et de l'intervention en cas de sinistre;
- Analyse coûts-avantages;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Élaboration et exécution d'évaluations des risques ou des répercussions, d'analyses de rentabilisation et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

4.13 GESTIONNAIRE DE PROJET

Description de travail de base

- Gérer les projets de technologies de l'information tout au long de leur cycle de vie.

Principales tâches liées à la cybersécurité

- Surveiller et évaluer tous les aspects des projets de cybersécurité et régler tout problème;
- Évaluer les tendances et les risques technologiques et déterminer les répercussions possibles sur les projets;
- Élaborer des mécanismes pour surveiller et mesurer les risques, la conformité et les efforts d'assurance;
- Prêter conseils en matière de cybersécurité et de gestion des risques aux fins de l'élaboration d'opérations de continuité des activités, de plans stratégiques et de procédures;
- Examiner les coûts des projets, les concepts de design et tout changement;
- Examiner, mettre en œuvre, mettre à jour et documenter les politiques, les normes et les procédures de cybersécurité;
- Résoudre les conflits dans les lois, les règlements, les politiques ou les procédures;
- Examiner ou effectuer des audits de projets ou de rapports de sécurité, relever tout problème important, prendre des mesures correctives et s'assurer que les questions en suspens font l'objet d'un suivi;
- Diriger les activités et les procédures sous-jacentes qui appuient les activités de l'organisation;
- Établir et maintenir des voies de communication avec les intervenants sur les procédures opérationnelles de cybersécurité qui appuient les activités de l'organisation;
- Préparer et publier des documents de gestion des risques;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;
- Cerner et régler les problèmes de planification et de gestion des effectifs en cybersécurité.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, génie informatique, technologies de l'information, systèmes d'information de gestion, ingénierie de systèmes ou l'équivalent);
- Attestations constituant un atout : Professionnel en gestion de projet (PGP);
- Il est souhaitable d'avoir une formation et de l'expérience relatives à l'infrastructure de sécurité des TI ou à la gestion de projet. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse opérationnelle;
- Maintenir une connaissance pratique des principes et des éléments de cybersécurité;
- Connaissance technique des systèmes informatiques et réseau, de la sécurité intégrée et des plateformes;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Politiques, exigences et pratiques en matière de gestion des risques;
- Principes et techniques de gestion des ressources;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Élaboration d'évaluations des risques, de rapports d'audit et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

4.14 GESTIONNAIRE DE LA CHAÎNE D'APPROVISIONNEMENT

Description de travail de base

- Gérer les failles et les vulnérabilités en matière de cybersécurité dans les opérations de la chaîne d'approvisionnement d'une organisation et prêter conseils et orientation pour aider à réduire ces risques liés à la chaîne d'approvisionnement.

Principales tâches liées à la cybersécurité

- Créer des processus et des méthodes pour recueillir de l'information sur la chaîne d'approvisionnement;
- Définir, élaborer, examiner et tenir à jour des politiques, des normes et des processus pour cerner, évaluer et atténuer les risques liés à la chaîne d'approvisionnement;
- Élaborer et tenir à jour des évaluations des risques et des menaces ainsi que des rapports connexes sur les fournisseurs et les produits ou services acquis, en fonction du niveau de risque ou de menace;
- Évaluer et documenter les risques et les vulnérabilités en matière de cybersécurité tout au long du cycle de vie de l'approvisionnement;
- Élaborer, tenir à jour et améliorer les approches et les procédures d'atténuation des risques;
- Analyser les solutions de cybersécurité disponibles sur le marché qui répondent le mieux aux besoins organisationnels;
- Assurer la conformité aux politiques, aux règlements et aux procédures de l'organisation en matière de cybersécurité;
- Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation;
- Assurer la coordination avec les experts en cybersécurité afin de surveiller régulièrement les systèmes et les contrôles et de mettre à jour les politiques et les procédures de l'organisation;
- Diriger les activités et les procédures sous-jacentes qui appuient les activités de l'organisation;
- Établir et maintenir des voies de communication avec les intervenants relativement à la chaîne d'approvisionnement;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;
- Cerner et régler les problèmes de planification et de gestion des effectifs en cybersécurité.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, informatique, génie informatique ou l'équivalent);
- Il est souhaitable d'avoir une formation et de l'expérience en sécurité réseau. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse de l'information et des données;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex. pare-feu, chiffrement, dispositifs de réseau privé virtuel);
- Connaissances techniques pour comprendre les exigences en matière de sécurité et d'intégrité des données, les exigences de sécurité, ainsi que la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- 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;
- Gestion de la configuration liée à la cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité;
- Élaboration d'évaluations des menaces et des risques.

Principales compétences

- Analyse, résolution de problèmes, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

5 PROTÉGER ET DÉFENDRE

5.1 ANALYSTE EN CYBERSÉCURITÉ

Description de travail de base

- Coordonner les interventions et contrer les cyberincidents ainsi que les cybermenaces à l'égard d'une organisation et au sein de celle-ci en utilisant les données recueillies à partir de divers outils de cyberdéfense pour surveiller, cerner, analyser, signaler et prévenir les menaces et les événements.

Principales tâches liées à la cybersécurité

- Différencier et analyser le trafic réseau pour repérer les activités irrégulières ou malveillantes et les menaces pour les ressources du réseau;
- Analyser les activités irrégulières ou malveillantes et les menaces à l'aide de renseignements recueillis auprès de diverses sources au sein de l'organisation afin d'acquérir une connaissance de la situation et de déterminer la cause profonde et l'efficacité d'une attaque;
- Détecter et établir les activités irrégulières ou malveillantes et les menaces ou attaques potentielles, et lancer l'alerte en temps opportun, et distinguer ces incidents et événements des activités inoffensives;
- Documenter les incidents ou les menaces qui peuvent avoir des répercussions continues et immédiates sur l'organisation et en faire part aux échelons supérieurs;
- Aviser la direction, les intervenants et les responsables/répondants en cas de cyberincident, ainsi que les collègues, des incidents et des menaces soupçonnés et de leurs répercussions possibles afin qu'ils prennent d'autres mesures fondées sur le plan d'intervention en cas de cyberincident de l'organisation;
- Utiliser des outils de cyberdéfense pour la surveillance et l'analyse continues du trafic et des systèmes réseau afin de repérer les activités irrégulières ou malveillantes et les menaces;
- Recommander et installer des outils et des contre-mesures appropriés en fonction des menaces et des vulnérabilités;
- Définir, élaborer, mettre en œuvre et tenir à jour les politiques et les procédures de cybersécurité;
- Planifier, mettre en œuvre et améliorer les mesures, les contrôles et les protocoles de sécurité pour protéger les systèmes d'information contre les cyberincidents ou les cybermenaces;
- Effectuer des tests de vulnérabilité, des analyses des risques et des évaluations de sécurité;
- Isoler et supprimer les logiciels malveillants;
- Prévoir les alertes, les incidents et les menaces liés à la sécurité, et en réduire la probabilité d'occurrence;
- Fournir de l'aide et coordonner les activités avec des collègues afin de valider les alertes, les incidents et les menaces liés à la sécurité;
- Effectuer des recherches et des analyses, et préparer des rapports sur les tendances en matière de cyberdéfense ainsi que des rapports d'audit internes et externes.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, technologies de l'information, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP); Computing Technology Industry Association (CompTIA) Security+;

- Il est préférable d'avoir de la formation et de l'expérience en sécurité réseau – un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, de l'architecture informatique, des structures de données et des algorithmes;
- C, C++, Java, Python et autres langages de programmation similaires;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex. pare-feu, chiffrement, dispositifs de réseau privé virtuel);
- Authentification, autorisation et méthodes de contrôle de l'accès;
- Contrôles liés à l'utilisation, au traitement, au stockage et à la transmission des données.
- Accès réseau, identité et gestion de l'accès;
- Protocoles de réseau et outils d'analyse de paquets;
- Techniques de renforcement des systèmes d'exploitation et de l'administration des systèmes;
- Système de détection des intrusions (SDI)/système de prévention des intrusions (SPI), tests de pénétration et de vulnérabilité;
- Méthodes et processus de mise à l'essai et d'évaluation de la sécurité;
- Prévention de la perte de données (PPD), antivirus et antimaliciels;
- Méthodes d'intervention et de prise en charge des incidents;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Lois, règlements, politiques et éthique applicables en matière de cybersécurité.

Principales compétences

- Analyse, souci du détail, relations interpersonnelles et communications.

5.2 ANALYSTE DE LA SÉCURITÉ DES SYSTÈMES DE CONTRÔLE INDUSTRIEL (SCI)

Description de travail de base

- Effectuer des tâches techniques et d'ingénierie à l'appui du système de contrôle industriel (SCI) pour s'assurer qu'il fonctionne correctement et en toute sécurité.

