**Les compétences des professionnels en cybersécurité dans les organisations du secteur financier canadien.**

Par Marc-André Léger, PHD, MScA (MIS), MBA, Adm.A.  
Université du Québec en Outaouais  
**Contact:**  [marcandre@leger.ca](mailto:marcandre@leger.ca)  
**Mots-clés:**  sécurité de l’information, cybersécurité, compétence, KSA

**Résumé :** Cet article présente les compétences et les éléments de compétence exigés des professionnels de la cybersécurité qui ont été identifiés lors d’une étude sur les compétences en cybersécurité dans les institutions financières canadiennes, entre 2019 et 2021. L’objectif principal de cet article est d’aider les institutions financières et les établissements d’enseignement à concevoir et à mettre en œuvre des programmes de formation continue axés sur les compétences. Les institutions financières peuvent utiliser cet article et les données qui soutiennent les recommandations pour les aider à accroître l’expertise des travailleurs de la cybersécurité. Les collèges et universités peuvent trouver cet article intéressant pour les aider à concevoir de nouveaux programmes ou à améliorer des programmes existants.

# Introduction

Les organisations financières canadiennes font face à de multiples défis en matière de cybersécurité dans le monde d’aujourd’hui. Depuis 2019, accéléré par la crise du COVID, une dépendance accrue aux technologies connectées combinée à une montée en puissance de la cybercriminalité a augmenté la pression sur les équipes de cybersécurité. Bien que cela puisse être abordé de plusieurs façons, nous avons choisi d’étudier la question des compétences des acteurs en cybersécurité, au cœur de nos intérêts de chercheurs et d’enseignants dans le domaine de la gestion des technologies d’affaires. Il est bien documenté que le facteur humain est une source importante de vulnérabilité, ce qui entraîne une augmentation du risque. Les individus qui occupent des postes en cybersécurité sont l’une des nombreuses sources de ces vulnérabilités du facteur humain, en raison de leur rôle central dans l’exploitation, la surveillance et le support des activités de cybersécurité, jouent un rôle clef dans le bon fonctionnement des technologies de l’information qui soutiennent les activités commerciales des entreprises. Ainsi, une hypothèse sous-jacente à notre enquête empirique est que des acteurs plus compétents conduiront à une réduction du risque inacceptable. Dans cet article, nous présentons quelques-uns des résultats d’une étude réalisée dans une grande institution financière canadienne, entre 2019 et 2021.

# Méthodologie de l’étude de recherche

L’étude qualitative qui fut réalisée a adopté l’Action Design Research (ADR) pour mettre en œuvre la méthodologie de recherche Design Science (Mullarkey & Hevner, 2019). L’ADR a été choisi parce que cette méthodologie a été déployée avec succès dans un cadre organisationnel pour générer des connaissances grâce à un processus itératif de construction et d’évaluation des artefacts (Keijzer-Broers & de Reuver, 2016; McCurdy et coll., 2016; Sein et coll., 2011). Grâce à de multiples itérations du cycle bâtir, intervenir et évaluer, le cycle BIE, la question de recherche et les sous-questions ont été étudiés in situ afin de générer des connaissances généralisables. Le projet et les résultats ont finalement été documentées dans une thèse de doctorat, soumise au jury en juin 2021. Cet article présente certains des résultats de l’étude.

# Questions de recherche étudiées dans l’étude

L’objectif principal de l’étude était de déterminer si une ontologie des compétences en cybersécurité pouvait fournir un outil efficace aux institutions financières pour gérer les talents en cybersécurité. La question de recherche a ensuite été structurée en trois parties :

1. Ingénierie ontologique,
2. Alignement de l’ontologie au domaine de la cybersécurité,
3. Validation et test à l’aide de requêtes sémantiques et d’inférences en utilisant des règles et des scénarios de cybersécurité.

Pour la première partie, différentes approches pour le développement de l’ontologie ont été considérées, comme celles proposées par (Keet, 2020), (Sure-Vetter et al., 2009) ou (Stadlhofer et al., 2013). Cependant, il a été décidé d’aller de l’avant avec l’ADR pour développer et documenter une nouvelle méthodologie d’ingénierie ontologique des compétences afin de faciliter la réutilisation future et de fournir des preuves utiles de la rigueur du processus. À la suite de cela, une méthodologie d’ingénierie ontologique des compétences en cybersécurité a été développée et documentée.

La deuxième partie a débuté par une cartographie du domaine de la cybersécurité dans l’ontologie. Ce travail fut réalisé à partir du modèle de compétences en cybersécurité proposé par le Département du travail, de l’emploi et de la formation des États-Unis et le National Institute of Science and Technology (NIST). Ce modèle est mieux connu sous le nom de National Cybersecurity Workforce Framework (NCWF) de la National Initiative for Cybersecurity Education (NICE) (Newhouse et al., 2017; NIST, 2021; Petrella, 2017). Ce modèle été complété par les données recueillies dans l’étude durant les cycles BIE. Suite à cela, une ontologie de compétence en cybersécurité a été développée. Cette ontologie peut servir à de multiples fins, telles que l’aide aux organisations et aux établissements d’enseignement à définir des programmes d’études, comme le présente cet article.

Enfin, pour la troisième partie, plusieurs outils ont été envisagés pour effectuer le test. Le système Stardog a été sélectionné et utilisé avec les requêtes SPARQL dans l’ontologie pour recommander des rôles et des postes qui correspondent aux scénarios de risque MITRE Att&ck. Les résultats de 50 requêtes ont été analysés pour identifier les vrais positifs, les vrais négatifs, les faux positifs et les faux négatifs. Cela a permis le calcul de la précision, du rappel, de scores F1 et MCC. Le coefficient de corrélation de Matthews (MCC) fournit des informations concernant la corrélation entre les classifications observées et prédites (Tharwat, 2020). Il est considéré comme un bon indicateur de la qualité et de l’exactitude de la classification (Chicco et al., 2021). Un résumé de ces résultats est présenté dans le tableau 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Précision** | **Rappel** | **Score F1** | **MCC** |
| **Moyenne** | 0.77 | 0.63 | 0.67 | 0.06 |
| **Écart-type** | 0.02 | 0.16 | 0.13 | 0.03 |
| **Variance** | 0.000 | 0.027 | 0.018 | 0.001 |

Tableau 1 : Résumé des résultats pour 50 scénarios

Nous avons conclu que le test fut réussi et que la valeur prédictive de l’ontologie des compétences en cybersécurité à l’aide de Stardog, telle que présentée ci-dessus, est statistiquement significative. Cela appuierait la troisième sous-question, indiquant que l’ontologie peut représenter avec précision le domaine de la cybersécurité et être utilisée comme outil d’aide à la prise de décision en matière de gestion des talents à partir des compétences en cybersécurité.

# Compétence

Au centre de cette étude se trouve le concept de compétence, qui peut être défini comme une caractéristique d’un acteur performant dans un rôle professionnel (Boyatzis, 2008; Prescott, 2012; Subramaniam et al., 2019), démontrés par le comportement et les actions (Man et al., 2002a). Les compétences peuvent êtes apprises, ce qui permet d’intervenir pour les affecter, par exemple par l’éducation (Draksler & Širec, 2018a; Man et coll., 2002a; McClelland, 1973; Mitchelmore et Rowley, 2010). Elles peuvent être définies par rapport au savoir, au savoir-faire et au savoir-être, mais aussi dans certains modèles par rapport aux connaissances, aptitudes et habiletés.

Le savoir, c’est la connaissance. Le savoir peut s’acquérir par l’éducation comme un mélange de connaissances tacites et explicites (Draganidis & Mentzas, 2006). Ce n’est pas une garantie de succès dans un rôle professionnel, mais c’est un pas vers la compétence. En plus du savoir, la véritable compétence nécessite des capacités de résolution de problèmes qui respectent les meilleures pratiques et les normes reconnues dans un domaine, ainsi qu’une maîtrise technique et procédurale. À des niveaux de compétence élevés, les acteurs sont en mesure de combiner des savoirs pour proposer des solutions innovantes à des problèmes du monde réel (Bacigalupo et al., 2016; Man et coll., 2002a).

Le savoir-faire fait référence à la capacité de personnes compétentes à démontrer habilement une connaissance pratique du travail, des tâches, des méthodes, des processus d’affaires et de l’écosystème d’une organisation en appliquant le savoir. Il est lié aux aptitudes et habiletés dans certains modèles de compétences, comme le NCWF en cybersécurité. Lorsque les individus ont un savoir-faire, ils ont également une maîtrise approfondie de la façon dont leur domaine de compétence fonctionne en tant que système cohérent. De même que le savoir et le savoir-faire, la performance professionnelle peut être liés à l’intelligence émotionnelle, sociale et cognitive des individus, c’est-à-dire au savoir-être (Bacigalupo et al., 2016; Boyatzis, 2008, 2008; Man et coll., 2002b).

Le savoir-être est une caractéristique des personnes compétentes qui démontrent des capacités élevées en matière de relations émotionnelles et humaines, des capacités mentales et physiques, des attitudes, des systèmes de valeurs solides et des comportements compatibles avec la culture de l’organisation et les valeurs socioculturelles dominantes des divers intervenants internes et externes, y compris la capacité d’interagir avec ses collègues (Bacigalupo et coll., 2016; Boyatzis, 2008, 2008; Draksler et Širec, 2018b; Man et coll., 2002b; McClelland, 1973; Mitchelmore et Rowley, 2010).