Principales tâches liées à la cybersécurité

- Surveiller activement le rendement et la santé du SCI, et régler les problèmes d'interopérabilité du matériel ou des logiciels, ainsi que les pannes et défaillances du système et les cybermenaces;
- Concevoir, installer, faire fonctionner et entretenir l'équipement, les serveurs, les réseaux et les autres composants du SCI;
- Effectuer la maintenance et les mises à niveau;
- Effectuer des tests de vulnérabilité, des analyses des risques et des évaluations de sécurité;
- Analyser et examiner les vulnérabilités du système et en faire rapport;
- Étudier et évaluer de nouvelles technologies et de nouveaux processus qui améliorent les capacités en matière de sécurité;
- Faire des recherches et élaborer un contexte de sécurité des systèmes et définir les exigences de sécurité des systèmes en fonction des normes et des politiques et pratiques de cybersécurité de l'industrie;
- S'assurer que les systèmes acquis ou développés sont conformes aux politiques et aux pratiques en matière de cybersécurité;
- Effectuer des examens de sécurité et déterminer les lacunes ou les cybermenaces dans le SCI;
- Préparer des rapports techniques qui documentent le processus de développement des systèmes;
- Documenter et traiter les exigences de l'organisation en matière de sécurité de l'information et de sécurité des systèmes tout au long du cycle de vie des systèmes;
- Définir, élaborer, mettre en œuvre et maintenir des politiques, des normes et des procédures en matière d'infrastructure;
- Élaborer et tenir à jour des rapports et des évaluations de projet, et d'autres documents pertinents;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique, systèmes d'information, ingénierie des systèmes de contrôle, mathématiques ou l'équivalent);
- Il est préférable d'avoir de la formation et de l'expérience liées au contrôle des procédés ou au SCI – de deux à trois ans d'expérience au niveau d'entrée; de cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Logiciels et matériel des SCI, contrôleurs logiques programmables et relais numériques et analogiques;
- Systèmes de télémétrie, communications de données, acquisition de données et contrôle des processus;
- Systèmes d'exploitation, réseaux et systèmes de communication;
- Procédures de dépannage et de maintenance des ordinateurs et des réseaux;
- Principes et pratiques de l'administration réseau;

- 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;
- 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;
- Élaboration d'évaluations, de rapports et de documents pertinents.

Principales compétences

- Recherche, analyse, résolution de problèmes, organisation, relations interpersonnelles et communications.

5.3 ANALYSTE DE LA SÉCURITÉ DE L'INFORMATION

Description de travail de base

- Coordonner la protection de l'information et des systèmes d'information contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité.

Principales tâches liées à la cybersécurité

- Surveiller et analyser les systèmes pour déceler les atteintes à la sécurité;
- Détecter et établir les atteintes à la sécurité, et lancer l'alerte en temps opportun;
- Documenter les atteintes qui peuvent avoir des répercussions continues et immédiates sur l'organisation et en faire part aux échelons supérieurs;
- Informer la direction et les collègues de toute atteinte à la sécurité soupçonnée et de toute répercussion éventuelle en vue de prendre des mesures supplémentaires en fonction du plan d'intervention en cas de cyberincident et des politiques de cybersécurité de l'organisation;
- Recommander, installer et tenir à jour des logiciels pour protéger l'information;
- Définir, élaborer, mettre en œuvre et tenir à jour les politiques et procédures de cybersécurité;
- Planifier, mettre en œuvre et améliorer les mesures, les contrôles et les protocoles de sécurité pour protéger les systèmes d'information et les fichiers numériques contre les cyberincidents ou les cybermenaces;
- Effectuer des tests de vulnérabilité, des analyses des risques et des évaluations de sécurité;
- Effectuer des recherches et des analyses, ainsi que préparer des rapports, sur les tendances en matière de cyberdéfense ainsi que des rapports d'audit internes et externes.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, technologies de l'information, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP); Computing Technology Industry Association (CompTIA) Security+;
- Il est préférable d'avoir de la formation et de l'expérience en sécurité de l'information : d'un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, de l'architecture informatique, des structures de données et des algorithmes;
- C, C++, Java et autres langages de programmation informatique similaires;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex., pare-feu, zones démilitarisées, chiffrement, dispositifs de réseau privé virtuel);
- Authentification, autorisation et méthodes de contrôle de l'accès;
- Contrôles liés à l'utilisation, au traitement, au stockage et à la transmission des données;
- Assurance de l'information;
- Accès réseau, identité et gestion de l'accès;

- Protocole de contrôle de la transmission et protocole Internet;
- Système de détection des intrusions (SDI)/système de prévention des intrusions (SPI), et tests de pénétration et de vulnérabilité;
- Méthodes et processus de mise à l'essai et d'évaluation de la sécurité;
- Prévention de la perte de données (PPD), antivirus et antimaliciels;
- Méthodes d'intervention et de prise en charge des incidents;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Lois, règlements, politiques et éthique applicables en matière de cybersécurité.

Principales compétences

- Analyse, résolution de problèmes, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

5.4 ANALYSTE DE L'ÉVALUATION DES VULNÉRABILITÉS

Description de travail de base

- Analyser les applications et les systèmes d'exploitation pour déceler les lacunes et les vulnérabilités; effectuer et présenter des évaluations de vulnérabilité sur les réseaux et les systèmes d'une organisation.

Principales tâches liées à la cybersécurité

- Cerner les lacunes 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.

Études, formation et expérience de travail couramment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. technologies de l'information, informatique ou l'équivalent);
- Attestations constituant un atout : Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Il est préférable d'avoir de la formation et de l'expérience en gestion de l'identité et de l'accès – de deux à trois ans d'expérience de travail pertinente pour le niveau d'entrée; de cinq à sept ans d'expérience pour le niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Menaces et vulnérabilités liées à la sécurité des systèmes et des applications (p. ex. dépassement de mémoire tampon, scripts intersites, langage SQL, code malveillant);
- Principes, outils et techniques relatifs aux tests de pénétration;
- 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;
- Processus de gestion des risques pour évaluer et atténuer les risques;
- Concepts d'administration du système;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Effectuer des analyses des vulnérabilités et cerner les vulnérabilités dans les systèmes de sécurité;
- Exécution d'évaluations des vulnérabilités, des répercussions et des risques;
- Examen les registres du système pour repérer des traces d'intrusion;
- Utilisation d'outils d'analyse réseau pour déterminer les vulnérabilités;
- Utilisation de techniques de piratage psychologique;

- Établissement des problèmes de sécurité en fonction de l'analyse des données sur les vulnérabilités et la configuration.

Principales compétences

- Recherche, analyse, souci du détail, relations interpersonnelles et communications.

5.5 TESTEUR DE PÉNÉTRATION

Description de travail de base

- Effectuer 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.

Principales tâches liées à la cybersécurité

- 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, des systèmes et des installations d'une organisation;
- Élaborer des tests de pénétration et les outils nécessaires à leur exécution;
- 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 exploiter;
- Élaborer 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.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. technologies de l'information, informatique, génie informatique, informatique judiciaire ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Computing Technology Industry Association (CompTIA) Security+; Professionnel certifié de sécurité offensive (OSCP);
- Il est préférable d'avoir de la formation et de l'expérience dans le domaine de la cybersécurité à l'appui de la cyberdéfense ou de la gestion des incidents ou des vulnérabilités – d'un à trois ans d'expérience dans le domaine de la sécurité au niveau d'entrée; sept à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Dispositifs de réseau privé virtuel et solutions de chiffrement;
- Principes, outils et techniques relatifs aux tests de pénétration;
- Méthodologies et applications d'évaluation des vulnérabilités et de tests de pénétration;
- Menaces et vulnérabilités liées à la sécurité des systèmes et des applications (p. ex., dépassement de mémoire tampon, scripts intersites, langage SQL, code malveillant);
- Concepts et principes de l'architecture de sécurité réseau;
- Exécution de vérifications de sécurité;
- Élaboration de code sécurisé;
- Utilisation de techniques de rétro-ingénierie.

Principales compétences

- Recherche, analyse, relations interpersonnelles et communications.

5.6 INTERVENANT/RESPONSABLE EN CAS D'INCIDENT DE CYBERSÉCURITÉ

Description de travail de base

- Proposer 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.

Principales tâches liées à la cybersécurité

- 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);
- Effectuer le triage 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 pour détecter les menaces;
- 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;
- 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.

Études, formation et expérience de travail couramment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, génie informatique, informatique judiciaire ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Il est préférable d'avoir de la formation et de l'expérience en sécurité réseau : de deux à trois ans d'expérience de la réponse à des incidents ou à des questions de sécurité au niveau d'entrée; cinq ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Menaces et vulnérabilités pour la sécurité des systèmes et des applications;
- Tactiques, techniques et procédures (TTP) avancées des auteurs de cybermenace;
- Méthodologies, outils et techniques d'analyse des logiciels malveillants;

- Enquêtes de cybersécurité et préservation des preuves;
- Rudiments de l'évaluation des vulnérabilités;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Méthodologies de gestion et d'intervention en cas d'incident;
- Traitement des incidents dans les environnements en nuage et virtualisés;
- Traitement des incidents dans les environnements d'appareils sans fil et mobiles;
- Rudiments de la continuité des activités et de l'intervention en cas de sinistre.

Principales compétences

- Analyse, résolution de problèmes, organisation, gestion du temps, relations interpersonnelles et communications.

5.7 ANALYSTE EN CRIMINALISTIQUE NUMÉRIQUE

Description de travail de base

- Effectuer des analyses de criminalistique numérique pour analyser les preuves provenant d'ordinateurs, de réseaux et d'autres dispositifs de stockage de données, notamment l'enquête et la préservation des preuves électroniques, la planification et le développement d'outils, l'établissement des priorités des activités et le soutien des opérations de reprise et de l'analyse après incident.

Principales tâches liées à la cybersécurité

- 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;
- 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;
- Élaborer 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/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.

Études, formation et expérience de travail couramment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, informatique judiciaire, génie informatique ou l'équivalent);
- Attestations constituant un atout : Professionnel certifié en sécurité des systèmes d'information (CISSP); Certification en assurance de l'information globale (GIAC);
- Il est préférable d'avoir de la formation et de l'expérience en analyse de la sécurité des TI ou en intervention en cas d'incident : d'un à trois ans d'expérience en criminalistique pour le niveau d'entrée; cinq ans d'expérience pour le niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Méthodes d'intervention et de prise en charge des incidents;
- 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, appareil mobile, réseau, ordinateur [boîte DEAD], etc.);
- Outils et techniques d'analyse des logiciels malveillants;
- Rétro-ingénierie.

Principales compétences

- Recherche, analyse, souci du détail, relations interpersonnelles et communications.

6 EXPLOITER ET MAINTENIR

6.1 OPÉRATEUR/SPÉCIALISTE DE LA SÉCURITÉ DES RÉSEAUX

Description de travail de base

- Développer, créer, intégrer, tester et maintenir la sécurité des systèmes informatiques et des systèmes d'information tout au long du cycle de vie des systèmes, et rendre compte du rendement des systèmes d'information;
- Surveiller activement les réseaux pour détecter et prévenir les menaces à la sécurité et assurer la reprise en cas d'occurrence.

Principales tâches liées à la cybersécurité

- Définir et examiner les systèmes informatiques et les réseaux 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 les 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;
- Planifier, faire des recherches, mettre en œuvre et maintenir des réseaux et des systèmes informatiques sécurisés à l'aide d'analyses scientifiques et de modèles mathématiques;
- Faire des recherches sur les technologies actuelles et nouvelles pour comprendre les capacités des réseaux ou systèmes requis;
- 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;
- Définir, élaborer, mettre en œuvre et tenir à jour les politiques et les procédures de cybersécurité;
- Élaborer et mener des procédures de mise à l'essai et de validation du réseau, de programmation et de codage sécurisé, et rendre compte de la fonctionnalité et de la résilience;
- Effectuer des tests de vulnérabilité et des examens de sécurité sur les réseaux afin de cerner les lacunes, et examiner les contrôles et les mesures nécessaires pour protéger les réseaux contre les activités irrégulières ou malveillantes et les menaces;
- Surveiller et analyser activement le trafic et les systèmes du réseau pour détecter les activités irrégulières ou malveillantes et les menaces;
- Détecter et établir les activités irrégulières ou malveillantes et les menaces ou attaques potentielles, et lancer l'alerte en temps opportun, et distinguer ces incidents et événements des activités inoffensives;
- Documenter les incidents ou les menaces qui peuvent avoir des répercussions continues et immédiates sur l'organisation et en faire part aux échelons supérieurs;
- Aviser la direction, les intervenants et les responsables des cyberincidents, ainsi que les collègues des incidents et des menaces soupçonnés, et de leurs répercussions possibles afin qu'ils prennent d'autres mesures en fonction du plan d'intervention en cas de cyberincident de l'organisation;
- Recommander, installer et améliorer des mesures, des contrôles et des protocoles de sécurité pour protéger les fichiers numériques et les réseaux ou systèmes contre les cybermenaces et les vulnérabilités.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, technologies de l'information, génie informatique ou l'équivalent);
- Attestations constituant un atout : Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Il est préférable d'avoir de la formation et de l'expérience en sécurité réseau – d'un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, de la technologie d'alimentation électrique, des protocoles de système et des logiciels de cybersécurité;
- Principes dans les domaines de la sécurité de l'information, de l'ingénierie, du réseautage et des mathématiques;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Concepts des systèmes d'exploitation, des microprocesseurs, de l'accès réseau, de la gestion de l'identité et de l'accès, et des tests de pénétration;
- Protocoles de réseau et outils d'analyse de paquets;
- Techniques de renforcement des systèmes d'exploitation et de l'administration des systèmes;
- Outils, méthodes et techniques de conception de systèmes;
- Techniques de codage et de configuration sécurisés;
- Architecture informatique, structures des données et algorithmes;
- Algèbre linéaire/matricielle et/ou mathématiques discrètes;
- C, C++, Java, Python et autres langages de programmation similaires;
- 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;
- Système de détection des intrusions (SDI)/système de prévention des intrusions (SPI), et tests de pénétration et de vulnérabilité;
- Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données;
- Méthodes d'intervention et de prise en charge des incidents;
- Conception de contre-mesures aux risques de sécurité cernés;
- Politiques, exigences et pratiques en matière de gestion des risques;
- Planification de la continuité des activités et de l'intervention en cas de sinistre;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex., pare-feu, zones démilitarisées, chiffrement, dispositifs de réseau privé virtuel);
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Élaboration et exécution d'évaluations des risques et de documents pertinents;
- Technologies actuelles et nouvelles, et technologies de cybersécurité.

Principales compétences

- Recherche, analyse, souci du détail, relations interpersonnelles et communications.

6.2 ADMINISTRATEUR DE SYSTÈMES

Description de travail de base

- Établir et maintenir des réseaux ou des composants précis d'un système informatique (p. ex. l'installation, la configuration et la mise à jour du matériel, des logiciels et des réseaux; la surveillance des problèmes de rendement et le dépannage des systèmes; la mise en œuvre de contrôles de sécurité opérationnels et techniques; et le respect des politiques et procédures de cybersécurité de l'organisation).

Principales tâches liées à la cybersécurité

- Installer, configurer et mettre à jour le matériel, les logiciels et les réseaux;
- Effectuer des tests fonctionnels et de connectivité pour assurer l'opérabilité et l'efficacité continues;
- Gérer les serveurs réseau et les outils technologiques, y compris le rendement, la capacité, la disponibilité, la fonctionnalité et la récupérabilité, ainsi que l'accès aux systèmes et aux postes de travail;
- Surveiller le rendement et maintenir la configuration des systèmes et des serveurs conformément aux exigences de sécurité;
- Résoudre les problèmes d'interopérabilité du matériel ou des logiciels et les pannes;
- Diagnostiquer et réparer les systèmes et les serveurs défectueux;
- Maintenir la sécurité du système au moyen de contrôles d'accès, de sauvegardes et d'autres contrôles, conformément aux politiques et aux procédures organisationnelles;
- Mettre en œuvre les politiques de cybersécurité, la sécurité des réseaux, la sécurité des applications, les contrôles d'accès et les mesures de protection des données organisationnelles;
- Élaborer de la documentation sur les procédures normalisées d'exploitation de l'administration des systèmes.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, technologies de l'information ou l'équivalent);
- Attestations constituant un atout : Professionnel certifié en sécurité des systèmes d'information (CISSP); Computing Technology Industry Association (CompTIA) Security+;
- Il est préférable d'avoir de la formation et de l'expérience en sécurité réseau – d'un à trois ans d'expérience au niveau d'entrée; cinq ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissances techniques, principes et méthodes de sécurité (p. ex. pare-feu, chiffrement), conception fonctionnelle et technique des réseaux et des systèmes, et solutions de cybersécurité;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Mesures ou indicateurs des problèmes de rendement, de disponibilité, de capacité ou de configuration du système;
- Outils d'analyse et protocoles de réseau;
- Techniques d'administration des systèmes et techniques de renforcement des réseaux et des systèmes d'exploitation;
- Systèmes d'exploitation des serveurs et des dispositifs clients;
- Concepts d'administration des systèmes;

- Configuration et optimisation de logiciels, de systèmes ou de serveurs;
- Sécurité du système et sauvegarde/récupération des données;
- Outils de diagnostic et techniques d'identification des défaillances.

Principales compétences

- Résolution de problèmes, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

6.3 CRYPTOGRAPHE/CRYPTANALYSTE

Description de travail de base

- Développer des algorithmes, des chiffres et des systèmes de sécurité pour chiffrer l'information.
- Analyser les systèmes de codage et décoder les messages.
- Concevoir et percer du code protégeant les renseignements personnels des organisations et des personnes en surveillant la sécurité en ligne des systèmes de données.

Principales tâches liées à la cybersécurité

- Protéger les renseignements importants contre l'interception, l'accès et la modification;
- Évaluer, analyser et cibler les faiblesses des systèmes et algorithmes de sécurité;
- Élaborer des systèmes de sécurité robustes pour prévenir les vulnérabilités;
- Élaborer des modèles statistiques et mathématiques pour analyser les données et régler les problèmes de sécurité;
- Mettre à l'essai les modèles computationnels pour en vérifier la fiabilité et l'exactitude;
- Faire de la recherche, déterminer 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.