# Cartographie des compétences en cybersécurité

Le consensus qui s’est dégagé de l’étude est qu’il existe deux catégories principales de postes en cybersécurité avec certaines exigences communes en matière de compétences en cybersécurité et d’autres qui sont distinctes. L’utilisation des catégories et des rôles professionnels du NCWF n’était pas pratique car elle est perçue comme trop complexe. Une catégorisation plus simple, à un niveau élevé, a été perçue par les participants aux rôles de gestion comme plus pratique et représentant la réalité observée sur le terrain. Cela peut être comme une structure organisationnelle matricielle, où un acteur dans un rôle professionnel peut être dans une catégorie de haut niveau selon les lignes présentées, ainsi que dans un rôle professionnel NCWF. Par exemple, un analyste d’affaires qui fait équipe de gouvernance peut également être défini comme un analyste de la sécurité système, rôle professionnel NCWF OM-ANA-001.

La première catégorie, **cybersécurité affaires,** est composée d’acteurs qui sont des experts des aspects métiers ou cybersécurité. Ces acteurs ont une vision plus stratégique, comprenant comment la cybersécurité apporte de la valeur à l’organisation, aux clients et aux autres parties prenantes. La deuxième catégorie, **cybersécurité technique,** comprend les acteurs impliqués dans divers aspects techniques de la cybersécurité, y compris souvent la gestion et l’utilisation du matériel, des logiciels et des outils. Ceci dit, les participants à l’étude nous ont informés que les experts en affaires ont besoin de savoir et de savoir-faire technique, tandis que les experts techniques doivent comprendre les processus d’affaires de l’entreprise avant d’acquérir une réelle compétence dans leur rôle. Ainsi, il existe un continuum de compétences en cybersécurité, des rôles d’affaires aux rôles techniques, avec de nombreux rôles entre ces deux pôles. Ce continuum nous a amenés à identifier neuf spécialités parmi les deux catégories identifiées dans le modèle. De plus, au sein de chaque spécialité, des niveaux variés d’exigences en matière de compétences sont identifiés, selon le rôle. Par exemple, il pourrait y avoir un besoin justifié d’une gamme allant d’un travailleur junior, ou d’un spécialiste qui débute dans un rôle professionnel, jusqu’à un travailleur plus senior, expérimenté et hautement compétent.

Cet article présente certains des éléments de compétence du NCWF qui ont été identifiés, en utilisant les numéros d’identification KSA du NCWF, ainsi que les éléments de compétence proposés dans l’étude. Les numéros NCWF peuvent être très utiles car de nombreuses études et formations, certifications et autres fournisseurs les utilisent pour présenter les résultats d’apprentissage de leur offre. Cela peut être considéré comme une pierre de Rosette pour faire des liens entre les résultats de cette étude et de cet article à des produits et services qui utilisent le NCWF.

# Mesurer le niveau de compétence

Un aspect important de l’utilisation de la compétence dans un contexte organisationnel est la façon dont elle peut être mesurée et évaluée. Disposer d’une mesure permettant de quantifier les compétences est un aspect essentiel de l’évaluation des niveaux de compétence en cybersécurité des acteurs dans des rôles professionnels en cybersécurité. Cela sera utilisé à de nombreuses fins, comme mesurer l’efficacité des programmes de formation continue ou démontrer la conformité des exigences en matière de compétences aux autorités. Ce qui est proposé comme un bénéfice de l’étude est d’utiliser l’évaluation des niveaux de compétence pour les éléments de compétence en cybersécurité par rapport aux six niveaux de la taxonomie révisée de Bloom (Krathwohl, 2002). Un septième niveau est implicite, zéro (0), pour indiquer l’absence de connaissances ou de compétences pour un élément de compétence en particulier. Les six niveaux sont les suivants :

1. **Rappel :** À ce premier niveau, les acteurs présentent une mémoire d’information précédemment apprises. À ce niveau, il n’y a pas de compétence.
2. **Comprendre :** Il s’agit du niveau minimum auquel une compétence embryonnaire peut être considérée. À ce niveau, les acteurs démontrent une compréhension de faits et de concepts. Ils commencent à développer un savoir-faire mais pas nécessairement comment comme l’utiliser.
3. **Appliquer :** Lorsque les acteurs peuvent utiliser avec succès leur savoir pour résoudre des problèmes et démontrer un savoir-faire, des aptitudes et des habiletés pour trouver et appliquer des solutions aux problèmes du monde réel. Ils démontrent la capacité de fonctionner avec d’autres parties prenantes dans le cadre de contraintes organisationnelles, démontrant un savoir-faire.
4. **Analyser :** À ce niveau plus avancé, les acteurs compétents peuvent également identifier des motifs ou des causes, faire des inférences et trouver des preuves à l’appui des généralisations.
5. **Évaluer :** À un niveau élevé de compétence, les acteurs peuvent présenter et défendre des opinions et porter des jugements sur l’information, la validité des idées ou la qualité du travail en fonction d’un critère prédéterminé.
6. **Créer :** Au plus haut niveau de compétence de ce modèle, des acteurs hautement compétents peuvent compiler des informations, combiner des éléments de nouvelles manières ou proposer des solutions alternatives aux problèmes existants ou nouveaux auxquels ils sont confrontés.

# Résultats

Dans les sections suivantes de cet article, nous présentons certaines de nos conclusions de l’étude sur les compétences requises des travailleurs en cybersécurité dans une institution financière canadienne. Cela commence par l’identification des compétences de base pour toutes les catégories. Il présente ensuite les compétences par catégories de rôles professionnels et inclut les différentes spécialités pour chacune des deux catégories. Il convient de noter que cela pourrait être plus détaillé en examinant les exigences par rôles professionnels spécifiques, tels que les 52 rôles décrits par le NCWF ou par rôles professionnels réels dans une organisation particulière. Cet article, en tant qu’étude, s’est concentré sur les deux catégories de niveau supérieur et neuf spécialités et n’a pas cherché à décrire les compétences spécifiques d’un acteur spécifique dans un rôle professionnel, qui pourraient être déduites des informations présentées ici, complétées par les fonctions et la situation de l’acteur.

# Connaissances de base pour tous les travailleurs de la cybersécurité

Tout au long de l’étude, la combinaison de connaissances qui constitue les éléments de compétence de tous les rôles professionnels en cybersécurité dans l’organisation a été définie. Déjà, cette information a été utilisée par l’organisation pour repenser la gestion des talents et la formation en cybersécurité. Parallèlement, le niveau de compétence requis pour chaque élément de compétence d’un rôle professionnel a été déterminé, en référence aux sept niveaux (0 à 6). Par exemple, il a été déterminé que le niveau de compétence minimum requis pour tous les éléments de compétence de base est le niveau 2, « Comprendre ». Cela a conduit à définir le niveau 2 comme l’exigence de connaissances de base requise pour les éléments de compétence communs à tous les rôles professionnels en cybersécurité. Cela a été établi comme une exigence de base. Il a été utilisé pour définir un programme de formation minimal pour tous les travailleurs en cybersécurité de l’organisation, comme présenté dans la section suivante. Ce savoir-faire de base comprend :

* Résolution de problèmes
* Concepts et protocoles de mise en réseau
* Lois, règlements, politiques et éthique en matière de cybersécurité et de protection de la vie privée
* Principes de cybersécurité et de confidentialité
* Gestion des cybermenaces et des vulnérabilités
* Normes, cadre de gestion et méthodologies de cybersécurité
* Gestion du risque
* Gestion du changement

En plus du savoir-faire de base, il a été identifié que tous les acteurs dans les rôles professionnels en cybersécurité doivent avoir des compétences minimales en matière de savoir-faire. Il s’agit notamment des compétences en communication et en relations interpersonnelles, souvent appelées compétences générales, à un niveau minimal de 3, « Appliquer ». Ces compétences ont souvent été décrites comme problématiques pour de nombreux travailleurs de la cybersécurité. Par exemple, il a été observé et mentionné dans les discussions qu’il n’est pas inhabituel pour certains travailleurs ayant des niveaux élevés de compétence dans leur domaine particulier, d’être moins efficaces dans leur rôle professionnel en raison de la difficulté d’interagir avec les parties prenantes, étant ainsi perçus comme moins compétents.