Études, formation et expérience de travail fréquemment demandées

- Diplôme d'études postsecondaires en génie informatique, en informatique ou en mathématiques. Une maîtrise ou un doctorat en sciences est fortement préférable;
- Il est préférable d'avoir de la formation et de l'expérience dans le domaine de la cybersécurité ou de l'infrastructure de sécurité des TI – trois ans d'expérience au niveau d'entrée, cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Architecture informatique, structures de 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;
- C, C++, Java, Python et autres langages de programmation similaires;
- 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.);
- Lois, codes juridiques, règlements, politiques et éthique applicables en matière de cybersécurité.

Principales compétences

- Analyse, résolution de problèmes, gestion du temps, relations interpersonnelles et communications.

6.4 SPÉCIALISTE DU SOUTIEN TECHNIQUE

Description de travail de base

- Fournir un soutien technique à une organisation en fonction des composantes des processus, des systèmes et des protocoles établis ou approuvés.

Principales tâches liées à la cybersécurité

- Surveiller activement le rendement et l'état de santé du système informatique, 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 du système d'exploitation en fonction des politiques, des normes et des procédures organisationnelles;
- 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 et recommander des améliorations et des changements aux environnements informatiques;
- Administrer les comptes d'utilisateur, les privilèges d'accès à un réseau et l'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;

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, systèmes d'information ou l'équivalent);
- Il est préférable d'avoir de la formation et de l'expérience en soutien technique – d'un à trois ans d'expérience de travail connexe pour le niveau d'entrée; de cinq à sept ans d'expérience pour le niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système, des logiciels de cybersécurité, de la technologie infonuagique;
- Concepts liés à l'administration de systèmes, aux systèmes d'exploitation, aux microprocesseurs et à la gestion de l'identité et de l'accès;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Mesures ou indicateurs du rendement, de la convivialité et de la disponibilité des systèmes;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Opérations et processus relatifs aux incidents, aux problèmes de sécurité et à la gestion des événements;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Élaboration, mise à jour et tenue à jour des procédures opérationnelles normalisées ainsi que des rapports sur les incidents, les problèmes de sécurité ou les événements.

Principales compétences

- Analyse, résolution de problèmes, relations interpersonnelles et communications.

7 CONCEVOIR ET DÉVELOPPER

7.1 INGÉNIEUR DES INFRASTRUCTURES ESSENTIELLES

Description de travail de base

- Concevoir, construire, déployer et maintenir l'infrastructure de technologies de l'information (TI); veiller à ce que tous les systèmes TI soutiennent l'organisation de façon efficace.

Principales tâches liées à la cybersécurité

- Définir et examiner les systèmes d'information, les configurations et les contrôles 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 les exigences en matière de basculement ou de sauvegarde pour la restauration des systèmes;
- Planifier, effectuer des recherches et concevoir des solutions de sécurité robustes pour les systèmes et les réseaux;
- S'assurer que les systèmes acquis ou développés sont conformes aux politiques et aux pratiques en matière de cybersécurité;
- Effectuer la maintenance préventive courante de l'infrastructure réseau, y compris la mise en œuvre de logiciels et de mises à jour, et examiner les lacunes potentielles de l'infrastructure et les cybermenaces, et y remédier;
- Effectuer des tests de vulnérabilité ainsi que des évaluations des risques et de la sécurité;
- Documenter les défaillances du réseau et les mesures correspondantes prises pour assurer un registre détaillé des activités;
- Analyser et recommander des améliorations et des changements aux environnements informatiques;
- Assurer la sécurité des transferts d'information entre les systèmes et applications;
- Améliorer ainsi que planifier la capacité et la conception pour des projets d'ingénierie des infrastructures;
- Préparer des rapports techniques qui documentent le processus de développement des systèmes;
- Documenter et prendre en considération les exigences techniques d'une organisation en ce qui a trait à ses systèmes d'information tout au long du cycle de vie du système;
- Prêter conseils sur les exigences en matière de sécurité, les activités du processus de gestion des risques et d'autres documents connexes;
- Procéder à des examens de sécurité et donner des conseils sur les plans de continuité des activités, d'urgence et de reprise après sinistre;
- Élaborer des rapports de projet, des évaluations et d'autres documents pertinents;
- Intervenir en cas d'incident lié à la sécurité et fournir une analyse approfondie après l'événement;
- Définir, élaborer, mettre en œuvre et maintenir des politiques, des normes et des procédures en matière d'infrastructure;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique ou l'équivalent);
- Il est préférable d'avoir de la formation et de l'expérience dans le domaine de la cybersécurité ou de l'infrastructure de sécurité des TI – trois ans d'expérience au niveau d'entrée, cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Modèles d'ingénierie de la sécurité;
- 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 l'architecture informatique;
- Concepts relatifs à l'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;
- Protocoles de réseautage et processus de conception;
- 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.

Principales compétences

- Recherche, analyse, souci du détail, résolution de problèmes, organisation, relations interpersonnelles et communications.

7.2 ANALYSTE DES EXIGENCES

Description de travail de base

- Évaluer les exigences fonctionnelles et de sécurité des contrôles et des systèmes, et traduire les exigences en solutions de cybersécurité.

Principales tâches liées à la cybersécurité

- Définir la portée et les objectifs du projet en fonction des buts et des activités de l'organisation;
- Effectuer des recherches et des analyses pour élaborer, documenter et préciser les exigences fonctionnelles et de sécurité des contrôles et des systèmes;
- S'assurer que les exigences fonctionnelles et de sécurité sont conformes aux politiques et aux pratiques de cybersécurité de l'organisation et aux lignes directrices applicables de l'industrie;
- Consulter la direction et les collègues pour évaluer les exigences fonctionnelles et de sécurité;
- Traduire les exigences fonctionnelles et de sécurité en solutions de cybersécurité;
- Élaborer et documenter les exigences fonctionnelles et de sécurité, les capacités et les contraintes pour les procédures et processus de conception et de construction;
- Assurer la coordination avec les architectes de la sécurité, les ingénieurs de la sécurité et les développeurs, au besoin, pour assurer la surveillance du développement de solutions de cybersécurité;
- Surveiller la mise en œuvre des contrôles et des systèmes de sécurité en fonction des exigences fonctionnelles et de sécurité, et formuler des recommandations à cet égard;
- Cerner et documenter les risques liés aux solutions de cybersécurité et aux activités de l'organisation;
- Élaborer des évaluations des risques des contrôles et des systèmes, et des solutions de cybersécurité connexes, ou y participer;
- Effectuer des analyses pour déterminer les possibilités de trouver de nouvelles solutions et d'améliorer les solutions de cybersécurité de l'organisation;
- Élaborer et documenter le concept des opérations de sécurité du système.

Études, formation et expérience de travail fréquemment demandées

- Diplôme d'études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Computing Technology Industry Association (CompTIA); Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Les personnes qui occupent habituellement ce poste ont une vaste expérience des activités de cybersécurité. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, de la technologie d'alimentation électrique, des protocoles de système et des logiciels de cybersécurité;
- 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 l'architecture informatique;
- Concepts relatifs à l'architecture de sécurité et modèles de référence relatifs à l'architecture d'entreprise;
- Accès réseau, identité et gestion de l'accès;

- Techniques de gestion de la configuration sécurisée;
- Processus d'évaluation et d'autorisation de sécurité;
- Analyse des capacités et des besoins;
- 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;
- Exigences en matière de fonctionnalité, de qualité et de sécurité, et leur application à des composants et à des outils particuliers;
- Protocoles de réseautage et processus de conception;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Contrôles liés à l'utilisation, au traitement, au stockage et à la transmission des données.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.3 ARCHITECTE DE LA SÉCURITÉ

Description de travail de base

- Concevoir, élaborer et surveiller la mise en œuvre des structures de sécurité des réseaux et des ordinateurs pour une organisation, s'assurer 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.

Principales tâches liées à la cybersécurité

- Définir les besoins et examiner la technologie et 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 les exigences en matière de basculement ou de sauvegarde pour la restauration des systèmes;
- Planifier, effectuer des recherches et élaborer des architectures de sécurité robustes pour les systèmes et les réseaux;
- 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 et 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;
- Intervenir immédiatement en cas d'incident de sécurité et fournir une analyse approfondie après l'événement;
- Mettre à jour et mettre à niveau les systèmes de sécurité au besoin.

Études, formation et expérience de travail fréquemment demandées

- Diplôme d'études postsecondaires (universitaires) en génie informatique ou dans une discipline connexe. Spécialisation en cybersécurité ou en sécurité des TI souhaitable.
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Computing Technology Industry Association (CompTIA); Professionnel certifié en sécurité des systèmes d'information (CISSP); Professionnel en architecture de la sécurité des systèmes d'information (ISSAP);
- Il est préférable d'avoir de la formation et de l'expérience en matière d'infrastructure de sécurité des TI, d'analyse des besoins ou de gestion de programme – de cinq à dix ans d'expérience pertinente en TI pour un niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- 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 l'architecture informatique;
- Concepts relatifs à l'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;
- Protocoles de réseautage et processus de conception;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Cadres de conformité en matière de sécurité;
- Configuration et utilisation des outils de protection informatique basés sur des logiciels;
- Conception de solutions matérielles et logicielles.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.4 INGÉNIEUR DE LA SÉCURITÉ

Description de travail de base

- Développer et maintenir des solutions de sécurité robustes pour les réseaux et les systèmes d'une organisation, en veillant à ce que les exigences de sécurité soient adéquatement prises en compte dans tous les aspects de la conception des systèmes en fonction des normes et des pratiques de l'industrie, ainsi que des politiques et procédures de l'organisation, et donner des conseils sur les questions de sécurité et les vulnérabilités à toutes les étapes du cycle de vie du système.

Principales tâches liées à la cybersécurité

- Définir et examiner la technologie et les systèmes d'information, les configurations et les contrôles 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 les exigences en matière de basculement ou de sauvegarde pour la restauration des systèmes;
- Planifier, effectuer des recherches et concevoir des solutions de sécurité robustes pour les systèmes et les réseaux;
- Effectuer des tests de vulnérabilité ainsi que des évaluations des risques et de la sécurité;
- Enquêter sur les intrusions, mener des enquêtes judiciaires et préparer des interventions en cas d'incident;
- Collaborer avec des collègues sur des solutions d'authentification, d'autorisation et de chiffrement;
- Étudier et évaluer de nouvelles technologies et de nouveaux processus qui améliorent les capacités en matière de sécurité;
- Effectuer de la recherche et élaborer un contexte de sécurité des systèmes, et définir les exigences de sécurité des systèmes en fonction des normes de l'industrie ainsi que des politiques et pratiques de cybersécurité;
- S'assurer que les systèmes acquis ou développés sont conformes aux politiques et aux pratiques en matière de cybersécurité;
- Effectuer des examens de sécurité et déterminer les lacunes dans les architectures et les conceptions de sécurité (p. ex. pare-feu, réseaux privés virtuels, routeurs, serveurs, etc.);
- Préparer des rapports techniques qui documentent le processus de développement des systèmes;
- Documenter et traiter les exigences de l'organisation en matière de sécurité de l'information et de sécurité des systèmes tout au long du cycle de vie des systèmes;
- Prêter conseils sur les exigences en matière de sécurité, les activités du processus de gestion des risques et d'autres documents connexes;
- Procéder à des examens de sécurité et donner des conseils sur les plans de continuité des activités, d'urgence et de reprise après sinistre;
- Intervenir en cas d'incident lié à la sécurité et fournir une analyse approfondie après l'événement;
- Mettre à jour et mettre à niveau les systèmes de sécurité au besoin.

Études, formation et expérience de travail fréquemment demandées

- Diplôme d'études postsecondaires (universitaires) en génie informatique, en informatique ou dans une discipline connexe. Spécialisation en cybersécurité ou en sécurité des TI souhaitable;
- Au Canada, le terme « ingénieur » désigne un ingénieur professionnel agréé, conformément aux règles d'agrément de l'administration provinciale. Ainsi, tous les ingénieurs de la sécurité doivent être agréés pour exercer la profession d'« ingénieur » dans leur province;

- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP); Professionnel certifié en ingénierie de la sécurité des systèmes d'information (ISSEP);
- Il est préférable d'avoir de la formation et de l'expérience en matière d'infrastructure de sécurité des TI, d'analyse des besoins ou de gestion de programme – de cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Modèles d'ingénierie de la sécurité;
- 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 l'architecture informatique;
- Concepts relatifs à l'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;
- Protocoles de réseautage et processus de conception;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Cadres de conformité en matière de sécurité;
- Configuration et utilisation des outils de protection informatique basés sur des logiciels;
- Conception de solutions matérielles et logicielles.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.5 CHERCHEUR EN CYBERSÉCURITÉ

Description de travail de base

- Étudier et évaluer les technologies actuelles et nouvelles afin de développer des capacités et de veiller à ce que la cybersécurité soit pleinement intégrée;
- Mobiliser et maintenir un réseau de recherche professionnelle aligné sur les exigences organisationnelles

Principales tâches liées à la cybersécurité

- Faire des recherches sur les technologies actuelles et nouvelles pour comprendre les capacités des réseaux ou systèmes requis;
- Concevoir et mettre au point de nouveaux outils ou de nouvelles technologies en matière de cybersécurité;
- Collaborer avec des collègues pour définir et développer des solutions technologiques appropriées;
- Respecter les normes et les processus relatifs au cycle de vie des logiciels et des systèmes;
- Résoudre les problèmes de conception et de processus des prototypes tout au long des phases de développement des produits;
- Évaluer les vulnérabilités du réseau ou du système afin d'améliorer les capacités en cours de développement;
- Documenter et présenter les résultats de recherche aux intervenants appropriés;
- Participer à des forums de recherche et de développement et à des événements connexes;
- Élaborer et fournir le matériel de formation, et surveiller les efforts d'éducation;

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certification en assurance de l'information globale (GIAC); Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Formation et expérience liées aux activités de sécurité ou d'évaluation et de mise à l'essai de la sécurité. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Technologies actuelles et nouvelles, et technologies de cybersécurité;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Systèmes des infrastructures essentielles;
- Concepts d'architecture de sécurité réseau, y compris la topologie, les protocoles, les composants et les principes;
- Structures et fonctionnement interne du système d'exploitation;
- Outils d'analyse réseau;
- Application des concepts et des processus d'ingénierie;
- Création et utilisation de modèles mathématiques;
- Conception de processus et de solutions technologiques.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.6 TESTEUR ET ÉVALUATEUR DE LA SÉCURITÉ

Description de travail de base

- Planifier, préparer et mettre 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; documenter les résultats et formuler des recommandations qui peuvent améliorer la confidentialité, l'intégrité et la disponibilité de l'information.

Principales tâches liées à la cybersécurité

- 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; 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;

Études, formation et expérience fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique ou l'équivalent);
- Attestations constituant un atout : Professionnel certifié en sécurité des systèmes d'information (CISSP);
- Formation et expérience dans un rôle de sécurité des TI associé à la mesure de la sécurité des systèmes et/ou des logiciels, comme l'évaluation des vulnérabilités et la sécurité des logiciels. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Effectuer des tests indépendants de validation et de vérification de la sécurité;
- Méthodes et techniques d'essai et d'évaluation 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.

Principales compétences

- Analyse, résolution de problèmes, souci du détail, relations interpersonnelles et communications.

7.7 ANALYSTE DE L'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Description de travail de base

- Recueillir et analyser 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, et prêter conseils et orientation pour aider à réduire ces risques de la chaîne d'approvisionnement.

Principales tâches liées à la cybersécurité

- 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 politiques et les procédures de cybersécurité;
- Assurer la conformité aux politiques, aux règlements et aux procédures de l'organisation en matière de cybersécurité;
- Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation;
- Élaborer et tenir à jour des évaluations des risques et des rapports connexes sur les fournisseurs et les produits et services, en fonction de la fiabilité et de la crédibilité.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. administration des affaires, génie informatique, informatique, technologies de l'information ou l'équivalent);
- Il est souhaitable d'avoir une formation et de l'expérience en sécurité réseau.
- Les personnes qui remplissent ce rôle peuvent avoir divers niveaux d'expertise en cybersécurité. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Techniques d'analyse de l'information et des données;
- Connaissance pratique des principes et des méthodes de cybersécurité et de protection des renseignements personnels (p. ex. pare-feu, chiffrement, dispositifs de réseau privé virtuel);
- Connaissances techniques pour comprendre la sécurité et l'intégrité des données, les exigences de sécurité, ainsi que la conception fonctionnelle et technique des réseaux et des systèmes, et les solutions de cybersécurité;
- Processus, responsabilités et pouvoirs en matière de gestion des risques;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Gestion de la configuration liée à la cybersécurité;
- Lois, règlements et lignes directrices applicables en matière de cybersécurité;
- Élaboration d'évaluations des menaces et des risques.

Principales compétences

- Analyse, résolution de problèmes, souci du détail, organisation, gestion du temps, relations interpersonnelles et communications.

7.8 DÉVELOPPEUR D'APPLICATIONS

Description de travail de base

- Concevoir, développer, tester et améliorer des logiciels et des applications visant à aider une organisation à réaliser des tâches ou des programmes.