Dans l’étude, nous avons identifié les éléments de compétence communs pour tous les rôles professionnels en cybersécurité. Voici les compétences de base recommandées pour tous les travailleurs de la cybersécurité :

* Connaissance des concepts de mise en réseau, des protocoles et des méthodologies de sécurité (K0001)
* Connaissance des processus de gestion des risques (K0002)
* Connaissance des lois, des règlements, des politiques et de l’éthique en matière de cybersécurité et de protection de la vie privée (K0003)
* Connaissance des principes de cybersécurité et de confidentialité et des exigences organisationnelles (K0004, K0044, A0123 et S0367)
* Connaissance des politiques, procédures et réglementations en matière de cyberdéfense et de sécurité de l’information (K0157)
* Connaissance du programme de classification de l’information d’une organisation et des procédures de compromission de l’information (K0287)
* Connaissance des pratiques, des politiques, des exigences et des procédures de gestion des risques de la chaîne d’approvisionnement (TI) (K0126, K0169)
* Connaissance des cybermenaces et des vulnérabilités (K0005)
* Connaissance des impacts opérationnels spécifiques des défaillances en matière de cybersécurité (K0006)
* Interpréter et respecter les normes et la normalisation mondiales (WPC0022A)
* Connaissance des lois, statuts, lignes directrices, procédures, normes et exigences de conformité applicables à l’appui des cyberactivités organisationnelles (K0168, A0033, K0267)
* Connaissance des technologies de l’information (TI) et de cybersécurité nouvelles et émergentes (K0059)

À un niveau d’entrée, un travailleur en cybersécurité aurait besoin d’un niveau de compétence très basique de « Comprendre », niveau 2, qui aide à expliquer l’utilisation du terme connaissance. Cela n’indique aucune compétence, car un niveau de « Appliquer », niveau (3) ou supérieur est nécessaire pour qu’une compétence soit prise en compte. Ainsi, un nouveau travailleur dans un poste de niveau d’entrée, comme un récent diplômé universitaire en cybersécurité embauché dans une institution financière canadienne, aurait rapidement besoin d’être exposé à des situations réelles, d’encadrement et de formation pour acquérir des compétences. Cela se ferait au fur et à mesure qu’ils seraient intégrés à l’organisation et recevraient une formation initiale pour entrer dans le rôle professionnel. Les sections suivantes présentent les exigences en matière de compétences par catégorie de poste de travail et par spécialité, en commençant par la catégorie d’affaires et les spécialités.

**Rôles professionnels dans les entreprises de cybersécurité**

La catégorie d’affaires de cybersécurité (CAT002) est composée d’acteurs qui sont des experts dans tous les aspects commerciaux de la cybersécurité liés à la mission et aux objectifs commerciaux de l’organisation. Ils combinent une compréhension des technologies avec une solide compréhension stratégique de la cybersécurité et comprennent comment la cybersécurité apporte de la valeur à l’organisation et à toutes ses parties prenantes. Par exemple, un conseiller stratégique d’un gestionnaire d’une unité d’affaires qui peut le conseiller sur la planification de la sécurité de l’information dans un projet fait son devoir. Pour s’assurer que le niveau minimum de compétence est atteint, l’organisation s’est rendu compte que la formation CISSP serait la voie la plus opportune et la plus rentable, car elle était offerte par les universités locales. Lors du développement de l’ontologie, il a été démontré qu’il y avait une bonne adéquation entre les compétences requises et la formation CISSP. Ainsi, il a été rendu obligatoire pour tous les acteurs de la catégorie de rôle professionnel des entreprises de cybersécurité. Des parcours de formation Business Cybersecurity 1 et 2 ont également été créés sur Udemy pour compléter la formation de tous les travailleurs.

Les principales tâches de la catégorie de rôle professionnel de l’entreprise de cybersécurité:

* Soutenir et conseiller les intervenants en sécurité de l’information et l’organisation en termes de sécurité logique et physique afin de protéger adéquatement les informations et d’en assurer la confidentialité.
* Protégez les informations des clients, des employés et des fournisseurs en développant, en maintenant et en surveillant les processus et les cadres de sécurité. Assurez-vous qu’il est lié aux processus et technologies métier pour les rendre plus sécurisés.
* S’assurer que les exigences de sécurité sont correctement prises en compte dans tous les aspects de la gestion de l’information, y compris les cadres de gestion, les architectures, les solutions et les systèmes nécessaires pour réaliser la mission de l’organisation et la fourniture de produits et services aux clients.

Les principales responsabilités de la catégorie de rôle professionnel d’entreprise de cybersécurité :

* Déterminez les besoins en matière de protection des informations et traduisez-les en exigences tout en respectant la culture, les valeurs, l’appétit pour le risque, les contraintes et la stratégie commerciale de l’organisation.
* Identifier, analyser, quantifier, hiérarchiser, vérifier (auditer) et documenter les risques de cybersécurité.
* Recommander et suivre des plans de traitement des risques inacceptables.
* Évaluer et concevoir des mécanismes de gestion de la sécurité appropriés.
* Surveillez l’évolution des menaces, des vulnérabilités et des risques de sécurité et faites des recommandations.
* Définir, opérationnaliser, surveiller, vérifier, mesurer et améliorer les processus de gestion de la sécurité.
* Définissez, mettez en œuvre et surveillez les cadres de sécurité stratégiques, tactiques et opérationnels conformément aux meilleures pratiques et aux normes de sécurité de l’information.
* Fournir des conseils, des opinions et des recommandations sur les exigences de sécurité à inclure dans les projets ou à intégrer dans les opérations informatiques.
* Produire et surveiller des indicateurs de rendement clés pour mesurer l’atteinte des objectifs de sécurité et assurer la responsabilisation envers les intervenants ciblés.
* Identifier, produire, diffuser, mesurer et surveiller les programmes de formation continue et de sensibilisation à la sécurité pour les clients, les employés et les gestionnaires.

Certaines des tâches les plus courantes de la cybersécurité Les travailleurs d’entreprise comprennent :

* Fournir un contexte commercial à la cybersécurité.
* Contribuer aux activités de gouvernance, de gestion des risques, de conformité et de cybersécurité.
* Fournir des commentaires sur les exigences en matière de cybersécurité.
* Traduire et les exigences des utilisateurs en informations de cybersécurité exploitables et en exigences techniques
* Analyser les besoins et faire des recommandations selon les besoins de l’organisation
* Traduire et expliquer les exigences en matière de cybersécurité aux parties prenantes
* Contribuer à la conception, à l’analyse et à la mise en œuvre de l’architecture des systèmes de cybersécurité.
* Effectuer des activités de gestion de projet et de gestion du changement.

De nombreux titres d’emploi et postes en cybersécurité d’entreprise différents peuvent être identifiés dans cette catégorie, tels que :

* Analyste en cybersécurité
* Conseiller en conformité en cybersécurité
* Auditeur de cybersécurité
* Responsable de la sécurité de l’information d’entreprise (BISO)
* Responsable de la sécurité de l’information (RSSI)

Les éléments de compétence de base communs pour toutes les spécialités commerciales en cybersécurité (4) et les rôles professionnels (26) sont déjà présents dans les éléments de compétence de base pour tous les travailleurs en cybersécurité identifiés précédemment. L’analyste en cybersécurité (SP006) et le conseiller en cybersécurité (SP007) forment les plus grandes cohortes du rôle professionnel de l’entreprise. Il semble approprié de les placer dans un continuum en ce qui concerne les tâches et les responsabilités mentionnées ci-dessus. Dans les rôles professionnels en cybersécurité, le niveau de compétence minimum requis est « Appliquer », niveau 3. Par exemple, dans un continuum d’équipe de gouvernance de la cybersécurité, un acteur dans un rôle d’analyste en cybersécurité devrait être au niveau de compétence « Analyser » (4) et dans le rôle de conseiller en cybersécurité être au niveau « Évaluer » (5) ou au niveau « Créer » (6), dans un rôle de conseiller principal.

Un autre rôle professionnel dans la catégorie des entreprises est le spécialiste de la sensibilisation et de la formation à la cybersécurité (SP008). Bien que cette spécialité soit souvent plus à l’appui des activités de sensibilisation à la cybersécurité de l’organisation, elle est néanmoins très critique, car les clients, les employés et les autres parties prenantes constituent souvent le maillon le plus faible de la cybersécurité dans les organisations financières. Enfin, le rôle de gestionnaire (SP005) est identifié comme la quatrième spécialité commerciale en cybersécurité. Pour chacune de ces spécialités, l’organisation a identifié les exigences détaillées en matière d’éléments de compétence, dont un aperçu est présenté dans les sections suivantes.

**Spécialité responsable de la cybersécurité**

Le rôle professionnel de gestionnaire comprend le poste de niveau le plus élevé dans les équipes de cybersécurité de l’organisation. L’acteur typique dans ce rôle professionnel est un diplômé d’un premier cycle universitaire ou, dans la plupart des cas observé dans l’organisation participante, un programme d’études supérieures en gestion des technologies d’entreprise, en ingénierie, en gouvernance ou en gestion, tel qu’un MBA avec de nombreuses années (8+) d’expérience dans l’organisation ou dans le secteur financier. En plus des éléments de compétence de base déjà identifiés pour tous les rôles de cybersécurité, le responsable de la cybersécurité doit avoir des compétences de haut niveau dans le savoir-faire à être ainsi que dans les domaines liés à l’équipe ou au rôle spécifique de l’acteur.