Principales tâches liées à la cybersécurité

- Chercher, analyser et utiliser des techniques de développement d'applications sécurisées;
- Élaborer, mettre en œuvre et modifier des applications à l'aide d'analyses scientifiques et de modèles mathématiques;
- Analyser les exigences du code pour déterminer les contraintes de temps et de coûts, ainsi que les risques pour l'organisation;
- Élaborer et mener des procédures de mise à l'essai et de validation des applications, de programmation et de codage sécurisé, et faire rapport sur la fonctionnalité et la résilience;
- Effectuer des analyses des vulnérabilités et des examens des applications, et examiner les contrôles et les mesures nécessaires pour protéger les applications;
- Effectuer des essais des applications pour s'assurer que l'information voulue est produite et que les niveaux de sécurité et les procédures sont appropriés;
- Préparer la documentation sur les applications et les révisions subséquentes;
- Mettre à jour et mettre à niveau les applications au besoin pour corriger les erreurs et améliorer le rendement et les interfaces;
- Préparer des rapports sur les correctifs ou les versions d'applications qui rendraient les systèmes vulnérables;
- Élaborer des contre-mesures contre l'exploitation potentielle de vulnérabilités dans les applications;
- Effectuer une analyse des risques chaque fois qu'une application fait l'objet d'une modification;
- Prêter conseils et orientation et coordonner les efforts d'application des procédures de sécurité afin de protéger les données sensibles contre les menaces et les vulnérabilités.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. génie informatique, informatique ou l'équivalent). Il est préférable d'avoir une maîtrise;
- Il est préférable de posséder de la formation et de l'expérience dans la conception et le développement d'applications – de deux à trois ans d'expérience au niveau d'entrée et de cinq à dix ans d'expérience au niveau avancé. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Concepts et fonctions des systèmes de sécurité des applications;
- Outils, méthodes et techniques de conception de logiciels et de systèmes;
- Méthodologies, essais et protocoles d'analyse des logiciels;
- Techniques de codage et de configuration sécurisés;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Architecture informatique, structures des données et algorithmes;

- Algèbre linéaire/matricielle et/ou mathématiques discrètes;
- Théorie des probabilités et théorie de l'information;
- C, C++, Java, Python et autres langages de programmation similaires;
- Principes de la programmation informatique, de la conception et du débogage de logiciels et des essais;
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels;
- Création ou adaptation des programmes et du code en fonction des préoccupations propres à l'application;
- Méthodes et processus de mise à l'essai et d'évaluation de la sécurité;
- Conduite d'analyses des vulnérabilités et établissement des vulnérabilités dans les systèmes de sécurité;
- Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données;
- Conception de contre-mesures aux risques de sécurité cernés;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Élaboration et exécution d'évaluations des risques ou des répercussions, d'analyses de rentabilisation et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.9 DÉVELOPPEUR EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Description de travail de base

- Développer, créer, intégrer, tester et maintenir la sécurité du système d'information tout au long du cycle de vie des systèmes, et rendre compte du rendement du système en assurant la confidentialité, l'intégrité et la disponibilité, et recommander des mesures correctives pour corriger les lacunes.

Principales tâches liées à la cybersécurité

- 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;
- Planifier, chercher et mettre en œuvre des systèmes d'information sécurisés à l'aide d'analyses scientifiques et de modèles mathématiques;
- Faire des recherches sur les technologies actuelles et nouvelles pour comprendre les capacités des réseaux ou systèmes requis;
- 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, de la programmation et du codage sécurisé, et rendre compte de la fonctionnalité et de la résilience;
- Effectuer des tests de vulnérabilité et des 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 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;
- Élaborer 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 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;
- 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;
- Prêter conseils et orientation et coordonner les efforts sur les procédures de gestion des risques et de reprise après sinistre afin de protéger les données sensibles contre les menaces et les vulnérabilités

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, mathématiques, technologie de réseaux, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certified Secure Software Lifecycle Professional (CSSLP);
- Il est préférable de posséder une formation et de l'expérience en développement et en soutien de systèmes – cinq ans d'expérience. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, des protocoles de système et des logiciels de cybersécurité;
- Principes dans les domaines de la sécurité de l'information, de l'ingénierie, du réseautage et des mathématiques;
- Concepts de la cryptographie et de la gestion des clés cryptographiques;
- Concepts dans les systèmes d'exploitation, les microprocesseurs, l'accès au réseau, la gestion de l'identité et de l'accès, et les tests de pénétration;
- Conceptions et fonctions de sécurité des données, méthodes d'analyse, tests et protocoles;
- Outils, méthodes et techniques de conception de systèmes;
- Techniques de codage et de configuration sécurisés;
- Architecture informatique, structures des données et algorithmes;
- Théorie des probabilités et théorie de l'information;
- C, C++, Java, Python et autres langages de programmation similaires;
- 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;
- Conduite d'analyses des vulnérabilités et établissement des vulnérabilités dans les systèmes de sécurité;
- Protocoles de réseautage et processus de conception;
- Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données;
- Conception de contre-mesures aux risques de sécurité cernés;
- Politiques, exigences et pratiques en matière de gestion des risques;
- Planification de la continuité des activités et de l'intervention en cas de sinistre;
- Analyse coûts-avantages;
- Connaissance pratique des principes et des éléments de cybersécurité;
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation;
- Élaboration et exécution d'évaluations des risques ou des répercussions, d'analyses de rentabilisation et de documents de gestion des risques.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

7.10 DÉVELOPPEUR DE LOGICIELS SÉCURISÉS

Description de travail de base

- Développer, créer, intégrer et maintenir des logiciels, des applications ou des programmes spécialisés de sécurité, et faire rapport sur les réalisations en matière de sécurité des logiciels et des données, et recommander des mesures correctives pour corriger les lacunes.

Principales tâches liées à la cybersécurité

- Chercher, analyser et utiliser des techniques de développement d'applications sécurisées;
- Élaborer, mettre en œuvre et modifier des systèmes ou des applications logiciels à l'aide d'analyses scientifiques et de modèles mathématiques;
- Analyser les besoins en logiciels afin de cerner les contraintes de temps et de coûts, ainsi que les risques pour l'organisation;
- 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;
- 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;
- Effectuer des essais de systèmes ou d'applications logiciels pour s'assurer que l'information voulue est produite et que les niveaux et procédures de sécurité sont appropriés;
- Préparer des rapports sur les développements du système ou de l'application et les révisions subséquentes;
- Mettre à jour et mettre à niveau les logiciels ou les applications, au besoin, pour corriger les erreurs et améliorer le rendement et les interfaces;
- Préparer des rapports sur les logiciels, 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;
- Prêter conseils et orientation et coordonner les efforts d'application des procédures de sécurité afin de protéger les données sensibles contre les menaces et les vulnérabilités.

Études, formation et expérience de travail fréquemment demandées

- Études postsecondaires dans un domaine lié à la cybersécurité ou aux TI (p. ex. informatique, mathématiques, technologie de réseaux, génie informatique ou l'équivalent);
- Attestations constituant un atout : Certified Secure Software Lifecycle Professional (CSSLP);
- Il est souhaitable d'avoir une formation et de l'expérience en développement de logiciels ou en codage – cinq ans d'expérience. L'expérience demandée dépendra du besoin organisationnel.

Exigences primaires en matière de formation technique – Résultats d'apprentissage

- Connaissance technique des réseaux, des composants informatiques, de la technologie d'alimentation électrique, des protocoles de système et des logiciels de cybersécurité;
- Principes de la programmation informatique, de la conception et du débogage de logiciels et des tests de pénétration;
- Concepts et fonctions des systèmes de sécurité des applications;
- Conceptions et fonctions de sécurité des données;

- Outils, méthodes et techniques de conception de logiciels et de systèmes;
- Méthodologies, essais et protocoles d'analyse de la sécurité des logiciels et des données;
- Techniques de codage et de configuration sécurisés;
- Architecture informatique, structures des données et algorithmes;
- Algèbre linéaire/matricielle et/ou mathématiques discrètes;
- Théorie des probabilités et théorie de l'information;
- C, C++, Java, Python et autres langages de programmation similaires;
- Création ou adaptation de programmes et de code en fonction des préoccupations propres à l'application;
- Conduite d'analyses des vulnérabilités et établissement des vulnérabilités dans les systèmes de sécurité;
- Menaces, risques et vulnérabilités liés à la sécurité des systèmes, des applications et des données;
- Conception de contre-mesures aux risques pour la sécurité cernés.

Principales compétences

- Recherche, analyse, résolution de problèmes, relations interpersonnelles et communications.

8 CONTENU COMPLÉMENTAIRE

8.1 LISTE D'ACRONYMES, D'ABRÉVIATIONS ET DE SIGLES

Acronyme, abréviation ou sigle	Définition
CCC	Centre canadien pour la cybersécurité
CISSP	Professionnel certifié en sécurité des systèmes d'information
CompTIA	*Computing Technology Industry Association*
CSSLP	*Certified Secure Software Lifecycle Professional*
CST	Centre de la sécurité des télécommunications
CWF	*Cybersecurity Workforce Framework*
DPI	Dirigeant principal de l'information
DPS	Dirigeant principal de la sécurité
DPSI	Dirigeant principal de la sécurité de l'information
EMR	Évaluation des menaces et des risques
GCSI	Gestionnaire certifié en sécurité de l'information
GIAC	Certification en assurance de l'information globale (*Global Information Assurance Certification*)
IAPP	*International Association of Privacy Professionals*
NICE	*National Initiative on Cybersecurity Education* (É.-U.)
OSCP	Professionnel certifié de sécurité offensive
SFIA	*Skills Framework for the Information Age* (Global IT)
SI	Système d'information
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TIC	Technologies de l'information et des communications
TTP	Tactiques, techniques et procédures

9 DOCUMENTS DE RÉFÉRENCE

[1] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Josang, T. Pereira and E. Stavro, « Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline, » dans *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE Companion '18)*, Larnaca, 2018.

[2] Association for Computing Machinery (ACM); IEEE Computer Society (IEEE-CS); Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC); International Federation for Information Processing Technical, « Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity », 2017.

[3] Sécurité publique Canada, « Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique », Ottawa, 2018.

[4] Rapid7 Labs, « National Exposure Index », 7 juin 2018. [En ligne] Accessible à : https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf. [consulté en juillet 2019].

[5] ITAC Talent, « Canadianization of the NICE Cybersecurity Workforce Framework: A Proposed Model », Mississauga, 2019.

[6] D. O'Brien, « Internet Security Threat Report: Ransomware 2017 », Symantec, 2017.

[7] J. Porup, « What is cyber security? How to build a cyber security strategy », CSO Online, 27 décembre 2017. [En ligne]. Accessible à : https://www.csoonline.com/article/3242690-what-is-cyber-security-how-to-build-a-cyber-security-strategy.html. [Consulté en juillet 2019]

[8] US Department of Homeland Security, « Cybersecurity Careers of the Future », 2018.

10 ANNEXE A : MÉTHODOLOGIE ET ANALYSE

Le Centre de la sécurité des télécommunications (CST) a effectué une analyse de l'environnement des programmes d'études universitaires entre 2016 et 2017 afin de déterminer les programmes et les cours liés à la cybersécurité actuellement offerts dans les établissements d'enseignement postsecondaire partout au Canada. Cette analyse a par la suite été mise à jour en 2018. Les programmes ont été recensés au moyen de recherches par mots-clés, principalement au moyen du moteur de recherche universitystudy.ca et d'autres sites Web comme canadian-universities.net, studyincanada.com et ontariocolleges.ca, ainsi que de recherches dans Google. Pour chaque analyse, plusieurs recherches différentes ont été effectuées en utilisant les termes « sécurité », « cybersécurité », « sécurité informatique », « système d'information » et « réseau ».

L'analyse de l'environnement a porté sur deux typologies, à savoir les programmes propres à la cybersécurité, de nature surtout technique, et les programmes liés aux activités, de nature essentiellement non technique. L'analyse a porté sur les diplômes collégiaux, les programmes universitaires de premier cycle et les programmes d'études supérieures. Les programmes désignés comme des programmes propres à la cybersécurité comprenaient des disciplines liées à l'informatique ou aux TI, comme l'informatique, le génie informatique ou des communications, le développement de logiciels et l'administration de systèmes TI, où il y avait d'importantes composantes de cybersécurité, ainsi que des cours spécialisés de TI ou de cybersécurité. Les programmes désignés comme liés au domaine des affaires ont été examinés afin de déterminer dans quelle mesure les concepts et les principes de cybersécurité ont été intégrés. Ce volet comprenait des programmes comme l'administration des affaires, les communications, les finances, la gestion et la gestion de projet.

En plus de l'analyse de l'environnement et de l'analyse subséquente de ces résultats, une quantité importante de renseignements anecdotiques ont été recueillis auprès d'experts en la matière, de conseils d'entreprises, d'associations professionnelles, de groupes communautaires et d'autres intervenants qui ont renforcé les résultats.

10.1 PRINCIPALES CONCLUSIONS

En résumé, la première analyse et l'analyse subséquente ont révélé ce qui suit :

- Le nombre et la qualité des cours et des programmes universitaires et collégiaux augmentent d'année en année;
- Les programmes universitaires et collégiaux visent principalement à former des diplômés prêts pour le marché du travail;
- La plupart des cours et des programmes universitaires et collégiaux se trouvaient dans des facultés techniques (p. ex. informatique, TI, etc.). Ils se concentraient principalement sur les rôles liés aux opérations de sécurité : détecter les cybermenaces, y réagir et les atténuer.
- Pour les programmes de génie informatique ou de génie des communications, il semblait y avoir très peu de contenu lié à la cybersécurité ou à la sécurité en général dans les exigences du programme.
- Certains cours ou programmes portant la mention « cybersécurité » portent uniquement sur certains aspects de la cybersécurité ou constituent une refonte des cours de TI existants pour y inclure certains éléments de cybersécurité. Tout en contribuant aux exigences fondées sur les rôles, ces cours ou programmes pourraient peut-être être mieux étiquetés pour indiquer l'orientation du programme (p. ex., les opérations de cybersécurité ou le traitement des incidents de cybersécurité).
- Certains cours ou programmes universitaires et collégiaux portant la mention « cybersécurité » reflètent la nature interdisciplinaire du domaine. Tout en répondant aux besoins éducatifs généraux des généralistes ou de ceux qui peuvent être employés à proximité de la cybersécurité, ils ne fournissent souvent pas

suffisamment de renseignements pour appuyer des responsabilités particulières en matière de cybersécurité au sein d'une organisation.

- Certains cours et programmes de cybersécurité n'ont pas attiré suffisamment d'inscriptions pour être viables d'une année à l'autre. Certains qui étaient planifiés et annoncés ne suscitaient pas suffisamment d'intérêt pour être offerts.
- Peu de programmes dans le domaine des affaires avaient un contenu intégré pertinent en matière de cybersécurité qui s'applique aux organisations.
- Les sujets pertinents, mais sous-représentés, étaient les suivants : le contexte juridique et stratégique canadien, y compris la protection des renseignements personnels et la protection de la vie privée; les considérations éthiques, y compris le milieu de travail et les pratiques d'enquête dans les contextes organisationnels; la gestion intégrée des risques, les communications opérationnelles et les nouveaux enjeux.

11 ANNEXE B : PROGRAMMES POSTSECONDAIRES LIÉS À LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité reçoit régulièrement des demandes de renseignements sur les possibilités d'éducation et de formation en cybersécurité. Plusieurs établissements d'enseignement ont mis en place des programmes ou parcours d'études dans le cadre de programmes existants qui peuvent servir d'exemples ou de modèles pour l'ensemble de la collectivité. Si un établissement ou un organisme estime offrir un programme ou un cours qui devrait être considéré comme un exemple ou un modèle, veuillez le soumettre par courriel à contact@cyber.gc.ca.

Établissement	Province	Titre du programme	Certification
Collège Alison	Alberta	Information Technology and Cyber Security	Diplôme
Collège Algonquin	Ontario	Computer Systems Technology - Security (un an supplémentaire au Computer Systems Technician Program)	Diplôme
Université Athabasca	Alberta	Post-Baccalaureate Certificate in Information Security (PBC-IS)	Certificat
Collège Bow Valley	Alberta	Cybersecurity	Certificat
British Columbia Institute of Technology	Colombie-Britannique	Forensic Investigation - Digital Forensics and Cybersecurity Option	Certificat
		Network Administration and Security Professional (NASP)	
		Industrial Network Cybersecurity	Diplôme
		Computer Systems - Network Security Administration Option	Baccalauréat
		Computer Systems - Network Security Applications Development Option	
		Forensic Investigation - Digital Forensics and Cybersecurity Option	
		Bachelor of Technology in Computer Systems, Network Security Applications Development	
Université Carleton	Ontario	Graduate Diploma in Infrastructure Protection and International Security	Diplôme
		Master of Infrastructure Protection and International Security	Maîtrise

Établissement	Province	Titre du programme	Certification
		Computer and Internet Security	Baccalauréat
Cégep de l'Outaouais	Québec	Techniques de l'informatique – Programmation et sécurité	Diplôme d'études collégiales (DEC) technique
		Techniques de l'informatique – Réseaux et cybersécurité	
Cégep de Saint-Hyacinthe	Québec	Techniques de l'informatique – Réseaux et cybersécurité	Diplôme d'études collégiales (DEC) technique
Cégep de Sherbrooke	Québec	Cybersécurité et sécurité intégrée	Attestation d'études collégiales (AEC)
Cégep Garneau	Québec	Cyberenquête	Attestation d'études collégiales (AEC)
Cégep Limoilou	Québec	Techniques de l'informatique – Gestion des réseaux	Diplôme d'études collégiales (DEC) technique
Cégep Saint-Jean-sur-Richelieu	Québec	Administration des réseaux et sécurité informatique	Attestation d'études collégiales (AEC)
Centennial College	Ontario	Cybersecurity	Certificat d'études supérieures
College of the North Atlantic	Newfoundland	Cyber Security Infrastructure	Diplôme
Collège Ahunstic	Québec	Réseautique et sécurité informatique	Attestation d'études collégiales (AEC)
		Techniques de l'informatique – profil réseaux et sécurité	Diplôme d'études collégiales (DEC) technique
Collège CDI	Québec	Gestionnaire en réseautique : Spécialiste sécurité	Attestation d'études collégiales (AEC)