La spécialité de gestionnaire de cybersécurité (SP005) comprend plusieurs rôles professionnels NCWF :

* Leadership cybernétique exécutif (OV-EXL-001)
* Responsable de la sécurité des systèmes d’information (OV-MGT-001)
* Responsable de la sécurité des communications (COMSEC) (OV-MGT-002)
* Développeur et gestionnaire de la main-d’œuvre cybernétique (OV-SPP-001)

Les éléments de compétence de la spécialité de gestionnaire de cybersécurité sont les suivants :

* Connaissance des processus opérationnels et de mission de base de l’organisation (K0146)
* Connaissance des buts et objectifs de l’organisation en matière de technologie de l’information (TI) d’entreprise (K0101)
* Connaissance des exigences du cadre de gestion des risques (CGR) (K0048)
* Connaissance des menaces, des vulnérabilités et des risques liés à la sécurité des systèmes et des applications (K0070, K0624)
* Connaissance des principes et techniques de gestion des ressources (K0072)
* Connaissance des principes de cybersécurité et de confidentialité utilisés pour gérer les risques liés à l’utilisation, au traitement, au stockage et à la transmission d’informations ou de données (K0038)
* Connaissance des contrôles liés à l’utilisation, au traitement, au stockage et à la transmission des données (K0622)

**Spécialité d’analyste en cybersécurité**

Le rôle d’analyste en cybersécurité (SP006) est parfois un rôle subalterne, mais le plus souvent à un niveau intermédiaire dans l’organisation. L’acteur typique dans ce rôle professionnel est un diplômé d’un programme universitaire de premier cycle en gestion des technologies d’entreprise, en informatique, en gestion ou dans un domaine connexe qui se joindrait à une équipe de cybersécurité en tant qu’analyste. De même, le titulaire d’un diplôme d’études collégiales professionnelles en informatique qui a quelques années (5+) d’expérience dans l’organisation pourrait occuper un poste d’analyste. Dans certains cas, il a été observé que des personnes d’autres domaines, comme la criminologie, l’application de la loi ou la psychologie, ainsi que des anciens combattants, peuvent obtenir de bonnes performances dans cette spécialité grâce à une formation supplémentaire en cybersécurité en cours d’emploi offerte une fois embauchée, lorsque le rôle professionnel est approprié. En plus des éléments de compétence de base déjà identifiés, l’analyste en cybersécurité doit avoir des compétences à « Analyser » (niveau 4) dans les domaines qui sont pertinents pour son rôle spécifique dans l’organisation, qui pourraient inclure :

* Systèmes d’information et systèmes d’exploitation
* Principes de classification des données
* Technologies de sécurité de l’information
* Gestion des services réseau
* Gestion des infrastructures critiques
* Technologies opérationnelles
* Gestion des identités et des accès
* Solutions de protection des renseignements personnels
* Cryptographie

Les rôles professionnels NCWF NIST suivants relèvent de cette spécialité:

* Analyste de la sécurité des systèmes (OM-ANA-001)4
* Planificateur Cyber Intel (CO-OPL-001)
* Planificateur cyberopérations (CO-OPL-002)
* Représentant officiel autorisé/désignant (SP-RSK-001)
* Évaluateur du contrôle de sécurité (SP-RSK-002)
* Spécialiste en recherche et développement (SP-TRD-001)
* Planificateur de configuration système requise (SP-SRP-001)
* Analyste de données (OM-DTA-002)
* Gestionnaire de connaissances (OM-KMG-001)
* Auditeur de programme informatique (OV-PMA-005)
* Gestionnaire de toutes les sources (CO-CLO-001)
* Gestionnaire de toutes les exigences de collecte des sources (CO-CLO-002)

Les éléments de compétence de la spécialité d’analyste en cybersécurité sont les suivants :

* Connaissance des systèmes d’exploitation (K0060)
* Connaissance des systèmes d’infrastructures critiques avec les technologies de l’information et de la communication qui ont été conçus sans considérations de sécurité du système (K0170)
* Connaissance de la gestion des services et des normes connexes (K0200)
* Connaissance de la cryptographie et de la gestion des clés cryptographiques (K0018, K0019)

De plus, d’autres éléments de compétence seront requis en fonction du rôle professionnel d’un analyste de cybersécurité spécifique.

**Conseiller en cybersécurité**

Le conseiller en cybersécurité (SP007) est un rôle de haut niveau. Les responsables de la sécurité de l’information d’entreprise (BISO) sont un exemple de rôle de conseiller très senior. Ce n’est pas un rôle pour un nouveau travailleur en cybersécurité; cependant, un récent diplômé d’un programme de maîtrise universitaire en gestion des technologies d’affaires, en informatique, en ingénierie, en cybersécurité, en gouvernance ou en gestion ayant une expérience antérieure dans le secteur financier pourrait se joindre aux équipes de sécurité en tant que conseiller. De même, le titulaire d’un baccalauréat ou d’un diplôme d’études collégiales qui a plusieurs années (8+) d’expérience dans le secteur financier pourrait occuper un poste de conseiller. En plus des éléments déjà identifiés, le spécialiste du conseiller en cybersécurité doit avoir des compétences « Évaluer » (niveau 5) ou « Créer » (niveau 6) dans plusieurs des domaines suivants, selon ses responsabilités :

* Processus d’affaires stratégique
* Identification et gestion des besoins informatiques
* Interface homme-machine
* Architecture informatique
* Mise en réseau et services connectés
* Virtualisation, conteneurs et DevSecOps
* Informatique en nuage
* Menaces et vulnérabilités émergentes
* Technologies émergentes en matière de cybersécurité

En plus de tous les rôles professionnels de la spécialité d’analyste en cybersécurité, les rôles professionnels suivants de la NWCF entrent dans cette catégorie :

* Architecte d’entreprise (SP-ARC-001)
* Architecte de sécurité (SP-ARC-002)
* Conseiller juridique en cybersécurité (OV-LGA-001)
* Responsable de la protection de la vie privée/Responsable de la conformité à la vie privée (OV-LGA-002)
* Planificateur de politiques et de stratégies cybernétiques (OV-SPP-002)
* Gestionnaire de programme (OV-PMA-001)
* Chef de projet informatique (OV-PMA-002)
* Responsable du support produit (OV-PMA-003)
* Investissement informatique/Gestionnaire de portefeuille (OV-PMA-004)

Les éléments de compétence de la spécialité de conseiller en cybersécurité sont les suivants :

* Capacité d’appliquer des compétences critiques en lecture/pensée (A0070)
* Connaissance des processus opérationnels et de mission de base de l’organisation (K0146)
* Connaissance de la façon dont les besoins en informations et les exigences de collecte sont traduits, suivis et hiérarchisés dans l’ensemble de l’entreprise étendue (K0120)
* Connaissance des principes d’interaction homme-machine (K0036)
* Connaissance des composants et architectures informatiques physiques, y compris les fonctions de divers composants et périphériques (K0109)
* Connaissance des concepts, principes, limites et effets fondamentaux de la cybersécurité (K0435)
* Connaissance des réseaux informatiques et des communications de données (K0395, K0417)
* Connaissance des technologies de communication en évolution et émergentes (K0431)
* Connaissance des applications Internet, des réseaux sans fil, numériques et de téléphonie (K0444, K0445, K0446, K0560)
* Connaissance du réseau et du routage courants, des services et de la façon dont ils interagissent pour fournir des communications réseau (K0565)
* Connaissance des bases de la sécurité réseau et des menaces (K0480, K0561, K0612)
* Connaissance des produits de virtualisation (K0610)
* Connaissance des technologies et des concepts de gestion des connaissances basés sur le cloud liés à la sécurité, à la gouvernance, à l’approvisionnement et à l’administration (K0194)

**Spécialiste de la sensibilisation et de la formation à la cybersécurité**

La spécialité de sensibilisation et de formation (SP008) est également un rôle à différents niveaux, du junior au senior. Un récent diplômé d’un programme de certificat universitaire en pédagogie ou en andragogie pourrait combler ce poste. Le titulaire d’un diplôme de premier cycle ou d’études supérieures en psychologie, en sociologie, en criminologie ou en sécurité publique, idéalement avec un stage, un projet de synthèse ou une thèse sur un aspect de la cybersécurité serait un candidat idéal. De même, un analyste ou un conseiller en cybersécurité qui a plusieurs années (5+) d’expérience en tant que chargé de cours postsecondaire pourrait combler ce poste. Dans cette spécialité, nous trouvons également des spécialistes en pédagogie et andragogie, en apprentissage de la création et de la gestion de contenu et en éducation. Les rôles professionnels NWF Cyber Instructional Curriculum Developer (OV-TEA-001) et Cyber Instructor (OV-TEA-002) entrent dans cette catégorie.

**Cybersécurité Rôles professionnels techniques**

La catégorie technique de cybersécurité (CAT001) comprend des spécialistes des technologies de l’information, des programmeurs, des techniciens et des ingénieurs qui sont impliqués dans les différents aspects techniques de la cybersécurité. Ils sélectionnent, configurent, exploitent et gèrent le matériel, les logiciels et les outils qui protègent l’organisation contre les risques inacceptables et contribuent à l’atténuation des risques. Les travailleurs de la catégorie technique combinent une solide expertise technique avec une compréhension du contexte de l’entreprise. Certains des acteurs de cette catégorie de rôles professionnels ont des rôles de soutien informatique, qui comprennent une composante de cybersécurité. Par exemple, un administrateur réseau qui configure les services Microsoft Active Directory sur des serveurs, des testeurs d’intrusion ou un analyste d’évaluation des vulnérabilités joue un rôle professionnel technique en cybersécurité. Pour s’assurer que le niveau minimum de compétence est atteint, l’organisation utilise la formation de certification CEH comme un parcours d’apprentissage opportun et rentable. Il y avait une bonne adéquation entre les éléments de compétence requis et la formation CEH. Ainsi, il a été rendu obligatoire la formation pour tous les acteurs de la catégorie des rôles professionnels technique en cybersécurité. Cela a été offert à tous les travailleurs techniques en partenariat avec une université locale. Des parcours d’apprentissage techniques de cybersécurité 1 et 2 ont également été créés sur Udemy pour compléter la formation.

Les principales tâches de la catégorie technique cybersécurité :

* Sélectionnez, installez, configurez et utilisez des outils, des techniques et des méthodes pour la gestion sécurisée des données, des systèmes d’information, des réseaux et des bâtiments.
* Identifiez, analysez, signalez et résolvez les menaces, les vulnérabilités, les événements et les incidents qui se sont produits ou pourraient se produire au sein du réseau afin de protéger adéquatement les données, les systèmes d’information, les réseaux et les bâtiments.

Les principales responsabilités de la catégorie technique cybersécurité :

* Exploitez les outils de sécurité et surveillez la cybersécurité.
* Déterminer le fonctionnement sécuritaire des systèmes d’information.
* Appliquer les meilleures pratiques en matière de cybersécurité aux exigences organisationnelles.
* Évaluer les contrôles conformément aux meilleures pratiques.
* Évaluer l’adéquation des mesures de cybersécurité dans les exigences.
* Reconnaître et classer les vulnérabilités et les attaques associées.
* Fournissez des recommandations sur les menaces et les vulnérabilités.
* Recevez et analysez des données pour identifier les activités anormales, les menaces potentielles, les activités malveillantes présumées, les méthodes d’exploitation et les impacts.
* Identifiez, documentez et gérez les incidents de cybersécurité.
* Effectuez une surveillance, une recherche et une analyse stratégiques des menaces et des vulnérabilités.

De nombreux titres d’emploi et postes techniques en cybersécurité différents peuvent être identifiés dans cette catégorie, tels que :

* Testeur d’intrusion
* Analyste des menaces et des vulnérabilités
* Membre ou coordonnateur de l’équipe d’intervention en cas d’incident
* Architecte de sécurité

En plus des compétences de base communes pour tous les rôles professionnels mentionnés précédemment, les éléments de compétence communs pour tous les rôles professionnels des spécialités techniques en cybersécurité sont les suivants :

* Connaissance des principes de cybersécurité et de confidentialité et des exigences organisationnelles (K0044)
* Connaissance des normes de sécurité des données de l’industrie des informations personnellement identifiables (PII) et de l’industrie des cartes de paiement (PCI) (K0260, K0261)
* Connaissance des stades de cyberattaque, des cibles, des méthodes et techniques d’attaque, des infections et des méthodes d’infection (K0362, K0177, S0229, S0228, K0392)
* Connaissance des composants informatiques, des systèmes d’exploitation et des architectures, y compris les fonctions de divers composants et périphériques (K0060, K0109)
* Connaissance des concepts, de la terminologie et des opérations d’un large éventail de supports de communication (K0108)
* Connaissance des réseaux informatiques, des dispositifs et infrastructures de réseau physiques et logiques, des communications numériques, des principes fondamentaux des réseaux de téléphonie et de la terminologie et des protocoles de communication de données (K0395, K0417, K0471, K0516)
* Connaissance des protocoles réseau tels que TCP/IP, DHCP, DNS et des services d’annuaire (K0332)
* Connaissance des concepts d’architecture de sécurité réseau, y compris la topologie, les protocoles, les composants, les principes et les modèles de sécurité (K0179, K0203)

Pour toutes les compétences de base du travail technique en cybersécurité, le niveau minimum de compétence requis est « Appliquer », niveau 3. Idéalement, tous les acteurs de ce rôle professionnel devraient être en mesure d'«analyser », niveau 4, et dans les rôles professionnels supérieurs «évaluer », niveau 5, ou dans de nombreux cas la compétence pour réussir « Créer », niveau 6. Il existe cinq spécialités dans la catégorie de la cybersécurité technique, telles que l’exploitation informatique, la sécurité défensive, la sécurité offensive, l’architecte de sécurité et la sécurité physique.

**Spécialiste de la cybersécurité offensive**

Le spécialiste de la cybersécurité offensive (SP001) joue le rôle d’un attaquant qui cherche à tester les limites des protections et des processus pour identifier et atténuer les risques inacceptables et éviter les incidents indésirables. Ce rôle est fortement axé sur le savoir-faire et se concentre sur la capacité de tester éthiquement les limites de la cybersécurité d’une organisation. Les rôles professionnels se trouvent à plusieurs niveaux, du junior au senior. Il n’y a pas d’exigences spécifiques de diplôme universitaire pour ce rôle professionnel. Un large éventail de personnes, du secondaire aux diplômés postsecondaires, ayant un talent démontré pourraient trouver leur place dans les équipes de sécurité offensives. Par exemple, un finaliste d’un concours national de cybersécurité avec un diplôme d’études secondaires ou une certification de collège professionnel serait un candidat idéal pour ce rôle. En plus des éléments déjà identifiés, le spécialiste de la cybersécurité offensive doit avoir un minimum de compétences de niveau 4 dans les domaines suivants :

* Techniques de pénétration et d’intrusion
* Planification et exécution d’attaques

Les rôles professionnels NCWF NIST suivants relèvent de cette spécialité :

* Spécialiste de l’évaluation de mission (AN-ASA-002)
* Développeur cible (AN-TGT-001)
* Analyste de réseau cible (AN-TGT-002)
* Analyste linguistique multidisciplinaire (AN-LNG-001)

Les autres éléments de compétence de la spécialité de cybersécurité offensive sont les suivants :

* Connaissance des produits de sécurité basés sur l’hôte et de la façon dont ces produits affectent l’exploitation et réduisent la vulnérabilité (K0440)
* Connaissance des technologies de communication en évolution et émergentes (K0431)
* Connaissance des principes, des outils et des techniques de test d’intrusion (K0342)
* Connaissance des types de sites Web, de l’administration, des fonctions et du système de gestion de contenu (K0349)
* Capacité d’élaborer ou de recommander des approches analytiques ou des solutions à des problèmes et à des situations pour lesquels l’information est incomplète ou pour lesquels il n’existe aucun précédent (A0080)
* Capacité d’évaluer, d’analyser et de synthétiser de grandes quantités de données et de métadonnées, d’identifier les lacunes en matière de renseignement et de produire des résultats utilisables (A0084, K0449, A0066, A0091, A0101, A0102, A0106, A0109, S0187, S0194, S0218)

**Spécialiste de la cybersécurité défensive**

Le spécialiste de la cybersécurité défensive (SP002) intervient pour protéger de manière proactive les systèmes d’information et les données, par exemple en identifiant et en atténuant les vulnérabilités ou en utilisant les résultats du travail effectué par les spécialistes de la cybersécurité offensive. Ce rôle s’adresse à tous les niveaux de compétence. Un récent diplômé d’un programme postsecondaire en gestion des technologies d’affaires, en informatique ou en génie pourrait entrer dans une équipe de sécurité défensive dans un rôle subalterne. De même, le titulaire d’un diplôme d’études collégiales techniques et professionnelles avec quelques années (5+) d’expérience professionnelle pourrait remplir ce rôle. De plus, les diplômés en informatique et en génie peuvent être de bons candidats. En plus des éléments déjà identifiés, le spécialiste de la cybersécurité défensive doit avoir un minimum de compétences de niveau 3 dans plusieurs des domaines suivants :

* Sécurité des applications
* Opérationnalisation des correctifs de sécurité
* TCP-IP et protocoles dérivés (DNS, DHCP, LDAP)
* Réseaux et services de serveurs Microsoft (AD, GPO, etc.)
* Architecture de sécurité réseau
* Top 10 de l’OWASP, Vulnérabilités et expositions courantes et MITRE ATT&CK

Les rôles professionnels NCWF NIST suivants relèvent de cette spécialité :

* Développeur de logiciels (SP-DEV-001)
* Évaluateur de logiciels sécurisés (SP-DEV-002)
* Spécialiste des essais et de l’évaluation des systèmes (SP-TST-001)
* Analyste en cyberdéfense (PR-CDA-001)
* Spécialiste du soutien à l’infrastructure de cyberdéfense (PR-INF-001)
* Intervenant en cas d’incident de cyberdéfense (PR-CIR-001)
* Analyste de l’évaluation des vulnérabilités (PR-VAM-001)
* Analyste des menaces/avertissements (AN-TWA-001)
* Gestionnaire de toutes les sources (CO-CLO-001)
* Enquêteur sur la cybercriminalité (IN-INV-001)
* Analyste en criminalistique de l’application de la loi et du contre-espionnage (IN-FOR-001)
* Analyste en criminalistique de la cyberdéfense (IN-FOR-002)

Les éléments de compétence supplémentaires de la spécialité de cybersécurité défensive sont les suivants :

* Connaissance des langages de programmation (K0068, K0139)
* Connaissance des exigences d’évaluation et de validation de l’organisation (K0028)
* Connaissance des méthodologies de réponse et de traitement des incidents (K0042)
* Connaissance de la gouvernance juridique liée à l’admissibilité de la preuve (K0123, K0155, K0156)
* Connaissance de la collecte, de l’emballage, du transport et du stockage des preuves électroniques tout en maintenant la chaîne de traçabilité (K0118, K0125, S0047, S0068)
* Connaissance de la sauvegarde et de la restauration des données (K0021)
* Connaissance de l’architecture de sécurité de l’information d’entreprise de l’organisation, des concepts d’architecture de sécurité et des modèles de référence de l’architecture d’entreprise (K0027, K0199)
* Connaissance de la fluidité du trafic sur le réseau et des méthodes d’analyse du trafic réseau (K0058, K0061)
* Connaissance de l’analyse au niveau des paquets à l’aide d’outils appropriés (K0301, K0565)
* Connaissance des mécanismes de contrôle d’accès hôte/réseau (K0033)
* Connaissance des méthodologies et techniques de détection d’intrusion pour détecter les intrusions sur l’hôte et le réseau (K0046)
* Connaissance des différentes classes de cyber-attaquants (K0161, K0162)
* Connaissance de ce qui constitue une attaque réseau et de la relation d’une attaque réseau avec les menaces et les vulnérabilités (K0106)
* Connaissance des systèmes d’infrastructures critiques avec les technologies de l’information et de la communication qui ont été conçus sans considérations de sécurité du système (K0170)
* Connaissance des types et collecte de données persistantes (K0128)
* Connaissance des techniques d’administration système, de réseau et de renforcement des systèmes d’exploitation (K0167)
* Connaissance des menaces et des vulnérabilités de sécurité des systèmes et des applications (K0070, K0624)
* Connaissance des enquêtes sur les menaces internes, des rapports, des outils d’enquête et des lois / règlements. (K0107)
* Connaissance des principes, outils et techniques de test d’intrusion (K0342, S0001)