Établissement	Province	Titre du programme	Certification
	Alberta	Cyber Security Specialist	Certificat
	Manitoba	Network and Internet Security Specialist	Certificat
Collège communautaire du Nouveau-Brunswick	Nouveau-Brunswick	Réseautique et sécurité Informatique	Diplôme
		Cybersécurité	
Collège de Bois-de-Boulogne	Québec	Sécurité informatique et réseautique	Attestation d'études collégiales (AEC)
		Techniques de l'informatique – Profil Infrastructures et sécurité	Diplôme d'études collégiales (DEC) technique
Collège de Maisonneuve	Québec	Gestion de réseaux et sécurité des systèmes	Attestation d'études collégiales (AEC)
		Techniques de l'informatique – Infrastructure et sécurité des réseaux	Diplôme d'études collégiales (DEC) technique
Collège La Cité	Ontario	Technologies de l'information – sécurité informatique	Diplôme
Collège LaSalle	Québec	Techniques de l'informatique – Gestion de réseaux et sécurité	Diplôme d'études collégiales (DEC) technique
Collège Lionel-Groulx	Québec	Administration des réseaux et sécurité informatique	Attestation d'études collégiales (AEC)
Collège Montmorency	Québec	Techniques de l'informatique – Spécialisation : Réseaux et sécurité informatiques	Diplôme d'études collégiales (DEC) technique
Collège Rosemont	Québec	Microprogramme de perfectionnement en sécurité des réseaux	Attestation d'études collégiales (AEC)

Établissement	Province	Titre du programme	Certification
		Techniques de l'informatique – Profil réseautique : sécurité et virtualisation	Diplôme d'études collégiales (DEC) technique
Université Concordia	Québec	Information Systems Security (MASc)	Maîtrise
		Information Systems Security (MEng)	
Université Concordia d'Edmonton	Alberta	Graduate Diploma in Information Assurance	Diplôme
		Graduate Diploma in Information Security	
		Master of Information Systems Assurance Management	Maîtrise
		Master of Information Systems Security Management	
Collège Conestoga	Ontario	Network Security Investigations	Certificat
		Cyber Security	Certificat d'études supérieures
		Computer Application Security	
		Information Technology Network Security	
Durham College	Ontario	Information Systems Security – Computers and Networking	Certificat d'études supérieures
Collège Eastern	Nouveau-Brunswick	Advanced Systems Management and Cyber Security	Diplôme
Collège Fanshawe	Ontario	Cyber Security	Diplôme
		Information Security Management	Certificat d'études supérieures
		Network and Security Architecture	
Collège Fleming	Ontario	Computer Security and Investigations	Diplôme
Collège George Brown	Ontario	Network Security Fundamentals Certificate	Certificat

Établissement	Province	Titre du programme	Certification
		Information Security Management Certificate	
		Network and System Security Analysis	Certificat d'études supérieures
Georgian College	Ontario	Information Systems Security	Certificat d'études supérieures
HEC Montréal	Québec	Certificat en analyse de la sécurité de l'information et des systèmes	Certificat
Cégep Heritage College	Québec	Administrateur de la sécurité et du réseau de Microsoft	Attestation d'études collégiales (AEC)
Collège Humber	Ontario	Cyber Crime Specialist	Certificat
Institut supérieur d'informatique	Québec	Réseaux informatiques et sécurité	Attestation d'études collégiales (AEC)
		Réseaux Informatiques et sécurité	
Collège Lambton	Ontario	Cyber Security and Computer Forensics	Certificat d'études supérieures
		Cyber Security	
		Cyber Infrastructure Specialist	
Collège Loyalist	Ontario	Cyber Security	Certificat
Manitoba Institute of Trades and Technology	Manitoba	Network Security Diploma	Diplôme
		Cyber Defence and Cloud Administration Diploma	
Mohawk College	Ontario	Computer Systems Technology - Network Engineering and Security Analyst	Diplôme
		Cyber Security Analytics	Certificat d'études supérieures

Établissement	Province	Titre du programme	Certification
Université Mount Royal	Alberta	Cyber Security Fundamentals	Certificate
		Advanced Cyber Security	Certificate
Collège communautaire du Nouveau-Brunswick	Nouveau-Brunswick	Information Technology: Cybersecurity	Post-graduate diploma
New York Institute of Technology	Colombie-Britannique	Master of Information, Network, and Computer Security	Maîtrise
Université Northeastern	Ontario	Master of Science in Cybersecurity	Maîtrise
Northern Alberta Institute of Technology	Alberta	Core Security+ Certificate	Certificat
		Enterprise Security Certificate	
		System Security Certificate	
Collège communautaire de la Nouvelle-Écosse	Nouvelle-Écosse	Cyber Security	Diplôme
		IT Systems Management and Security	
Okanagan College	Colombie-Britannique	Blockchain Certificate	Certificat
Oulton College	Nouveau-Brunswick	System Management and Cyber Security	Diplôme
Polytechnique Montréal	Québec	Certificat en Cyberenquête	Certificat
		Certificat en cyberfraude	
		Certificat en Cybersécurité des réseaux informatiques	
		Undergraduate microprogram in Networking and Security	Microprogramme

Établissement	Province	Titre du programme	Certification
		Microprogramme de 1er cycle en Cyberinvestigation	
		Microprogramme de 1er cycle en Réseautique et sécurité	
Collège QCT	Alberta	Cyber Security Specialist	Diplôme
Université Queens	Ontario	NSERC CREATE Cybersecurity	
Collège Red River	Manitoba	Information Security	Diplôme d'études supérieures
Collège Robertson	Alberta	Network Security Technician	Diplôme
Université Ryerson	Ontario	Computer Security and Digital Forensics	Certificat
		MBA in Management of Technology and Innovation, Data Security and Privacy Specialization	Maîtrise
Saskatchewan Polytechnic	Saskatchewan	Cyber Security	Post-graduate Certificate
Collège Sault	Ontario	Network Architecture and Security Analytics	Certificat d'études supérieures
		Cyber Security Canadian Context	Certificat
Collège Seneca	Ontario	Honours Bachelor of Technology - Informatics and Security	Baccalauréat
		Cyber Security and Threat Management	Certificat
		Cyber Security	Certificat d'études supérieures
Collège Sheridan	Ontario	Honours Bachelor of Applied Information Sciences (Information Systems Security)	Baccalauréat
		Cybersecurity - Legal and Ethical Policies and Procedures	Recognition of achievement
		Cybersecurity Foundations	
	Alberta	Cyber Security for Control Systems	Certificat

Établissement	Province	Titre du programme	Certification
Southern Alberta Institute of Technology		Information Security Analyst	
		Information Systems Security	
		IT Security Certificate of Achievement	
The King's University	Alberta	Computer Science – Cyber Security Stream	Baccalauréat
Université de Moncton	Nouveau-Brunswick	Certificat en gestion de la sécurité de l'information des entreprises	Certificat
Université de Sherbrooke	Québec	Gouvernance, audit et sécurité des technologies de l'information	Diplôme d'études supérieures spécialisées (DESS)
		Gouvernance, audit et sécurité des technologies de l'information	Microprogramme
		Gouvernance, audit et sécurité des technologies de l'information (GASTI)	Maîtrise
University of Alberta	Alberta	Information Access and Protection of Privacy	Certificat
Université de Calgary	Alberta	Bachelor of Computer Science (Security Concentration Option)	Baccalauréat
		Graduate Certificate in Network Security	Certificat d'études supérieures
		Graduate Certificate in Software Security	
Université de Guelph	Ontario	Certificate in Information Management, Privacy, and Access	Certificat
		Cybersecurity Threat Intelligence Program	Maîtrise
Université du Nouveau-Brunswick	Nouveau-Brunswick	Computer Science (Cybersecurity specialization)	Baccalauréat
		Cyber Security	Maîtrise
University of Ontario Institute of Technology	Ontario	Information Technology (Honours) – Bridge	Baccalauréat
		Information Technology (Honours) Networking and Information Technology Security	

Établissement	Province	Titre du programme	Certification
		Information Technology (Honours) Networking and Information Technology Security – Advanced Entry	
		Information Technology Security	Maîtrise
University of Toronto	Ontario	Computer Science (H.B.Sc.) Specialist Program in Information Security	Baccalauréat
	Ontario	Certificate in Cyber Security Management	Certificat
		M. Eng. in Communications with focus on Identity, Privacy and Security (IPS)	Maîtrise
		Master of Information, with a Specialization in Identity, Privacy and Security	
Université de Victoria	Colombie-Britannique	Master of Engineering in Telecommunications and Information Security (MTIS)	Maîtrise
Université de Waterloo	Ontario	Graduate Diploma (GDip) in Computer Networking and Security	Diplôme
Université de Winnipeg	Manitoba	Information Assurance and Security Certificate	Certificat
		Network Security Diploma	Diplôme
Willis College	Ontario	Cyber Security Analyst Diploma Program	Diplôme
Université York	Ontario	Certificate in Advanced Cyber Security	Certificat
		Certificate in Cyber Security	
		Certificate in Cyber Security Fundamentals	
		Computer Security (BSc, BA)	Baccalauréat
		LLM in Privacy and Cybersecurity Law	Maîtrise