**Architecte de cybersécurité**

Un architecte de cybersécurité (SP004) est un rôle de haut niveau. Dans ce rôle, les acteurs collaborent avec les équipes de développement dans la conception et la mise en œuvre de solutions qui respectent l’appétit pour le risque de l’organisation. Le titulaire d’un baccalauréat ou d’un diplôme d’études professionnelles en informatique avec plusieurs années (8+) d’expérience en architecture de systèmes, idéalement dans le secteur financier, et une expertise en cybersécurité pourrait occuper un poste d’architecte en cybersécurité. Les rôles professionnels Enterprise Architect (SP-ARC-001) et Security Architect (SP-ARC-002) NCWF sont dans cette spécialité.

Les éléments de compétence supplémentaires de la spécialité d’architecte de cybersécurité sont les suivants :

* Connaissance des mathématiques (K0052)
* Connaissance de la théorie de l’information (K0325)
* Connaissance des principes et méthodes d’analyse (K0043, S0050 S0122)
* Connaissance du génie système et logiciel (K0082, K0102, S0005, S0024)
* Connaissance des méthodes d’essai et d’évaluation des systèmes (K0091)
* Connaissance des modèles d’amélioration et de maturité des processus organisationnels (K0198)
* Connaissance de la gestion des services et des normes connexes (K0200)
* Capacité d’optimiser les systèmes pour répondre aux exigences de performance (A0038)
* Connaissance de la confidentialité, de l’intégrité et de la disponibilité (K0211, S0374)
* Connaissance des produits logiciels compatibles avec la cybersécurité (K0212, S0027)
* Possibilité d’effectuer des analyses de vulnérabilité (A0015)
* Connaissance de l’évaluation de la gestion des risques (K0214)
* Connaissance des concepts clés de la gestion de la sécurité (K0074).
* Connaissance du processus d’évaluation et d’autorisation de sécurité (K0037)
* Connaissance des systèmes d’infrastructures critiques avec les technologies de l’information et des communications qui ont été conçus sans considérations de sécurité du système (K0170)
* Connaissance des méthodologies de tolérance aux pannes du système (K0323)
* Connaissance des différents types d’architectures informatiques (K0227)
* Connaissance de l’architecture des technologies de l’information d’entreprise (K0291)
* Connaissance de l’intégration des buts et objectifs dans l’architecture (K0293, A0027)
* Capacité d’identifier les systèmes d’infrastructure critiques dotés de technologies de l’information et de la communication qui ont été conçus sans considérations de sécurité du système (A0170)
* Capacité d’appliquer les méthodes, les normes et les approches pour décrire, analyser et documenter une architecture (A0008)
* Connaissance de la planification de la protection des programmes (K0264)
* Connaissance de l’installation, de l’intégration et de l’optimisation (K0035)
* Connaissance des techniques de gestion de configuration (K0275)
* Connaissance des systèmes de bases de données (K0024)
* Connaissance de l’architecture de sécurité de l’information d’entreprise de l’organisation (K0027)
* Connaissance des typologies à plusieurs niveaux (K0286)
* Connaissance des concepts de calcul parallèle et distribué (K0063)
* Connaissance des systèmes de sécurité multi-niveaux et des solutions inter-domaines (K0240)
* Connaissance du génie électrique appliqué à l’architecture informatique (K0030)
* Connaissance des concepts de télécommunications (K0093)
* Connaissance des protocoles réseau tels que TCP/IP, la configuration dynamique de l’hôte, le système de noms de domaine (DNS) et les services d’annuaire (K0332)
* Connaissance des processus de conception de réseau, y compris la compréhension des objectifs de sécurité, des objectifs opérationnels et des compromis (K0333)
* Connaissance de l’accès au réseau, de l’identité et de la gestion des accès (K0056)
* Connaissance de la gestion de réseau (K0180, A0172)
* Connaissance de la circulation du trafic sur le réseau (K0061)
* Connaissance des zones démilitarisées (K0326)

**Spécialiste de l’exploitation de la cybersécurité**

La spécialité d’exploitation de la cybersécurité (SP003) comprend plusieurs rôles de gestion et de support informatique où l’une des composantes du rôle professionnel de l’acteur est liée à la cybersécurité. Faisant parfois partie d’un service informatique, en dehors du service de cybersécurité principal, ce rôle professionnel est souvent une passerelle permettant à un travailleur de rejoindre éventuellement le service de cybersécurité. Cela joue un rôle essentiel dans le contrôle et la gestion des risques dans l’organisation. Un récent diplômé d’un programme professionnel d’études secondaires, d’un programme technique postsecondaire ou d’un programme de premier cycle en gestion des technologies d’entreprise, en informatique ou en soutien informatique pourrait être embauché dans un rôle professionnel d’exploitation informatique. Par la suite, après quelques années dans l’organisation, cet acteur pourrait occuper un poste de sécurité défensif ou offensif ou un rôle d’analyste dans un département de cybersécurité.

Les rôles professionnels NCWF NIST suivants relèvent de cette spécialité :

* Développeur de sécurité des systèmes d’information (SP-SYS-001)
* Développeur de systèmes (SP-SYS-002)
* Administrateur de base de données (OM-DTA-001)
* Spécialiste du support technique (OM-STS-001)
* Spécialiste des opérations réseau (OM-NET-001)
* Administrateur système (OM-ADM-001)
* Analyste de l’exploitation (AN-EXP-001)
* Analyste toutes sources (AN-ASA-001)
* Planificateur de l’intégration des partenaires (CO-OPL-003)
* Cyber-opérateur (CO-OPS-001)

Les éléments de compétence supplémentaires de la spécialité d’exploitation sont les suivants :

* Capacité à communiquer des informations complexes (A0013)
* Capacité à collaborer efficacement avec les autres (A0074, A0089)
* Possibilité de trouver des données (A0066)
* Connaissance des objectifs de l’organisation (K0560)
* Connaissance des principes d’interaction homme-machine (K0036)
* Connaissance de la sécurité des technologies de l’information (TI) (K0049)
* Connaissance des réseaux locaux et étendus (K0050)
* Connaissance des concepts de télécommunications (K0093)
* Connaissance des indicateurs de performance et de disponibilité du système (K0053)
* Connaissance de l’accès au réseau, de l’identité et de la gestion des accès (K0056)
* Connaissance de l’accès au réseau, de l’identité et de la gestion des accès (K0061)
* Connaissance des contrôles d’accès basés sur des politiques et adaptatifs aux risques (K0065)
* Connaissance des concepts de gestion des services (K0200)
* Connaissance des modèles de sécurité (K0203)

# Formation continue en cybersécurité

Un résultat pratique de ce projet de recherche pour l’organisation participante a été la création d’une stratégie de formation continue en cybersécurité. La stratégie se concentre sur trois domaines : la formation formelle, l’apprentissage actif et l’opportunisme, en plus de l’objectif d’accroître le niveau de compétence des acteurs dans leurs rôles professionnels actuels. L’étude vise à atténuer les vulnérabilités potentielles causées par l’absence de certains éléments de compétence au niveau requis. Il vise également à accroître la résilience organisationnelle en matière de cybersécurité. Les activités de formation, par spécialité et par rôle professionnel, sont basées sur les informations recueillies dans le projet de recherche et intégrées dans l’ontologie. La stratégie de formation continue comprend quatre niveaux :

1. Un noyau commun pour tous les rôles professionnels en cybersécurité. Une reconnaissance interne a été créée, nommée certificat de sécurité, et a été utilisée pour reconnaître la réalisation de ce tronc commun. L’objectif principal de cette formation était d’assurer un niveau de compétence minimum de 2 pour tous les rôles professionnels en cybersécurité pour les éléments de compétence essentiels, comme mentionné à la section 9.3.1.
2. Un parcours d’apprentissage requis a ensuite été créé pour chacune des deux catégories de rôles professionnels. À l’aide d’une mise en correspondance des certifications de cybersécurité existantes avec le NCWF, la formation CISSP a été sélectionnée pour tous les acteurs de la catégorie des entreprises de cybersécurité et la formation CEH a été sélectionnée pour tous les acteurs de la catégorie technique de cybersécurité. En outre, des parcours d’apprentissage ciblés dans Udemy et Pluralsight ont été créés pour tous les acteurs intéressés par l’utilisation de ces services d’apprentissage en ligne.
3. Une sélection de cours ciblés a été mise à disposition, adaptée par spécialités, pour tous les acteurs. Par exemple, pour la spécialité de cybersécurité défensive, l’organisation est en train de mettre en œuvre le système de formation pratique Immersive Labs Cyber-range. Les listes d’exercices suggérés ont été identifiées par rôle professionnel, car le fournisseur de cet outil a mis en correspondance tous les exercices avec le NCWF.
4. Des cours individuels ont été proposés aux acteurs selon un plan de formation individualisé créé pour chaque acteur, à leur demande ou à la demande de leur manager. En plus de tenir compte des besoins actuels et futurs de l’organisation, le plan individualisé tient compte des intérêts actuels et futurs de l’employé.

# Comment l’information sur les compétences dans l’élaboration du programme d’études

À titre d’exemple, nous présentons deux exemples d’utilisation des résultats de l’étude pour la conception de programmes d’études postsecondaires axés sur les compétences. Le premier exemple est pour un programme de premier cycle pour les analystes en cybersécurité et le second est pour un programme d’études supérieures pour un travailleur offensif en cybersécurité. Pour obtenir le résultat présenté, il est nécessaire d’utiliser les éléments de compétence présentés dans cet article pour le travail sélectionné en combinaison avec les informations détaillées sur les éléments de compétence dans l’ontologie des compétences en cybersécurité, fournies sur le GitHub mentionné. Une analyse peut être effectuée à l’aide de diverses technologies, telles que l’utilisation de l’inférence avec Stardog, comme cela a été fait dans l’étude, ou manuellement à l’aide d’Excel.

**Exemple 1 : Programme de premier cycle de travail d’analyste en cybersécurité (SP006)**

Ce premier exemple présente comment les informations sur le rôle d’analyste en cybersécurité (SP006) un programme de premier cycle universitaire de trois ans, 90 crédits, en gestion des technologies d’entreprise. Comme l’objectif est de développer des compétences de niveau 4 ou supérieures, le programme proposé intégrerait soit l’apprentissage intégré au travail, soit des stages. Ce qui est décrit dans cet exemple est un programme basé sur trois semestres par année civile, avec deux semestres de cours dans les compétences de base et un stage d’été rémunéré.

**Semestre 1**

* Systèmes d’information
  + Technologies de sécurité de l’information
  + Systèmes d’exploitation
* Analyse d’affaires
  + Compétences en communication et en relations interpersonnelles
  + Résolution de problèmes
* Cybersécurité 101
  + Principes de classification des données
  + Principes de cybersécurité et de confidentialité
* Mise en réseau 101
  + Concepts et protocoles de mise en réseau
  + Gestion des services réseau
* Mise en réseau appliquée

**Semestre 2**

* Cybersécurité 201
  + Programme de classification des données
  + Prévention de la perte de données
* Conception et mise en œuvre de la politique de cybersécurité
  + Lignes directrices et procédures
  + Exigences de conformité
* Mise en réseau 201
  + Gestion des infrastructures critiques
  + Technologies opérationnelles
* Concepts de gestion de serveur
  + Services d’annuaire
  + Renforcement du serveur
* Introduction aux tests d’intrusion
  + Outils et utilitaires (en laboratoire)
  + Chaîne de cyber-destruction

**Semestre 3**

* Aspects juridiques de la cybersécurité
  + Lois, règlements, politiques et éthique
  + Règlement fédéral et provincial canadien sur la protection de la vie privée
* Pratiques exemplaires, normes et cadres
  + Les processus de normalisation
  + ISO
  + COBIT
  + Normes et cadres du NIST
  + Gestion des services
  + Autres normes connexes
* Gouvernance 101
  + Principes de gouvernance
* Cybersécurité 301
  + Menaces et vulnérabilités (K0005)
  + Gestion des menaces et des vulnérabilités
* Gestion des risques 101
  + Pratiques, politiques, exigences et procédures de gestion des risques
  + Méthodologies de sécurité
* Gestion du changement
  + Processus et stratégies

**Semestre 4**

* Gestion des risques 201
  + Méthodologies de gestion des risques
  + Cas
* Contrôles internes
  + Contrôle la sélection et la mise en œuvre
* Conformité et certification
* Planification de la continuité des activités
  + Analyse de l’impact sur l’entreprise
  + Conception et approbation du plan
  + Test du plan

**Semestre 5**

* Principes de confidentialité
  + Gestion des identités et des accès
  + Solutions de protection des renseignements personnels
* Gestion des risques 301
  + Application de la gestion des risques dans un contexte réel
* Audits de cybersécurité
  + Audits internes
  + Audits externes
* Gestion des incidents
* Cryptographie

**Semestre 6**

* Certifications professionnelles en cybersécurité
  + CISSP, CCSP ou CISA (selon le chemin préféré)
* Technologies émergentes en matière de cybersécurité
* Projet d’intégration

**Exemple 2 : Rôle de premier cycle en cybersécurité offensive (SP006)**

Ce premier exemple présente comment les informations sur le spécialiste de la cybersécurité offensive (SP001) un programme d’études supérieures universitaires de 1,5 an, 60 crédits en gestion des technologies d’entreprise. Comme l’objectif est de développer des compétences de niveau 4 ou supérieures, le programme proposé intégrerait soit l’apprentissage intégré au travail qui comprend une thèse, soit un projet de synthèse.

L’admission au programme pourrait nécessiter l’un des profils suivants :

* Un diplômé postsecondaire très motivé, avec plus de 3 ans d’expérience
* Un finaliste à un concours national de capture du drapeau de la cybersécurité
* Un non diplômé en informatique ou en ingénierie avec une GPA 3.0 ou supérieure

**Semestre 1**

* Analyse de données appliquéeavec Python
* Introduction à la cybersécurité offensive avancée
* Droit et éthique appliqués à la cybersécurité offensive
* Sécurité basée sur l’hôte
* Tests d’intrusion 101 (principes, outils et techniques)

**Semestre 2**

* Compétences en communication et en relations interpersonnelles
* Sécurité basée sur le serveur
* Sécurité du réseau
* Tests d’intrusion 201 (Planification et exécution d’attaques, avec laboratoires)
* Capture-The-Flag

**Semestre 3**

* Sécurité Internet et cloud
* Test d’intrusion 301 (Utilisation des résultats)
* Champ de bataille cyber-champ de bataille
* Technologies de communication émergentes
* Projet ou thèse Capstone

# Limites de cette étude

L’efficacité des méthodologies qualitatives en général et des questions de cybersécurité en particulier est certainement certaine (Richter et Koch, 2004). La cybersécurité est un sujet sensible pour toute organisation et introduit des limites à ce qu’elle peut permettre de publier et de rendre public. En même temps, l’organisation et les chercheurs reconnaissent que, comme il s’agit d’un sujet important qui a des intérêts nationaux et stratégiques, il y a de bonnes raisons pour que la recherche soit menée et publiée. Cette étude a pu assurer le mérite scientifique de l’entreprise. Les mécanismes de contrôle des biais et l’adhésion à une méthodologie de recherche scientifique, l’ADR, faisaient partie de l’effort visant à maximiser la validité. Néanmoins, pour obtenir la permission de l’organisation participante, certaines informations n’ont été partagées qu’avec l’équipe de recherche et n’ont pas été publiées dans les résultats, la thèse ou les articles ultérieurs dans des revues scientifiques à la demande de l’organisation. Cela a introduit des limites à cette étude qui seront documentées mais pas nécessairement publiées. Sans cela, cependant, la recherche ne pourrait pas avoir lieu.

De plus, cette étude présentait certaines limites inhérentes aux processus formels de validation et d’essai (Whittemore et coll., 2001). Les chercheurs ont été confrontés à un défi difficile en partie à cause de l’équilibre difficile à maintenir entre rigueur, subjectivité et créativité. Le processus continu d’examen par les pairs impliquant l’équipe de recherche, y compris les superviseurs de thèse universitaires, les experts en la matière au sein de l’organisation et les informateurs, contribue à assurer l’intégrité, l’authenticité et la crédibilité des résultats, permettant ainsi une qualité descriptive et interprétative. Dans le même temps, le choix de l’ADR nous a permis de maximiser la congruence et la rigueur des résultats. Tout cela contribue à la validité interne de l’étude, en présentant et en interprétant fidèlement la réalité de l’institution financière où cette étude a été menée et en permettant aux chercheurs de développer une compréhension de la situation qui a conduit à développer et à tester avec succès la solution proposée. En ce qui concerne la notion de validité externe, en raison de l’implication des acteurs de l’industrie, certains aspects de la solution pourraient être généralisés, et cela s’appliquait à d’autres organisations financières similaires au Canada. Cependant, cela nécessiterait d’autres études et des recherches empiriques supplémentaires.

# Considérations éthiques

L’étude n’incluait pas l’expérimentation sur des êtres humains, ce qui n’indique pas l’absence de préoccupations éthiques. L’approche qualitative de la recherche adoptée dans les organisations nécessite l’établissement d’une confiance entre l’équipe de recherche et les participants à l’étude. Cette confiance ne peut exister sans respect pour les personnes impliquées. Les chercheurs devaient rester attentifs et sensibles aux valeurs et à la culture des participants et de l’organisation. La confiance a permis d’acquérir l’accès aux données de l’organisation et à la perspective interne des participants qui ont formé les connaissances brutes nécessaires à la réussite de l’étude.

Cette étude a été soumise et approuvée par le Comité d’éthique de la recherche de l’UQO au début du projet. De plus, le consentement éclairé des participants a été obtenu par écrit lorsqu’ils ont été inscrits à l’étude avant que le processus de collecte de données puisse commencer. La participation à cette étude était volontaire et les participants avaient la possibilité de se retirer à tout moment. Quelques participants n’ont participé qu’à certaines phases de l’étude. En particulier, quelques participants aux entrevues initiales sont passés à une autre organisation au cours de l’étude. Cependant, leur contribution avait pris fin à ce moment-là et ils n’avaient aucune objection à ce que l’utilisation des renseignements qu’ils fournissaient soit incluse dans l’étude. De plus, conformément à l’accord de confidentialité pour effectuer l’étude, aucune information permettant d’identifier facilement l’organisation et les participants n’est incluse dans cet article.

# Travaux futurs

Cette étude a donné lieu à une ontologie complète des compétences en cybersécurité qui décrit les rôles professionnels des travailleurs en cybersécurité dans une institution financière canadienne. Cela permet à l’institution d’améliorer la sécurité de l’information en réduisant les vulnérabilités qui peuvent résulter des lacunes en matière de compétences et d’autres avantages mentionnés. Une fois l’étude terminée, l’organisation a élaboré des mesures de compétences, un outil de mesure et un tableau de bord de gestion. Ces mesures peuvent contribuer à limiter la subjectivité et les préjugés dans l’allocation des ressources humaines et économiques afin d’atténuer les risques créés par les lacunes et les vulnérabilités en matière de compétences en cybersécurité. Cela peut également aider à créer des parcours d’apprentissage individuels pour les travailleurs de la cybersécurité.

Un autre domaine d’investigation est l’intégration de l’apprentissage automatique ou d’autres composants pour aider à faire correspondre les candidats potentiels à des postes de travail en utilisant des sources de données volumineuses, telles que LinkedIn, Indeed ou d’autres sources. L’utilisation de l’ontologie comme base de la solution pourrait aider les organisations à réduire les listes de candidats potentiels afin d’identifier les personnes qui pourraient être des recrues potentielles, y compris les candidats non traditionnels, tels que les minorités ou d’autres groupes sous-représentés. De plus, il est possible d’identifier des personnes compétentes qui peuvent émerger d’autres sources que les profils académiques et d’octroi de diplômes habituels et qui ont acquis des compétences qui pourraient être reconnues et prouvées. L’ontologie peut également fournir un outil aux organisations pour les aider à résoudre les problèmes de conformité juridique et réglementaire.

# Conclusion

Dans le cadre de cette recherche, telle que présentée dans la présente proposition de recherche, la méthodologie de recherche en conception d’action, ADR, a été utilisée pour élaborer et tester une ontologie des compétences professionnelles en cybersécurité pour le secteur des services financiers au Canada. Avec l’aide d’un panel d’experts, l’étude a réussi à combiner des cadres renommés, tels que le NIST NICE, des corpus de connaissances (Newhouse et al., 2017; NIST, 2021; Petrella, 2017), et les pratiques exemplaires actuelles avec les expériences in vivo réelles des praticiens de la cybersécurité d’une institution financière canadienne de classe mondiale travaillant avec une équipe de chercheurs universitaires.

Cela a permis aux chercheurs de concevoir, développer, remplir et tester une ontologie de compétences en cybersécurité représentant le besoin réel de compétences des organisations financières nécessaires pour remplir sa mission avec succès. Le succès de cette ontologie est l’un des éléments qui ont été testés sur le terrain. Néanmoins, la nature itérative cyclique de l’ADR devrait nous permettre de sortir de l’étude avec un outil utile qui pourra être encore amélioré lors de sa mise en œuvre. La nature réflexive du MARC et l’implication des membres de l’organisation ont apporté des avantages supplémentaires en aidant à créer une culture de sécurité et d’apprentissage tout au long de la vie.

Comme l’informatique est un élément si important de la création d’un avantage concurrentiel pour les institutions financières, la cybersécurité est devenue un sujet crucial. En outre, divers défis rencontrés dans le monde d’aujourd’hui, tels que les pandémies, l’augmentation des cas de cybercriminalité, la réduction du nombre de talents disponibles et compétents et le nombre de nombreux autres problèmes augmentent l’importance de la cybersécurité et la nécessité de cette étude. Il s’agit d’un problème critique pour lequel les organisations ont besoin de solutions.

# Bibliographie

Bacigalupo, M., Kampylis, P., McCallum, E., & Punie, Y. (2016). *Promouvoir la compétence entrepreneuriale des jeunes adultes en Europe : vers un outil d’auto-évaluation*. 611-621. https://doi.org/10.21125/iceri.2016.1150

Boyatzis, R. E. (2008). Compétences au 21e siècle. *Journal of Management Development*, *27*(1), 5-12. https://doi.org/10.1108/02621710810840730

Chicco, D., Tötsch, N., & Jurman, G. (2021). Le coefficient de corrélation de Matthews (MCC) est plus fiable que la précision équilibrée, l’information du bookmaker et la notation dans l’évaluation de la matrice de confusion à deux classes. *BioData Mining*, *14*(1), 13. https://doi.org/10.1186/s13040-021-00244-z

Draganidis, F., & Mentzas, G. (2006). Gestion axée sur les compétences : Examen des systèmes et des approches. *Gestion de l’information et sécurité informatique.*

Draksler, T. Z., & Širec, K. (2018a). Modèle de recherche conceptuelle pour l’étude des compétences entrepreneuriales des étudiants. *Konceptualni raziskovalni model za raziskovanje podjetniških kompetenc študentov.* , *64*(4), 23-33. https://doi.org/10.2478/ngoe-2018-0020

Draksler, T. Z., & Širec, K. (2018b). Modèle de recherche conceptuelle pour l’étude des compétences entrepreneuriales des étudiants. *Konceptualni raziskovalni model za raziskovanje podjetniških kompetenc študentov.* , *64*(4), 23-33. https://doi.org/10.2478/ngoe-2018-0020

Keet, C.M. (2020). *Une introduction à l’ingénierie de l’ontologie*.

Keijzer-Broers, W., & de Reuver, M. (2016). Action Design Research for Social Innovation : Lessons from Designing a Health and Wellbeing Platform. *Actes de la Conférence internationale sur les systèmes d’information (ICIS)*, 1-20.

Man, T. W. Y., Lau, T., & Chan, K. F. (2002a). La compétitivité des petites et moyennes entreprises Une conceptualisation axée sur les compétences entrepreneuriales$. *Journal of Business Venturing*, 20.

Man, T. W. Y., Lau, T., & Chan, K. F. (2002b). La compétitivité des petites et moyennes entreprises Une conceptualisation axée sur les compétences entrepreneuriales$. *Journal of Business Venturing*, 20.

McClelland, D.C. (1973). Tester la compétence plutôt que l’intelligence. *Psychologue américain*, *28*(1), 1.

McCurdy, N., Dykes, J., & Meyer, M. (2016). Recherche en conception d’action et conception de visualisation. *Proceedings of the Beyond Time and Errors on Novel Evaluation Methods for Visualization - BELIV '16*, 10-18. https://doi.org/10.1145/2993901.2993916

Mitchelmore, S., et Rowley, J. (2010). Compétences entrepreneuriales : Une revue de la littérature et un programme de développement. *International Journal of Entrepreneurial Behavior & Research*, *16*(2), 92-111. https://doi.org/10.1108/13552551011026995

Mullarkey, M. T., & Hevner, A. R. (2019). Un modèle élaboré de processus de recherche en conception d’action. *Revue européenne des systèmes d’information*, *28*(1), 6-20. https://doi.org/10.1080/0960085X.2018.1451811

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (NIST SP 800-181). Institut national des normes et de la technologie. https://doi.org/10.6028/NIST.SP.800-181

NIST. (2021). *CADRE NICE pour la main-d’œuvre en cybersécurité*.https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

Petrella, E. (2017, janvier 10). *Cadre de main-d’œuvre en cybersécurité NICE*. NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Prescott, R. K. (2012). *The Encyclopedia of Human Resource Management, Volume 1 : Short Entries* (Vol. 1). John Wiley & Fils.

Richter, A., & Koch, C. (2004). Intégration, différenciation et ambiguïté dans les cultures de sécurité. *Science de la sécurité*, *42*(8), 703-722.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Recherche sur la conception d’actions. *MIS trimestriel*, 37-56.

Stadlhofer, B., Salhofer, P., & Durlacher, A. (2013). *Un aperçu des méthodologies d’ingénierie ontologique dans le contexte de l’administration publique*. 36-42. https://www.thinkmind.org/index.php?view=article&articleid=semapro\_2013\_2\_30\_50039

Subramaniam, T., Nizam, I., & Kamil Eissa, A.M. (2019). L’impact des compétences de base des professionnels de l’informatique sur la réussite des entreprises en Malaisie. *International Journal of Management, Accounting & Economics*, *6*(7), 496-520.

Sure-Vetter, Y., Staab, S., & Studer, R. (2009). Méthodologie d’ingénierie ontologique. Dans *Handbook on Ontologies* (p. 135-152). https://doi.org/10.1007/978-3-540-92673-3\_6

Tharwat, A. (2020). Méthodes d’évaluation de la classification. *Informatique appliquée et informatique*, *17*(1), 168-192. https://doi.org/10.1016/j.aci.2018.08.003

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validité dans la recherche qualitative. *RECHERCHE QUALITATIVE EN SANTÉ*.